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.
# Table of Contents

1. Document Scope and Purpose ................................................................. 1
2. Introduction ............................................................................................... 7
   2.1 Features ................................................................................................. 8
   2.2 Package Contents ................................................................................ 9
3. Hardware Description ............................................................................. 11
   3.1 Camera Dimensions ........................................................................... 11
   3.2 Internal Connectors ............................................................................ 12
   3.3 Cable Connectors ............................................................................... 13
      3.3.1 Waterproofing the Cable Connectors ............................................. 14
4. System Requirements ........................................................................... 17
5. Installation ............................................................................................... 19
   5.1 Pre-Installation Checklist ................................................................... 19
   5.2 Indoor Installation .............................................................................. 19
   5.3 Outdoor Installation ........................................................................... 20
   5.4 Powering the Camera ......................................................................... 20
   5.5 Connecting the Camera to the Network ............................................. 21
   5.6 Mounting the Camera ........................................................................ 22
   5.7 Adjusting and Framing-Up the Camera View ..................................... 24
6. Using DNA to Access the Camera ........................................................... 25
7. Configuring the Unit’s Initial IP Address ............................................... 27
8. Configuring Communication Settings .................................................... 31
9. Configuration and Operation ................................................................... 37
   9.1 Browser-Based Viewer Introduction .................................................. 37
   9.2 Live View .............................................................................................. 39
   9.3 System Tab ........................................................................................... 42
      9.3.1 System ............................................................................................ 43
      9.3.2 Security .......................................................................................... 45
      9.3.3 Network .......................................................................................... 55
      9.3.4 Events Setup .................................................................................. 64
      9.3.5 Edge Recording ............................................................................. 76
      9.3.6 Motion Detection .......................................................................... 82
      9.3.7 Schedule ....................................................................................... 85
      9.3.8 File Location .................................................................................. 86
      9.3.9 Maintenance .................................................................................. 87
      9.3.10 Import/Export ............................................................................. 94
# Table of Contents

- **9.4 Streaming Tab** .............................................................................................................................. 95
  - 9.4.1 Video Format .......................................................................................................................... 96
  - 9.4.2 Video Compression ............................................................................................................... 104
  - 9.4.3 Video OCX Protocol ............................................................................................................. 105
  - 9.4.4 Video Frame Rate .................................................................................................................. 106
  - 9.4.5 Video Mask ........................................................................................................................... 107
  - 9.4.6 Audio .................................................................................................................................... 108

- **9.5 Camera Tab** .................................................................................................................................... 109
  - 9.5.1 Exposure Screen .................................................................................................................... 110
  - 9.5.2 Picture Adjustment .................................................................................................................. 112
  - 9.5.3 Advanced Picture Settings .................................................................................................... 113
  - 9.5.4 IR Function ........................................................................................................................... 117
  - 9.5.5 Misc. Screen ........................................................................................................................... 118

- **9.6 Logout** .......................................................................................................................................... 119

- **10. Appendices** ................................................................................................................................. 121
  - 10.1 Technical Specifications ......................................................................................................... 122
  - 10.2 Internet Security Settings on Internet Explorer ....................................................................... 126
  - 10.3 Installing UPnP Settings on Internet Explorer ........................................................................ 128
  - 10.4 Deleting Temporary Internet Files on Internet Explorer .......................................................... 131
  - 10.5 Installing and Deleting the Web Player ...................................................................................... 132
  - 10.6 Network Settings ...................................................................................................................... 134
  - 10.7 Troubleshooting ....................................................................................................................... 135
  - 10.8 Acronyms and Abbreviations ................................................................................................. 137
  - 10.9 Mounting Accessories .............................................................................................................. 138
1 Document Scope and Purpose

The purpose of this document is to provide instructions and installation procedures for physically connecting the CM-6212 unit. After completing the physical installation, additional setup and configurations are required before video analysis and detection can commence.

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

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

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

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

Disclaimer

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

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

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

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

Avis de non-responsabilité

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

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

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

Les spécifications et informations contenues dans ce guide sont sujettes à modification sans préavis.
### Document Scope and Purpose

<table>
<thead>
<tr>
<th><strong>Warning</strong></th>
<th><strong>Avertissement</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Warning</strong> is a precautionary message that indicates a procedure or condition where there are potential hazards of personal injury or death.</td>
<td></td>
</tr>
<tr>
<td><strong>Avertissement</strong> est un message préventif indiquant qu'une procédure ou condition présente un risque potentiel de blessure ou de mort.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Caution</strong></th>
<th><strong>Attention</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Caution</strong> 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.</td>
<td></td>
</tr>
<tr>
<td><strong>Attention</strong> 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.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Note</strong></th>
<th><strong>Remarque</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong> is useful information to prevent problems, help with successful installation, or to provide additional understanding of the products and installation.</td>
<td></td>
</tr>
<tr>
<td><strong>Remarque</strong> est une information utile permettant d'éviter certains problèmes, d'effectuer une installation correcte ou de mieux comprendre les produits et l'installation.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Tip</strong></th>
<th><strong>Conseil</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tip</strong> is information and best practices that are useful or provide some benefit for installation and use of FLIR products.</td>
<td></td>
</tr>
<tr>
<td><strong>Conseil</strong> correspond à une information et aux bonnes pratiques utiles ou apportant un avantage supplémentaire pour l'installation et l'utilisation des produits FLIR.</td>
<td></td>
</tr>
</tbody>
</table>
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:

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

Attention:

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

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

Caution:

To avoid damage from overheating or unit failure, assure that there is sufficient temperature regulation to support the unit’s requirements (cooling/heating). Operating temperature should be kept in the range -10°C to 50°C (14° to 122°F), with no more than 90% non-condensing humidity.

Attention:

Afin d'éviter tout dommage dû à une surchauffe ou toute panne de l'unité, assurez-vous que la régulation de température est suffisante pour répondre aux exigences de l'unité (refroidissement/chauffage). La température de fonctionnement doit être maintenue dans la plage -10°C à 50°C/14° à 122°F), sans condensation d'humidité supérieur à 90%.

Site Preparation

There are several requirements that should be properly addressed prior to installation at the site. The following specifications are requirements for proper installation and operation of the unit:

- Ambient Environment Conditions: Avoid positioning the unit near heaters or heating system outputs. Avoid exposure to direct sunlight. Use proper maintenance to ensure that the unit is free from dust, dirt, smoke, particles, chemicals, smoke, water or water condensation, and exposure to EMI.
- Accessibility: The location used should allow easy access to unit connections and cables.
- Safety: Cables and electrical cords should be routed in a manner that prevents safety hazards, such as from tripping, wire fraying, overheating, etc. Ensure that nothing rests on the unit’s cables or power cords.
- Ample Air Circulation: Leave enough space around the unit to allow free air circulation.
- Cabling Considerations: Units should be placed in locations that are optimal for the type of video cabling used between the unit and the cameras and external devices. Using a cable longer than
the manufacturer’s specifications for optimal video signal may result in degradation of color and video parameters.

- Physical Security: The unit provides threat detection for physical security systems. In order to ensure that the unit cannot be disabled or tampered with, the system should be installed with security measures regarding physical access by trusted and un-trusted parties.

- Network Security: The unit transmits over IP to security personnel for video surveillance. Proper network security measures should be in place to assure networks remain operating and free from malicious interference. Install the unit on the backbone of a trusted network.

- Electrostatic Safeguards: The unit and other equipment connected to it (relay outputs, alarm inputs, racks, carpeting, etc.) shall be properly grounded to prevent electrostatic discharge.

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

The FLIR Quasar Gen II CM-6212-H1-I camera is an indoor/outdoor, vandal-proof, IP hemispheric camera. The camera can support:

- One 12MP H.264 stream at 20 fps
- One 12MP H.264 stream at 15 fps and one Full HD 1080p H.264/MJPEG stream at 12/15 fps (PAL/NTSC)
- One 12MP H.264 stream at 15 fps and two HD 720p H.264/MJPEG streams at 12/15 fps (PAL/NTSC)
- One 12MP H.264 stream at 15 fps, two HD 720p H.264/MJPEG streams at 12/15 fps (PAL/NTSC), and one D1 H.264/MJPEG stream at 12/15 fps (PAL/NTSC)

The camera includes a 1/1.7" Sony Progressive CMOS sensor and features an F2.4, hemispheric lens with a 1.29mm focal length and 360° Field of View (FOV) at full resolution. It provides real-time, quad-stream compression using MJPEG and H.264 baseline, main and high profiles. It also supports software dewarping, which enables the highest video resolutions.

The camera is ideal for operation in low-light environments, as it features a Day/Night cut-off filter (ICR), infrared IR illuminator, and 2D/3D/color noise reduction.

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

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

- F2.4, 1.29mm panoramic lens
- 1/1.7" Progressive scan CMOS sensor
- 12 Megapixels

- Supports software dewarping
- Supports up to four video streams
- Digital PTZ

- Low-lux mode
- Electronic day/night (ICR)
- Infrared LED illuminator

- WDR
- 2D/3D/color noise reduction
- Backlight compensation

- Built-in web application/ web server
- HTTP streaming MJPEG
- H.264 and MJPEG compression

- Two-way audio
- Alarm input-driven events
- Relay output actions on alarm

- Edge motion detection
- Motion detection with Region of Interest (ROI) masking
- Historical motion detection levels detected/recorded at frame levels

- Detection event-driven alarms
- Tampering detection and notification
- Dual HTTP notification server support (up to two servers)

- FTP upload
  (up to two locations)
- Upload alarm images to FTP
- Send images on alarm to e-mail

- E-mail SMTP alarm notification
  (up to two e-mails)
- 128GB microSDXC (Class 10) recording support
- Record snapshots to microSDXC card on alarm

- Sequential snapshot numbering
- SNMP v1/v2/v3 and SNMP traps
- Privacy masks

- ONVIF support
- RTSP support
- Per-user permissions

- Security IP restricted access allow/deny list
- Multiple users
- Group permissions

- UPnP support
- Vandal-proof IP66 enclosure
- Supports PoE/12VDC

- Includes heater
2.2 Package Contents

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

<table>
<thead>
<tr>
<th>Hemispheric camera</th>
<th>(Torx wrench)</th>
<th>Power Terminal Block</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-Tapping Screw (x3)</td>
<td>Plastic Anchor (x3)</td>
<td>CD (Bundled software and documentation)</td>
</tr>
<tr>
<td>Quick Installation Guide</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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.

**Related Documentation**
- CM-6212-H1-I Mini Hemispheric Camera Quick Installation Guide
- DNA 2.1 User Manual
3 Hardware Description

This chapter provides information about the camera hardware for reference before installation. The connectors included on the camera’s system cable are described.

- Camera Dimensions
- Internal Connectors
- Cable Connectors

3.1 Camera Dimensions

Following are the CM-6212 camera's dimensions.

![Side View](image1)

![Top View](image2)
3.2 Internal Connectors

The camera housing includes a microSD card drive, which supports a 128GB microSDXC card (Class 10). It also includes a Reset button for easily resetting the camera. The button enables you to save configured settings and to restore factory defaults, including network settings.

Note:
It is not recommended to record with the microSD card for 24/7 continuously.

To perform a hard reset to full factory defaults using the Reset button

1. Insert a pointed object into the Reset button.
2. Press the button for 30 seconds. Both LEDs on the RJ45 connector are extinguished. After one second, the green network LED flashes once and then remains lighted. The yellow activity LED flashes as soon as it detects network activity. The unit returns to full factory defaults.

Note:
Desiccants are included inside the camera housing and must be replaced every time the housing is opened. After desiccants are replaced, reconnect the front housing to the camera as soon as possible. Otherwise, the desiccant will become damp and cannot be used. For instructions on removing the desiccant, refer to the Desiccant User Guide.
3.3 Cable Connectors

The camera is shipped with an Ethernet cable for network and Power over Ethernet (PoE) connection and a system cable for ground, power, I/O, and audio connections. The figure below shows the various connectors included with the camera. The connectors, pin numbers and signal definitions are listed below.

![CM-6212 Camera Input/Output Connections](image_url)

<table>
<thead>
<tr>
<th>No.</th>
<th>Cable</th>
<th>Pin</th>
<th>Definition</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Audio I/O</td>
<td>Pink</td>
<td>Audio In</td>
<td>Two-way audio transmission</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Green</td>
<td>Audio Out</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Power (12VDC)</td>
<td>Black</td>
<td>DC 12V -</td>
<td>Power connection</td>
</tr>
<tr>
<td></td>
<td>(2-pin Terminal Block)</td>
<td>Red</td>
<td>DC 12V +</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Alarm I/O</td>
<td>1</td>
<td>Alarm In -</td>
<td>Alarm connection</td>
</tr>
<tr>
<td></td>
<td>(4-pin Terminal Block)</td>
<td>2</td>
<td>Alarm In +</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>Alarm Out -</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>Alarm Out +</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>GND</td>
<td>-</td>
<td>GND</td>
<td>Ground connection</td>
</tr>
<tr>
<td>5</td>
<td>Ethernet Cable</td>
<td>-</td>
<td>RJ45 connector with LEDs for network and PoE connections.</td>
<td></td>
</tr>
</tbody>
</table>

The alarm input and output connectors are shown below.

<table>
<thead>
<tr>
<th>Pin No.</th>
<th>Designation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Alarm In (-)</td>
</tr>
<tr>
<td>2</td>
<td>Alarm In (+)</td>
</tr>
<tr>
<td>3</td>
<td>Alarm Out (-)</td>
</tr>
<tr>
<td>4</td>
<td>Alarm Out (+)</td>
</tr>
</tbody>
</table>
3.3.1 Waterproofing the Cable Connectors

Follow the instructions below to waterproof the connectors for the different types of cables included in the system cable. The cables are shown below.

To waterproof the system cable

1. Connect all the required devices to the system cable. See figure above.
2. Coat the joints with silicone gel. There should be no gap between the connectors and the cables. For alarm I/O connector and power connector, make sure the side with wires attached is also sealed with silicone gel.
3. Seal the end of the rubber coating of the system cable as indicated in the figure below. Use enough silicone gel to fill in the hose and wrap around each wire in order to properly waterproof the cable.

To waterproof the RJ45 cable

1. Plug the Ethernet cable to the connector of the RJ45 cable.
2. Coat the joint with silicone gel. Make sure there is no gap between the Ethernet cable and the connector in order to properly waterproof the cable.
To waterproof the IP66-Rated RJ45 cable

1. Remove the supplied connector from the IP66-rated RJ45 plug.

2. Loosen the thread-lock sealing nut on the IP66-rated RJ45 plug.

3. Thread the Ethernet cable through the thread-lock sealing nut and the IP66-rated RJ45 plug. If the Ethernet cable is already attached to a connector, remove it first.

4. Carefully remove a section of rubber coating from the end of the Ethernet cable to reveal the wires.
5. Insert the wires into the correct pins of the connector.
6. Plug the Ethernet cable into the connector of the IP66-rated RJ45 cable.
7. Fasten the RJ45 plug to the connector of the IP66-rated RJ45 cable.
8. Tighten the thread-lock sealing nut to the plug.
## 4 System Requirements

<table>
<thead>
<tr>
<th>Item</th>
<th>Minimum System Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Computer</td>
<td>Minimum: Intel® Core™ i5-2430M @ 2.4 GHz, 4GB RAM</td>
</tr>
<tr>
<td></td>
<td>Recommended: Intel® Core™ i7-870 @ 2.93 GHz, 8GB RAM</td>
</tr>
<tr>
<td>Operating System</td>
<td>Windows 7, 8, and 8.1 (all 64-bit versions)</td>
</tr>
<tr>
<td>Web Browser</td>
<td>Microsoft Internet Explorer 10 and above (32-bit version)</td>
</tr>
<tr>
<td>Network Card</td>
<td>10/100/1000 Mbps</td>
</tr>
<tr>
<td>Viewer</td>
<td>ActiveX control plug-in for Internet Explorer</td>
</tr>
</tbody>
</table>
5 Installation

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

- Pre-Installation Checklist
- Indoor Installation
- Outdoor Installation
- Powering the Camera
- Connecting the Camera to the Network
- Mounting the Camera
- Adjusting and Framing-Up the Camera View

5.1 Pre-Installation Checklist

Before installing the unit, make sure that:

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

Caution:
To avoid damage from overheating or unit failure, assure that there is sufficient temperature regulation to support the unit’s requirements (cooling/heating). Operating temperature should be kept in the range -10°C to 50°C (14°F to 122°F), with no more than 90% non-condensing humidity.

Attention:
Afin d'éviter tout dommage dû à une surchauffe ou toute panne de l'unité, assurez-vous que la régulation de température est suffisante pour répondre aux exigences de l'unité (refroidissement/chauffage). La température de fonctionnement doit être maintenue dans la plage (-10°C à 50°C/14°F à 122°F), sans condensation d'humidité supérieure à 90%.

5.2 Indoor Installation

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.
5.3 Outdoor Installation

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

- For outside wiring installation, always use weatherproof equipment, such as boxes, receptacles, connectors, etc.
- For electrical wiring, use the properly rated sheathed cables for conditions to which the cable will be exposed (for example, moisture, heat, UV, physical requirements, etc.).
- Plan ahead to determine where to install infrastructure weatherproof equipment. Whenever possible, ground components to an outdoor ground.
- Use best security practices to design and maintain secured camera access, communications infrastructure, tamper-proof outdoor boxes, etc.
- All electrical work must be performed in accordance with local regulatory requirements.

5.4 Powering the Camera

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

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

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

Caution:

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

Attention:

1. Si la caméra est connectée à un réseau PoE, notez que la puissance nominale de l'alimentation PoE est 48VDC, 0.2A.
2. Si la caméra est installée pour une utilisation extérieure, l'alimentation PoE doit être installé avec l'étanchéisation appropriée.
4. Ce produit doit être installé par un technicien qualifié. L'installation doit se conformer à tous les codes locaux.
5.5 Connecting the Camera to the Network

A Cat 5 Ethernet cable is recommended for network connection. To ensure transmission quality, cable length should not exceed 100 meters (328 feet). Connect one end of the Ethernet cable to the RJ45 connector of the system cable. Plug the other end of the cable into the network switch or PC. Check the status of the link and the activity LEDs. If the LEDs are unlit, check the LAN connection.

<table>
<thead>
<tr>
<th>A steady green link LED indicates good network connection.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The yellow activity LED flashes to indicate network activity.</td>
</tr>
</tbody>
</table>

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

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

To eliminate IR reflection
1. Clean the bubble from dirt and finger prints.
2. Make sure the bubble has no scratches.
3. Avoid aiming the IR where there are nearby objects closer than the scene of interest which might reflect back into the lens.

To mount the camera
1. Do one of the following:
   - For drilled wall or ceiling mounting:
     a. Using the supplied template, mark with a pointed pencil the mounting surface through the plate holes where the four screw holes need to be drilled.

     ![Drill Template](image)

     **Note:**
     Before marking and drilling the holes, ensure that the base plate alignment is oriented correctly so that the required camera field of view can be achieved when the system is assembled.

     b. In the marked locations, drill each hole using a drill bit of a slightly smaller diameter than the supplied screw anchors (molly-plug anchor). You want to achieve a snug insertion so that the plug expansion holds firm after the screws are screwed in.

     c. Fully insert the supplied anchors into drilled holes. You may need to tap them flush with the wall using a hammer.
• For installing on a 4S recessed electrical box:
  a. Have a qualified installer (check your local electrical codes) rough-in the 4S recessed electrical box and run the wires and power (if not PoE) through the wall/conduits to the box location.
  b. Ensure that the box is sufficiently sturdy (attach to the wall stud, ceiling joist, or reinforced surface as needed) to securely hold the weight of the camera.

• For bracket, pole and pendant installations:
  a. Feed the system cable through the mounting accessory.

  
  Note:
  The power cable is not required if using PoE.

  Tip:
  Even if you are not using alarm inputs and audio input/output at the time of installation, you may want to consider pre-wiring these connections for future use.
  Use shims for shoring up mounts on uneven surfaces.
  b. Thread the wires through the base plate and screw it to the pre-drilled wall, ceiling, CM Series Recessed Mount, CM Series Corner Mount, or 4S electrical box. Check that the installation is not flimsy, will not wobble, and is flush with the mounting surface.
  c. Plug the Cat 5 cable into the camera’s Ethernet port and, if needed, plug the power terminal block into the power terminals.
  d. If applicable, wire the Alarm In, Alarm Out, Audio In, and Audio Out terminal blocks to external devices. See Cable Connectors.
  e. If needed, connect the other end of the Cat 5 cable to the network and turn on the power from the power supply.

  Note:
  1. Do not reassemble the camera’s inner cover and hemispheric cover until after hardware configurations are made.
  2. Remember to replace desiccants every time the cover is opened.
5.7 Adjusting and Framing-Up the Camera View

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

To adjust and frame-up the camera view

1. In the DNA application, click DNA.
2. In the Discovery list, click to select the camera.
3. Right-click the context menu and select Web, or enter the camera’s IP address in your browser’s URL address bar.
4. When the browser connects to the camera and prompts for login, do the following:
   a) Log in using the default user name Admin and password 1234. If the password has previously been changed, use the new password.

   ![Note]
   
   Both the user name and password are case sensitive.

   b) Allow the ActiveX to download and choose to install the Quasar Web Player.
5. Replace the cover and tighten the screw.
6 Using DNA to Access the Camera

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

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

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

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

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

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

Note:
For detailed guidelines about DNA and its usage, refer to the DNA 2.1 User Manual, which is included in the CD provided with the camera.
7 Configuring the Unit’s Initial IP Address

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

- If the camera is located on a network that uses a DHCP server, or is managed by FLIR's Horizon or Meridian VMS and is configured as a DHCP server, configure the camera with *DHCP-enabled*. Horizon or Meridian automatically assigns the camera an IP address.

- If the camera is located on a network that does not use a DHCP server, or is managed by FLIR’s Latitude VMS, manually enter its IP address in the DNA utility.

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

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

1. Insert the CD included in the package in your computer’s disk drive.

2. Run the `dna.exe` file by clicking the icon. The DNA application opens and the device is displayed in the window.

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

**Note:**

The camera's default IP Address and the subnet mask IP Address are automatically supplied by the DHCP server.

4. In the dialog box that is displayed, enter values for the IP Address, Gateway and Netmask.
5. Click **Update** and wait for ✔ OK status to be displayed.

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

7. Enter the default User Name (**Admin**) and Password (**1234**).

   **Note:**
   The user name and password are case-sensitive.

8. Click on the unit in DNA’s Discover List. The CM-6212 **Login** window opens.

9. Click **Login**. The camera’s web interface opens.

10. Follow the instructions in the **Appendix** for installing the Player. After installing the Player, the **Live View** is displayed.

11. Disconnect the Ethernet cable. The camera is ready for deployment (mounting) in a site installation.
**Note:**

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

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

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

1. Insert the CD included in the package in your computer’s disk drive.
2. Run the dna.exe file by clicking the icon. The DNA application opens and the device is displayed in the DNA Discovery window. See Figure: DNA Discovery Window.
3. Select the unit by right-clicking it. The DNA - Assign IP window is displayed.
4. Uncheck *Use DHCP*.
5. Enter the unit’s default IP address (192.168.0.250), Subnet mask, and Gateway IP address in the respective field.
6. Click *Update*. The unit reboots with the new settings.
7. Click on the unit in DNA’s Discover List. The camera’s Login window opens. See Figure: Login Window.
8. Enter the default User Name (Admin) and Password (1234).

**Note:**
The user name and password are case-sensitive.

9. Click **Login**. The camera’s web interface opens. See Figure: [Live View](#).
8 Configuring Communication Settings

To configure communication settings on the camera

1. Connect the camera to the network on the same VLAN/LAN as the workstation.

2. If the network supports the default, open the DNA utility by running dna.exe which can be found in the DNA utility folder in the supplied CD, or click the DNA icon.

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

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

5. To continue, click Allow Access. Latitude users should consult the Latitude Installation Instructions on disabling the Windows Firewall.

6. Click Assign IP. All the discovered IP devices will be listed in the page, as shown in the figure below. The camera's default IP Address is automatically supplied by the DHCP server.
7. Right-click the camera whose network property is to be changed. From the context menu that opens, select **Assign IP**. The **Assign IP** dialog is displayed.

8. To access DNA, do one of the following:
   a. For DHCP (not supported by Latitude):
      i. Select **Use DHCP**. Do not use for Latitude.
      ii. Click **Update** and wait for status.
   b. For Static IP (recommended for Latitude users):
      i. Do not select the **Use DHCP** checkbox. This is recommended for security purposes and for and Latitude users. In the IP Address, Gateway, and Netmask, enter the respective LAN/VLAN (optional DNS) values.
      ii. Click **Update** and wait for ☑ OK status to be displayed.
9. Right-click and select **Web** to directly access the camera via a web browser. The web browser opens on the unit’s **Login** dialog box.

![Login Dialog Box]

10. Log into the unit with the default user name **Admin** and password **1234**.

**Note:**

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

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

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

IE Tools > Internet Options > Advanced Window

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

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

Note:
If the password is changed and the Latitude AdminCenter Discovery feature is in use, deselect all other proprietary types. Select DVTEL Quasar Gen II Series as the Unit Type so that the new password can be configured in the Discovery tab settings.

Additionally, you can change the camera’s network properties (either DHCP or Static IP) directly from the camera’s web interface on the System > Network > Basic screen.
12. Install the web player.

**Note:**
If you have previously installed a web player application on the PC, you should delete the existing web player from the PC before accessing the camera. For information on how to install the new player, uninstall a previous player, and clear temporary Internet files, see [Installing and Deleting the Web Player](#).
9 Configuration and Operation

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

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

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

---

### Note:

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

This section includes the following information:

- **Browser-Based Viewer Introduction**
- **Live View**
- **System Tab**
- **Streaming Tab**
- **Camera Tab**
- **Logout**

#### 9.1 Browser-Based Viewer Introduction

The camera's web interface can be configured and operated from a 32-bit version of Internet Explorer 9 and above.

**To access the unit via the web browser**

1. Open your browser.
2. Enter the unit’s IP address in the browser’s address bar.
3. Press the ENTER key on your PC keyboard. The unit’s **Login** window is displayed. See Figure: Login Window.
4. Enter the user name (default: **Admin**) and password (default: **1234**) to log into the system. The unit’s web interface opens.

---

### Note:

The user name and password are case-sensitive.
The user interface 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 section 9.2.
   - **Settings Button**
     Clicking the Settings button opens the Settings screen, whose sidebar which includes three tabs – **System**, **Streaming**, and **Camera** – that are used for to configure system settings.
     - **System Settings**
       The administrator can configure settings for basic system parameters, security, network operation, events, recording, storage, system maintenance, and more. Details are discussed in the System Tab section.
     - **Streaming Settings**
       The administrator can modify video and audio settings on this page. Details are discussed in the Streaming Tab section.
     - **Camera Settings**
       The administrator can adjust many of the camera settings on this page, such as Exposure, Picture Adjustment, IR Function, Digital Zoom, and TV System. Details are discussed in the Camera Tab section.
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 number is displayed under the Log out link.

5. Function buttons are displayed to the left of the Live View window. These are discussed in the following section.

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

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

8. In the center of the interface is the Live View window, which displays the image that the camera is monitoring.

9. The firmware version of the camera is displayed under the Live View window on the right side.

9.2 Live View

The camera’s Live screen is used to monitor live video. See Figure: Browser-Based User Interface. Double-clicking the Live View window opens the Info dialog box, which displays key details about the video stream:

![Live Video Info Dialog Box](image)

**To view the Live View window in Fullscreen mode**

1. Click the Full-screen icon. The Live View image is displayed in the entire monitor screen.

**To exit Fullscreen mode**

1. Press the Escape key on your keyboard. The image is displayed in the Live View window of the Live screen.
The View Mode pane in the Live screen includes the following function buttons:

**Full-Window Display**
Click this button to view the live video in the full Live Video window.

**Half-Window Display**
Click this button to view the live video in half of the Live View window.

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

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

**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.

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

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

Manual Trigger

This button enables you to trigger an action defined on the **System > Events Setup > IO** screen, which enables control over input and output alarms.

Speaker

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

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

![CM-6212 System Menu](image)

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

- System
- Security
- Network
- Events Setup
- Edge Recording
- Motion Detection
- Schedule
- File Location
- Maintenance
- Import/Export
9.3.1 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 Screen](image)

The System screen includes the following fields:

**Host Name**

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

**Time Zone**

Select the time zone from the drop-down menu.

**Enable Daylight Saving Time**

To enable daylight saving time, check the 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.
### 9.3.2 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**

#### 9.3.2.1 User

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

![User Screen](image)

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

Note:
You must enter the user password and also select the authorized function(s).

Click Save to modify the account credentials and privileges, or Close to discard changes.
Streaming Authentication Setting

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

- **Disable** – Do not use streaming authentication (default setting).
- **Basic** – A form of authentication that uses unencrypted base64 encoding. Basic Authentication should generally only be used where transport layer security, such as HTTPS, is provided.
- **Digest** – A form of authentication used over RTSP in which credentials are encrypted when transmitted.

Click **SAVE**.

9.3.2.2 HTTPS

To use HTTPS on the camera, an HTTPS certificate must be installed. The HTTPS certificate can be obtained either by creating and sending a certificate request to a Certificate Authority (CA) or by creating a self-signed HTTPS certificate as described below.

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

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

Before a CA-issued certificate is obtained, you can first create and install a self-signed certificate. Under the Security category, click the HTTPS tab in the sidebar to display the following screen.

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.

3. **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.

4. Click **OK** to save the certificate request after completion. The details are displayed in the **Subject** field of the **Installed Certificate** section.

5. 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**.

6. When the signed certificate is returned from the CA, click **Browse** in the **Install Signed Certificate** section to locate the file.
7. Click **UPLOAD** to install the certificate, as seen below.

![HTTPS Screen – Upload Signed Certificate](image)

**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.

![HTTPS Screen – Install Signed Certificate](image)
The **Create Certificate Request** dialog box opens.

![Create Certificate Request Dialog Box](image)

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.

![Created Request Subject](image)
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**.

<table>
<thead>
<tr>
<th>Certificate Request Properties Dialog Box</th>
</tr>
</thead>
</table>

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

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

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

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

To add or delete an IP address
1. Enter the IP address in the Filtered IP Addresses text box.
2. Click ADD to add a new filtered address. The Filtered IP Addresses box shows the currently configured IP addresses. Up to 256 IP address entries may be specified.
3. To remove an IP address from the list, select the IP address and then click DELETE.
9.3.2.4 IEEE 802.1X

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

**CA Certificate**

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

**Client Certificate**

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

**Private Key**

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

**Settings**

- **Identity** – Enter the user identity (user name) associated with the certificate. Up to 16 characters can be used.
- **Private Key Password** – Enter the password associated with the user identity. Up to 16 characters can be used.
- **Enable IEEE 802.1X** – Select the checkbox to enable IEEE 802.1X security. The setting is disabled by default.

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

### 9.3.3 Network

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

- Basic
- QoS
- SNMP
- UPnP
- DDNS
- Mail
- FTP
- HTTP

#### 9.3.3.1 Basic

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

![Network > Basic Screen](image)

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

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

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

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

Get IP address automatically

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

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

Use fixed IP address

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

To set up a new static IP address

1. Select the Use fixed IP address option.
2. Enter the following information:
   - IP address – The IP address is necessary for network identification.
   - Subnet mask – Used to determine if the destination is in the same subnet. The default value is 255.255.255.0.
   - Default gateway – Used to forward frames to destinations in a different subnet. An invalid gateway setting causes transmission to destinations in other subnets to fail.
   - Primary DNS – The primary domain name server that translates host names into IP addresses.
   - Secondary DNS – A secondary domain name server that backs up the primary DNS.

To use PPPoE

1. Enter your PPPoE user name and password into the respective fields.
2. Click SAVE to confirm the settings.
Advanced

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

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

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

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

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

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

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

Click **SAVE** to save the settings.

**IPv6 Address Configuration**

**To enable IPv6**

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

**9.3.3.2 QoS**

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

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

- **Video DSCP** – This class consists of applications such as MJPEG over HTTP, RTP/RTSP and RTSP/HTTP.
- **Audio DSCP** – The camera supports audio.
- **Management DSCP** – This class consists of HTTP traffic (web browsing).

Click **SAVE** when complete.

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

### 9.3.3.3 SNMP

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.

![SNMP Settings Screen](image)
SNMP v1/v2

- **Enable SNMP v1 or Enable SNMP v2** – Select the version of SNMP (v1 or v2) to use by checking the relevant box.
- **Read Community** – Specify the community name that has read-only access to all supported SNMP objects. The default value is `public`.
- **Write Community** – Specify the community name that has read/write access to all supported SNMP objects (except read-only objects). The default value is `private`.

SNMP v3

SNMP v3 provides important security features including:

- **Confidentiality** – Encryption of packets to prevent snooping by an unauthorized source.
- **Integrity** – Message integrity to ensure that a packet has not been tampered with in transit including an optional packet replay protection mechanism.
- **Authentication** – To verify that the message is from a valid source.

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

- **Enable SNMP v3** – Select the checkbox.
- **Security Name** – See note below.
- **Authentication Type** – Select MD5 or SHA from the drop-down list. See note below.
- **Authentication Password** – See note below.
- **Encryption Type** – Select DES or AES from the drop-down list. See note below.
- **Encryption Password** – See note below.

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

Traps for SNMP v1/v2/v3

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

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

Click **SAVE** when complete.
9.3.3.4 UPnP

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

**UPnP Settings**

- **Enable UPnP** – If UPnP is enabled and a camera is discovered on the LAN, the icon of the connected camera appears in **My Network Places**, allowing direct access, as seen below.

**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, and 8.1 procedure.

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

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

Click **SAVE** to save the settings.

### 9.3.3.5 DDNS

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

![DDNS Screen](image)

**To use DDNS**

1. Select the **Enable DDNS** checkbox.
2. From the **Provider** drop-down list, select a DDNS host provider name.
3. In the **Host name** text box, enter the registered domain name.
4. In the **Username/E-mail** text box, enter the username or e-mail address required by the DDNS provider for authentication.
5. In the **Password/Key** text box, enter the password or key required by the DDNS provider for authentication.
6. Click **SAVE** to save the setting.
9.3.3.6  Mail

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

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

![Mail Screen – SMTP](image)

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

Click SAVE when finished.

9.3.3.7  FTP

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

![FTP Screen](image)

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)

Click **SAVE** when finished.

### 9.3.3.8 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 **IO**, **Tampering**, **Manual Trigger**, and **Motion Detection** screens.
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:

![HTTP Screen]

Click SAVE when finished.

### 9.3.4 Events Setup

The Events Setup tab includes the following screens:

<table>
<thead>
<tr>
<th>IO</th>
<th>Network Failure Detection</th>
<th>Tampering</th>
<th>Day/Night Trigger</th>
<th>Periodic Event</th>
<th>Manual Trigger</th>
</tr>
</thead>
</table>
9.3.4.1 IO

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

![IO Screen](image)

**Alarm Switch**

The Administrator can select from the following options:

- Select Off to disable an alarm.
- Select On to enable an alarm (default setting).
- Select By Schedule to set a schedule. Then click Please Select to select up to 10 schedules from the drop-down list that opens. The selected schedules are displayed in the Please Select text box. To set a schedule, open the Schedule tab.

Click SAVE after configuring the settings.

**Alarm Type**

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

**Alarm Output**

Define the normal alarm output signal as Output high or Output low, according to the current alarm application. Output high is the default setting. Click SAVE after configuring the settings.
Trigger Action

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

- **Enable alarm output** – Select this checkbox to enable alarm relay output. The checkbox is not selected by default.
- **Send message by FTP** – Select the checkbox send an alarm message by FTP when an alarm is triggered.
- **Upload image by FTP** – Select this box to assign an FTP site and configure the parameters shown. When an alarm is triggered, event images are uploaded to the designated FTP site.

**Note:**
Images can be sent by FTP only when MJPEG is selected as the video stream from the Video Format screens in the Streaming tab.

Follow these steps:

- From the FTP address drop-down list, select one of the two FTP addresses to use.
- From the Pre-trigger buffer and Post-trigger buffer drop-down lists, select the number of frames for the buffer from 1-20 frames.
- Select the **Continue image upload** checkbox to upload an image by FTP for a defined period of time or while the trigger is active. Select one of the following options:
  - To specify the length of time for the upload, select **Upload for** and enter the number of seconds in the text box.
  - To upload while the trigger is active, select **Upload while the trigger is active**.

In the Image Frequency text box, from the drop-down list select the number of frames per seconds from 1-15 for the upload.
Note:
Make sure that FTP configuration has been completed. See FTP for details.

- **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 specified HTTP servers. See figure below.

- **Record video clip** – Select this box in order to save the alarm-triggered recording to your microSDXC 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.

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

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

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

Note:
Images can be sent by e-mail only when MJPEG is selected as the video stream from the Video Format screens in the Streaming tab.
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.

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

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

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

Click **SAVE** after configuring the settings.

**File Name**

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

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

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

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

The file name suffix ends at the number being set. For example, if the setting is up to “10,” the file name will start from 00, end at 10, and then start over again.
- **Overwrite**
  The original image in the FTP site will be overwritten by the new uploaded file with a static filename.

Click **SAVE** after configuring the settings.

### 9.3.4.2 Network Failure Detection

Settings on the **Network Failure Detection** screen enable the camera to periodically ping another IP device within the network to detect a network failure, for example, if a video server is disconnected. By implementing local recording through a microSDXC card, the camera can operate as a backup recording device for the surveillance system if network communication is lost due to a network failure.

#### Detection Switch

The Administrator can select from the following options:

- **Select** *Off* to disable an alarm (default setting).
- **Select** *On* to enable an alarm.
- **Select** *By Schedule* to set a schedule. Then click **Please Select** to select up to 10 schedules from the drop-down list that opens. The selected schedules are displayed in the **Please Select** text box. To set a schedule, open the **Schedule** tab.

Click **SAVE** after configuring the settings.

#### Detection Type

In the text box, enter the IP address to ping and the time interval (in minutes) between pings. Click **SAVE** after configuring the settings.
Triggered Action
The Administrator can specify various alarm actions to be taken when an alarm is triggered. See the IO screen for details. The options are listed below.

- **Enable alarm output** – Check this box and select the predefined type of alarm output (low or high) to enable alarm relay when a network failure is detected.
- **Send message by FTP** – Select whether to send an alarm message by FTP when a network failure is detected.
- **Record video clip** – Select this box in order to save the alarm-triggered recording into a microSDXC card or the NAS.
- **Send message by E-Mail** – Select whether to send an alarm message by e-mail when a network failure is detected.

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

9.3.4.3 Tampering
The Tampering screen enables the camera to deal with tampering (such as blocking, paint-spraying, and obscuring the lens, etc.). Using video analysis, the camera can react to such events by sending notifications or uploading snapshots to the specified destination(s). Detection of camera tampering is achieved by measuring the differences between the older frames of video (which are stored in buffers) and more recent frames.

Tampering Alarm
The Administrator can select from the following options:

- Select **Off** to disable the tampering alarm (default setting).
- Select **On** to enable the tampering alarm.
- Select **By Schedule** to set a schedule. Then click **Please Select** to select up to 10 schedules from the drop-down list that opens. The selected schedules are displayed in the **Please Select** text box. To set a schedule, open the **Schedule** tab.

Click **SAVE** after configuring the settings.
Tampering Duration

Minimum tampering duration is the time for video analysis to determine whether camera tampering has occurred. Minimum duration can also be interpreted as defining the tampering threshold; a longer duration represents a higher threshold.

In the Minimum duration text box, enter the tampering duration time in seconds. The range is from 10 to 3600 seconds.

In the Sensitivity level text box, select a number from 1-100. The default level is 80, which means if 20% or more sampling pixels are detected differently, the system will detect motion. The bigger the value, the more sensitive it is. When the value is bigger, the red horizontal line in the motion detection window will be lowered accordingly.

Tampering Action

The Administrator can specify multiple alarm actions to be taken when tampering is detected. See the IO screen for details. The options are listed as follows:

- Enable alarm output – Check this box and select the predefined type of alarm output (high or low) to enable alarm relay when tampering is detected.
- Send Message by FTP – The Administrator can select whether to send an alarm message by FTP when tampering is detected.
- Upload Image by FTP – Selecting this option enables you to assign an FTP site and configure various parameters.
- Send HTTP notification – Check this option, select the destination HTTP address, and specify the parameters for HTTP notifications.
- Record video clip – Select this box in order to save the alarm-triggered recording into a microSDXC card.
- Send message by E-Mail – The Administrator can select whether to send an alarm message by e-mail when tampering is detected.
- Upload Image by E-Mail – Selecting this option enables you to assign an e-mail address and configure various parameters.

File Name

- File Name – Enter a file name in the field, for example image.jpg. The uploaded image’s file name format is set in this section. Select one that meets your requirements.
- Add date/time suffix (default setting)
  File name: imageYYMMDD_HHNNSS_XX.jpg
  Y: Year, M: Month, D: Day
  H: Hour, N: Minute, S: Second
  X: Sequence Number
- Add sequence number suffix (no maximum value)
  File name: imageXXXXXXX.jpg
  X: Sequence Number
Add sequence number suffix (limited value)
File Name: imageXX.jpg
X: Sequence Number
The file name suffix ends at the number being set. For example, if the setting is up to “10,” the file name will start from 00, end at 10, and then start over again.

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

Click SAVE after configuring the settings.

9.3.4.4 Day/Night Trigger

The Day/Night Trigger screen is used to enable the camera to trigger a device connected to the camera’s alarm output when the camera switches to Day or Night mode, which is set on the IR Function screen.

To configure the day/night trigger
1. In the Day/Night Trigger section, select On to enable the Day/Night Trigger or Off to disable it.
2. In the Day/Night Type section, select Day when the camera enters Day mode, for example to deactivate an external device, such as a lighting source. Select Night to activate an external device when the camera enters Night mode.
3. In the Triggered Action section, check Enable alarm output to activate an external lighting source. Depending on the voltage requirements of the external device, from the drop-down menu select high or low.
9.3.4.5 Periodic Event

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

**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.

**Triggered Action**
The Administrator can specify multiple alarm actions to be taken when a triggering event occurs. See the IO screen for details. The options are listed as follows:

- **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.
**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: `imageX00000X.jpg`
  X: Sequence Number

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

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

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

Click **SAVE** after configuring the settings.

### 9.3.4.6 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.

![Manual Trigger Screen](image)
Manual Trigger
Select Off or On to activate this function. The default is Off.

Triggered Action
Specify one or both alarms to trigger:

- **Enable alarm output** – Check this box and select the predefined type of alarm output (high or low) to enable alarm relay 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.
- **Upload Image by FTP** – Selecting this option enables you to assign an FTP site and configure various parameters.
- **Send HTTP notification** – Check this option, select the destination HTTP address, and specify the parameters for HTTP notifications.
- **IR Cut Filter** – Select this checkbox to trigger an event when the IR cut filter is activated. From the drop-down menu, select on or off. When the IR Cut filter is set to on, the IR LED illuminator is activated for use in low-light environments in which Night mode is normally used.
- **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 E-Mail** – Selecting this option enables you to assign an e-mail address and configure various parameters.
- **Record video clip** – Select this box in order to save the alarm-triggered recording into a microSDXC 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 (limited value)**
  File Name: imageXX.jpg
  X: Sequence Number
  The file name suffix ends at the number being set. For example, if the setting is up to “10,” the file name will start from 00, end at 10, and then start over again.
- **Overwrite**
  The original image in the FTP site will be overwritten by the new uploaded file with a static filename.

Click **SAVE** after configuring the settings.
9.3.5  Edge Recording

The Events Handler 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

9.3.5.1  SD Card

You can locally record up to 128GB on a Class 10 microSDXC card. 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 microSDXC card recording, see Recording.

![SD Card Screen](image)

**Note:**
Format the microSDXC 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 microSDXC card, card information, such as the memory capacity and status, is displayed.
Device Setting

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 microSDXC card is listed in the Recording List table below. 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 microSDXC 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.

- **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.

**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).
- *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.

![Selected File Window](image)

### 9.3.5.2 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.

![Network Share Screen](image)

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)
- **Protocol** – Displays the protocol used by the NAS. The default is SAMBA.

Enter the details for the following fields:

- **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.

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. See Figure: Video File Recording List.

- **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.
9.3.5.3  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.

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

Note:
It is not recommended 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

**Recording Screen**

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 microSDXC card is installed in the camera or (b) the NAS is configured properly.
9.3.6 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.

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 Latitude, it is recommended to set the motion detection from AdminCenter.
To activate Motion Detection

1. From the Motion Detection dropdown 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. Create a Motion Detection region. See instructions below.
4. Paint the Motion Detection region. See instructions below.
5. Configure the Motion Detection settings. See instructions below.
6. Set triggered actions. See instructions below.

To create a Motion Detection region

1. Click Edit. The Region Configuration editing options are displayed.
   - Click Add. A motion detection region is created on-screen.
   - To change the size of the region, drag an edge of the box to the desired cell.
   - Click SAVE.

To paint a motion detection region

1. Check Region paint.
2. To set the number of cells to paint, from the brush drop-down list, select 1x1, 3x3, or 5x5.
3. Click SAVE.
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](image)

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.

Set Triggered Actions

The Administrator can specify alarm actions to be taken when motion is detected. See the IO screen for details. The options are listed as follows:

- **Enable alarm output** – Check this box and select the predefined type of alarm output (low or high) to enable alarm relay when tampering is detected.
- **Record video clip** – Select this box to store the motion detection alarm recording in a microSDXC card or on the NAS when tampering is detected.
- **Send alarm message by FTP** – Select whether to send an alarm message by FTP 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.
- **Send HTTP notification** – Check this box to send a notification by HTTP.
- **Send alarm message by E-Mail** – Select whether to send an alarm message by e-mail when motion is detected.
• **Upload image by E-Mail** – Select this box in order to assign an e-mail address and configure various parameters.

**File Name**

The uploaded image’s filename format is set in this section. Select one that meets your requirements.

Click **SAVE** to save the motion detection settings.

**9.3.7 Schedule**

The **Schedule** screen is used for setting schedules for the network failure detection, tampering 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. See figure below.

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

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

![Schedule Screen](image)

**To create a new schedule or edit an existing schedule**

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

**To remove a schedule**

1. To remove a schedule, select the setup data line by line.
2. Click **DELETE** to remove.
9.3.8 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.

Note:
1. Make sure the selected file path contains valid characters.
2. When using Windows 8 OS, the storage location cannot be C:\. You must define a storage location that does not require Administrator privileges on the PC.
9.3.9 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

9.3.9.1 Log File

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

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

View User Login Information

Click GET USER INFORMATION to see each user’s details. For example: Admin: 1234. This indicates that the user’s login username is Admin and the password is 1234.
View User Privilege

Click **GET USER PRIVACY** to view each user’s privileges.

![User Information – Get User Privacy](image)

In the screen above, both *Admin* and *User* are granted privileges of 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.
9.3.9.3  Factory Default

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

![Factory Default Screen](image)

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.
Partial Restore

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

![Partial Restore Screen](image)

Reboot

Click REBOOT to restart the system without changing current settings.

9.3.9.4 Software Version

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

![Software Version Screen](image)
9.3.9.5 Software Upgrade

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

![Software Upgrade Screen](image)

**Note:**
1. Make sure that the software upgrade file is available before performing a software upgrade.
2. Do not change the file name. If you change the upgrade file name, the system will fail to find the file.

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

**Attention:**
1. Ne débranchez pas l'alimentation pendant la modification des noms de fichiers.
2. Ne débranchez pas l'alimentation pendant la mise à niveau du logiciel.

**To upgrade the software**

1. In the **Step 1** text box, click **Browse** and select the binary file to be uploaded, for example, uImage+userland.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, 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. From the Windows Start menu, select **Control Panel**.

6. Select **Uninstall a Program**.

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

8. Click **Uninstall** to delete the existing DVPlayer or DCViewer plug-in file.

9. Install the new ActiveX plug-in.

### 9.3.9.6 Parameters

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

![Parameters Screen](image)

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

9. Install the new ActiveX plug-in.
9.3.10 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.

![Import/Export Screen]

To export a configuration file

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

![File Download Screen]

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

To import a configuration file

1. Click **Browse** to select the configuration file
2. Click **UPLOAD**. The file is uploaded to the camera.

**Caution:**
Do not unplug power while changing file names.

**Attention:**
*Ne débranchez pas l'alimentation pendant la modification des noms de fichiers.*
9.4 Streaming Tab

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

Details of these settings are specified in the following sections:

- Video Format
- Video Compression
- Video OCX Protocol
- Video Frame Rate
- Video Mask
- Audio
9.4.1 Video Format

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

- **Video Resolutions**
- **Text Overlay Settings**
- **Video Rotate Type**
- **GOV Settings**
- **H.264 Profile**

![Video Format Screen](image-url)
9.4.1.1 Video Resolutions

The camera's web interface supports software dewarping when implemented on the Latitude VMS. The default resolution setting is H.264 @ 4000x3000 (20 fps). The following video resolutions are supported:

- H.264-only
- MJPEG-only
- H.264/MJPEG + H.264/MJPEG

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

<table>
<thead>
<tr>
<th>H.264-Only</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PAL</strong></td>
<td><strong>NTSC</strong></td>
</tr>
<tr>
<td>4000 x 3000 (20 fps)</td>
<td>4000 x 3000 (20 fps)</td>
</tr>
<tr>
<td>3840 x 2160 (24 fps)</td>
<td>3840 x 2160 (24 fps)</td>
</tr>
<tr>
<td>3840 x 2160 (25 fps)</td>
<td>3840 x 2160 (30 fps)</td>
</tr>
<tr>
<td>1920 x 1080 (25 fps)</td>
<td>1920 x 1080 (30 fps)</td>
</tr>
<tr>
<td>1280 x 720 (25 fps)</td>
<td>1280 x 720 (30 fps)</td>
</tr>
<tr>
<td>720 x 576 (25 fps)</td>
<td>720 x 480 (30 fps)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MJPEG-Only</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PAL</strong></td>
<td><strong>NTSC</strong></td>
</tr>
<tr>
<td>1920 x 1080 (25 fps)</td>
<td>1920 x 1080 (30 fps)</td>
</tr>
<tr>
<td>1280 x 720 (25 fps)</td>
<td>1280 x 720 (30 fps)</td>
</tr>
<tr>
<td>720 x 576 (25 fps)</td>
<td>720 x 480 (30 fps)</td>
</tr>
</tbody>
</table>
### H.264/MJPEG + H.264/MJPEG (PAL)

<table>
<thead>
<tr>
<th>Stream 1</th>
<th>Stream 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>4000 x 3000 (15 fps)</td>
<td>1920 x 1080 (12 fps)</td>
</tr>
<tr>
<td></td>
<td>1280 x 720 (12 fps)</td>
</tr>
<tr>
<td></td>
<td>720 x 576 (12 fps)</td>
</tr>
<tr>
<td>3840 x 2160 (20 fps)</td>
<td>1920 x 1080 (20 fps)</td>
</tr>
<tr>
<td></td>
<td>1280 x 720 (20 fps)</td>
</tr>
<tr>
<td></td>
<td>720 x 576 (20 fps)</td>
</tr>
<tr>
<td>1920 x 1080 (25 fps)</td>
<td>1920 x 1080 (25 fps)</td>
</tr>
<tr>
<td></td>
<td>1280 x 720 (25 fps)</td>
</tr>
<tr>
<td></td>
<td>720 x 576 (25 fps)</td>
</tr>
<tr>
<td>1280 x 720 (25 fps)</td>
<td>1280 x 720 (25 fps)</td>
</tr>
<tr>
<td></td>
<td>720 x 576 (25 fps)</td>
</tr>
<tr>
<td>720 x 576 (25 fps)</td>
<td>720 x 576 (25 fps)</td>
</tr>
</tbody>
</table>

### H.264/MJPEG + H.264/MJPEG (NTSC)

<table>
<thead>
<tr>
<th>Stream 1</th>
<th>Stream 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>4000 x 3000 (15 fps)</td>
<td>1920 x 1080 (15 fps)</td>
</tr>
<tr>
<td></td>
<td>1280 x 720 (15 fps)</td>
</tr>
<tr>
<td></td>
<td>720 x 480 (15 fps)</td>
</tr>
<tr>
<td>3840 x 2160 (20 fps)</td>
<td>1920 x 1080 (20 fps)</td>
</tr>
<tr>
<td></td>
<td>1280 x 720 (20 fps)</td>
</tr>
<tr>
<td></td>
<td>720 x 480 (20 fps)</td>
</tr>
<tr>
<td>1920 x 1080 (30 fps)</td>
<td>1920 x 1080 (30 fps)</td>
</tr>
<tr>
<td></td>
<td>1280 x 720 (30 fps)</td>
</tr>
<tr>
<td></td>
<td>720 x 480 (30 fps)</td>
</tr>
<tr>
<td>1280 x 720 (30 fps)</td>
<td>1280 x 720 (30 fps)</td>
</tr>
<tr>
<td></td>
<td>720 x 480 (30 fps)</td>
</tr>
<tr>
<td>720 x 480 (30 fps)</td>
<td>720 x 480 (30 fps)</td>
</tr>
</tbody>
</table>
### H.264/MJPEG + H.264/MJPEG + H.264/MJPEG (PAL)

<table>
<thead>
<tr>
<th>Stream 1</th>
<th>Stream 2</th>
<th>Stream 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>4000 x 3000 (15 fps)</td>
<td>1280 x 720 (12 fps)</td>
<td>1280 x 720 (12 fps)</td>
</tr>
<tr>
<td></td>
<td>720 x 576 (12 fps)</td>
<td>720 x 576 (12 fps)</td>
</tr>
<tr>
<td>3840 x 2160 (12 fps)</td>
<td>1920 x 1080 (12 fps)</td>
<td>1280 x 720 (12 fps)</td>
</tr>
<tr>
<td></td>
<td>1280 x 720 (12 fps)</td>
<td>1280 x 720 (20 fps)</td>
</tr>
<tr>
<td>1920 x 1080 (25 fps)</td>
<td>1280 x 720 (25 fps)</td>
<td>1280 x 720 (25 fps)</td>
</tr>
<tr>
<td></td>
<td>720 x 576 (25 fps)</td>
<td>720 x 576 (25 fps)</td>
</tr>
<tr>
<td>1280 x 720 (25 fps)</td>
<td>1280 x 720 (25 fps)</td>
<td>1280 x 720 (25 fps)</td>
</tr>
<tr>
<td></td>
<td>720 x 576 (25 fps)</td>
<td>720 x 576 (25 fps)</td>
</tr>
<tr>
<td>720 x 576 (25 fps)</td>
<td>720 x 576 (25 fps)</td>
<td>720 x 576 (25 fps)</td>
</tr>
</tbody>
</table>

### H.264/MJPEG + H.264/MJPEG + H.264/MJPEG (NTSC)

<table>
<thead>
<tr>
<th>Stream 1</th>
<th>Stream 2</th>
<th>Stream 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>4000 x 3000 (15 fps)</td>
<td>1280 x 720 (15 fps)</td>
<td>1280 x 720 (15 fps)</td>
</tr>
<tr>
<td></td>
<td>720 x 480 (15 fps)</td>
<td>720 x 480 (15 fps)</td>
</tr>
<tr>
<td>3840 x 2160 (15 fps)</td>
<td>1920 x 1080 (15 fps)</td>
<td>1280 x 720 (15 fps)</td>
</tr>
<tr>
<td></td>
<td>1280 x 720 (15 fps)</td>
<td>1280 x 720 (15 fps)</td>
</tr>
<tr>
<td>1920 x 1080 (30 fps)</td>
<td>1280 x 720 (30 fps)</td>
<td>1280 x 720 (30 fps)</td>
</tr>
<tr>
<td></td>
<td>720 x 480 (30 fps)</td>
<td>720 x 480 (30 fps)</td>
</tr>
<tr>
<td>1280 x 720 (30 fps)</td>
<td>1280 x 720 (30 fps)</td>
<td>1280 x 720 (30 fps)</td>
</tr>
<tr>
<td></td>
<td>720 x 480 (30 fps)</td>
<td>720 x 480 (30 fps)</td>
</tr>
<tr>
<td>720 x 480 (30 fps)</td>
<td>720 x 480 (30 fps)</td>
<td>720 x 480 (30 fps)</td>
</tr>
</tbody>
</table>
### H.264/MJPEG + H.264/MJPEG + H.264/MJPEG + H.264/MJPEG (PAL)

<table>
<thead>
<tr>
<th>Stream 1</th>
<th>Stream 2</th>
<th>Stream 3</th>
<th>Stream 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>4000 x 3000 (15 fps)</td>
<td>1280 x 720 (12 fps)</td>
<td>1280 x 720 (12 fps)</td>
<td>720 x 480 (12 fps)</td>
</tr>
<tr>
<td></td>
<td>720 x 480 (12 fps)</td>
<td>720 x 480 (12 fps)</td>
<td></td>
</tr>
<tr>
<td>3840 x 2160 (12 fps)</td>
<td>1920 x 1080 (12 fps)</td>
<td>1280 x 720 (12 fps)</td>
<td>720 x 576 (12 fps)</td>
</tr>
<tr>
<td></td>
<td>1280 x 720 (12 fps)</td>
<td>1280 x 720 (12 fps)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>720 x 576 (12 fps)</td>
<td>720 x 576 (12 fps)</td>
<td></td>
</tr>
<tr>
<td>1920 x 1080 (25 fps)</td>
<td>1920 x 1080 (25 fps)</td>
<td>1280 x 720 (25 fps)</td>
<td>720 x 576 (25 fps)</td>
</tr>
<tr>
<td></td>
<td>1280 x 720 (25 fps)</td>
<td>1280 x 720 (25 fps)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>720 x 576 (25 fps)</td>
<td>720 x 576 (25 fps)</td>
<td></td>
</tr>
<tr>
<td>1280 x 720 (25 fps)</td>
<td>1280 x 720 (25 fps)</td>
<td>1280 x 720 (25 fps)</td>
<td>720 x 576 (25 fps)</td>
</tr>
<tr>
<td></td>
<td>720 x 576 (25 fps)</td>
<td>720 x 576 (25 fps)</td>
<td></td>
</tr>
<tr>
<td>720 x 576 (25 fps)</td>
<td>720 x 576 (25 fps)</td>
<td>720 x 576 (25 fps)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Stream 1</th>
<th>Stream 2</th>
<th>Stream 3</th>
<th>Stream 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>4000 x 3000 (15 fps)</td>
<td>1280 x 720 (15 fps)</td>
<td>1280 x 720 (15 fps)</td>
<td>720 x 480 (15 fps)</td>
</tr>
<tr>
<td></td>
<td>720 x 480 (15 fps)</td>
<td>720 x 480 (15 fps)</td>
<td></td>
</tr>
<tr>
<td>3840 x 2160 (15 fps)</td>
<td>1920 x 1080 (15 fps)</td>
<td>1280 x 720 (15 fps)</td>
<td>720 x 480 (15 fps)</td>
</tr>
<tr>
<td></td>
<td>1280 x 720 (15 fps)</td>
<td>720 x 480 (15 fps)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>720 x 480 (15 fps)</td>
<td>720 x 480 (15 fps)</td>
<td></td>
</tr>
<tr>
<td>1920 x 1080 (30 fps)</td>
<td>1920 x 1080 (30 fps)</td>
<td>1280 x 720 (30 fps)</td>
<td>720 x 480 (30 fps)</td>
</tr>
<tr>
<td></td>
<td>1280 x 720 (30 fps)</td>
<td>720 x 480 (30 fps)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>720 x 480 (30 fps)</td>
<td>720 x 480 (30 fps)</td>
<td></td>
</tr>
<tr>
<td>1280 x 720 (30 fps)</td>
<td>1280 x 720 (30 fps)</td>
<td>720 x 480 (30 fps)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>720 x 480 (30 fps)</td>
<td>720 x 480 (30 fps)</td>
<td></td>
</tr>
<tr>
<td>720 x 480 (30 fps)</td>
<td>720 x 480 (30 fps)</td>
<td>720 x 480 (30 fps)</td>
<td></td>
</tr>
</tbody>
</table>

**Note:**
Latitude does not accept settings above 25 fps when operating on a PAL system or above 30 fps when operating in an NTSC system.

### 9.4.1.1 Text Overlay Settings

**Text Overlay Settings**

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

- *Include date*
- *Include time*
- *Include text string* – When this checkbox is selected, enter the string in the text box that opens.
- *Include subtitle* – When this checkbox is selected, enter the string in the text box that opens.
9.4.1.1.2 Video Rotate Type

You can change video display type if necessary. Selectable video rotate types include Normal video, Flip video, Mirror video, 90 degree clockwise, 180 degree rotate, and 90 degree counterclockwise (referred to as “90 and 270 degrees” in Latitude). Differences among these types are illustrated below. Suppose the displayed image of the camera is shown as follows.

To rotate the image vertically, for example, select Flip video. The displayed image is reversed as shown below.

Following are descriptions of different video rotate types.

- **Normal video** – The image appears as it is viewed. This is the default setting.
- **Flip video** – The image is reversed along its horizontal axis.
- **Mirror video** – The image is reversed along its vertical axis.
- **90 degree clockwise** – The image rotates 90° clockwise (to the right) and is displayed in 9:16 aspect ratio. This mode is ideal for use when monitoring a long, narrow area, such as an aisle, hallway or corridor.
- **180 degree rotate** – The image rotates 180° counter-clockwise (to the left).
- **90 degree counterclockwise** – The image rotates 90° counter-clockwise (to the left) and is displayed in 9:16 aspect ratio. This mode is recommended when monitoring a long, narrow area, such as an aisle, hallway or corridor. This mode is referred to in Latitude as “90 and 270 degrees” mode.

Click **SAVE** to confirm the setting.
9.4.1.1.3 GOV Settings

You can set the GOV length to determine the frame structure (I-frames and P-frames) in a video stream for saving bandwidth. The setting range is from 1 to 255. A longer GOV means decreasing the frequency of I-frames. The default GOV setting for H.264-1 and H.264-2 is 25/30 (PAL/NTSC). The default GOV setting for H.264-3 and H.264-4 is 25/30 (PAL/NTSC). Click **SAVE** to confirm the GOV setting.

9.4.1.1.4 H.264 Profile

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

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

- **Main Profile (MP)**  
  This profile provides improved picture quality at reduced bandwidths and storage costs and is becoming more common as the camera processors (DSPs) become more able to handle the processing load. *Main Profile* can save 10-12% over *Baseline*. This is the default profile.

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

Click **SAVE** to confirm the settings.
9.4.2 Video Compression

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

**Video Compression Screen**

**MJPEG Compression Setting**

A higher value implies higher bit rates and higher visual quality. The default setting of the MJPEG Q factor is 35. The setting range is from 1 to 70. Click **SAVE** to confirm the setting.

**H.264 Compression Setting**

The default setting of H.264-1 is 4096. The default setting for the other streams is 1024 kbps. Each stream can be configured individually. The setting range is from 64 to 20,480 kbps. Click **SAVE** to confirm the setting.

**Note:**

A total of 26,624 kbps is available on the camera for streaming. A single stream is limited to 20,480 kbps.
Quality

The Encoding Priority function enables the user to adjust the quality of the picture along a single axis. The slider is configured according to Quantization Parameter (QP) values. Setting QP to a high value increases the bit rate and results in high compression, but this is at the expense of poor decoded image quality. Setting QP to a low value results in better decoded image quality, but with lower compression.

Encoding Priority should be set for each H.264 stream. The slider ranges from 1 (low bit rate) to 10 (high picture quality). The default setting is 7. Click SAVE to confirm the setting.

Note:
The Encoding Priority setting is displayed only when H.264 is selected.

Compression Information Setting

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

CBR Mode Setting

To enable CBR mode on a stream, select the checkbox for that stream. Click SAVE to confirm the setting.

9.4.3 Video OCX Protocol

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

- **RTP over UDP**
- **RTP over RTSP (TCP)**
- **RTSP over HTTP**
- **MJPEG over HTTP**
- **Multicast mode** – Enter in each field all required data, including Multicast H.264-1 Video Address, Multicast H.264-2 Video Address, Multicast H.264-3 Video Address, Multicast H.264-4 Video Address, Multicast MJPEG Video Address, Multicast Audio Address, and Multicast TTL.

Click **SAVE** to confirm the settings.

### 9.4.4 Video Frame Rate

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

**Video Frame Rate Screen**

**MJPEG/H.264 Frame Rate Setting**

The default setting is single stream H.264-only 4000x3000 @20 fps (NTSC). The setting range for MJPEG is 1-30 fps in NTSC and 1-25 fps in PAL.

**Note:**

A lower frame rate decreases video smoothness.

The following settings apply when operating the unit in any mode other than H.264-only:

- **MJPEG** – The setting range of the MJPEG Frame Rate at 4000x3000 is from 1 to 30 in NTSC and 1 to 25 in PAL. The default setting is 30 fps in NTSC and 25 fps in PAL.
• **H.264-1** – The setting range for the H-264-1 Frame Rate at 4000x3000 is from 1 to 20 fps (PAL/NTSC).

• **H.264-2** – The setting range for the H-264-2 Frame Rate is from 1 to 15 fps (PAL/NTSC) for Stream 1. The maximum resolution and frame rate for Stream 2 is 1920x1080 @ 12/15 fps (PAL/NTSC).

• **H.264-3** – The maximum frame rate for Stream 1 is from 1 to 20 fps (PAL/NTSC). The maximum resolution and frame rate for Stream 2 and Stream 3 is 1280x720 @ 12/15 fps (PAL/NTSC).

• **H.264-4** – The maximum frame rate for Stream 1 is from 1 to 20 fps (PAL/NTSC). The maximum resolution and frame rate for Stream 2 and Stream 3 is 1280x720 @ 12/15 fps (PAL/NTSC). The maximum frame rate for Stream 4 is 720x480/576 @ 12/15 fps (PAL/NTSC).

Click **SAVE** to confirm the settings.

---

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

### 9.4.5 Video Mask

From the **Video Mask** screen, you may select up to five rectangular portions of the View Area to ‘Mask.’ Below is an illustration with one mask displayed in the View Area.

![Video Mask Screen](image)

**Active Mask Function**

When a Video [Privacy] Mask is turned on, the area within the mask or box is blocked out or obscured from view.

**To enable a mask**

1. Check a **Video Mask** checkbox. A red frame is displayed in the Live Video pane on the right side.
2. Use the mouse to drag and drop, adjust the mask’s size, and place it on the target zone.

**Note:**
It is suggested to set the Video Mask twice as large as the object it covers.
To disable a mask

1. Uncheck the checkbox of the Video Mask meant to be deleted. The selected mask disappears from the Live Video pane.

Mask Setting

- Mask color – The selections of Mask color include red, black, white, yellow, green, blue, cyan, and magenta.

Click SAVE to confirm the setting.

9.4.6 Audio

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

Transmission Mode

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

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

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

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

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

Server Gain Setting

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

Selectable audio transmission bit rate include 16 kbps (G.726), 24 kbps (G.726), 32 kbps (G.726), 40 kbps (G.726), µLAW (G.711), ALAW (G.711), and AAC. 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 AAC.

Note:
Latitude does not support G.726.

Click SAVE to confirm the settings.

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 Disabled.

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.

9.5 Camera Tab

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

Exposure   Picture Adjustment   Advanced Picture Settings   IR Function   Misc.
9.5.1 Exposure Screen

The Exposure screen is used to configure lens settings and exposure modes. The exposure is the amount of light received by the image sensor 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.

In Auto Mode, a Minimum Shutter Speed may be set from the drop-down menu to ensure a maximum level of exposure. In Manual Mode, you can choose fixed shutter speeds from a drop-down menu.

Exposure Mode

The bottom section of the screen enables you to select one of two exposure modes: Auto Mode (default) or Manual Mode. Administrators may either allow the camera to automatically select an exposure level using a programmed algorithm or choose the level themselves.

9.5.1.1 Auto Mode

Auto Mode is the default mode. It automatically and smoothly adjusts the iris when the light level drops to a point where it is insufficient to support the iris setting. A minimum shutter speed may be set from the drop-down menu to ensure a maximum level of exposure.

The following setting is available:

- *Min Shutter Speed* – When selecting this mode, the shutter is completely open and the exposure priority is given to the iris. Shutter speed and AGC circuit function automatically in cooperating with the iris to achieve a consistent exposure output.

  The shutter speed range is selectable on the drop-down menu from 1/2 to 1/500 sec (NTSC) and 1/1.5 to 1/425 sec (PAL). The following table lists the options.
9.5.1.2 Manual Mode

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

Manual Mode opens the iris completely with a fixed gain to a fixed shutter speed. Users can select a suitable shutter speed according to the environmental luminance. Increasing the value of the fixed shutter increases the amount of light entering the sensor. This allows a brighter and more detailed image. Similarly, utilizing gain and increasing its level increases the sensitivity of the image sensor, which brightens the image and adds details. This increases the level of noise in the image.

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

The following settings are available:

- **Shutter Speed** – The fixed shutter speed is selectable from 1/2 to 1/10000 sec (NTSC) and 1/1.5 to 1/10000 sec (PAL). Select the suitable shutter speed according to the environmental luminance. The following table lists the options.
Gain – A nominal video signal level is usually 1-volt peak-to-peak for composite video, 0.7 volts for component or RGB video, or 0.3 volts for the chrominance subsection, at which level a fully saturated picture is transmitted to the acceptor. However, for cases where the video signal is attenuated, a low-noise, high-gain analog amplifier is built into quality video processing equipment. This amplifier provides video gain control whereby the video signal can be boosted or reduced. Dark pictures caused by low level lighting are easily adjusted. The Gain drop-down menu turns the video gain Off or moves it in steps from 1 to 9.

Click SET when you finish setting the gain.

9.5.2 Picture Adjustment

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

Camera Settings Screen – Picture Adjustment

**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. Click SET to confirm the new setting.

**Sharpness**

Increasing the sharpness level can make the image look sharper, especially enhancing the object’s edge. Select from the range between 0 to +15. The default setting is DEFAULT. Click SET to confirm the new setting.

<table>
<thead>
<tr>
<th>Manual Mode Fixed Shutter Speeds</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/300</td>
</tr>
<tr>
<td>1/215</td>
</tr>
<tr>
<td>1/150</td>
</tr>
</tbody>
</table>
**Contrast**

Camera image contrast level is adjustable. Select from a range of -6 to +19. The default setting is *DEFAULT*. Click SET to confirm the new setting.

**Saturation**

Camera image saturation level is adjustable. Select from a range of -6 to +19. The default setting is *DEFAULT*. Click SET to confirm the new setting.

**Hue**

Camera image hue level is adjustable: select from a range of -12 to +13. The default setting is *DEFAULT*. Click SET to confirm the new setting.

### 9.5.3 Advanced Picture Settings

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

- White Balance
- Backlight
- WDR Function
- Noise Reduction Settings

#### 9.5.3.1 White Balance

Options for controlling the camera’s white balance (color balance) are shown below.

![Advanced Picture Settings Screen – White Balance](image)

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.

<table>
<thead>
<tr>
<th>Light Sources</th>
<th>Color Temperature (in K°)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloudy Sky</td>
<td>6,000 to 8,000</td>
</tr>
<tr>
<td>Noon Sun and Clear Sky</td>
<td>6,500</td>
</tr>
<tr>
<td>Household Lighting</td>
<td>2,500 to 3,000</td>
</tr>
<tr>
<td>75-watt Bulb</td>
<td>2,820</td>
</tr>
<tr>
<td>Candle Flame</td>
<td>1,200 to 1,500</td>
</tr>
</tbody>
</table>
Four white balance modes are available:

- **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 function 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.

- **One Push** – This button activates the factory-optimized setting for white balance. This setting may not be ideal for every lighting environment.

- **Manual** – In this mode, you can manually change the white balance value. You can select a number between 0 – 127 for either/both Rgain and Bgain to increase the red and/or blue luminance.

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

### 9.5.3.2 Backlight

Backlight compensation is used in images where a bright light source is behind the subject of interest. Without backlight compensation, the subject would normally appear in silhouette. The backlight function of the camera allows it to adjust the exposure of the entire image to properly expose the subject in the foreground. Select **On** or **Off**. The default setting is **Off**.

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

### 9.5.3.3 WDR Function

WDR (Wide Dynamic Range) resolves high contrast or changing light issues in order to enhance the image quality. It does this by producing a larger amount of details in both the dark and bright areas of the image. Such scenes combine areas with different lighting conditions, where some areas are very bright and others are dark. If this function was not used, the image either would be overexposed or too bright in bright areas and completely dark in dark areas.
The \textit{WDR function} setting is adjustable among \textit{Off}, \textit{Low}, \textit{Mid} and \textit{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 \textit{Mid}.

Click \textbf{SET} to confirm the new settings.
9.5.3.4 Noise Reduction Settings

The noise reduction function consists of three settings:

- 3DNR
- 2DNR
- 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 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 Hi. The default setting is 3DNR Low. Click SET to confirm the new settings.

### 2DNR

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

Settings include On and Off. The default setting is On. Click SET to confirm the new settings.
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 Med, and Color Hi. The highest setting (Color Hi) 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. Click SET to confirm the new settings. The default setting is Color Hi.

9.5.4 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 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/On/Off/Smart modes. The default mode is Smart. Following is an explanation of the four settings:

- Auto Mode – The camera converts from Day mode (color) to Night mode (monochrome) automatically at nighttime or in low light conditions. When there is sufficient light, the camera converts automatically from Night mode to Day mode.
- On – Activates IR mode (puts camera into monochrome/Night mode).
- Off – Deactivates IR mode (puts camera into color/Day mode).
- Smart – Smart mode enhances monochrome/Night mode stability when IR illumination is dominant and keeps the camera from switching between Day and Night modes. In this mode, the IR Cut filter is on (i.e. monochrome/Night mode) when the IR LED illuminator also is activated. This prevents the camera from returning to color/Day mode.

Click SET to confirm the new setting.
**IR LED Illuminator**

This setting is used in low-light conditions or at night. IR LED lights are turned On or Off, depending on the light sensor. The default mode is Auto. Two settings are available:

- **Auto** – The light sensor operates automatically.
- **Off** – The IR light is always off.

Click SET to confirm the new setting.

**Day/Night Threshold**

Set the threshold at which you want to activate the IR function:

- For the daytime to nighttime threshold, from the upper drop-down list, select a number between 1-9, where 1 is darker and 9 is brighter.
- For the nighttime to daytime threshold, from the upper drop-down list, select a number between 1-9, where 1 is darker and 9 is brighter.

Click SET to confirm the new setting.

**IR Compensation**

From the drop-down list, set the IR Compensation to On or Off. Setting IR Compensation to On compensates for the reflection of infrared light emitted from the camera onto reflective objects, thus improving image sharpness and definition. Without IR compensation, objects may appear blurred. IR Compensation is enabled by default.

Click SET to confirm the new setting.

### 9.5.5 Misc. Screen

From the Misc. (Miscellaneous) tab you can set the TV system.

![Camera > Miscellaneous Screen](image)
Note:
After changing TV System settings, the camera restarts automatically. Refresh your browser in order to use the unit with the new settings.

**TV System Settings**

Select the video system setting: 25 fps (PAL) or 30 fps (NTSC). The default TV system is 30 fps (NTSC).

Click SET to confirm the setting.

### 9.6 Logout

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

![Logout Message](image)

Upon clicking **Login**, the **Login** dialog box opens. See Figure: [Login Dialog Box](image).
10 Appendices

The following appendices are included in this section:

- Technical Specifications
- Internet Security Settings on Internet Explorer
- Installing UPnP Settings on Internet Explorer
- Deleting Temporary Internet Files on Internet Explorer
- Installing and Deleting the Web Player
- Network Settings
- Troubleshooting
- Acronyms and Abbreviations
- Mounting Accessories
## 10.1 Technical Specifications

Following are the CM-6212 technical specifications:

<table>
<thead>
<tr>
<th>Camera</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Image Sensor</td>
<td>1/1.7” 4000x3000 (12 MP) Progressive Scan BSI CMOS</td>
</tr>
<tr>
<td>Effective Pixels (H x V)</td>
<td>4000x3000 (H x V)</td>
</tr>
<tr>
<td>Shutter Speed</td>
<td>1.0 to 1/10,000 (auto)</td>
</tr>
<tr>
<td>Digital Slow Shutter (DSS)</td>
<td>1/1 to 1/25 or 1/30 with ≤ 32x sensitivity boost in day/night mode</td>
</tr>
<tr>
<td>Sensitivity</td>
<td></td>
</tr>
<tr>
<td>Color Mode</td>
<td>0.1 lux @ F2.4</td>
</tr>
<tr>
<td>B/W Mode</td>
<td>0.01 lux @ F2.4 in night mode with IR illuminator ON, measured with DSS OFF at 30 IRE</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Video</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Video Compression</td>
<td>H.264 and MJPEG</td>
</tr>
<tr>
<td>Video Resolution</td>
<td>Scalable from 12MP (H.264)/Full HD 1080p (MJPEG) to QVGA</td>
</tr>
<tr>
<td>Maximum Performance</td>
<td>12MP @ 20 fps (PAL/NTSC)</td>
</tr>
<tr>
<td></td>
<td>12MP @ 15 fps + Full HD 1080p @ 12/15 fps (PAL/NTSC)</td>
</tr>
<tr>
<td></td>
<td>12MP @ 15 fps + HD 720p @ 12/15 fps + HD 720p @ 12/15 fps (PAL/NTSC)</td>
</tr>
<tr>
<td></td>
<td>12MP @ 15 fps + HD 720p @ 12/15 fps + HD 720p @ 12/15 fps + D1 @ 12/15 fps (PAL/NTSC)</td>
</tr>
<tr>
<td>Bit Rate Control</td>
<td>CBR (64 – 20,480 Kbps) and VBR</td>
</tr>
<tr>
<td>S/N Ratio</td>
<td>&gt;50dB (AGC off)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lens</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Lens Type</td>
<td>1.29mm hemispheric F2.4 lens with True Day/Night</td>
</tr>
<tr>
<td>Viewing Angle</td>
<td>190°</td>
</tr>
</tbody>
</table>
### Operation

<table>
<thead>
<tr>
<th>Feature</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brightness</td>
<td>Manual</td>
</tr>
<tr>
<td>Exposure Control</td>
<td>Auto/Manual</td>
</tr>
<tr>
<td>Sharpness</td>
<td>Manual</td>
</tr>
<tr>
<td>Contrast</td>
<td>Manual</td>
</tr>
<tr>
<td>Hue</td>
<td>Manual</td>
</tr>
<tr>
<td>White Balance</td>
<td>Auto/ATW/One-Push/Manual</td>
</tr>
<tr>
<td>Gain (AGC)</td>
<td>Automatic</td>
</tr>
<tr>
<td>Backlight Compensation</td>
<td>On/Off</td>
</tr>
<tr>
<td>Digital Zoom</td>
<td>Supported (x2 to x10)</td>
</tr>
<tr>
<td>Wide Dynamic Range (WDR)</td>
<td>On/Off + 3 levels</td>
</tr>
<tr>
<td>Noise Reduction</td>
<td>3DNR: On/Off + 3 levels (with Latitude), On/Off + 3 levels (without Latitude); 2DNR (On/Off); ColorNR (On/Off + 3 levels)</td>
</tr>
<tr>
<td>Privacy Mask (Video Mask)</td>
<td>Web interface: On/Off. Up to five embedded web interfaces are supported in the streaming video output, but are not supported by Latitude. In the Latitude interface, the Privacy Mask is independent of the camera's on-screen display and is not embedded.</td>
</tr>
<tr>
<td>IR Function</td>
<td>Day/Night (Auto/On/Off/Smart)</td>
</tr>
</tbody>
</table>

### Audio

<table>
<thead>
<tr>
<th>Feature</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compression</td>
<td>G.711 (µLAW and ALAW), G.726, and AAC</td>
</tr>
<tr>
<td>Two-way Audio</td>
<td>1x Audio-in/1x Audio-out</td>
</tr>
<tr>
<td>Speaker/Mic</td>
<td>Built-in</td>
</tr>
</tbody>
</table>

### Alarm

<table>
<thead>
<tr>
<th>Feature</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>1x 5V 10kΩ pull up dry contact</td>
</tr>
<tr>
<td>Output</td>
<td>1x Photo Relay Output 300V DC/AC @ 130mA maximum</td>
</tr>
</tbody>
</table>

### S/N Ratio

<table>
<thead>
<tr>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;50dB (AGC off)</td>
</tr>
</tbody>
</table>

### Languages

<table>
<thead>
<tr>
<th>Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>English, German, Spanish, French, Italian, Japanese, Korean, Portuguese, Russian, Simplified Chinese, and Traditional Chinese</td>
</tr>
</tbody>
</table>

### MicroSD Card Recording

<table>
<thead>
<tr>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 128GB Class 10 microSDXC card (card not included)</td>
</tr>
</tbody>
</table>
### Analytics

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motion Detection</td>
<td>On/Off, plus sampling pixel interval, detection level, sensitivity level, and time interval settings.</td>
</tr>
<tr>
<td>Regions of Interest</td>
<td>Web interface: Configurable up to 10 ROI masks. Latitude interface: Configurable up to six ROI masks.</td>
</tr>
<tr>
<td>Motion Metadata</td>
<td>Streaming and recorded video includes per frame level motion metadata. Motion metadata is archive searchable by ROI via the Latitude Control Center user interface</td>
</tr>
<tr>
<td>Triggered Actions</td>
<td>Notifications, On-Event Recording and Relay Output Command. Includes configurable alarms and broad range of recording on detection of video and snapshots</td>
</tr>
<tr>
<td>Tampering Alarm</td>
<td>On/Off, plus duration, on-event notification, recording to SD card, recording to NAS, and more are supported as events in Latitude.</td>
</tr>
</tbody>
</table>

### IR Illuminator

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Working Distance</td>
<td>5 meters (16 ft.) at 360°</td>
</tr>
<tr>
<td>Wavelength</td>
<td>850nm</td>
</tr>
<tr>
<td>LEDs</td>
<td>4</td>
</tr>
</tbody>
</table>

### Network

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>10/100/1000Mbps Ethernet, Auto-sensing, Full/Half-Duplex</td>
</tr>
<tr>
<td>Video Streaming</td>
<td>RTSP/RTP</td>
</tr>
<tr>
<td>Event Notification</td>
<td>HTTP, FTP, SMTP</td>
</tr>
<tr>
<td>Event Storage</td>
<td>Recordings and snapshots</td>
</tr>
<tr>
<td>Password Levels</td>
<td>User and Administrator</td>
</tr>
<tr>
<td>Security</td>
<td>HTTPS, IP Filter, IEEE 802.1x</td>
</tr>
<tr>
<td>Firmware Upgrade</td>
<td>Flash memory for upgrading camera firmware via HTTP</td>
</tr>
<tr>
<td>Operating Systems</td>
<td>Windows 7, 8, and 8.1 (64-bit versions)</td>
</tr>
<tr>
<td>Internet Browser</td>
<td>Microsoft Internet Explorer 10 (32-bit version) and above</td>
</tr>
<tr>
<td>User Accounts</td>
<td>20</td>
</tr>
</tbody>
</table>
### Mechanical

<table>
<thead>
<tr>
<th>Connectors</th>
<th>Power</th>
<th>2-pin terminal block</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Ethernet</td>
<td>RJ45</td>
</tr>
<tr>
<td></td>
<td>Audio</td>
<td>1x Line-in and 1x Line-out 1.5mm audio jack</td>
</tr>
<tr>
<td></td>
<td>Alarm</td>
<td>4-pin terminal block with 2-pin alarm input and 2-pin relay output</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LED Indicator</th>
<th>Power, Link, ACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress Protection</td>
<td>IP66</td>
</tr>
<tr>
<td>Vandal Resistant Rating</td>
<td>IK10</td>
</tr>
<tr>
<td>Bubble Rating</td>
<td>IK10 Vandal-Resistant Polycarbonate</td>
</tr>
<tr>
<td>Bubble F-Stop</td>
<td>Clear Bubble: F0.0, Smoke Bubble (optional): F1.0</td>
</tr>
<tr>
<td>Pan/Rotate/Tilt</td>
<td>355° pan/ ±100° rotate/80° tilt</td>
</tr>
<tr>
<td>Mechanical IR Cut Filter</td>
<td>Included</td>
</tr>
<tr>
<td>Heater</td>
<td>Included</td>
</tr>
</tbody>
</table>

### Power

<table>
<thead>
<tr>
<th>Source</th>
<th>12VDC (± 10%)/PoE (802.3af Class 0)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Consumption</td>
<td>8W (12VDC)/10W (PoE)</td>
</tr>
</tbody>
</table>

### Physical

<table>
<thead>
<tr>
<th>Dimensions</th>
<th>Ø163 x 104mm (6.43 x 4.1”)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weight</td>
<td>0.95 kg (2.1 lbs.)</td>
</tr>
</tbody>
</table>

### Environmental Specifications

<table>
<thead>
<tr>
<th>Operating Temperature</th>
<th>-10°C to 50°C (14°F to 122°F) with heater</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>-10°C to 50°C (14°F to 122°F) for cold start with POE</td>
</tr>
<tr>
<td>Operating Humidity</td>
<td>10 to 90% relative humidity (non-condensing)</td>
</tr>
</tbody>
</table>

### General

<table>
<thead>
<tr>
<th>Regulatory</th>
<th>US/Canada</th>
<th>ANSI C63.4-2009 (FCC 47 CFR Part 15, Subpart B, Class A; CISPR Pub. 22); UL 60950-1; ICES-003 Issue 5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>International</td>
<td>EN 50130-4; EN 55022-1998 Class A; EN 55032; EN 60950-1; IEC 60950-1:2005+A1:2009; EN 61000-3/2/3; EN 61000-4-2/3/4/5/6/8/11; EN 61000-6-4 (Class A); AS/NZS CISPR22 (Class A); RoHS; WEEE</td>
</tr>
<tr>
<td>Warranty</td>
<td>Four-year limited warranty</td>
<td></td>
</tr>
</tbody>
</table>
10.2 Internet Security Settings on Internet Explorer

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

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

To set the default Internet security level

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

   ![Command Bar Toolbar – Select Internet Options](image)

3. In the Internet Options window that appears, select the Security tab.
4. Select ![Internet](image) in Select a zone to view or change security settings.
5. If the settings are not defined as default, select Default Level and move the Allowed levels for this zone slider to Medium-high and select OK.

   ![Internet Options > Security Tab](image)

6. Close all browsers and reopen so that the settings take effect.
Configuring ActiveX Controls and Plug-in Settings

To create a custom level

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

   ![Command Bar Toolbar – Internet Options](image)

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

4. If not already selected, select Internet, then select Custom Level. The Security Settings-Internet Zone dialog box opens.

5. In the Security Settings-Internet Zone dialog box, under ActiveX controls and plug-ins set all the following options to Enable or Prompt:

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

   ![Security Settings-Internet Zone Screen](image)

6. Click OK to accept the settings and close the Security tab.
7. Click OK to close the Internet Options window.
8. Close the browser window and restart IE again to access the camera.
10.3 Installing UPnP Settings on Internet Explorer

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

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

1. Click (Start) and select Control Panel.
2. Click Network and Internet.
3. Click Network and Sharing Center.
4. Click Change advanced sharing settings.
5. Expand the Home or Work node, select Turn on network discovery.
6. Click Save Changes.
Note:
Network discovery requires that the DNS Client, Function Discovery Resource Publication, SSDP Discovery, and UPnP Device Host services are started, that network discovery is allowed to communicate through Windows Firewall, and that other firewalls are not interfering with network discovery.

To enable UPnP discovery in Windows 10

1. Open the Control Panel.
2. Click Network and Sharing Center.
3. Click Change advanced sharing settings.
4. In the Network discovery and File and printer sharing sections, select Turn on network discovery.
5. Click Save Changes.
To check that the UPnP Device Host services are running

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

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

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

**To delete temporary Internet files**

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

   ![Command Bar Toolbar – Select Internet Options]

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

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

   ![Delete Browser History Dialog Box]
10.5 Installing and Deleting the Web Player

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

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

To install the Quasar Player

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

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

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

2. In the **Control Panel**, click **Uninstall a program**.

3. From the installed program list, select **DVPlayer** or **DCViewer**.

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

5. If prompted to confirm the Uninstall, click **Yes**.

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

To clear your computer’s cache memory

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

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

3. From the **Delete Browsing History** dialog box, select **Preserve Favorites website data**, **Temporary Internet files and website files**, **Cookies and website data**, and **Tracking Protection**, **ActiveX Filtering** and **Do Not Track**.

4. Click **Delete**. The **Internet Properties** dialog box opens.

5. Click **OK**. Your computer's cache memory is deleted. After the cache is cleared, the Quasar Player installation wizard opens.

6. Follow instructions above to install the Quasar Player.
## 10.6 Network Settings

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

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

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

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>No network connection</td>
<td><strong>Hardware issues:</strong>&lt;br&gt; 1. Check that the network is working and the unit is powered on.&lt;br&gt; 2. Check that the network (Ethernet) cable is properly attached to the unit.&lt;br&gt; 3. Confirm that the network cables are not damaged and replace if necessary.&lt;br&gt;&lt;br&gt;<strong>IP Address issues:</strong>&lt;br&gt; 1. Change the default IP address/addresses of the unit.&lt;br&gt; 2. From the PC running the web browser, ping the unit IP address and confirm that it can be reached.&lt;br&gt; 3. Confirm that the network settings/firewalls are set according to the requirements.&lt;br&gt; 4. The camera might be located on a different subnet. Contact your IT administrator to get the IP address of the camera.</td>
</tr>
<tr>
<td>How do I find IP address of my unit?</td>
<td><strong>Possible Solution:</strong>&lt;br&gt; 1. Check the network DHCP server IP address assignments and lease.&lt;br&gt; 2. 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.</td>
</tr>
<tr>
<td>The IP address responds to a ping on the network from the workstation but does not show in the Discovery List</td>
<td><strong>Possible Solution:</strong>&lt;br&gt; 1. 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.&lt;br&gt; 2. Check the network port and ensure that it is working OK.&lt;br&gt; 3. Ensure that the switch ports provide the necessary power.</td>
</tr>
<tr>
<td>The unit IP address is in use by another computer (collision)</td>
<td><strong>Possible Solution:</strong>&lt;br&gt; 1. Check the DHCP settings. Obtain a new IP address using DHCP. Ensure this is a unique IP address.&lt;br&gt; 2. Alternatively, change the unit IP address after connecting to it directly (not through the system network).</td>
</tr>
</tbody>
</table>
## Appendices

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Solution</th>
</tr>
</thead>
</table>
| Cannot login to the camera                        | • Check the login user ID of the user or admin.  
• Check the login password of the user or admin.                                                                                             |
| No video image displayed on the main menu or the  | • Reset the browser security settings to the default value.  
• Check that the correct port was configured. The default port is 554.                                                                       |
| view menu of the web interface                    |                                                                                                                                                   |
| 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 | Adjust the White balance configuration to Auto. If the lighting in the scene is fixed, manually adjust the White balance to an acceptable image.     |
| indoor and outdoor lighting)                      |                                                                                                                                                   |
| 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. |
### 10.8 Acronyms and Abbreviations

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

The following mounting accessories are available from FLIR for installation of your Quasar Gen II CM-6212 Series Hemispheric IP Camera. For more information on available options, contact your FLIR sales representative or visit www.flir.com/security.

<table>
<thead>
<tr>
<th>Image</th>
<th>Part Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="cm-capx-ind-w" alt="Image" /></td>
<td>CM-CAPX-IND-W</td>
<td>Indoor wall mounting kit. Includes pendant cap with 18cm (7.1 in.) threaded wall mount bracket.</td>
</tr>
<tr>
<td><img src="cm-capx-ind-p" alt="Image" /></td>
<td>CM-CAPX-IND-P</td>
<td>Indoor pendant mounting cap. Ready for ¾” conduit or 1-1/2” threaded mount.</td>
</tr>
<tr>
<td><img src="cm-capx-out-w" alt="Image" /></td>
<td>CM-CAPX-OUT-W</td>
<td>Outdoor wall mounting kit. Includes sunshield and pendant cap with 18cm (7.1 in.) threaded wall mount bracket.</td>
</tr>
<tr>
<td><img src="cm-capx-out-p" alt="Image" /></td>
<td>CM-CAPX-OUT-P</td>
<td>Outdoor pendant cap. Includes 1-1/2” male pipe threaded mount and ¾” female EMT conduit compatibility.</td>
</tr>
<tr>
<td><img src="cm-rcsd-g2" alt="Image" /></td>
<td>CM-RCSD-G2</td>
<td>Recessed mounting kit. Included peel and stick template, top-mounted 4S electrical box attachment points. For maximum surface thickness of 42mm (1-3/4”).</td>
</tr>
<tr>
<td><img src="cm-smoke-62" alt="Image" /></td>
<td>CM-SMOKE-62</td>
<td>Smoked bubble cover. Full F-stop darkening of camera interior.</td>
</tr>
<tr>
<td>Image</td>
<td>Part Number</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><img src="Image1" alt="Image" /></td>
<td>CM-4S-62</td>
<td>4S electrical box mounting adapter. Rotates camera position by 45° when mounting to a 4S electrical box.</td>
</tr>
<tr>
<td><img src="Image2" alt="Image" /></td>
<td>CX-POLE-0</td>
<td>Pole Mount. Packaged with CX-AMRX-1 Mounting Bracket, CM-150-62 adapter, and CM-CAPX-IND-P or CM-CAPX-OUT-P.</td>
</tr>
<tr>
<td><img src="Image3" alt="Image" /></td>
<td>CM-F150-62</td>
<td>1-1/2” threaded quarter-turn adapter.</td>
</tr>
</tbody>
</table>