FLIR®

IOI HD
User and Installation Guide
CF-5212/CF-5222

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 +1.888.388.3577 or visit the Service & Support page at www.flir.com/security.

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

Proper Disposal of Electrical and Electronic Equipment (EEE)

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

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

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

Document History

Version	Date	Comment
2	April 25, 2017	Second FLIR release

Table of Contents

List of Figures

1 Document Scope and Purpose

The purpose of this document is to provide instructions and installation procedures for physically connecting the CF-5212/CF-5222 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:

⚠

Warning:

- The unit's cover is an essential part of the product. Do not open or remove it.

- Never operate the unit without the cover in place. Operating the unit without the cover poses a risk of fire and shock hazards.

- Do not disassemble the unit or remove screws. There are no user serviceable parts inside the unit.

- Only qualified trained personnel should service and repair this equipment.

- Observe local codes and laws and ensure that installation and operation are in accordance with fire, security and safety standards.

Avertissement:

- *Le cache de l'unité est une partie essentielle du produit. Ne les ouvrez et ne les retirez pas.*

- *N'utilisez jamais l'unité sans que le cache soit en place. L'utilisation de l'unité sans cache présente un risque d'incendie et de choc électrique.*

- *Ne démontez pas l'unité et ne retirez pas ses vis. Aucune pièce se trouvant à l'intérieur de l'unité ne nécessite un entretien par l'utilisateur.*

- *Seul un technicien formé et qualifié est autorisé à entretenir et à réparer cet équipement.*

- *Respectez les codes et réglementations locaux, et assurez-vous que l'installation et l'utilisation sont conformes aux normes contre l'incendie et de sécurité.*

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

> ⚠
>
> **Caution:**
> To avoid damage from overheating or unit failure, assure that there is sufficient temperature regulation to support the unit's requirements (cooling/heating). Operating temperature should be kept in the range -40° to 50°C (-40° to 122°F), with no more than 90% non-condensing humidity.
>
> ***Attention:***
> *Afin d'éviter tout dommage dû à une surchauffe ou toute panne de l'unité, assurez-vous que la régulation de température est suffisante pour répondre aux exigences de l'unité (refroidissement/chauffage). La température de fonctionnement doit être maintenue dans la plage (-40° à 50°C/-40° à 122°F), sans condensation d'humidité supérieur à 90%.*

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 Overview

The IOI HD CF-5212/CF-5222 fixed cameras provide real-time, H.264 and MJPEG streaming video with the highest quality image and video analytics. Featuring a compact, sophisticated and aesthetic mechanical design, the lightweight CF-5212 and CF-5222 cameras are easy to install and operate. Two models are available:

- The CF-5212 is a 1.3 megapixel, HD 720p device.

- The CF-5222 is a 2.1 megapixel, Full HD 1080p device

The cameras include a DC-Iris lens with True Day/Night performance. They provide real-time, H.264 and MJPEG streaming video with the highest quality image. The lightweight, weatherproof, indoor/outdoor cameras are easy to install and operate and feature a compact, sophisticated and aesthetic mechanical design.

Figure 1: IOI HD Analytic Fixed IP Camera

The IOI HD fixed camera delivers outstanding analytic performance. It offers enhanced detection, even of small objects from a distance, even in scenes where there are large or multiple objects and movement in up to 80% of the frame. The system can detect sophisticated intruders and enable the identification of people standing upright, which reduces false alarms.

The camera's video analytics provides alarms when it automatically detects specific events, such as region entrance, fence trespassing, tripwire crossover, which trigger an automatic notification. You can define the events and location in the video of the image that can be detected with user-customizable rules, positioning criteria, responses, and scheduled actions.

⚠️

Caution:

If you are using FLIR's Latitude VMS, we recommend that you configure the camera's settings via the AdminCenter. This is because the camera's web-based interface might be overwritten by Latitude settings. Refer to the Latitude online help for information regarding configuring camera settings.

Attention:
Si vous utilisez le logiciel de gestion de vidéo Latitude de FLIR, nous vous conseillons de configurer les paramètres de la caméra via l'AdminCenter. En effet, l'interface Internet de la caméra peut être remplacée par les paramètres Latitude. Veuillez consulter l'aide en ligne Latitude pour de plus amples informations sur la configuration des paramètres de la caméra.

2.1 Features

The camera supports the following analytic functions:

- Analytic relay events
- Unattended baggage detection
- Stopped vehicle detection
- Automatic depth calibration

- Reduced false alarm rate
- Intrusion detection
- Loitering detection

- Increased detection distance
- Object removal detection
- Camera tampering detection

The camera includes the following key general features:

- Advanced video analytics
- Low lux
- 2D/3D noise reduction
- Detection event-driven alarms
- Built-in web application/ web server
- FTP upload (up to two addresses)
- Up to two E-mail SMTP alarms (excluding analytic alarms)
- ONVIF-conformant
- Sequential snapshot numbering
- Security IP restricted access allow/deny list

- Superior intruder detection
- True Day/Night (IRC)
- dWDR
- Alarm input driven events
- HTTP streaming MPEG
- Upload alarm images to FTP (excluding analytic alarms)
- UPnP support
- RTSP support
- SNMP v1/v2/v3 SNMP traps
- Multiple users

- Customizable rules and actions
- Progressive scan CMOS sensor
- True multi-shutter WDR
- Relay output actions on alarm
- H.264 and MJPEG compression
- Hand-off to PTZ camera
- BNC analog video output
- Per-user permissions
- Supports PoE/12VDC/ 24VAC
- Group permissions

2.2 Package Contents

Before proceeding, check that the box contains the items listed here. If any item is missing or has defects, do not install or operate the product. Contact your dealer for assistance.

IP Fixed Analytic Camera

Back focus adjuster

1x 3-pin male connector
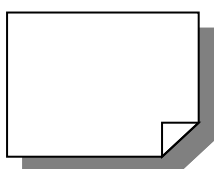
Quick Installation Guide

CD with bundled software and documentation

Figure 2: Package Contents

Related Documentation

- *IOI HD CF-5212/CF-5222 Quick Installation Guide*
- *DNA 2.1 User Manual*
- *IOI HTML Edition Units User's Guide*

3 Introduction to the CF-5212/CF-5222 IP Fixed Camera

This chapter provides information about the camera hardware for reference before installation. The connectors included on the camera's connector panel are described.

- Camera Dimensions
- Camera Connections
- Connecting the Unit to the Network

3.1 Camera Dimensions

The mechanical dimensions of a CF-5212/CF-5222 Fixed IP Camera are shown below.
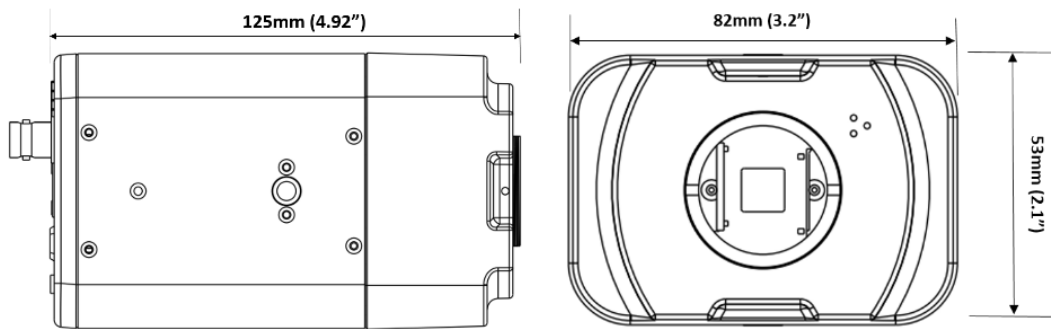
Figure 3: CF-5212/CF-5222 Camera Dimensions

3.2 Camera Connections

Figure 4 shows the connectors and reset button on the connector panel of the CF-5212 and CF-5222 cameras. The connectors, pin numbers and signal definitions related to each pin are listed below.
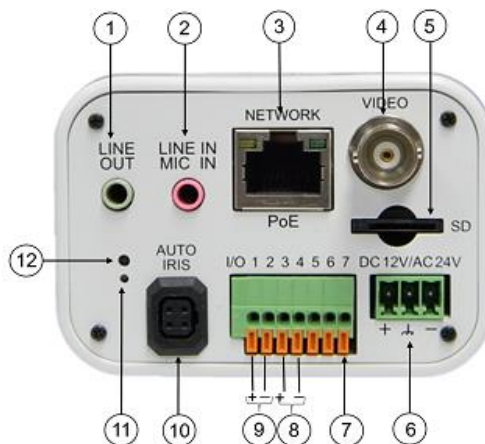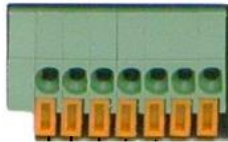
Figure 4: CF-5212/CF-5222 Camera Input/Output Connections

ID	Connector Name	Pin Number/ Connector Type	Definition	Description
1	**Line Out**		Audio out	2-way audio transmission
2	**Line In/Mic In**		Audio in	
3	**Network/PoE**	RJ45, Network LEDs	10/100 Mbps Ethernet/PoE	Power over Ethernet and Network Port
4	**Video**	BNC	Analog video	Connect video coax cable
5	**SD**		microSD card slot	Not supported
6	**DC 12V/AC 24V**	1 – Power (+) 2 – Reserved 3 – GND (-)	12V DC	3-pin power terminal block
		1- Power (+) 2- Earth GND 3- Power (-)	24V AC	
7 to 9	**I/O 1-7**	1 - Output (+) 2 - Output (-)	Alarm output	7-pin I/O terminal block
		3 - Input (+) 4 - Input (-)	Alarm input	
		5 – GND	Grounding	
		6 - D (-) 7 - D (+)	Reserved Do NOT connect	
10	**Auto Iris**	DC iris lens connector	DC iris port	Connect cable from lens
11		N/A	Power LED	Power indication (Green LED indicates Power On)
12		N/A	Reset	Resets full factory defaults

3.2.1 Alarm Input/Output Pin-out

The alarm input and output connections are shown below.

Pin No.	Designation	Terminal Block Alarm Connections
1	Output (+)	
2	Output (-)	
3	Input (+)	
4	Input (-)	

3.3 Connecting the Unit to the Network

A Cat 5 Ethernet cable is recommended for network connection. For best transmission quality, the cable length should not exceed 100 meters (328 feet). Connect one end of the Ethernet cable to the Network/PoE port on the connector panel and plug the other end into the network switch or PC. Check the status of the link and activity LEDs. The LEDs on the Network/PoE port illuminate green (indicating a stable network connection) or flashing yellow (to indicate network activity). If the LEDs are unlit, check the LAN connection.

> **Note:**
> An Ethernet crossover cable can be used when connecting the CF-5212/CF-5222 camera directly to the PC.

3.3.1 Connecting Power to the Camera

The camera can be powered by Power over Ethernet (PoE) or by an external 12VDC or 24VAC adaptor (not included in the package).

- If using an external power supply, connect the power leads or three-pin power terminal block to the power supply.
- If using PoE, make sure that a Power Sourcing Equipment (PSE) device is used in the network.

Make sure the camera's power cable is properly connected. All electrical work must be performed in accordance with local regulatory requirements.

4 System Requirements

To access the camera via a web browser, ensure that your PC has the proper network connection and meets system requirements as described below.

Item	Minimum System Requirement
Personal Computer	Minimum: Intel® Core™ i5-2430M @ 2.4 GHz, 4GB RAM Recommended: Intel® Core™ i7-870 @ 2.93 GHz, 8GB RAM
Operating System	Windows XP, 7, 8, 8.1, and 10
Web Browser	Microsoft Internet Explorer 9, 10, or 11
Network Card	10BaseT (10 Mbps), 100Base-TX (100 Mbps), or 1000BaseT (1000Mbps) operation
Viewer	ActiveX control plug-in for Microsoft IE

5 Installation

Follow the instructions below for indoor and outdoor installation of the camera.

Related Links

- Outdoor Installation
- Lens Mounting
- Initial Camera Configuration
- Mounting Instructions

5.1 Outdoor Installation

Read the instructions provided in this chapter thoroughly before installing the camera. Following are additional considerations for outdoor installation:

- For outside wiring installation, always use weatherproof equipment, such as boxes, receptacles, connectors, etc.

- For electrical wiring, use the properly rated sheathed cables for conditions to which the cable will be exposed (for example, moisture, heat, UV, physical requirements, etc.).

- Plan ahead to determine where to install infrastructure weatherproof equipment. Whenever possible, ground components to an outdoor ground.

- 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

5.2 Lens Mounting

Before installing your camera, install the camera lens.

Note:
The camera lens is sold separately and should be selected to match the needs of the scene and to optimize the use of the camera capabilities. See Mounting and Lens Accessories.

5.2.1 Selecting the Proper Lens

5.2.1.1 DC Auto Iris vs. Manual Iris Lens

A DC auto iris lens is required when operating the camera in *Auto Iris* exposure mode. *Auto iris* mode is recommended for use in indoor environments with mixed lighting sources, where the main source is fluorescent lighting and natural lighting enters the scene through windows and other exposed areas. In all other cases, *Auto Shutter* exposure mode is recommended. The camera can operate in one of the following three exposure modes: *Manual* (using set values for shutter and iris), *Auto Iris,* and *Auto Shutter*. *Auto Shutter* and *Manual* modes do not require an auto iris lens. A manual iris lens can be used instead.

5.2.1.2 Setting the Camera's Focal Length

Focal length determines the scene's viewing angle, or, in other words, the dimensions of the scene which will be generated by the camera. The trade-off for focal length is between the width of the scene and the magnification of objects appearing in the scene. The longer the focal length is, a narrower scene will be achieved, while the size of objects will increase. Greater size means that more pixels will be used to represent each object, and greater level of details will be present.

In a similar manner, the shorter the focal length is, the smaller the size of each object will be, while the captured scene will become wider.

> ⊘
>
> **Note:**
> Use a short focal length to cover a wide area and detect objects at close distances. Use a long focal length to achieve greater detection distances while narrowing the Field of View.

After you select your lenses and see the amount of detail provided, consider your security surveillance coverage, camera locations, and any additional needs that may be discovered. Consult your FLIR representative if you have any questions.

To mount a lens on the CF-5212/CF-5222 camera

1. Remove the plastic insert covering the threaded camera lens mount.

    > ◈
    >
    > **Tip:**
    > 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 (see figures below).

Figure 5: C-CS Mount Adaptor

> ⊘
>
> **Note:**
> The camera is NOT shipped with a C to CS adapter. The adaptor is shipped only with lenses that require it in order to work with the camera.

3. Align the lens threads into the lens mount and screw in the lens.

Figure 6: Installed C-CS Mount

4. If your lens has a DC auto iris, plug the auto iris cable from the lens assembly into the AUTO IRIS port of the camera.

Figure 7: Auto Iris Port Connection

Tip:
If there are problems focusing, it might be necessary adjust the back focus. See Back Focus Adjustment (page 119).

5.3 Initial Camera Configuration

> ⚠️
>
> **Caution:**
> If you are using Latitude, we recommend that you configure the camera's settings via the
> AdminCenter. This is because the camera's web-based interface might be overwritten by Latitude
> settings. Refer to the Latitude online help for information regarding configuring camera settings.
>
> ***Attention:***
> *Si vous utilisez Latitude, nous vous conseillons de configurer les paramètres de la caméra via
> l'AdminCenter. En effet, l'interface Internet de la caméra peut être remplacée par les paramètres
> Latitude. Veuillez consulter l'aide en ligne Latitude pour de plus amples informations sur la
> configuration des paramètres de la camera.*

To perform the initial camera configuration

1. Unpack the camera and remove the protective cover.

2. Connect one end of the network Cat 5 Ethernet cable to the RJ45 connector on the
   camera's connector panel.

3. Connect the other end of the network cable to a Power Sourcing Equipment (PSE)
   device, such as a switch.

4. Verify that the LEDs on the RJ45 connector illuminate green (indicating a stable network
   connection) and flashing yellow (to indicate network activity).

5. Do the following:

   a. Copy and run `dna.exe` (see note below) from the included CD.
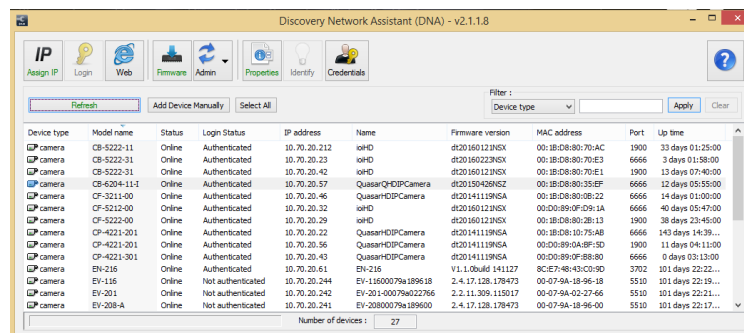
   > 🧭
   >
   > **Note:**
   > DNA is a user-friendly utility that is designed to easily discover and configure FLIR
   > edge devices on a network. The IOI HD fixed camera is supported by DNA version
   > 2.0.4.8 and above. For instructions how to use DNA, click here to download the *DNA
   > User Manual* from the *Tools* section.

   b. Click the ![FLIR icon] icon.

   c. Select the unit requiring IP assignment.

Figure 8: Discovered IP Devices

d. Right-click the mouse and select the assigned IP address or click the **Assign IP** button to open the **DNA Assign IP** dialog box.

> **Note:**
> The camera default IP Address and the subnet mask IP Address are automatically supplied by the DHCP server.

e. In the dialog box that is displayed, enter values for the *IP Address, Gateway and Netmask*.

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

Figure 9: DNA Assign IP Dialog Box

g. Disconnect the Ethernet cable. The camera is ready for deployment (mounting) in a site installation.

> **Note:**
>   1. The camera can be connected to a PC for bench installation via an Ethernet cross-cable.
>   2. The camera default IP Address is automatically set by the DHCP server. If using Latitude, the Address must be set manually.

> **Tip:**
> A camera setup adapter, such as Veracity Pinpoint, can be used to connect a laptop directly to the camera when using PoE.

5.4 Mounting Instructions

The following are mounting instructions for the CF-5212 and CF-5222 fixed IP cameras.

> ⚠️
>
> **Caution:**
> To avoid damage from overheating or unit failure, assure that there is sufficient temperature regulation to support the unit's requirements (cooling/heating). Operating temperature should be kept in the range -40° to 50°C (-40° to 122°F), with no more than 90% non-condensing humidity.
>
> ***Attention:***
> *Afin d'éviter tout dommage dû à une surchauffe ou toute panne de l'unité, assurez-vous que la régulation de température est suffisante pour répondre aux exigences de l'unité (refroidissement/chauffage). La température de fonctionnement doit être maintenue dans la plage (-40° à 50°C/-40° à 122°F), sans condensation d'humidité supérieur à 90%.*

To mount the camera, follow one of these procedures:

- For outdoor installations using a typical protective camera housing:

  a. Thread the wires through any of the infrastructure and brackets (e.g. pole bracket/corner bracket/etc.) as needed as well as through the wall bracket arm.

  b. Bolt the wall bracket (arm) to the prepared surface.

  c. Loosen the screws or unlatch the camera housing lid, open the housing and loosen the plastic cable glands (cable fittings).

  d. Thread the cables through the cable glands into the camera housing.

Figure 10: Cable Gland

  e. Attach the camera housing to the wall bracket (arm) using the provided screws and wrench.

  f. Remove the housing plate (base for camera) and using the provided camera mount screw, thread the screw through the plate into the camera's bottom mounting socket.

  g. Put the camera mounted on the base plate back in the housing. Adjust forward positioning when you adjust the lens.

  h. For housings with internal blowers and heaters, connect the wiring to the camera housing terminals (power input) according to the manufacturer's instructions for heaters (heater output) and fans (blower output) that the camera housing features. Connect any ground (GND) to the camera housing ground connection.

i. Connect the cables and wiring to the camera. See Figure 4: CF-5212/CF-5222 Camera Input/Output Connections.

> **Note:**
>
> For outdoor installation, the camera must be installed in a protective housing such as a CF-X200-00 camera housing. See the figure below.

Figure 11: CF-X200-01 Camera Housing with Bracket

6 Using the DNA Utility to Search and Access the Camera

The Discovery Network Assistant (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.

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 the camera is managed by FLIR's Horizon or Meridian NVR and is configured as a DHCP server, Horizon or Meridian automatically assigns the camera an IP address. Configure the camera with *DHCP-enabled*.

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.

The camera must be made accessible for setting network addresses.

Note:

The IOI HD fixed camera is supported by DNA version 2.1 and above. For detailed guidelines about DNA and its usage, refer to the *DNA 2.1 User Manual*, which is included in the CD provided with the camera, or click here to download the *DNA User Manual* from the *Tools* section.

---

7 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` which can be found in the DNA utility folder in the supplied CD, or click the DNA icon [FLIR icon] .

3. In the DNA application, click the **DNA** button.

4. If the Windows Firewall is enabled, a security alert window pops up.

5. To continue, click **Allow Access**. Latitude users should consult the Latitude Installation Instructions on disabling the Windows Firewall.
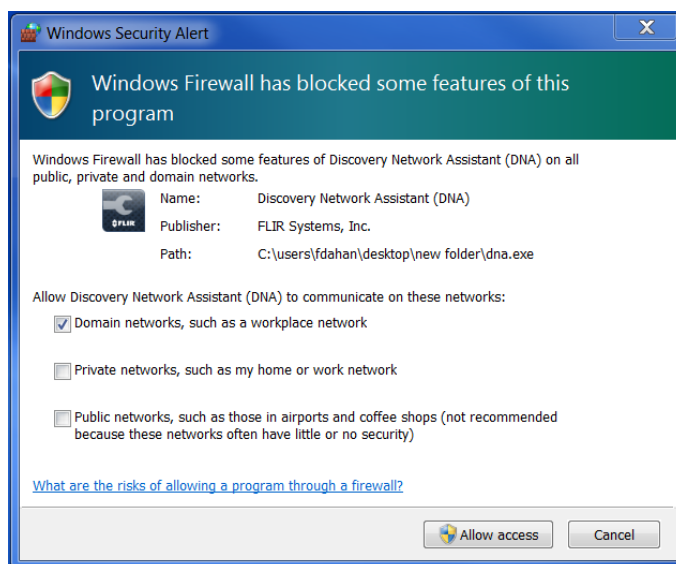
Figure 12: Windows Firewall Screen

6. 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.

Figure 13: Discovered IP Devices

7. 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.
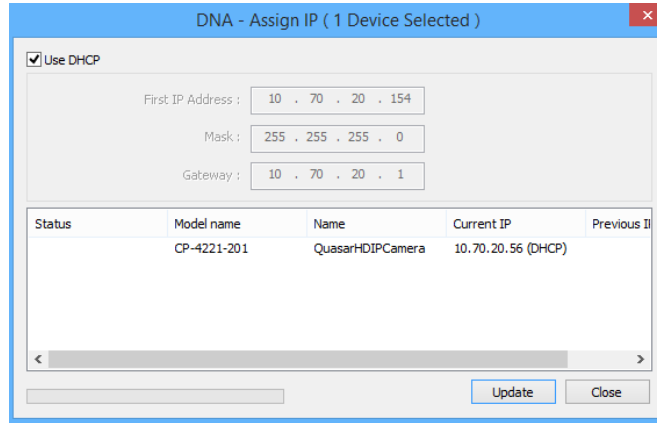
Figure 14: DNA Assign IP – Use DHCP Dialog Box

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

8. To access DNA, 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.

   a. For Static IP (recommended for Latitude users):
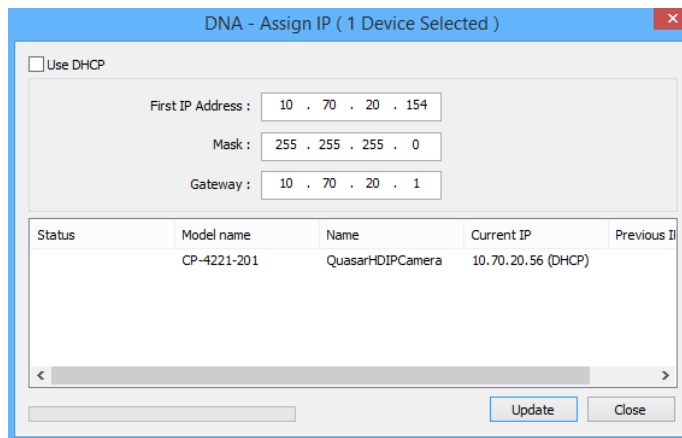
Figure 15: DNA Assign IP – Static IP Dialog Box

      i. Do not select the *Use DHCP* checkbox. This is recommended for security purposes and for and Latitude users. 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.

9. 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.

Figure 16: Login Dialog Box

10. 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.

3. If the password is changed and the Latitude AdminCenter Discovery feature is in use, deselect all other proprietary types. Select *IOimage* as the Unit Type so that the new password can be configured in the Latitude Discovery tab settings.

-   If the **User Account Control** dialog 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 settings 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**.
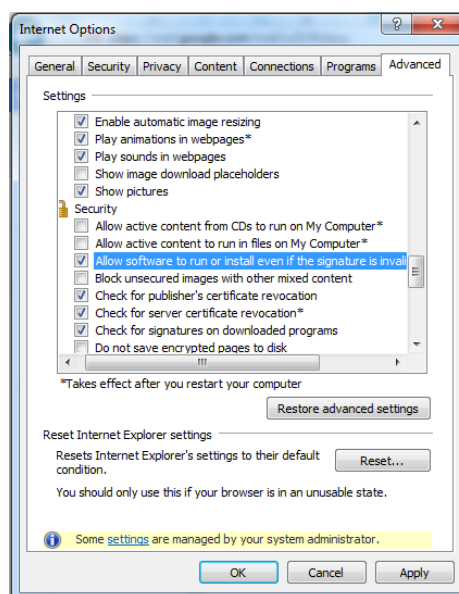
Figure 17: IE Tools > Internet Options > Advanced Window

- If the existing certificate is old or invalid, the ActiveX installation may fail in systems that are not connected to the internet and therefore cannot update their security certificates. In this case, the `Setup.exe` file in the ActiveX folder on the supplied CD should be run. The user can then continue with the installation.

| Internet Explorer blocked this website from installing an ActiveX control. | What's the risk? | Install | × |
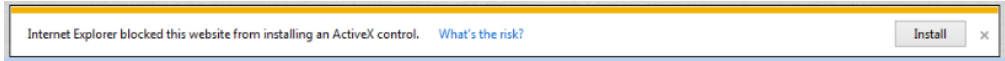
Figure 18: ActiveX Installation Error Message

11. 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 **IOimage** as the Unit Type so that the new password can be configured in the Discovery tab settings.

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 > Basic** screen.

12. 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. For information on how to install the new player, uninstall a previous player, and clear temporary Internet files, see Installing and Deleting the Web Player (page 116).

8 Adjusting and Framing-Up the Camera View

After the camera is connected to the network and running, it is necessary to frame-up the scene and adjust the camera settings to optimize the picture for the individual scenes. If Latitude is being used, consider scheduling different settings for changing ambient conditions throughout the day, week, month or seasons.

To adjust and frame-up the camera view

1. After the unit's web interface opens, adjust the zoom and focus.

> **Tip:**
> To view greater image detail for more accurate high-definition focusing, on the web interface **Home** page, click the **Full Screen** ⊠ button and use the full screen view to check the focus.

> **Note:**
> Best focusing results can be achieved when the lens iris is fully open (such as at night in low light). This prevents loss of sharpness if light levels are reduced at night.

2. If the lens cannot maintain the focus throughout its zoom range, adjust the back focus. See Back Focus Adjustment (page 119).

3. From the unit's **Camera > Exposure** screen, do one of the following:

   a. If you selected Shutter WDR *On* from the Misc screen, select the default mode (*WDR Multiple Shutter)*.

   b. If you selected Shutter WDR *Off* from the Misc screen, select the default mode (*Auto Shutter)*.

4. Save changes and complete the focusing steps.

5. When finished, set your exposure settings as needed.

9 Configuration and Operation

The IOI HD camera is provided with a browser-based configuration interface for video playback and recording. If FLIR's Latitude VMS is used, many of the configurations and features of FLIR's VMS provide additional configuration and automation options for the camera.

This section includes the following information:

- Browser-Based View Introduction

- Live Screen

- System Tabs

- Streaming Tab

- Camera Tab

- Log Out

9.1 Browser-Based Viewer Introduction

The figure below explains the IOI HD camera's browser-based user interface.

Figure 19: Browser-Based User Interface

The user interface displays the following information:

- The Navigation Bar is displayed in the center of the screen containing **Live** and **Settings** buttons.

  - **Live Button**
    The **Live** screen opens by default when the camera logs on. It is used to monitor live video of the targeted area, adjust the display size, take snapshots of the view area, stop/start video streaming, record video in a designated file location, activate or de-activate a loudspeaker (audio function), and to perform a digital zoom. An explanation of the items on the screen is included below and in section 9.2.

  - **Settings Button**
    Clicking the **Settings** button opens the **Settings** screen, whose sidebar which includes three tabs − **System, Streaming,** and **Camera** − that are used for to configure system settings.

    - **System Settings**
      The administrator can configure settings for basic system parameters, security, network operation, events, recording, storage, system maintenance, and more. Details are discussed in System Settings.

    - **Streaming Settings**
      The administrator can modify video and audio settings on this page. Details are discussed in Streaming Settings.

    - **Camera Settings**
      The administrator can adjust many of the camera settings on this page, such as Exposure, Picture Adjustment, IR Function, and TV System. Details are discussed in Camera Settings.

    - **Streaming Settings**
      The **Analytics** tab is used for configuring video analytics settings for depth, rules, responses, scheduled actions, on-screen display, firmware, and backup & restore. Details are discussed in Analytics.

- The Language Bar is displayed to the right of the Navigation Bar. Supported languages include English, Spanish, Japanese, Russian, and Simplified Chinese.

- The *Log out* link is located to the right of the Language Bar. Click the *Log Out* link to exit the application or log into the camera with a different username and password. See Log Out.

- The camera model number is displayed under the *Log out* link.

- The current date and time are displayed under the model number.

- The video format is displayed and can be selected to the left of the date and time.

- Function buttons are displayed to the left of the Live View window. These are discussed in the following section. In the center of the interface is the Live View window, which displays the image that the camera is monitoring.

- The Live View window in the center of the interface displays the monitored scene.

- The camera's firmware version is displayed under the Live View window on the right side.

- The **Arm/Disarm** button is displayed under the Live View window. Click **Arm** to start the analytics engine. Click **Disarm** to stop the analytics engine.

- The **Clear Alarms** button is displayed under the **Arm/Disarm** button. Click **Clear Alarms** to stop the alarms and return analytics to their initial stage.

9.2 Live Screen

The camera's **Live** screen is used to monitor live video. See Figure 19: Browser-Based User Interface (page 33). Double-clicking the Live window opens the **Info** dialog box, which displays key details about the video stream:
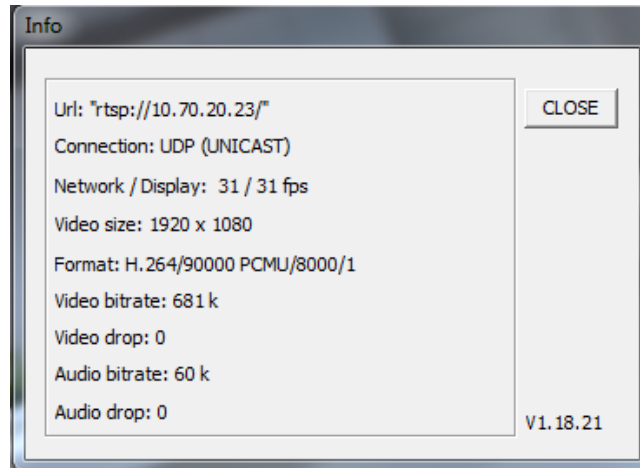
Figure 20: Live Video Info Dialog Box

To view the Live View screen in Fullscreen mode

      1.   Double-click the screen. The image is displayed in the entire monitor screen.

To exit Fullscreen mode

      1.   Click **CLOSE**. The **Live View** screen is displayed in the monitor screen.

The *View Mode* pane in the **Live** screen includes the following function buttons:
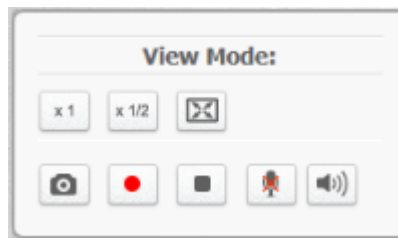
Figure 21: View Mode Pane

Full-Window Display

Click this button to view the live video in the full Live Video window.

Half-Window Display

Click this button to view the live video in half of the Live View window.

Full-Screen Mode

Click this button to view the live video on the full screen of your monitor. Click the ESC (Escape) key on your keyboard to exit Full-Screen Mode.

Snapshot

Click this button to automatically save the JPEG snapshots in the specified location. The default location to save snapshots is: C:\.To change the storage location, refer to File Location.

Note:

When using Windows 8 OS, the storage location cannot be C:\. You must define a storage location that does not require Administrator privileges on the PC.

Record/Pause

Pressing the **Recording** button stores recordings from the Live View in the location specified on the local hard drive, which can be configured in the **File Location** screen. The default storage location for the web recording is: C:/. Refer to File Location for details.

Note:

When using Windows 8 OS, the storage location cannot be C:\. You must define a storage location that does not require Administrator privileges on the PC.

Video Streaming Restart/Stop

Press the **Stop** button to disable video streaming and to display the live video as black. Press **Restart** to show the live video again.

Mic

The **Microphone** button allows the local site to talk to the remote site. Click the button to switch it on/off. This function is available only to a user who has been granted this privilege by the Administrator. Refer to User in the Security section for further details.

Speaker

Click the **Speaker** button to mute/activate the audio. This function is available only to a user who has been granted this privilege by the Administrator. Refer to User in the Security section for further details.

9.3 System Tab

The **Settings** tab in the Navigation Bar opens the sections in the sidebar that are used for configuring the camera. The sections available for configuration include System, Streaming, Camera, and Analytics.

 ⊘

Note:

The **System** screen is accessible only by the Administrator.

9.3.1 System Settings

The **System** section includes the following tabs:
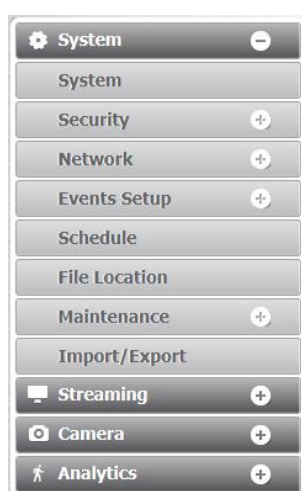
Figure 22: System Section Tabs

- System
- Security
- Network
- Events Setup
- Schedule
- File Location
- Maintenance
- Import/Export

System Screen

The **System** screen is used for entering the camera's friendly name and date and time settings. Click the **System** tab in the sidebar. The **System** screen is displayed.

Figure 23: System Screen

The **System** screen includes the following fields:

Host Name

The host name is for camera identification. If the alarm function is enabled and is set to send an alarm message by Mail or FTP, the host name entered here is displayed in the alarm message. See Events Setup.

Time Zone

Select the time zone from the drop-down menu.

Enable Daylight Saving Time

To enable daylight saving time, check the *Enable daylight saving time* box. Then specify time offset (number of hours or minutes difference between daylight saving time and standard time). The format for time offset is [hh:mm:ss]. For example, if the amount of time offset is one hour, enter 01:00:00 in the field. Finally, enter the start date and time for daylight saving time, and end date and time for daylight saving time.

Time format

Enables a choice of formats: either year, month and day (yyyy/mm/dd) or day, month and year (dd/mm/yyyy).

Sync with Computer Time

Select this button to synchronize video date and time display with the PC. You can change the PC date and time in the respective text box.

Manual

The Administrator can set video date and time manually. Entry format should be identical with that displayed to the right of the text box.

Sync with NTP Server

Network Time Protocol (NTP) is an alternate way to synchronize the camera's clock with an NTP server. Select *Sync with NTP Server.* In the *NTP server* text box, enter the network time server host name or IP address to synchronize. Then, from the *Update interval* drop-down list, select an update interval (every hour, day or week). For further information about NTP, visit www.ntp.org.

Click **SAVE** when finished.

9.3.2 Security Screens

Clicking the **Security** tab in the **System** sidebar opens a drop-down menu with the following screens:

- User
- HTTPS
- IP Filter
- IEEE 802.1X

9.3.2.1 User

The **User** screen is used for entering and managing user credentials and privileges, as well as configuring authentication settings.

Figure 24: User Screen

Admin Password

Change the administrator's password by entering the new password in both text boxes. The input characters/numbers are displayed as dots for security purposes. After clicking **SAVE**, the web browser asks the Administrator for the new password (maximum 14 digits).

Note:

The following characters are valid: A-Z, a-z, 0-9,!#$%&'-.@^_~.

Add user

The user name and passwords are limited to 14 characters. There is a maximum of 20 user accounts.

To add a new user

1. Type the new user name and password in the respective fields.

2. Select the appropriate check boxes to give the user Camera Control, Talk and Listen permissions.

    - *I/O access* – Basic functions that enable you to view video when accessing to the camera.

    - *Camera control* – Allows you to change camera parameters on the **Camera** tab.

    - *Talk* – *Talk* allows the user at the local site to talk from the remote site to the administrator

    - *Listen* – *Listen* allows the user at the local site to listen from the remote site to the administrator.

    - *Analytics* – Allows the user to define analytic parameters from the **Analytics** tab

3. Click **ADD**.

Manage User

- To delete a user, click the *User name* drop-down list and select the user. Click **DELETE** to remove the user.

- To edit a user, click the *User name* drop-down list and select the user. Click **EDIT** to edit the user's password and privileges.

    Note:

    You <u>must </u>enter the user password and also select the authorized function(s).
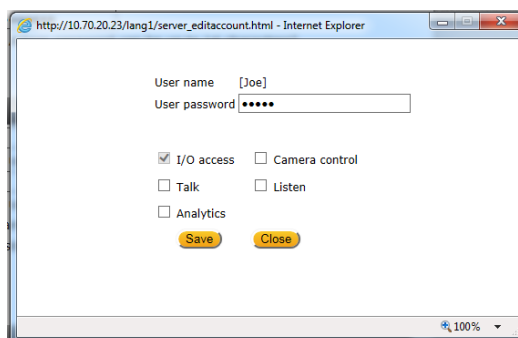
Figure 25: Edit User Account Dialog Box

- Click **Save** to modify the account credentials and privileges, or **Close** to discard changes.

Streaming Authentication Setting

From the drop-down list, select one of the following options:

- *Disable* – Do not use streaming authentication (default setting).

- *Basic* – A form of authentication that uses unencrypted base64 encoding. Basic Authentication should generally only be used where transport layer security, such as HTTPS, is provided.

- *Digest* – A form of authentication used over RTSP in which credentials are encrypted when transmitted.

Click **SAVE**.

9.3.2.2 HTTPS

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.

HTTPS allows secure connections between the camera and web browser using Secure Socket Layer (SSL) or Transport Layer Security (TLS) to protect camera settings and username/password info. A self-signed certificate or a CA-signed certificate is required to implement HTTPS.

To create a self-signed certificate

Before a CA-issued certificate is obtained, users can first create and install a self-signed certificate. Under the **Security** category, click the **HTTPS** tab in the sidebar to display the following screen.
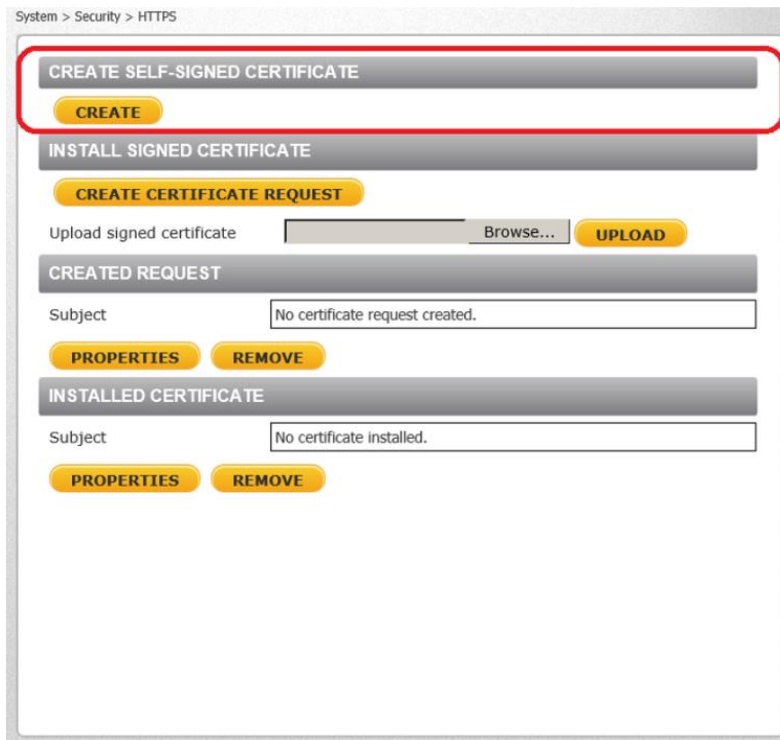
Figure 26: HTTPS Screen – Create Self-Signed Certificate

1. On the **HTTPS** page, click **CREATE** under *Create Self-Signed Certificate.* The **Create Self-Signed Certificate** dialog box opens.

Figure 27: Create Self-Signed Certificate Dialog Box

2. Enter the information in the appropriate field. A definition of each of the required fields follows.
   - *Country* – 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.
   - *State or province* – Enter the local administrative region.
   - *Locality* – Enter other geographical information.
   - *Organization* – Enter the name of the organization to which the entity identified in *Common Name* belongs.
   - *Organizational Unit* – Enter the name of the organizational unit to which the entity identified in the *Common Name* field belongs.
   - *Common Name* – Indicate the name of the person or other entity that the certificate identifies (often used to identify the website).
   - *Valid days* – Enter the period in days (1 ~ 9999) to indicate the valid period of certificate.
3. Click **OK** to save the certificate request after completion. The details are displayed in the *Subject* field of the *Installed Certificate* section.
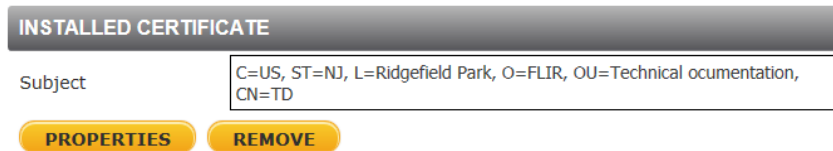
Figure 28: Installed Certificate Section

4. To view the details of the Installed Certificate, click **PROPERTIES**. The details are displayed in the **Certificate Properties** dialog box. If you want to remove the certificate, click **REMOVE**.
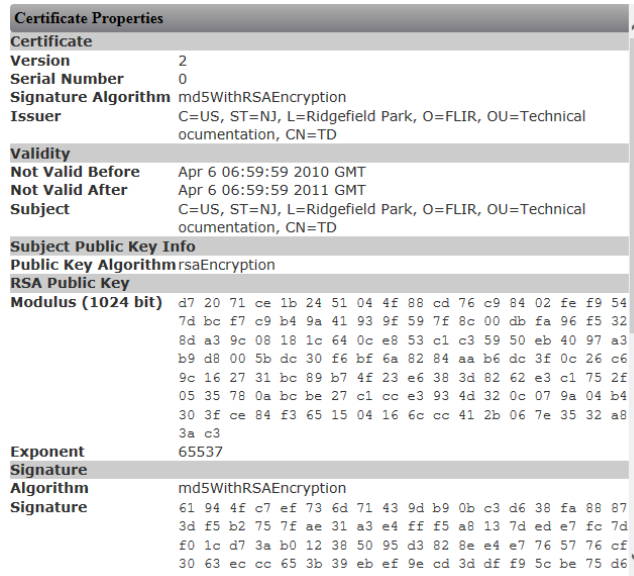
Figure 29: Certificate Properties

5. When the signed certificate is returned from the CA, click **Browse** in the *Install Signed Certificate* section to locate the file.

6. Click **UPLOAD** to install the certificate, as seen in Figure 30.
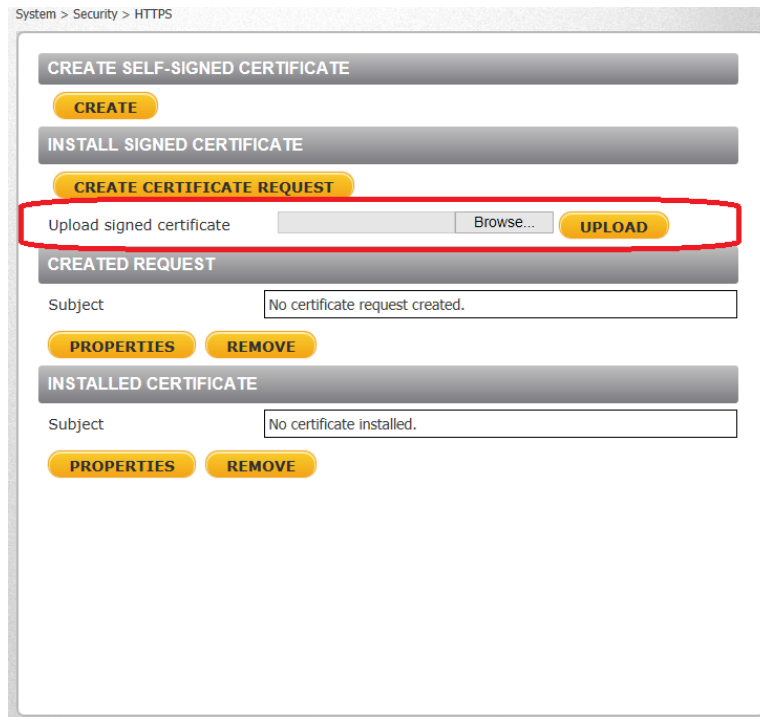
Figure 30: HTTPS Screen – Upload Signed Certificate

To create a certificate request

1. Click **CREATE CERTIFICATE REQUEST** to create and submit a certificate request in order to obtain a signed certificate from a CA.
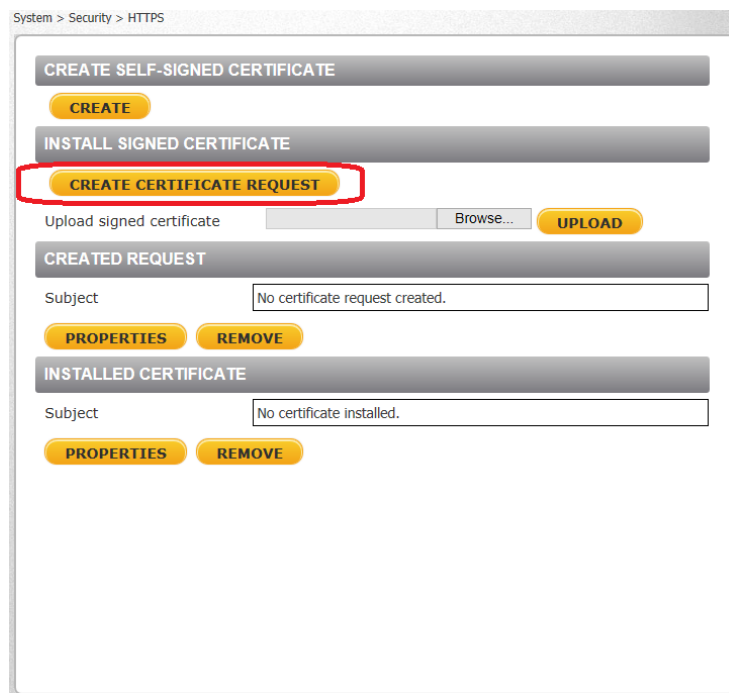
Figure 31: HTTPS Screen – Install Signed Certificate

The **Create Certificate Request** dialog box opens.

Figure 32: Create Certificate Request Dialog Box

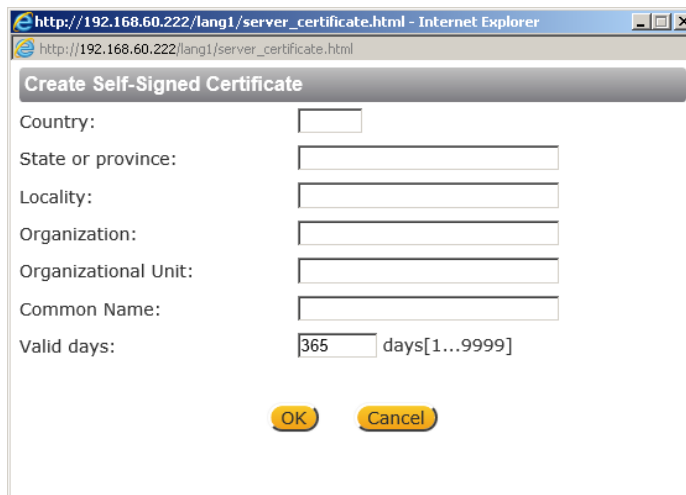2. Enter the information in the appropriate field. A definition of each of the required fields follows.
   - *Country* – Enter a two-letter combination code to indicate the specific country in which the certificate will be used. For instance, type "US" to indicate United States.
   - *State or province* – Enter the local administrative region.
   - *Locality* – Enter other geographical information.
   - *Organization* – Enter the name of the organization to which the entity identified in Common Name belongs.
   - *Organizational Unit* – Enter the name of the organizational unit to which the entity identified in the Common Name field belongs.
   - *Common Name* – Indicate the name of the person or other entity that the certificate identifies (often used to identify the website).
3. Click **OK** to save the details of the certificate request after completion. When the request is complete, the subject of the Created Request is displayed in the *Subject* field

Figure 33: Created Request Subject

4. To view details of the Certificate Request, click **PROPERTIES** below the *Subject* field. The **Certificate Request Properties** dialog box opens. If you want to remove the certificate, click **REMOVE**.

Figure 34: Certificate Request Properties Dialog Box

5. Copy the PEM-formatted request and send it to your CA.

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

9.3.2.3 IP Filter

The IP filter restricts access to the camera by denying/allowing specific IP addresses. Click the **IP filter** tab under the category **Security** in the sidebar to display the following page.
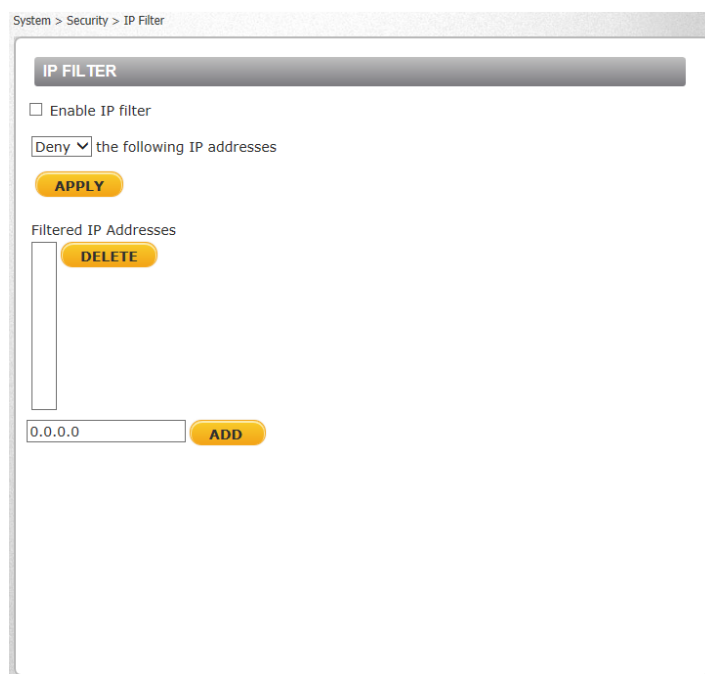
Figure 35: IP Filter Screen

To enable the IP filter

1. Check the box to enable the IP filter function. Once enabled, the listed IP addresses (IPv4) are allowed or denied access to the camera.

2. Select *Allow* or *Deny* from the drop-down list.

3. Click **APPLY** to determine the IP filter behavior.

To add or delete an IP address

1. Enter the IP address in the *Filtered IP Addresses* text box.

2. Click **ADD** to add a new filtered address. The *Filtered IP Addresses* box shows the currently configured IP addresses. Up to 256 IP address entries may be specified.

3. To remove an IP address from the list, select the IP address and then click **DELETE**.

9.3.2.4 IEEE 802.1X

The camera is allowed to access a network protected by 802.1X/EAPOL (Extensible Authentication Protocol over LAN). Users must contact the network administrator to obtain certificates, user IDs, and passwords.
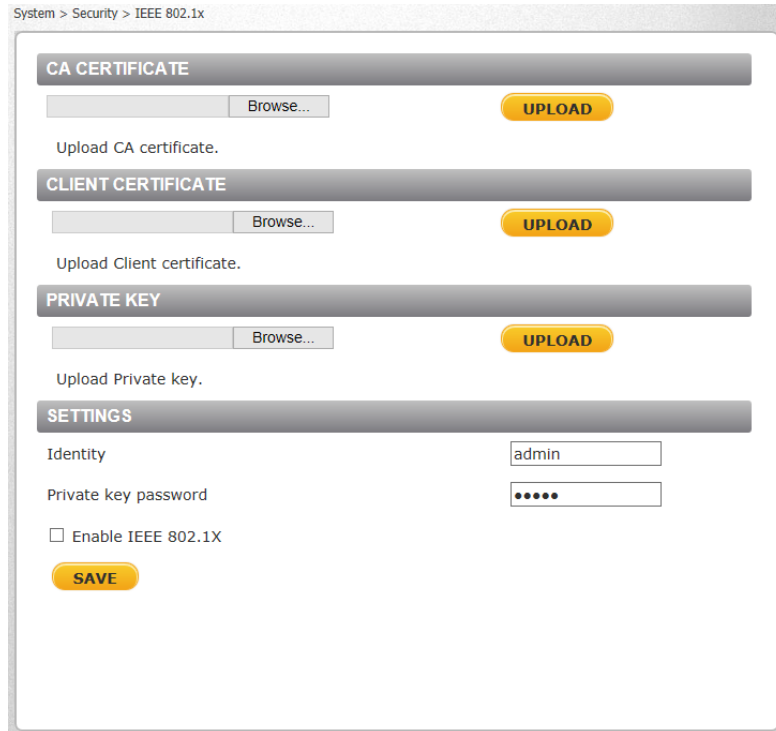
Figure 36: IEEE 802.1X/EAP-TLS Screen

CA Certificate

The CA certificate is created by the Certificate Authority for the purpose of validating itself. Click **Browse** to locate the file and **UPLOAD** to upload the certificate to check the server's identity.

Client Certificate

Upload the Client Certificate to authenticate the camera. Click **Browse** to locate the file and **UPLOAD** to upload the certificate.

Private Key

Upload the Private Key to authenticate the camera. Click **Browse** to locate the file and **UPLOAD** to upload the private key.

Settings

- *Identity* – Enter the user identity (user name) associated with the certificate. Up to 16 characters can be used.

- *Private Key Password* – Enter the password associated with the user identity. Up to 16 characters can be used.

Enable IEEE 802.1X

Select the checkbox to enable IEEE 802.1X security. The setting is disabled by default.

Click **SAVE** to save the IEEE 802.1X/EAPTLS setting.

9.3.3 Network

From the **System** screen, click the **Network** tab.

The following screens are available from the **Network** tab:

- [Basic](#) • [QoS](#) • [SNMP](#) • [UPnP](#) • [DDNS](#) • [Mail](#) • [FTP](#)

9.3.3.1 Basic

The **Basic** screen is used to configure the camera's basic network settings.

Figure 37: Network > Basic Screen

It is possible to connect to the camera with either fixed or dynamic (DHCP) IP address. The camera also provides PPPoE (Point-to-Point Protocol over Ethernet) support for users who connect to the network via PPPoE.

The **Basic** screen is divided into three sections: *General, Advanced* and *IPv6 Configuration*.

General

Select one of the following options in the *General* area for configuring network settings:

- Get IP address automatically
- Use fixed IP address
- User PPPoE

Get IP address automatically

If you select *Get IP address automatically*, you can use the DNA utility, which is provided in the supplied CD, to obtain the IP address from a DHCP server on the network. See Using the DNA Utility to Search and Access the Camera.

> **Note:**
>
> For future reference, record the camera's MAC address, which is found on the camera label.

Use fixed IP address

The camera's default setting is *Use fixed IP address*. Refer to Using the DNA Utility to Search and Access the Camera for login with the default IP address. You may use DNA or enter the IP address in your Internet browser's URL address bar.

To set up a new static IP address

1. Select the *Use fixed IP address* option.

2. Enter the following information:

   - *IP address* – The IP address is necessary for network identification.

   - *Subnet mask* – Used to determine if the destination is in the same subnet. The default value is 255.255.255.0.

   - *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.

   - *Primary DNS* – The primary domain name server that translates host names into IP addresses.

   - *Secondary DNS* – A secondary domain name server that backs up the primary DNS.

To use PPPoE

1. Enter your PPPoE user name and password into the respective fields.

2. Click **SAVE** to confirm the settings.

Advanced

Enter the following advanced parameters in the *Advanced* section of the screen:

- *Web Server port* – The default web server port is 80. Once the port is changed, the user must be notified the change for the connection to be successful. For instance, when the Administrator changes the HTTP port of the camera whose IP address is 192.168.0.100 from 80 to 8080, the user must type in the web browser http://192.168.0.100:8080 instead of http://192.168.0.100.

- *RTSP port* – The default setting of the RTSP port is 554. The range is from 1024 to 65535.

- *MJPEG over HTTP port* – The default setting of MJPEG over HTTP port is 8008. The range is from 1024 to 65535.

- *HTTPS port* – The default setting of HTTPS port is 443. The range is from 1024 to 65535.

- *MTU* – The MTU (Maximum Transmission Unit) is the greatest amount of data that can be transferred in one physical frame on the network. For Ethernet, the MTU is *1500* bytes (default setting). For PPPoE, the MTU is *1492*. The range is from *700* to *1500* bytes.

> **Note:**
>
> Be sure to assign a different port number for each service mentioned above.

Click **SAVE** to save the settings.

IPv6 Address Configuration

IPv6 is not supported.

9.3.3.2 QoS

QoS (Quality of Service) provides differentiated service levels for different types of traffic packets and guarantees delivery of priority services during periods of network congestion. Adapting the Differentiated Services (DiffServ) model, traffic flows are classified and marked with DSCP (DiffServ Code point) values, and as a result receive the corresponding forwarding treatment from DiffServ-capable routers. DSCP configuration settings are entered in the **System > Network > QOS** screen:

Figure 38: QoS Screen

DSCP Settings

The DSCP value range is from 0 to 63. The default DSCP value is 0 (DSCP disabled). The camera uses the following QoS classes: Video, Audio, and Management.

- *Video DSCP* – This class consists of applications such as MJPEG over HTTP, RTP/RTSP and RTSP/HTTP.

- *Audio DSCP* – The camera supports audio.

- *Management DSCP* – This class consists of HTTP traffic (web browsing).

Click **SAVE** when complete.

>
> **Note:**
>
> To enable this function, make sure the switches/routers in the network support QoS.

9.3.3.3 SNMP Settings

The Simple Network Management Protocol (SNMP) enables the camera to be monitored and managed remotely by the network management system. SNMP configuration settings are entered in the **System > Network > SNMP** screen.

Figure 39: SNMP Settings Screen

SNMP v1/v2

- *Enable SNMP v1* or *Enable SNMP v2* – Select the version of SNMP (v1 or v2) to use by checking the relevant box.

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

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

SNMP v3

SNMP v3 provides important security features including:

- Confidentiality – Encryption of packets to prevent snooping by an unauthorized source.

- Integrity – Message integrity to ensure that a packet has not been tampered with in transit including an optional packet replay protection mechanism.

- Authentication – To verify that the message is from a valid source.

To enable the SNMP v3 protocol, enter the appropriate data and passwords requested:

- *Enable SNMP v3* – Select the checkbox.

- *Security Name* – See note below.

- *Authentication Type* – Select *MD5* or *SHA* from the drop-down list. See note below.

- Authentication Password – See note below.

- *Encryption Type* – Select *DES* or *AES* from the drop-down list. See note below.

- Encryption Password – See note below.

> **Note:**
> You may have to consult with your System Administrator to activate this function.

Traps for SNMP v1/v2/v3

Traps are used by the camera to send messages to a management system for important events or status changes.

- *Enable traps* – Check this box to activate trap reporting.
    - *Trap address* – Enter the IP address of the management server.
    - *Trap community* – Enter the community to use when sending a trap message to the management system. The default value is *public*.
- Trap Option
    - *Warm start* – A warm start SNMP trap signifies that the SNMP device, such as the camera, performs a software reload.

Click **SAVE** when complete.

9.3.3.4 UPnP

The **System > Network > UPnP** screen enables the Universal Plug-and-Play protocol on your network devices.

Figure 40: UPnP Screen

UPnP Settings

- *Enable UPnP* – If UPnP is enabled and a camera is discovered on the LAN, the icon of the connected camera appears in **My Network Places**, allowing direct access, as seen below.
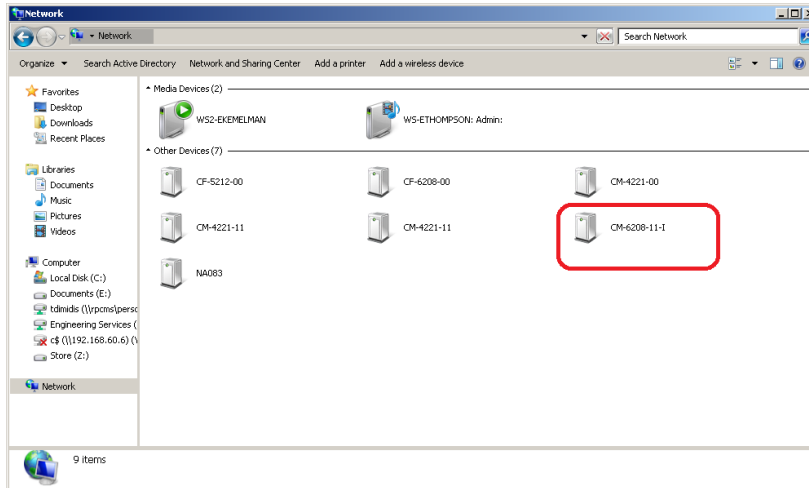
Figure 41: Direct Access to Camera with UPnP Enabled

> **Note:**
> To enable this function, make sure the UPnP component is installed on your computer. Refer to Install UPnP Components for the Windows 7, 8, 8.1, and 10 procedure.

- *Enable UPnP port forwarding* – When UPnP port forwarding is enabled, the camera is allowed to open the web server port on the router automatically.

> **Note:**
> To enable this function, make sure that your router supports UPnP and that it is activated.
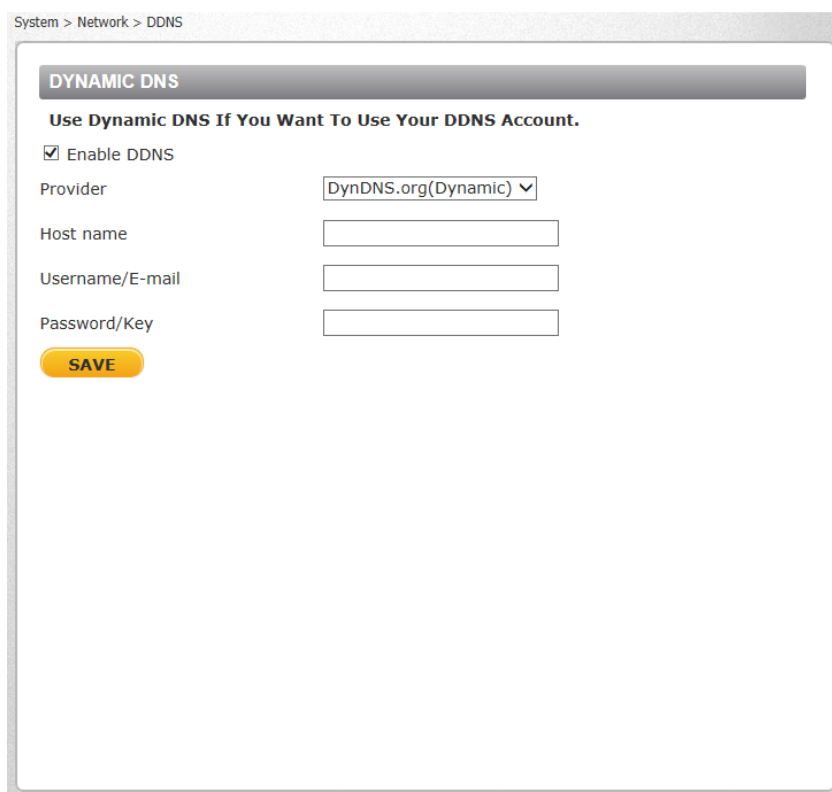
- *Friendly name* – Enter the name for the camera for identification.

Click **SAVE** to save the settings.

9.3.3.5 DDNS

Dynamic Domain Name System (DDNS) allows a host name to be constantly synchronized with a dynamic IP address. This permits those using a dynamic IP address to be accessed by a static domain name. DDNS configuration settings are entered in the **System > Network > DDNS** screen:

Figure 42: DDNS Screen

To use DDNS

1. Select the *Enable DDNS* checkbox.

2. From the *Provider* drop-down list, select a DDNS host provider name.

3. In the *Host name* text box, enter the registered domain name.

4. In the *Username/E-mail* text box, enter the username or e-mail address required by the DDNS provider for authentication.

5. In the *Password/Key* text box, enter the password or key required by the DDNS provider for authentication.

6. Click **SAVE** to save the setting.

9.3.3.6 Mail

Simple Mail Transfer Protocol (SMTP) is a protocol for sending e-mail messages between servers. It is a relatively simple, text-based protocol, where a text message is transferred to one or more specified recipients. The Administrator can send an e-mail via Simple Mail Transfer Protocol (SMTP) when an alarm is triggered. E-mail notifications are set by selecting the checkbox for an e-mail-related triggered action on the IO and Network Failure Detection screens.

SMTP (E-mail) server configuration settings are entered in the **System > Network > Mail** screen:

Figure 43: Mail Screen – SMTP

Two SMTP server accounts can be configured with or without SSL encryption. Enter the settings for the 1st SMTP server and 2nd SMTP server in the appropriate fields. Settings include SMTP server, server port (the default port is 25), account name, password, and recipient e-mail address settings. To encrypt e-mail with SSL, select the *1st SMTP SSL* and/or *2nd SMTP SSL* checkbox. For SMTP server details, contact your network service provider. Click **SAVE** when finished.

9.3.3.7 FTP

The Administrator can send an alarm message to one or two File Transfer Protocol (FTP) sites when motion is detected. FTP notifications are set by selecting the checkbox for an FTP-related triggered action on the IO and Network Failure Detection screens.

For each server, enter the server IP address, server port number, user name, password, and remote folder path. Settings are entered in the **System > Network > FTP** screen:

Figure 44: FTP Screen

To use passive mode, select the *1st FTP passive mode* or *2nd FTP passive mode* checkbox for the respective server. 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)

To test the connection to the specified FTP server, click **TEST** for the first or second server.

Click **SAVE** when finished.

9.3.4 Events Setup

The **Events Setup** tab includes the following screens:

- IO
- Network Failure Detection

9.3.4.1 IO

The **IO** screen is used to control input and output alarms and messages, which are generated when an event is recognized by the system.

Figure 45: IO Screen

Alarm Switch

The Administrator can select from the following options:

- Select *Off* to disable an alarm.

- Select *On* to enable an alarm (default setting).

- Select *By Schedule* to set a schedule. Then click *Please Select* to select up to 10 schedules from the drop-down list that opens. The selected schedules are displayed in the *Please Select* text box. To set a schedule, open the Schedule tab.

Click **SAVE** after configuring the settings.

> **Note:**
>
> Actions related to an analytic event that is defined in the **Analytics > Responses** screen are not affected by the status of the alarm switch.

Alarm Type

Select an alarm type (*Normal close* or *Normal open*) that corresponds to the alarm application. *Normal open* is the default setting. Click **SAVE** after configuring the settings.

Alarm Output

Define the normal alarm output signal as *Normal Open* or *Normal Close*, according to the current alarm application. *Normal open* is the default setting. Click **SAVE** after configuring the settings.

Trigger Action

The Administrator can specify various alarm actions to take when an alarm is triggered. The following options are available:

- *Enable alarm output* – Select this checkbox to enable alarm relay output. The checkbox is not selected by default.

- *Send message by FTP* – Select the checkbox send an alarm message by FTP when an alarm is triggered.

- *Upload image by FTP* – Select this box to assign an FTP site and configure the parameters shown. When an alarm is triggered, event images are uploaded to the designated FTP site.

> **Note:**
>
> Images can be sent by FTP only when MJPEG is selected as the video stream from the Video Format screen.

Follow these steps:

- From the *FTP address* drop-down list, select one of the two FTP addresses to use.

- From the *Pre-trigger buffer* and *Post-trigger buffer* drop-down lists, select the number of frames for the buffer from 1-20 frames.

Figure 46: Upload Image by FTP

- Select the *Continuous image upload* checkbox to upload an image by FTP for a defined period of time or while the trigger is active. Select one of the following options:
  - To specify the length of time for the upload, select *Upload for* and enter the number of seconds in the text box.
  - To upload while the trigger is active, select *Upload while the trigger is active*.

In the *Image Frequency* text box, from the drop-down list select the number of frames per seconds from 1-15 for the upload.

> **Note:**
> Make sure that FTP configuration has been completed. See [FTP](#) for details.

- *IR Cut Filter* – Select this checkbox to switch the camera between Day and Night mode.

- *Send message by E-Mail* – Select the checkbox send an alarm message by e-mail when an alarm is triggered. The e-mail address is entered in the [Mail](#) screen.

- *Upload image by E-Mail* – Select this checkbox to assign an e-mail address for sending the image captured by a triggered alarm. The e-mail address is entered in the [Mail](#) screen.

> **Note:**
> Images can be sent by e-mail only when MJPEG is selected as the video stream from the [Video Format](#) screen.

- From the *E-Mail address* drop-down list, select one of the two e-mail addresses.

- From the *Pre-trigger buffer* and *Post-trigger buffer* drop-down lists, select the number of frames for the buffer from 1-20 frames.

Figure 47: Upload Image by E-Mail

- Check the *Continuous image upload* box if you wish to upload an image by e-mail for a defined period of time or while the trigger is active. Select one of the following options:
  - To specify the length of time for the upload, select *Upload for* and enter the number of seconds in the text box.
  - To upload while the trigger is active, select *Upload while the trigger is active*.

In the *Image Frequency* text box, from the drop-down list select the number of frames per seconds from 1-15 for the upload.

> **Note:**
> Make sure that SMTP configuration has been completed. See [Mail](#) for details.

Click **SAVE** after configuring the settings.

File Name

- *File Name* – Enter a file name in the field, for example *image.jpg.* The uploaded image's file name format is set in this section. Select one that meets your requirements.

- Add date/time suffix (default setting)
  File name: imageYYMMDD_HHNNSS_XX.jpg
  Y: Year, M: Month, D: Day
  H: Hour, N: Minute, S: Second
  X: Sequence Number

- Add sequence number suffix (no maximum value)
  File name: imageXXXXXXX.jpg
  X: Sequence Number

- Add sequence number suffix (limited value)
  File Name: imageXX.jpg
  X: Sequence Number

  The file name suffix ends at the number being set. For example, if the setting is up to "10," the file name will start from 00, end at 10, and then start over again.

- Overwrite
  The original image in the FTP site will be overwritten by the new uploaded file with a static filename.

Click **SAVE** after configuring the settings.

9.3.4.2 Network Failure Detection

Settings on the **Network Failure Detection** screen enable the camera to periodically ping another IP device within the network to detect a network failure, for example, if a video server is disconnected.
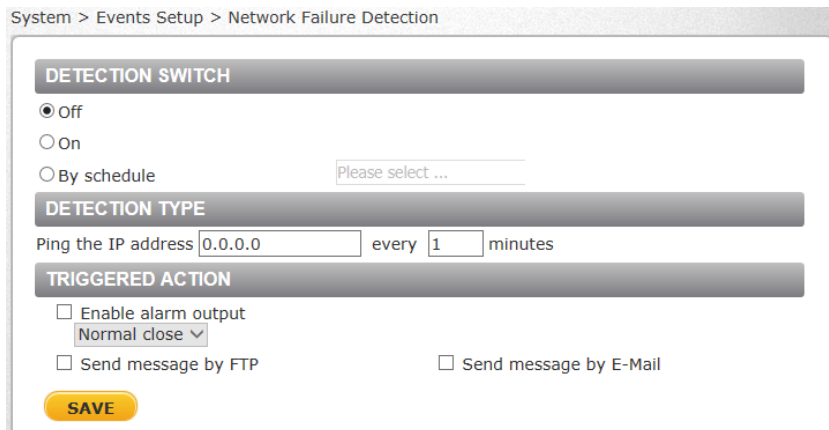
Figure 48: Network Failure Detection Screen

Detection Switch

The Administrator can select from the following options:

- Select *Off* to disable an alarm (default setting).

- Select *On* to enable an alarm.

- Select *By Schedule* to set a schedule. Then click *Please Select* to select up to 10 schedules from the drop-down list that opens. The selected schedules are displayed in the *Please Select* text box. To set a schedule, open the Schedule tab.

Click **SAVE** after configuring the settings.

Detection Type

In the text box, enter the IP address to ping and the time interval (in minutes) between pings. Click **SAVE** after configuring the settings.

Triggered Action

The Administrator can specify various alarm actions to be taken when an alarm is triggered. The options are listed below.

- *Enable alarm output* – Check this box and select the predefined type of alarm output *(low* or *high*) to enable alarm relay when a network failure is detected.

- *Send message by FTP* – Select whether to send an alarm message by FTP when a network failure is detected.

- *Send message by E-Mail* – Select whether to send an alarm message by e-mail when a network failure is detected.

Click **SAVE** to save the network failure detection settings.

9.3.5 Schedule

The **Schedule** screen is used for setting schedules for the recording of events triggered in the Events Setup > IO and Events Setup > Network Failure Detection screens. The functions in this tab allow administrators to create customized schedules for the camera that uses this option. If a schedule exists, the administrator can apply that schedule to this camera using the available drop-down list. See Figure 49: Schedule Screen.

To access the schedule function, open the **Main** window, select the **System** tab, and click the **Schedule** tab.

> ⊘
>
> **Note:**
> This application is not the same as the Recording Schedule function. It is not used for recording live video.

Figure 49: Schedule Screen

To create a new schedule or edit an existing schedule
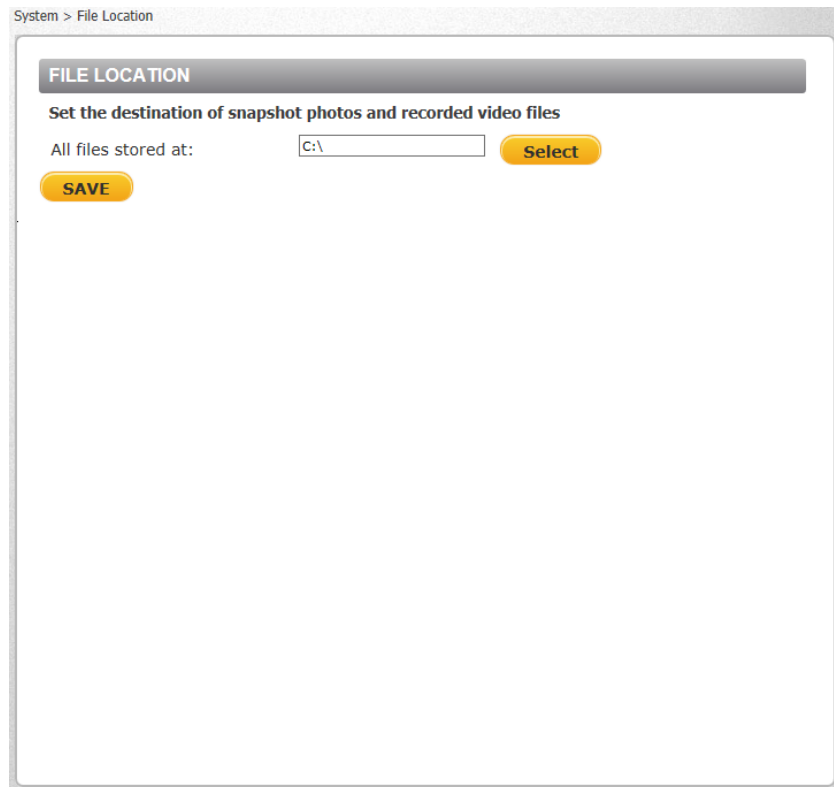
1. Select the appropriate checkbox for the day(s) of the week (Sun, Mon, Tue, Wed, Thu, Fri and Sat) to create a schedule.

2. Set *Start time* (for example, 09:00) and *Duration* (for example, 4:00 hours).

3. Click **SAVE** to apply the newly created schedule to the camera.

To remove a schedule

1. To remove a schedule, select the setup data line by line.

2. Click **DELETE** to remove.

9.3.6 File Location

From the **File Location** page, specify a storage location for snapshots and web recordings. The default setting is: C:\. After confirming the setting, click **SAVE** to save the snapshots and recordings in the designated location.

Figure 50: File Location Screen

Note:
1. Make sure the selected file path contains valid characters.
2. When using Windows 8 OS, the storage location cannot be C:\. You must define a storage location that does not require Administrator privileges on the PC.

9.3.7 Maintenance

Clicking the **Maintenance** tab in the **System** screen opens a drop-down menu with the following tabs**:**

- Log File
- User Information
- Factory Default
- Software Version
- Software Upgrade
- Parameters

9.3.7.1 Log File

Click **Log file** to view the system log file. The content of the file provides information about connections after system boot-up.
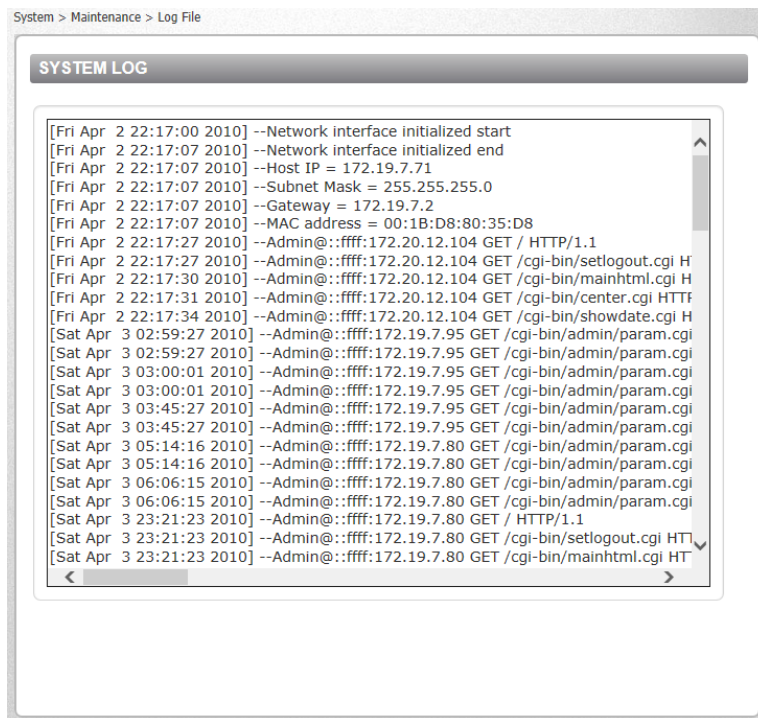
Figure 51: Log File Screen

9.3.7.2 User Information

The Administrator can view each user's login information and privileges in the **User information** screen shown below.

View User Login Information

Click **GET USER INFORMATION** to see each user's details. For example: *admin: admin*. This indicates that the user's login username is *admin* and the password is *admin*.
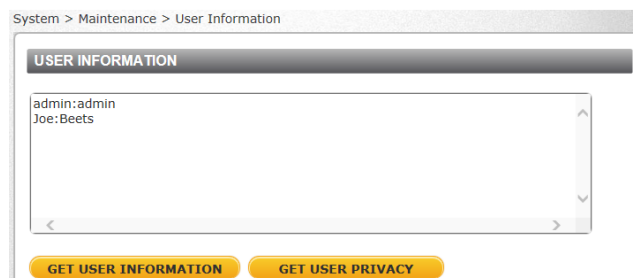
Figure 52: User Information Screen – Get User Information

View User Privilege

Click **GET USER PRIVACY** to view each user's privileges.
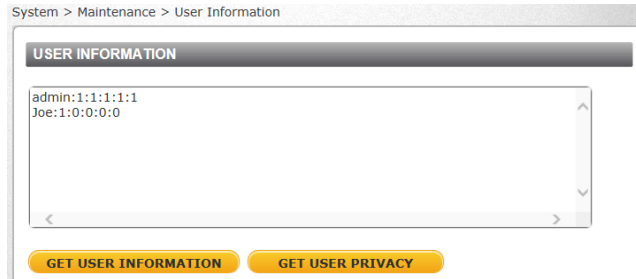
Figure 53: User Information – Get User Privacy

In the screen above, the a*dmin* is granted privileges of I/O access, Camera control, Talk and Listen, and Analytics, which are the maximum privileges that can be granted. The user Joe has only I/O access privilege.

> **Note:**
> User credentials and privileges are set in the User screen (page 39).

9.3.7.3 Factory Default

The **Factory default** page is shown below. Follow the instructions to reset the camera system settings to factory default settings if needed.
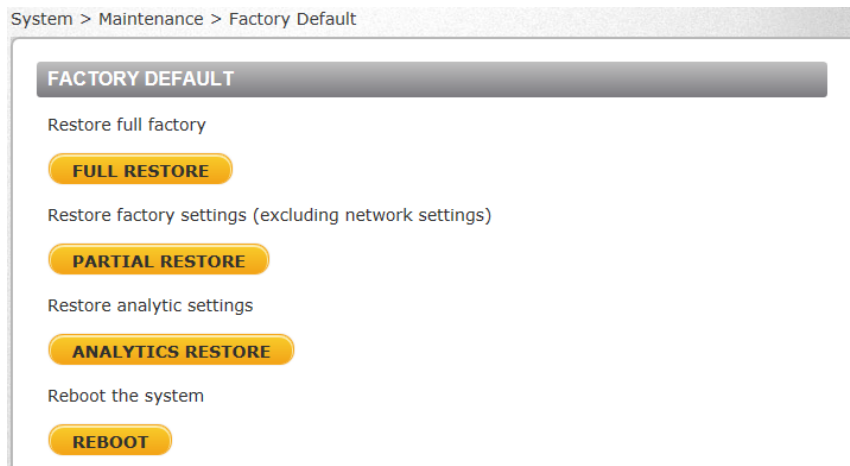
Figure 54: Factory Default Screen

Full Restore

Click **FULL RESTORE** to restore the factory default settings of the camera system. The system restarts in 30 seconds.

> **Note:**
> The IP address and all other settings will be restored to factory default settings.

Partial Restore

Click **PARTIAL RESTORE** to restore the factory default settings of the camera system, but save the network settings. The system restarts in 30 seconds.
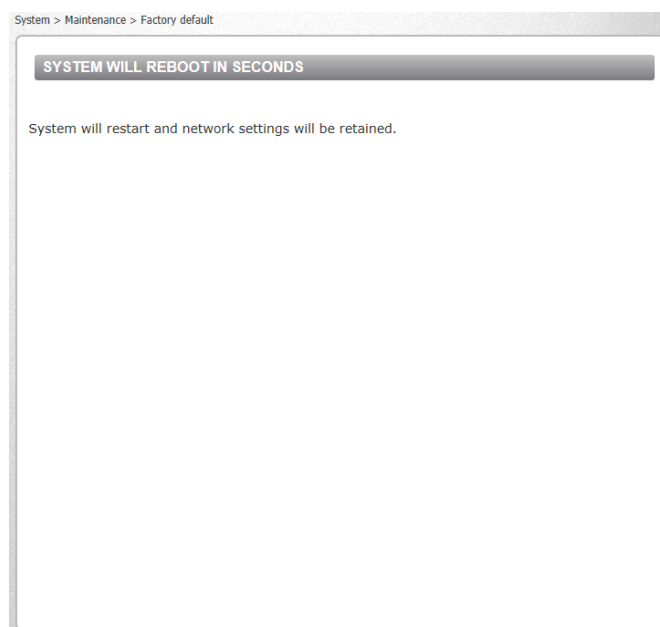
Figure 55: Partial Restore Screen

Analytics Restore

Click **ANALYTICS RESTORE** to reset the analytic firmware.

> **Note:**
> Analytics firmware is stored in a separate file than the camera system firmware. To backup and restore the analytics firmware version, see Analytics > Backup & Restore.

Reboot

Click **REBOOT** to restart the system without changing current settings.

9.3.7.4 Software Version

The current version of the camera system software is displayed in the **Software Version** screen.

Figure 56: Software Version Screen

> **Note:**
> To view the analytics firmware version, see Analytics > Firmware.

9.3.7.5 Software Upgrade

The **Software Upgrade** screen enables you to select a software file to upload.
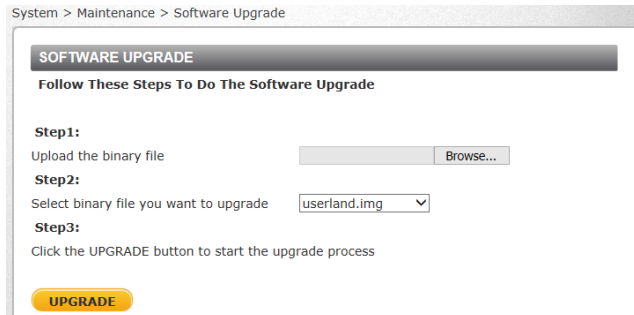
Figure 57: Software Upgrade Screen

Note:

1. Make sure that the software upgrade file is available before performing a software upgrade.
2. Do not change the file name. If you change the upgrade file name, the system will fail to find the file.
3. Analytics firmware is stored in a separate file than the camera system software. To upgrade the analytics firmware version, see Analytics > Firmware.

Warning:

1. Do not unplug power while entering file names.
2. Do not unplug power or change the screen while upgrading software.

Avertissement:

1. Ne débranchez pas l'alimentation pendant la modification des noms de fichiers.

2. Ne débranchez pas l'alimentation pendant la mise à niveau du logiciel.
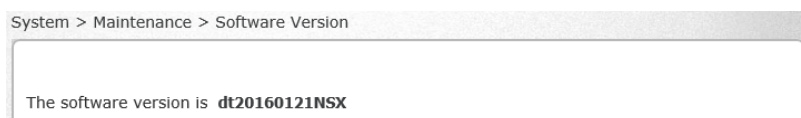
To upgrade the software

1. In the *Step 1* text box, click **Browse** and select the binary file to be uploaded, for example, `uImage_userland_ioi_HD_camera_20151023.img` (`uImage_userland_all.img`).

2. Select the file to upgrade. In the above example `uImage_userland` (userland.img) is selected.

3. Click **UPGRADE**. The system verifies that the upgrade file exists and begins to upload the file. The upgrade status bar is displayed on the page. When the upgrade process is completed, the **Live** page is displayed.

4. Close and reopen the web browser.

Note:

If you have problems with the ActiveX plugin, see Installing and Deleting the Web Player (page 116)

9.3.7.6 Parameters

The **Parameters** screen displays all of the system's parameter settings.
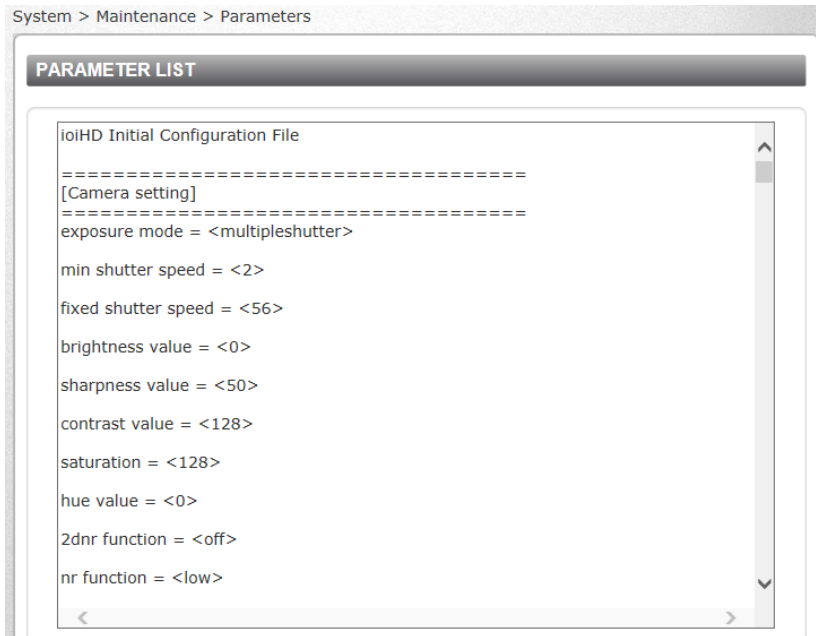
Figure 58: Parameter Screen

> **Note:**
> Slide the sidebar located on the right of the screen to view the entire list of parameters.

9.3.8 Import/Export

From the **Import/Export** screen you can export configuration files to a specified location and retrieve data by uploading an existing configuration file to the camera.
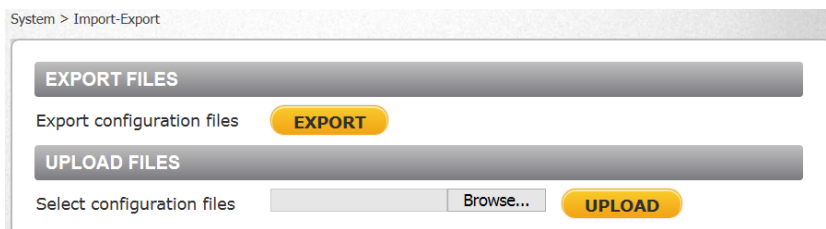
Figure 59: Import/Export Screen

> **Note:**
> 1. The camera firmware and the analytics firmware use separate configuration files. For analytic firmware configuration file, see Analytics > Backup & Restore.
> 2. It is not possible to import or export analytic settings from this screen.

⚠️

Warning:
Do not unplug power while changing file names.

Avertissement:
Ne débranchez pas l'alimentation pendant la modification des noms de fichiers.

To export a configuration file

1. Click **EXPORT.** An information bar opens.

| Do you want to open or save **config_file.bin** (202 KB) from **192.168.60.222**? | | Open | Save | ▼ | Cancel | × |

Figure 60: File Download Screen

2. Click **Save.**

3. Specify a location to save the configuration file.

To import a configuration file

1. Click **Browse** to select the configuration file

2. Click **UPLOAD**. The file is uploaded to the camera.

⚠️

Warning:
Do not unplug power while changing file names.

Avertissement:
Ne débranchez pas l'alimentation pendant la modification des noms de fichiers.

9.4 Streaming Tab

Select the **Streaming** tab in the navigation bar at the top of the page to display the configurable video and audio selections in the sidebar. From the **Streaming** sidebar, the Administrator can configure a specific video resolution, video compression mode, video protocol, audio transmission mode, etc. Details of these settings are specified in the following sections.
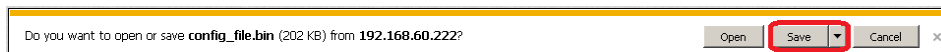
- Video Format
- Video Compression
- Video OCX Protocol
- Video Frame Rate
- Audio
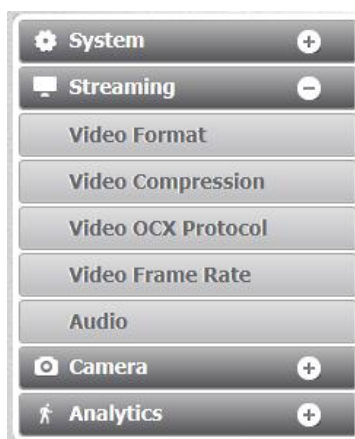
Figure 61: Streaming Section Tabs

9.4.1 Video Format

From the **Video Format** screen, you can configure the following settings:

- Video Resolution
- GOV Settings
- H.264 Profile

> **Note:**
> After changing the video format settings, you must restart the camera and re-enter the unit's IP address again in your browser in order to use the unit with the new settings.

9.4.1.1 Video Resolution

The IOI HD camera supports H.264/MJPEG streaming for resolutions up to 1080p. The default setting for CF-5212 is *1280 x 720*. The default setting for CF-5222 is *1920 x 1080*. Both H.264 and MJPEG streaming support analog BNC video connections. Following are the supported resolutions:

CF-5212		CF-5222	
PAL	**NTSC**	**PAL**	**NTSC**
1600 x 896	1600 x 896	1920 x 1080	1920 x 1080
1280 x 720	1280 x 720	1280 x 720	1280 x 720
720 x 576	720 x 480	720 x 576	720 x 480

9.4.1.2 GOV Settings

Users can set the GOV length to determine the frame structure (I-frames and P-frames) in a video stream for saving bandwidth. The setting range is from *1* to *255*. A longer GOV means decreasing the frequency of I-frames. The default setting is *30*. Click **SAVE** to confirm the GOV setting.

9.4.1.3 H.264 Profile

The H.264 standard defines 21 sets of capabilities. These are referred to as profiles and they target specific classes of applications. In the security industry, the most common are as follows:

- **Baseline Profile (BP)**
  Primarily for low-cost applications that require additional data loss robustness, *Baseline Profile* is used in some videoconferencing and mobile applications. This is the most common profile used in IP security cameras due to the low computational cost of processing the video using this 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. *Main Profile* can save 10-12% over *Baseline*. This is the default profile.

- High **Profile (HP)**
  High Profile is the primary profile for HD broadcast applications. It can save 10-12% of the storage cost over *Main Profile*. However, it may also increase video latency, depending on the stream structure. Units default to the *Main Profile* to provide the best trade-off between storage size and video latency.

Click **SAVE** to confirm the settings.

9.4.2 Video Compression

From the **Video Compression** page, you can specify MJPEG and H.264 compression settings.

Figure 62: Video Compression Screen

MJPEG Compression Setting

A higher value implies higher bit rates and higher visual quality. The default setting of the MJPEG Q factor is 35. The setting range is from *1* to *45*. Click **SAVE** to confirm the setting.

H.264-1 Compression Setting

The default setting of H.264 is *2074* kbps. The setting range is from *64* to *8192* kbps. Click **SAVE** to confirm the setting.

Compression Information Setting

Select the checkbox to display compression information on the **Home** page. The default setting is *Display compression information in the home page*. Click **SAVE** to confirm the setting.

CBR Mode Setting

If available bandwidth is limited, check *Enable H.264 CBR mode* to use Constant Bit Rate. The default setting is *Enable H.264 CBR mode*. To operate the camera in Variable Bit Rate (VBR) mode, uncheck the CBR checkbox. Click **SAVE** to confirm the setting.

> **Note:**
> CBR mode affects image quality.

9.4.3 Video OCX Protocol

From the **Video OCX Protocol** page, you can select various protocols for streaming media over the network. In the case of multicast networking, select *Multicast mode*.

Figure 63: Video OCX Protocol Screen

Video OCX protocol setting options include:

- RTP over UDP

- RTP over RTSP (TCP)

- RTSP over HTTP

- MJPEG over HTTP

- Multicast mode – Enter in each field all required data, including *Multicast H.264 Video Address* and *Port, Multicast MJPEG Video Address, Multicast Audio Address,* and *Multicast TTL*. The default Multicast TTL (time-to-live) setting is *1*, which prevents multicast datagrams from being forwarded beyond a single sub-network.

Click **SAVE** to confirm the settings.

9.4.4 Video Frame Rate

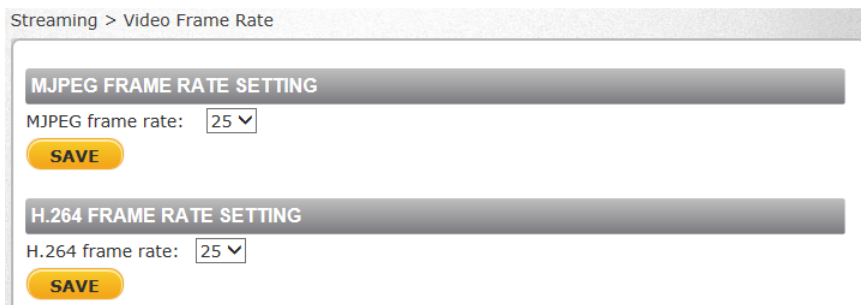From the **Video Frame Rate** screen, you can specify the frames per second (fps) for each video compression format.

Figure 64: Video Frame Rate Screen

MJPEG/H.264 Frame Rate Setting

The default setting of the MJPEG and H.264 frame rate is *30* fps in NTSC and *25* fps in PAL. Settings are:

- PAL: *1, 5, 13,* and *25* fps

- NTSC: *1, 2, 3, 6, 7.5, 10, 15,* and *30* fps

> **Note:**
> A lower frame rate decreases video smoothness.

Click **SAVE** to confirm the settings.

> **Note:**
> Images can be sent by FTP or email only when MJPEG steaming is selected as one of the streams.

9.4.5 Audio

From the **Audio** screen you can select the Transmission Mode, Server Gain, Bit Rate, and enable or disable storage of the audio recording.
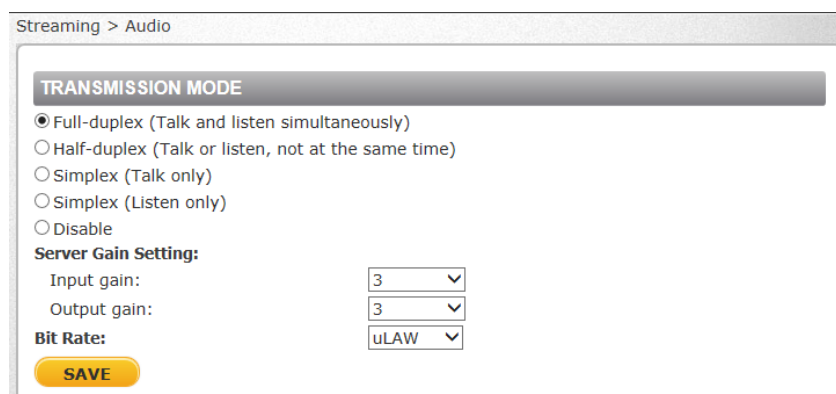

Figure 65: Audio Screen

Transmission Mode

- *Full-duplex (Talk and listen simultaneously)* – In the Full-duplex mode, the local and remote sites can communicate with each other simultaneously, i.e. both sites can speak and be heard at the same time.

- *Half-duplex (Talk or listen, not at the same time)* – In the Half-duplex mode, the local or remote site can only talk or listen to the other site at one time.

- *Simplex (Talk only)* – In the Talk only Simplex mode, the local/remote site can only talk to the other site.

- *Simplex (Listen only)* – In the Listen only Simplex mode, the local/remote site can only listen to the other site.

- *Disable* – Select this option to turn off the audio transmission function.

Server Gain Setting

Set the audio input/output gain levels for sound amplification. The audio input gain is adjustable from 1 to 10. The audio output gain is adjustable from 1-6. The sound will be turned off if the audio gain is set to *Mute*. The default audio input and output gain setting is 3.

Bit Rate

Selectable audio transmission bit rates include 16 kbps (G.726), 24 kbps (G.726), 32 kbps (G.726), 40 kbps (G.726), µLAW (G.711) and ALAW (G.711). Both µLAW and ALAW signify 64 kbps, but in different compression formats. A higher bit rate enables higher audio quality, but requires higher bandwidth. The default setting is *uLAW*.

Note:
Latitude does not support G.726.

Click **SAVE** to confirm the settings.

9.5 Camera Tab

From the **Camera** tab, the administrator can adjust any of the camera settings from the following tabs:

- [Exposure](#)
- [Picture Adjustment](#)
- [Advanced Picture Settings](#)
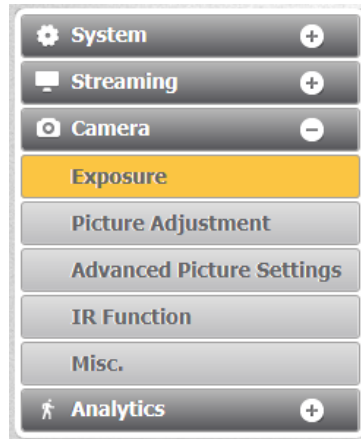- [IR Function](#)
- [Misc.](#)

Figure 66: Camera Section Tabs

9.5.1 Exposure Screen

The **Exposure** screen is used to configure lens settings and exposure modes. The exposure is the amount of light received by the image sensor. It is determined by the amount of exposure by the sensor's shutter speed, lens aperture, and screen illumination.

Administrators may either allow the camera to automatically select an exposure level using a programmed algorithm or choose the level themselves. The higher the shutter speed that the administrator selects, the lower the exposure level and vice versa.

The displayed **Exposure** screen depend on whether Shutter WDR is configured as *On* or *Off* in the [Misc](#). screen.

9.5.1.1 Exposure Screen with Shutter WDR On

Two exposure options are available when Shutter WDR is set to *On*: *WDR Multiple Shutter* and *WDR Multiple Shutter RSS*.

- *WDR Multiple Shutter* (True WDR) – The camera's shutter speed works automatically to achieve a consistent video output level. You can select a suitable shutter speed according to the environmental luminance.

- *WDR Multiple Shutter RSS* – This setting is recommended when flickering occurs in indoor applications where fluorescent lighting is used. The shutter speed decreases in order to compensate for decreased ambient lighting.
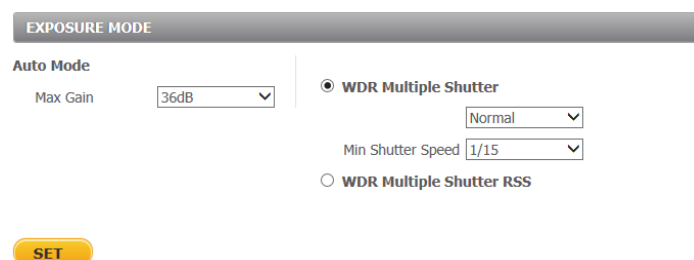

Figure 67: Exposure Screen with Shutter WDR On

> ⚠
>
> **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.*

To set the Exposure mode

1. From the *Auto Mode Max Gain* drop-down list, set the maximum gain in 3db steps from *Off* to 54dB. Increasing the gain lightens dark pictures resulting from low-level lighting. The default setting is 36dB.

> ⚠
>
> **Caution:**
> The noise level might increase if the gain level is set too high in low-light scenes.
>
> ***Attention:***
> *Le niveau de bruit peut augmenter si le niveau de gain est trop élevé dans les scènes à faible luminosité.*

2. Select one of the following modes:

- *WDR Multiple Shutter* (True WDR) – In WDR Multiple Shutter mode, the camera's shutter speed works automatically to achieve a consistent video output level. Select the shutter speed that provides the ideal image quality according to the environmental luminance. This setting is *Off* by default.

  a. From the drop-down list, select *Normal* or *WDR First*.

     - Normal – Select this setting for low-light conditions.

     - *WDR First* – This mode is recommended for indoor environments with mixed lighting sources where the main source is indoor lighting and natural light enters the scene through windows and other exposed areas. The setting reduces the overexposure in the area with natural lighting.

  b. From the Min Shutter Speed drop-down list, select a shutter speed from 1/12 to 1/425 sec (PAL) or 1/15 to 1/500 sec (NTSC). The default setting is 1/12 (PAL) or 1/15 (NTSC). The following table displays the options.

WDR Multiple Shutter Min Shutter Speed		WDR Multiple Shutter Min Shutter Speed	
PAL	**NTSC**	**PAL**	**NTSC**
1/425	1/500	1/100	1/100
1/300	1/350	1/75	1/90
1/215	1/250	1/50	1/60
1/150	1/180	1/25	1/30
1/120	1/125	1/12	1/15

  c. Click **SET** to confirm the new setting.

- *WDR Multiple Shutter RSS* – This setting is recommended when flickering occurs in indoor applications where fluorescent lighting is used. The shutter speed decreases in order to compensate for decreased ambient lighting.
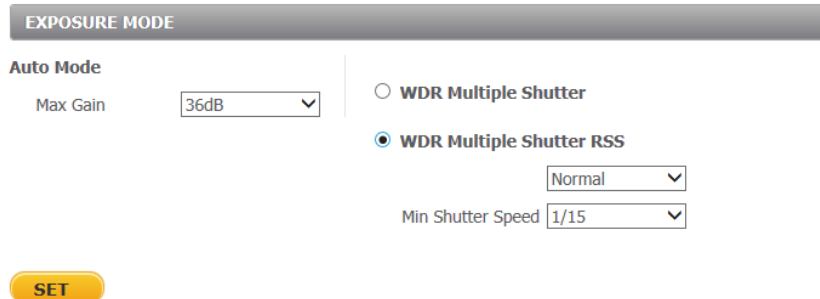

Figure 68: Multiple Shutter RSS Exposure Screen

a. From the drop-down list, select *Normal* or *WDR First*.

- *Normal* – See explanation above.

- *WDR First* – See explanation above.

b. From the *Min Shutter Speed* drop-down list, select a shutter speed. A fixed exposure is set, while other parameters can change. The range is from *1* to *1/500* sec (NTSC) or *1/1.5* to *1/425* sec (PAL). The following table displays the options.

WDR Multiple Shutter RSS Min Shutter Speed		WDR Multiple Shutter RSS Min Shutter Speed	
PAL	NTSC	PAL	NTSC
1/425	1/500	1/100	1/100
1/300	1/350	1/75	1/90
1/215	1/250	1/50	1/60
1/150	1/180	1/25	1/30
1/120	1/125	1/12	1/15

3. Click **SET** to confirm the new setting.

9.5.1.2 Exposure Screen with Shutter WDR Off

Five exposure options are available when Shutter WDR is set to *Off*: *Auto Iris, Auto Shutter, Shutter Priority, Flickerless,* and *Manual Mode*.

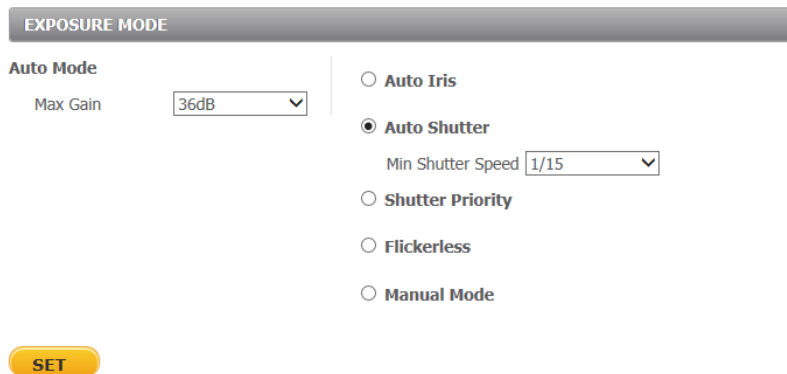*Figure 69: Exposure Screen with Shutter WDR Off*

⚠

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.

To set the Exposure mode

1. From the *Auto Mode Max Gain* drop-down list, set the maximum gain in 3db steps from *Off* to 54dB. Increasing the gain lightens dark pictures resulting from low-level lighting. The default setting is 36dB.

   ⚠

   Caution:
   The noise level might increase if the gain level is set too high in low-light scenes.

   Attention:
   Le niveau de bruit peut augmenter si le niveau de gain est trop élevé dans les scènes à faible luminosité.

2. Select one of the following modes:

   • *Auto 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 mode completely opens the shutter. The exposure priority is given to the iris. Shutter speed and AGC circuit function automatically in cooperating with the iris to achieve a consistent exposure output.

   From the *Min Shutter Speed* drop-down list, select one of the following shutter speed options. The default setting is *1/12* (PAL) or *1/15* (NTSC).

Auto Iris Min Shutter Speed	
PAL	**NTSC**
1/25	1/30
1/12	1/15

   • *Auto Shutter* – This is the default exposure mode of the camera. It is recommended for the following scenarios: outdoor environments or indoor environments with unified lighting (either with constant or changeable lighting conditions), as long as the main light source is fluorescent lighting.

   Select this mode so that the camera's shutter speed works automatically to achieve a consistent video output level. You can select a suitable shutter speed according to the environmental luminance.

   From the *Min Shutter Speed* drop-down list, select one of the following shutter speed options. The shutter speed range is from *1/12* to *1/425* sec (PAL) to *1/15* to *1/500* sec (NTSC). The default setting is *1/12* (PAL) or *1/15* (NTSC).

Auto Shutter Min Shutter Speed		Auto Shutter Min Shutter Speed	
PAL	NTSC	PAL	NTSC
1/425	1/500	1/100	1/100
1/300	1/350	1/75	1/90
1/215	1/250	1/50	1/60
1/150	1/180	1/25	1/30
1/120	1/125	1/12	1/15

- *Shutter Priority* – Select this mode to set a fixed exposure while other parameters can change. The shutter speed range is from *1/25* to *1/425* sec (PAL) to *1/30* to *1/500* sec (NTSC). The default setting is *1/25* (PAL) or *1/30* (NTSC). From the *Min Shutter Speed* drop-down list, select one of the following shutter speed options.

Shutter Priority Min Shutter Speed		Shutter Priority Min Shutter Speed	
PAL	NTSC	PAL	NTSC
1/425	1/500	1/100	1/100
1/300	1/350	1/75	1/90
1/215	1/250	1/50	1/60
1/150	1/180	1/25	1/30
1/120	1/125		

- *Flickerless* – This mode is used to eliminate flicker for indoor applications where fluorescent lighting is used. The darker the ambient lighting, the slower the shutter speed should be. The shutter speed range is from *1/12* to *1/100* sec (PAL) or *1/15* to *1/100* sec (NTSC). The default setting is *1/12* (PAL) or *1/15* (NTSC). From the *Min Shutter Speed* drop-down list, select one of the following shutter speed options.

Flickerless Min Shutter Speed	
PAL	NTSC
1/100	1/100
1/75	1/90
1/50	1/60
1/25	1/30
1/12	1/15

- *Manual Mode* – Manual mode is used generally where light levels are fixed and the auto settings do not provide the perfect exposure. It is recommended for scenes such as indoor scenes, where there is a fixed lighting contrast and a constant, precise exposure is required.

  Manual Mode opens the iris completely with a fixed gain to a fixed shutter speed. Users can select a suitable shutter speed according to the environmental luminance. Increasing the value of the fixed shutter increases the amount of light entering the sensor. This allows a brighter and more detailed image. Similarly, 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.

  In Manual Mode, the administrator can select a fixed shutter speed and gain from drop-down menus. The smaller the shutter speed number (the higher the shutter speed), the lower the exposure level. The higher the gain, the brighter the picture.

  From the *Shutter* drop-down list, select a suitable shutter speed from *1* to *1/10000* sec (PAL/NTSC), according to the environmental luminance The default setting is *1/150* (PAL) or *1/180* (NTSC). The following table displays the options.

Manual Mode Fixed Shutter Speeds	
PAL	NTSC
1/10000	1/10000
1/3500	1/4000
1/2500	1/3000
1/1750	1/2000
1/1250	1/1500
1/1000	1/1000
1/600	1/725
1/425	1/500
1/300	1/350
1/215	1/250
1/150	1/180
1/120	1/125
1/100	1/100
1/75	1/90
1/50	1/60
1/25	1/30
1/12	1/15

From the *Gain* drop-down list, set the maximum gain in 3db steps from *Off* to 54dB. Increasing the gain lightens dark pictures resulting from low-level lighting. The default setting is 36dB.

Click **SET**.

9.5.2 Picture Adjustment

Adjustment of some qualities of the video is made possible by selecting *Picture Adjustment* in the **Camera** tab. Brightness, Sharpness, Contrast, Saturation and Hue may all be adjusted via drop-down menus from this window, as shown below.

Figure 70: Camera Settings Screen – Picture Adjustment

Brightness

You can adjust the image's brightness by adjusting this parameter. Select from the range between *+1* to *+25*. To increase video brightness, select a larger number. The default setting is *0*. Click **SET** to confirm the new setting.

Sharpness

Increasing the sharpness level can make the image look sharper, especially enhancing the object's edge. Select from the range between *-15* to *+10* in 1dB steps. The default setting is *-10*. Click **SET** to confirm the new setting.

Contrast

Camera image contrast level is adjustable. Select from a range of *-13* to *+12* in 1dB steps. The default setting is *0*. Click **SET** to confirm the new setting.

Saturation

Camera image saturation level is adjustable. Select from a range of *-12* to *+13* in 1dB steps. The default setting is *0*. Click **SET** to confirm the new setting.

Hue

Camera image hue level is adjustable: select from a range of +1 to +12 in 1dB steps. The default setting is 0. Click **SET** to confirm the new setting.

9.5.3 Advanced Picture Settings

The options for the Advanced Picture Settings screen depend on whether Shutter WDR is configured as *On* or *Off* from the Misc screen. In both cases, 3DNR and 2DNR noise reduction settings are configured from this screen.

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

3DNR and 2DNR settings reduce luminance noise, which is composed of dots of various brightness levels (black, white and gray). It is not recommended to completely eliminate luminance noise, which can result in unnatural images.

Advanced Picture Settings with WDR On

When Advanced Picture Settings are enabled (configured as *On*), the user can configure only 3DNR and 2DNR settings from this screen.

Figure 71: Advanced Picture Settings Screen with WDR On

3DNR

3DNR (3D Noise Reduction) provides superior noise reduction and is recommended for use in in extra low-light conditions. It is especially useful for reducing blur with moving objects. The 3DNR function reduces image noise/snow in low-light conditions by comparing adjacent frames. A higher level of 3DNR generates relatively enhanced noise reduction, although it creates more motion blur than 2DNR on moving objects.

The noise reduction is selectable from *Off, Low, Middle,* and *High.* The default setting is *Low*. Click **SET** to confirm the new settings.

2DNR

2DNR (2D Noise Reduction) analyzes individual frames pixel by pixel and frame by frame to eliminate environmental noise and deliver optimized image quality, especially in low-light conditions. 2DNR tends to produce superior results for moving objects when applied to areas in the field of view where movement is present. However, it is less precise than 3DNR.

Settings include *Enable* and *Disable*. The default setting is *Disable*. Click **SET** to confirm the new settings.

⚠

Caution:
Noise levels can be compromised when using the 2DNR/3DNR functions.

__Attention:__
Les niveaux de bruits peuvent être compromis avec les fonctions 2DNR/3DNR.

Advanced Picture Settings with WDR Off

When Advanced Picture Settings are disabled (configured as *Off*), in addition to 3DNR and 2DNR settings, the user can configure Backlight Compensation and Gamma WDR from this screen.

Figure 72: Advanced Picture Settings Screen with WDR Off

Backlight compensation is used in images where a bright light source is behind the subject of interest. Without backlight compensation, 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.

Select *On* or *Off*. The default setting is *Off*. Click **SET** to confirm the new settings.

Gamma WDR, also known as dWDR. resolves high contrast or changing light issues in order to enhance the image quality. It does this by producing a larger amount of details in both the dark and bright areas of the image. 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.

Select *On* or *Off*. The default setting *On*. Click **SET** to confirm the new settings.

9.5.4 IR Function

The IR Function setting activates the IR Cut (IRC) filter for electronic day/night operation. The day/night IRC switching mechanism operates according to the ambient light level.

Figure 73: IR Function Screen

From the *Day/Night Function* drop-down list, select one of the four settings:

- *Auto Mode* – The camera converts from Day mode (color) to Night mode (monochrome) 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.

- *Night* – Activates IR mode (puts camera into monochrome/Night mode).

- *Day*– Deactivates IR mode (puts camera into color/Day mode).

- *Smart* – Smart mode enhances monochrome/Night mode stability when IR illumination is dominant and keeps the camera from switching between Day and Night modes. In this mode, the IR Cut filter is on (i.e. monochrome/Night mode) when the IR LED illuminator also is activated. This prevents the camera from returning to color/Day mode.

Click **SET** to confirm the new setting.

9.5.5 Miscellaneous

From the **Misc.** (Miscellaneous) tab, you can set the TV System and Shutter WDR.

Figure 74: Misc. Screen

> **Note:**
> The selection of Shutter WDR *On* or *Off* determines which **Camera > Exposure** screen is displayed.

TV System Settings

Select the video system setting: *25 fps (PAL)* or *30 fps (NTSC).* The default TV system is 30 fps (NTSC). Click **SET** to confirm the setting.

> **Note:**
> After changing TV System settings, the camera restarts automatically. You must re-enter the unit's IP address again in your browser in order to use the unit with the new settings. The camera restores to factory defaults and the analytics settings are deleted.

Shutter WDR

The Shutter WDR (Wide Dynamic Range) function, also known as True WDR or multi-exposure WDR, resolves high contrast or changing light issues and creates a constant video output level. The camera creates a new image with a wide dynamic range by using a combination of slow- and fast-exposure shutters and an algorithm to determine the optimal mix of light and dark regions within the scene from the two shutters.

Figure 75: Shutter WDR On   *Figure 76: Shutter WDR Off*

Shutter WDR is selectable between *On* or *Off:*

- When *On* is selected, the image has a wide dynamic range, so that the IP camera can capture a greater scale of brightness. This is the default setting.
- Selecting *Off* disables this function.

Click **SET** to confirm the new setting.

9.6 Analytics Tab

The IOI HD camera includes a rich set of video analytic functionality embedded in its firmware. The Analytics tab contains menus for defining the camera's Field of View depth and detection rules, including region entrance, loitering, tripwire crossover, fence trespass, unattended baggage, stopped vehicle, and object removal.
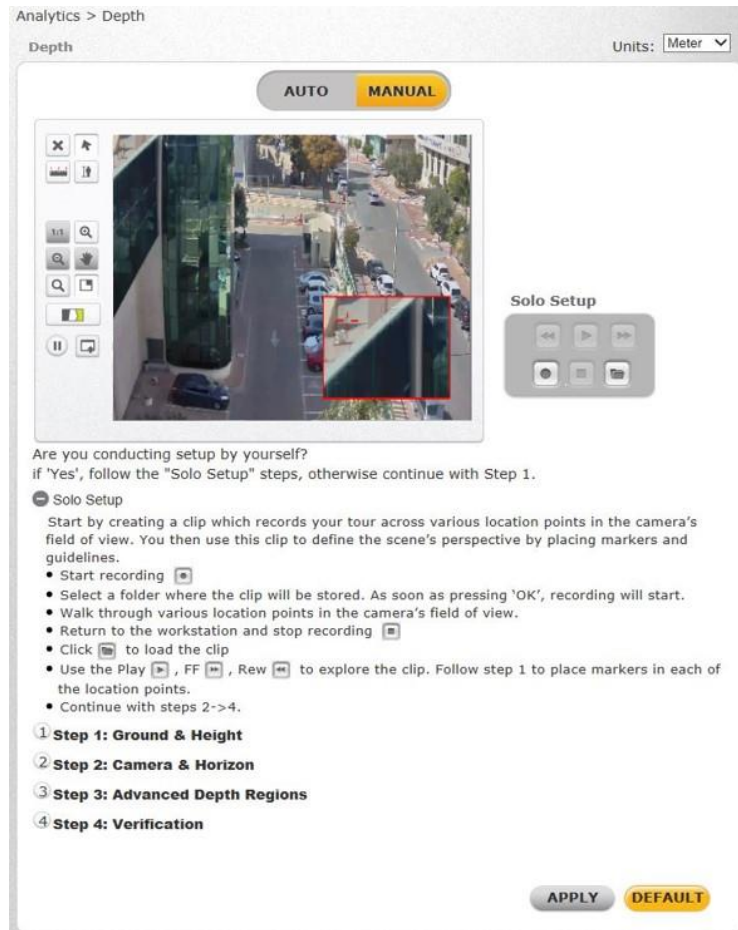
Figure 77: Analytics > Manual Depth Screen

In real-time, the camera sends notifications and alarms upon the occurrence of events. You can set customizable rules and criteria to define the perimeter, region, and what to detect. The camera's analytic software ensures a high probability of detection with an extremely low false alarm rate.

Use the **Analytics** tab to configure the following functions:

- Depth
- Rules
- Responses
- Scheduled Actions
- On-Screen Display
- Firmware
- Backup & Restore

⚠

Caution:
The camera is disarmed when configuring Analytics. Detection will not take place until the camera is manually re-armed from the **Home** screen.

Attention:
*La caméra est désactivée lors de la configuration d'Analytics. La détection n'aura lieu qu'après que la caméra soit réactivée depuis l'écran **Accueil**.*

9.6.1 Depth

The **Depth** screen enables you define the perspective of the scene being monitored and to. It is used to set human markers, ground guidelines, camera height, horizon, and advanced depth regions (such as hills, planes and fences), which create a virtual 3D model for measurement of distances and sizes from the perspective of the camera. The screen contains a wizard that facilitates configuring the depth settings. See Figure 77: Analytics > Manual Depth Screen (page 85).

Automatic Depth Calibration

Depth settings can be configured automatically by using the Auto Calibration (automatic depth calibration) algorithm from the **Auto** depth screen. By default, the **Auto** screen is displayed.

Figure 78: Auto Depth Screen - Auto Calibration

✎

Note:
The **Auto** screen remains the default setting unless you select the **Manual** depth screen. If you select the **Manual** screen and click **APPLY**, the **Manua**l screen remains the default setting until you select the **Auto** screen again and the Auto Calibration process is completed.

The Auto Calibration function automatically configures scene depth and calculates camera height, focal length, and tilt angle according to the scene depth. The system discovers people in the scene and configures human markers automatically. This function eliminates the time and effort required to manually add human markers.

> **Note:**
> If you use the Auto Calibration function, it is possible to configure additional settings manually and verify the Auto Calibration settings after the Auto Calibration process is completed. Click **MANUAL** in order to configure additional settings.

To automatically configure depth settings

1. Verify that the camera is installed at a height of at least four meters (13 feet).

2. Verify that the horizon is less than 30% of the Field of View (FoV).
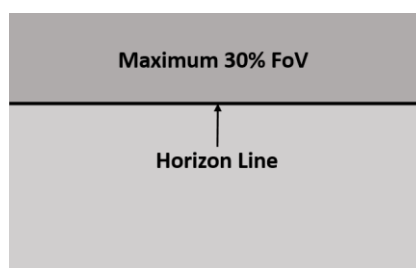
Figure 79: Horizon Line

3. From the **Settings** tab, select **Analytics > Depth**. The **Auto** depth screen opens. See Figure 78: Auto Depth Screen - Auto Calibration.

4. From the *Units* drop-down list, select *Feet* or *Meter*.

5. Select *Set estimated height*.

6. Enter the estimated camera height in the text box.

7. Click **START**. The camera automatically calibrates the depth.

8. Be sure that a person is walking along the Y (Vertical) axis of the FoV while Auto Calibration is in process. When the progress bar reaches 100%, the Auto Calibration is completed and the calculated results are displayed.

> **Note:**
> While Auto Calibration is in progress, you can proceed with the next steps in the analytic configuration.

> **Caution:**
> 1. The Auto Configuration algorithm takes at least five minutes to run. If you stop the procedure before the progress bar reaches 100%, the analytic process will reset.
> 2. If you change from Auto to Manual mode, you must wait until the analytic process resets in order to use Manual mode.

9. Select the **Auto > Step 2: Verification** tab.

10. Verify that the horizon, camera height, and human marker settings are correct.

> ⊘
>
> **Note:**
> If the results are unsatisfactory, run Auto Calibration again (follow Step #1 on-screen) or click **MANUAL** to manually configure the depth settings.

11. After finishing the Auto Configuration, click the **MANUAL** tab.

12. Select the **Manual > Step 4: Verification** tab to complete the depth configuration.

Manual Depth Calibration

If you select the **MANUAL** depth button, there are two methods to manually configure depth settings:

- If you are performing setup by yourself, click the Solo Setup tab.
- If you are not performing setup alone, proceed to [Configuring Ground and Height Settings](#).

> ⊘
>
> **Note:**
> 1. It is possible to select the **Step 4: Verification** tab to verify and apply settings at any time.
> 2. For detailed instructions how to set markers and guidelines, follow instructions in the *HTML Edition Units User's Guide*.

Solo Setup

The Solo Setup function enables you to install and setup the camera at a remote site without requiring another person's assistance. It is very useful and should be used even if you have another person's assistance.

With this feature, you can:

- Move around within the camera's Field of View.
- Use the camera to record a set of snapshots of the scene while the user is moving around the camera Field of View. Creating the recording of the person in the FoV can be used to adjust settings without requiring another physical walk through the FoV.
- Use the recording of his movement to setup the depth by marking his height on the camera's Field of View.

Follow the instructions in the **Solo Setup** tab to single-handedly setup the camera:
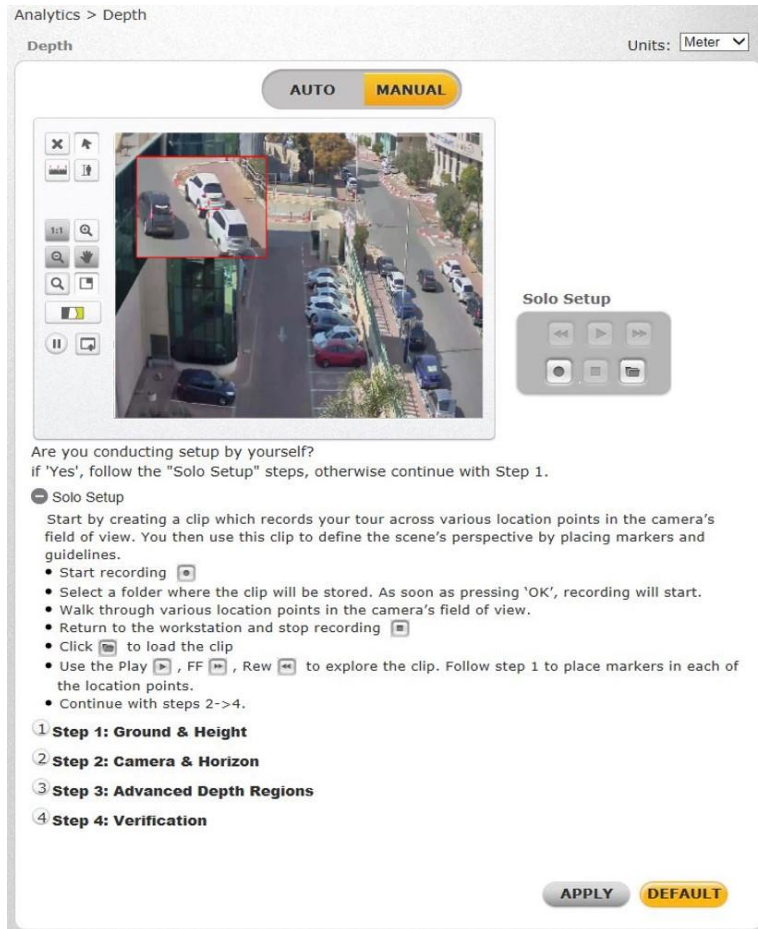
Figure 80: Analytics > Depth > Solo Setup Instructions

To perform a solo setup

1. Click the **Solo Setup** tab. The Solo Setup keypad opens with the following control icons:

Icon	Function	Notes
	Start Recording	Starts recording and browses to destination folder where the clip will be saved
	Stop Recording	Stops recording
	Browse	Browses to the destination folder where clip is stored and loads the clip
	Play/Pause	Speed X1/X0
	Fast Forward	Speed X2, X4, X8, X16. Click to increase or decrease speed.
	Rewind	Speed -X2, -X4, -X8, -X16. Click to increase or decrease speed.

2. On the Solo Setup control keypad, click **Start Recording** to record a view in the camera's Field of View.

3. Select a folder where to store the clip. Recording starts when the folder is selected.

4. Walk through various locations across the vertical axis of the camera's Field of View in order to place ground and height markers and guidelines in the clip.

5. Click **Stop Recording** .

6. Click **Step 1: Ground & Height** and follow the instructions.

7. Click **Browse** to load the clip from the folder where it is saved.

8. Use the **Play** , **Pause** , **Fast Forward** , and **Rewind** buttons on the Solo Setup keypad to explore the clip. The status of the view is displayed on the bottom left side of the screen.

9. Click the round **Play** button on the control panel located to the left of the monitor to exit Clip mode and return to Live mode. The caption under the monitor changes from *Clip* to *Live.*

Figure 81: Analytics > Depth Control Panel

10. Proceed to the tabs for Steps 2-4 of the Depth Setup to complete the setup and apply settings.

> **Note:**
> At any time it is possible to click the **Verification** tab to verify and apply settings.

Configuring Ground and Height Settings

If you are not performing a solo setup, do the following:

To configure ground and height settings

1. Click the **Step 1: Ground & Height** tab. The **Step 1: Ground & Height** screen opens.
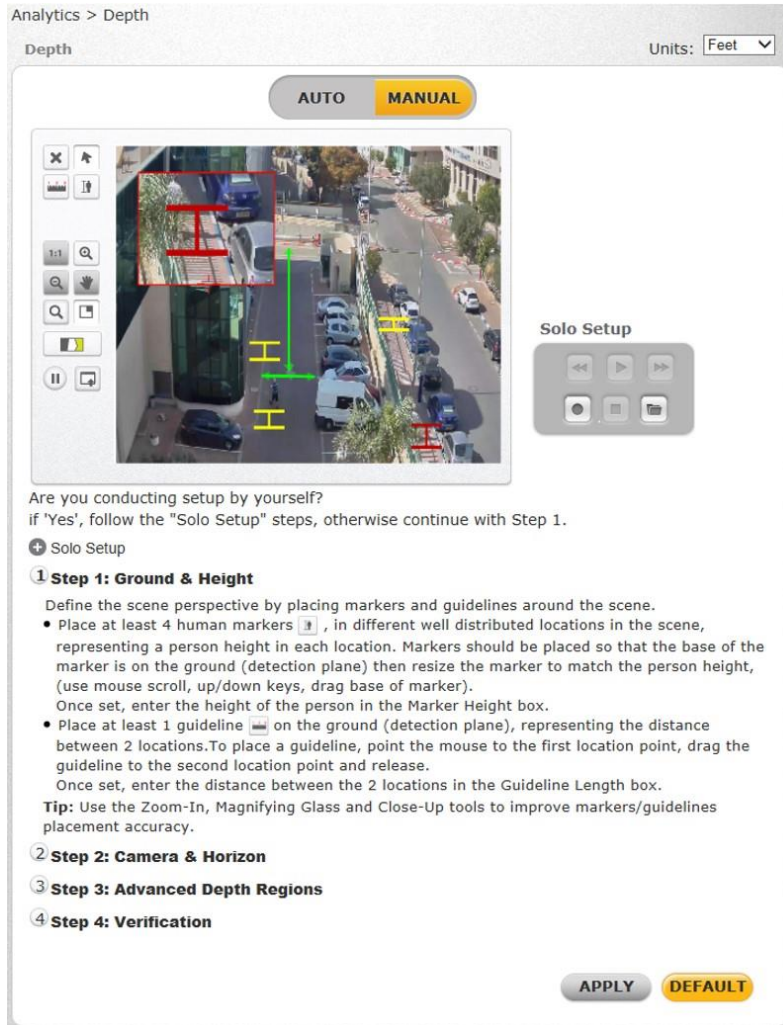
Figure 82: Analytics > Depth > Step 1: Ground & Height Screen

2. Follow the instructions on screen.

Figure 83: Analytics > Depth > Step 1: Ground & Height Instructions

3. Refer to the *HTML Edition Units User's Guide* for detailed instructions on configuring these settings.

4. Click **APPLY** when finished or continue to the next step.

Configuring Camera and Horizon Settings

After completing Solo Setup or manually configuring ground and height settings, configure camera height and horizon settings. The **Camera & Horizon** tab is used for manually discovering people in the scene and configuring human markers.

To manually configure camera and horizon settings

1. Click the **Step 2: Camera & Horizon** tab. The **Step 2: Camera & Horizon** screen opens.
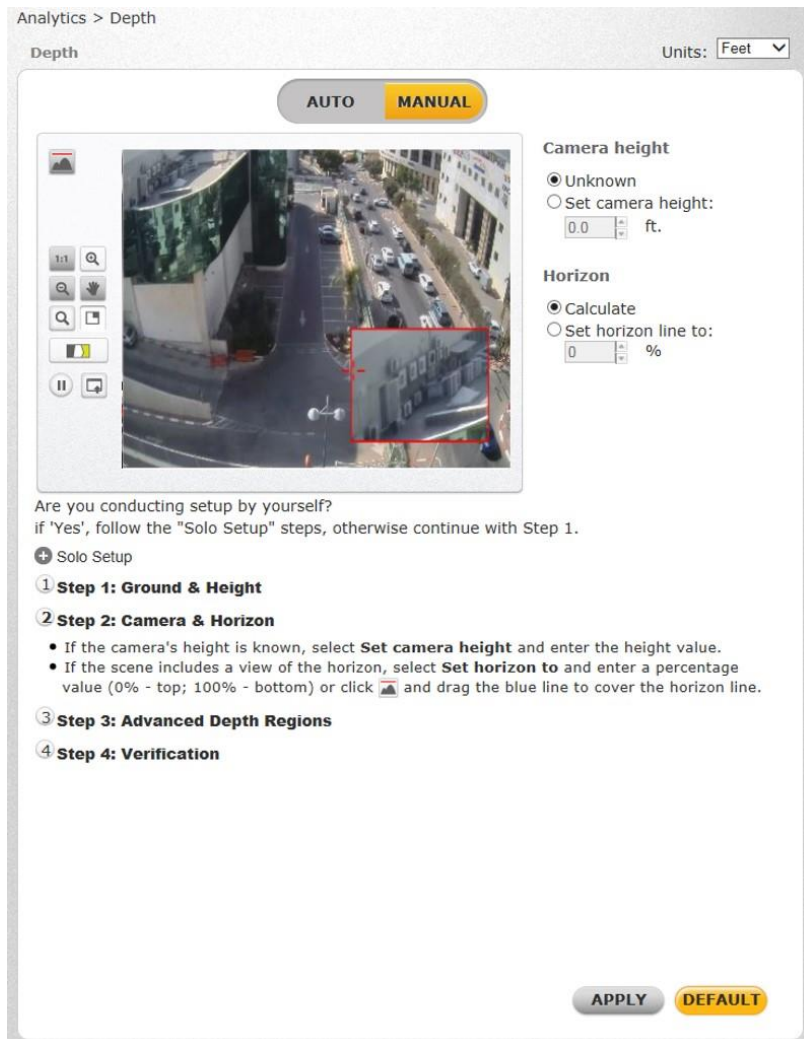
Figure 84: Analytics > Depth > Step 2: Camera & Horizon Screen

2. Follow the on-screen instructions to configure camera and horizon settings.

Figure 85: Analytics > Depth > Step 2: Camera & Horizon Instructions

3. Refer to the *HTML Edition Units User's Guide* for detailed instructions on configuring these settings.

4. Click **APPLY** when finished or continue to the next step.

Configuring Advanced Depth Region Settings

After configuring camera and horizon settings, configure advanced depth region settings.

To configure advanced depth region settings

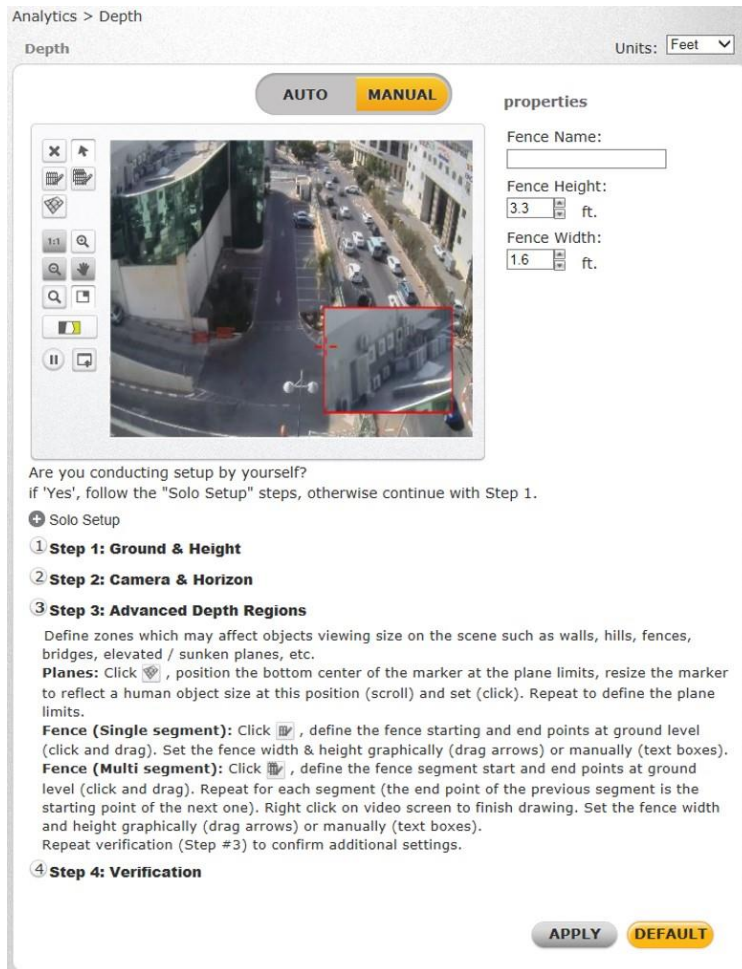1. Click the **Step 3: Advanced Depth Regions** tab. The **Step 3: Advanced Depth Regions** screen opens.

Figure 86: Analytics > Depth > Step 3: Advanced Depth Regions Screen

2. Follow the on-screen instructions to configure advanced depth region settings.

Figure 87: Analytics > Depth > Step 3: Advanced Depth Regions Instructions

3. Refer to the *HTML Edition Units User's Guide* for detailed instructions on configuring these settings.

4. Click **APPLY** when finished or continue to the next step.

Settings Verification

After configuring advanced depth region settings, verify your settings.

To verify settings

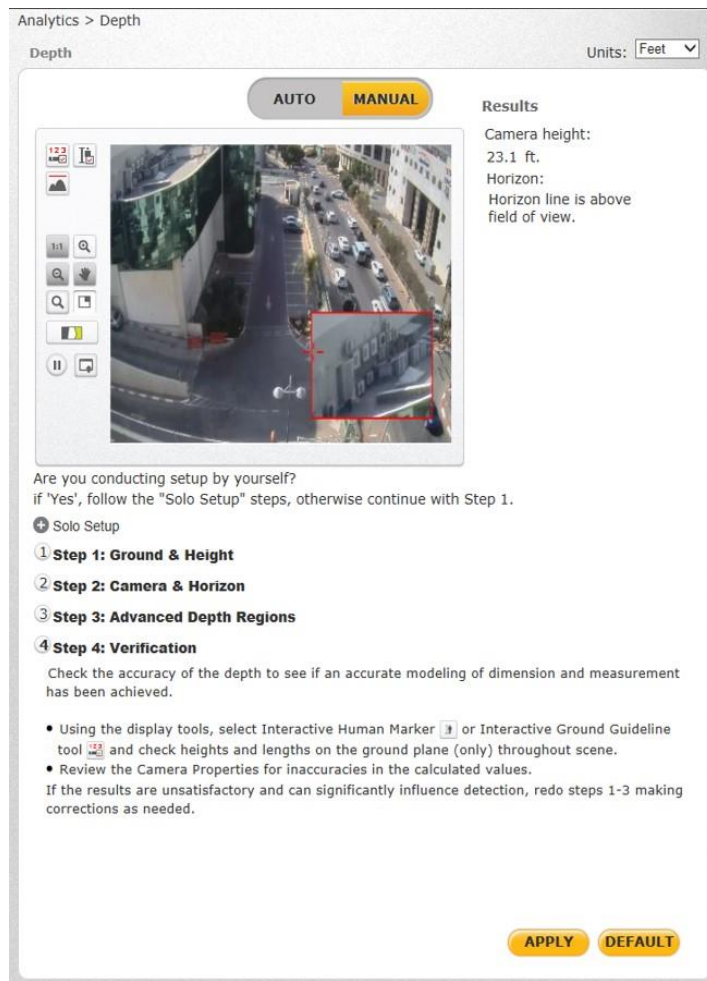1. Click the **Step 4: Verification** tab. The **Step 4: Verification** screen opens.

Figure 88: Analytics > Depth > Step 4: Verification Screen

2. Follow the on-screen instructions to verify settings.

Figure 89: Analytics > Depth > Step 4: Verification Instructions

3. Refer to the *HTML Edition Units User's Guide* for detailed instructions on configuring these settings.

4. Click **APPLY** when finished.

9.6.2 Rules

The **Rules** tab enables you to define detection rules according to the type of detection you want to be notified about. By default, the *Human or vehicle enter region* rule is enabled.
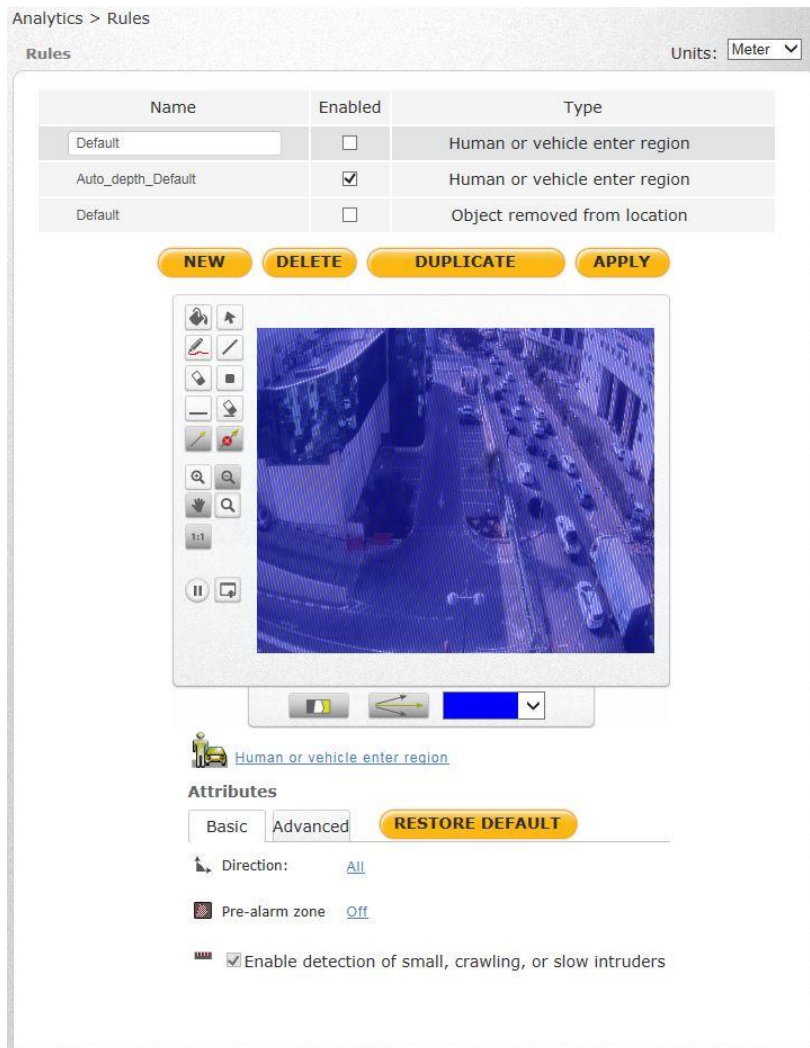

Figure 90: Analytics > Rules Screen

To select a different rule, click the *Human or vehicle enter region* link. Select the rule from the drop-down list.
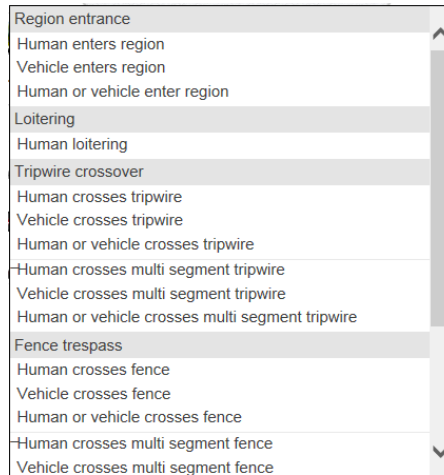

Figure 91: Rules Drop-down List

You can assign a name for the rule in the *Name* text box at the top of the screen. Select the *Enable* checkbox to activate the rule.

Detection occurs when one or more detection rules are active, the camera is in *Arm* mode, and the scenario on the video (scene) fits the detection criterion specified. When the conditions of a detection rule are met, an alarm is shown in which you can observe the detection and take the appropriate action.

Rules are configured by clicking the **Basic** or **Advanced** Attributes tabs. The **Basic** tab displays minimal information for the rule. Click **RESTORE DEFAULT** to return to factory default settings.

Figure 92: Analytics > Rules > Basic Attributes Tab

The **Basic** tab includes a setting, *Enable detection of small, crawling, or slow intruders*, which is enabled by default. The setting can detect sophisticated intruders (for example a camouflaged or crawling person) and identify people who are standing or moving upright, which helps to reduce false alarms.

> **Note:**
>
> The following limitations apply to this function:
>
> 1. It is possible that a person who is not standing upright might not be detected when:
>   - Crawling
>   - Walking on all four (like an animal)
>   - Camouflaged to look like an inanimate object (i.e., small tree)
>   - Running and viewed from the side
>   - Bent over and viewed from the side
>
> 2. The camera should not be facing straight down (i.e., it should be at a 30-40 degree angle from the object).

The **Advanced** tab displays additional information for the rule. Click **RESTORE DEFAULT** to return to factory default settings.

Figure 93: Analytics > Rules > Advanced Attributes Tab

Refer to the *HTML Edition Units User's Guide* for detailed instructions on configuring these settings.

9.6.3 Responses

The camera's embedded event engine enables you to define a set of responses (automatic actions) for selected events and to perform actions (scheduled actions) at pre-defined times during a defined monitoring period. Refer to the *HTML Edition Units User's Guide* for detailed instructions on configuring these settings.
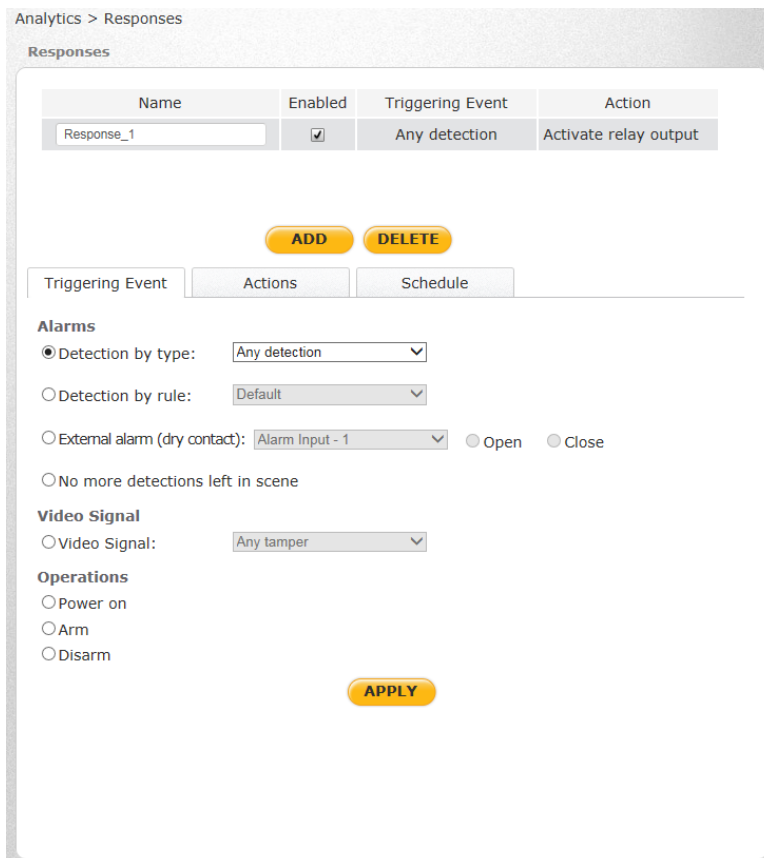

Figure 94: Analytics > Responses Screen

Each automatic response definition includes the following three parameters: Triggering event, Actions and Schedule.

1. Triggering event – Select the event that will start the automatic response.

Figure 95: Responses > Triggering Event Tab

To define a triggering event

1. Click **ADD**. A new Response is displayed in the top of the screen.

2. Select *Enable* to activate the Response.

3. From the *Detection by type* drop-down list, select one of the following detection types: *Any detection* (default), *Intrusion detection, Vehicle Stopped, Unattended Object, Object Removed, Tripwire detection, Fence detection,* or *Loitering detection.* The selection is displayed in the top of the screen.

4. From the *Detection by rule* drop-down list, select a rule that was defined in the *Rules* tab.

5. From the *External alarm (dry contact)* drop-down list, select *Alarm Input -1* or *Alarm Input - 2*. Then select *Open* or *Close* to trigger an event when the contact is Normally Open or Normally Closed.

6. Select *No more detections left in scene* if you want the triggering event to occur when there are no additional objects remaining in the scene to be detected.

7. From the *Video Signal* drop-down list, select one of the following: *Any tamper, Video Signal Ok, No Video Signal, Low Video Signal, Bad Video Signal,* or *Camera Shift.*

8. Select one of the following operations to define when the triggering action will occur:
   - Power on
   - Arm
   - Disarm

9. Click **APPLY** to save the configuration.

To delete a triggering event

1. Select the event from the top of the **Responses** screen.

2. Click **DELETE**. The event is deleted.

2. Actions – Select the action to perform in response to the occurrence of the triggering event. The configurable settings depend on the selected action.

Figure 96: Responses > Actions Tab

> **Note:**
> Actions related to an analytic event that is defined in this screen are not affected by the status of the alarm switch configured on the **Events Setup > IO** screen.

To define an action

1. From the *Action* drop-down list, select one of the following Actions. The selection is displayed at the top of the screen.

   - Activate relay output

     a. Select Activate relay immediately or enter the number of seconds (1-999) in After x seconds drop-down list.

     b. Select the Relay number.

     c. Select the Activation signal:

        - Continuous – From the drop-down list, select *On* or *Off*.

        - Pulse activation – In the *Sec.* text box, enter the number of seconds for the Pulse duration.

     d. Click **APPLY**.

   - Clear alarms

     a. Select *Clear alarms immediately* or enter the number of seconds (1-999) in *After x seconds* drop-down list.

     b. Click **APPLY**.

   - Arm camera

     a. Select *Arm immediately* or enter the number of seconds (1-999) in *After x seconds* drop-down list.

     b. Click **APPLY**.

   - Disarm camera

     a. Select *Disarm immediately* or enter the number of seconds (1-999) in *After x seconds* drop-down list.

     b. Click **APPLY**.

   - Enable detection rule

     a. Select *Perform immediately* or enter the number of seconds (1-999) in *After x seconds* drop-down list.

     b. Click **APPLY**.

   - Disable detection rule

     a. Select *Perform immediately* or enter the number of seconds (1-999) in *After x seconds* drop-down list.

     b. Click **APPLY**.

2. To add an action, click **ADD**. The action is displayed in the *Actions* table.

Triggering Event	Actions	Schedule

Step	Action	Settings
1	Activate relay output	...
2	Arm camera	...

UP   DOWN   ADD   DELETE

Figure 97: Responses > Actions Table

3. Repeat step 1 for each new Action.

4. To change the order of the Actions, click **UP** or **DOWN**.

5. To delete an action, select the Action and click **DELETE**.

6. Click **APPLY** when finished.

7. Schedule – Define when to monitor the triggering event occurrence.

Triggering Event	Actions	Schedule

○ Always
◉ Monitor event occurrences:
   From: 09/07/2015   To: 09/07/2015
   ☐ No end date
   Weekdays: ☐ Sun ☑ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat
   Between: 8:00-14:00   **?** (Ex: 8:00-12:00 14:30-17:00...)

APPLY

Figure 98: Responses > Schedule Tab

To set a schedule

1. Do one of the following:

    *   Select *Always.*

    *   Select Monitor event occurrences.

        *   In the *From* text box, enter the start date.

        *   In the *To* text box, enter the end date. If there is no end date, check *No end date.*

        *   From the *Weekday*s list, select the day of the week.

        *   In the *Between* text box, enter the hours during which the monitoring will occur.

2. Click **APPLY**.

9.6.4 Scheduled Actions (Sched. Actions Screen)

The **Sched. Actions** screen is used for setting schedules for actions to be taken when an event occurs.

Figure 99: Sched. Actions > Actions Tab

Each scheduled action includes the following two parameters: Actions and Schedule

1. Actions – Select the action to perform at the scheduled time

To define an action

1. From the *Action* drop-down list, select one of the following actions: *Activate relay output, Clear alarms, Arm camera, Disarm camera, Enable detection rule,* or *Disable detection rule*. The selection is displayed at the top of the screen.

   - Activate relay output

   a. Select *Activate relay immediately* or enter the number of seconds (1-999) in *After x seconds* drop-down list.

   b. Select the Relay number.

   c. Select the Activation signal:

      - Continuous – From the drop-down list, select *On* or *Off*.
      - Pulse activation – In the *Sec.* text box, enter the number of seconds for the Pulse duration.

   d. Click **APPLY**.

- Clear alarms

    a. Select *Clear alarms immediately* or enter the number of seconds (1-999) in *After x seconds* drop-down list.

    b. Click **APPLY**.

- Arm camera

    a. Select *Arm immediately* or enter the number of seconds (1-999) in *After x seconds* drop-down list.

    b. Click **APPLY**.

- Disarm camera

    a. Select *Disarm immediately* or enter the number of seconds (1-999) in *After x seconds* drop-down list.

    b. Click **APPLY**.

- Enable detection rule

    a. Select *Perform immediately* or enter the number of seconds (1-999) in *After x seconds* drop-down list.

    b. Select the name of the rule defined in the **Rules** tab.

    c. Click **APPLY**.

- Disable detection rule

    a. Select *Perform immediately* or enter the number of seconds (1-999) in *After x seconds* drop-down list.

    b. Select the name of the rule defined in the **Rules** tab.

    c. Click **APPLY**.

2. To add an Action, click **ADD**. The action is displayed in the *Actions* table at the top of the screen.

Triggering Event	Actions	Schedule
Step	**Action**	**Settings**
1	Activate relay output	...
2	Arm camera	...

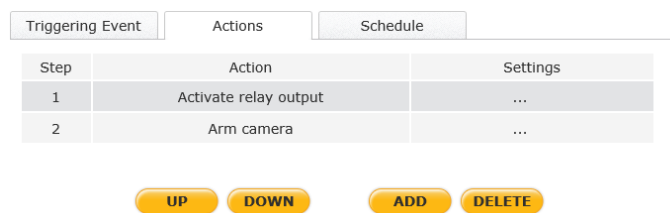UP   DOWN   ADD   DELETE

Figure 100: Responses > Actions Table

3. Repeat step 1 for each Action.

4. To change the order of the actions, click **UP** or **DOWN**.

5. To delete an action, select the action and click **DELETE**.

6. Click **APPLY** when finished.

2. Schedule – Select when to perform the actions.

Figure 101: Sched. Actions > Schedule Tab

To set a schedule

1. Do one of the following:

   - Select *Always.*

   - Select Monitor event occurrences.

     - In the *From* text box, enter the start date.

     - In the *To* text box, enter the end date. If there is no end date, check *No end date.*

     - From the *Weekday*s list, select the day of the week.

     - In the *Between* text box, enter the hours during which the monitoring will occur.

2. Click **APPLY**.

Refer to the *HTML Edition Units User's Guide* for detailed instructions on configuring these settings.

9.6.5 On Screen Display

The **On Screen Display** screen determines the information to be displayed on the video screen as an overlay on top of the video. The settings on this screen define the selection, alignment and color configuration of the various overlays that appear during normal monitoring, events and detection.

Figure 102: Analytics > On Screen Display Screen

The **On Screen Display** screen includes the following default settings:

* Enable analog video output

* Display tracking information

* Tracking shape: Rectangle

* Display trail enabled (10 seconds)

* Tracking color: Custom

* Radial button 1: Red

* Display camera information

* Font: Terminal

* Font size: Medium

In the table, select the settings that you want to configure:

- In the *Display* column, select the checkbox to display the display item.

- In the *Caption* column, click *Set* to change the name of the display item. You cannot change the names *Channel name, Date, Time* and *Status*.

- In the *Background color, Foreground color, Horizontal Align,* and *Vertical Align* columns, clicking a field opens a drop-down list. Select one of the options from the drop-down list.

Click **APPLY** when finished.

Refer to the *HTML Edition Units User's Guide* for detailed instructions on configuring these settings.

9.6.6 Firmware

The **Firmware** screen displays the current analytics firmware version and enables you to update the unit's analytics firmware file.
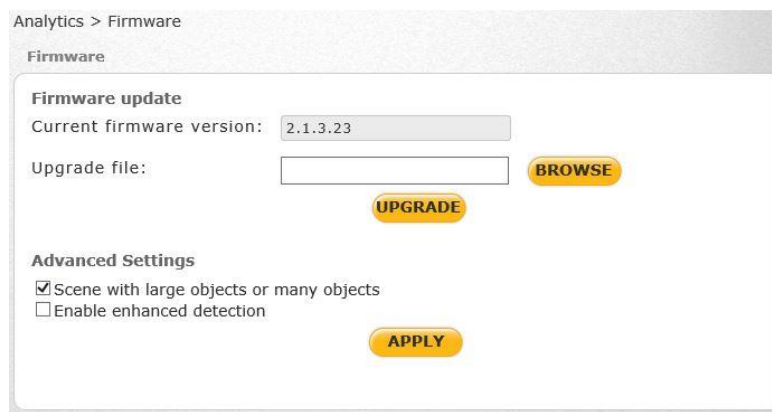

Figure 103: Analytics > Firmware Screen

To update the analytics firmware file

1. Click **Browse**

2. Select the file.

3. Click **UPGRADE**.

Using Advanced Settings

In the *Advanced Settings* area, the *Scene with large objects or many objects* setting improves analytic detection in scenes where there are large or multiple objects, and where there is movement in up to 80% of the frame. The setting is enabled by default.

Also in the A*dvanced Settings* area, the *Enable enhanced detection* setting improves the distance from which smaller objects are detected. This function is disabled by default.

Click **Apply** when finished.

> **Note:**
> 1. Analytics firmware is stored in a separate file than the camera system software. To view the camera system software version, see System > Software Version. To upgrade the camera system software version, see System > Software Upgrade.
> 2. You must close and restart Internet Explorer in order to view the new firmware version.

Refer to the *HTML Edition Units User's Guide* for detailed instructions on configuring these settings.

9.6.7 Backup & Restore

The **Backup & Restore** screen enables you to create backup files of the unit's analytics settings and to restore them.
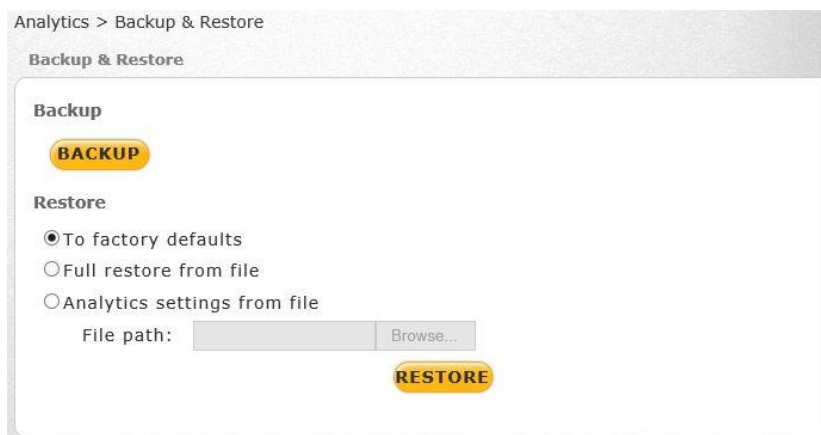

Figure 104: Analytics > Backup & Restore Screen

To back up the analytic firmware file

1. Click **BACKUP**.

To restore the analytic firmware file

1. Do one of the following:

   - To restore factory defaults, select *To factory defaults.*

   - To restore all defaults from a stored file, select *Full restore from file,* click **Browse** to locate the file path, then select the file.

   - To restore analytic settings from a stored file, select *Analytic settings from file,* click **Browse** to locate the file path, then select the file.

2. Click **RESTORE**.

   Note:
   Analytics firmware is stored in a separate file than the camera system software. To backup and restore the camera system software version, see System > Factory Default.

Refer to the *HTML Edition Units User's Guide* for detailed instructions on configuring these settings.

9.7   Log Out

Select the *Log Out* link in the navigation bar to close the session. The following message appears:
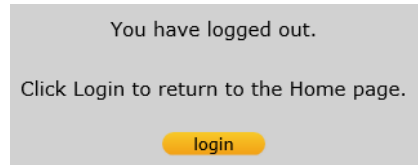
Figure 105: Logout Message

To return to the application, click **Login**. The **Login** dialog box opens. See Figure 16: Login Dialog Box.

10 Appendices

- [Technical Specifications](#)

- [Internet Security Settings](#)

- [Install UPnP Components](#)

- [Installing and Deleting the Web Player](#)

- [Deleting Temporary Internet Files](#)

- [Back Focus Adjustment](#)

- [Connecting Wires to a Spring Clamp Terminal Block](#)

- [Mounting and Lens Accessories](#)

A.1. Technical Specifications

Camera	CF-5212	CF-5222
Image Sensor	1/3" Progressive 1.3MP CMOS	1/2.8" Progressive 2.1MP CMOS
Effective Pixels	1600 x 896	1920 x 1080
Shutter Speed	1/1.5 to 1/10,000 (PAL) 1 to 1/10,000 (NTSC)	

Sensitivity (w/ analytics)	Color Mode	0.1 lux @ F1.4 @ 15 FPS, 36dB max. gain	0.2 lux @ F1.4@ 15 FPS, 36dB max. gain
	Night Mode	0.05 lux @ F1.4 @ 15 FPS, 36dB max. gain	0.1 lux @ F1.4@ 15 FPS, 36dB max. gain
Enclosure		Tamper-resistant surface mount plastic case or IK10 rated vandal IP66	

Lens	CF-5212	CF-5222
Lens Type	See Mounting and Lens Accessories for a list of optional lenses	
Lens Mounting	CS mount	

Video		
Video Compression	Fully compliant H.264 main profile/MJPEG	
Video Resolution	1600 x 896/HD 720p/D1 (H.264/MJPEG)	Full HD 1080p/HD 720p/D1 (H.264/MJPEG)
Video Streaming	Single stream H.264 1600 x 896 (25/30fps) or MJPEG 1600 x 896 (25/30fps)	Single stream H.264 1080p (25/30fps) or MJPEG 1080p (25/30fps)
Maximum Performance	30fps @ HD 720p/1.3 MP	30fps@ Full HD 1080p
Rate Control Option	CBR (64Kbps – 20,480Kbps), VBR	

Operation		CF-5212	CF-5222
Image Setting	Brightness	Manual	
	Sharpness	Manual	
	Contrast	Manual	
	Hue	Manual	
	Exposure	With Shutter WDR Enabled	With Shutter WDR Disabled
		Auto Mode	DC Auto Iris/Auto Shutter/ Shutter Priority/Flickerless/ Manual Mode
	Backlight	With Shutter WDR Enabled	With Shutter WDR Disabled
		N/A	On/Off
	Digital (Gamma) WDR	With Shutter WDR Enabled	With Shutter WDR Disabled
		N/A	On/Off
	WDR	Digital and True (120dB) Shutter WDR (On/Off)	Digital and True Shutter (96dB) WDR On/Off
	Noise Reduction	3DNR: On/Off + 3 levels (with Latitude), On/Off + 3 levels (without Latitude); 2DNR (On/Off)	
	Privacy Mask (Video Mask)	Web interface: On/Off. Up to five embedded web interfaces are supported in the streaming video output, but are not supported by Latitude. In the Latitude interface, the Privacy Mask is independent of the camera's on-screen display and is not embedded.	
	IR Function	Day/Night (Auto/On/Off/Smart)	

Operation		
Audio	Two-way Audio	Line out and Line in/Mic-in
	Compression	G.711/G.726 (not supported by Latitude)
	Connections	Terminal block
Alarm	Input	1x 5V 10kΩ pull up dry contact
	Output	1x Photo Relay Output 300V DC/AC @ 130mA maximum
Event Notification		HTTP, FTP, SMTP
Languages		English, Spanish, Japanese, Russian, and Simplified Chinese
MicroSD Card Recording		This function is not supported in the current version and is not supported by Latitude.

Network	
Interface	1 x 10/100/1000Mbps (IEEE 802.3/802.3u/802.3ab) RJ45
Protocols	IPv4, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, ICMP, FTP, NTP, SMTP, DHCP, PPPoE, UPnP, IGMP, SNMP, QoS, and ONVIF™ Profile S
Password Levels	User and Administrator
Security	HTTPS, IP Filter, IEEE 802.1x
Firmware Upgrade	Flash memory for upgrade of camera firmware over the network (4GB Flash/8GB RAM)
Operating Systems	Windows XP, 7, 8, 8.1, and 10
Internet Browser	Internet Explorer (IE 9, 10, and 11)
User Accounts	20

Mechanical		
Connectors	Power	3-pin terminal block
	Ethernet	RJ45
	Audio	Line-out: 3.5 mm audio jack Line-in/Mic-in: 3.5 mm audio jack
	Alarm	7-pin terminal block with 2-pin alarm input and 2-pin relay output
	Analog Video	1.0V p-p/75Ω, BNC (continuously enabled)
	MicroSD card	Not supported
LED Indicator		Power, Link, ACT
Enclosure Standards		IP66, NEMA 4, 1K10 vandal-resistant
Mechanical IR Cut Filter		Included

Physical	
Dimensions (L x W)	125 x 82 x 52 mm (4.9 x 3.2 x 2 in.) without lens
Weight	330g (0.73 lbs.)

Electrical	
Power Consumption	8W
Power Source	12VDC (± 10%), 24VAC (± 10%), PoE (802.3af Class 0)

Environmental	
Operating Temperature	-10º to 50º C (14° to 122°F)
Humidity	10-90% non-condensing

General		
Regulatory	US	FCC (47 CFR) Part 15, Subpart B, Class A; UL
	International	CE-marked (IEC 60950-1:2005+A1:2009 and EN 60950-1:2006+A11:2009+A1:2010+A12:2011); EN55032:2012; EN55024, IEC 61000; EN61000; CISPR 22: 2009 Class A; EN 50130; ICES-003 Issue 5; RCM; RoHS
Warranty		Four-year limited warranty

A.2. Internet Security Settings

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.
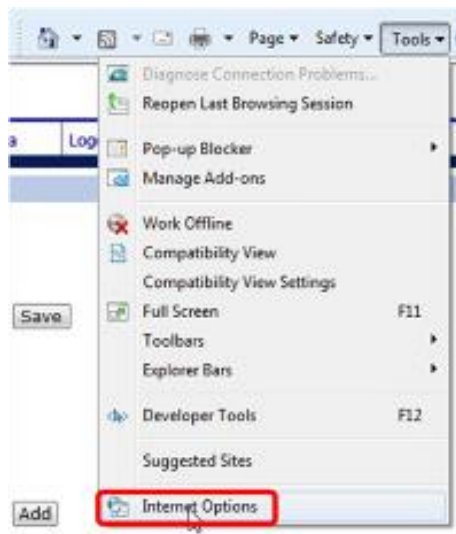

Figure 106: Command Bar Toolbar – Select Internet Options

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

Figure 107: Internet Options Screen

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

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.

Figure 108: Command Bar Toolbar – Internet Options

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

4. If not already selected, select [Internet] , then select *Custom Level.*

5. In the dialog that appears, under **ActiveX controls and plug-ins** set ALL the following options (listed below) 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
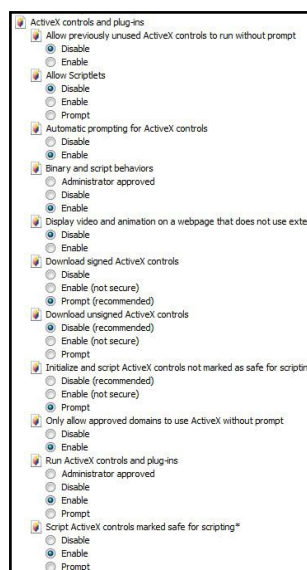
Figure 109: Schedule Screen

6. Click **OK** to accept the settings and close the **Security** screen.

7. Click **OK** to close the **Internet Options** screen.

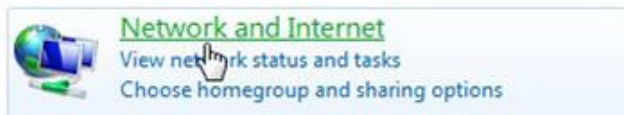8. Close the browser window and restart IE again to access the camera.

A.3. Install UPnP Components

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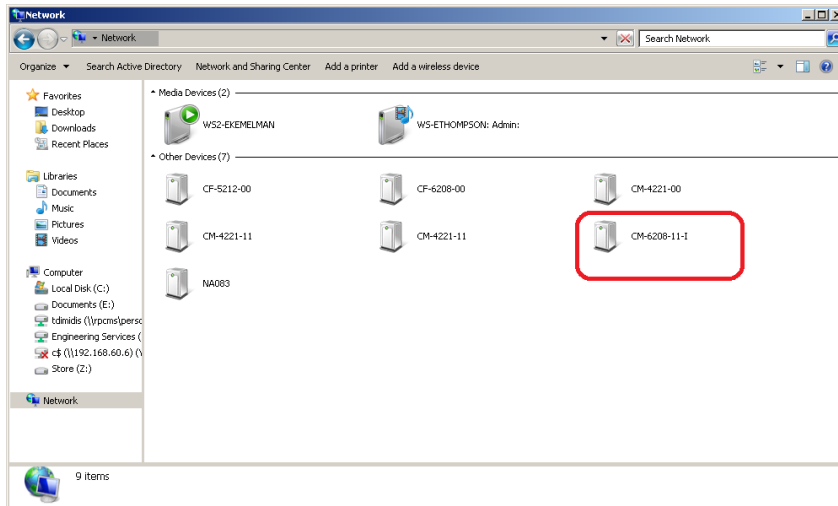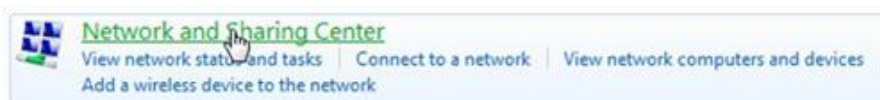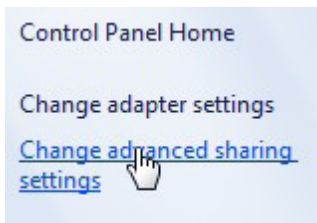

To enable UPnP discovery in Windows 7, 8, 8.1, and 10

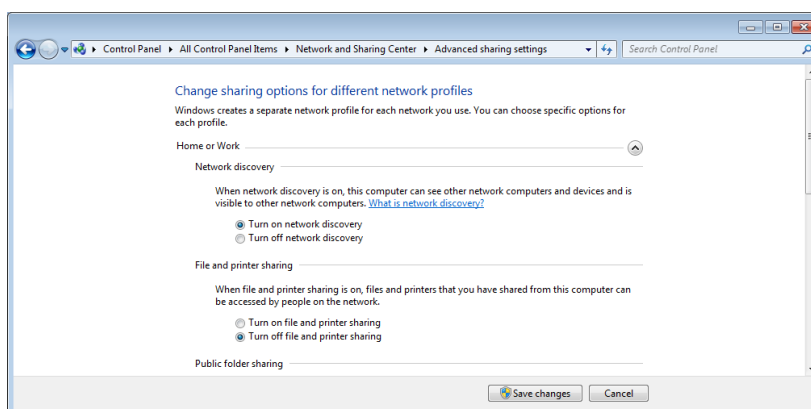1. Click (Start) and select *Control Panel*.

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.*


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 check that the UPnP Device Host services are running

1. Click (Start) and type in the Search programs and files field **services.msc** and then select **services.msc** from the displayed Programs. The **Services manager** dialog box appears.
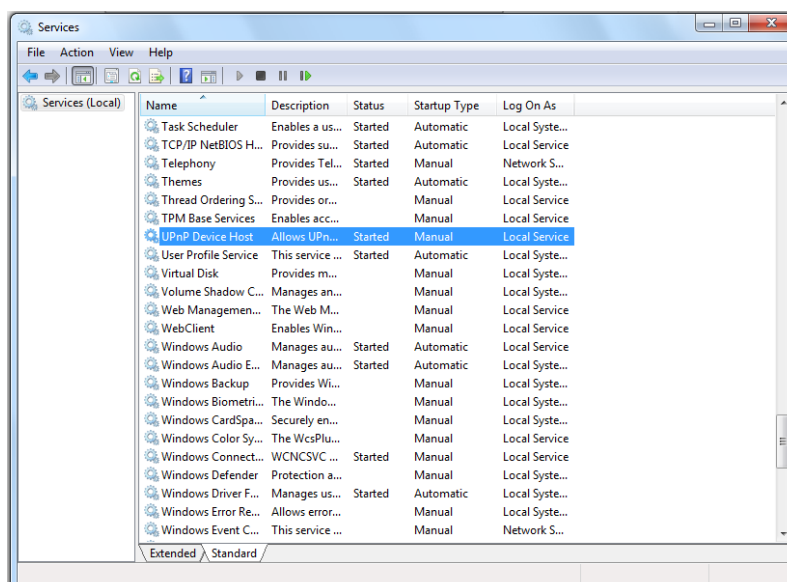
2. In the **Services manager** dialog box, scroll down the list to *UPnP Device Host* and verify that it shows the status *Started*. If *Started* is not displayed, right-click and select **Start** from the shortcut menu.

A.4. Installing and Deleting the Web Player

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

If this is a first-time installation of the camera, the Quasar Player installation wizard opens after accessing the camera.
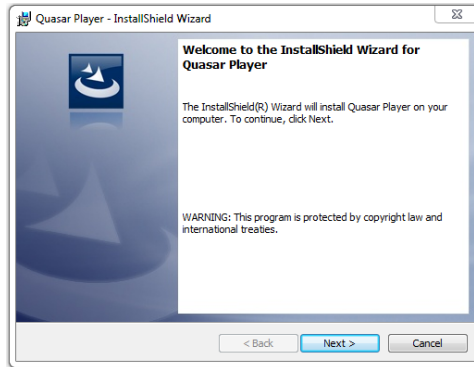

Figure 110: Quasar Player Installation Wizard

To install the Quasar Player

1. Click **Next**. The Player is installed.

1. Click **Finish** when the next screen opens. The installation is completed. **Quasar Player** is displayed in the list of installed programs.
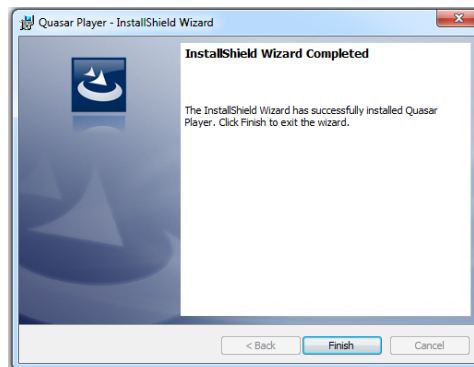

Figure 111: Quasar Player Installation Completed

Users who have previously installed the DVPlayer or DCViewer web player in the PC should first delete the existing player file from the PC and then install the Quasar Player before accessing the camera.

To delete an existing DVPlayer or DCViewer file

1. Click **Start** and select **Control Panel**. The **Control Panel** opens.

2. In the Control Panel, click **Uninstall a program**.
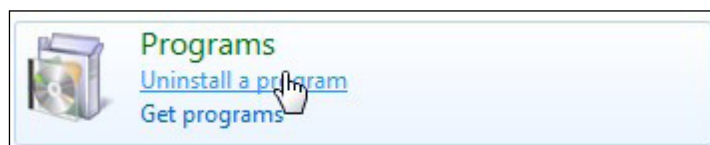
2. From the installed program list, select **DVPlayer** or **DCViewer.**

3. On the banner bar, click **Uninstall**.

4. 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.

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

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 Quasar Player installation wizard opens.

6. Follow instructions above to install the Quasar Player.

A.5. Deleting Temporary Internet Files

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.
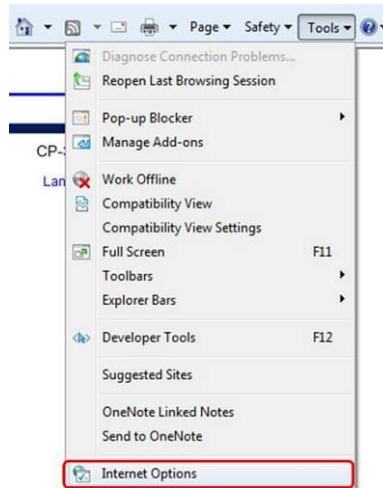
2. In the **General** tab in the *Internet Options* dialog box, click **Delete**.

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**.
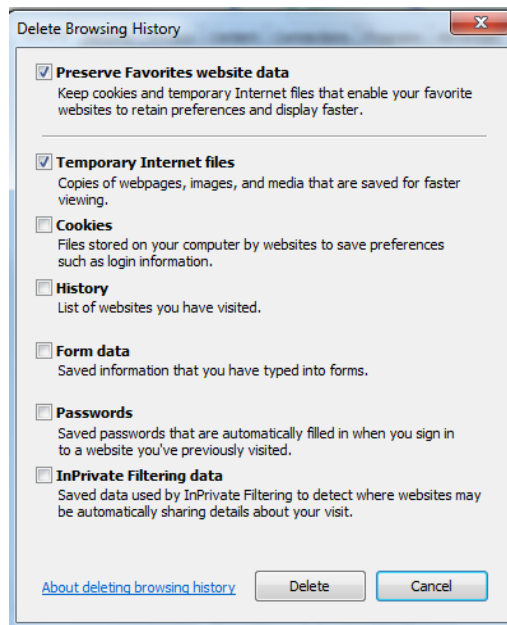
A.6. Back Focus Adjustment

When to adjust back focus

Back focus refers to the distance from the rear lens element to the camera focal plane. In most cases, it is required to adjust back focus only when the camera's lens cannot hold focus throughout its zoom range. If the focus cannot be achieved within the zoom range, you may need to adjust the back focus.

Requirements:

Tools required when carrying out back focus adjustment include:

- Back focus adjuster (in the IP camera's package)
- Test chart/contrasting object

To adjust back focus

1. Set the Exposure Settings as follows:
   a. In the Viewer, select the **Camera** tab.
   b. From the **Exposure** menu, select *Auto Shutter mode*. See Camera-Related Settings.
2. Do the following:
   a. View an object at least 75 feet (23 meters) away. For greater telephoto capable lenses, the object can be located further away. If the field of view is less than this distance, the object should be as distant as possible.
   b. Adjust the zoom to the extreme telephoto position.
   c. Adjust the focus to the best possible focused image.
   d. If the image is not focused (sharp), loosen the back focus ring retaining screw with the supplied hex tool and rotate the lens mount to adjust the back focus as needed to achieve a sharp picture in focus.

Figure 112: Back Focus Adjustment

   e. Zoom out to wide-angle position (for close FOV) and attempt to focus on a close object (e.g. 1-3m.).
   f. Repeat steps a. through e. until focus is optimal throughout the zoom range.
   g. Tighten the back focus ring retaining screw to secure the ring in place.
   h. Return the camera's Exposure Setting to *Auto Iris* if this was temporarily changed to *Auto Shutter* mode during focusing.

A.7. Connecting Wires to a Spring Clamp Terminal Block

The unit is delivered with a 3-pin terminal block connector. The terminal block enables you to connect power wires to the unit.

Figure 113: Typical Spring Clamp Terminal Block

To connect a wire to the spring clamp terminal block

1. Strip the insulation from the end of each wire that is to be connected to the terminal block. Approximately 1 cm (2.54") of wire should be exposed.

2. With a small screwdriver, press in and hold the orange spring clamp button next to the female outlet where the wire will be inserted.

3. Insert the stripped end of the wire into the female outlet.
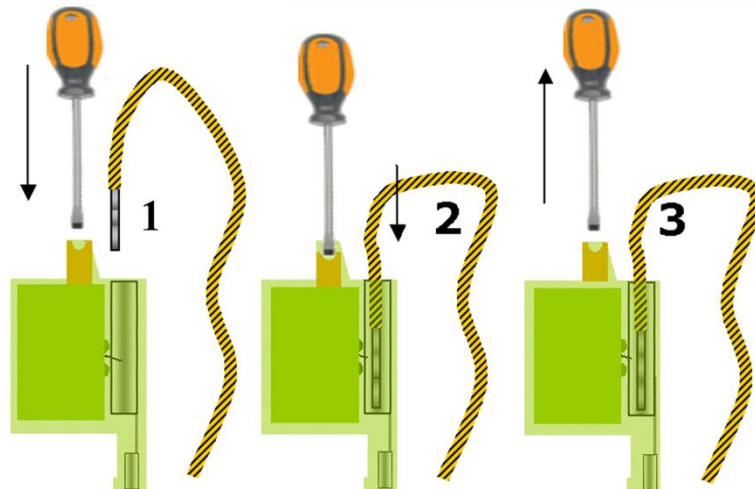
4. Release the orange spring clamp button.

Figure 114: Connecting a Wire to a Terminal Block

A.8. Mounting and Lens Accessories

The following mounting accessories are available from FLIR for installation of your IOI HD CF-5212/CF-5222 Fixed IP Camera. For more information on available options, contact your FLIR sales representative or visit www.FLIR.com/security to request details on where to get the accessories you need.

Image	Name	Description
	Mounting Accessories	
	CF-X200-01	Outdoor fixed camera housing: • Equipped with heater and fan • 24VAC @ 20W • Aluminum with sunshield • -30 to +50C (-22 to +122F) • 140 x 112x 340mm/ 5.5 x 4.4 x 13.4" (W x H x L) • 1.51Kg/3.4 lbs. Mounting bracket, screws and wrenches
	CF-X200-POLE	Pole Mount Option for CF-X200-01 Housing
	Lenses	
	CF-L131-08-50	8-50mm, f1.6, 1/2.7", 5MP Auto Iris, IR Corrected, CS-Mount
	CF-L131-31	3.1-8mm, f1.2, 1/2.7", 5MP Auto Iris, IR Corrected, CS-Mount
	CF-L131-08	8-80mm, f1.4, 1/2", 5MP Auto Iris, IR Corrected, C-Mount, packaged with CS adapter
	CF-L131-12	12.5-50mm, f1.4, 1/2.7", 5MP Auto Iris, IR Corrected, CS-Mount