Quasar™ Mini-Dome

Installation and User Guide

CM-6405/CM-6408

This document does not contain any export-controlled information.

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

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

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

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

Support: https://www.flir.com/support/
product.enterprise.support@flir.com

Important Instructions and Notices to the User:

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

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

Proper Disposal of Electrical and Electronic Equipment (EEE)

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

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

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

Document History

Revision	Date	Comment
100	December 2020	Initial FLIR release

Product Registration and Warranty Information

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

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

Table of Contents

Table of Contents

Table of Contents

1 Document Scope and Purpose

The purpose of this document is to provide installation, operation, and configuration instructions for Quasar CM-640x cameras.

Note:

This document is intended for use by technical users who have a basic understanding of CCTV camera/video equipment and LAN/WAN network connections.

Remarque:

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

Warning:

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

Avertissement:

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

Disclaimer

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

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

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

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

Avis de non-responsabilité

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

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

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

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

General Cautions and Warnings

This section contains information that indicates a procedure or condition where there are potential hazards.

SAVE ALL SAFETY AND OPERATING INSTRUCTIONS FOR FUTURE USE.

Although the unit is designed and manufactured in compliance with all applicable safety standards, certain hazards are present during the installation of this equipment.

To help ensure safety and to help reduce risk of injury or damage, observe the following:

Précautions et avertissements d'ordre général

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

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

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

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

Caution:

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

Attention:

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

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

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

⚠

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

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

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

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

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

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

2 Camera Overview

Quasar CM-640x cameras provide real-time video with 4K UHD (CP-6408-11-I) or 2560x1920 (CP-6405-11-I) high definition quality, up to 25/30 frames per second (fps). They feature True Shutter Wide Dynamic Range up to 130db; line-level audio in/out; digital I/O; and infrared (IR) illumination. When the camera is connected to an IP network, it functions as a server, providing services such as camera control, video streaming, and network communications.

Up to four streams can be run simultaneously with H.265, H.264, or MJPEG compression, providing an ideal solution when differing levels of image quality are required. The camera can increase frame rate and level of detail when events are triggered. In addition, FLIR's adaptive streaming algorithms provide the highest image quality with the lowest bandwidth and storage requirements.

If help is needed during the installation process, contact the local FLIR service representative or call the support number that appears on the product's page at https://www.flir.com/support/. All installers and integrators are encouraged to take advantage of the training offered by FLIR; visit https://www.flir.com/support-center/training/ for more information.

For safety, and to achieve the highest levels of performance from the camera system, always follow the warnings and cautions in this manual when handling and operating the camera.

Related Documentation

- *CM-640x Quick Install Guide*
- *FLIR Security Cameras - Accessory Guide*
- *DNA User Guide (see Accessing Product Information from the FLIR Website)*

2.1 Features

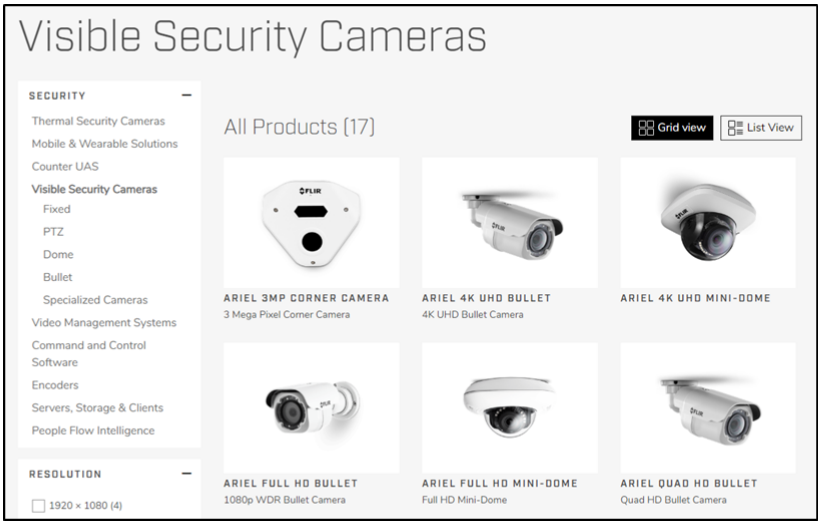
- Progressive 4K 1/1.8" or 5MP 1/2.7" CMOS sensor, depending on the model
- CP-6408-11-I: Up to 4K (3840x2160) at 25/30fps
- CP-6405-11-I: Up to 5MP (2560x1920) at 25/30fps
- Powered by IEEE 802.3af class 0 PoE, 24 VAC, or 12 VDC
- Supports Internet Explorer 11.0 (recommended), Chrome, Firefox, and Safari browsers
- Supports 8GB to 512GB microSD/microSDHC/microSDXC (Class 10) cards
- H.265, H.264, and MJPEG compression
- Motion detection event-driven alarms
- 802.1X and SSL/TLS security protocols
- Shutter (True) WDR
- 3DNR image noise reduction
- Backlight compensation
- IP66 enclosure with IK10 vandal-proof protection
- HTTP streaming MJPEG
- Built-in web server
- Tampering detection and notifications
- Infrared LED illuminator
- True day/night (ICR)
- Five privacy masks
- White balance
- Up to 20 users
- Audio line-in/line-out
- SNMP v1/v2/v3 and SNMP traps
- ONVIF© Profile S/G/T
- Alarm in/out
- UPnP support

2.2 Accessing Product Information from the FLIR Website

Up-to-date resources for the camera, including the camera’s specifications, the FLIR Discovery Network Assistant (DNA) software tool, and this installation and user guide, are available from the camera’s product details and support pages on FLIR.com.

To access product information from the FLIR website

1. Open FLIR.com and navigate to Products > Security > Visible Security Cameras.



Visible Security Cameras

SECURITY –
Thermal Security Cameras
Mobile & Wearable Solutions
Counter UAS
Visible Security Cameras
Fixed
PTZ
Dome
Bullet
Specialized Cameras
Video Management Systems
Command and Control Software
Encoders
Servers, Storage & Clients
People Flow Intelligence

RESOLUTION –
□ 1920 × 1080 (4)

All Products (17)

Grid view | List View

ARIEL 3MP CORNER CAMERA
3 Mega Pixel Corner Camera

ARIEL 4K UHD BULLET
4K UHD Bullet Camera

ARIEL 4K UHD MINI-DOME

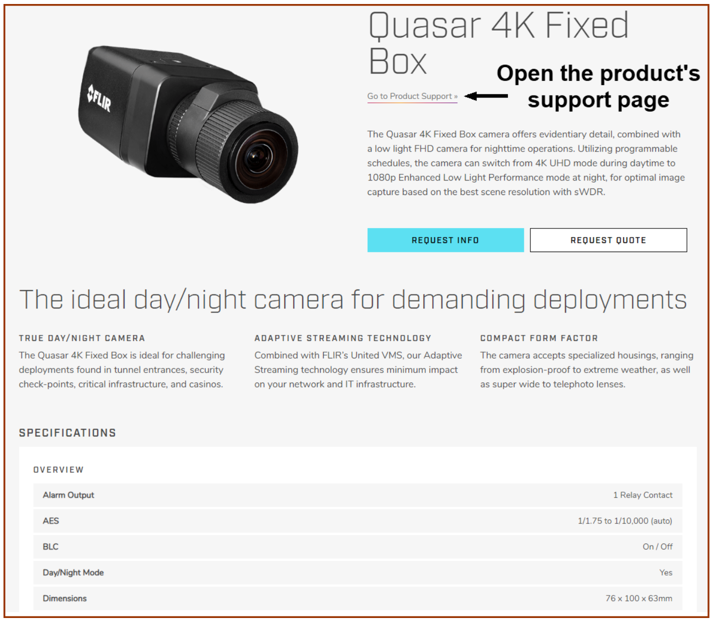
ARIEL FULL HD BULLET
1080p WDR Bullet Camera

ARIEL FULL HD MINI-DOME
Full HD Mini-Dome

ARIEL QUAD HD BULLET
Quad HD Bullet Camera

Visible Security Cameras Page on FLIR.com

2. Find and click the camera. The camera’s product details page appears. For example,



Quasar 4K Fixed Box

Go to Product Support »

Open the product's support page

The Quasar 4K Fixed Box camera offers evidentiary detail, combined with a low light FHD camera for nighttime operations. Utilizing programmable schedules, the camera can switch from 4K UHD mode during daytime to 1080p Enhanced Low Light Performance mode at night, for optimal image capture based on the best scene resolution with sWDR.

REQUEST INFO | REQUEST QUOTE

The ideal day/night camera for demanding deployments

TRUE DAY/NIGHT CAMERA
The Quasar 4K Fixed Box is ideal for challenging deployments found in tunnel entrances, security check-points, critical infrastructure, and casinos.

ADAPTIVE STREAMING TECHNOLOGY
Combined with FLIR’s United VMS, our Adaptive Streaming technology ensures minimum impact on your network and IT infrastructure.

COMPACT FORM FACTOR
The camera accepts specialized housings, ranging from explosion-proof to extreme weather, as well as super wide to telephoto lenses.

SPECIFICATIONS

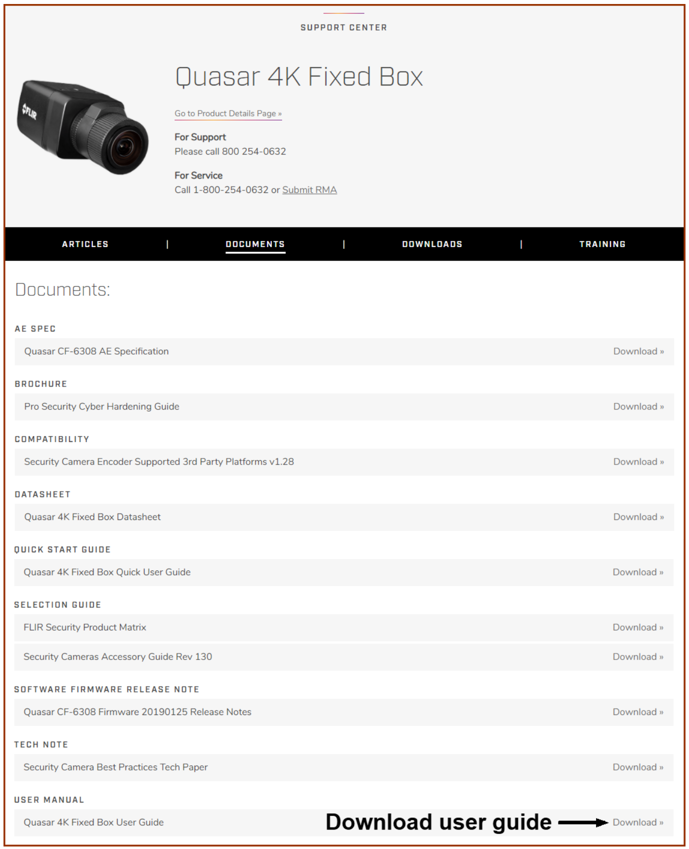
OVERVIEW

Alarm Output	1 Relay Contact
AES	1/1.75 to 1/10,000 (auto)
BLC	On / Off
Day/Night Mode	Yes
Dimensions	76 x 100 x 63mm

Product Information Page on FLIR.com (Example)

3. Scroll down to see the camera’s specifications and related documents.

4. Click **Go to Product Support** to open the camera's support page. For example,



SUPPORT CENTER

Quasar 4K Fixed Box

Go to Product Details Page »

For Support
Please call 800 254-0632

For Service
Call 1-800-254-0632 or Submit RMA

ARTICLES | DOCUMENTS | DOWNLOADS | TRAINING

Documents:

AE SPEC

Quasar CF-6308 AE Specification — Download »

BROCHURE

Pro Security Cyber Hardening Guide — Download »

COMPATIBILITY

Security Camera Encoder Supported 3rd Party Platforms v1.28 — Download »

DATASHEET

Quasar 4K Fixed Box Datasheet — Download »

QUICK START GUIDE

Quasar 4K Fixed Box Quick User Guide — Download »

SELECTION GUIDE

FLIR Security Product Matrix — Download »

Security Cameras Accessory Guide Rev 130 — Download »

SOFTWARE FIRMWARE RELEASE NOTE

Quasar CF-6308 Firmware 20190125 Release Notes — Download »

TECH NOTE

Security Camera Best Practices Tech Paper — Download »

USER MANUAL

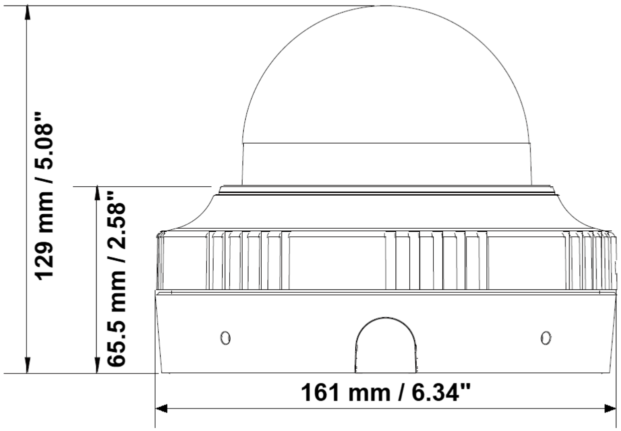
Quasar 4K Fixed Box User Guide — **Download user guide** → Download »

Product Support Page Documents Tab (Example)

5. For documents, click the Documents tab. For downloads, including the DNA (Discovery Network Assistant) tool, click the Downloads tab.

6. Click the relevant **Download** link.

2.3 Camera Dimensions



CM-640x Dimensions

3 Installation

⚠

Caution:

- Except as described in this manual, do not open the camera for any reason. Damage to the camera can occur as the result of careless handling or electrostatic discharge (ESD). Always handle the camera with care to avoid damage to electrostatic-sensitive components.
- Prior to making any connections, ensure the power supply or circuit breaker is switched off.
- Operating the camera outside of the specified input voltage range or the specified operating temperature range can cause permanent damage.

Installing the camera consists of:

1. Preparation
2. Initial Configuration
3. Mounting and Connecting the Camera
4. Additional Configuration Steps
5. Attaching the Camera to a Supported VMS

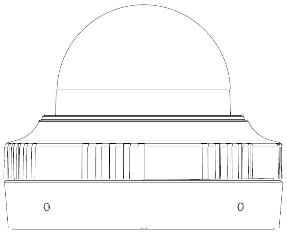
3.1 Preparation

This section contains the following important preparation information:

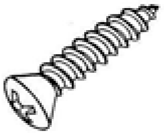
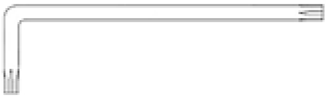
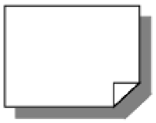
- Supplied Components
- Site Preparation - General
- Indoor Mounting
- Outdoor Mounting
- Pre-Installation Checklist
- Power Supply Options

3.1.1 Supplied Components

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



CM-640x Mini-Dome Camera

 M4 25mm Self-Tapping Screw x 4	 Plastic Screw Anchor x 4
 Torx Security (Tamper Resistant) Wrench	 *CM-640x Quick Install Guide*

Note:

The self-tapping screws are mainly for softer substrate/material installation such as wood. For other installation materials such as cement ceilings, it is necessary to pre-drill and use plastic anchors before fastening the supplied self-tapping screws into the wall.

3.1.2 Site Preparation - General

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.

⚠

Warning:

Before drilling into surfaces for camera mounting, verify that electrical or other utility service lines are not present. Serious injury or death may result from failure to heed this warning.

The physical installation of the unit is the first phase of making the unit operational in a security plan. The goal is to physically place the unit, connect it to other devices in the system, and to establish network connectivity. When finished with the physical installation, complete the second phase of installation, which is the setup and configuration of the unit.

3.1.3 Indoor Mounting

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

- There must be a fuse or circuit breaker at the starting point of the electrical wiring infrastructure.
- For indoor installations, such as industrial applications, the camera must be protected from hostile external elements (e.g. corrosive environment, metallic dust, extreme temperatures, soot, over spray, etc.).
- Do not place the camera on or near radiators and heat sources.
- All electrical work must be performed in accordance with local regulatory requirements.

3.1.4 Outdoor Mounting

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.

3.1.5 Pre-Installation Checklist

Before installing the unit, make sure that:

- Instructions in the Document Scope and Purpose section are followed.
- All related equipment is powered off during the installation.
- Use best security practices to design and maintain secured camera access, communications infrastructure, tamper-proof outdoor boxes, etc.

⚠

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 following ranges, with no more than 90% non-condensing humidity:

- With heater: -55°C to 60°C (-67°F to 140°F)
- Cold start with heater: -55°C to 60°C (-67°F to 140°F)

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 temperature de fonctionnement doit etre maintenue dans la fourchette de temperature suivante, avec un maximum de 90% d'humidite non condensee:

- *Avec chauffage: -55°C à 60°C (-67°F à 140°F)*
- *Démarrage à froid avec chauffage: -55°C à 60°C (-67°F à 140°F)*

3.1.6 Power Supply Options

The camera can be powered by:

- A UL-listed L.P.S. (Limited Power Supply) unit, rated to a maximum temperature of 60° C:
  - 12 VDC, 1.21A minimum
  - 24 VAC, 50/60Hz, 1.2A minimum
- IEEE 802.3af class 0 PoE (Power over Ethernet): 48 VDC, 0.27A minimum. Make sure that a Power Sourcing Equipment (PSE) device is used in the network.

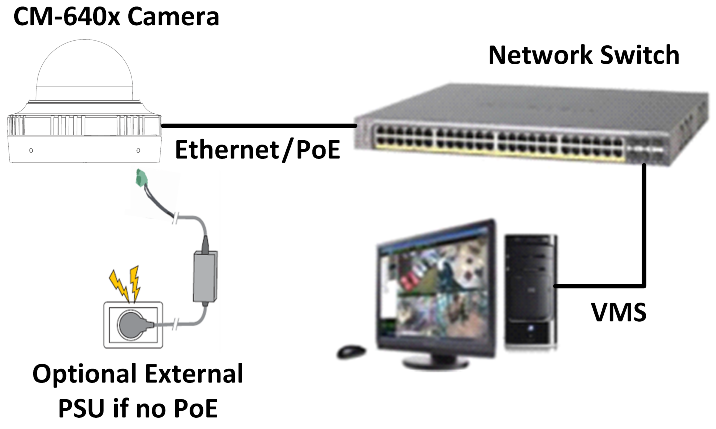
⚠

Warning:

All electrical work must be performed by a qualified service person in accordance with local regulatory requirements.

Avertissement:

Toutes les interventions électriques doivent être effectuées par un technicien qualifié conformément aux reglementations locales.



Powering the Camera

For assistance with purchasing a power supply, contact your FLIR representative.

3.2 Initial Configuration

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

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

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

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

To configure the camera for the first time:

1. Remove Dome Cover and Separate Base from Mounting Bracket
2. Connect the Camera
3. Configure for Networking
4. Change Video Format (Optional)
5. Re-attach Dome Cover

Using DNA to Configure the Camera

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

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

The camera must be made accessible for setting network addresses.

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

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

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.

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

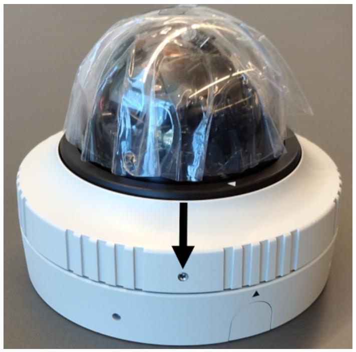
3.2.1 Remove Dome Cover and Separate Base from Mounting Bracket

Tip:

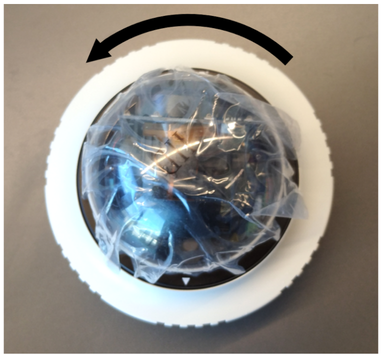
When unpacking the camera, do not remove the plastic sheet protecting the dome.

To remove the dome cover:

1. Using the Torx wrench, loosen the screw on the camera's outer circular ring that secures the dome cover to the camera base.
2. While firmly holding the base, rotate the ring counterclockwise to loosen it.
3. Carefully pull the ring and cover away from the base.



Outer Ring Locking Screw

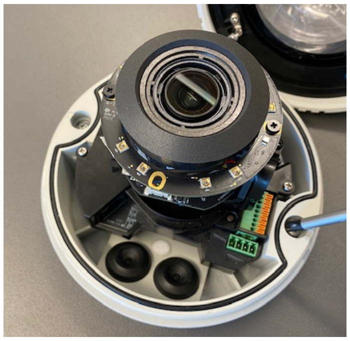


Loosen Ring

This document does not contain any export-controlled information.

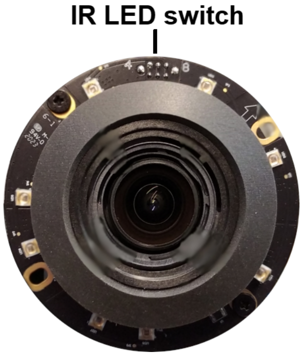
To separate the camera base from the mounting bracket:

1. Using a screwdriver, loosen the two twist-lock screws securing the camera and its base to the mounting bracket.
2. Gently pull the camera and its base away from the mounting bracket.



Change the number of LEDs (optional)

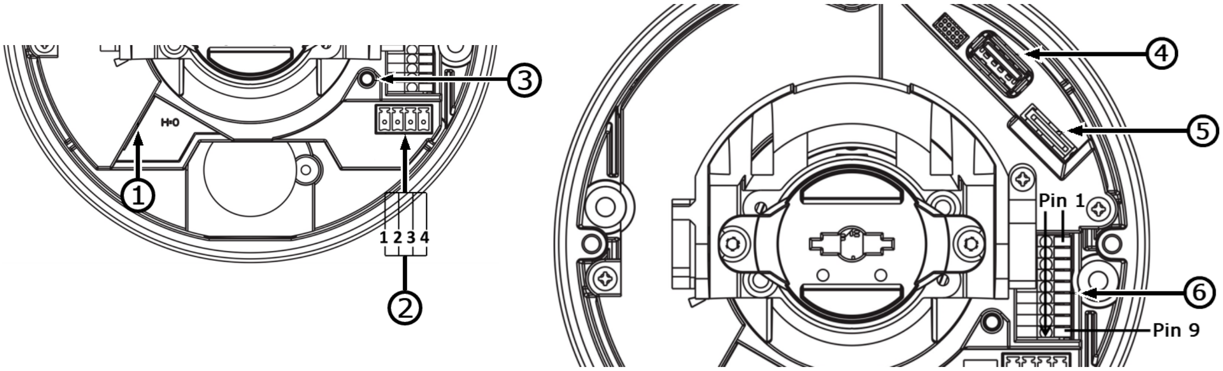
The camera has a total of eight IR illumination LEDs. On the 3D lens assembly, there is a 4 / 8 (default) switch that determines the number of enabled IR LEDs. With the dome cover removed, you can change the switch setting.



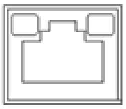
3.2.2 Connect the Camera

Warning:

This product contains a battery that is soldered to the PCB. There is a risk of explosion if the battery is replaced by an incorrect type. **Do not replace the battery.** The battery should be disposed of in accordance with the battery manufacturer's instructions.



Connectors

Connector			Connection
1	RJ-45 Two LEDs		Attach a Cat 6 cable from the network switch to the RJ45 connector for a 10/100/1000 Mbps Ethernet and IEEE 802.3af class 0 PoE connection. Ethernet is required for streaming video and for configuring the camera. The green link LED indicates a good network connection. The orange activity LED flashes to indicate network activity.

Connector		Connection				
2	Four-pin power terminal block	1	24VAC -	3	12VDC -	If using a 24VAC or 12VDC power supply, connect the wires to the power terminal block connector according to the pin assignment shown.
		2	24VAC +	4	12VDC +	
3	Default Button	To restore the camera to its factory defaults, use a proper tool to press the default button for at least 20 seconds.				
4	USB	Connects to Wi-Fi dongle (future release support)				
5	microSD Card Slot	For video clip and snapshot recording and file storage, insert a microSD / SDHC / SDXC card (up to 512 GB, Class 10) in the card slot. When the camera is powered on, do not remove the microSD card.				
6	Nine-pin I/O terminal block	1	Audio In L	6	Alarm Out +	Attach wires from external devices to the terminal block connector for alarm and audio in/out according to the pin assignment shown.
		2	Audio In R	7	Alarm Out −	
		3	GND	8	Alarm In +	
		4	Audio Out L	9	Alarm In −	
		5	Audio Out R			

Warning:
Do not connect an external power supply to the nine-pin audio/alarm I/O terminal block connector.

Warnings:

- The power cord to the 12 VDC or 24 VAC power supply unit must be connected to a socket outlet with an earthing connector.
- The PoE unit and all interconnected equipment must be installed indoors within the same building, including all PoE-powered network connections, as described by Environment A of the IEEE 802.3af standard.
- All electrical work must be performed by a qualified service person in accordance with local regulatory requirements.

Avertissement:

- *Le cordon du bloc d'alimentation 12V ou 24V doit être connecté à une prise de courant avec un connecteur de mise à la terre.*
- *L'unité PoE et tous les équipements interconnectés doivent être installés à l'intérieur du même bâtiment, y compris toutes les connexions réseau alimentées par PoE, comme décrit par l'environnement A de la norme IEEE 802.3af.*
- *Toutes les interventions électriques doivent être effectuées par un technicien qualifié conformément aux reglementations locales.*

Tip:

To make it easier to mount and install the camera, while the camera is on the bench or in the lab, you can connect Ethernet and other cable patch cords to the camera's connectors and route them through the grommets on the base and through the mounting bracket. Then, you'll be able to mount and install the camera without separating the camera base from the mounting bracket a second time.

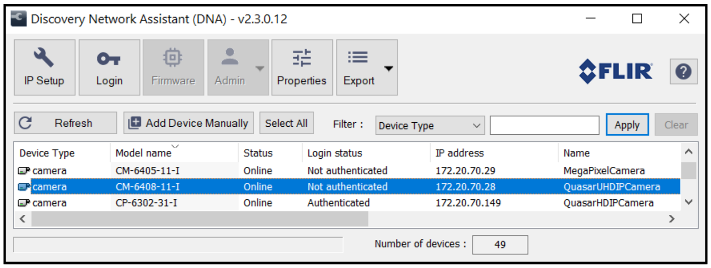
3.2.3 Configure for Networking

By default, DHCP is enabled on the camera and a DHCP server on the network assigns the camera an IP address. For example, if FLIR's Horizon or Meridian VMS is managing the camera and the VMS is configured as a DHCP server, the VMS automatically assigns the camera an IP address.

If FLIR’s Latitude VMS is managing the camera or it is on a network with static IP addressing, 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. You can manually specify the camera’s static IP address using the DNA tool or the camera's web page. The camera's default IP address is 192.168.0.250.

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

1. Make sure the camera and the PC are on the same LAN segment.
2. Run the DNA tool (DNA.exe) by double-clicking . The Discover List appears, showing compatible devices on the VLAN and their current IP addresses.



Device Type	Model name	Status	Login status	IP address	Name
camera	CM-6405-11-I	Online	Not authenticated	172.20.70.29	MegaPixelCamera
camera	CM-6408-11-I	Online	Not authenticated	172.20.70.28	QuasarUHDIPCamera
camera	CP-6302-31-I	Online	Authenticated	172.20.70.149	QuasarHDIPCamera

Number of devices : 49

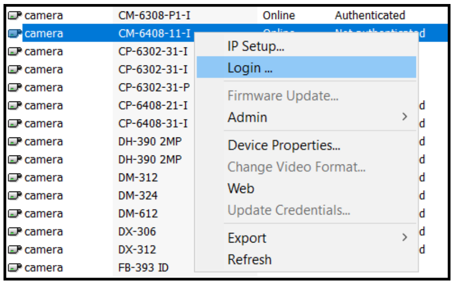
DNA Discover List

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

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

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

In the DNA Discover List, right-click the camera and select **Login**.



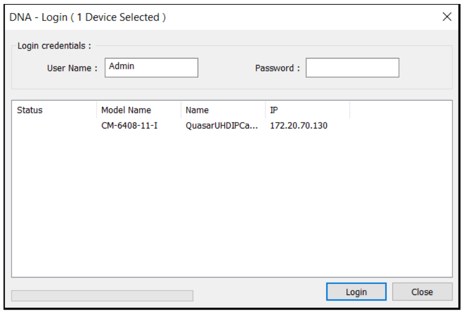
camera	CM-6308-P1-I	Online	Authenticated
camera	CM-6408-11-I	Online	Not authenticated
camera	CP-6302-31-I		
camera	CP-6302-31-I		
camera	CP-6302-31-P		
camera	CP-6408-21-I		d
camera	CP-6408-31-I		d
camera	DH-390 2MP		d
camera	DH-390 2MP		d
camera	DM-312		d
camera	DM-324		d
camera	DM-612		d
camera	DX-306		d
camera	DX-312		d
camera	FB-393 ID		

DNA > Right-click > Select Login

This document does not contain any export-controlled information.

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

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



DNA - Login (1 Device Selected)

Login credentials :

User Name : Admin

Password :

Status	Model Name	Name	IP
	CM-6408-11-I	QuasarUHDIPCa...	172.20.70.130

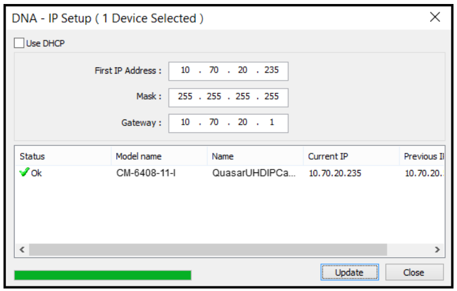
DNA - Login Window

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

3. Change the camera’s IP address.

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

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



DNA - IP Setup (1 Device Selected)

□ Use DHCP

First IP Address : 10 . 70 . 20 . 235

Mask : 255 . 255 . 255 . 255

Gateway : 10 . 70 . 20 . 1

Status	Model name	Name	Current IP	Previous II
✓ Ok	CM-6408-11-I	QuasarUHDIPCa...	10.70.20.235	10.70.20.

DNA - IP Setup Window

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

1. Access the camera's web page and navigate to the System > Network > Basic screen.

2. Select *Use fixed IP address* and then specify the camera's IP address. You can also specify the *Subnet mask*, *Default gateway*, *Primary DNS*, and *Secondary DNS*.

3. Click **Save**.

3.2.4 Change Video Format (Optional)

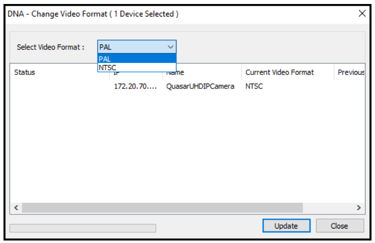
By default, NTSC is the camera's video format.

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

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

2. In the **Change Video Format** window, select PAL.

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



DNA - Change Video Format (1 Device Selected)

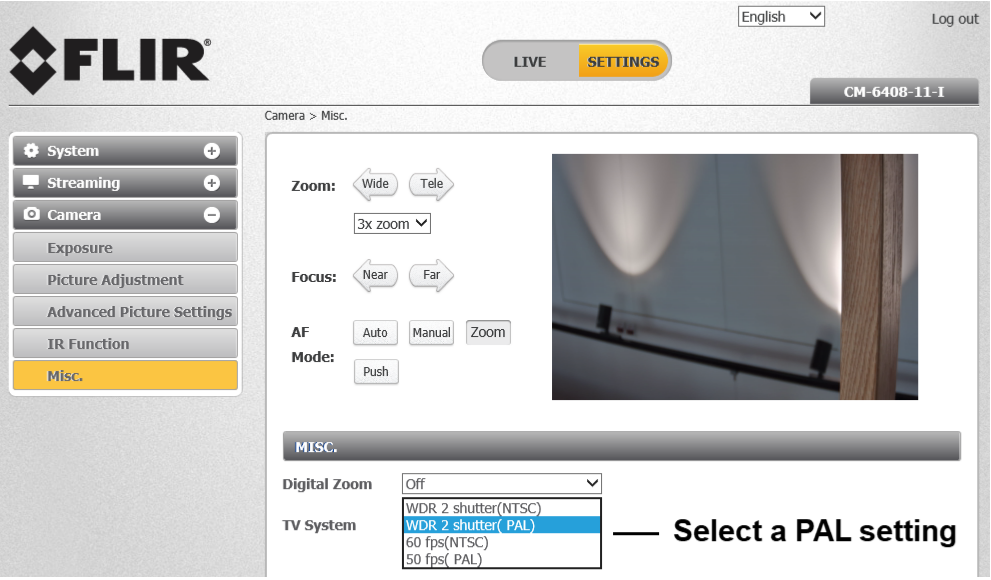
Select Video Format : PAL

Status	IP	Name	Current Video Format	Previous
	172.20.70....	QuasarUHDIPCamera	NTSC	

DNA - Change Video Format Window

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

1. Navigate to the System > Camera > Misc. screen.



Digital Zoom: Off

TV System:
WDR 2 shutter(NTSC)
WDR 2 shutter(PAL)
60 fps(NTSC)
50 fps(PAL)

Select a PAL setting

Misc. Screen

2. For *TV System*, select one of the PAL settings.

   To apply a change to the *TV System* setting, the camera needs to reboot.

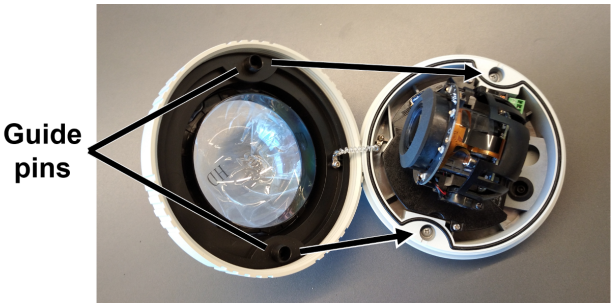
3.2.5 Re-attach Dome Cover

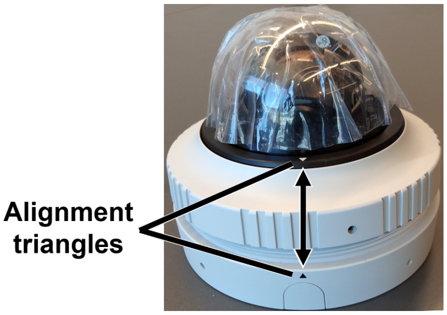
To prevent damaging the camera's internal components while moving it from the bench or lab to its mounting location, re-attach the dome cover to the base and then remove it again at the mounting location.

Before doing so, you can connect the camera to Ethernet re-attach the camera base to the mounting bracket. Use a screwdriver to tighten the two twist-lock screws securing the camera and its base to the mounting bracket. If you do not re-attach the camera base to the mounting bracket, remember to bring the screwdriver to the mounting location.

To re-attach the dome cover:

1. Using the two guide pins on the dome cover and the triangles on the cover and on the base, carefully align and position the dome cover onto the base.





2. Securely tighten the outer ring.

3. Lock the ring. Using the Torx wrench, tighten the screw on the outer ring that secures the cover to the base.

3.3 Mounting and Connecting the Camera

To mount and connect the camera:

1. Fit Mounting Hardware
2. Remove Dome Cover and Separate Base from Mounting Bracket
3. Install Mounting Bracket
4. Route Cables and Connect the Camera
5. Mount and Aim the Camera

3.3.1 Fit Mounting Hardware

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

For the list of mounting accessories available from FLIR for installing your CM-640x camera, see Accessories.

3.3.2 Remove Dome Cover and Separate Base from Mounting Bracket

Repeat the steps described in Remove Dome Cover and Separate Base from Mounting Bracket.

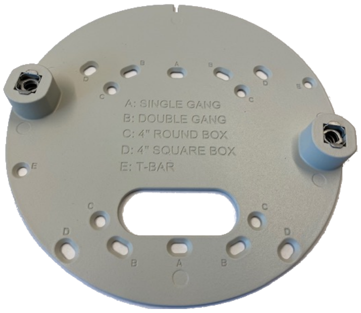
3.3.3 Install Mounting Bracket

You can install the mounting bracket on standard electrical boxes or directly on a secure, flush, and vibration-free surface.

To install the mounting bracket on a standard electrical box:

Attach the bracket to the box using:

- The holes in the mounting bracket, according to the types of boxes engraved on the bracket
- The corresponding holes in the box
- Suitable bolts, washers, and nuts (not included in the camera kit)



To install the mounting bracket directly on a surface:

1. Choose four widely spaced mounting holes on the bracket for optimum flat surface mounting.
2. Using the bracket as a template to mark the surface, drill four anchor holes.
3. (Optional) If necessary, also drill a hole wide enough through which to route the cables.
4. Hammer the four plastic screw anchors into the drilled holes.
5. Insert the anchors and then attach the bracket to the surface using the four M4 25mm self-tapping screws included in the camera kit.

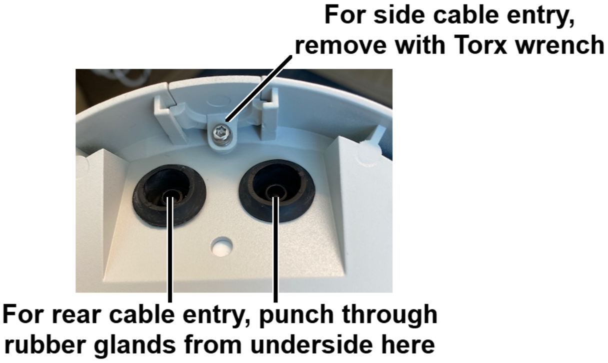
When tightening the screws, the holes in the mounting plate allow for making small adjustments to the bracket's position.

3.3.4 Route Cables and Connect the Camera

Cables can enter the camera either through the rear of the camera via the mounting bracket or through a conduit hole on the side of the camera. If the cables enter through the rear, make sure that the location provides a suitable method for routing the cables.

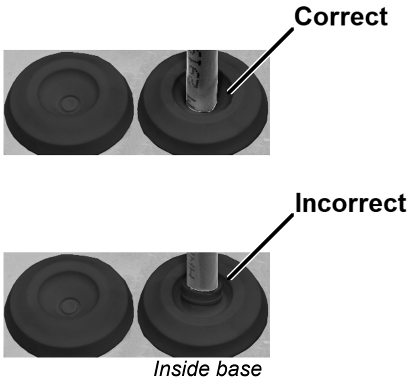
To route cables through the side of the camera:

1. Use the Torx wrench to loosen the screw securing the side conduit hole cover and remove the hole cover.
2. Route cables through the hole.


For side cable entry, remove with Torx wrench
For rear cable entry, punch through rubber glands from underside here

To route cables through the rear of the camera:

1. For each cable, use the Torx wrench to punch a hole in the center of the rubber glands in the camera's base, from the underside.
2. Route cables through the hole in the mounting bracket and through the holes in the grommet.
3. Push the cables back through the seal so that the seal extends out of the base.



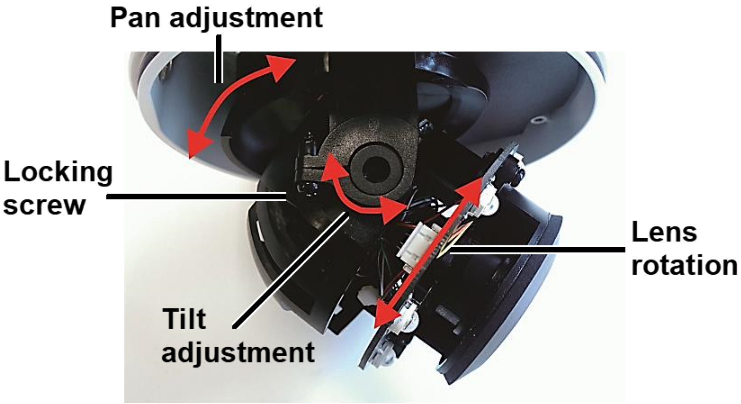
Connect the camera according to the information in Connect the Camera.

Note:

Connect the camera to a 24VAC or PoE power source as the main power supply, and then connect 12VDC as the secondary power supply. If the main power source fails, the camera switches power input seamlessly to 12VDC until the main power source is restored.

3.3.5 Mount and Aim the Camera

1. Make sure that the camera is facing the required field of view. Then, carefully re-attach the camera base to the mounting bracket. Use a screwdriver to tighten the two twist-lock screws securing the camera and its base to the mounting bracket.
2. Aim the camera, which has three axes to adjust the field of view:
   - *Pan adjustment* – Rotate the lens base until satisfied with the field of view. Do not rotate it beyond its mechanical limit, 356°.
   - *Tilt adjustment* – Loosen the screw locking the camera in its tilt angle. Tilt the camera lens until satisfied with the field of view. Do not tilt it beyond its mechanical limit, ±80°. Then, tighten the screw.
   - *Lens rotation* – Rotate the 3D assembly in the lens until satisfied with the field of view. Do not rotate the assembly beyond its mechanical limit, ±98°.



Aiming the Camera

⚠

Caution:

Note the mechanical limits for each axis:

- Pan adjustment range : 356°
- Tilt adjustment range : ±80°
- Lens rotation range: ±98° – Rotating the 3D assembly in the lens beyond its mechanical limit can twist, disconnect, or break the camera's internal cables.

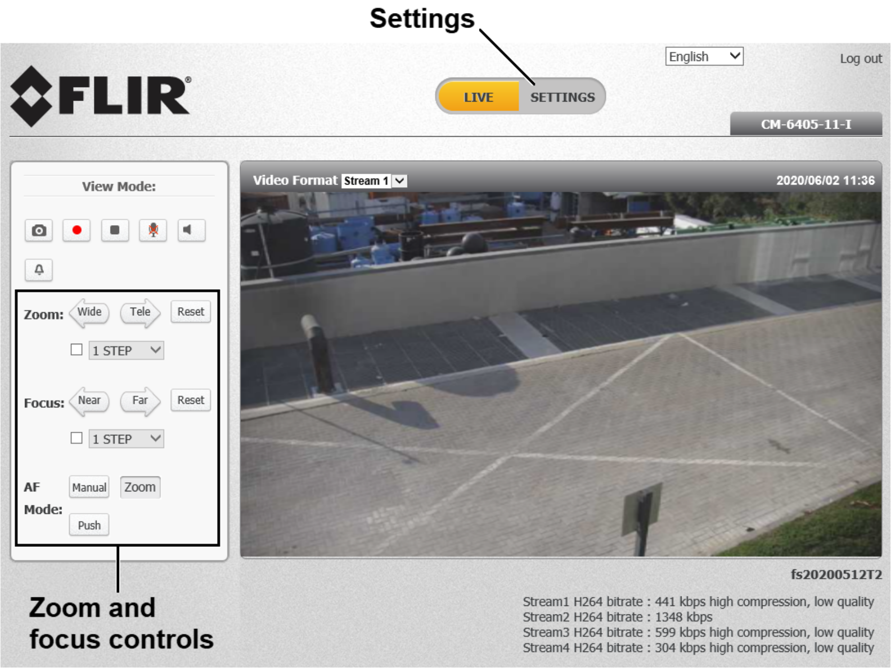
Repeat the steps described in Re-attach Dome Cover.

3.4 Additional Configuration Steps

Use the camera's web page to:

- Configure the camera's zoom and focus.
- Format the SD card.

1. Access the camera's web page. FLIR recommends using Microsoft Internet Explorer 11.0, with the ActiveX plug-in. The camera's web page supports other browsers that do not support ActiveX. However, using another browser requires configuring MJPEG encoding for at least one of the camera's video streams.

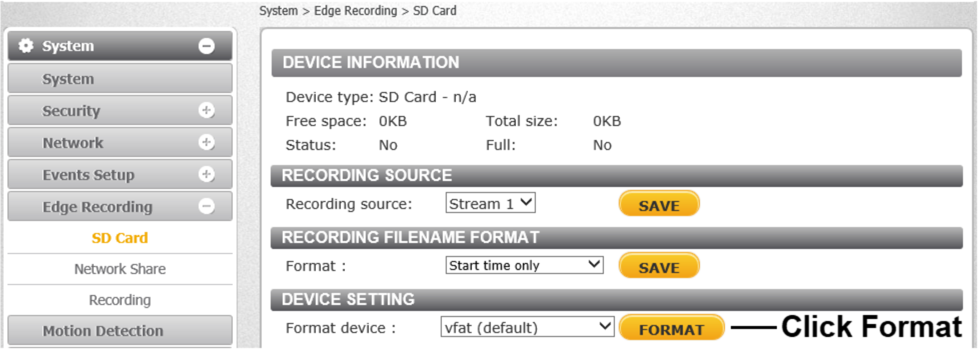


Video Format Stream 1
2020/06/02 11:36
fs20200512T2
Stream1 H264 bitrate : 441 kbps high compression, low quality
Stream2 H264 bitrate : 1348 kbps
Stream3 H264 bitrate : 599 kbps high compression, low quality
Stream4 H264 bitrate : 304 kbps high compression, low quality

Camera Web Page (CM-6405-11-I)

2. On the Live page, adjust the zoom or focus using the controls.
3. Format the SD card.

   From the navigation bar, click **Settings**.Then, in the sidebar, click **System > Edge Recording > SD Card.**



DEVICE INFORMATION

Device type: SD Card - n/a
Free space: 0KB Total size: 0KB
Status: No Full: No

RECORDING SOURCE

Recording source: Stream 1

RECORDING FILENAME FORMAT

Format : Start time only

DEVICE SETTING

Format device : vfat (default)

SD Card Screen

   Under Device Setting, you can select *vfat* (default) or *ext4* (recommended).

   Click **Format**.

Depending on how you are using the Quasar CM-640x camera and the network or VMS to which it is connected, initial configuration using the camera's web page can also consist of configuring the camera's:

- Security, advanced networking, event notification, and other system settings
- Video streams
- Exposure, white balance, WDR, and other picture settings

Many of these configuration steps can be performed before or after mounting the camera, but some of them can or should only be performed after Mounting and Connecting the Camera.

3.5 Attaching the Camera to a Supported VMS

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

4 Operation and Configuration

CM-640x cameras provide a browser-based configuration web page for video playback and recording. This section includes information about:

- Accessing the Camera's Web Page
- Camera Web Page Introduction
- Live Screen
- System Tab
- Streaming Tab
- Camera Tab
- Log Out

Caution:

If you are using a FLIR VMS, we recommend that you configure the camera's settings via the AdminCenter. The VMS can overwrite settings specified on the web page of the camera. For information about configuring the camera using the VMS, see the VMS online help or user guide.

Attention:

Si vous utilisez un FLIR VMS, nous vous recommandons de configurer les paramètres de la caméra via l'interface AdminCenter. VMS peut remplacer les paramètres définis sur l'interface Web de la caméra. Pour plus d'informations sur la configuration de la caméra à l'aide de VMS, consultez l'aide en ligne ou le guide utilisateur de VMS.

4.1 Accessing the Camera's Web Page

FLIR recommends using Microsoft Internet Explorer 11.0, with the ActiveX plug-in. The web page also supports browsers that do not support ActiveX such as Google Chrome, Mozilla Firefox, and Apple Safari. However, using another browser requires configuring MJPEG encoding for at least one of the camera's video streams.

To log in to the camera's web page:

1. Do one of the following:

   - In the FLIR Discovery Network Assistant (DNA) tool, double-click the camera in the Discover List.

     The DNA tool does not require a license to use and is a free download from the product's web page on FLIR.com. Download the DNA tool; unzip the file; and then double-click to run the tool (DNA.exe). The Discover List appears, showing compatible devices on the VLAN.

   - Type the camera's IP address in a browser's address bar (when the PC and the camera are on the same network). If you do not know the camera's IP address, you can use the DNA tool to discover it (see Initial Configuration).

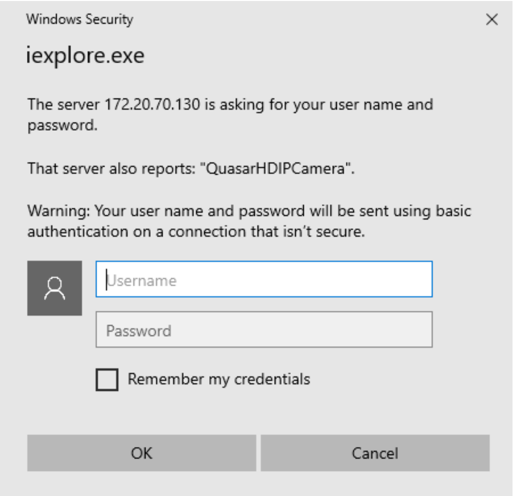
   A login screen or dialog box appears.

2. Type a user name and the password.

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

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

   Note:
   Both the user name and password are case-sensitive.



Windows Security

iexplore.exe

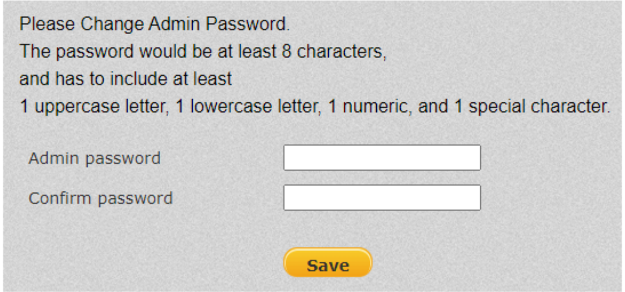
The server 172.20.70.130 is asking for your user name and password.

That server also reports: "QuasarHDIPCamera".

Warning: Your user name and password will be sent using basic authentication on a connection that isn't secure.

Internet Explorer Login Dialog Box

3. When logging in to the camera for the first time or for the first time after resetting the camera to its factory defaults, specify a new password for the admin user and then log back in using the new password.



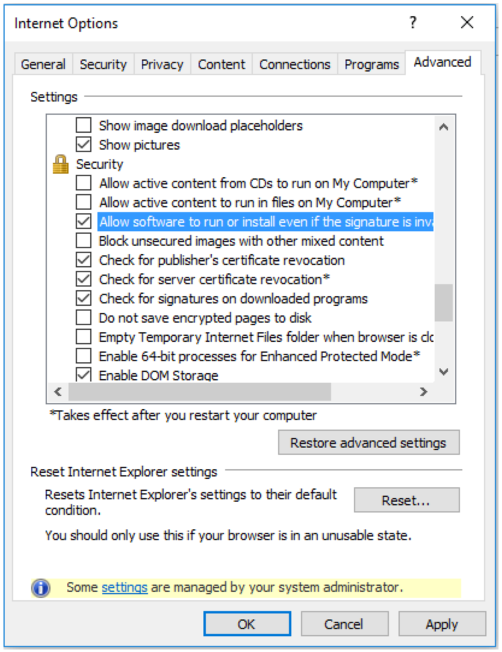
Please Change Admin Password.
The password would be at least 8 characters,
and has to include at least
1 uppercase letter, 1 lowercase letter, 1 numeric, and 1 special character.

Reset Admin Password

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

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

5. 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**.



Settings

- ☐ Show image download placeholders
- ☑ Show pictures
- Security
  - ☐ Allow active content from CDs to run on My Computer*
  - ☐ Allow active content to run in files on My Computer*
  - ☑ Allow software to run or install even if the signature is inv
  - ☐ Block unsecured images with other mixed content
  - ☑ Check for publisher's certificate revocation
  - ☑ Check for server certificate revocation*
  - ☑ Check for signatures on downloaded programs
  - ☐ Do not save encrypted pages to disk
  - ☐ Empty Temporary Internet Files folder when browser is clc
  - ☐ Enable 64-bit processes for Enhanced Protected Mode*
  - ☑ Enable DOM Storage

*Takes effect after you restart your computer

Reset Internet Explorer settings

Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.

Some settings are managed by your system administrator.

IE Tools > Internet Options > Advanced Window

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

Note:

If the password is changed and the UVMS AdminCenter Discovery feature is in use, deselect all other proprietary types. Select "*FLIR*" and "*Auto Select*" for UVMS 8 and newer systems as the Unit Type so that the new password can be configured in the Discovery tab settings.

7. Install the web player.

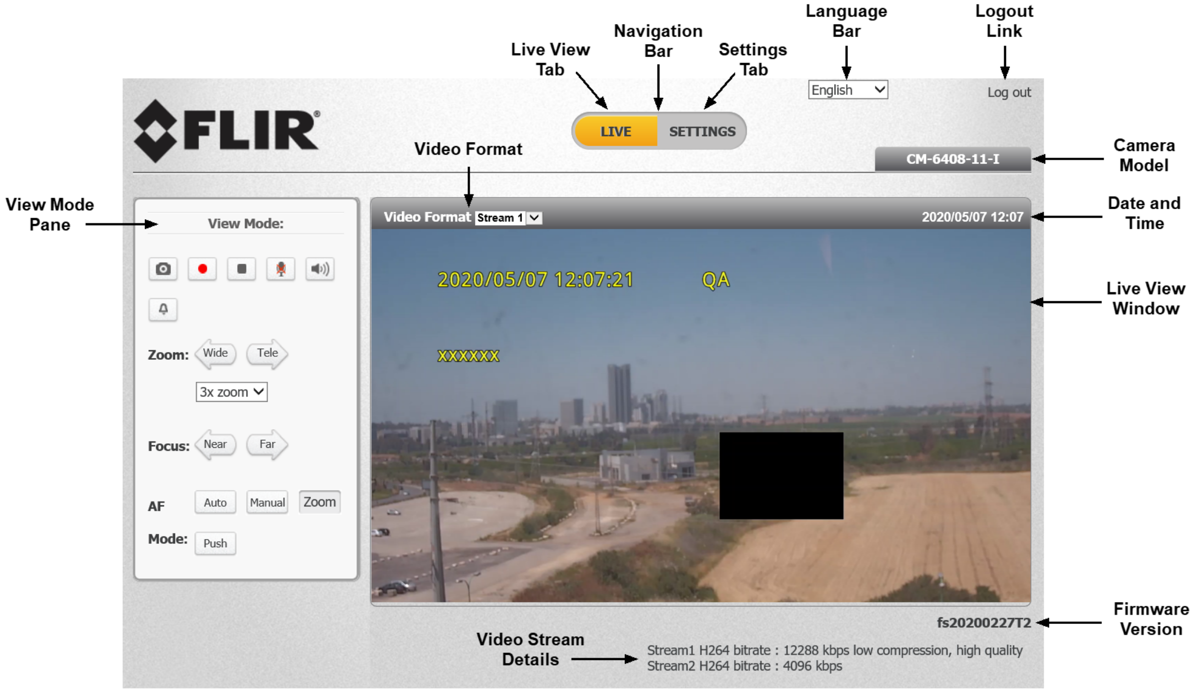
Note:

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.

The camera's web page opens.

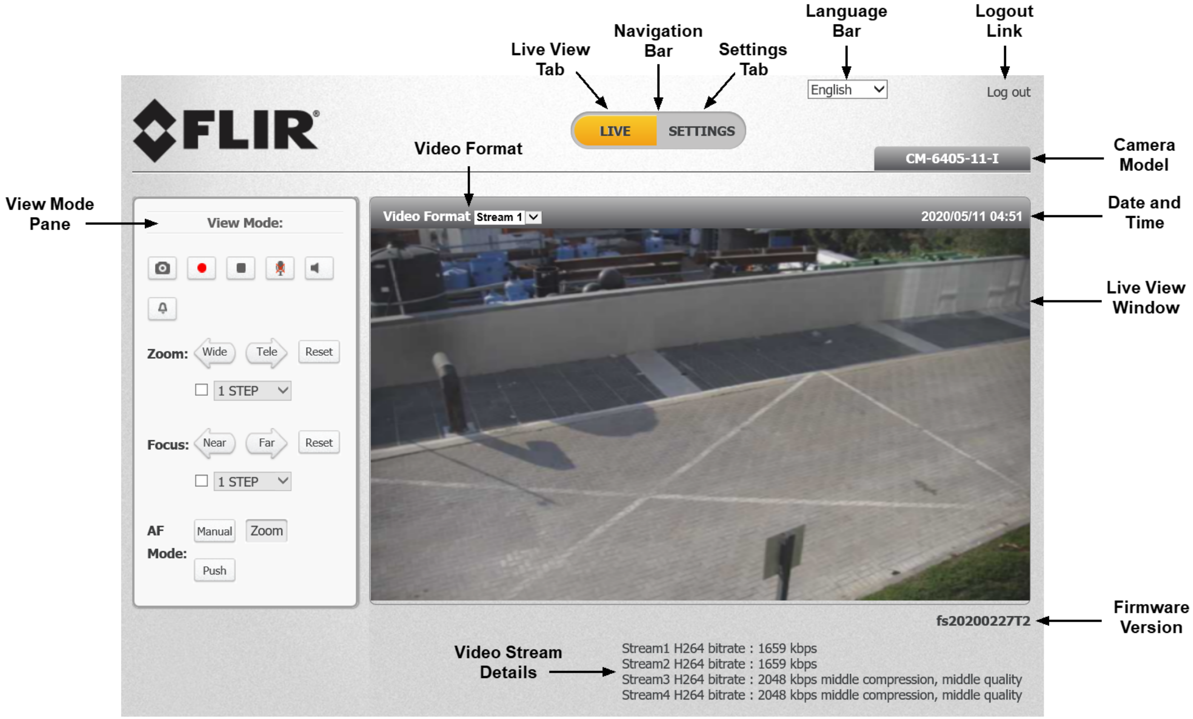
4.2 Camera Web Page Introduction

The figures below illustrate the camera's web page.



Stream1 H264 bitrate : 12288 kbps low compression, high quality
Stream2 H264 bitrate : 4096 kbps

Camera Web Page (CM-6408-11-I)



Stream1 H264 bitrate : 1659 kbps
Stream2 H264 bitrate : 1659 kbps
Stream3 H264 bitrate : 2048 kbps middle compression, middle quality
Stream4 H264 bitrate : 2048 kbps middle compression, middle quality

Camera Web Page (CM-6405-11-I)

The web page displays the following information:

1. 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 the Live Screen section.

    - **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**
          The administrator can configure settings for basic system parameters, security, network operation, events, recording, storage, system maintenance, and more.

        - **Streaming**
          The administrator can modify video and audio settings on this page.

        - **Camera**
          The administrator can adjust many of the camera settings on this page, such as Exposure, Picture Adjustment, Advanced Picture Settings, IR Function, and Miscellaneous settings.

2. The *Language Bar* is displayed to the right of the Navigation Bar. Supported languages include English, German, Spanish, French, Italian, Japanese, Korean, Portuguese, Russian, Simplified Chinese, and Traditional Chinese.

3. 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.

4. The camera *Model* is displayed under the *Log out* link.

5. The current *Date and Time* are displayed under the model number.

6. In the center of the page is the **Live View** window, which displays the image that the camera is monitoring.

7. The *Firmware Version* of the camera is displayed under the **Live View** window on the right side.

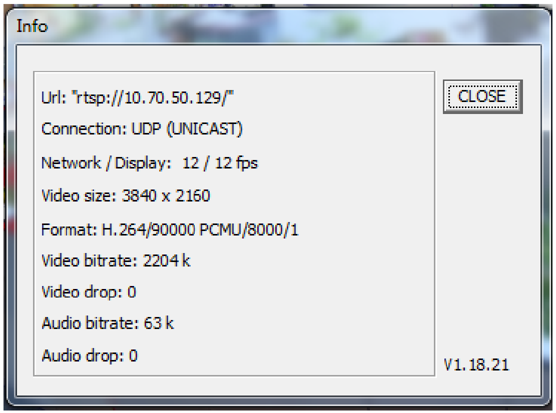
8. The *Video Stream Details* are displayed under the Firmware Version.

9. The *Video Format* is displayed and can be selected to the left of the *Date and Time*.

10. The *View Mode* pane to the left of the **Live View** window contains function buttons which facilitate camera control. This pane is discussed in the following section.

4.3 Live Screen

The camera's **Live** screen is used to monitor live video. See Camera Web Page Introduction. Double-clicking the Live window opens the **Info** dialog box, which displays key details about the video stream.



Url: "rtsp://10.70.50.129/"
Connection: UDP (UNICAST)
Network / Display: 12 / 12 fps
Video size: 3840 x 2160
Format: H.264/90000 PCMU/8000/1
Video bitrate: 2204 k
Video drop: 0
Audio bitrate: 63 k
Audio drop: 0

V1.18.21

Live Video Info Dialog Box

Two viewing modes are available: Fullscreen and Center Mode.

To view the Live View screen in Fullscreen mode:

1. Right-click the screen.
2. Click **Fullscreen**. The image is displayed in the entire monitor screen.

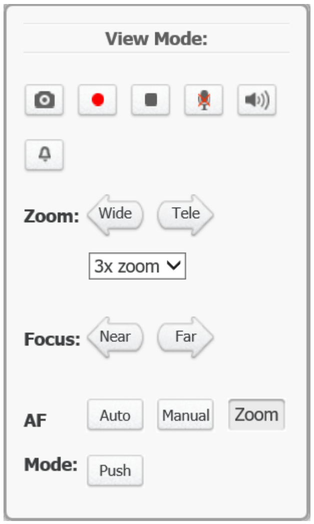
To exit Fullscreen mode:

Do one of the following:

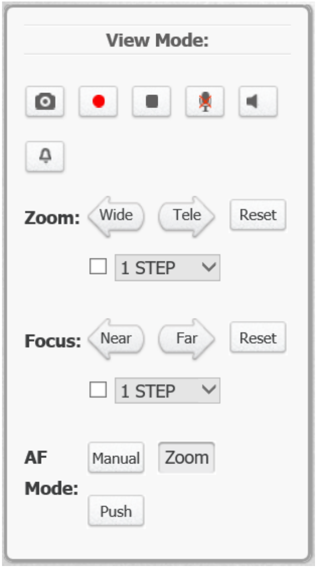
- Press the Escape key on your keyboard. The **Live View** screen is displayed in the monitor screen.
- Right-click the screen and then click **Normal view**. The **Live View** screen is displayed in the monitor screen.

View Mode Pane

The View Mode pane includes buttons that enable convenient camera control from the **Live** screen.



View Mode Pane (CM-6408-11-I)



View Mode Pane (CM-6405-11-I)

This document does not contain any export-controlled information.

The *View Mode* pane includes the following function buttons:

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.

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.

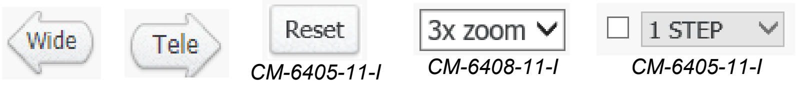
Video Streaming Restart/Stop

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

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.

Zoom



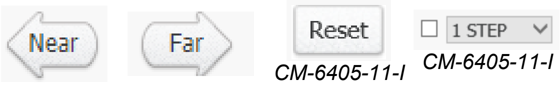
Press the **Wide** or **Tele** button to control zoom out/in.

On the CM-6408-11-I model, you can also manually select the zoom range (1x, 2x, or 3x). The default is 1x.

On the CM-6405-11-I model, you can reset the camera's zoom to full wide. You can also enable and define the number of zoom steps when you press the **Wide** and **Tele** buttons. The range is from 1 step to 128 steps, with 1 step being the default.

In Normal View display mode, you can also zoom out/in by moving the cursor to the Live Video pane and scrolling the mouse wheel. Digital zoom is only available when the function is activated and set up on the Camera > Misc screen.

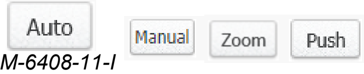
Focus



Press the **Near** or **Far** button to implement continuous focus adjustment.

On the CM-6405-11-I model, you can reset the camera to infinity focus. You can also enable and define the number of focus steps. The range is from 1 step to 128 steps, with 1 step being the default.

AF Mode



CM-6408-11-I

Auto (Continuous autofocus (AF); available only on the CM-6408-11-I model) – Click the **Auto** button to enable continuous AF. In this mode, the camera automatically and continuously maintains focus regardless of zoom or view changes.

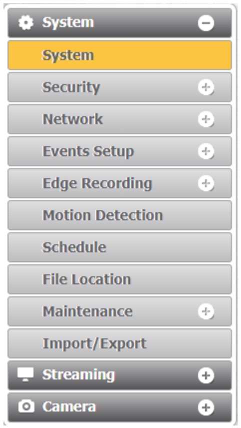
Manual Focus – Click the **Manual** button to adjust focus manually using the **Near** and **Far** buttons.

Zoom – Clicking the **Zoom** button causes the camera to focus when the zoom changes.

Push – Click the **Push** button to trigger the camera's focus.

4.4 System Tab

The **Settings** tab in the Navigation Bar opens the sections in the sidebar that are used for configuring the camera. It opens on the **System** section, which includes the following tabs:



System Section Tabs

Details of these settings are specified in the following sections:

System Security Network Events Setup Edge Recording

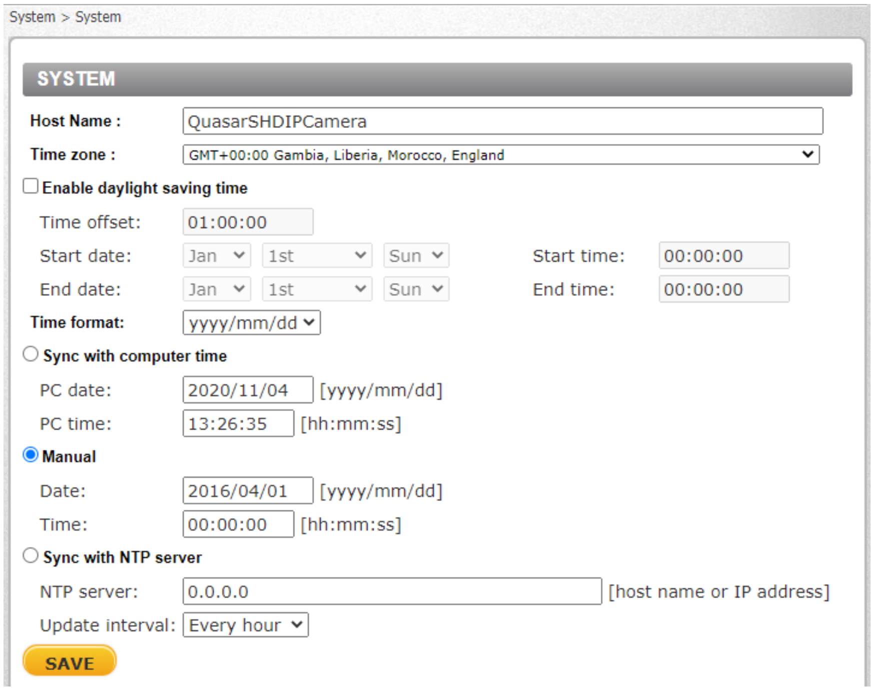
Motion Detection Schedule File Location Maintenance Import/Export

Note:

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

4.4.1 System

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.



System > System

SYSTEM

Host Name : QuasarSHDIPCamera

Time zone : GMT+00:00 Gambia, Liberia, Morocco, England

□ Enable daylight saving time

Time offset: 01:00:00

Start date: Jan 1st Sun Start time: 00:00:00

End date: Jan 1st Sun End time: 00:00:00

Time format: yyyy/mm/dd

○ Sync with computer time

PC date: 2020/11/04 [yyyy/mm/dd]

PC time: 13:26:35 [hh:mm:ss]

● Manual

Date: 2016/04/01 [yyyy/mm/dd]

Time: 00:00:00 [hh:mm:ss]

○ Sync with NTP server

NTP server: 0.0.0.0 [host name or IP address]

Update interval: Every hour

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.

Time Zone

Select the time zone from the drop-down menu.

Enable Daylight Saving Time

To enable daylight saving time, check the box and then specify time offset (number of hours or minutes difference between daylight saving time and standard time), start date and time for daylight saving time, and end date and time for daylight saving 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.

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. Enter the network time server host name or IP address to synchronize in the text box. Then select an update interval (every hour, day or week) from the drop-down menu. For further information about NTP, visit www.ntp.org.

Click **SAVE** when finished.

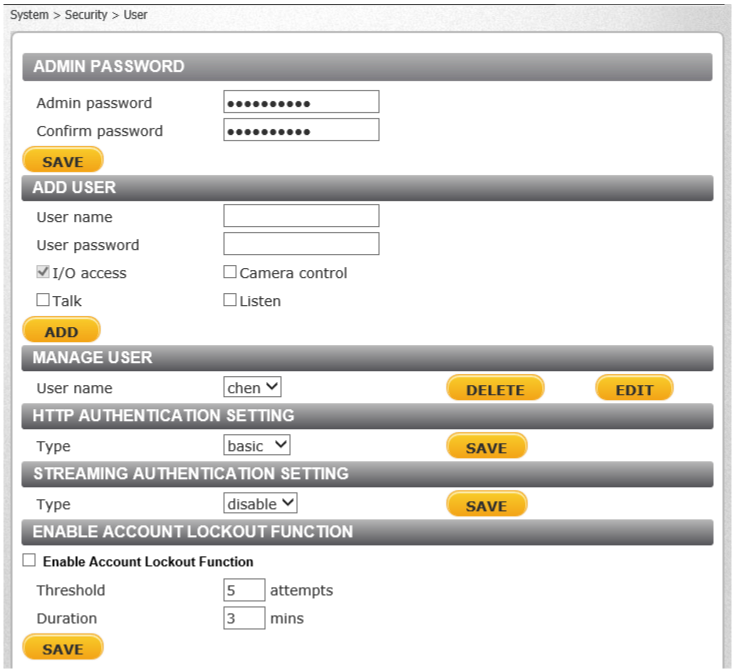
4.4.2 Security

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

User HTTPS IP Filter IEEE 802.1X

4.4.2.1 User

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



System > Security > User

ADMIN PASSWORD

Admin password ●●●●●●●●●●

Confirm password ●●●●●●●●●●

ADD USER

User name

User password

☑ I/O access ☐ Camera control

☐ Talk ☐ Listen

MANAGE USER

User name chen

HTTP AUTHENTICATION SETTING

Type basic

STREAMING AUTHENTICATION SETTING

Type disable

ENABLE ACCOUNT LOCKOUT FUNCTION

☐ Enable Account Lockout Function

Threshold 5 attempts

Duration 3 mins

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.

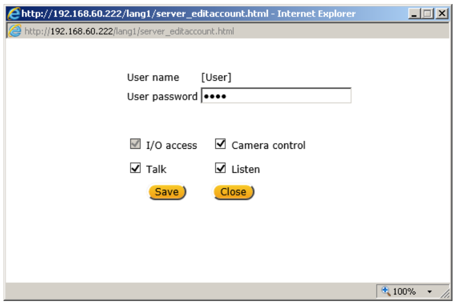
To add a new user

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.
3. Click **ADD**.

Manage User

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



http://192.168.60.222/lang1/server_editaccount.html - Internet Explorer

http://192.168.60.222/lang1/server_editaccount.html

User name [User]
User password ••••

☑ I/O access ☑ Camera control
☑ Talk ☑ Listen

Edit User Account Dialog Box

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

HTTP Authentication Setting

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

- *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**.

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**.

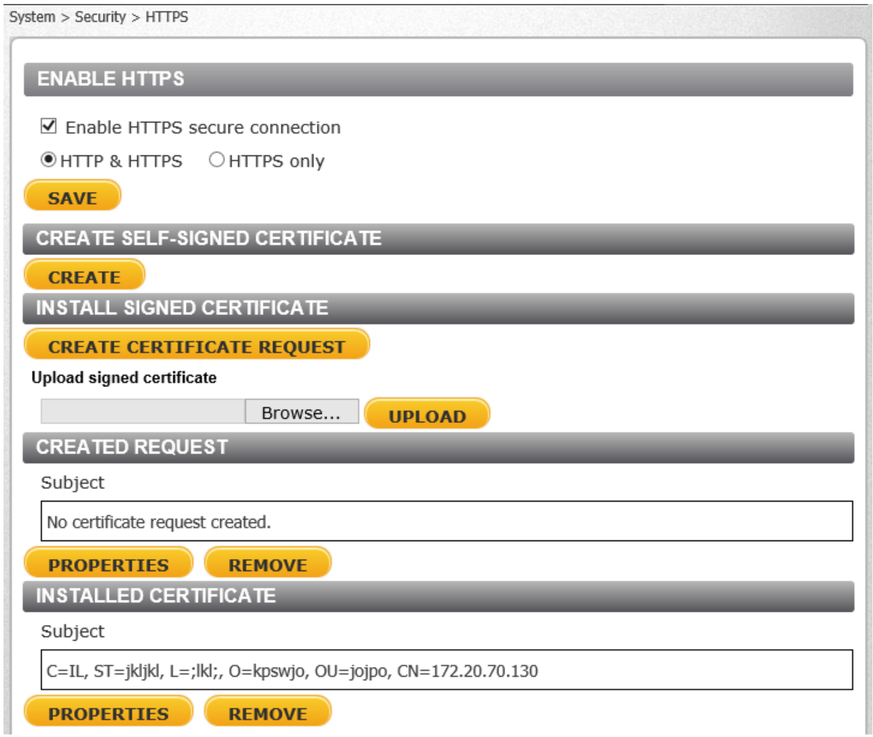
Enable Account Lockout Function Setting

To enable the account lockout function

1. Check the box to enable the account lockout function. Once enabled, accounts are locked out if a user unsuccessfully attempts to login the specified number of times within the specified duration.
2. Enter the account lockout *Threshold* and the *Duration*, in minutes.
3. Click **SAVE**.

4.4.2.2 HTTPS

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.


System > Security > HTTPS
ENABLE HTTPS
SAVE
CREATE SELF-SIGNED CERTIFICATE
CREATE
INSTALL SIGNED CERTIFICATE
CREATE CERTIFICATE REQUEST
Browse...
UPLOAD
CREATED REQUEST
PROPERTIES
REMOVE
INSTALLED CERTIFICATE
PROPERTIES
REMOVE

☑ Enable HTTPS secure connection

● HTTP & HTTPS ○ HTTPS only

Upload signed certificate

Subject: No certificate request created.

Subject: C=IL, ST=jkljkl, L=;lkl;, O=kpswjo, OU=jojpo, CN=172.20.70.130

HTTPS Screen

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

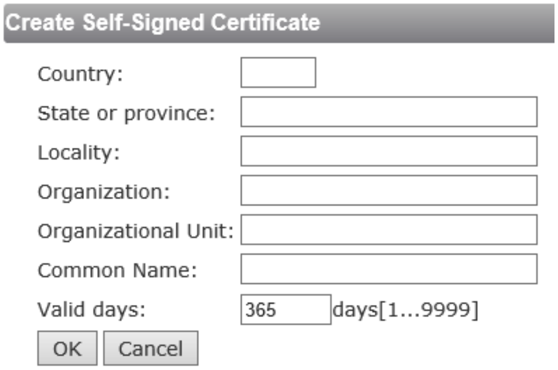
To enable HTTPS

1. Check the box to enable secure HTTPS communication.
2. Select one of the following:
   - *HTTP & HTTPS*: Allows both unsecured and secure communication between the camera and web browser.
   - *HTTPS*: Allows only secure communication between the camera and web browser.
3. Click **SAVE**.

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.

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



Create Self-Signed Certificate

Country:

State or province:

Locality:

Organization:

Organizational Unit:

Common Name:

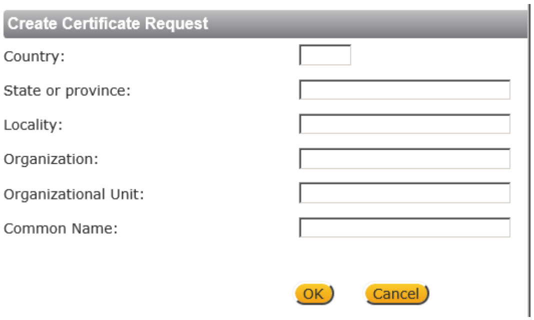
Valid days: 365 days[1...9999]

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.
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**.
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.

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



Create Certificate Request

Country:

State or province:

Locality:

Organization:

Organizational Unit:

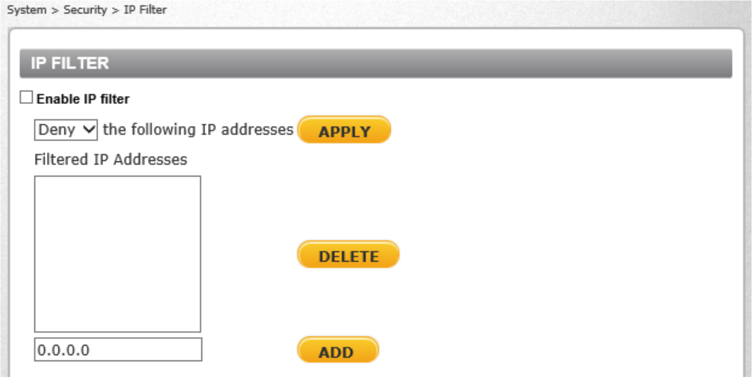
Common Name:

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

4.4.2.3 IP Filter

Use the **IP Filter** screen to restrict access to the camera by denying/allowing specific IP addresses.



IP Filter Screen

To enable the IP filter

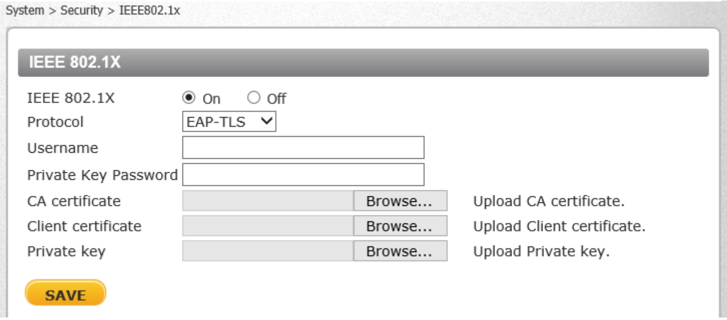
1. Check the box to enable the IP filter function. Once enabled, the listed IP addresses (IPv4) are allowed or denied access to the camera.
2. Select *Allow* or *Deny* from the drop-down list.The default setting is *Deny*.
3. Click **APPLY** to determine the IP filter behavior.

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**.

4.4.2.4 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.



System > Security > IEEE802.1x

IEEE 802.1X

IEEE 802.1X	● On ○ Off	
Protocol	EAP-TLS	
Username		
Private Key Password		
CA certificate	Browse...	Upload CA certificate.
Client certificate	Browse...	Upload Client certificate.
Private key	Browse...	Upload Private key.

IEEE 802.1X Screen - EAP-TLS Selected

Enable IEEE 802.1X – To enable IEEE 802.1X security, select the checkbox. The setting is disabled by default.

Protocol – Select one of the EAP protocols (*EAP-MD5*, *EAP-TLS*, *EAP-TTLS*, or *EAP-PEAP*).

EAP-MD5 Settings

When *EAP-MD5* is selected, specify the username and password to use for secure communication.

EAP-TLS Settings

When *EAP-TLS* is selected, the following settings are available:

- *Username* – 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 private key. Up to 16 characters can be used.
- *CA certificate* – To upload a certificate created by a Certificate Authority, click **Browse** to locate the file.
- *Client certificate* – To upload a client certificate, click **Browse** to locate the file.
- *Private key* – To upload the private key associated with the certificate, click **Browse** to locate the file.

EAP-TTLS Settings

When *EAP-TTLS* is selected, the following settings are available:

- *Inner Auth* – Select the inner authentication method (*CHAP*, *EAP-MSCHAPV2*, *EAP-MD5*, *MSCHAP*, *MSCHAPV2*, or *PAP*).
- *Username* – Enter the user identity (user name) associated with the certificate. Up to 16 characters can be used.
- *Password* – Enter the password associated with the user identity. Up to 16 characters can be used.
- *Anonymous ID* – Enter the anonymous ID associated with the user identity. Up to 16 characters can be used.

- *CA certificate* – To upload a certificate created by a Certificate Authority, click **Browse** to locate the file.

EAP-PEAP Settings

When *EAP-PEAP* is selected, the following settings are available:

- *Username* – Enter the user identity (user name) associated with the certificate. Up to 16 characters can be used.
- *Password* – Enter the password associated with the user identity. Up to 16 characters can be used.
- *CA certificate* – To upload a certificate created by a Certificate Authority, click **Browse** to locate the file.

To save any changes to the IEEE 802.1X settings and to upload any files, click **SAVE**.

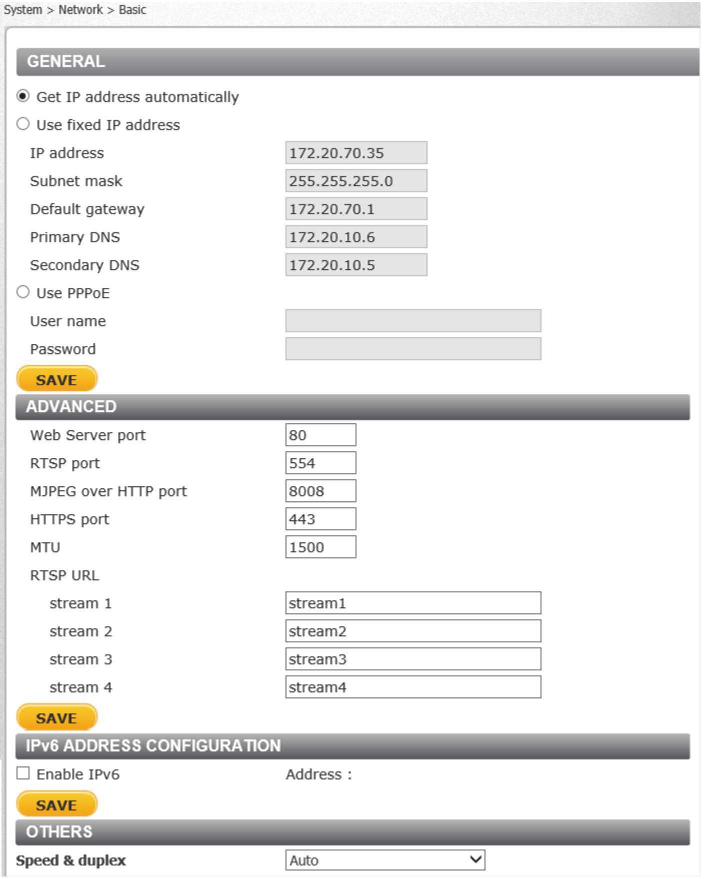
4.4.3 Network

From the **System** screen, click the **Network** tab. The following screens are available:

Basic QoS SNMP UPnP DDNS Mail FTP HTTP

4.4.3.1 Basic

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



System > Network > Basic

GENERAL

● Get IP address automatically

○ Use fixed IP address

IP address	172.20.70.35
Subnet mask	255.255.255.0
Default gateway	172.20.70.1
Primary DNS	172.20.10.6
Secondary DNS	172.20.10.5

○ Use PPPoE

User name	
Password	

SAVE

ADVANCED

Web Server port	80
RTSP port	554
MJPEG over HTTP port	8008
HTTPS port	443
MTU	1500
RTSP URL	
stream 1	stream1
stream 2	stream2
stream 3	stream3
stream 4	stream4

SAVE

IPv6 ADDRESS CONFIGURATION

□ Enable IPv6 Address :

SAVE

OTHERS

Speed & duplex Auto

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 four sections: *General, Advanced, IPv6 Configuration*, and *Others*.

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 can be accessed from the FLIR website - see Accessing Product Information from the FLIR Website, to obtain the IP address from a DHCP server on the network. See Initial Configuration.

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 Initial Configuration to log in 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.

Use PPPoE

If you wish to use PPPoE to configure network settings, select the *Use PPPoE* radial button.

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 1200 to 1500 bytes.
- *RTSP URL*– Enter a friendly name for each stream in the text box.

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

Click **SAVE** when finished.

IPv6 Address Configuration

To enable IPv6

1. Check *Enable IPv6.*
2. In the *Address* text box, enter the unit's IPv6 IP Address.

Click **SAVE** when finished.

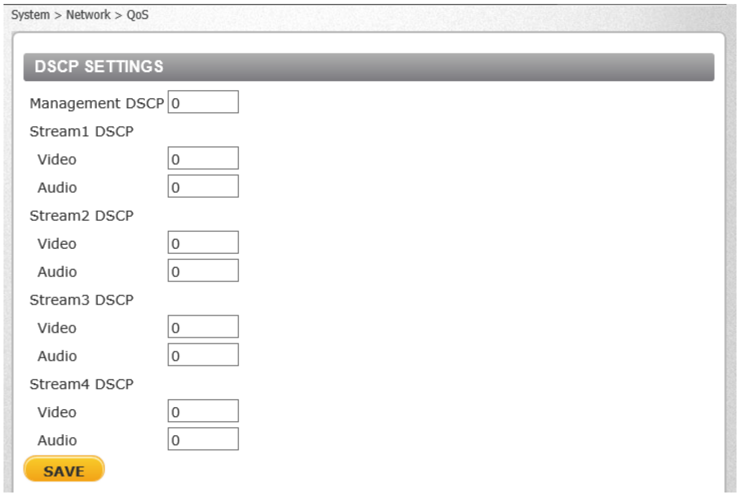
Others

Speed & duplex – Select the Ethernet speed the network supports:

- *Auto* – automatic 10/100/1000 Mbps detection
- *100 Mbps*

4.4.3.2 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.



System > Network > QoS

DSCP SETTINGS

Management DSCP 0

Stream1 DSCP
Video 0
Audio 0

Stream2 DSCP
Video 0
Audio 0

Stream3 DSCP
Video 0
Audio 0

Stream4 DSCP
Video 0
Audio 0

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:

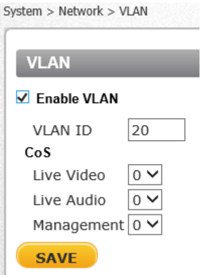
- *Management DSCP* – Specified for all of the camera's streams, this class consists of HTTP traffic (web browsing).
- *Video DSCP* – Specified for each stream, this class consists of applications such as MJPEG over HTTP, RTP/RTSP, and RTSP/HTTP.
- *Audio DSCP* – Specified for each stream, this class consists of audio applications.

Click **SAVE** when finished.

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

4.4.3.3 VLAN

The **System > Network > VLAN** screen enables communication to and from the camera when it is on a VLAN.



System > Network > VLAN

VLAN

☑ Enable VLAN

VLAN ID 20

CoS
Live Video 0
Live Audio 0
Management 0

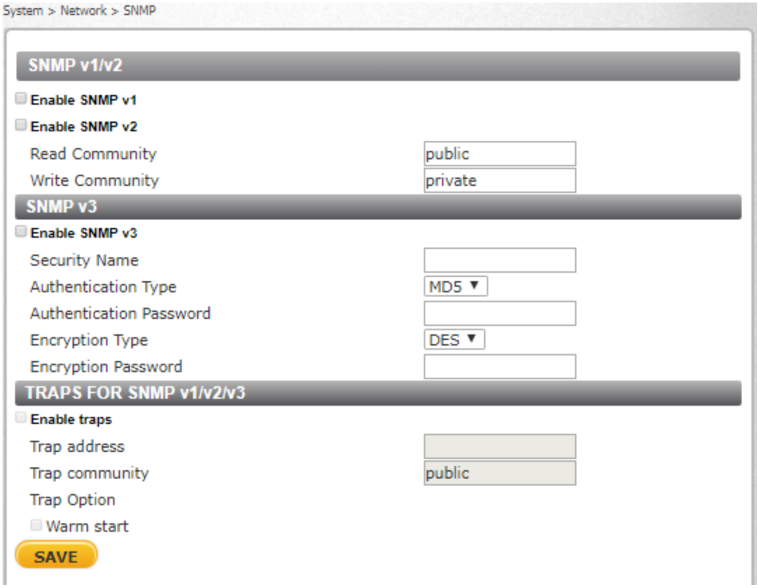
VLAN Screen
VLAN Enabled

Enable VLAN – If VLAN is enabled, specify the ID of the VLAN the camera is on and the class of service (*CoS*) for live video, live audio, and management, from *0-7*.

Click **SAVE** when finished.

4.4.3.4 SNMP

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.



System > Network > SNMP

SNMP v1/v2

□ Enable SNMP v1

□ Enable SNMP v2

Read Community: public

Write Community: private

SNMP v3

□ Enable SNMP v3

Security Name:

Authentication Type: MD5 ▼

Authentication Password:

Encryption Type: DES ▼

Encryption Password:

TRAPS FOR SNMP v1/v2/v3

□ Enable traps

Trap address:

Trap community: public

Trap Option

□ Warm start

SAVE

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. The default setting is *MD5*. See note below.
- *Authentication Password* – See note below.

- *Encryption Type* – Select *DES* or *AES* from the drop-down list. The default setting is *DES.* 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

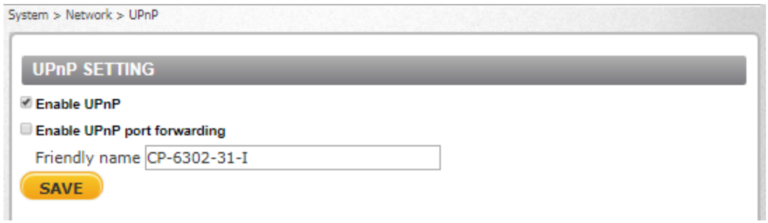
Traps are used by the camera to send messages to a management system for important events or status changes.

- *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 finished.

4.4.3.5 UPnP

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



System > Network > UPnP

UPnP SETTING

☑ Enable UPnP

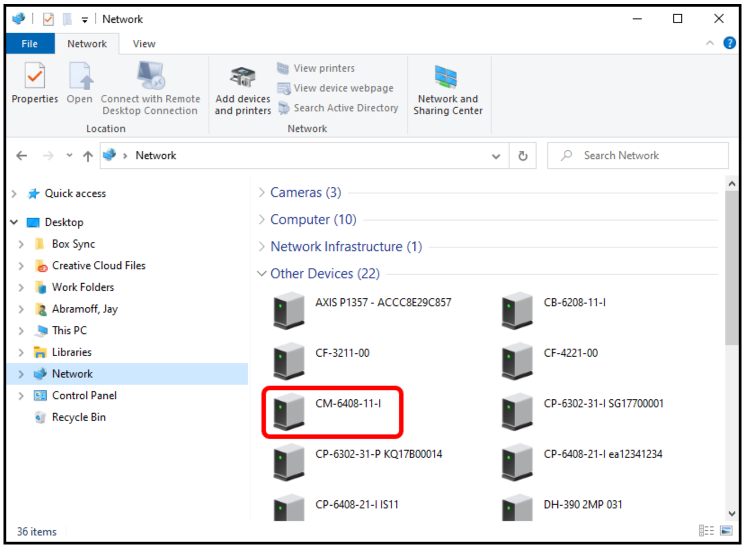
□ Enable UPnP port forwarding

Friendly name CP-6302-31-I

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.



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:

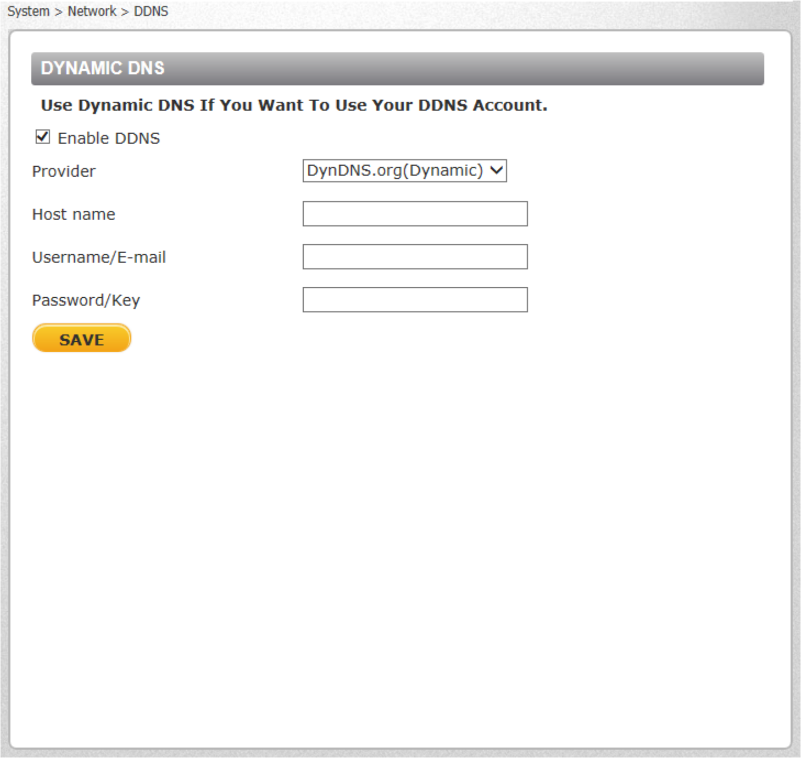
To enable this function, make sure that your router supports UPnP and that it is activated.

- *Friendly name* – Enter the name for the camera for identification.

Click **SAVE** when finished.

4.4.3.6 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.



System > Network > DDNS

DYNAMIC DNS

Use Dynamic DNS If You Want To Use Your DDNS Account.

☑ Enable DDNS

Provider: DynDNS.org(Dynamic)

Host name:

Username/E-mail:

Password/Key:

DDNS Screen

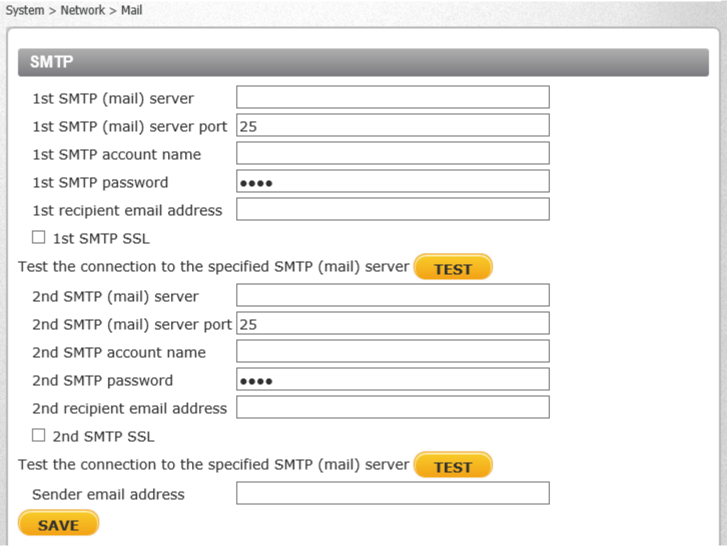
To use DDNS

1. Select the *Enable DDNS* checkbox.
2. From the *Provider* drop-down list, select a DDNS host provider name.The default setting is *DynDNS.org (Dynamic)*.
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** when finished.

4.4.3.7 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, Network Failure Detection, and Motion Detection screens.

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



1st SMTP (mail) server	
1st SMTP (mail) server port	25
1st SMTP account name	
1st SMTP password	●●●●
1st recipient email address	
□ 1st SMTP SSL	
Test the connection to the specified SMTP (mail) server	TEST
2nd SMTP (mail) server	
2nd SMTP (mail) server port	25
2nd SMTP account name	
2nd SMTP password	●●●●
2nd recipient email address	
□ 2nd SMTP SSL	
Test the connection to the specified SMTP (mail) server	TEST
Sender email address	

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 *1st SMTP SSL* or 2nd *SMTP SSL*. For SMTP server details, contact your network service provider. To test the connection with either SMTP server using the values specified, click the appropriate **TEST** button.

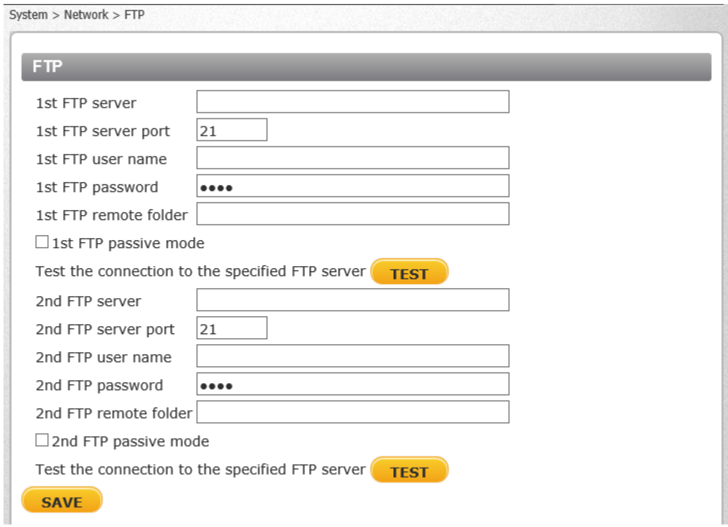
For *Sender e-mail address*, enter the address that appears as the sender on e-mail the camera triggers.

Click **SAVE** when finished.

4.4.3.8 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, Network Failure Detection, and Motion 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.



1st FTP server	
1st FTP server port	21
1st FTP user name	
1st FTP password	●●●●
1st FTP remote folder	
□ 1st FTP passive mode	
Test the connection to the specified FTP server	TEST
2nd FTP server	
2nd FTP server port	21
2nd FTP user name	
2nd FTP password	●●●●
2nd FTP remote folder	
□ 2nd FTP passive mode	
Test the connection to the specified FTP server	TEST

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)

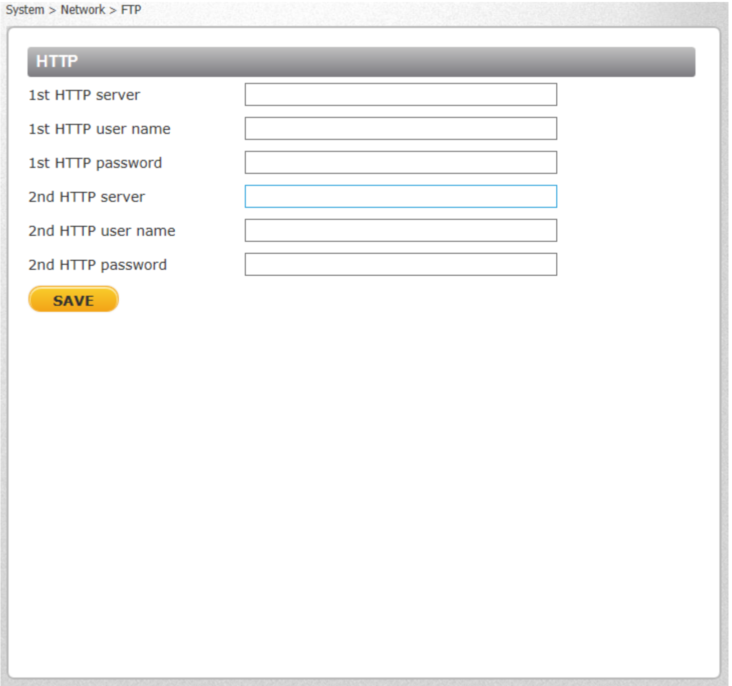
To test the connection with either FTP server using the values specified, click the appropriate **TEST** button.

Click **SAVE** when finished.

4.4.3.9 HTTP

An HTTP notification server detects notification messages of triggered events sent from cameras. HTTP notifications are set by selecting the *Send HTTP notification* checkbox on the Motion Detection screen.

Two notification server accounts (Alarm Triggered and Motion Detection) can be set up and sent to the specified HTTP servers. For each server, enter the HTTP details, including server IP address, user name, and password. Settings are entered in the **System > Network > HTTP** screen:



1st HTTP server	
1st HTTP user name	
1st HTTP password	
2nd HTTP server	
2nd HTTP user name	
2nd HTTP password	

HTTP Screen

Click **SAVE** when finished.

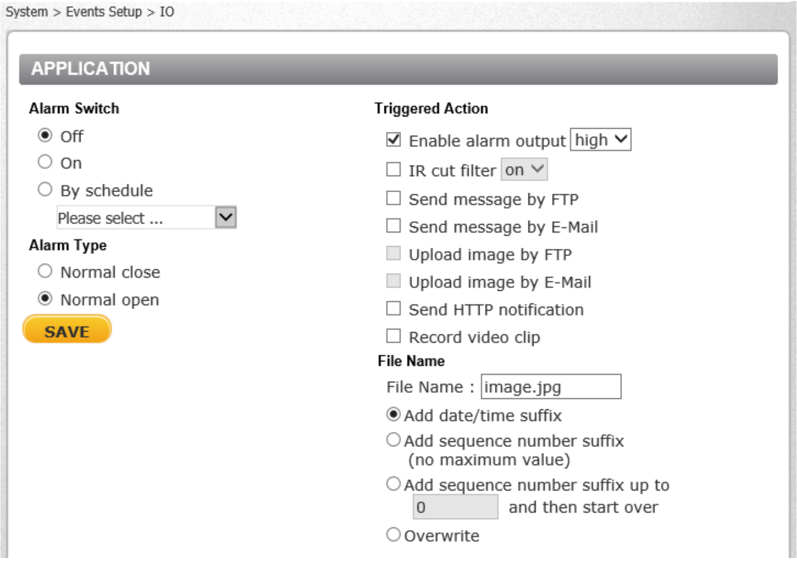
4.4.4 Events Setup

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

IO Network Failure Detection Periodic Event Manual Trigger Audio Detection Tampering

4.4.4.1 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.



System > Events Setup > IO

APPLICATION

Alarm Switch

● Off
○ On
○ By schedule
Please select ...

Alarm Type

○ Normal close
● Normal open

SAVE

Triggered Action

☑ Enable alarm output: high
□ IR cut filter: on
□ Send message by FTP
□ Send message by E-Mail
□ Upload image by FTP
□ Upload image by E-Mail
□ Send HTTP notification
□ Record video clip

File Name

File Name : image.jpg
● Add date/time suffix
○ Add sequence number suffix (no maximum value)
○ Add sequence number suffix up to 0 and then start over
○ Overwrite

IO Screen

Alarm Switch

The Administrator can select from the following options:

- Select *Off* to disable the 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.

Alarm Type

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

Triggered Action

The Administrator can specify various alarm actions to take when an alarm is triggered. See the Triggered Actions section for detailed descriptions of the actions. The following options are available:

- *Enable alarm output* – To enable the alarm relay output, check this box and select the preferred type of alarm output *(low* or *high*). The default setting is *low*.
- *IR cut filter* – The Administrator can select whether to enable (*on*) or disable (*off*) the IR cut filter when an alarm is triggered.

- *Send Message by FTP* – The Administrator can select whether to send an alarm message by FTP when an alarm is triggered.
- *Send message by E-Mail* – The Administrator can select whether to send an alarm message by e-mail when an alarm is triggered.
- *Upload Image by FTP* – Selecting this option enables you to assign an FTP site and configure various parameters.
- *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.
- *Send HTTP notification* – Select this checkbox to send a notification by HTTP.
- *Record video clip* – Select this box in order to save the alarm-triggered recording to your microSD card or to the NAS.

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 up to <specify a sequence number> and then start over
  File Name: imageXX.jpg
  X: Sequence Number

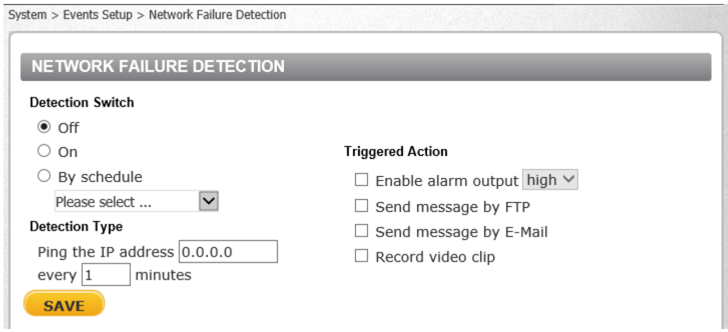
  The file name suffix ends at the number being set. For example, if the setting is up to "10," the file name will start from 00, end at 10, and then start over again.

- 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.

4.4.4.2 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. By implementing local recording through a microSD card, the camera can operate as a backup recording device for the surveillance system if network communication is lost due to a network failure.



System > Events Setup > Network Failure Detection

NETWORK FAILURE DETECTION

Detection Switch

● Off
○ On
○ By schedule
Please select ...

Detection Type

Ping the IP address 0.0.0.0
every 1 minutes

SAVE

Triggered Action

□ Enable alarm output high
□ Send message by FTP
□ Send message by E-Mail
□ Record video clip

Network Failure Detection Screen

Detection Switch

The Administrator can select from the following options:

- Select *Off* to disable the 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.

Detection Type

In the text box, enter the IP address to ping and the time interval (in minutes) between pings.

Triggered Action

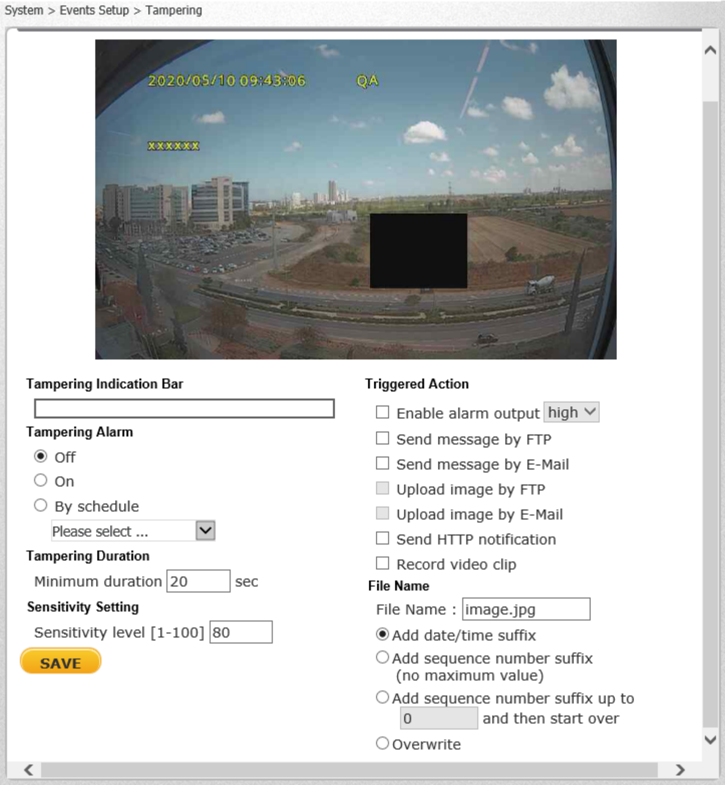
The Administrator can specify various alarm actions to take when an alarm is triggered. See the Triggered Actions section for detailed descriptions of the actions. The following options are available:

- *Enable alarm output* – To enable the alarm relay output, check this box and select the preferred type of alarm output *(low* or *high*). The default setting is *high*.
- *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.
- *Record video clip* – Select this box in order to save the alarm-triggered recording into the local microSD card.

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

4.4.4.3 Tampering

The **Tampering** screen is used to configure settings for tamper detection alarms. Tampering alarm is defined by a minimum duration of a tampering action and a sensitivity level. When triggered, the tampering event can perform several actions in response.



System > Events Setup > Tampering

Tampering Indication Bar

Tampering Alarm

● Off
○ On
○ By schedule

Please select ...

Tampering Duration

Minimum duration 20 sec

Sensitivity Setting

Sensitivity level [1-100] 80

SAVE

Triggered Action

□ Enable alarm output high
□ Send message by FTP
□ Send message by E-Mail
□ Upload image by FTP
□ Upload image by E-Mail
□ Send HTTP notification
□ Record video clip

File Name

File Name : image.jpg

● Add date/time suffix
○ Add sequence number suffix (no maximum value)
○ Add sequence number suffix up to 0 and then start over
○ Overwrite

Tampering Screen

Tampering Indication Bar

The Tampering Indication bar gives the user a visual display of the threshold for how much Tampering is accruing. This indication bar will be affected by the Sensitivity Setting.

Tampering Alarm

The Administrator can select from the following options:

- Select *Off* to disable the 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.

Tampering Duration

The minimum duration set for tampering indicates the amount of time tampering must take place before the camera considers it a tampering event.

Sensitivity Setting

Setting the sensitivity [1-100] determines the amount of tampering that will trigger an event (i.e. how much movement of the camera).

Triggered Action

The Administrator can specify various alarm actions to take when an alarm is triggered. See the Triggered Actions section for detailed descriptions of the actions. The following options are available:

- *Enable alarm output* – To enable the alarm relay output, check this box and select the preferred type of alarm output *(low* or *high*). The default setting is *high*.
- *Send Message by FTP* – The Administrator can select whether to send an alarm message by FTP when an alarm is triggered.
- *Send message by E-Mail* – The Administrator can select whether to send an alarm message by e-mail when an alarm is triggered.
- *Upload Image by FTP* – Selecting this option enables you to assign an FTP site and configure various parameters.
- *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.
- *Send HTTP notification* – Select this checkbox to send a notification by HTTP.
- *Record video clip* – Select this box in order to save the alarm-triggered recording to the local microSD card or to the NAS.

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 up to <specify a sequence number> and then start over
  File Name: imageXX.jpg
  X: Sequence Number

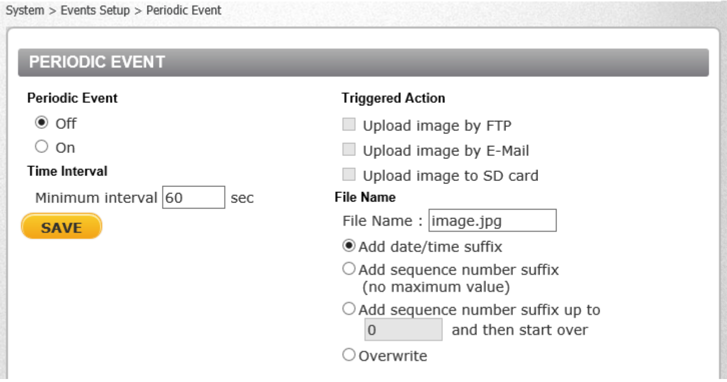
  The file name suffix ends at the number being set. For example, if the setting is up to "10," the file name will start from 00, end at 10, and then start over again.

- 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.

4.4.4.4 Periodic Event

The **Periodic Event** screen is used to specify an alarm to be triggered at a specified time interval.



System > Events Setup > Periodic Event

PERIODIC EVENT

Periodic Event

● Off
○ On

Time Interval

Minimum interval 60 sec

Triggered Action

□ Upload image by FTP
□ Upload image by E-Mail
□ Upload image to SD card

File Name

File Name : image.jpg

● Add date/time suffix
○ Add sequence number suffix (no maximum value)
○ Add sequence number suffix up to 0 and then start over
○ Overwrite

Periodic Event Screen

Periodic Event

Select *Off* or *On* to activate this function. The default is *Off*.

Time Interval

In the *Minimum interval* text box, enter the number of seconds for the minimum interval between alarms. The range is from 20 to 3600 seconds. The default is *60*.

Triggered Action

The Administrator can specify various alarm actions to take when an alarm is triggered. See the Triggered Actions section for detailed descriptions of the actions. The following options are available:

- *Upload Image by FTP* – Selecting this option enables you to assign an FTP site and configure various parameters.
- *Upload Image by E-Mail* – Selecting this option enables you to assign an e-mail address and configure various parameters.
- *Upload Image to SD card* – When this option is selected and an alarm is triggered, the camera uploads a snapshot to the SD card.

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 up to <specify a sequence number> and then start over
  File Name: imageXX.jpg
  X: Sequence Number

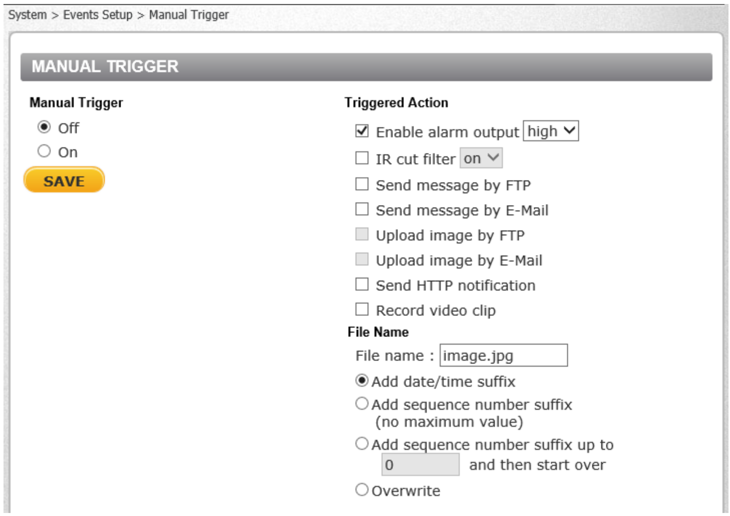
  The file name suffix ends at the number being set. For example, if the setting is up to "10," the file name will start from 00, end at 10, and then start over again.

- 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.

4.4.4.5 Manual Trigger

The **Manual Trigger** screen is used to specify an alarm to be manually triggered. You can define action to take when an alarm occurs from the System > Events Setup > IO screen.



System > Events Setup > Manual Trigger

MANUAL TRIGGER

Manual Trigger

● Off
○ On

SAVE

Triggered Action

☑ Enable alarm output high
□ IR cut filter on
□ Send message by FTP
□ Send message by E-Mail
□ Upload image by FTP
□ Upload image by E-Mail
□ Send HTTP notification
□ Record video clip

File Name

File name : image.jpg

● Add date/time suffix
○ Add sequence number suffix (no maximum value)
○ Add sequence number suffix up to 0 and then start over
○ Overwrite

Manual Trigger Screen

Manual Trigger

Select *Off* or *On* to activate this function. The default is *Off*.

Triggered Action

The Administrator can specify various alarm actions to take when an alarm is triggered. See the Triggered Actions section for detailed descriptions of the actions. The following options are available:

- *Enable alarm output* – To enable the alarm relay output, check this box and select the preferred type of alarm output *(low* or *high*). The default setting is *high*.
- *IR cut filter* – The Administrator can select whether to enable (*on*) or disable (*off*) the IR cut filter when an alarm is triggered.
- *Send Message by FTP* – The Administrator can select whether to send an alarm message by FTP when an alarm is triggered.
- *Send message by E-Mail* – The Administrator can select whether to send an alarm message by e-mail when an alarm is triggered.
- *Upload Image by FTP* – Selecting this option enables you to assign an FTP site and configure various parameters.
- *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.
- *Send HTTP notification* – Select this checkbox to send a notification by HTTP.
- *Record video clip* – Select this box in order to save the alarm-triggered recording to the local microSD card or to the NAS.

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.

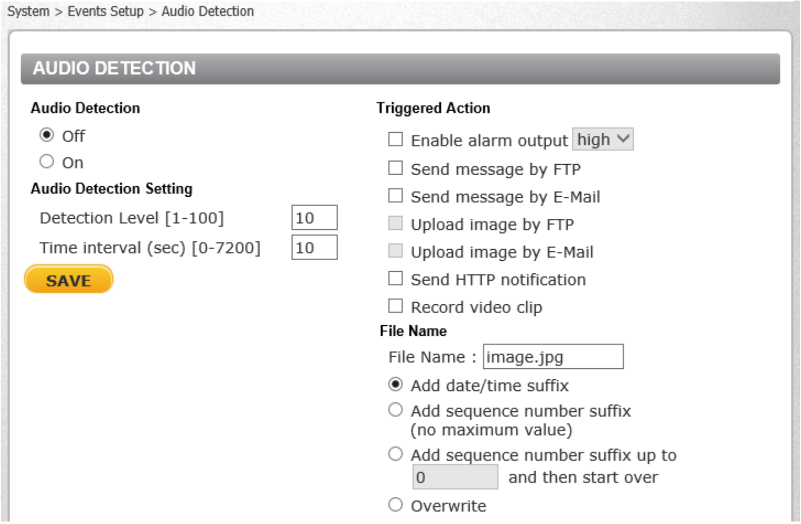
- Add date/time suffix (default setting)
  File name: imageYYMMDD_HHNNSS_XX.jpg
  Y: Year, M: Month, D: Day
  H: Hour, N: Minute, S: Second
  X: Sequence Number
- Add sequence number suffix (no maximum value)
  File name: imageXXXXXXX.jpg
  X: Sequence Number
- Add sequence number suffix up to <specify a sequence number> and then start over
  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.

4.4.4.6 Audio Detection

The **Audio Detection** screen is used to configure settings for audio detection alarms, including the audio input threshold level. When that threshold is exceeded, an audio event is created. When triggered, the audio detection event can perform several actions in response.



System > Events Setup > Audio Detection

AUDIO DETECTION

Audio Detection
● Off
○ On

Audio Detection Setting
Detection Level [1-100]: 10
Time interval (sec) [0-7200]: 10

Triggered Action
□ Enable alarm output: high
□ Send message by FTP
□ Send message by E-Mail
□ Upload image by FTP
□ Upload image by E-Mail
□ Send HTTP notification
□ Record video clip

File Name
File Name : image.jpg
● Add date/time suffix
○ Add sequence number suffix (no maximum value)
○ Add sequence number suffix up to 0 and then start over
○ Overwrite

Audio Detection Screen

Audio Detection

The Administrator can select from the following options:

- Select *Off* to disable audio detection (default setting).
- Select *On* to enable audio detection.

Audio Detection Setting

The Administrator can define the following settings:

- *Detection Level [1-100]* – Setting a low threshold (for example, 25) means that the camera is more sensitive to noise, which results in more alerts (displayed in red). The setting depends on the situation and environment. If the scene is located in a quiet place, it is possible to use lower threshold. A noisy location requires a higher threshold.

- *Time interval (sec) [0-7200]* – Select a number from 0-7200 (seconds). The default interval is 10. The value is the minimum amount of time between each audio detected event.

Triggered Action

The Administrator can specify various alarm actions to take when an alarm is triggered. See the Triggered Actions section for detailed descriptions of the actions.

The following options are available:

- *Enable alarm output* – To enable the alarm relay output, check this box and select the preferred type of alarm output *(low* or *high*). The default setting is *high*.
- *Send Message by FTP* – The Administrator can select whether to send an alarm message by FTP when an alarm is triggered.
- *Send message by E-Mail* – The Administrator can select whether to send an alarm message by e-mail when an alarm is triggered.
- *Upload Image by FTP* – Selecting this option enables you to assign an FTP site and configure various parameters.
- *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.
- *Send HTTP notification* – Select this checkbox to send a notification by HTTP.
- *Record video clip* – Select this box in order to save the alarm-triggered recording to the local microSD card or to the NAS.

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 up to <specify a sequence number> and then start over
  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.

4.4.4.7 Triggered Actions

Triggered Action

The Administrator can specify various alarm actions to take when an alarm is triggered. The following options are available, although not all options are available for all events:

- *Enable alarm output* – To enable the alarm relay output, check this box and select the preferred type of alarm output *(low* or *high*). The default setting is *high*.
- *IR cut filter* – The Administrator can select whether to enable (*on*) or disable (*off*) the IR cut filter when an alarm is triggered.
- *Send Message by FTP* – The Administrator can select whether to send an alarm message by FTP when an alarm is triggered.
- *Send message by E-Mail* – The Administrator can select whether to send an alarm message by e-mail when an alarm is triggered.

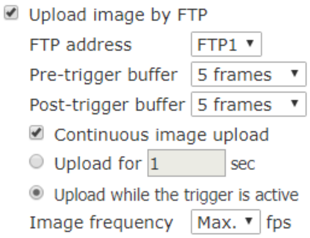
Note:
Images can be sent by email only when *MJPEG* is selected as the video stream from the Video Configuration screen.

Select one of two e-mail addresses from the drop-down menu. Select the number of frames for the pre-trigger and post-trigger buffers from the drop-down menu of 1-20 frames.

Check the box for *Continuous image upload* if you wish to use this option. To specify the length of time for the upload, click this radial button and enter the number of seconds. To upload while the trigger is active, click this radial button. Finally, select the number of frames per second from the drop-down menu next to *Image frequency.*

Note:
Make sure SMTP or FTP configuration has been completed. See the Mail and FTP sections for further details.

- *Upload Image by FTP* – Selecting this option enables you to assign an FTP site and configure various parameters. When an alarm is triggered, event images will be uploaded to the designated FTP site.



☑ Upload image by FTP

FTP address FTP1 ▾

Pre-trigger buffer 5 frames ▾

Post-trigger buffer 5 frames ▾

☑ Continuous image upload

○ Upload for 1 sec

● Upload while the trigger is active

Image frequency Max. ▾ fps

Upload Image by FTP Settings

Note:

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

Specify the FTP address to use from the drop-down menu. Select the number of frames for the pre-trigger and post-trigger buffers from the drop-down menu of 1-20 frames.

Check the box for *Continuous image upload if* you wish to use this option. To specify the length of time for the upload, click this radial button and enter the number of seconds. To upload while the trigger is active, click this radial button.

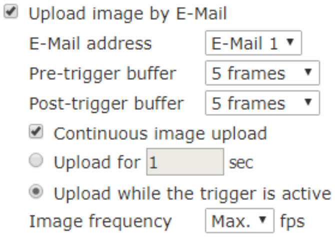
Finally, select the number of frames per second from the drop-down menu next to *Image frequency*.

- *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 Configuration 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.



☑ Upload image by E-Mail

E-Mail address: E-Mail 1

Pre-trigger buffer: 5 frames

Post-trigger buffer: 5 frames

☑ Continuous image upload

○ Upload for 1 sec

● Upload while the trigger is active

Image frequency: Max. fps

Upload Image by E-Mail Settings

  - 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*.

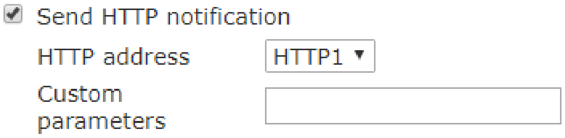
  In the *Image Frequency* text box, from the drop-down list select the number of frames per seconds from 1-15 for the upload.

Note:
Make sure that SMTP configuration has been completed. See Mail for details.

- *Upload Image to SD card* – When this option is selected and an alarm is triggered, the camera uploads a snapshot to the SD card.

Note:
In order to use this function, make sure that local recording with a microSD card is activated and properly configured. See SD Card and Recording for further details.

- *Send HTTP notification* – Select this checkbox to send a notification by HTTP. Select the destination HTTP address from the drop-down menu and specify the parameters for event notifications by the IO event triggered. When an alarm is triggered, the notification will be sent to one of two HTTP servers specified on the HTTP screen. See figure below.



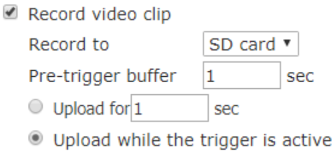
☑ Send HTTP notification

HTTP address: HTTP1 ▾

Custom parameters:

Send HTTP Notification Settings

- *Record video clip* – Select this box in order to save the alarm-triggered recording to the local microSD card or to the NAS. Enter the number of seconds for the pre-trigger buffer. Select the first radial button if you wish to upload for a specified length of time and enter the number of seconds. Alternatively, select the second radial button to upload while the trigger is active.



☑ Record video clip

Record to: SD card ▾

Pre-trigger buffer: 1 sec

○ Upload for 1 sec

● Upload while the trigger is active

Record Video Clip Settings

Note:
In order to use this function, make sure that local recording with a microSD card is activated and that the NAS is properly configured. See Recording for further details.

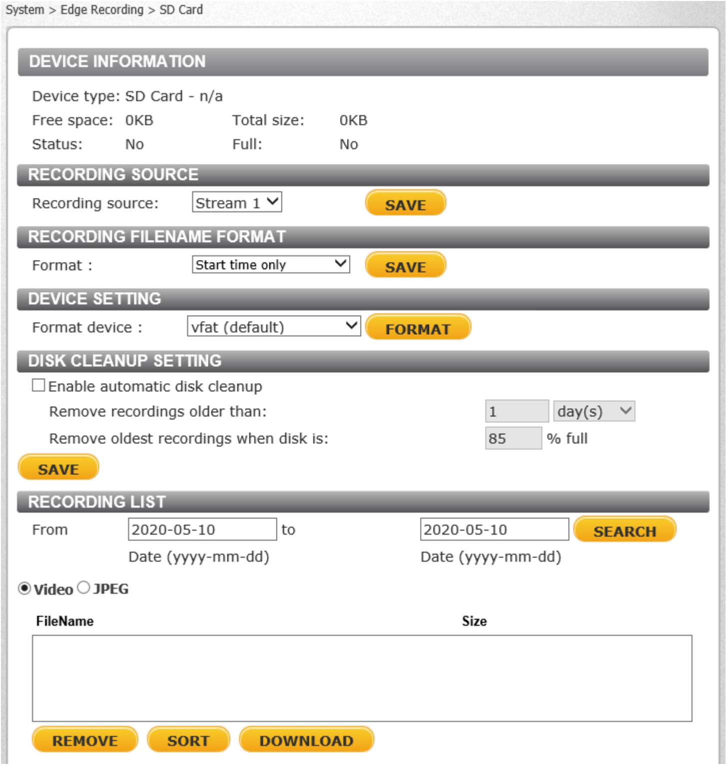
4.4.5 Edge Recording

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

SD Card Network Share Recording

4.4.5.1 SD Card

You can locally record up to 512GB on a Class 10 microSD/microSDHC/microSDXC card (minimum 8GB). The **SD Card** page shows the capacity information of the memory card and a recording list of all the recording files saved on the card. You can also format the card and implement automatic recording cleanup on this page. To implement microSD card recording, see Recording.



System > Edge Recording > SD Card

DEVICE INFORMATION

Device type: SD Card - n/a

Free space: 0KB Total size: 0KB

Status: No Full: No

RECORDING SOURCE

Recording source: Stream 1

RECORDING FILENAME FORMAT

Format : Start time only

DEVICE SETTING

Format device : vfat (default)

DISK CLEANUP SETTING

□ Enable automatic disk cleanup

Remove recordings older than: 1 day(s)

Remove oldest recordings when disk is: 85 % full

RECORDING LIST

From 2020-05-10 to 2020-05-10

Date (yyyy-mm-dd) Date (yyyy-mm-dd)

● Video ○ JPEG

FileName	Size

SD Card Screen
No SD Card Inserted

Note:
Format the microSD card when using it for the first time. Formatting is also required when a memory card has been used on one camera and is then transferred to a camera that uses a different software platform.

Device Information

Upon inserting the microSD card, card information, such as the memory capacity and status, is displayed.

Recording Source

Select *Stream 1* or *Stream 2*, and then click **SAVE**.

Recording Filename Format

Select *Start time only* or *Start time + end time*, and then click **SAVE**.

Device Setting

Select *vfat* (default) or *ext4* (recommended). Click **FORMAT** to format the memory card.

Disk Cleanup Setting

Enable automatic recording cleanup by selecting *Enable automatic disk cleanup*. From the pull-down menu, specify the minimum length of time over which to remove recordings. For example, remove recordings over 10 days old. Enter the percent of disk capacity used in order to remove the oldest recordings. Click **SAVE** when finished.

Recording List

Each video file on the microSD card is listed in the Recording List. The maximum file size is 60 MB per file. See Recording for further details.

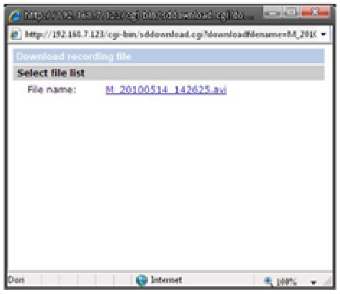
When the recording mode in the **Recording** screen is set as *Always* (consecutive recording) and the microSD card recording is enabled by events triggered, the system immediately saves a recorded event on the memory card once an event occurs. The camera then returns to the regular recording mode after events recording.

Note:

The capital letters: R, N, A, (A0), M, (M0) followed by an underscore, appear at the beginning of the file name. They denote the type of recording.

- R - Regular (always or schedule)
- N - Network failure
- M - Motion (M0 refers to the first motion window trigger)
- A - Alarm (A0 refers to the first alarm trigger input).

- *Remove* – To remove a file, first select the file and then click **REMOVE**.
- *Sort* – Click **SORT** to list the files in the Recording List table in order of name and date.
- *Download* – To open or download a video clip, first select the file and then click **DOWNLOAD**. The selected file window appears. Click the file to play the video in the player or download it to a specified location.



http://192.168.7.123/cgi-bin/sddownload.cgi?downloadfilename=M_201(

Download recording file

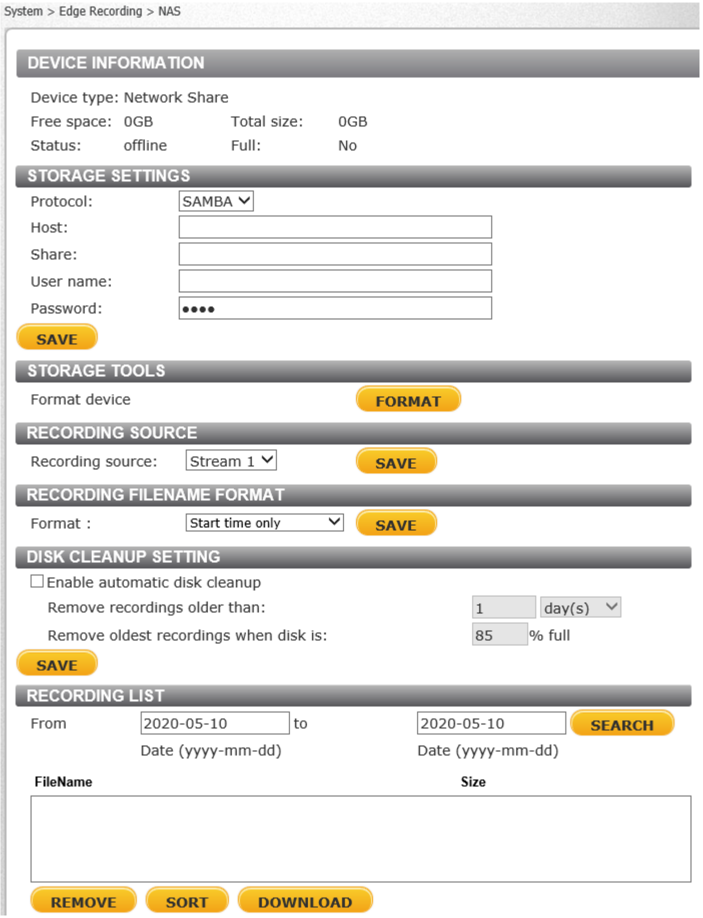
Select file list

File name: M_20100514_142625.avi

Selected File Window

4.4.5.2 Network Share

The **Network Share** screen shows the capacity information of the Network Attached Storage (NAS) disk and provides a list of all the recording files saved on the disk.



System > Edge Recording > NAS

DEVICE INFORMATION

Device type: Network Share

Free space: 0GB Total size: 0GB

Status: offline Full: No

STORAGE SETTINGS

Protocol: SAMBA

Host:

Share:

User name:

Password: ••••

STORAGE TOOLS

Format device

RECORDING SOURCE

Recording source: Stream 1

RECORDING FILENAME FORMAT

Format : Start time only

DISK CLEANUP SETTING

☐ Enable automatic disk cleanup

Remove recordings older than: 1 day(s)

Remove oldest recordings when disk is: 85 % full

RECORDING LIST

From 2020-05-10 to 2020-05-10

Date (yyyy-mm-dd) Date (yyyy-mm-dd)

FileName	Size

Network Share Screen

You can also format the disk and implement automatic recording cleanup on this page. To implement NAS recording, see Recording.

Device Information

Upon connecting to the NAS, the following information about the disk is displayed:

- Device type – Displays Network Share.
- Free space – Displays the amount of available storage space in GB.
- Total size – Displays the total amount of storage space in GB.
- Status – Indicates if the camera is online or offline.
- Full – Indicates if the disk is full (Yes/No).

Storage Settings

- Protocol – Select the protocol used by the NAS. The default is SAMBA.
- Host – Enter the host IP address.
- Share – Enter the path for a shared network storage device.
- User name – Enter the name of the user accessing the NAS.
- Password – Enter the password of the user accessing the NAS.

Storage Tools

Click **FORMAT** to format the NAS.

Recording Source

Select *Stream 1* or *Stream 2*, and then click **SAVE**.

Recording Filename Format

Select *Start time only* or *Start time + end time*, and then click **SAVE**.

Disk Cleanup Setting

Enable automatic recording cleanup by selecting *Enable automatic disk cleanup*. From the pull-down menu, specify the minimum length of time over which to remove recordings. For example, remove recordings over 10 days old. Enter the percent of disk capacity used in order to remove the oldest recordings. Click **SAVE** when finished.

Recording List

Each video file stored on the NAS is listed in the Recording list. See Recording for further details. When the recording mode in the **Recording** screen is set as *Always* (consecutive recording) and the NAS recording is enabled by events triggered, the system immediately saves a recorded event on the network disk once an event occurs. Then the camera will return to the regular recording mode after events recording.

Note:

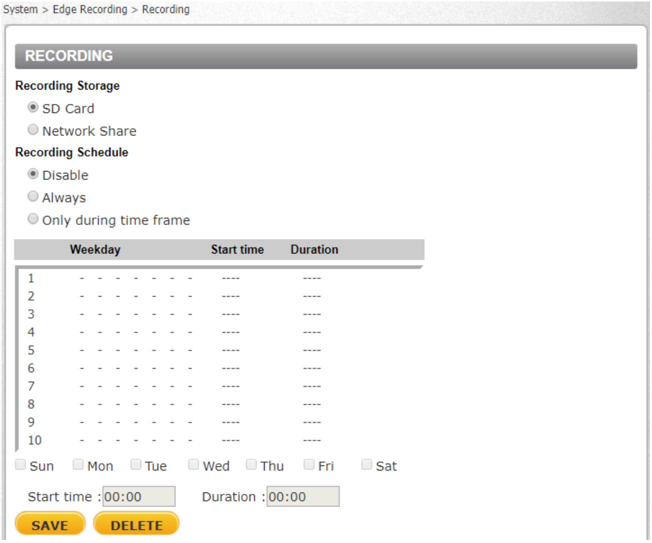
The capital letters: R, N, A, (A0), M, (M0) followed by an underscore, appear at the beginning of the file name. They denote the type of recording.

- R - Regular (always or schedule)
- N - Network failure
- M - Motion, (M0 refers to the first motion window trigger)
- A - Alarm (A0 refers to the first alarm trigger input).

- *Remove* – To remove a file, first select the file and then click **REMOVE**.
- *Sort* – Click **SORT** to list the files in the Recording list in order of name and date.
- *Download* – To open/download a video clip, first select the file and then click **DOWNLOAD**. The selected file window pops up as shown below. Click the AVI file to play the video in the player or download it to a specified location. See SD Card.

4.4.5.3 Recording

The **Recording** screen is used to select a device and to set a schedule for recording clips. Up to 10 schedules can be set.



System > Edge Recording > Recording

RECORDING

Recording Storage

● SD Card

○ Network Share

Recording Schedule

● Disable

○ Always

○ Only during time frame

	Weekday	Start time	Duration
1	- - - - - - -	----	----
2	- - - - - - -	----	----
3	- - - - - - -	----	----
4	- - - - - - -	----	----
5	- - - - - - -	----	----
6	- - - - - - -	----	----
7	- - - - - - -	----	----
8	- - - - - - -	----	----
9	- - - - - - -	----	----
10	- - - - - - -	----	----

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Start time : 00:00 Duration : 00:00

SAVE DELETE

Recording Screen

In the *Recording Storage* section, select the recording device: *SD Card* or *Network Share*.

Note:
It is not recommend to record with the microSD card for 24/7 continuously, as it may not be able to support long term continuous data read/write. Contact the manufacturer of the microSD card for information regarding its reliability and life expectancy.

In the *Recording Schedule* section, specify the recording schedule. Select one of three options:

- *Disable* – Disable this function
- *Always* – Always use this function
- *Only during time frame* – Records only during a specified time frame

To set the recording schedule

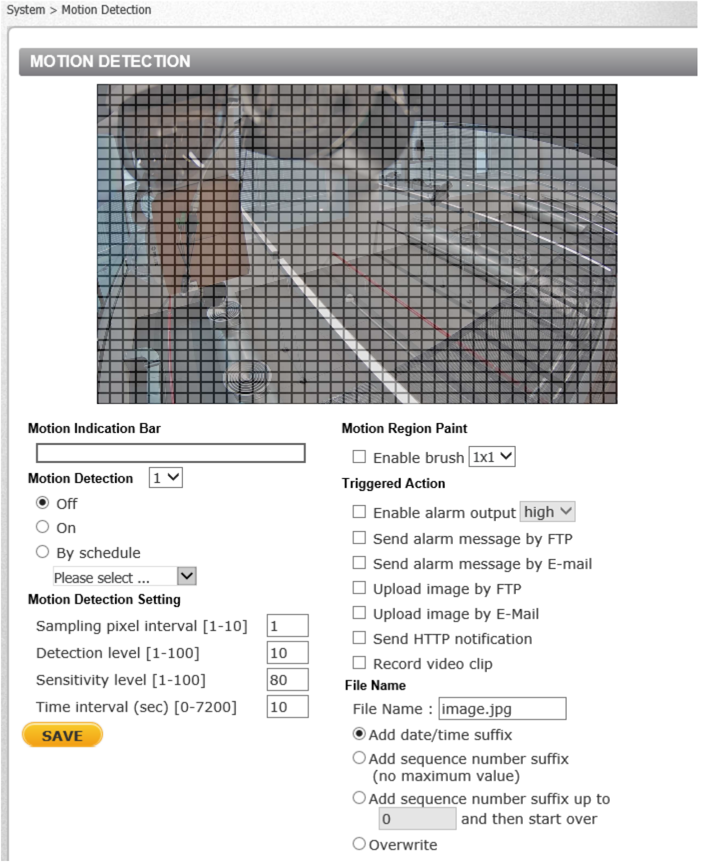
1. Select the day.
2. Set the start time.
3. Set the duration for recording.
4. Click **SAVE** to confirm the schedule. The schedule is displayed in the table.

Note:

This option works only if (a) the microSD card is installed in the camera or (b) the NAS is configured properly.

4.4.6 Motion Detection

The motion detection function detects suspicious motion and triggers alarms when motion volume in the detected region reaches or exceeds the determined sensitivity threshold value. The Live View pane on the **Motion Detection** screen is used for creating motion detection regions and indicating motion detection. It is possible to define up to four motion detection regions within the Live View pane**.** The motion detection function is disabled by default.



System > Motion Detection

MOTION DETECTION

Motion Indication Bar

Motion Detection 1

● Off
○ On
○ By schedule

Please select ...

Motion Detection Setting

Sampling pixel interval [1-10] 1
Detection level [1-100] 10
Sensitivity level [1-100] 80
Time interval (sec) [0-7200] 10

SAVE

Motion Region Paint

□ Enable brush 1x1

Triggered Action

□ Enable alarm output high
□ Send alarm message by FTP
□ Send alarm message by E-mail
□ Upload image by FTP
□ Upload image by E-Mail
□ Send HTTP notification
□ Record video clip

File Name

File Name : image.jpg

● Add date/time suffix
○ Add sequence number suffix (no maximum value)
○ Add sequence number suffix up to 0 and then start over
○ Overwrite

Motion Detection Screen

Detected motion is displayed in the Motion Indication Bar. After motion detection has been activated, the bar is divided into 10 segments; each one representing a sensitivity level. Once the motion exceeds the set sensitivity level, the bar turns from green to red.

Note:

If you are using UVMS, it is recommended to set the motion detection from AdminCenter.

To activate Motion Detection

1. From the *Motion Detection* drop-down list, select a number from 1 to 4.
2. Do one of the following for each detection region:
   - Select *On* for continuous detection*.*
   - Select *By schedule* for scheduled detection. For instructions how to set a schedule for motion detection, refer to Schedule.

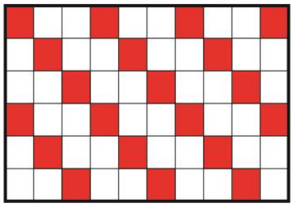
3. To create a Motion Detection region, select *Enable brush*.
4. From the *Enable brush* drop-down menu, select the size of the region (*1x1, 3x3,* or *5x5)*.
5. To clear the region, right-click your mouse and scroll over the region.
6. Configure the motion detection settings. See instructions below.
7. Set triggered actions. See instructions below.

To set a schedule

1. Select *By schedule*. The message "Please Select" is displayed.
2. Click *Please select*. A drop-down menu opens.
3. From the drop-down menu, select a schedule from 1 to 10. The selected schedules are displayed in a horizontal field above the drop-down menu.
4. Click **SAVE**.

To configure motion detection settings

1. *Sampling pixel interval* [*1-10]* – Select a number from 1-10. The default value is 1. If the value is set as 3, within the detection region, the system will take one sampling pixel for every 3 pixels by each row and each column (see the figure below).



Pixel Interval Illustration

2. *Detection level* [*1-100]* – Select a number from 1-100. The default level is 40. This sets detection level for each sampling pixel; the smaller the value, the more sensitive it is.
3. *Sensitivity level [1-100]* – Select a number from 1-100. The default level is 60, which means if 40% or more sampling pixels are detected differently, the system will detect motion. The bigger the value, the more sensitive it is and more colored segments will be displayed in the Motion Indication Bar.
4. *Time interval (sec) [0-7200]* – Select a number from 0-7200 (seconds). The default interval is 10. The value is the interval between each detected motion.

Triggered Action

The Administrator can specify various alarm actions to take when an alarm is triggered. See the Triggered Actions section for detailed descriptions of the actions. The following options are available:

- *Enable alarm output* – To enable the alarm relay output, check this box and select the preferred type of alarm output *(low* or *high*). The default setting is *high*.
- *Send alarm message by FTP* – Select whether to send an alarm message by FTP when motion is detected.
- *Send alarm message by E-Mail* – Select whether to send an alarm message by e-mail when motion is detected.
- *Upload image by FTP* – Select this box in order to upload an image to a designated FTP site when motion is detected according to various parameters.

- *Upload image by E-Mail* – Select this box in order to assign an e-mail address and configure various parameters.
- *Send HTTP notification* – Check this box to send a notification by HTTP.
- *Record video clip* – Select this box in order to save the alarm-triggered recording to the local microSD card.

File Name

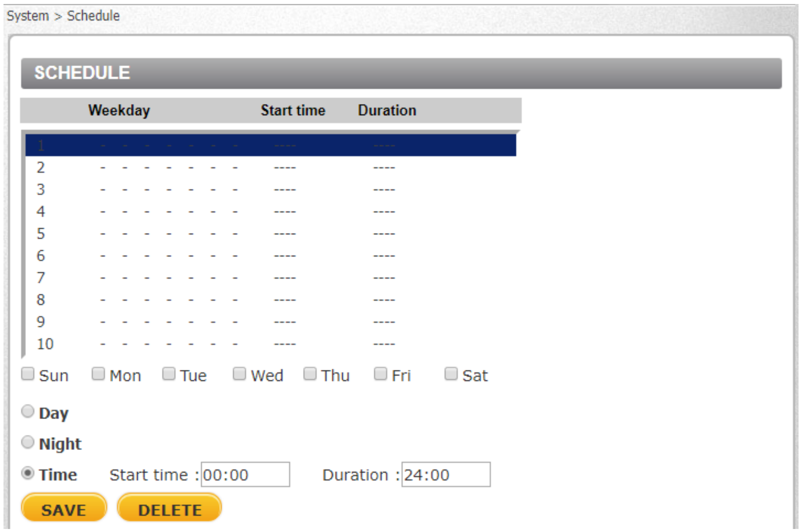
- *File Name* – Enter a file name in the field, for example *image.jpg.* The uploaded image's file name format is set in this section. Select one that meets your requirements.
- Add date/time suffix (default setting)
  File name: imageYYMMDD_HHNNSS_XX.jpg
  Y: Year, M: Month, D: Day
  H: Hour, N: Minute, S: Second
  X: Sequence Number
- Add sequence number suffix (no maximum value)
  File name: imageXXXXXXX.jpg
  X: Sequence Number
- Add sequence number suffix up to <specify a sequence number> and then start over
  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** to save the motion detection settings.

4.4.7 Schedule

The **Schedule** screen is used for setting schedules for the network failure detection and motion detection functions. 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.



System > Schedule

SCHEDULE

	Weekday	Start time	Duration
1	- - - - - - -	----	----
2	- - - - - - -	----	----
3	- - - - - - -	----	----
4	- - - - - - -	----	----
5	- - - - - - -	----	----
6	- - - - - - -	----	----
7	- - - - - - -	----	----
8	- - - - - - -	----	----
9	- - - - - - -	----	----
10	- - - - - - -	----	----

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

○ Day

○ Night

● Time Start time : 00:00 Duration : 24:00

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.

To create a new schedule or edit an existing schedule

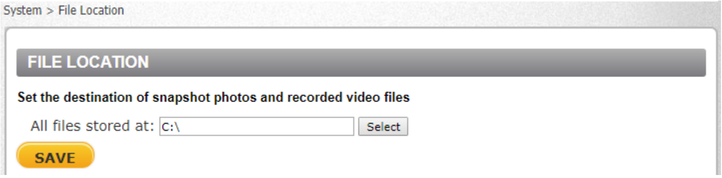
1. Select the appropriate checkbox for the day(s) of the week (Sun, Mon, Tue, Wed, Thu, Fri and Sat) to create a schedule.
2. Set *Start time* (for example, 09:00) and *Duration* (for example, 4:00 hours).
3. Click **Save** to apply the newly created schedule to the camera.

To remove a schedule

1. To remove a schedule, select the setup data line by line.
2. Click **Delete** to remove.

4.4.8 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.



Set the destination of snapshot photos and recorded video files

All files stored at: C:\

File Location Screen

Notes:

- Make sure the selected file path contains valid characters.
- When using Windows 8 or 10 OS, the storage location must not require Administrator access; for example, it cannot be the root directory, C:\.

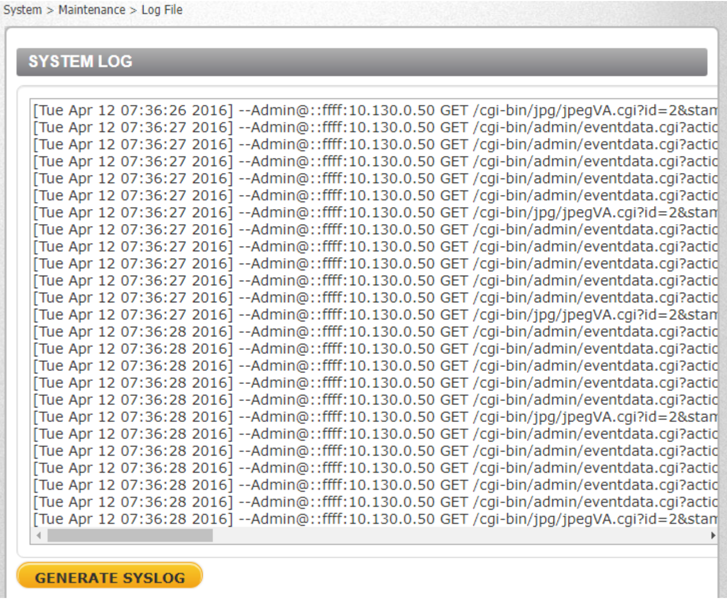
4.4.9 Maintenance

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

4.4.9.1 Log File

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

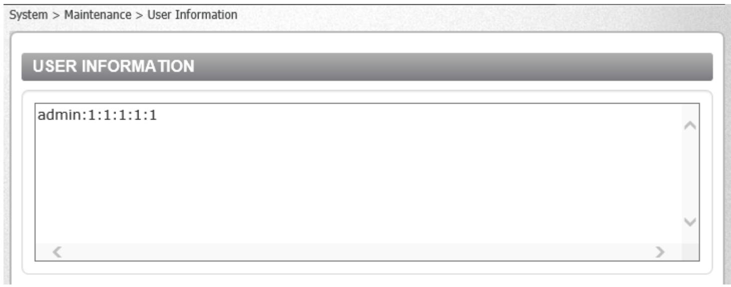


```
[Tue Apr 12 07:36:26 2016] --Admin@::ffff:10.130.0.50 GET /cgi-bin/jpg/jpegVA.cgi?id=2&stan
[Tue Apr 12 07:36:27 2016] --Admin@::ffff:10.130.0.50 GET /cgi-bin/admin/eventdata.cgi?actic
[Tue Apr 12 07:36:27 2016] --Admin@::ffff:10.130.0.50 GET /cgi-bin/admin/eventdata.cgi?actic
[Tue Apr 12 07:36:27 2016] --Admin@::ffff:10.130.0.50 GET /cgi-bin/admin/eventdata.cgi?actic
[Tue Apr 12 07:36:27 2016] --Admin@::ffff:10.130.0.50 GET /cgi-bin/admin/eventdata.cgi?actic
[Tue Apr 12 07:36:27 2016] --Admin@::ffff:10.130.0.50 GET /cgi-bin/admin/eventdata.cgi?actic
[Tue Apr 12 07:36:27 2016] --Admin@::ffff:10.130.0.50 GET /cgi-bin/jpg/jpegVA.cgi?id=2&stan
[Tue Apr 12 07:36:27 2016] --Admin@::ffff:10.130.0.50 GET /cgi-bin/admin/eventdata.cgi?actic
[Tue Apr 12 07:36:27 2016] --Admin@::ffff:10.130.0.50 GET /cgi-bin/admin/eventdata.cgi?actic
[Tue Apr 12 07:36:27 2016] --Admin@::ffff:10.130.0.50 GET /cgi-bin/admin/eventdata.cgi?actic
[Tue Apr 12 07:36:27 2016] --Admin@::ffff:10.130.0.50 GET /cgi-bin/admin/eventdata.cgi?actic
[Tue Apr 12 07:36:27 2016] --Admin@::ffff:10.130.0.50 GET /cgi-bin/admin/eventdata.cgi?actic
[Tue Apr 12 07:36:27 2016] --Admin@::ffff:10.130.0.50 GET /cgi-bin/jpg/jpegVA.cgi?id=2&stan
[Tue Apr 12 07:36:28 2016] --Admin@::ffff:10.130.0.50 GET /cgi-bin/admin/eventdata.cgi?actic
[Tue Apr 12 07:36:28 2016] --Admin@::ffff:10.130.0.50 GET /cgi-bin/admin/eventdata.cgi?actic
[Tue Apr 12 07:36:28 2016] --Admin@::ffff:10.130.0.50 GET /cgi-bin/admin/eventdata.cgi?actic
[Tue Apr 12 07:36:28 2016] --Admin@::ffff:10.130.0.50 GET /cgi-bin/admin/eventdata.cgi?actic
[Tue Apr 12 07:36:28 2016] --Admin@::ffff:10.130.0.50 GET /cgi-bin/admin/eventdata.cgi?actic
[Tue Apr 12 07:36:28 2016] --Admin@::ffff:10.130.0.50 GET /cgi-bin/jpg/jpegVA.cgi?id=2&stan
[Tue Apr 12 07:36:28 2016] --Admin@::ffff:10.130.0.50 GET /cgi-bin/admin/eventdata.cgi?actic
[Tue Apr 12 07:36:28 2016] --Admin@::ffff:10.130.0.50 GET /cgi-bin/admin/eventdata.cgi?actic
[Tue Apr 12 07:36:28 2016] --Admin@::ffff:10.130.0.50 GET /cgi-bin/admin/eventdata.cgi?actic
[Tue Apr 12 07:36:28 2016] --Admin@::ffff:10.130.0.50 GET /cgi-bin/admin/eventdata.cgi?actic
[Tue Apr 12 07:36:28 2016] --Admin@::ffff:10.130.0.50 GET /cgi-bin/admin/eventdata.cgi?actic
[Tue Apr 12 07:36:28 2016] --Admin@::ffff:10.130.0.50 GET /cgi-bin/jpg/jpegVA.cgi?id=2&stan
```

System Log Screen

4.4.9.2 User Information

The Administrator can view each user's login privileges on the **User information** screen.



```
admin:1:1:1:1:1
```

User Information – Get User Privacy

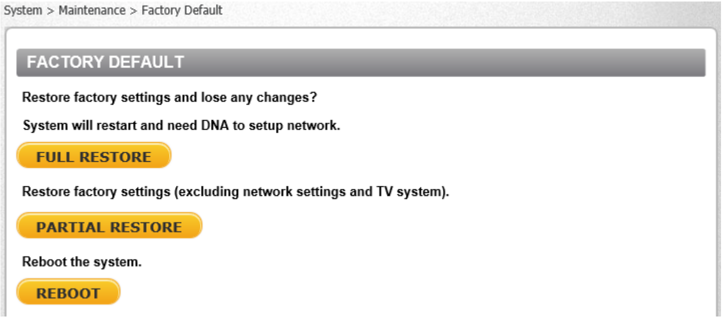
In the screen above, the *admin* user has privileges to I/O access, Camera control, Talk, and Listen, which are the maximum privileges that can be granted.

Note:

User credentials and privileges are set in the User screen.

4.4.9.3 Factory Default

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



System > Maintenance > Factory Default

FACTORY DEFAULT

Restore factory settings and lose any changes?

System will restart and need DNA to setup network.

Restore factory settings (excluding network settings and TV system).

Reboot the system.

Factory Default Screen

Full Restore

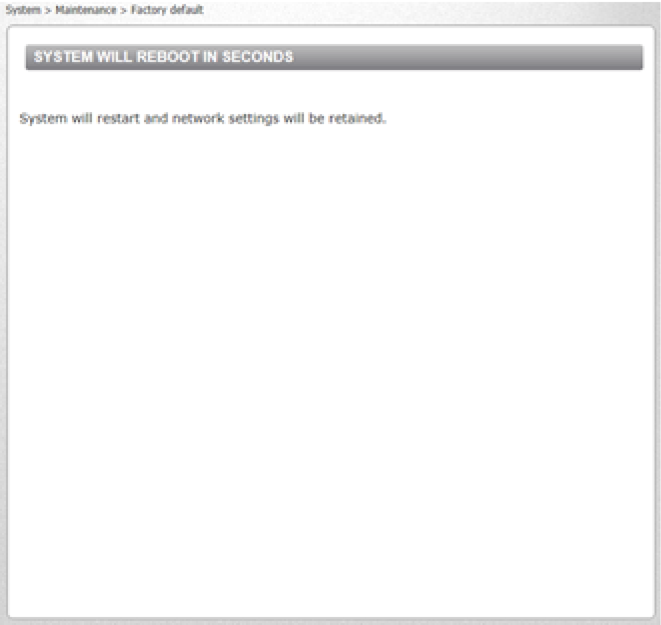
Click **FULL RESTORE** to restore the factory default settings. The system restarts in 30 seconds.

Note:

The IP address and all other settings will be restored to factory default settings and you will need the DNA to discover the camera again and reconfigure its network configuration.

Partial Restore

Click **PARTIAL RESTORE** to restore the factory default settings, but save the network settings and the TV system. The system restarts in 30 seconds.



System > Maintenance > Factory default

SYSTEM WILL REBOOT IN SECONDS

System will restart and network settings will be retained.

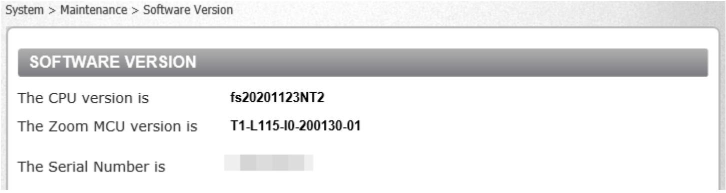
Partial Restore Screen

Reboot

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

4.4.9.4 Software Version

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



System > Maintenance > Software Version

SOFTWARE VERSION

The CPU version is fs20201123NT2

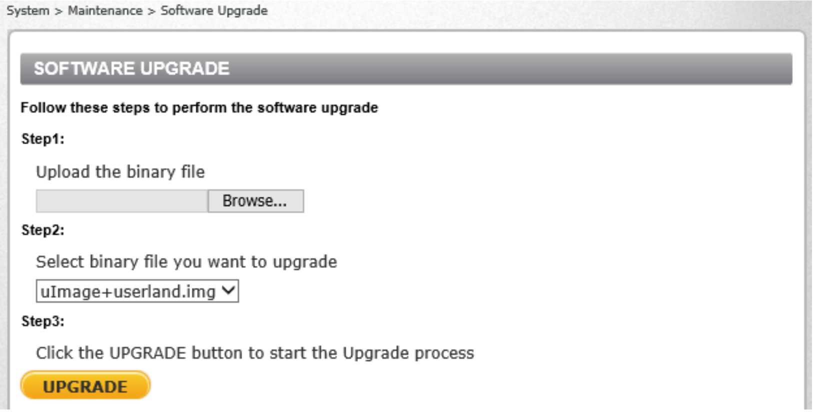
The Zoom MCU version is T1-L115-I0-200130-01

The Serial Number is [redacted]

Software Version Screen

4.4.9.5 Software Upgrade

The **Software Upgrade** screen enables you to select a software file to upload.



System > Maintenance > Software Upgrade

SOFTWARE UPGRADE

Follow these steps to perform the software upgrade

Step1:

Upload the binary file

Step2:

Select binary file you want to upgrade

uImage+userland.img

Step3:

Click the UPGRADE button to start the Upgrade process

Software Upgrade Screen

Notes:

- Make sure that the software upgrade file is available before performing a software upgrade.
- Do not change the file name. If you change the upgrade file name, the system will fail to find the file.
- Software can also be upgraded via DNA version 2.3.0.17 or higher.

Caution:

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

Attention:

- *Ne débranchez pas l'alimentation pendant la modification des noms de fichiers.*
- *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.img`.

> **Note:**
>
> Do not change the file name. If you change the upgrade file name, the system will fail to find the file.

2. From the drop-down menu of binary files in Step 2, select the file to upgrade. In the above example `uImage+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 the web browser.
5. Delete the existing Quasar Player.

    a. From the Windows Start menu, select *Control Panel*.

    b. Select *Uninstall a Program*.

> **Note:**
>
> An installed program should be deleted and a new Quasar Player should be installed only when prompted.

    c. In the *Currently installed programs* list, select *Quasar Player.*

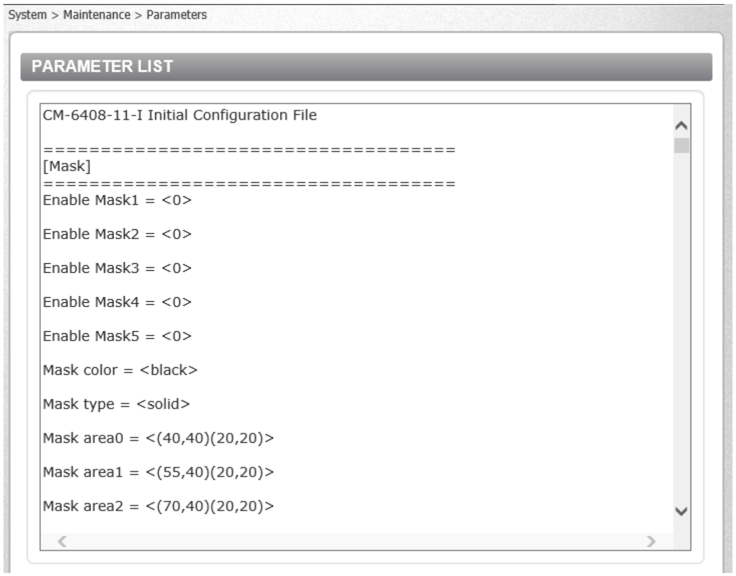
    d. Click **Uninstall** to delete the existing plug-in file.

> **Note:**
>
> For more information about deleting an existing web player, see Installing and Deleting the Web Player.

6. After logging back into the camera's web page, install the new Quasar Player.

4.4.9.6 Parameters

The **Parameters** screen displays all of the system's parameter settings.



System > Maintenance > Parameters

PARAMETER LIST

```
CM-6408-11-I Initial Configuration File

==================================
[Mask]
==================================
Enable Mask1 = <0>

Enable Mask2 = <0>

Enable Mask3 = <0>

Enable Mask4 = <0>

Enable Mask5 = <0>

Mask color = <black>

Mask type = <solid>

Mask area0 = <(40,40)(20,20)>

Mask area1 = <(55,40)(20,20)>

Mask area2 = <(70,40)(20,20)>
```

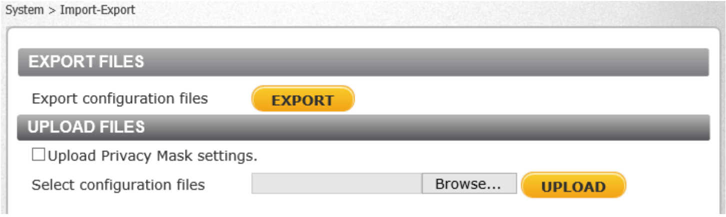
Parameters Screen

Note:

To view the entire list of parameters, use the scrollbar on the right of the screen.

4.4.10 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.



System > Import-Export

EXPORT FILES

Export configuration files EXPORT

UPLOAD FILES

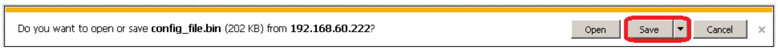
□Upload Privacy Mask settings.

Select configuration files Browse... UPLOAD

Import/Export Screen

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**?

Export Configuration File Information Bar

2. Click **Save.**
3. Specify a location to save the configuration file.

To import a configuration file

1. (Optional) If you are importing privacy mask settings, select the checkbox.
2. Click **Browse** to select the configuration file.

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

Note:

Do not change the file name. If you change the upgrade file name, the system will fail to find the file.

⚠

Caution:

Do not unplug power while changing file names.

Attention:

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

4.5 Streaming Tab

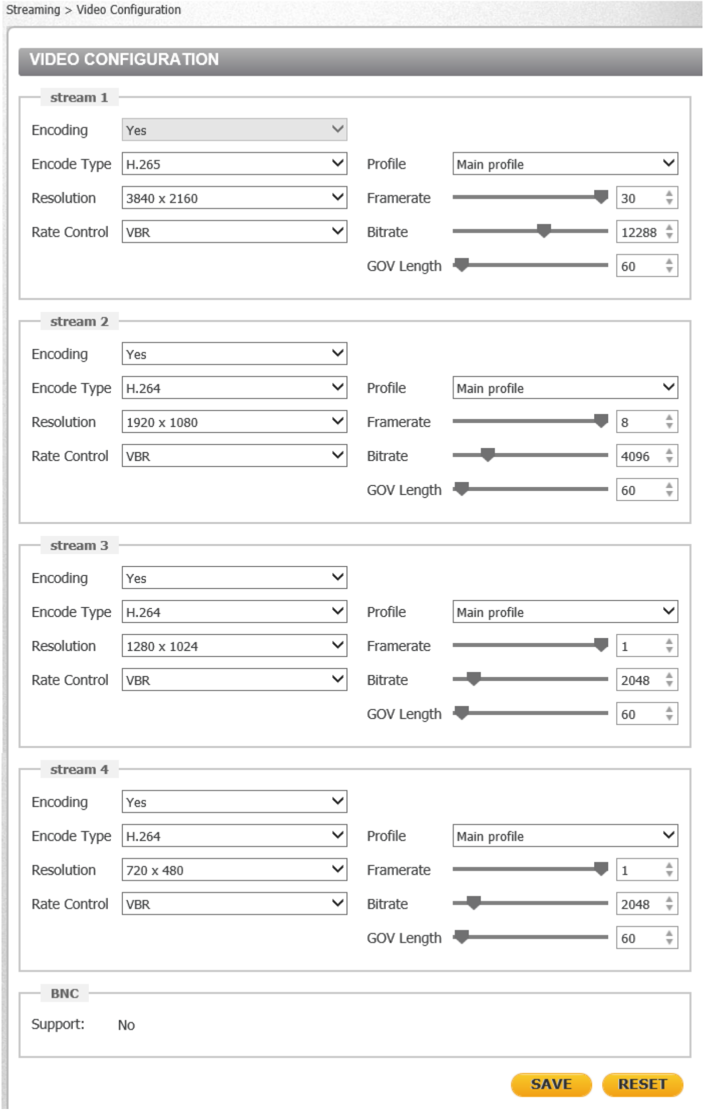
Select the **Streaming** tab in the navigation bar at the top of the page to display the configurable video and audio selections in the sidebar. From the **Streaming** sidebar, the Administrator can configure a specific video resolution, video compression mode, video protocol, video frame rate, and audio transmission mode.

Details of these settings are specified in the following sections:

Video Configuration Video Rotation Video Text Overlay Video OCX Protocol Audio

4.5.1 Video Configuration

On the **Video Configuration** screen, you can configure most of the camera's video settings.



Streaming > Video Configuration

VIDEO CONFIGURATION

stream 1

Encoding: Yes
Encode Type: H.265 — Profile: Main profile
Resolution: 3840 x 2160 — Framerate: 30
Rate Control: VBR — Bitrate: 12288
GOV Length: 60

stream 2

Encoding: Yes
Encode Type: H.264 — Profile: Main profile
Resolution: 1920 x 1080 — Framerate: 8
Rate Control: VBR — Bitrate: 4096
GOV Length: 60

stream 3

Encoding: Yes
Encode Type: H.264 — Profile: Main profile
Resolution: 1280 x 1024 — Framerate: 1
Rate Control: VBR — Bitrate: 2048
GOV Length: 60

stream 4

Encoding: Yes
Encode Type: H.264 — Profile: Main profile
Resolution: 720 x 480 — Framerate: 1
Rate Control: VBR — Bitrate: 2048
GOV Length: 60

BNC

Support: No

Video Configuration Screen

CM-640x cameras support up to four IP video streams. For each video stream, you can individually specify the Encode Type (video compression), the resolution, the frame rate, and other settings for that stream. CM-640x cameras support H.265, H.264, and MJPEG video compression. The selected Encode Type determines the other settings that are available.

The resolutions and maximum frame rate available on Streams 2, 3, and 4 depend on:

- The combination and settings of each stream configured before it. For example, Stream 4 performance depends on the settings for Streams 1, 2, and 3. Stream 3 performance depends on the settings for Streams 1 and 2.
- The TV System setting on the Camera > Misc. screen. When WDR 2 Shutter (PAL) or WDR 2 Shutter (NTSC) is selected, the maximum frame rate available is 25/30 frames per second. For 50 fps (PAL) or 60 fps (NTSC), which is also known as linear mode, the maximum is 50/60 frames per second.

By default, the camera is configured with Stream 1 and Stream 2 enabled at 3840 x 2160 (CM-6408 models) or 2688x1944 (CM-6405 models) and D1.

For more information about video configuration settings, see:

- Encode Type
- CM-6408 Video Resolutions
- CM-6405 Video Resolutions

Note:

United VMS supports up to three streams.

4.5.1.1 Encode Type

The selected Encode Type — H.265, H.264, or MJPEG — determines the other settings that are available.

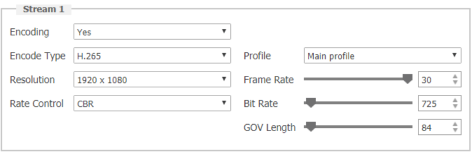
Notes:

- When Accessing the Camera's Web Page using a browser other than MS IE 11.0, the camera's web page only supports MJPEG streaming. To see live video in the web page when using other browsers, select MJPEG encoding for at least one of the video streams.
- Images can be sent by FTP or email only when MJPEG is selected as the Encode Type for one of the streams.

H.265 and H.264 Settings

When H.265 or H.264 compression is selected, you can configure the following:

- *Rate Control*: Select *CBR, VBR,* or *LBR*. The default setting is *VBR*.
  - ○ *CBR* (Constant Bit Rate) is used for setting a constant, maximum bit rate. CBR is not optimal for storage or quality, because it does not allocate enough data for complex sections (which results in degraded quality), and wastes data on simple sections. Choosing a higher bit rate results in better quality, but requires more storage. The following options are available if you select *CBR* Rate Control:



Stream 1

Encoding: Yes

Encode Type: H.265

Resolution: 1920 x 1080

Rate Control: CBR

Profile: Main profile

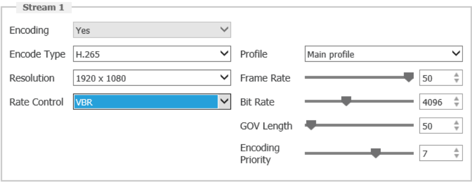
Frame Rate: 30

Bit Rate: 725

GOV Length: 84

H.264/H.265 with CBR Rate Control

  - *VBR* (Variable Bit Rate) files vary the amount of data per time segment. VBR enables a higher bit rate (and therefore requires more storage space) for more complex video or audio, while a lower bit rate and less storage space is allocated to less complex media. VBR files may take longer to encode and might be more problematic for streaming if the maximum bit rate is not set high enough to allow for high instantaneous bit rates. The following options are available if you select *VBR* Rate Control:

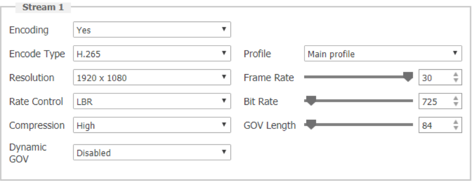


Stream 1

Encoding	Yes		
Encode Type	H.265	Profile	Main profile
Resolution	1920 x 1080	Frame Rate	50
Rate Control	VBR	Bit Rate	4096
		GOV Length	50
		Encoding Priority	7

H.264/H.265 with VBR Rate Control

  - *LBR* (Low Bit Rate) encoding is used primarily for speech at rates below 4kbps. With this encoding, not all of the voice frequency range is encoded. LBR consumes less storage space than CBR or VBR. The following options are available if you select *LBR* Rate Control and disable Dynamic GOV:

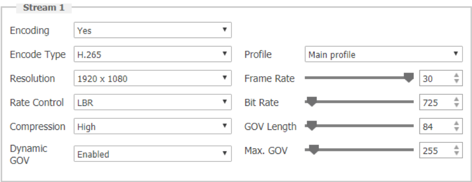


Stream 1

Encoding	Yes		
Encode Type	H.265	Profile	Main profile
Resolution	1920 x 1080	Frame Rate	30
Rate Control	LBR	Bit Rate	725
Compression	High	GOV Length	84
Dynamic GOV	Disabled		

H.264/H.265 with LBR Rate Control

If you select *LBR* Rate Control and enable Dynamic GOV The following options are available:



Stream 1

Encoding	Yes		
Encode Type	H.265	Profile	Main profile
Resolution	1920 x 1080	Frame Rate	30
Rate Control	LBR	Bit Rate	725
Compression	High	GOV Length	84
Dynamic GOV	Enabled	Max. GOV	255

H.264/H.265 with LBR
Rate Control and Dynamic GOV

- *Compression:* Select *Hi, Mid,* or *Low.* Low produces the highest image quality, but increases the file size. High produces the lowest image quality, but decreases the file size. The default setting is *High*. Available only with LBR Rate Control.

- *Dynamic GOV*: Select *Enabled* or *Disabled.* The default setting is *Disabled*. If you select *Enabled*, move the *Max. GOV* slider to a value between 0-255. The default setting is *255*. Available only with LBR Rate Control.

- *Profile*:

  - *High Profile* (HP) provides the best trade-off between storage size and video latency and is the primary profile for HD broadcast applications. It can save 10-30% of the storage cost over Main Profile. However, it may also increase video latency, depending on the stream structure.

  - *Main Profile* (MP) is the default setting. It provides improved picture quality at reduced bandwidths and storage costs.

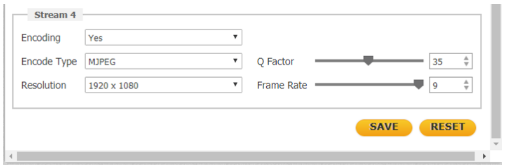
- *Frame Rate*: Move the slider to the desired setting. A maximum 25/30 frames per seconds is available for *WDR 2 Shutter (PAL)* or *WDR 2 Shutter (NTSC).* A maximum 50/60 frames per second is available for *50 fps (PAL)* or *60 fps (NTSC).* The higher the frame rate, the smoother the motion in the video.

- *Bit Rate*: Move the slider to the desired setting between 1-10240. The default setting is *4096*. The higher the bit rate, the better the image quality. Set the maximum bit rate high enough to allow for a high instantaneous bit for more complex video. A higher bit rate consumes more storage space.

- *GOV Length*: Move the slider to a value between 0-4095. The setting determines the frame structure (I-frames and P-frames) for saving bandwidth in a video stream. A longer GOV means decreasing the frequency of I-frames. The default setting is *50*.
- *Encoding Priority*: Move the slider to a value between *1* (low bit rate) to *10* (high picture quality). This function enables the user to adjust the quality of the picture along a single axis.The default is 7. Available only with VBR Rate Control.

Click **SAVE**. To reset the values, click **RESET**.

MJPEG Settings



Stream 4

Encoding: Yes

Encode Type: MJPEG

Resolution: 1920 x 1080

Q Factor: 35

Frame Rate: 9

MJPEG Compression Settings

When MJPEG compression is selected, you can configure the following:

- *Q Factor*: Select the desired value. 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 70.
- *Frame Rate*: Move the slider to the desired setting. A maximum 25/30 frames per seconds is available for *WDR 2 Shutter (PAL)* or *WDR 2 Shutter (NTSC).* A maximum 50/60 frames per second is available for *50 fps (PAL)* or *60 fps (NTSC).* The higher the frame rate, the smoother the motion in the video.

Click **SAVE**. To reset the values, click **RESET**.

4.5.1.2 CM-6408 Video Resolutions

When a PAL TV System is selected, the D1 resolution is 720x576. NTSC D1 resolution is 720x480.

Linear Mode

When the TV System is *50 fps (PAL)* or *60 fps (NTSC)* on a CM-6408 camera, the following resolutions are available:

Stream 1	Stream 2	Stream 3	Stream 4
3840x2160 (25/30 fps)	OFF	OFF	OFF
	1080P (25/30 fps)	OFF	OFF
	720P (25/30 fps)	OFF	OFF
		720P (25/30 fps)	OFF
			D1 (25/30 fps)
		D1 (25/30 fps)	OFF
			D1 (25/30 fps)
	D1 (25/30 fps)	OFF	OFF
		D1 (25/30 fps)	OFF
			D1 (25/30 fps)

Stream 1	Stream 2	Stream 3	Stream 4
1080P (50/60 fps)	OFF	OFF	OFF
	1080P (50/60 fps)	OFF	OFF
		1080P (25/30 fps)	OFF
		720P (50/60 fps)	OFF
			D1 (25/30 fps)
		D1 (50/60 fps)	OFF
			D1 (50/60 fps)
	720P (50/60 fps)	OFF	OFF
		720P (50/60 fps)	OFF
			720P (50/60 fps)
			D1 (50/60 fps)
		D1 (50/60 fps)	OFF
			D1 (50/60 fps)
	D1 (50/60 fps)	OFF	OFF
		D1 (50/60 fps)	OFF
			D1 (50/60 fps)
720P (50/60 fps)	OFF	OFF	OFF
	720P (50/60 fps)	OFF	OFF
		720P (50/60 fps)	OFF
			720P (50/60 fps)
			D1 (50/60 fps)
		D1 (50/60 fps)	OFF
			D1 (50/60 fps)
	D1 (50/60 fps)	OFF	OFF
		D1 (50/60 fps)	OFF
			D1 (50/60 fps)

Shutter Mode

When the TV System is *WDR 2 Shutter (PAL)* or *WDR 2 Shutter (NTSC)* on a CM-6408 camera, the following resolutions are available:

Stream 1	Stream 2	Stream 3	Stream 4
3840x2160 (25/30 fps)	OFF	OFF	OFF
	1080P (25/30 fps)	OFF	OFF
	720P (25/30 fps)	OFF	OFF
		720P (25/30 fps)	OFF
			D1 (25/30 fps)
		D1 (25/30 fps)	OFF
			D1 (25/30 fps)
	D1 (25/30 fps)	OFF	OFF
		D1 (25/30 fps)	OFF
			D1 (25/30 fps)
1080P (25 fps)	OFF	OFF	OFF
	1080P (25/30 fps)	OFF	OFF
		1080P (25/30 fps)	OFF
			1080P (25/30 fps)
			720P (25/30 fps)
			D1 (25/30 fps)
		720P (25/30 fps)	OFF
			720P (25/30 fps)
			D1 (25/30 fps)
		D1 (25/30 fps)	OFF
			D1 (25/30 fps)
	720P (25/30 fps)	OFF	OFF
		720P (25/30 fps)	OFF
			720P (25/30 fps)
			D1 (25/30 fps)
		D1 (25 fps)	OFF
			D1 (25/30 fps)
	D1 (25/30 fps)	OFF	OFF
		D1 (25/30 fps)	OFF
			D1 (25/30 fps)

This document does not contain any export-controlled information.

Stream 1	Stream 2	Stream 3	Stream 4
720P (25/30 fps)	OFF	OFF	OFF
	720P (25/30 fps)	OFF	OFF
		720P (25/30 fps)	OFF
			720P (25/30 fps)
			D1 (25/30 fps)
		D1 (25/30 fps)	OFF
			D1 (25/30 fps)
	D1 (25/30 fps)	OFF	OFF
		D1 (25/30 fps)	OFF
			D1 (25/30 fps)

4.5.1.3 CM-6405 Video Resolutions

When a PAL TV System is selected, the D1 resolution is 720x576. NTSC D1 resolution is 720x480.

Linear Mode

When the TV System is *50 fps (PAL)* or *60 fps (NTSC)* on a CM-6405 camera, the following resolutions are available:

Stream 1	Stream 2	Stream 3	Stream 4
2688x1944 (25/30 fps)	OFF	OFF	OFF
	2688x1944 (25/30 fps)	OFF	OFF
	1080P (25/30 fps)	OFF	OFF
		1080P (25/30 fps)	OFF
			720P (25/30 fps)
			D1 (25/30 fps)
		720P (25/30 fps)	OFF
			720P (25/30 fps)
			D1 (25/30 fps)
		D1 (25/30 fps)	OFF
			D1 (25/30 fps)
	720P (25/30 fps)	OFF	OFF
		720P (25/30 fps)	OFF
			720P (25/30 fps)
			D1 (25/30 fps)
		D1 (25/30 fps)	OFF
			D1 (25/30 fps)
	D1 (25/30 fps)	OFF	OFF
		D1 (25/30 fps)	OFF
			D1 (25/30 fps)

Stream 1	Stream 2	Stream 3	Stream 4
1080P (50 fps)	OFF	OFF	OFF
	1080P (50 fps)	OFF	OFF
		1080P (25/30 fps)	OFF
		720P (50 fps)	OFF
			D1 (25/30 fps)
		720P (25/30 fps)	720P (25/30 fps)
		D1 (50 fps)	OFF
			D1 (50 fps)
	720P (50 fps)	OFF	OFF
		720P (50 fps)	OFF
			720P (50 fps)
			D1 (50 fps)
		D1 (50 fps)	OFF
			D1 (50 fps)
	D1 (50 fps)	OFF	OFF
		D1 (50 fps)	OFF
			D1 (50 fps)
1080P (25/30 fps)	1080P (25/30 fps)	1080P (25/30 fps)	1080P (25/30 fps)
			720P (25/30 fps)
			D1 (25/30 fps)
		720P (25/30 fps)	720P (25/30 fps)
720P (50 fps)	OFF	OFF	OFF
	720P (50 fps)	OFF	OFF
		720P (50 fps)	OFF
			720P (50 fps)
			D1 (50 fps)
		D1 (50 fps)	OFF
			D1 (50 fps)
	D1 (50 fps)	OFF	OFF
		D1 (50 fps)	OFF
			D1 (50 fps)

Shutter Mode

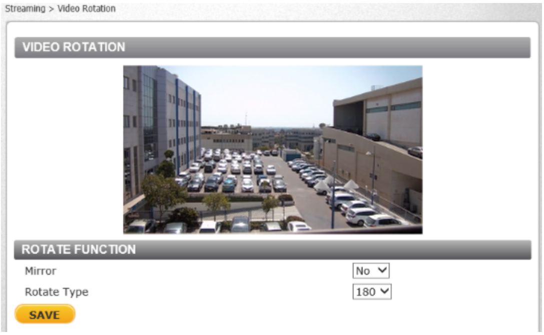
When the TV System is *WDR 2 Shutter (PAL)* or *WDR 2 Shutter (NTSC)* on a CM-6405 camera, the following resolutions are available:

Stream 1	Stream 2	Stream 3	Stream 4
2688x1944 (25/30 fps)	OFF	OFF	OFF
	2688x1944 (25/30 fps)	OFF	OFF
	1080P (25/30 fps)	OFF	OFF
		1080P (25/30 fps)	OFF
			720P (25/30 fps)
			D1 (25/30 fps)
		720P (25/30 fps)	OFF
			720P (25/30 fps)
			D1 (25/30 fps)
		D1 (25/30 fps)	OFF
			D1 (25/30 fps)
	720P (25/30 fps)	OFF	OFF
		720P (25/30 fps)	OFF
			720P (25/30 fps)
			D1 (25/30 fps)
		D1 (25/30 fps)	OFF
			D1 (25/30 fps)
	D1 (25/30 fps)	OFF	OFF
		D1 (25/30 fps)	OFF
			D1 (25/30 fps)

Stream 1	Stream 2	Stream 3	Stream 4
1080P (25/30 fps)	OFF	OFF	OFF
	1080P (25/30 fps)	OFF	OFF
		1080P (25/30 fps)	OFF
			1080P (25/30 fps)
			720P (25/30 fps)
			D1 (25/30 fps)
		720P (25/30 fps)	OFF
			720P (25/30 fps)
			D1 (25/30 fps)
		D1 (25/30 fps)	OFF
			D1 (25/30 fps)
	720P (25/30 fps)	OFF	OFF
		720P (25/30 fps)	OFF
			720P (25/30 fps)
			D1 (25/30 fps)
		D1 (25/30 fps)	OFF
			D1 (25/30 fps)
	D1 (25/30 fps)	OFF	OFF
		D1 (25/30 fps)	OFF
			D1 (25/30 fps)
720P (25/30 fps)	OFF	OFF	OFF
	720P (25/30 fps)	OFF	OFF
		720P (25/30 fps)	OFF
			720P (25/30 fps)
			D1 (25/30 fps)
		D1 (25/30 fps)	OFF
			D1 (25/30 fps)
	D1 (25/30 fps)	OFF	OFF
		D1 (25/30 fps)	OFF
			D1 (25/30 fps)

4.5.2 Video Rotation

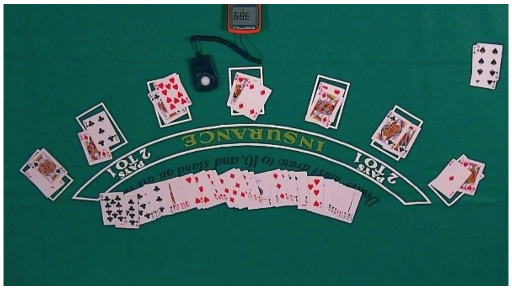
The **Video Rotation** screen enables you to flip the video and select the rotation angle.



Mirror No
Rotate Type 180

Video Rotation Screen

From the *Mirror* drop-down menu, select *Yes* or *No*. *Yes* reverses the image along its vertical axis.



Source Image Before Reversing the Image

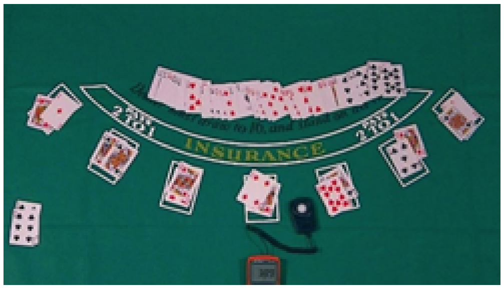


Image After Reversal

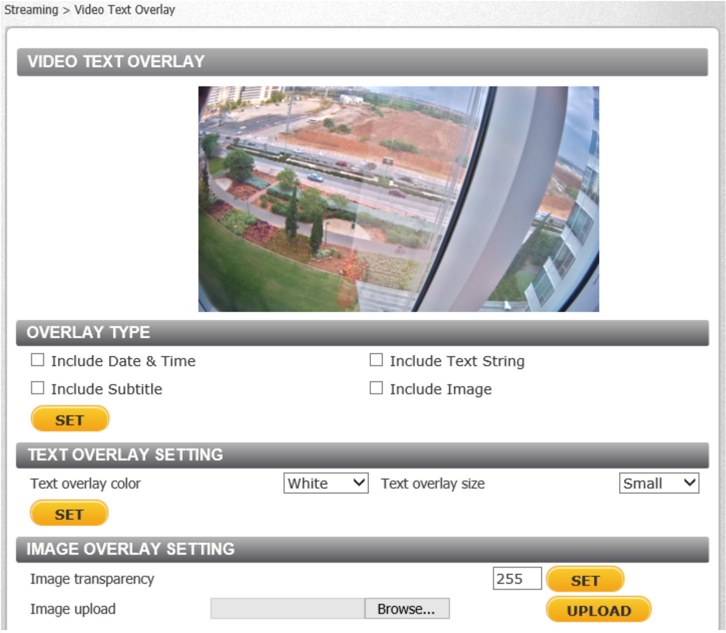
From the *Rotate Type* drop-down menu, select 0, 90, 180, or 270 (degrees):

- 0 – The image does not rotate.
- 90 – The image rotates 90° clockwise (to the right).
- 180 – The image rotates 180° counter-clockwise (to the left).
- 270 – The image rotates 90° counter-clockwise (to the left).

Click **SAVE** to confirm the settings.

4.5.3 Video Text Overlay

The **Video Text Overlay** screen enables you configure settings for the text displayed over the live video.



Streaming > Video Text Overlay

VIDEO TEXT OVERLAY

OVERLAY TYPE

☐ Include Date & Time ☐ Include Text String

☐ Include Subtitle ☐ Include Image

SET

TEXT OVERLAY SETTING

Text overlay color: White | Text overlay size: Small

SET

IMAGE OVERLAY SETTING

Image transparency: 255 SET

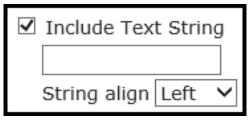
Image upload: Browse... UPLOAD

Video Text Overlay Screen

Select the relevant checkbox for the data to include in the on-screen display:

Overlay Type

- *Include Date & Time* − Display the date and time.
- *Include Subtitle* − When this checkbox is selected, enter the string that you wish to display in the text box that opens.
- *Include Text String* − When this checkbox is selected, enter the string that you wish to display in the text box that opens and the string alignment (*Left* or *Right*). The maximum length of the string is 20 alphanumeric characters.



☑ Include Text String

String align: Left

- *Include Image* − When this checkbox is selected, an image, such as a logo, is displayed in the overlay. Select the image alignment (*Left* or *Right*) and then use the Image Overlay Setting section to upload the image.

Click **SET** when finished.

Text Overlay Setting

- *Text Overlay Color* − From the drop-down menu, select the desired color.
- *Text Overlay Size* − From the drop-down menu, select the desired text size.

Click **SET** when finished.

Image Overlay Setting

- *Image Transparency* − Select a number from 0-255. The default is *255*. The lower the value, the more transparent the image will be. Click **SET** when finished.

Note:

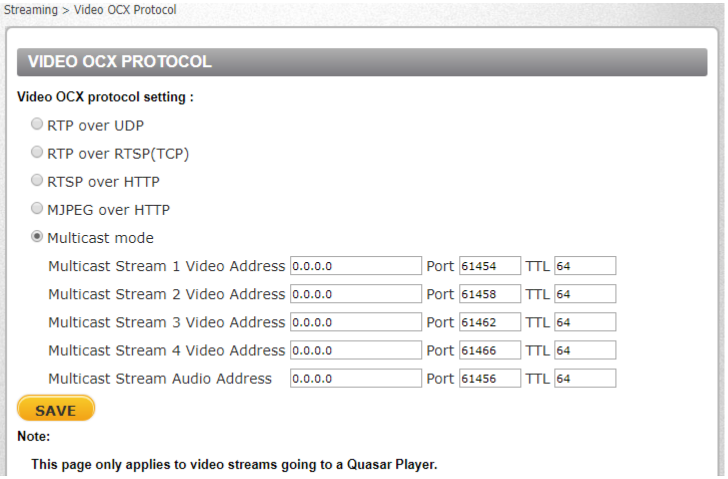
The file must be saved as an 8-bit `.bmp` file.The length should be a multiple of 32 (for example, 320 pixels) and the width should be a multiple of 4 (for example 40 pixels). The maximum resolution of the image should not exceed 32,768 pixels.

- *Image Upload* − Select a file to upload. Then click **UPLOAD**.

Users can select the items to display data including date/time/text on the Live Video pane.

4.5.4 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*.



Streaming > Video OCX Protocol

VIDEO OCX PROTOCOL

Video OCX protocol setting :

○ RTP over UDP
○ RTP over RTSP(TCP)
○ RTSP over HTTP
○ MJPEG over HTTP
● Multicast mode

Multicast Stream 1 Video Address	0.0.0.0	Port	61454	TTL	64
Multicast Stream 2 Video Address	0.0.0.0	Port	61458	TTL	64
Multicast Stream 3 Video Address	0.0.0.0	Port	61462	TTL	64
Multicast Stream 4 Video Address	0.0.0.0	Port	61466	TTL	64
Multicast Stream Audio Address	0.0.0.0	Port	61456	TTL	64

Note:

This page only applies to video streams going to a Quasar Player.

Video OCX Protocol Screen

The screen includes the following settings:

- *RTP over UDP*
- *RTP over RTSP (TCP)*
- *RTSP over HTTP*
- *MJPEG over HTTP*
- *Multicast mode* – For Stream 1,2,3, and 4 (where applicable), enter the following details: *Video Address, Port, and TTL.* Also enter the *Multicast Stream Audio Address*.

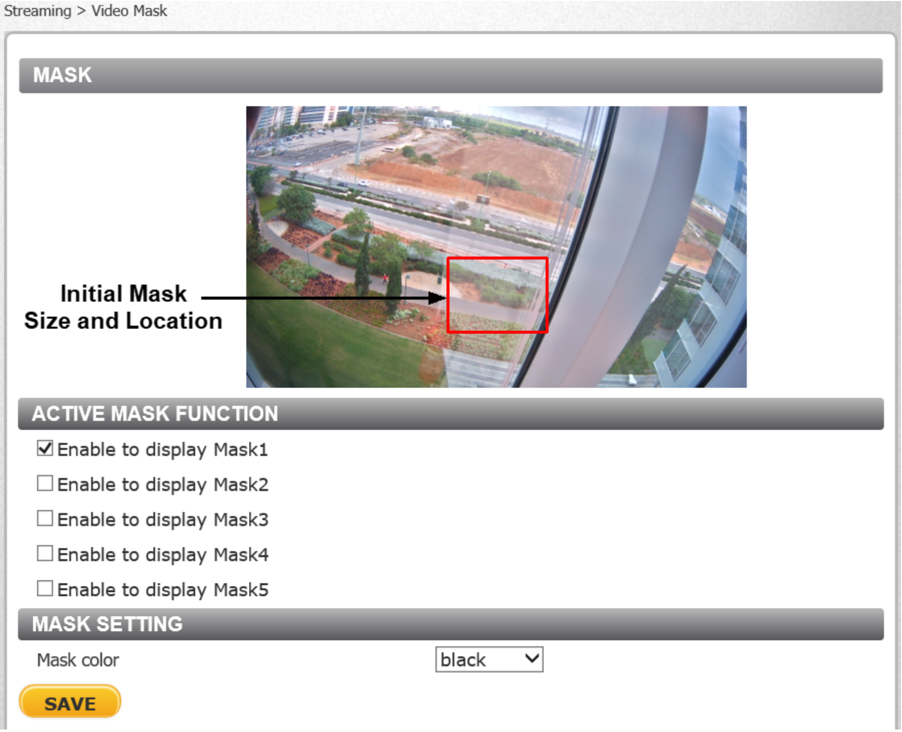
Note:

The TTL (Time to Live) value instructs the network router whether or not to discard a packet and is reduced every time the datagram is forwarded to another router. The packet is discarded if the TTL reaches 0. The recommended value is 64.

Click **SAVE** to confirm the settings.

4.5.5 Video Mask

From the **Video Mask** page, you can set up to five privacy masks. Masks conceal sensitive portions of the camera image to avoid intrusive monitoring.



Streaming > Video Mask

☑ Enable to display Mask1

□ Enable to display Mask2

□ Enable to display Mask3

□ Enable to display Mask4

□ Enable to display Mask5

Mask color: black

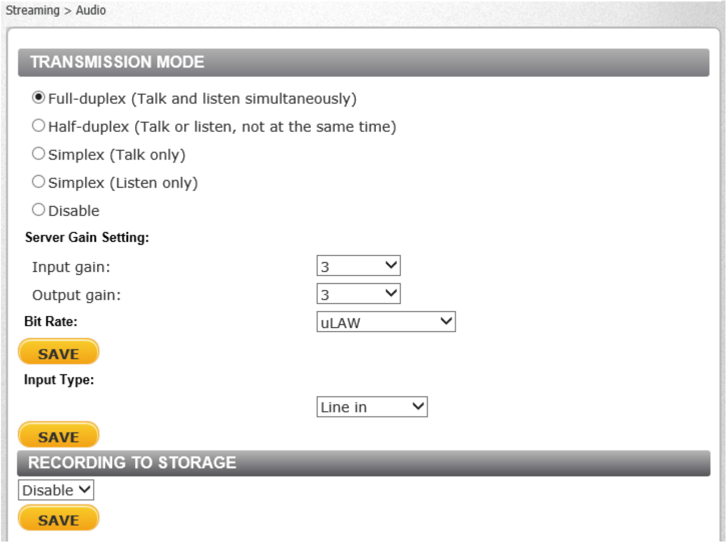
Video Mask Screen - Mask1 Enabled

To enable and modify masks

1. Select Enable to display MaskX. The mask appears on the **Live View** window. The mask with red borders is the one you are currently editing. When multiple masks are enabled, you can click the sides or corners of any mask or inside any mask to edit it.
2. To change the size of the mask, click and drag the sides or corners of the mask area.
3. To move the mask, click inside the mask area and drag it.
4. Under **Mask Setting**, select the fill color for all enabled masks.
5. Click **SAVE**. Enabled masks appear in the **Live View** window.

4.5.6 Audio

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



Streaming > Audio

TRANSMISSION MODE

● Full-duplex (Talk and listen simultaneously)

○ Half-duplex (Talk or listen, not at the same time)

○ Simplex (Talk only)

○ Simplex (Listen only)

○ Disable

Server Gain Setting:

Input gain: 3

Output gain: 3

Bit Rate: uLAW

SAVE

Input Type: Line in

SAVE

RECORDING TO STORAGE

Disable

SAVE

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 sound will be turned off if the input or output gain is set to *Mute*.

- The audio input gain is adjustable from *1-10*. The default setting is *3*.
- The audio output gain is adjustable from *1-6*. The default setting is *3*.

Bit Rate

Selectable audio transmission bit rate include 16 kbps (G.726), 24 kbps (G.726), 32 kbps (G.726), 40 kbps (G.726), µ-law (G.711), a-law (G.711), AAC, PCM (128 kbps), PCM (256 kbps), PCM (384 kbps), and PCM (768 kbps). 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 / UVMS does not support G.726.

Click **SAVE** to confirm the settings.

Input Type
Select *Line in* or *External Mic*.

Recording to Storage

This function enables recording of the audio on the SD card and NAS. The *Recording to Storage* function may be enabled or disabled in the **Audio** screen. The default setting is *Disable.*

Note:

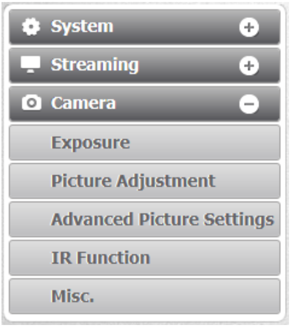
This function works only if the *Recording to Storage* option has been selected or if the *Schedule* option has been set.

Click **SAVE** to confirm the settings.

4.6 Camera Tab

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

Exposure Picture Adjustment Advanced Picture Settings IR Function Misc.

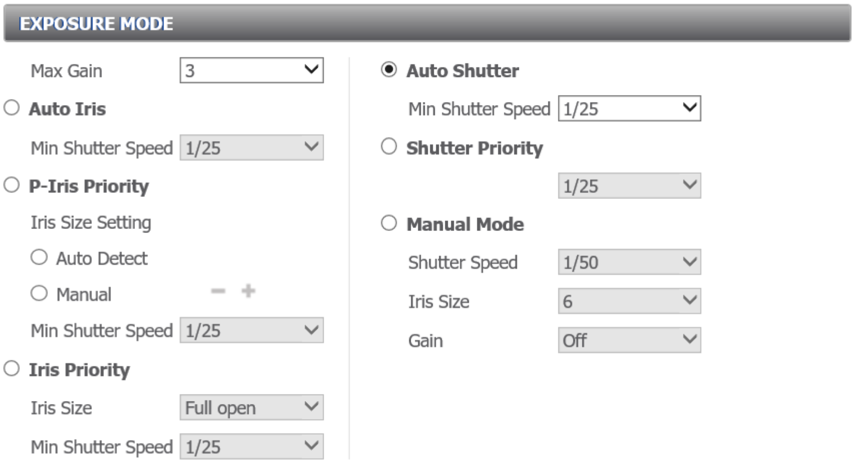


Camera Section Tabs

4.6.1 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 and is determined by the amount of exposure by the sensor (shutter speed), and other exposure parameters.

Administrators may either allow the camera to automatically select an exposure level using a programmed algorithm or choose the level themselves. The smaller the number (the higher the shutter speed) that the administrator selects, the lower the exposure level and vice versa. The configurable settings depend on the selected exposure mode.



EXPOSURE MODE

Max Gain 3

○ Auto Iris

Min Shutter Speed 1/25

○ P-Iris Priority

Iris Size Setting

○ Auto Detect

○ Manual − +

Min Shutter Speed 1/25

○ Iris Priority

Iris Size Full open

Min Shutter Speed 1/25

● Auto Shutter

Min Shutter Speed 1/25

○ Shutter Priority

1/25

○ Manual Mode

Shutter Speed 1/50

Iris Size 6

Gain Off

Exposure Screen
CP-6408-11-I

On the CM-6408-11-I model, specify the *Max Gain*, the maximum amount of gain (*1*-*3*) to apply to the image or turn it *Off*, for all modes. Increasing gain increases the sensitivity of the image sensor, brightens the image, and adds details. It also increases the level of noise in the image.

Select the Exposure Mode:

- Auto Iris Mode *
- P-Iris Priority Mode
- Iris Priority Mode *
- Auto Shutter Mode *
- Shutter Priority Mode *
- Manual Mode

* Only available on the CP-6408-11-I model.

4.6.1.1 Auto Iris Mode

In *Auto Iris* mode, specify a minimum shutter speed and the camera automatically adjusts the iris size and other exposure settings.

Min Shutter Speed – Select a suitable shutter speed according to the environmental luminance:

Auto Iris Min Shutter Speed			
PAL		**NTSC**	
1/25	1/3	1/30	1/4
1/12	1/1.5	1/15	1/2
1/6	-	1/8	1

⚠

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.

4.6.1.2 P-Iris Priority Mode

In *P-iris Priority* mode, the iris size is fixed. However, if the amount of light entering the camera lens drops below the level required for that setting, the iris automatically fully opens. The camera automatically adjusts other exposure settings.

Iris Size Setting (CP-6408-11-I) – Select one of the following:

- *Auto Detect* – When you select *Auto Detect*, the camera automatically detects the optimal iris size for the current light conditions.
- *Manual* – When you select *Manual*, manually adjust the iris size:

− The minus (-) button closes the iris.

+ The plus (+) button opens the iris.

Iris Size Setting > *P-Iris* (CP-6405-11-I) – Manually adjust the iris size:

− The minus (-) button closes the iris.

+ The plus (+) button opens the iris.

■ The stop button stops the iris.

↻ The reset button resets the iris.

Max Gain (CM-6405-11-I) – Specify the maximum amount of gain (*1-3*) to apply to the image or turn it *Off*. Increasing gain increases the sensitivity of the image sensor, brightens the image, and adds details. It also increases the level of noise in the image.

Min Shutter Speed – When selecting this mode, the camera's shutter speed automatically achieves a consistent video output level. Users can select a suitable shutter speed according to the environmental luminance. The following tables list the options:

P-Iris Priority Min Shutter Speed CM-6408-11-I	
PAL	**NTSC**
1/25	1/30
1/12	1/15
1/6	1/8
1/3	1/4
1/1.5	1/2
-	1

P-Iris Priority Min Shutter Speed CM-6405-11-I					
PAL			**NTSC**		
1/425	1/100	1/6	1/500	1/100	1/8
1/300	1/75	1/3	1/350	1/90	1/4
1/215	1/50	1/1.5	1/250	1/60	1/2
1/150	1/25	-	1/180	1/30	1
1/120	1/12	-	1/120	1/15	-

4.6.1.3 Iris Priority Mode

In *Iris Priority* mode, the camera prioritizes the iris size, which remains fixed, and automatically adjusts other exposure settings to achieve a consistent exposure level.

Iris Size – The iris size is adjustable from *0* to *9* or *Full Open*. When the iris size increases, the more light reaches the camera sensor and, therefore, the faster the minimum shutter speed should be.

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

Iris Priority **Min Shutter Speed**			
PAL		**NTSC**	
1/25	1/3	1/30	1/4
1/12	1/1.5	1/15	1/2
1/6	-	1/8	1

4.6.1.4 Auto Shutter Mode

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

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

Auto Shutter **Min Shutter Speed**					
PAL			**NTSC**		
1/425	1/100	1/6	1/500	1/100	1/8
1/300	1/75	1/3	1/350	1/90	1/4
1/215	1/50	1/1.5	1/250	1/60	1/2
1/150	1/25	-	1/180	1/30	1
1/120	1/12	-	1/120	1/15	-

4.6.1.5 Shutter Priority Mode

In *Shutter Priority* mode, specify a fixed shutter speed and the camera automatically adjusts other exposure settings.

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

4.6.1.6 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.

In *Manual Mode*, users define a fixed iris size, a fixed shutter speed, and a fixed gain. A larger iris and slower shutter speed allows more light to enter the sensor, producing a brighter and more detailed image. The larger the iris size, the slower the shutter speed should be. Increasing the gain increases the sensitivity of the image sensor, which also produces a brighter and more detailed image. However, it also increases the level of noise in the image.

Iris Size Setting > *P-Iris* (CP-6405-11-I) – Manually adjust the iris size:

− The minus (-) button closes the iris.

+ The plus (+) button opens the iris.

◉ The stop button stops the iris.

↻ The reset button resets the iris.

Shutter Speed – Select the fixed shutter speed according to the environmental luminance. The following table lists the options:

Manual Mode Fixed Shutter Speeds			
PAL		NTSC	
1/32000	1/120	1/32000	1/120
1/10000	1/100	1/10000	1/100
1/3500	1/75	1/3000	1/90
1/2500	1/50	1/2000	1/60
1/1250	1/25	1/1000	1/30
1/600	1/12	1/725	1/15
1/425	1/6	1/500	1/8
1/300	1/3	1/350	1/4
1/215	1/1.5	1/250	1/2
1/150	-	1/180	1

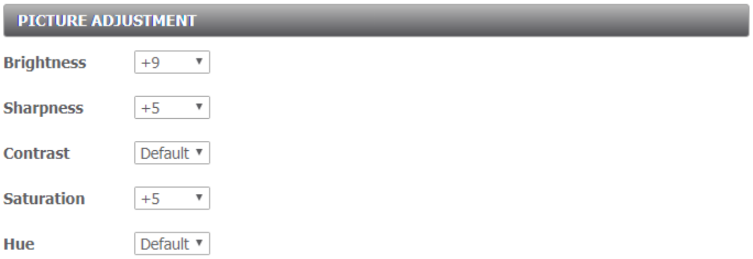
A slower shutter speed increases the amount of light entering the sensor, producing a brighter and more detailed image.

Iris Size (CP-6408-11-I) – The iris size is adjustable from *0* to *9* or *Full Open.* The higher the *Iris Size*, the lower the *Shutter Speed* should be.

Gain – Select a fixed amount of gain (*1-9*) or turn it *Off*.

4.6.2 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.



PICTURE ADJUSTMENT

Brightness	+9 ▼
Sharpness	+5 ▼
Contrast	Default ▼
Saturation	+5 ▼
Hue	Default ▼

Picture Adjustment Screen

Brightness

You can adjust the image's brightness by adjusting this parameter. Select from the range between -12 to +13. To increase video brightness, select a larger number. The default setting is *DEFAULT.* The setting is applied automatically.

Sharpness

Increasing the sharpness level can make the image look sharper, especially enhancing the object's edge. Select from the range between 0 to +15. The default setting is *DEFAULT.* The setting is applied automatically.

Contrast

Camera image contrast level is adjustable. Select from a range of -6 to +19. The default setting is *DEFAULT.* The setting is applied automatically.

Saturation

Camera image saturation level is adjustable. Select from a range of -6 to +19. The default setting is *DEFAULT.* The setting is applied automatically.

Hue

Camera image hue level is adjustable: select from a range of -12 to +13. The default setting is *DEFAULT.* The setting is applied automatically.

4.6.3 Advanced Picture Settings

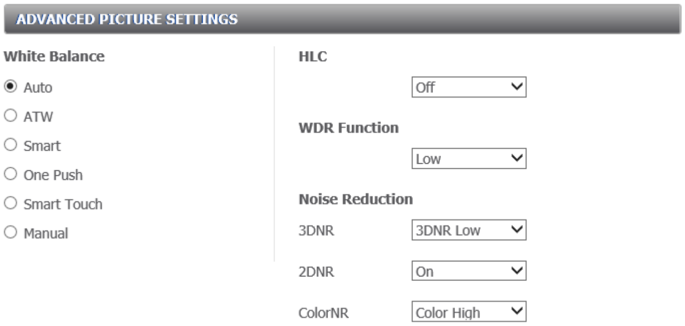
The **Advanced Picture Settings** screen is used for configuring the following settings:

White Balance

Highlight Compensation (HLC)

WDR Function

Noise Reduction Settings



ADVANCED PICTURE SETTINGS

White Balance

● Auto
○ ATW
○ Smart
○ One Push
○ Smart Touch
○ Manual

HLC: Off

WDR Function: Low

Noise Reduction

3DNR: 3DNR Low

2DNR: On

ColorNR: Color High

Advanced Picture Settings Screen
Auto White Balance Selected

4.6.3.1 White Balance

A camera needs to find a reference color temperature as a way of measuring the quality of a light source for calculating all other colors. The unit for measuring this ratio is in Kelvin (°K) degrees. You can select one of the White Balance control modes according to the operating environment. The table below shows the color temperature of some light sources for reference.

Light Sources	Color Temperature (in K°)
Cloudy Sky	6,000 to 8,000
Noon Sun and Clear Sky	6,500
Household Lighting	2,500 to 3,000
75-watt Bulb	2,820
Candle Flame	1,200 to 1,500

Select one of the following white balance modes:

- *Auto* – The Auto Balance White mode computes the white balance value output using color information from the entire screen. It is suitable for an environment with a light source color temperature in the range of approximately 2,700 ~ 7,500K. This is the default setting.
- *ATW (Auto Tracking White Balance)* – The Auto Tracking White Balance mode automatically adjusts the white balance in a scene while temperature color is changing. The ATW Mode is suitable for an environment with a light source color temperature in the range of approximately 2500 ~ 10,000K. This is the default setting.
- *Smart* – The Smart mode is suitable for environments with a single background color that is strongly saturated; for example, in a forest.
- *One Push* – When you click the ◉ button, the camera adjusts and fixes the white balance according to the scene at that moment. This mode is best for situations with minimal scene changes and continuous lighting. It is suitable for light sources with any kind of color temperature.

Note:

The white balance is fixed and does not change as the scene or the light source varies. You might have to re-adjust the white balance by clicking the ◉ button again when needed.

- *Smart Touch* – With the Smart Touch mode, you can specify the portion of the scene the camera uses as the reference for white balance. Make sure that the background color of the selected area is white. This mode is suitable for environments where the brightness level does not change.

Reference Area

You can move and resize the reference area by clicking inside the square or its borders.

- *Manual* – In this mode, you can manually specify the white balance value. You can select a number between 0 – 249 for either/both Rgain and Bgain to increase the red and/or blue luminance.

Changes to the settings immediately take effect.

4.6.3.2 Highlight Compensation (HLC)

HLC detects areas of the image overexposed by bright light sources such as headlights or spotlights and reduces image exposure only in these areas to enhance overall image quality. From the *HLC* drop-down menu, select *On* or *Off*. The default setting is *Off*. Changing the setting immediately takes effect.

4.6.3.3 WDR Function

The *WDR Function* setting applies to the camera's digital Wide Dynamic Range (dWDR), which improves the image quality and amount of detail in high contrast scenes. Such scenes combine areas with different lighting conditions, where some areas are very bright and others are dark. If this function was not used, the image either would be overexposed or too bright in bright areas and underexposed or too dark in dark areas. Digital WDR helps improve image quality by producing more detail in both the dark and bright areas of the image.

It can be set to *Off*, *Low, Mid,* or *Hi*. A higher level of WDR represents wider dynamic range, so that the IP camera can capture a greater scale of brightness. The default setting is *Low.* Changing the setting takes immediate effect.

The *WDR Function* setting operates separately from the camera's Shutter (True) WDR feature, which can be enabled or disabled by selecting the TV System on the Misc. Screen.

4.6.3.4 Noise Reduction Settings

The noise reduction function consists of three settings:

- 3DNR
- 2DNR (Default setting)
- ColorNR

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) luminance noise contains dots of varying brightness levels (black, white, and gray). It is not recommended to completely eliminate luminance noise, which can result in unnatural images. 3DNR and 2DNR settings should be configured after configuring ColorNR.

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 adjustable from *Off, 3DNR Low, 3DNR Mid,* and *3DNR High.* The setting is applied automatically.

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 *On* and *Off*. The default setting is *On*. The setting is applied automatically.

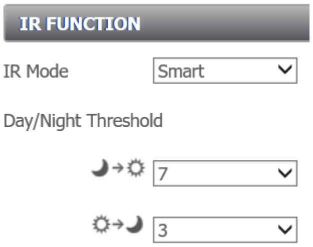
ColorNR

The *ColorNR* setting controls the noise displayed as red, green and blue dots that are visible between light and dark areas. Four settings are available: *Off, Color Low, Color Mid,* and *Color High.* The highest setting (*Color High)* maximizes the blending of the color noise with the image, effectively removing the dots, while the *Color Low* setting minimizes the blending. The *Off* setting disables this function. The default setting is *Color High.* The setting is applied automatically.

4.6.4 IR Function

The IR Function setting activates two functions:

- The IR Cut (IRC) filter for electronic day/night operation (*IR mode*)
- The IR LED illuminator for use in low-light conditions or at night



IR FUNCTION

IR Mode: Smart

Day/Night Threshold

☾→☼ 7

☼→☾ 3

IR Function Screen

IR Mode

The day/night IRC switching mechanism operates according to the ambient light level rather than activation of the IR LED mode. The *IR Mode* drop-down menu enables you to select from *Auto/Night/Day/Light Sensor/Light On/Light Off/Smart* modes. The default mode is *Light Sensor*. The setting is applied automatically.

Following is an explanation of the settings:

- *Auto* – 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.
- *Night* – Use this mode when the light level is low. The IR Cut filter is removed, allowing the camera to deliver clear images in black and white.

- *Day* – Select this mode to turn on the IR Cut filter. The IR Cut filter filters out IR light and allows the camera to deliver high quality images in color.
- *Light Sensor* – IR LEDs are turned on or off depending on the light sensor.
- *Light On* – Activates IR mode (puts camera into monochrome/Night mode). The IR LEDs are continuously illuminated.
- *Light Off* – Deactivates IR mode (puts camera into color/Day mode). The IR LEDs are continuously off.
- *Smart* – Smart mode enhances monochrome/Night mode stability and keeps the camera from switching between Day and Night modes. In this mode, when IR illumination is dominant, the camera decides when to remove the IR Cut filter. When the IR Cut filter is on (i.e. monochrome/Night mode), the IR LED illuminator also is activated. This prevents the camera from returning to color/Day mode.

Note:

When video transitions from day-to-night and night-to-day, it can appear off-color. This should be resolved within a few seconds as the level of light decreases or increases, respectively.

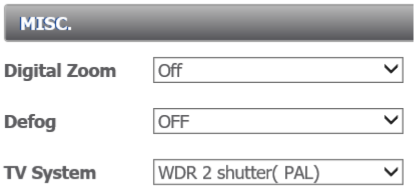
Day/Night Threshold

Set the threshold at which you want to activate the IR function. The setting is applied automatically.

- For the nighttime to daytime threshold ☾→☼, from the drop-down list, select a number between 1-9, where 1 is darker and 9 is brighter, or select *Darker* or *Brighter*. The default setting is *7*.
- For the daytime to nighttime threshold ☼→☾, from the drop-down list, select a number between 1-9, where 1 is darker and 9 is brighter, or select *Darker* or *Brighter*. The default setting is *3*.

4.6.5 Misc. Screen

The **Misc.** screen is used for enabling or disabling digital zoom and the camera's defog feature, and for specifying the TV system.



MISC.

Digital Zoom: Off

Defog: OFF

TV System: WDR 2 shutter(PAL)

Misc. Screen
WDR 2 Shutter (PAL) TV System Selected

Digital Zoom

Select the camera’s digital zoom from x2 to x10 or turn it *Off* (default). Changing the setting takes immediate effect.

Defog

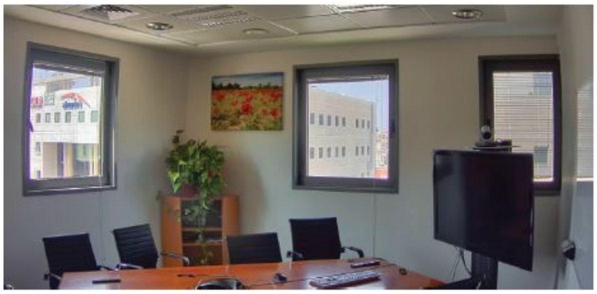
Increases image contrast and quality in rain, mist, or foggy conditions. OFF by default. When ON, areas of the original image that are already bright can lose some detail.

TV System

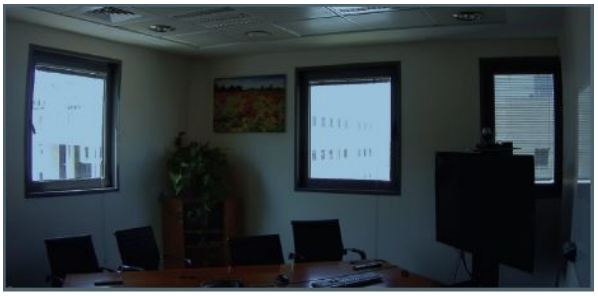
Select the camera's video output format:

- *60 fps (NTSC)*
- *50 fps (PAL)*
- *WDR 2 Shutter (NTSC)* – default setting
- *WDR 2 Shutter (PAL)*

Selecting a *WDR 2 Shutter* TV system enables True (Multi-Shutter) WDR. When is enabled, the camera combines one frame taken with a slow shutter speed with another frame taken with a fast shutter speed to create a single video frame with wider dynamic range. It uses an algorithm to determine the optimal mix of regions within the scene. Without Shutter WDR, scenes with high contrast or changing light issues would be overexposed or too bright in bright areas and underexposed or too dark in dark areas.



Shutter WDR On



Shutter WDR Off

With Shutter WDR enabled, the maximum frame rate of the camera's video output is 25/30 fps (PAL/NTSC).

Tips:

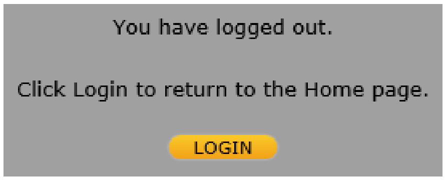
- For most lighting conditions, to achieve video with a consistent exposure level regardless of changing contrast or lighting conditions, FLIR recommends selecting a *WDR 2 Shutter* TV system.
- When the frequency of a light source around the camera (including reflected light) is closely synced with the Shutter WDR operation, a pixelization effect can appear. In these cases, FLIR recommends selecting either *60 fps NTSC* or *50 fps PAL*, also known as *linear modes*.

After changing the TV Setting, the camera automatically reboots. To view the camera's video with the new setting, refresh the page. There is no need to log in again. However, if the camera is attached to a VMS, after it reboots, you need to Initial Configuration.

The camera also supports digital WDR (dWDR), which can be enabled for all TV systems and configured on the Advanced Picture Settings screen.

4.7 Log Out

Selecting **Log out** link at the top of the camera web page closes the session.



You have logged out.

Click Login to return to the Home page.

Logout Message

To log back in, click **Login**. The Login Dialog Box opens.

5 Appendices

5.1 Technical Specifications

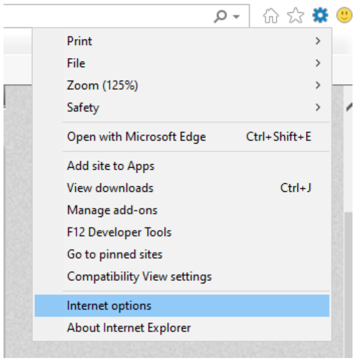
Up-to-date resources for the camera, including the camera’s specifications, are available from the camera’s product information and support pages on FLIR.com. See Accessing Product Information from the FLIR Website.

5.2 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

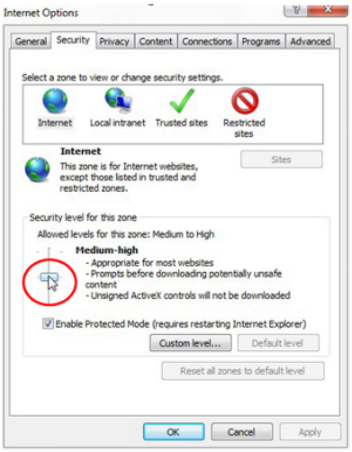
1. Start Internet Explorer (IE).
2. From the Command Bar toolbar, select **Tools** ⚙ and select *Internet Options* from the menu that appears.



Command Bar Toolbar –
Select Internet Options
(Internet Explorer 11)

3. In the **Internet Options** dialog box that appears, select the **Security** tab.
4. Select 🌐 Internet 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**.



Select a zone to view or change security settings.

Internet
This zone is for Internet websites, except those listed in trusted and restricted zones.

Security level for this zone

Allowed levels for this zone: Medium to High

Medium-high
- Appropriate for most websites
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

☑ Enable Protected Mode (requires restarting Internet Explorer)

Internet Options > Security Screen

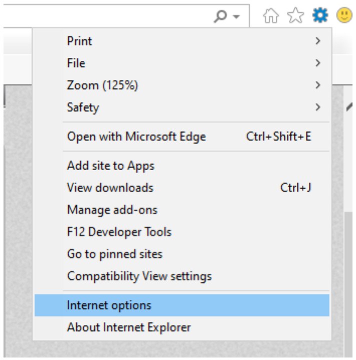
6. Close all browsers and reopen so that the settings take effect.

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.



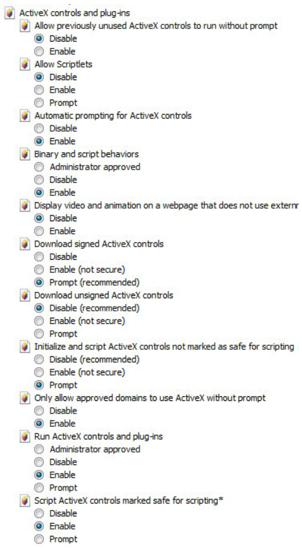
Command Bar Toolbar – Internet Options

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 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



ActiveX controls and plug-ins
- Allow previously unused ActiveX controls to run without prompt
  - ● Disable
  - ○ Enable
- Allow Scriptlets
  - ● Disable
  - ○ Enable
  - ○ Prompt
- Automatic prompting for ActiveX controls
  - ○ Disable
  - ● Enable
- Binary and script behaviors
  - ○ Administrator approved
  - ○ Disable
  - ● Enable
- Display video and animation on a webpage that does not use extern
  - ● Disable
  - ○ Enable
- Download signed ActiveX controls
  - ○ Disable
  - ○ Enable (not secure)
  - ● Prompt (recommended)
- Download unsigned ActiveX controls
  - ● Disable (recommended)
  - ○ Enable (not secure)
  - ○ Prompt
- Initialize and script ActiveX controls not marked as safe for scripting
  - ○ Disable (recommended)
  - ○ Enable (not secure)
  - ● Prompt
- Only allow approved domains to use ActiveX without prompt
  - ○ Disable
  - ● Enable
- Run ActiveX controls and plug-ins
  - ○ Administrator approved
  - ○ Disable
  - ● Enable
  - ○ Prompt
- Script ActiveX controls marked safe for scripting*
  - ○ Disable
  - ● Enable
  - ○ Prompt

Security Settings-Internet Zone Screen

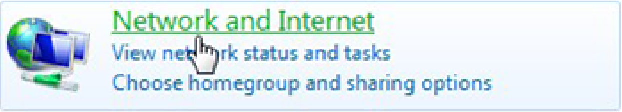
6. Click **OK** to accept the settings and close the **Security** screen.
7. Click **OK** to close the **Internet Options** screen.
8. Close the browser window and restart IE again to access the camera.

5.3 Install UPnP Components

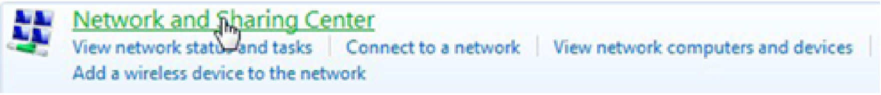
Follow the instructions below to enable UPnP so that the camera can be discovered and displayed in the *Network and Sharing Center*.

To enable UPnP discovery

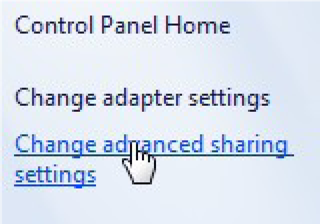
1. Click or (**Start**) and select *Control Panel*.
2. Click *Network and Internet* (Win 7, 8, 8.1, or 10).


Network and Internet
View network status and tasks
Choose homegroup and sharing options

3. Click *Network and Sharing Center* (all OSs).


Network and Sharing Center
View network status and tasks
Connect to a network
View network computers and devices
Add a wireless device to the network

4. Click *Change advanced sharing settings*.

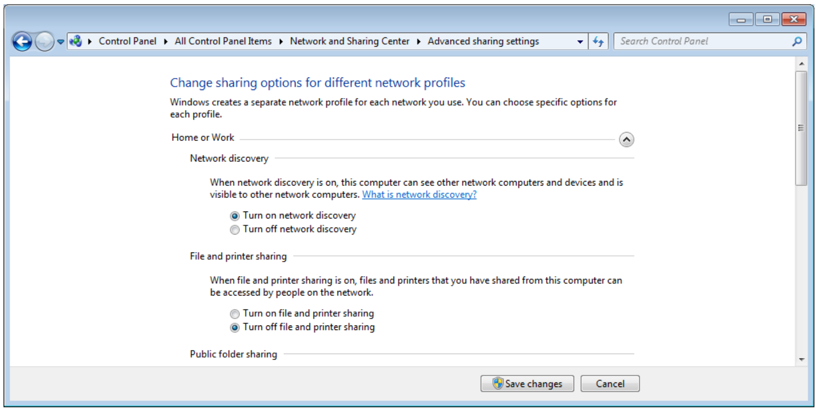


Control Panel Home

Change adapter settings

Change advanced sharing settings

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


Control Panel ▸ All Control Panel Items ▸ Network and Sharing Center ▸ Advanced sharing settings
Search Control Panel
Save changes
Cancel

Change sharing options for different network profiles

Windows creates a separate network profile for each network you use. You can choose specific options for each profile.

Home or Work

Network discovery

When network discovery is on, this computer can see other network computers and devices and is visible to other network computers. What is network discovery?

● Turn on network discovery
○ Turn off network discovery

File and printer sharing

When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

○ Turn on file and printer sharing
● Turn off file and printer sharing

Public folder sharing

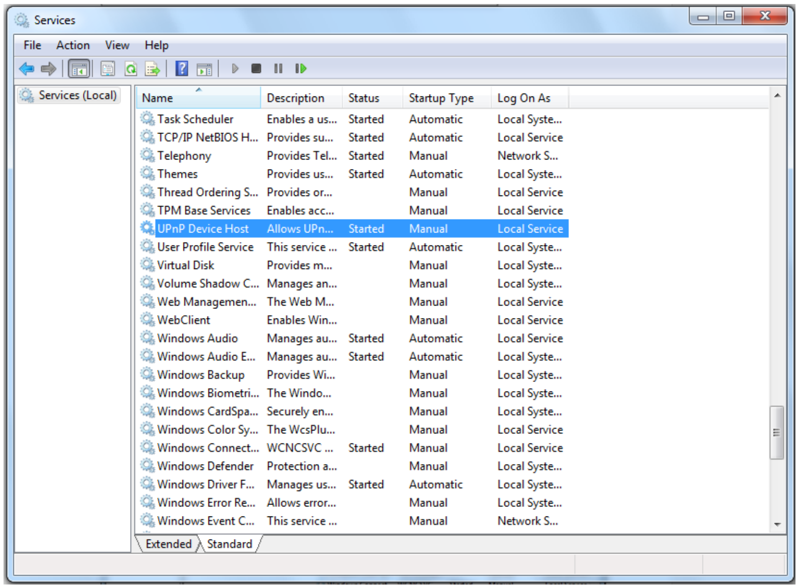
Advanced Sharing Settings Screen

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 ⊞ or ⊞ (**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.



Name	Description	Status	Startup Type	Log On As
Task Scheduler	Enables a us...	Started	Automatic	Local Syste...
TCP/IP NetBIOS H...	Provides su...	Started	Automatic	Local Service
Telephony	Provides Tel...	Started	Manual	Network S...
Themes	Provides us...	Started	Automatic	Local Syste...
Thread Ordering S...	Provides or...		Manual	Local Service
TPM Base Services	Enables acc...		Manual	Local Service
UPnP Device Host	Allows UPn...	Started	Manual	Local Service
User Profile Service	This service ...	Started	Automatic	Local Syste...
Virtual Disk	Provides m...		Manual	Local Syste...
Volume Shadow C...	Manages an...		Manual	Local Syste...
Web Managemen...	The Web M...		Manual	Local Service
WebClient	Enables Win...		Manual	Local Service
Windows Audio	Manages au...	Started	Automatic	Local Service
Windows Audio E...	Manages au...	Started	Automatic	Local Syste...
Windows Backup	Provides Wi...		Manual	Local Syste...
Windows Biometri...	The Windo...		Manual	Local Syste...
Windows CardSpa...	Securely en...		Manual	Local Syste...
Windows Color Sy...	The WcsPlu...		Manual	Local Service
Windows Connect...	WCNCSVC ...	Started	Manual	Local Service
Windows Defender	Protection a...		Manual	Local Syste...
Windows Driver F...	Manages us...	Started	Automatic	Local Syste...
Windows Error Re...	Allows error...		Manual	Local Syste...
Windows Event C...	This service ...		Manual	Network S...

Services Manager Dialog Box

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.

5.4 Installing and Deleting the Web Player

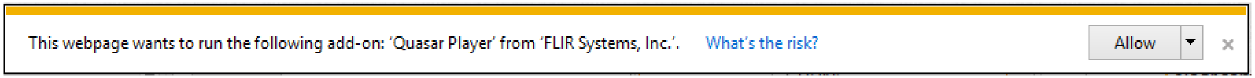
The Quasar Player enables you to view the camera's **Live View** window.

After logging into the unit, if the Quasar Player has been loaded previously, the **Live View** window opens.

If this the first time you are accessing the camera's web page or you have uninstalled an previous Quasar Player installation, depending on your Windows user permissions and Internet Explorer > Internet Options settings, either a **User Account Control** window or an information bar appears. If a **User Account Control** window appears and your Windows user does not have permissions to install programs, contact your PC administrator.

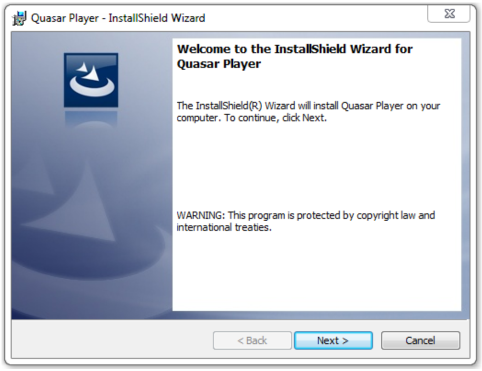
Users who have previously installed DVPlayer or DCViewer on the PC should first delete the existing player file from the PC before accessing the camera and installing the Quasar Player.

To install the Quasar Player


This webpage wants to run the following add-on: 'Quasar Player' from 'FLIR Systems, Inc.'.

"Run Quasar Player" Information Bar

1. On the Internet Explorer information bar, click **Allow**. The Quasar Player InstallShield Wizard opens.



Quasar Player - InstallShield Wizard

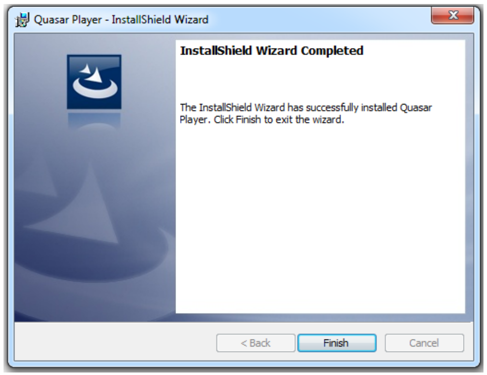
Welcome to the InstallShield Wizard for Quasar Player

The InstallShield(R) Wizard will install Quasar Player on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

Quasar Player InstallShield Wizard

2. Click **Next**. The player is installed.
3. When the next screen opens, click **Finish**. The installation is completed. **Quasar Player** is displayed in the list of installed programs.



Quasar Player - InstallShield Wizard

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed Quasar Player. Click Finish to exit the wizard.

Quasar Player Installation Completed

To delete an existing DVPlayer or DCViewer file

1. Click ⊞ or ⊞ (**Start**) and open the Control Panel.
2. In the Control Panel, click *Uninstall a program* (Win 7, 8, or 8.1) or *Programs and Features* (Win 10).
3. From the list of installed programs, select **DVPlayer** or **DCViewer**.
4. Do one of the following:
   - On the banner bar, click *Uninstall* (Win 7, 8, or 8.1).
   - Right-click the program, click *Uninstall/Change* (Win 10).
5. When prompted to confirm the Uninstall, click **Yes**.
6. After deleting the previous player file, you must clear your computer's cache memory.

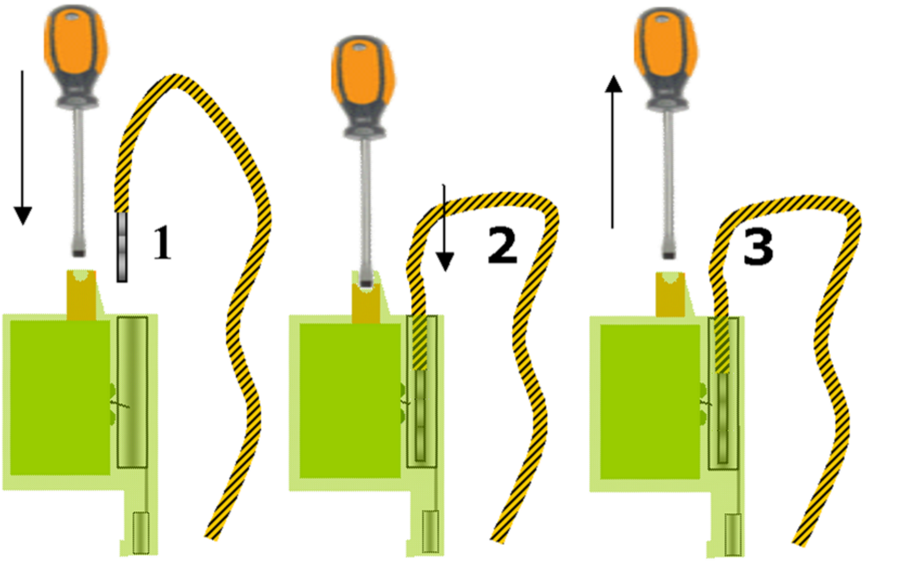
5.5 Connecting Leads to a Spring Clamp Terminal Block

The unit is delivered with 2-pin, 4-pin, and 9-pin terminal block connectors. The connectors enable you to connect wires for either the relay output or alarm input and then connect them to the unit.

To connect a wire to the spring clamp terminal block

1. Strip the insulation form 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.



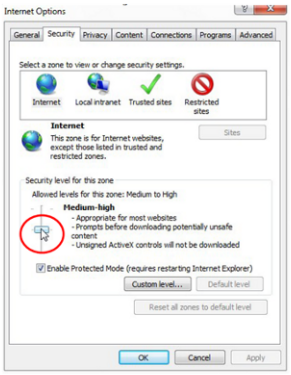
Connecting a Wire to a Terminal Block

5.6 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.



Select a zone to view or change security settings.

Internet
This zone is for Internet websites, except those listed in trusted and restricted zones.

Security level for this zone

Allowed levels for this zone: Medium to High

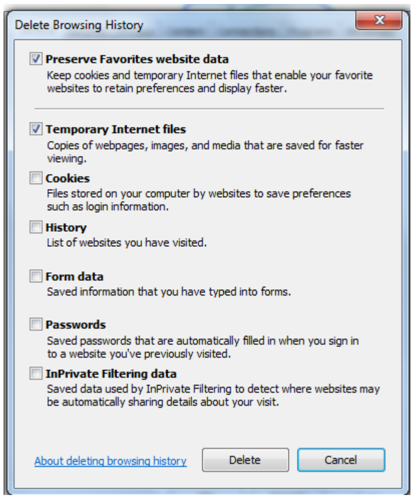
Medium-high
- Appropriate for most websites
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

☑ Enable Protected Mode (requires restarting Internet Explorer)

Tools >
Internet Options Dialog Box

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

3. In the **Delete Browsing History** dialog box that appears, select *Temporary Internet files* (Win 7, 8 or 8.1) or *Temporary Internet files and website files* (Win 10). Uncheck *Cookies* and *History* (Win 7, 8 or 8.1) or *Cookies and website data* (Win 10) to keep this data. Click **Delete**.



Delete Browsing History

☑ **Preserve Favorites website data**
Keep cookies and temporary Internet files that enable your favorite websites to retain preferences and display faster.

☑ **Temporary Internet files**
Copies of webpages, images, and media that are saved for faster viewing.

□ **Cookies**
Files stored on your computer by websites to save preferences such as login information.

□ **History**
List of websites you have visited.

□ **Form data**
Saved information that you have typed into forms.

□ **Passwords**
Saved passwords that are automatically filled in when you sign in to a website you've previously visited.

□ **InPrivate Filtering data**
Saved data used by InPrivate Filtering to detect where websites may be automatically sharing details about your visit.

Delete Browsing History Dialog Box

5.7 Troubleshooting

This section provides useful information and remedies for common situations.

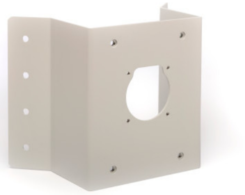
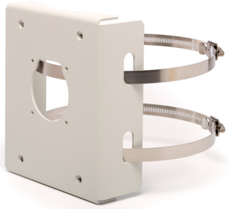
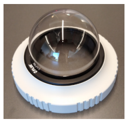
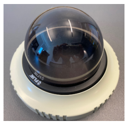
Problem	Possible Solution
No network connection	**Hardware issues:** • Check that the network is working and the unit is powered on. • Check that the network (Ethernet) cable is properly attached to the unit. • Confirm that the network cables are not damaged and replace if necessary. **IP Address issues:** • Change the default IP address/addresses of the unit. • From the PC running the web browser, ping the unit IP address and confirm that it can be reached. • Confirm that the network settings/firewalls are set according to the requirements. • The camera might be located on a different subnet. Contact your IT administrator to get the IP address of the camera.
How do I find IP address of my unit?	• Check the network DHCP server IP address assignments and lease. • Alternatively, move the camera to an isolated network and make sure camera gets DHCP address and is accessible. Move the camera back to the network and test it. If you still have issues, reset the camera physically by pressing the reset button on the rear of the camera and test the camera again. This will ensure the camera releases the IP address.

Problem	Possible Solution
The IP address responds to a ping on the network from the workstation but does not show in the Discovery List	• Disconnect the unit's Ethernet 10/100 port or turn the power to unit off, and then ping the IP address again. If the IP address responds, there is another device using the IP address. Consult with your network administrator to resolve the conflict. • Check the network port and ensure that it is working OK. • Ensure that the switch ports provide the necessary power.
The unit IP address is in use by another computer (collision)	• Check the DHCP settings. Obtain a new IP address using DHCP. Ensure this is a unique IP address. • Alternatively, change the unit IP address after connecting to it directly (not through the system network).
Cannot log in to the camera	• Check the login user ID of the user or admin. • Check the login password of the user or admin.
No video image displayed on the camera's web page	• Reset the browser security settings to the default value. • Check that the correct port was configured. The default port is 554.
Bad output video quality	• Check that the network cable is connected securely. • Check that the camera settings are correct on the camera and in the unit. • Check that the camera lens is clean and unobstructed. • Check that the cable length is within specification.
Streaming video image is hanging (stopped)	• Confirm the unit's video streaming settings. • Refresh your browser screen (F5). • Check that the bandwidth and bit rate settings of the network are set properly. • Check that other processes and applications are not causing undue latency. • Check that the firewall analysis or blocking is not interfering with the video stream and supports the required ports and communication protocols.
Bluish picture in an indoor scene (possibly mixing indoor and outdoor lighting)	Adjust the White balance configuration to *Auto*. If the lighting in the scene is fixed, manually adjust the White balance to an acceptable image.
Reddish picture and incorrect colors in the image	Check the PoE power supply and associated network cables. Connect directly to the PoE and compare the images. If the problem persists, contact support.
IR LEDs do not function	The cameras have a circuit protection mechanism that is activated if the cover is removed while the IR LEDs are on.

Problem	Possible Solution
	• Re-attach the cover (making sure that the IR contacts are in place). • Make sure that the cover is closed properly. • Power cycle the camera.

5.8 Accessories

The following mounting accessories are available from FLIR for installing your CM-640x camera. For more information, contact your FLIR sales representative or visit www.FLIR.com/security to request details on where to get the accessory.

Part number/ item code	Description and notes	Images (not to scale)
CM-RCSD-G4	Recessed mount kit for CM-640x mini-dome cameras: • Supplied with ceiling sticker template and trim ring • Supports conduit connections	*Mounted with camera*
421-0066-00 DH-CRNR-00	Corner mount kit	
421-0067-00 DH-POLE-00	Pole mount kit	
CM-SNSHLD-G4	Sun shield for CM-640x mini-dome cameras	
CM-CLEAR-64-11	Clear bubble for CM-640x mini-dome cameras	
CM-SMOKE-64-11	Smoked bubble for CM-640x mini-dome cameras	

This document does not contain any export-controlled information.

Part number/ item code	Description and notes	Images (not to scale)
~~421-0068-00~~ ~~DH-PDST-00~~	Pendant mount shroud kit *Currently not being shipped. For latest availability information, contact FLIR Support.*	
~~421-0069-00~~ ~~DH-PDST-01~~	Pendant mount kit *Currently not being shipped. For latest availability information, contact FLIR Support.*	

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

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

Support:
https://www.flir.com/support/
product.enterprise.support@flir.com

Document:
CM-640x Installation and User Guide
Revision: 100
Date: December 2020