Quasar Gen III

User and Installation Guide

CM-6308-P1-I
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

Document History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>V.02</td>
<td>November, 2017</td>
<td>Initial Release</td>
</tr>
<tr>
<td></td>
<td>March, 2019</td>
<td>Firmware upgrade</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SD card min/max</td>
</tr>
<tr>
<td>V.05a</td>
<td>June, 2019</td>
<td>PoE+ Minimum Rating 30W</td>
</tr>
<tr>
<td>Ver. 05d</td>
<td>February 24, 2020</td>
<td>Mounting instructions - Details on Waterproofing</td>
</tr>
</tbody>
</table>
Table of Contents

1. Document Scope and Purpose ........................................................................................................ 1
   1.1 Warnings, Cautions and Notes ...................................................................................... 2
   1.2 General Cautions and Warnings ................................................................................ 3
   1.3 Site Preparation - General .................................................................................... 4
   1.4 Accessing Camera Information from the Web ..................................................... 5
2. Introduction .................................................................................................................................... 6
   2.1 Features .................................................................................................................. 7
   2.2 Package Contents ................................................................................................. 7
   2.3 Hardware Description ............................................................................................ 8
   2.4 System Requirements ........................................................................................... 9
3. Installation ..................................................................................................................................... 10
   3.1 Pre-Installation Checklist .................................................................................... 10
   3.2 Outdoor Mounting Recommendations .................................................................. 10
   3.3 Resetting the Camera and Configuring the microSD Card ...................................... 11
   3.4 Powering the Camera .......................................................................................... 12
   3.5 Mounting and Positioning the Camera ................................................................. 13
   3.6 Changing the Lens Position from Wall Mode to Ceiling Mode ......................... 16
   3.7 Configuring Communication Settings ................................................................... 17
   3.8 Using DNA to Access the Camera ....................................................................... 21
   3.9 Configuring the Unit’s Initial IP Address ............................................................. 22
   3.10 Connecting the Camera to a Latitude VMS ......................................................... 27
4. Configuration and Operation ...................................................................................................... 28
   4.1 CM-6308 Web Interface ..................................................................................... 28
   4.2 Live View ............................................................................................................. 30
      4.2.1 Recording ........................................................................................................ 31
      4.2.2 Capturing a Picture .......................................................................................... 32
      4.2.3 Viewing Live Video from a Media Player ...................................................... 33
   4.3 Settings ............................................................................................................... 34
      4.3.1 System Tab .................................................................................................... 34
         4.3.1.1 Basic Configuration ................................................................................... 36
         4.3.1.2 User Accounts .......................................................................................... 42
         4.3.1.3 Network .................................................................................................... 45
         4.3.1.4 Events Source .......................................................................................... 58
         4.3.1.5 Events Handler ........................................................................................ 67
         4.3.1.6 Stitching .................................................................................................... 72
### Table of Contents

- 4.3.1.7 Display Sequence ................................................................. 74
- 4.3.1.8 270 Mode ................................................................. 74
- 4.3.2 Streaming Tab ................................................................. 76
  - 4.3.2.1 Video Settings ................................................................. 76
  - 4.3.2.2 Privacy Zone ................................................................. 84
  - 4.3.2.3 ROI ................................................................. 85
- 4.3.3 Camera Tab ................................................................. 85
  - 4.3.3.1 Exposure Screen ................................................................. 85
  - 4.3.3.2 Picture Adjustment ................................................................. 93
  - 4.3.3.3 White Balance ................................................................. 94
- 4.4 Logout ................................................................. 95

5. Appendices ................................................................. 96
- 5.1 Technical Specifications ................................................................. 97
- 5.2 Internet Security Settings on Internet Explorer ......................................................... 102
- 5.3 Installing UPnP Settings on Internet Explorer ......................................................... 103
- 5.4 Deleting Temporary Internet Files on Internet Explorer ......................................................... 107
- 5.5 Installing and Deleting the Web Player ......................................................... 107
- 5.6 Network Settings ................................................................. 113
- 5.7 Troubleshooting ................................................................. 114
- 5.8 Acronyms and Abbreviations ................................................................. 116
- 5.9 Fifth Imager - FLIR-CM-IMG5-63P ................................................................. 117
- 5.10 Mounting Accessories ................................................................. 118
1 Document Scope and Purpose

The purpose of this document is to provide instructions and installation procedures for physically connecting the Quasar Gen III CM-6308 unit. After completing the physical installation, additional setup and configurations are required before video analysis and detection can commence.

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

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

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

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

Disclaimer

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

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

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

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

Avis de non-responsabilité

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

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

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

Les spécifications et informations contenues dans ce guide sont sujettes à modification sans préavis.
1.1 Warnings, Cautions and Notes

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

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

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

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

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:

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

Attention:
- Le cache de l'unité est une partie essentielle du produit. Ne les ouvrez et ne les retirez pas.
- N'utilisez jamais l'unité sans que le cache soit en place. L'utilisation de l'unité sans cache présente un risque d'incendie et de choc électrique.
- Ne démontez pas l'unité et ne retirez pas ses vis. Aucune pièce se trouvant à l'intérieur de l'unité ne nécessite un entretien par l'utilisateur.
- Seul un technicien formé et qualifié est autorisé à entretenir et à réparer cet équipement.
- Respectez les codes et réglementations locaux, et assurez-vous que l'installation et l'utilisation sont conformes aux normes contre l'incendie et de sécurité.
Caution:
- Do not drop the camera or subject it to physical shock.
- Do not touch sensor modules with fingers. If cleaning is necessary, use a clean cloth with a bit of ethanol and wipe it gently. If the camera will not be used for an extended period of time, put on the lens cap to protect the sensor from dirt.
- Do not aim the camera lens at strong light, such as the sun or an incandescent lamp, which can seriously damage the camera.
- Make sure that the surface of the sensor is not exposed to a laser beam, which could burn out the sensor.
- If the camera will be fixed to a ceiling, verify that the ceiling can support more than 50 newtons (50-N) of gravity, or over three times the camera’s weight.
- The camera should be packed in its original packing if it is reshipped.

Caution:
To avoid damage from overheating or unit failure, assure that there is sufficient temperature regulation to support the unit’s requirements (cooling/heating). Operating temperature should be kept in the range -40° to 50°C (-40° to 122°F), with no more than 90% non-condensing humidity.

Attention:
Afin d'éviter tout dommage dû à une surchauffe ou toute panne de l'unité, assurez-vous que la régulation de température est suffisante pour répondre aux exigences de l'unité (refroidissement/chauffage). La température de fonctionnement doit être maintenue dans la plage (-40° à 50°C/-40° à 122°F), sans condensation d’humidité supérieur à 90%.

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

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

- 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 untrusted 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.

1.4 Accessing Camera Information from the Web

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

![QR Code to Access Camera Information](image)
2 Introduction

This User and Installation Guide is intended to help you physically install, configure settings for, and operate the CM-6308 indoor/outdoor 4x2KConvertible 180°/360° panoramic mini-dome IP camera. The camera is designed for operation in spaces that require video coverage of a wide area of interest.

The units feature the following sensor and lens:

<table>
<thead>
<tr>
<th>Image Sensor</th>
<th>4x 1/2.8” Progressive Scan BSI CMOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Pixels (H x V)</td>
<td>8MP (3840x2160)</td>
</tr>
<tr>
<td>Sensor resolution (pixels)</td>
<td>1920x1080</td>
</tr>
<tr>
<td>Field of View</td>
<td>3.6mm, 92°</td>
</tr>
<tr>
<td>Aperture</td>
<td>F2.0</td>
</tr>
</tbody>
</table>

The cameras support up to three streams at 8MP. Stream1 supports H.265 and H.264 compression only at 3840x2160/1440. Stream2 and Stream3 support H.265, H.265, and MJPEG compression with the following maximum performance:

<table>
<thead>
<tr>
<th>Stream Type</th>
<th>Stream1</th>
<th>Stream2</th>
<th>Stream3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single-stream</td>
<td>3840x1440 @ 30fps</td>
<td>3840x2160 @ 30fps with H.264 or 27fps with H.265</td>
<td>3840x2160 + 1920x1080 @ 15fps</td>
</tr>
<tr>
<td>Dual-stream</td>
<td>3840x1440 + 1920x720 @ 30fps</td>
<td>3840x2160 + 1920x1080 + 1280x720 + 720x576/480 @ 15fps</td>
<td>3840x2160 + 1280x720 + 720x576/480 @ 15fps</td>
</tr>
<tr>
<td>Triple-stream</td>
<td>3840x1440 + 1920x720 + 720x576/480 @ 30fps or 3840x1440 + 1280x480 + 1280x480 @ 20fps</td>
<td>3840x2160 + 1280x720 + 720x576/480 @ 15fps</td>
<td>3840x2160 + 1280x720 + 720x576/480 @ 15fps</td>
</tr>
</tbody>
</table>

The unit features True Day/Night (ICR) and an infrared LED illuminator. It also includes Audio Line-In, Audio Line-Out, Alarm-in, and Alarm-out connections, and a microSD card drive for storing recordings and snapshots. The camera is powered by an 802.3at PoE+ or 24VAC connection.
### 2.1 Features

- 4x 1/2.8" Progressive Scan BSI CMOS sensor
- True day/night (ICR)
- Shutter (True) WDR
- Built-in web server
- Motion detection event-driven alarms
- Gamma correction
- 802.1X and SSL/TLS security protocols
- Supports up to 128GB microSDXC card
- Alarm In/Out
- IP67 enclosure with IK10 vandal-proof protection

- Up to 8MP (3840x2160) at 25/30fps
- Infrared LED illuminator
- 3DNR image noise reduction
- Supports Internet Explorer, Edge, Chrome, and Firefox browsers
- Tampering detection and notifications
- White balance
- SNMP v1/v2c/v3 and SNMP traps
- UPnP support
- Audio Line-In/Line-Out

- Wall (180°) and Ceiling (360°) Operating Modes
- H.265, H.264 and MJPEG compression
- Backlight compensation
- HTTP streaming MJPEG
- Two regions of interest
- 8 privacy zones
- Up to 9 users
- ONVIF© Profile S & G
- Powered by 802.3at PoE+ (min 30W) or 24VAC

### 2.2 Package Contents

The unit package contains the following items:

<table>
<thead>
<tr>
<th>Quantity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CM-6308-P1-I mini-dome camera</td>
</tr>
<tr>
<td>1</td>
<td>Bag containing four screws and four plastic anchors</td>
</tr>
<tr>
<td>1</td>
<td>T20 Torx wrench</td>
</tr>
<tr>
<td>1</td>
<td>Drill template</td>
</tr>
<tr>
<td>2</td>
<td>Desiccants</td>
</tr>
<tr>
<td>1</td>
<td>2-pin power terminal connector</td>
</tr>
<tr>
<td>1</td>
<td>8-pin I/O terminal connector</td>
</tr>
<tr>
<td>1</td>
<td>3/4&quot; Rubber O-ring</td>
</tr>
<tr>
<td>1</td>
<td>CM-6308 Quick Install Guide</td>
</tr>
</tbody>
</table>

Related Information:

- DNA 2.2 User Manual (see Accessing General Camera Information)
- CM-CAPX-63P Pendant Mounting for Dome Camera Installation Guide
- CM-6308 Dessicants User Guide
2.3 Hardware Description

Dimensions

Connections

The CM-6308-P1-I camera various connectors on the printed circuit board.

Notes on Connectors:
1. The RJ45 jack connects to the network switch and supports an IEEE 803.3at PoE+ connection. It includes an LED that flashes green to indicate power on and network activity. The LED is not illuminated if there is no network activity.
2. An optional 24VAC supply supply can be connected to the two-pin terminal block connector.
3. Audio and alarm I/Os attach to the 8-pin terminal block connector.
4. The BNC connector supports video-out only when the camera is operating in 360 (Ceiling) Mode.
## 2.4 System Requirements

<table>
<thead>
<tr>
<th>Item</th>
<th>Minimum System Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Computer</td>
<td>Intel® Pentium® IV, 2.4GHz or higher with &gt;1GB RAM Monitor display with minimum 1024 x 768 resolution (NVIDIA GeForce 6 Series or ATI Mobility Radeon 9500)</td>
</tr>
<tr>
<td>Web Browser</td>
<td>Microsoft Internet Explorer 10 and above (32-bit version); Microsoft Edge 38 and above; Chrome v.55 and above; Firefox v.50 and above</td>
</tr>
<tr>
<td>Network Card</td>
<td>10Base-T (10 Mbps) or 100Base-TX (100 Mbps) operation</td>
</tr>
<tr>
<td>Viewer</td>
<td>ActiveX control plug-in for Internet Explorer; MJPEG viewer for Edge, Chrome, and Firefox</td>
</tr>
</tbody>
</table>
3  Installation

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

- Pre-Installation Checklist
- Outdoor Mounting Recommendations
- Resetting the Camera and Configuring the microSD card
- Powering the Camera
- Changing the Lens Position from Wall Mode to Ceiling Mode
- Mounting the Camera
- Connecting the Camera to the Network

3.1  Pre-Installation Checklist

Before installing the unit, make sure that:

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

![Caution]

To avoid damage from overheating or unit failure, assure that there is sufficient temperature regulation to support the unit’s requirements (cooling/heating). Operating temperature should be kept in the range -40° to 50°C (-40° to 122°F), with no more than 90% non-condensing humidity.

Afin d'éviter tout dommage dû à une surchauffe ou toute panne de l'unité, assurez-vous que la régulation de température est suffisante pour répondre aux exigences de l'unité (refroidissement/chauffage). La température de fonctionnement doit être maintenue dans la plage (-40° à 50°C/-40° à 122°F), sans condensation d'humidité supérieur à 90%.

3.2  Outdoor Mounting Recommendations

Following are additional considerations for outdoor installation:

- For outside wiring installation, always use weatherproof equipment, such as boxes, receptacles, connectors, etc.
- For electrical wiring, use the properly rated sheathed cables for conditions to which the cable will be exposed (for example, moisture, heat, UV, physical requirements, etc.).
- Plan ahead to determine where to install infrastructure weatherproof equipment. Whenever possible, ground components to an outdoor ground.
3.3  Resetting the Camera and Configuring the microSD Card

The camera includes a **microSD card drive** (1) and **reset button** (2) on the camera's printed circuit board.

**Note:** The camera is shipped without a microSDXC card. The card must be inserted in the camera's microSD slot (1) in order to locally store a snapshot or recording triggered by an event.

**To install a microSDXC card**
1. Format a microSDXC card (Min recommended 4GB, up to 128GB, Class 10) on your PC.
2. Insert the card into the card slot on the camera's printed circuit board (1).
3. Verify that the card status is displayed as mounted in the unit's **System > Events Handler > SD Card** screen.
4. Configure the camera to store snapshots and recordings from the **System > Events Source** screens.

**To reboot the camera**
1. Using a pointed tool, press the reset button (2) for approximately five seconds. The unit reboots.

**To restore factory defaults using the reset button**
1. Press the reset button (2) continuously for 30 seconds. The unit restores factory defaults.
3.4 Powering the Camera

This product is intended to be used with a Listed Power Adapter with LPS. The camera is powered by a PoE+ (802.3at) injector or optional external 24VAC power supply unit (PSU) (not included in the package).

- If using an external power supply, connect the power leads or two-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, rated to at least 30W.

System Connection

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

If the camera is connected to an incorrect power source, the camera will power up with limited features (MJPEG dark video displayed at 1 fps, SD card, IR LEDs, Heater, and USB port all disabled) and display a message to the user that the power level is inadequate.

By default, the camera is set to PoE+. If the camera detects insufficient levels, the camera may reboot up to 5 times in 20 minutes and enter a limited features state, as above. The user has an option on the Basic Configuration > Basic Operations page to manually set the camera Power option. The default is set to PoE+ and assumes that the PoE+ supply is rated to at least 30W. When using PoE+, the Auto setting should not be used.

Note: If the camera changes its power level, for example, by turning on IR LEDs or heater, it would consume additional power, and if that power is not available, it may change its power state to the limited features state or reboot several times, as described above.

Note:
An ITE PoE injector should be connected only to a PoE network inside a building and not routed outside the building.
Caution:

1. This product must be connected only to a PoE+ network.
2. The PoE+ supply's rated output is >0.52A.
3. The 24VAC supply's rated output should be >1.42A.
4. If the camera is installed for outdoor use, the PoE supply must be installed with proper weatherproofing.
5. As a Listed Power Unit, the PoE should be marked as “LPS” or “Limited Power Source”.
6. This product shall be installed by a qualified service person. Installation shall conform to all local codes.

Attention:

1. Ce produit doit être connecté uniquement à un réseau PoE+.
2. La puissance nominale de l'alimentation PoE est > 0.52A.
3. La puissance nominale de l'alimentation 24VCA doit être > 1.42A.
4. Si la caméra est installée pour une utilisation extérieure, l'alimentation PoE+ doit être installé avec l'étanchéisation appropriée.
5. Comme une unité d'alimentation «Listed», le PoE doit être marqué comme «LPS» ou «Limited Power Source».
6. Ce produit doit être installé par un technicien qualifié. L'installation doit se conformer à tous les codes locaux.

3.5 Mounting and Positioning the Camera

The CM-6308 4x2K Convertible 180º/360º panoramic mini-dome camera is designed to be installed on a wall for 180º coverage (operation in Wall Mode) or in the ceiling for 360º coverage (operation in Ceiling Mode). The camera is shipped with the lenses in position for wall mounting. See the following section for instructions how to change the lens position from Wall Mode to Ceiling Mode.

Tip

Be sure that there is a minimum distance of 6 meters (20 feet) between the camera and the region of interest when mounting the camera for operation in Wall Mode.
Before mounting the camera, place the supplied drill template over the installation surface.

To mount and position the camera

1. Verify that the operating temperature range is between -40°C ~ 50°C (−40° ~ 122°F), 0-90% relative humidity (non-condensing).
2. Be sure to have the required accessories and tools available.
3. Using the supplied Torx wrench, unscrew the four screws on the dome cover and remove the cover.
4. Place the supplied drill template over the installation surface.
5. Drill four holes into the surface.
6. Align the holes on the camera’s base plate with the drilled holes.
7. Screw the base into the installation surface.

Unscrew the cover over one of the cable conduits depending on where the cables must be routed (Base or Top)

1. To maximize water protection when using conduit, use the included rubber gland and add teflon tape to the threading.
2. Carefully puncture the rubber gland for each of the cables, and feed the system cables through. Unscrew the cover of the selected conduit, and position the gland in it. Use teflon tape to ensure waterproofing.

Attach the leads or connectors from the required system cables as follows:
1. Screw the lanyard from the dome cover onto the lanyard post on the camera base.
2. Align the IR contacts on the dome with the IR contacts on the camera base, and check the case markings to ensure that the case is correctly aligned for the IR illumination.
3. Replace the dome cover over the base and tighten the screws after all cables are inserted so that the base plate is flush with the surface.
Note:

The cameras have a circuit protection mechanism that is activated if the cover is removed while the IR LEDs are on.

If the IR LEDs are not operating:

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

3.6 Changing the Lens Position from Wall Mode to Ceiling Mode

The camera is shipped with the lenses mounted for 180° viewing (Wall Mode). The lens must be physically rotated for the camera to operate in 360° mode (Ceiling Mode). No change is required in the camera's user interface.

To rotate the lenses

1. Hold the two inner lenses together from the base and rotate them clockwise. Be sure to leave the protective lens caps on the lenses during this step.

2. Gently release the lenses until the spring is fully released.

3. Remove the lens caps. The camera reboots in Ceiling Mode (360° operation).
3.7 Configuring Communication Settings

To configure communication settings on the camera

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

2. If the network supports the default, open the DNA utility by running `dna.exe` which can be downloaded from the Camera Support page (see Accessing General Camera Information).

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.

![Windows Firewall Screen](image1)

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.

![Discovered IP Devices](image2)
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.

![DNA Assign IP – Use DHCP Dialog Box](image1)

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

8. To access DNA, do one of the following:
   a. For DHCP (not supported by Latitude):
      i. Select **Use DHCP**. Do not use for Latitude.
      ii. Click **Update** and wait for status.
   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 *admin*.

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

- If the **User Account Control** dialog box opens and requests you to install the `install.cab` file, **click Yes**.
- If the ActiveX installation is not successful after performing the previous step, in the Internet Explorer **Tools > Internet Options > Advanced > Security** section, select the **Allow software to run or install even if the signature is invalid** checkbox. Uncheck the checkbox after installing ActiveX. Then click **OK**.
If you are using ActiveX, but do not have the Microsoft Visual C++ 2008 Redistributable libraries installed on your PC, the following error message is displayed. In this case, download and install the vcredist_x86.exe file from the Internet, or contact your Network Administrator or FLIR Support.

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

### 3.8 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 2.2 User Manual, which can be downloaded from the Camera Support page (see Accessing General Camera Information), or see the DNA Help file.
3.9 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. Run the dna.exe file by clicking the [dna.exe](#) icon. (to download DNA, see Accessing General Camera Information ).
2. The DNA application opens and the device is displayed in the window.
3. Click on the unit in DNA’s Discover List. The CM-6308 **Login** window opens.
4. If the camera cannot connect to a DHCP server, the unit initializes with the default IP address (192.168.0.250).

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

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

6. Click **Login**. The camera’s web interface opens.
   - If your browser is Edge, Chrome or Firefox, the video is displayed in the Live View window.
   - If your browser is Internet Explorer, a message is displayed, requesting you to install a plug-in.

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

   **Installing Ariel Player**

   **MS Visual C++ 2008 Redistributable Error Message**
8. Click **Continue**. The `vcredist_x86.exe` information bar opens.

   ![Visual C Redistributable Plug-in Information Bar]

   - Click **Run**. The Microsoft Visual C++ 2008 Redistributable Setup wizard opens.

   ![Microsoft Visual C++ 2008 Redistributable Setup Wizard]

   - Click **Next**. The **License Terms** screen opens.

   ![Microsoft Visual C++ Redistributable License Terms Screen]

   - Select the **I have read and accept the license terms** check box.
Click **Install**. The **Setup Complete** screen opens.

![Microsoft Visual C++ Redistributable Setup Complete Screen]

Click **Finish**.

- If the Microsoft Visual C++ 2008 Redistributable libraries are installed on your PC, skip to the next step.

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

![Ariel Player Plug-in Information Bar]

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

![Corrupt/Invalid Signature]

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

![View Downloads Screen]
b. Right-click on the ArielPlayer.msi file.

Run Anyway Option

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

10. Click Run on the Ariel Player plug-in information bar.

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

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

1. 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.

DNA Assign IP - Use DHCP Screen

4. Uncheck Use DHCP.

5. Enter the unit’s default IP address (192.168.0.250), Subnet mask, and Gateway IP address in the respective field.

6. Click Update. The unit reboots with the new settings.

7. Click on the unit in DNA’s Discover List. The camera’s Login window opens. See Figure: Login Window.
8. Enter the default User Name (\textit{admin}) and Password (\textit{admin}).

\begin{table}[h]
\centering
\begin{tabular}{|l|}
\hline
\textbf{Note:} \\
\textbf{The user name and password are case-sensitive.} \\
\hline
\end{tabular}
\end{table}

9. Click \textbf{Login}. The camera’s web interface opens. See Figure: \textit{Web Interface}.

10. Click the on-screen message to install the Ariel Player plug-in. The Ariel Player Plug-in message is displayed. See Figure: \textit{Ariel Player Plug-in Download Information Bar}.

\section*{3.10 Connecting the Camera to a Latitude VMS}

1. Click \textbf{Physical View} on the sidebar.

2. On the Navigation Tree, click the system name.

3. From the Discovery tab, do the following:
   \begin{enumerate}
   \item Under \textit{Cameras and Encoders}, select \textit{FLIR}.
   \item Click \textbf{Save}.
   \item Click \textbf{Start Automatic Discovery}. The camera details are displayed in the Discovery table.
   \item If the camera was not discovered, click \textbf{Run Manual Discovery}.
   \item Enter the camera’s IP address, select Unit Type \textit{FLIR}. (On Latitude 8 and newer systems, \textit{Auto Detect} should be set)
   \item Click \textbf{OK}.
   \end{enumerate}

4. In the Discovery table, select the camera name.

5. In the Available Archivers list, click the Archiver name.

6. Click \textbf{Save}. The unit is attached.
4 Configuration and Operation

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

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

This section includes the following information:

- **CM-6308 Web Interface**
- **Live View**
- **System Tab**
- **Streaming Tab**
- **Camera Tab**
- **Logout**

### 4.1 CM-6308 Web Interface

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

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

1. Open the 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: **admin**) to log into the system. The unit’s web interface opens. See Figure: **Web Interface**.

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

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

6. Click **Allow**. The Windows Installer opens and the **Ariel Player Wizard** dialog box is displayed. Follow instructions in the **Configuring the Unit’s Initial IP Address** section.
7. Configure camera settings after setting the unit's IP address. After the player is installed, the video image is displayed in the browser's Live screen.

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

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

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

To the left of the **Live View** window, the View Mode buttons are displayed. All buttons are displayed in Internet Explorer browsers.

**Note:**

Only the **Snapshot** button is displayed in Microsoft Edge, Chrome, and Firefox.
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ActiveX/MJPEG Button</td>
<td>Click <strong>ActiveX</strong> to use Internet Explorer or click <strong>MJPEG</strong> to use Edge, Chrome, or Firefox. The button is displayed only with Internet Explorer.</td>
</tr>
<tr>
<td>Snapshot button</td>
<td>Click the 📸 button to take a snapshot.</td>
</tr>
<tr>
<td>Full screen button</td>
<td>Click the 📸 button to display the live view in full-screen mode. To switch back to Live View mode, right-click on the screen and click <strong>Normal Display</strong>, or press the ESC key on your keyboard. Displayed only with Internet Explorer.</td>
</tr>
<tr>
<td>Manual recording button</td>
<td>The button indicates the recording status: red when recording is On or gray when recording is Off. Displayed only with Internet Explorer.</td>
</tr>
<tr>
<td>Mic button</td>
<td>Click the <strong>Mic</strong> button to enable the local site to talk to the remote site. This function is available only to an Operator or Administrator. Click the button to switch it on/off. Displayed only with Internet Explorer.</td>
</tr>
<tr>
<td>Audio button</td>
<td>Click the <strong>Audio</strong> button to listen to the audio output through a loudspeaker. The button allows the user to listen to audio streaming over the web if (a) audio is enabled and (b) if an audio event is enabled and triggered by exceeding the threshold. Settings are configured on the Audio screen. Displayed only with Internet Explorer.</td>
</tr>
</tbody>
</table>

From the Navigation Bar, select one of these tabs:

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

### 4.2 Live View

**To start Live View**

1. From the Navigation Bar, click **Live View**. The Live View screen opens.

![Live Screen in 180° Mode](image)
2. From the toolbar, click the **Live** or **Settings** button for the desired action.

The following sections include the following topics:

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

### 4.2.1 Recording

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

**To start recording a Live View scene**

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

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

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

**To playback a Live View recording**

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

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

**To view a triggered event recording**

1. In your browser, enter the camera’s FTP address (`ftp://camera_ip/`).
2. Enter the Admin user name and password.
3. Open the folder for the event according to the type of event (motion detection, tampering, etc.). Files are displayed chronologically according to most recent date.
4. Select the file.
4.2.2 Capturing a Picture

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

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

**To capture a snapshot in Live View mode**

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

**To view a Live View snapshot**

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

Snapshots that are triggered by events (such as motion detection) are stored on the camera’s microSD card, which can store up to 64GB of data. The card is not included.

**To view a triggered event snapshot**

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

The Live View main stream and sub-stream can be viewed with a media player, such as VLC (download from http://www.videolan.org/vlc/index.html). Streams can be viewed for the three channels and two video encoding formats (H.264, H.265, and MJPEG).

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

To view a media stream with VLC

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

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

Note:
1. It is also possible to change the syntax on the RTSP page, although this is not recommended if the camera is attached to a VMS.
2. Verify that the resolution entered in URL string agree with the resolution set in the Streaming > Video Settings screen.
4. Click **Play**. The video stream is displayed in the media player. Audio will also be streamed.

4.3 **Settings**

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

4.3.1 **System Tab**

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

The CM-6308 includes the following **System** menu:
- **Note:**
  The **Stitching** tab is displayed and available only when the camera is operating in 180° (Wall) Mode.

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

<table>
<thead>
<tr>
<th>Basic Configuration</th>
<th>User Accounts</th>
<th>Network</th>
<th>Events Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events Handler</td>
<td>Stitching</td>
<td>Display Sequence</td>
<td>270 Mode</td>
</tr>
</tbody>
</table>
4.3.1.1 Basic Configuration

The Basic Configuration tab includes the following screens:

- **Date & Time**
- **Audio**
- **Firmware**
- **Basic Operations**
- **OSD**

### 4.3.1.1.1 Date & Time

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

To change the date and time:

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

   ![NTP Setting Section]

   a. Enter the following details in the NTP Setting section:
      - **Enable** – From the drop-down list, select *Manual* to set the NTP server manually, or *From DHCP Server* to set the time according to the network DHCP server.
      - **Server Address** – Enter the IP address for the NTP server.
      - **Synchronization Period** – Select a number between 1-24 for the frequency (in number of hours) that the camera will synchronize with the NTP time server (i.e., every one hour, every two hours, etc.).

2. In the Time Zone Setting section, from the Area drop-down list, select your local time zone.

3. Click Save. The new time is displayed in the *Current Camera Time* text box.
### 4.3.1.1.2 Audio

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

#### Basic Configuration > Audio Screen

**To enable Audio In settings**

1. From the **Source** drop-down list, select **Mic In** or **Line In**.
2. From the **Enable** drop-down list, select **ON**.
3. From the **Encoding** drop-down list, select **G.711 a-law**, **G.711 µ-law**, or **AAC**. The default is **AAC**.
4. From the **Level** drop-down list, select **High**, **Mid**, or **Low**.

**To enable Audio Out settings**

1. From the **Enable** drop-down list, select **ON**.
2. From the **Level** drop-down list, select **High**, **Mid**, or **Low**.

### 4.3.1.1.3 Firmware

The **Firmware** screen is used to upload new system firmware and FPGA firmware, as well to display the two firmware versions, hardware version, product name (model number), product serial number, product MAC address, and viewing mode (Ceiling or Wall mode).

#### Firmware Screen

**To update system firmware**

1. Click **Browse** to locate the firmware file.
   - **Note**: The folder includes a checksum file, which can be used to check file validity using the checksum validation software of your choice.
2. Select the file. The file name is displayed. For the system firmware, for example, `CM-6308-P1-I_20171107.bin`, for the FPGA firmware, for example, `flirpano_a7_1b021132_cs.bit`.
3. Upload each firmware file separately.
4. Click Upgrade. The upgrade process takes about three minutes. After the firmware has upgraded successfully, the camera reboots.

![Rebooting Complete Dialog Box]

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

4.3.1.1.4 Basic Operations

The Basic Operations screen is used for the following functions:

- Setting the TV format
- Enabling Analog-Out (360° Mode only)
- Manually setting power type
- Importing settings from another unit
- Exporting settings to another unit
- Downloading the system log
- Rebooting the camera
- Restoring partial factory defaults
- Restoring full factory defaults

![Basic Operations Screen-180° Mode]
Click Reboot to save configured settings.

Click Partial factory defaults to restore factory defaults, but retain network settings (IP address, netmask address, and gateway address), TV format, and image rotation settings.

Click Full factory defaults to restore factory defaults, including network settings.

**Caution:**
Clicking Full factory defaults causes the camera to lose all network settings.

**Attention:**
Sélection par Défaut Complet d’Usine entraîne la caméra de perdre tous les paramètres réseau.

### To select the TV format

1. Click Basic Configuration > Basic Operations. The Basic Operations screen is displayed.
2. From the drop-down list, select NTSC or PAL. The default is NTSC.

### To enable TV Out (Analog video output)

1. When operating in 360° Mode only, from the TV Out drop-down list, select Full, 4:3, or 16:9.

**Note:**
Analog video output is available only when the resolutions are equal to or lower than 3840x2160, 1280x720, and 1280x720 on Stream1, Stream2, and Stream3 respectively.

### To select power type

1. From the drop-down list select Auto or PoE+. The default is Auto

**Note:** For more information on the Power Type, see Powering the Camera
To import a setting
1. Click **Browse** to select the file.
2. Click **Import** to upload the file.

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

To download the System Log
1. Click **Download Log**.

To reboot the camera
1. Click **Reboot**. The camera reboots. After the reboot finishes, a popup window opens with the message “Rebooting completed”.
2. Click **OK**. The browser is refreshed.

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

**Note:**
Clicking **Partial factory defaults** restores all factory defaults except network settings.

2. Click **OK**. The browser is refreshed.

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

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

2. Click **OK**. The browser is refreshed.
4.3.1.1.5 OSD

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

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

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1x1</td>
<td>2x1</td>
<td>3x1</td>
<td>4x1</td>
<td>5x1</td>
<td>6x1</td>
<td>7x1</td>
<td>8x1</td>
<td>9x1</td>
<td>10x1</td>
</tr>
<tr>
<td>2</td>
<td>1x2</td>
<td>2x2</td>
<td>3x2</td>
<td>4x2</td>
<td>5x2</td>
<td>6x2</td>
<td>7x2</td>
<td>8x2</td>
<td>9x2</td>
<td>10x2</td>
</tr>
<tr>
<td>3</td>
<td>1x3</td>
<td>2x3</td>
<td>3x3</td>
<td>4x3</td>
<td>5x3</td>
<td>6x3</td>
<td>7x3</td>
<td>8x3</td>
<td>9x3</td>
<td>10x3</td>
</tr>
<tr>
<td>4</td>
<td>1x4</td>
<td>2x4</td>
<td>3x4</td>
<td>4x4</td>
<td>5x4</td>
<td>6x4</td>
<td>7x4</td>
<td>8x4</td>
<td>9x4</td>
<td>10x4</td>
</tr>
<tr>
<td>5</td>
<td>1x5</td>
<td>2x5</td>
<td>3x5</td>
<td>4x5</td>
<td>5x5</td>
<td>6x5</td>
<td>7x5</td>
<td>8x5</td>
<td>9x5</td>
<td>10x5</td>
</tr>
<tr>
<td>6</td>
<td>1x6</td>
<td>2x6</td>
<td>3x6</td>
<td>4x6</td>
<td>5x6</td>
<td>6x6</td>
<td>7x6</td>
<td>8x6</td>
<td>9x6</td>
<td>10x6</td>
</tr>
<tr>
<td>7</td>
<td>1x7</td>
<td>2x7</td>
<td>3x7</td>
<td>4x7</td>
<td>5x7</td>
<td>6x7</td>
<td>7x7</td>
<td>8x7</td>
<td>9x7</td>
<td>10x7</td>
</tr>
<tr>
<td>8</td>
<td>1x8</td>
<td>2x8</td>
<td>3x8</td>
<td>4x8</td>
<td>5x8</td>
<td>6x8</td>
<td>7x8</td>
<td>8x8</td>
<td>9x8</td>
<td>10x8</td>
</tr>
<tr>
<td>9</td>
<td>1x9</td>
<td>2x9</td>
<td>3x9</td>
<td>4x9</td>
<td>5x9</td>
<td>6x9</td>
<td>7x9</td>
<td>8x9</td>
<td>9x9</td>
<td>10x9</td>
</tr>
<tr>
<td>10</td>
<td>1x10</td>
<td>2x10</td>
<td>3x10</td>
<td>4x10</td>
<td>5x10</td>
<td>6x10</td>
<td>7x10</td>
<td>8x10</td>
<td>9x10</td>
<td>10x10</td>
</tr>
</tbody>
</table>

To configure OSD settings

1. Click Basic Configuration > OSD. The OSD screen is displayed.
2. In the Basic Settings section, configure the following settings for OSD-1 and OSD-2:

- **Enable** – From the drop-down list, select one of the following:
  - **Date** – Enables you to enter the date to display.
  - **Text** – Enables you to enter the time to display.
  - **OFF** – Disables the OSD function. This is the default setting.
- **Background Color** – From the drop-down list, select Black or Transparent (default setting).
- **Text Color** – From the drop-down list, select Black or White (default setting).
- **Location X** – Move the slider from 1 to 10 to set the location on the screen for the OSD. The default setting is 1.
- **Location Y** – Move the slider from 1 to 10 to set the location on the screen for the OSD. The default setting is 1.

3. In the Event section, configure the following settings in case an event occurs:

- **Background Color** – From the drop-down list, select Black or Transparent (default setting).
- **Text Color** – From the drop-down list, select Black or White (default setting).
- **Location X** – Move the slider from 1 to 10 to set the location on the screen for the OSD. The default setting is 1.
- **Location Y** – Move the slider from 1 to 10 to set the location on the screen for the OSD. The default setting is 1.

4. Click **Save** when finished.

### 4.3.1.2 User Accounts

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

![User Accounts-Account Setting Screen](image)

**Note:**

1. User Name and Password can include up to 16 characters, including '0' to '9', 'a' to 'z', 'A' to 'Z', '!', '@', '^', '&', '_', and '@'.
2. The user name and password are case-sensitive.
The following privileges are assigned to each access level:

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

**To modify default Administrator credentials**

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

   ![Default Administrator Access Level Dialog Box](image)

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

**To add a new operator or user**

1. Click the empty row.

   ![Add User Dialog Box](image)

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

   ![Empty Access Level Dialog Box](image)
3. Select *Operator* or *User*, and enter the User Name and Password.

   ![Filled Access Level Dialog Box](image)

   **Filled Access Level Dialog Box**

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

   ![Updated Account Setting List](image)

   **Updated Account Setting List**

**To modify an operator or user**

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

**To delete an operator or user**

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

The Network tab includes the following screens:

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

### 4.3.1.3.1 General

The General screen is used for configuring most network settings. Click Save after you finish configuring the settings.

![Network > General Screen](image)

**To configure basic settings**

1. In the Basic Settings section, do the following:
   a. In the Device Name text box, enter a friendly name for the camera.
   b. In the HTTP Port text box, enter the port number. The range is from 1025 to 65535. The default port is 80.
   c. From the Enable LDAP drop-down list, select ON or OFF. If you select ON, verify that the information in Network > LDAP page is correct and that the LDAP server is online. The default is OFF.
2. Click **View** to view current network settings. The Internet Explorer **Basic Settings** dialog box opens, displaying network interface information, including Ethernet connection speed, Ethernet NIC MAC address, unit IP address, multicast address, and subnet mask. In the case of an IPv6 connection, the IPv6 address and IPv6 DNS address also are displayed.

![Internet Explorer Basic Settings Dialog Box](image)

**To configure IP settings**

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

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

To enable UPnP settings

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

   ![UPnP User Input Screen](image)

To enable SSL

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

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

To configure the MTU setting

1. In the TCP/IP section, set the MTU (Maximum Transmission Unit), which 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 1100 to 1500 bytes.

4.3.1.3.2 FTP Server

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

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

2. Click Save.

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

4.3.1.3.3 RTSP

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

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

![Note]

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

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

To configure the multicast address

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

![Note]

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

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

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

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

To use SNMP v2c
1. From the SNMP v2c section’s Enable drop-down list, select ON. The default is OFF.
2. In the Read Community String text box, enter the community name that has read-only access to all supported SNMP objects. The default value is public.
3. In the Write Community String text box, enter the community name that has read/write access to all supported SNMP objects (except read-only objects). The default value is private.
4. In the Trap Community String text box, enter the community to use when sending a trap message to the management system. The default value is public. Traps are used by the camera to send messages to the management system for important events or status changes.
5. Click Save.

To use SNMP v3
1. From the SNMP v3 section’s Enable drop-down list, select ON. The default is OFF.
2. From the Authentication Mode drop-down list, select MD5, SHA, or NONE (default).
3. If you select MD5 or SHA, from the Privacy Mode drop-down list, select AES, DES, or NONE (default).
4. Enter the User Name. The default is initial.
5. If you select MD5 or SHA, enter the Authentication Password in the Authentication Password text box.
6. The Privacy Password text box is disabled.
7. Click Save.
To use traps
1. In the Trap section, from the Mode drop-down list, select V1, V2C, V3, or OFF, according to the SNMP version that you select above. The default is OFF.
2. From the Heartbeat drop-down list, select ON or OFF. The default is OFF. When selected, this enables you to ping the VMS.
3. From the Event drop-down list, select ON to notify the VMS in case of an event. The default is OFF.
4. In the Target IP text box, enter the IP address of the Trap Host.
5. In the Heartbeat Interval text box, enter the interval of time in seconds for the camera to ping the VMS, for example, every 10 seconds. The range is 5-600. The default is 30.
6. Click Save.

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

4.3.1.3.5 802.1X

The 802.1X screen is used for enabling the camera to access a network protected by the 802.1X/EAPOL (Extensible Authentication Protocol over LAN) authentication protocol. Before using this function, you must register a user name and password for the 802.1X server and configure the authentication server. Contact the network administrator to obtain certificates, user IDs, and passwords.

To enable 802.1X
1. From the Protocol drop-down list, select one of the following: EAP-MD5, EAP-TTLS, MD5-PEAP, or NONE. The default is NONE.
2. Click Save. The Basic Settings screen for the selected protocol opens.

To enable EAP-MD5
1. Select EAP-MD5. The Basic Settings screen opens.
2. Enter the User Name and Password in the respective text box.
3. Do one of the following:
   - Click Save. The status is displayed as “Not yet” until the configuration is saved.
   - Click Test and Save to test and save the configuration.

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

**To enable EAP-PEAP**

1. Select EAP-PEAP. The Basic Settings screen opens. By default the Inner Authentication protocol is MSCHAPV2.
2. Enter the User Name and Password in the respective text box.
3. Click Browse to download the CA Certificate.
4. Do one of the following:
   - Click Save. The status is displayed as “Not Installed” until the configuration is saved.
   - Click Test and Save to test and save the configuration.
4.3.1.3.6 IP Filter

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

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

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

4.3.1.3.7 DDNS

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

**To use DDNS**
1. From the Enable drop-down list, select ON. The default is OFF.
2. From the Type drop-down list, select the DDNS service provider:
   - DynDNS: custom@dyndns.org (default)
   - No-IP: default@no-ip.com
   - Two-DNS: default@two-dns.de
   - FreeDNS: default@freedns.afraid.org
3. Enter the Host Name, User Name, and Password in the respective text box.
4. If you are using FreeDNS, the Hash text box also is displayed. Enter the Hash value, which is a hash of your user name and password. It is available from http://freedns.afraid.org.
5. Click **Save**.

### 4.3.1.3.8 LDAP

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

![Network > LDAP Screen](image)

**To configure LDAP basic settings**

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

**To configure group mappings**

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

**To configure authentication settings**

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

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

**Note:**
SSL is enabled from the Network > General screen.

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

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

To configure SSL settings

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

   ![Network > SSL Screen](image)

To obtain a self-signed certificate

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

   ![SSL Self-Signed Screen](image)

2. Enter the following information in the appropriate field. A definition of each of the required fields follows.
   - **Country Code** – Enter a two-letter combination code to indicate the specific country in which the certificate will be used. For instance, type “US” to indicate United States.
Province Name – Enter the local administrative region.

City Name – Enter other geographical information.

Common Name – Indicate the name of the person or other entity that the certificate identifies (often used to identify the website).

Organization Name – Enter the name of the organization to which the entity identified in Common Name belongs.

Organization Unit Name – Enter the name of the organizational unit to which the entity identified in the Common Name field belongs.

Email Address – Enter the email address of the person responsible for maintaining the certificate.

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

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

To request a certificate

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

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

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

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

3. Click Upload. The certificate is uploaded.
4.3.1.4 Events Source

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

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Audio</th>
<th>Motion</th>
<th>Network</th>
<th>Schedule</th>
<th>Tampering</th>
</tr>
</thead>
</table>

### 4.3.1.4.1 Alarm

The **Events Source > Alarm** screen is used for enabling an alarm when an event occurs and for defining actions when an alarm occurs. Actions include:

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

![Events Source > Alarm Screen](image)

#### To enable an alarm

1. Select the *Enable* checkbox. By default, *Enable* is not checked.

#### To select the type of alarm

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

#### To define the method to store a snapshot

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

#### To record an event on the camera

1. In the *Recording* section, select the *Record on Edge* checkbox to record a clip on the camera’s microSD card. By default, it is not checked.
2. Click *Save*. 
To enable sending an email notification

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

To define OSD text

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

To set the arming schedule

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

![Updated Arming Schedule Setting Section]

**Note:**
You must separate the hours and minutes with a colon, i.e. "02:00".

### 4.3.1.4.2 Audio

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

A number of actions can be taken, including:

- Defining the method for storing a snapshot in the camera’s microSD card
- Sending a snapshot of the event to an FTP server
- Storing a recording of the audio event in the camera’s microSD card
- Displaying text on-screen over the recording or snapshot
- Sending an email notification of the audio event
- Setting the arming schedule
Note:
In order to use this function, audio must be enabled from the **System > Basic Configuration > Audio** screen.

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

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

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

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

To enable using audio

1. Select the **Enable** checkbox. By default, audio is not enabled.

To set the audio level
1. Move the *Sound Intensity Threshold* slider to the desired level between 1-100.

**To enable sending an alarm**

1. Select the *Alarm Out* checkbox.

**To define the method to store a snapshot**

2. See instructions in the *Alarm* section.

**To record the event on the camera**

1. See instructions in the *Alarm* section.

**To enable sending an email notification**

1. See instructions in the *Alarm* section.

**To define OSD text**

1. See instructions in the *Alarm* section.

**To set the arming schedule**

1. See instructions in the *Alarm* section.
4.3.1.4.3 Motion

The Events Source > Motion screen is used for:

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

![Events Source > Motion Screen](image)

**Note:**
If the camera is attached to Latitude, motion detection configuration should be done from Latitude Admin Center, not from the web interface.

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

To configure motion zone area settings
1. From the Sensitivity drop-down list, select High, Medium, or Low. The camera reacts to slight changes in motion or brightness in the motion zone when set to High, while the camera reacts to big changes in brightness or motion when set to Low.

To define the method to store a snapshot
1. See instructions in the **Alarm** section.

**To record the event on the camera**
1. See instructions in the **Alarm** section.

**To enable sending an email notification**
1. See instructions in the **Alarm** section.

**To define OSD text**
1. See instructions in the **Alarm** section.

**To set the arming schedule**
1. See instructions in the **Alarm** section.

### 4.3.1.4.4 Network

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

- Sending an alarm if the network connection is lost or if there is a network conflict
- Recording an event in the camera’s microSD card
- Displaying text on-screen if the network connection is lost or if there is a network conflict

**Events Source > Network Screen**

In the *Lost Network Connection* and *Network Conflict* sections, configure the following settings:

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

**To enable sending an alarm**
1. Select the *Alarm Out* checkbox.
2. Click *Save*.

**To enable using audio**
1. Select the *Audio Out* checkbox. By default, audio is not enabled.
2. From the *Audio Sound* drop-down menu, select the number of the prerecorded message that you want to play. You can select from 10 different messages.

**To start recording**
1. In the *Recording* section, select the *Record on Edge* checkbox. By default, it is not checked.
2. Click *Save*. 
To activate the on-screen display

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

### 4.3.1.4.5 Schedule

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

- Setting a trigger interval for notifications
- Sending an alarm
- Defining the method for storing a snapshot in the camera’s microSD card
- Sending a snapshot of the event to an FTP server
- Recording an event in the camera’s microSD card
- Sending email notifications
- Setting the alarm schedule

![Events Source > Schedule Screen](image.png)

#### To set a trigger interval

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

#### To enable sending an alarm

1. See instructions in the **Network** section.

#### To enable using audio

1. See instructions in the **Network** section.

#### To define the method to store a snapshot

1. See instructions in the **Alarm** section.

#### To record the event on the camera

1. See instructions in the **Alarm** section.

#### To enable sending an email notification
1. See instructions in the Alarm section.

To set the arming schedule

- See instructions in the Alarm section.

4.3.1.4.6 Tampering

The Events Source > Tampering screen enables you to:

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

To enable tamper detection

1. Select Enable. By default, Enable is not checked.
2. From the Sensitivity drop-down list, select High, Medium, or Low.

To enable sending an alarm

1. See instructions in the Network section.

To enable using audio

1. See instructions in the Network section.

To define the method to store a snapshot

1. See instructions in the Alarm section.

To record the event on the camera

1. See instructions in the Alarm section.

To enable sending an email notification
1. See instructions in the Alarm section.

To define OSD text
1. See instructions in the Alarm section.

To set the arming schedule
1. See instructions in the Alarm section.

4.3.1.5 Events Handler

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

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

4.3.1.5.1 Email

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

Note:
Before configuring email settings, check that:

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

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

![Events Handler > Email Screen](image)

2. In the Basic Settings area, configure the following settings:
   a. **Authentication** – From the drop-down list, select one of the following authentication methods:
      - *No_Auth* – No email authentication method is used. This is the default setting.
      - *SMTP Plain* – PLAIN is the least secure of all the SASL (Simple Authentication and Security Layer) authentication mechanisms because the password is sent unencrypted across the network. The PLAIN authentication mechanism is described in RFC 2595.
      - *Login* – The Login mechanism is supported by Microsoft's Outlook Express and by some other clients.
      - *TLS-TTLS* – The Tunneled Transport Layer Security is used to tunnel an entire network stack to create a VPN.
   b. **Server Address** – In the text box, enter the email server IP address.
   c. **Port** – In the text box, enter the email server port number. The default port is 25.
   d. **User Name** – In the text box, enter the email server user name.
   e. **Password** – In the text box, enter the email server password.

3. In the Sender Settings area, configure the following settings:
   a. **Sender Email Address** – In the text box, enter the sender’s email address.
   b. **Attach Image** – From the drop-down list, select ON or OFF (default setting).

4. In the Email Address List section, do the following for each email address:
   a. Select the checkbox in the Enable column. By default, Enable is not checked.
   b. Enter the email address in the Email Address column.
   c. Click Save.
4.3.1.5.2 Alarm Out

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

There are two methods for enabling Alarm Out:

- **Pulse** – When this is selected, the user can select the Type Normally Open or Normally Closed.
  - When Normally Open is selected, new text boxes are displayed in which the user can specify the following:
    - **On Time** – amount of time (in seconds) that the alarm is ON
    - **Off Time** – amount of time (in seconds) between ON states
    - **Count** – the number of frames for the post-trigger buffer
  - When Normally Closed is selected, these text boxes are not displayed, the alarm output is activated for the specified duration (On Time) during which the output opens. The same settings are displayed as on the Normally Open setting.
- **Normal** – When this is selected, a new field (Post Duration) is displayed. The Post Duration time determines the length of time that the alarm is triggered. It can be set to Infinite (the alarm is active until deactivated) or set to 5, 10, 15, or 30 seconds.

4.3.1.5.3 FTP

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

1. In the Server Address text box, enter the FTP server IP address.
2. In the Port text box, enter the email server port number.
3. In the User Name text box, enter the FTP server user name.
4. In the Password text box, enter the FTP server manager’s password.
5. From the Mode drop-down list, select Active or Passive (default setting). In passive mode, FTP
   the client initiates both connections to the server, solving the problem of firewalls filtering the
   incoming data port connection to the client from the server. In order to support passive mode
   FTP on the server-side firewall, the following communication channels must be opened:
   - FTP server’s port 21 from anywhere (client initiates connection)
   - FTP server’s port 21 to ports > 1023 (server responds to client’s control port)
   - FTP server’s ports > 1023 from anywhere (client initiates data connection to
     random port specified by server)
   - FTP server’s ports > 1023 to remote ports > 1023 (server sends ACKs and
     data to client’s data port)
6. Click Save.

4.3.1.5.4 Recording Settings

The Recording Settings screen is used to configure recording settings.

To configure recording settings

1. From the Record Status drop-down list, select Video or Audio and Video.
2. From the Record Status drop-down list, select One Shot (default) or Continuous.
   - If you select One Shot, do the following:
     a. In the Clip Duration text box, enter a value from 5 to 10 seconds.
     b. In the Clip Size text box, enter a value from 10 to 20 MB.
• If you select Continuous, in the Clip Size text box, enter a value from 10 to 20 MB.

3. Click Save.

4.3.1.5.5 SD Card

The SD Card screen is used for configuring the microSD card. The card status is displayed in the Mount Status row. The status is displayed as notMounted if the card is not installed. If the card is installed, as mounted is displayed as is the card’s capacity and free space.

Note:
The unit is shipped without a microSD card. The camera accepts microSDXC cards up to 128GB, Class 10.

To configure the microSD card
1. From the Overwrite drop-down list, select ON. The default is OFF.
2. Click Save.

4.3.1.5.6 Snapshot

The Snapshot screen is used for configuring snapshot settings.
To configure snapshot settings

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

### 4.3.1.5.7 Sound

The **Sound** screen enables you to upload up to 10 small PCM audio files. These sound files can be triggered upon any event that is set in the **Events Source** section. For example, you can trigger one warning recording that alerts an intruder that he has been detected and then a stronger warning to not to proceed if he has not left the scene. The file will be played when the audio is enabled on the **Sound** screen and the triggering event occurs.

![Sound Screen](image)

### 4.3.1.6 Stitching

The **Stitching** screen is used to optimize the stitching of the images from the four lenses into a single seamless picture when operating in 180° (Wall) mode. It is possible to create three user-defined stitching profiles. The gain and the vertical position of each of the four lenses can be configured separately. By default, Lens 1 is selected first. Each lens is highlighted in blue when selected.

![Stitching Screen](image)

**Note:**
The **Stitching** screen is available only when the camera is operating in 180° (Wall) Mode.
To stitch four images into one picture

1. In the Profile section, select *Current Profile 1, 2, or default*. You can enter a friendly name for the profile by clicking the edit icon.
2. From the drop-down menu, select the *Lens Index* (1-4). This is the number of the lens, counting from left to right.
3. Move the *Gain Offset* slider to a value between -10 to 10. The default is 0.
4. On the control pad, move the *Up* and/or *Down* arrows so as to align the image with the image in the adjacent lens. The position is indicated in the *Position Y* text box.
5. Click *Revert* to return to the previously set profile.
6. Click *Default* to return to the factory default setting.
7. Click *Save*. The camera reboots.

**Note:**

1. The video frame rate is set to 12fps when using Stitching mode. After exiting the *Stitching* screen, the video frame rate returns to the previous setting.
2. It takes about 30 seconds to stitch an image and several minutes to save a stitched image.
3. The video stops while saving the image.
4. Stitching is not supported when the Exposure Mode is set to *Shutter WDR* on the *Camera > Exposure* screen.
   If the camera is set in *Shutter WDR* mode and the user accesses this page, the exposure mode changes temporarily to *Auto Shutter* mode. When the user leaves the page, the camera returns to the previous *Shutter WDR* mode automatically.
4.3.1.7 Display Sequence

Display Sequence allows the user to rearrange the order of the scenes displayed when the camera is in 360 mode.

1. On the bottom right, select which camera scene you would like to display in which square (use reference of sequence at the bottom of the webpage)

2. Click Save

3. Click Default to set the scenes back to their original configuration.

4.3.1.8 270 Mode

270 Mode allows the user to disable one of the camera scenes while in 360 mode. Eg. if the camera is mounted in a corner, blocking one of the lenses, the user can disable that lens

1. Click on the desired lens number to disable (sequence listed at the bottom of the webpage)
2. Click Save
4.3.2 Streaming Tab

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

4.3.2.1 Video Settings

The Video Settings screen is used for configuring the streams and such video parameters as resolution; video compression type and related settings; quality of service; and frame rate. Additional settings are available when using H.265 and H.264 compression.
4.3.2.1.1 Configuring Video Settings

To configure video settings

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

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

   **Note:**
   Stream1 supports 3840 x 2160 @ 25 fps only when operating with D1 in Ceiling Mode with two streams.

2. In the Stream1 section, configure the following settings:
   
   a. From Resolution drop-down list, select the desired resolutions. The default resolution is 3840x2160/1440. See Video Resolutions for available resolutions.
   
   b. In the DSCP text box, enter a value between 0-63. The default DSCP value is 0 (DSCP disabled).

      The DSCP (Differentiated Services Code Point) value defines the priority level or QoS (Quality of Service) for the specified type of traffic. The higher the value that is entered, the higher the priority, which reduces network delay and congestion. The camera supports the Video DSCP class, which consists of applications such as HTTP, RTP/RTSP, and RTSP/HTTP.

   **Note:**
   Remember to synchronize the QoS setting of the camera with the network router.

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

   d. From the Rate Control drop-down list, select CBR or CVBR. The default is CBR.

      - Select CBR (Constant Bit Rate) if you are monitoring simple scenes. CBR uses more storage capacity than CVBR. It wastes storage on simple scenes, while not allocating enough storage for complex sections (resulting in degraded quality). Move the slider to a number between 64 and 20000 bits per second. The default settings are 2925 kbps in Stream1, 691 kbps for Stream2, and 442 kbps for Stream3. The higher the bit rate, the better the image quality. Set the maximum bit rate high enough to allow for a high instantaneous bit for more complex video. A higher bit rate consumes more storage space.

      - Select CVBR (Constrained Variable Bit Rate) to enable greater control over image parameters. CVBR uses less storage capacity than CBR. This is helpful in complex scenes which use more bits than simple scenes. CVBR is desirable if you want an optimum bit rate from frame-to-frame with a relatively predictable file size. Continue with the following steps.
a. Set the Max Bit Rate to a value between 64 to 20000. The default settings are H.264 at 2925 kbps for Stream1, 691 kbps for Stream2, and 375 kbps for Stream3. The higher the bit rate, the better the image quality. Set the maximum bit rate high enough to allow for a high instantaneous bit for more complex video. A higher bit rate consumes more storage space.

b. Set the Encoding Priority. This function enables the user to adjust the quality of the picture along a single axis. The slider ranges from 1 (low bit rate) to 10 (high picture quality). The default setting is 7.

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

e. From the Compression drop-down list, select H.265 or H.264 according to the required image quality and storage limitations. The default is H.264.

f. From the Profile drop-down list, select a profile: High Profile or Main Profile. Each profile targets specific classes of applications.

Note:
Only Main Profile is available with H.265.

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

- Main Profile (MP)
  This profile provides improved picture quality at reduced bandwidths and storage costs and is becoming more common as the camera processors (DSPs) become more able to handle the processing load.

g. Set the GOP to a value from 1-60 (NTSC) or 1-50 (PAL). The default is 30 for NTSC and 25 for PAL (one I-Frame transmitted every second).

The GOP is a group of successive pictures within a coded video stream. Each coded video stream consists of successive GOPs. GOP structure, specifies the order in which intra-coded frames and inter-coded frames are arranged.

The GOP uses I-Frames (Intra-coded Frames), which are static image files (frames), as a reference for efficient H.264 video compression. Transmitted video frames are compared to the I-Frame as they are transmitted. Video quality is higher when the interval between I-Frames is shorter, but the video needs more network capacity. When the interval between I-Frames is longer, the video transmission uses less bandwidth, but the video quality is lower.

3. Repeat the above steps for Stream2 and Stream3.

- If you require H.265 or H.264 compression, follow the instructions above.
- If you require MJPEG compression, do the following:
  a. From Resolution drop-down list, select the desired resolutions. The default is the highest resolution for each stream.
b. From the Compression drop-down list, select MJPEG according to the required image quality and storage limitations. The Quality Level drop-down list is displayed.

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

d. In the DSCP text box, enter a value between 0-63. See instructions above for Stream1.

e. Set the Frame Rate slider to the desired value. See instructions above for Stream1.

4. Click Save.

4.3.2.1.1.1 Video Resolutions-180° Mode

The camera supports up to three simultaneous streams, with up to 8MP on Stream1, Full HD 1080p on Stream2, and HD 720p on Stream3.

**Note:**

1. Stream1 supports MJPEG on all resolutions except 3840x1440.
2. The frame rate is limited to 12 fps when True WDR is enabled.
3. MJPEG does not support resolutions above 2MP.

The following resolutions are available:

<table>
<thead>
<tr>
<th>H.265/H.264-Only</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PAL</strong></td>
<td><strong>NTSC</strong></td>
</tr>
<tr>
<td>3840 x 1440 (25 fps)</td>
<td>3840 x 1440 (30 fps)</td>
</tr>
<tr>
<td>1920 x 720 (25 fps)</td>
<td>1920 x 720 (30 fps)</td>
</tr>
<tr>
<td>1280 x 480 (25 fps)</td>
<td>1280 x 480 (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>H.265/H.264/MJPEG + H.265/H.264/MJPEG (NTSC)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Stream1</strong></td>
<td><strong>Stream2</strong></td>
</tr>
<tr>
<td>3840 x 2160 (30 fps @ H.264/H.265)</td>
<td>1920 x 720 (30 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td>1280 x 480 (30 fps @ H.264/H.265/MJPEG)</td>
<td>1280 x 480 (30 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td>720 x 480 (30 fps @ H.264/H.265/MJPEG)</td>
<td>720 x 480 (30 fps @ H.264/H.265/MJPEG)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>H.265/H.264/MJPEG + H.265/H.264/MJPEG (PAL)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Stream1</strong></td>
<td><strong>Stream2</strong></td>
</tr>
<tr>
<td>3840 x 1440 (25 fps @ H.264/H.265)</td>
<td>1920 x 720 (25 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td></td>
<td>Stream1</td>
</tr>
<tr>
<td>----------</td>
<td>----------------</td>
</tr>
<tr>
<td></td>
<td>1280 x 480</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Stream1</th>
<th>Stream2</th>
<th>Stream3</th>
</tr>
</thead>
<tbody>
<tr>
<td>3840 x 2160 [20 fps @ H.264/H.265]</td>
<td>1920 x 720 [20 fps @ H.264/H.265/MJPEG]</td>
<td>720 x 480 [20 fps @ H.264/H.265/MJPEG]</td>
</tr>
<tr>
<td>1920 x 720 [30 fps @ H.264/H.265/MJPEG]</td>
<td>1280 x 480 [30 fps @ H.264/H.265/MJPEG]</td>
<td>720 x 480 [30 fps @ H.264/H.265/MJPEG]</td>
</tr>
<tr>
<td>1280 x 480 [30 fps @ H.264/H.265/MJPEG]</td>
<td>1280 x 480 [30 fps @ H.264/H.265/MJPEG]</td>
<td>720 x 480 [30 fps @ H.264/H.265/MJPEG]</td>
</tr>
<tr>
<td>720 x 480 [30 fps @ H.264/H.265/MJPEG]</td>
<td>720 x 480 [30 fps @ H.264/H.265/MJPEG]</td>
<td>720 x 480 [30 fps @ H.264/H.265/MJPEG]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Stream1</th>
<th>Stream2</th>
<th>Stream3</th>
</tr>
</thead>
<tbody>
<tr>
<td>3840 x 1440 (20 fps @ H.264/H.265)</td>
<td>1920 x 720 (20 fps @ H.264/H.265/MJPEG)</td>
<td>720 x 576 (20 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td></td>
<td>1280 x 480 (20 fps @ H.264/H.265/MJPEG)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>720 x 576 (20 fps @ H.264/H.265/MJPEG)</td>
<td></td>
</tr>
<tr>
<td>1920 x 720 (25 fps @ H.264/H.265/MJPEG)</td>
<td>1280 x 480 (25 fps @ H.264/H.265/MJPEG)</td>
<td>720 x 576 (25 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td></td>
<td>720 x 576 (25 fps @ H.264/H.265/MJPEG)</td>
<td></td>
</tr>
<tr>
<td>1280 x 480 (25 fps @ H.264/H.265/MJPEG)</td>
<td>1280 x 480 (25 fps @ H.264/H.265/MJPEG)</td>
<td>720 x 576 (25 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td></td>
<td>720 x 576 (25 fps @ H.264/H.265/MJPEG)</td>
<td></td>
</tr>
<tr>
<td>720 x 576 (25 fps @ H.264/H.265/MJPEG)</td>
<td>720 x 576 (25 fps @ H.264/H.265/MJPEG)</td>
<td></td>
</tr>
</tbody>
</table>

### 4.3.2.1.1.2 Video Resolutions-360° Mode

**Note:**
1. Stream1 supports 3840 x 2160 @ 25 fps only when operating with D1.
2. Stream1 supports MJPEG on all resolutions except 3840x2160/1440.
3. The frame rate is limited to 15 fps when True WDR is enabled.
4. An analog video output is available only when the camera is operating at resolutions equal to or less than 3840x2160, 1280x720, 1280x720 in Streams 1, 2, and 3 respectively when operating in 360° (Ceiling) Mode.
5. MJPEG does not support resolutions above 2MP.
The following resolutions are available when operating in 360° (Ceiling) Mode:

### H.265-Only

<table>
<thead>
<tr>
<th></th>
<th>PAL</th>
<th>NTSC</th>
</tr>
</thead>
<tbody>
<tr>
<td>3840 x 2160 (25 fps)</td>
<td>3840 x 2160 (27 fps)</td>
<td></td>
</tr>
<tr>
<td>1920 x 1080 (25 fps)</td>
<td>1920 x 1080 (27 fps)</td>
<td></td>
</tr>
<tr>
<td>1280 x 720 (25 fps)</td>
<td>1280 x 720 (27 fps)</td>
<td></td>
</tr>
<tr>
<td>720 x 576 (25 fps)</td>
<td>720 x 480 (27 fps)</td>
<td></td>
</tr>
</tbody>
</table>

### H.264-Only

<table>
<thead>
<tr>
<th></th>
<th>PAL</th>
<th>NTSC</th>
</tr>
</thead>
<tbody>
<tr>
<td>3840 x 2160 (25 fps)</td>
<td>3840 x 2160 (27 fps)</td>
<td></td>
</tr>
<tr>
<td>1920 x 1080 (25 fps)</td>
<td>1920 x 1080 (27 fps)</td>
<td></td>
</tr>
<tr>
<td>1280 x 720 (25 fps)</td>
<td>1280 x 720 (27 fps)</td>
<td></td>
</tr>
<tr>
<td>720 x 576 (25 fps)</td>
<td>720 x 480 (27 fps)</td>
<td></td>
</tr>
</tbody>
</table>

### H.265/H.264/MJPEG + H.265/H.264/MJPEG (NTSC)

<table>
<thead>
<tr>
<th>Stream 1</th>
<th>Stream 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>3840 x 2160 (15 fps @ H.264/H.265)</td>
<td>1920 x 1080 (15 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td></td>
<td>1280 x 720 (15 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td></td>
<td>720 x 480 (15 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td>1920 x 1080 (30 fps @ H.264/H.265/MJPEG)</td>
<td>1280 x 720 (30 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td></td>
<td>720 x 480 (30 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td>1280 x 720 (30 fps @ H.264/H.265/MJPEG)</td>
<td>1280 x 720 (30 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td></td>
<td>720 x 480 (30 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td>720 x 480 (30 fps @ H.264/H.265/MJPEG)</td>
<td>720 x 480 (30 fps @ H.264/H.265/MJPEG)</td>
</tr>
</tbody>
</table>

### H.265/H.264/MJPEG + H.265/H.264/MJPEG (PAL)

<table>
<thead>
<tr>
<th>Stream 1</th>
<th>Stream 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>3840 x 2160 (15 fps @ H.264/H.265)</td>
<td>1920 x 1080 (15 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td></td>
<td>1280 x 720 (15 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td></td>
<td>720 x 576 (15 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td>1920 x 1080 (25 fps @ H.264/H.265/MJPEG)</td>
<td>1280 x 720 (25 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td></td>
<td>720 x 576 (25 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td>1280 x 720 (25 fps @ H.264/H.265/MJPEG)</td>
<td>1280 x 720 (25 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td></td>
<td>720 x 576 (25 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td>720 x 576 (25 fps @ H.264/H.265/MJPEG)</td>
<td>720 x 576 (25 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td>Stream 1</td>
<td>Stream 2</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>3840 x 2160 (15 fps @ H.264/H.265)</td>
<td>1920 x 1080 (15 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td></td>
<td>1280 x 720 (15 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td></td>
<td>720 x 480 (15 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td>1920 x 1080 (30 fps @ H.264/H.265/MJPEG)</td>
<td>1280 x 720 (30 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td></td>
<td>720 x 480 (30 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td>1280 x 720 (30 fps @ H.264/H.265/MJPEG)</td>
<td>1280 x 720 (30 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td></td>
<td>720 x 480 (30 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td>720 x 480 (60 fps @ H.264/H.265/MJPEG)</td>
<td>720 x 480 (30 fps @ H.264/H.265/MJPEG)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Stream 1</th>
<th>Stream 2</th>
<th>Stream 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>3840 x 2160 (15 fps @ H.264/H.265)</td>
<td>1920 x 1080 (15 fps @ H.264/H.265/MJPEG)</td>
<td>720 x 576 (15 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td></td>
<td>1280 x 720 (15 fps @ H.264/H.265/MJPEG)</td>
<td>720 x 576 (15 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td></td>
<td>720 x 576 (15 fps @ H.264/H.265/MJPEG)</td>
<td>720 x 576 (15 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td>1920 x 1080 (25 fps @ H.264/H.265/MJPEG)</td>
<td>1280 x 720 (25 fps @ H.264/H.265/MJPEG)</td>
<td>720 x 576 (25 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td></td>
<td>720 x 576 (25 fps @ H.264/H.265/MJPEG)</td>
<td>720 x 576 (25 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td>1280 x 720 (25 fps @ H.264/H.265/MJPEG)</td>
<td>1280 x 720 (25 fps @ H.264/H.265/MJPEG)</td>
<td>720 x 576 (25 fps @ H.264/H.265/MJPEG)</td>
</tr>
<tr>
<td></td>
<td>720 x 576 (25 fps @ H.264/H.265/MJPEG)</td>
<td>720 x 576 (25 fps @ H.264/H.265/MJPEG)</td>
</tr>
</tbody>
</table>

#### 4.3.2.2 Privacy Zone

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

![Privacy Zone Screen](image)

**Privacy Zone Screen**

**To set a privacy zone**

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

**To delete a privacy zone**

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

### 4.3.2.3 ROI

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

![ROI Screen](image)

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

**To set a region of interest**

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

### 4.3.3 Camera Tab

The **Camera** tab includes three screens: **Exposure**, **Picture Adjustment**, and **White Balance**.

**Note:**

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

### 4.3.3.1 Exposure Screen

The **Exposure** screen is used for configuring basic exposure settings and day/night settings. The configurable settings depend on the selected Exposure mode. In the **Exposure** section, select one of the following modes: **Auto Shutter**, **Flickerless**, **Manual Mode**, or **Shutter WDR**. The choice of the Exposure mode determines the other configurable settings.
4.3.3.1.1 Auto Shutter Mode

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

This mode is recommended in indoor environments with mixed lighting sources where the main source is fluorescent lighting combined with natural light that enters the scene through windows and other exposed areas. This is the default setting.

![Auto Shutter Exposure Mode Settings](image-url)
Configure the settings in the *Exposure* section:

- **Exposure Mode** – From the drop-down menu, select *Auto Shutter*.
- **Min Shutter Speed** – Select a suitable shutter speed according to the environmental luminance. The following table displays the options:

<table>
<thead>
<tr>
<th>Auto Shutter Min Shutter Speed</th>
<th>PAL</th>
<th>NTSC</th>
<th>PAL</th>
<th>NTSC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/100</td>
<td>1/120</td>
<td>1/2500</td>
<td>1/120</td>
<td>1/2500</td>
</tr>
<tr>
<td>1/250</td>
<td>1/250</td>
<td>1/5000</td>
<td>1/250</td>
<td>1/5000</td>
</tr>
<tr>
<td>1/500</td>
<td>1/500</td>
<td>1/10000</td>
<td>1/500</td>
<td>1/10000</td>
</tr>
<tr>
<td>1/1000</td>
<td>1/1000</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Auto Shutter Max Shutter Speed</th>
<th>PAL</th>
<th>NTSC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/6.25</td>
<td>1/7.5</td>
<td></td>
</tr>
<tr>
<td>1/12.5</td>
<td>1/15</td>
<td></td>
</tr>
<tr>
<td>1/25</td>
<td>1/30</td>
<td></td>
</tr>
<tr>
<td>1/50</td>
<td>1/60</td>
<td></td>
</tr>
</tbody>
</table>

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

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

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

![Backlight Compensation Settings](image)

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

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

Configure the settings in the **Day/Night Switch Control** section:

• **Mode** – The Day/Night switch activates the IR Cut (IRC) filter for electronic day/night operation. Three modes are available: **Auto**, **Color**, and **B/W**.
  - **Auto** – Select **Auto** for automatic operation according to the ambient light level. The camera converts from **Day** (color) mode to **Night** mode (monochrome/black and white) automatically at nighttime or in low-light conditions. When there is sufficient light, the camera converts automatically from **Night** mode to **Day** mode. This is the default setting.
  - **Color** – Select **Color** for daylight operation. This deactivates IR mode by putting the camera into **Day** mode.
  - **B/W** – Select **B/W** (black and white) for nighttime operation. This activates IR mode by putting the camera into **Night** mode.

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

• **Sensitivity** – Use the slider to set the sensitivity between **Low** and **High** when switching from **Day** to **Night** mode or **Night** to **Day** mode. When set to **High**, the camera automatically switches between **Day** and **Night** modes upon minor changes in light intensity. When set to **Low**, the camera automatically switches between **Day** and **Night** modes upon major changes in light intensity.
In the IR Control section, configure the following settings:

- **Mode** – Select Auto, ON, or OFF. The default setting is Auto.
- **LED Brightness (Broad) Set 0-100** - (Applies to Left and Right LEDs) (Default 25)
- **LED Brightness (Narrow) Set 0-100** - (Applies to Top and Bottom LEDs) (Default 100)

Identifying ‘Narrow’ and ‘Broad’ LEDs

The LEDs on the Top and Bottom edges of the camera ("Narrow") produce a brighter illumination in the center of the overall field.

The LEDs on the Left and Right sides of the camera ("Broad") produce a brighter illumination for the edges of the overall field.

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

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

Configure the settings in the Exposure section:

- **Exposure Mode** – From the drop-down menu, select Flickerless.
- **Exposure Value** – See the explanation in the Auto Shutter Mode section above.
- **Backlight Compensation** – See the explanation in the Auto Shutter Mode section above.
- **Digital WDR** – See the explanation in the Auto Shutter Mode section above.

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

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

In the IR Control section, configure the following settings:

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

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

Manual mode opens the iris completely with a fixed gain. This mode should only be used in indoor scenes with consistent lighting. Manual mode requires the user to set fixed values for shutter and gain levels. Increasing the value of the fixed shutter increases the amount of light entering the sensor, which allows a brighter and more detailed image. In a similar manner, utilizing gain and increasing its level increases the sensitivity of the image sensor, which brightens the image and adds details. This increases the level of noise in the image.

Configure the settings in the Exposure section:

- **Exposure Mode** – From the drop-down menu, select Manual.
- **P Iris Level** (CM-3308) – Move the slider to a value between 1-6. A higher will reduce the shutter speed.
- **Shutter Speed** – Select the shutter speed from the following options:

<table>
<thead>
<tr>
<th>Shutter Speed</th>
<th>PAL</th>
<th>NTSC</th>
<th>PAL</th>
<th>NTSC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/25</td>
<td>1/30</td>
<td>1/1000</td>
<td>1/1000</td>
<td></td>
</tr>
<tr>
<td>1/50</td>
<td>1/60</td>
<td>1/2500</td>
<td>1/2500</td>
<td></td>
</tr>
<tr>
<td>1/100</td>
<td>1/120</td>
<td>1/5000</td>
<td>1/5000</td>
<td></td>
</tr>
<tr>
<td>1/250</td>
<td>1/250</td>
<td>1/10000</td>
<td>1/10000</td>
<td></td>
</tr>
<tr>
<td>1/500</td>
<td>1/500</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Gain** – Set the gain between 0-48 dB (CM-3304) or 0-36 dB (CM-3308). Increasing the gain lightens dark pictures resulting from low-level lighting. The default is 0.
- **Digital WDR** – See the explanation in the Auto Shutter Mode section above.

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

- **Mode** – See the explanation in the Auto Shutter Mode section above.
In the *IR Control* section, configure the following settings:

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

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

### 4.3.3.1.4 Shutter WDR

The Shutter WDR function is a form of multi-exposure (True) WDR, which is recommended when the image has a wide dynamic range. A combination of slow- and fast-exposure shutters is used to create a new image which adjusts the wide dynamic range of the scene and achieves a greater scale of brightness. When activated, the camera uses an algorithm to determine the optimal mix of light and dark regions within the scene from the two shutters.
Configure the settings in the Exposure section:

- **Exposure Mode** – From the drop-down menu, select Shutter WDR.
- **Exposure Value** – See the explanation in the Auto Shutter Mode section above.
- **Backlight Compensation** – See the explanation in the Auto Shutter Mode section above.
- **Enhanced WDR Level** – Select the setting that provides the ideal brightness according to the environmental luminance: High, Medium, Low or Off (default). Selecting High provides the most brightness, while Low reduces brightness.

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

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

In the **IR Control** section, configure the following settings:

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

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

### 4.3.3.2 Picture Adjustment

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

![Picture Adjustment Screen](image)

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

1. In the **Quality** section, configure the following settings:
   - **Sharpness** – Set the slider between 0-100, which provides the highest sharpness around the edges and for small features. The default setting is 50.
   - **3D Noise Reduction** – Set the slider between 0-100. The default setting is 20.
   - **Gamma Correction** – From the drop-down list, select 0.45 or 1. The default setting is 0.45. Gamma correction is used to ensure faithful reproduction of an image. When gamma = 1, the original image is the same as the image displayed on your screen. If the gamma is set at 0.45, there will be less contrast.

To configure color settings

1. In the **Color** section, configure the following settings:
   - **Brightness** – Set the image brightness between -100 to 100, which provides the highest brightness. The default is 0.
   - **Contrast** – Set the image contrast between -100 to 100, which provides the highest contrast. The default is 0.
   - **Saturation** – Set the image saturation -100 to 100. The lower the number, the closer the image is to a grayscale (i.e., monochrome or black-and-white) image. The higher the number, the deeper the color image (i.e., reds will be redder and blues will be bluer). The default is 0.
   - **Hue** – Set the image hue between -100 to 100, which provides the deepest hue. The default is 0.

   **Note:** These settings are applied to all 4 images coming from the individual sensors. When the camera is in 180 mode, users may see slight variations in the composite scene.

To configure mirror flip settings

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

**4.3.3.3 White Balance**

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

To set the White Balance mode

1. From the **Mode** drop-down list, select one of the following options:
   - **ATW** – In ATW mode, color is continuously adjusted according to the color temperature of the scene illumination. This is the default setting.
- *Auto* – In *Automatic* mode, the color in a scene is automatically adjusted according to the ambient lighting between 2500°K to 10000°K.

![White Balance Auto Mode Screen](image)

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

![White Balance Manual Mode Settings](image)

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

     o **R Gain:** Adjusts the red color in the image from 0 to 511. The higher the number, the redder the image. The default setting is 64.

     o **B Gain:** Adjusts the blue color in the image from 0 to 511. The higher the number, the bluer the image. The default setting is 64.

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

### 4.4 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).
Appendices

5 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
## 5.1 Technical Specifications

Following are the CM-6308 technical specifications:

<table>
<thead>
<tr>
<th>Camera</th>
<th>4x 1/2.8” BSI CMOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Pixels (H x V)</td>
<td>1920x1080 pixels (Full HD 1080p)</td>
</tr>
<tr>
<td>Sensor resolution</td>
<td>1920x1080 pixels (Full HD 1080p)</td>
</tr>
<tr>
<td>Shutter Speed (Digital Slow Shutter)</td>
<td>1/6.25 (PAL) or 1/7.5 (NTSC) to 1/10,000 with up to 32x sensitivity boost in color or night mode</td>
</tr>
<tr>
<td>Sensitivity</td>
<td></td>
</tr>
<tr>
<td>Color Mode</td>
<td>0.02 lux @ 30 IRE</td>
</tr>
<tr>
<td>B/W Mode</td>
<td>0 lux without IR, 0 lux with IR @ 30 IRE</td>
</tr>
<tr>
<td>Video Compression</td>
<td>Dual-stream H.265 (Main profile) + H.264 (Main and High profile) + MJPEG (Stream2 and Stream3 only)</td>
</tr>
<tr>
<td>Video Resolution (H.265, H.264, and MJPEG)</td>
<td></td>
</tr>
<tr>
<td>180° Mode</td>
<td>3840x1440 @ 25/30fps</td>
</tr>
<tr>
<td>360° Mode</td>
<td>3840x2160 @ 25/30fps</td>
</tr>
<tr>
<td>Maximum Performance</td>
<td>180° Mode</td>
</tr>
<tr>
<td></td>
<td>360° Mode</td>
</tr>
<tr>
<td>Bit Rate Control</td>
<td>CBR (Constant Bit Rate) and CVBR (Constrained Variable Bit Rate): 64 – 20,480 Kbps (with H.265 and H.264)</td>
</tr>
<tr>
<td>S/N Ratio</td>
<td>±50dB (with AGC off)</td>
</tr>
<tr>
<td>Analog Video Output (360° mode only)</td>
<td>1V p-p, 1x BNC 75Ω</td>
</tr>
<tr>
<td>Video Out Aspect Ratio</td>
<td>180° mode</td>
</tr>
<tr>
<td></td>
<td>360° mode</td>
</tr>
</tbody>
</table>
### Appendices

#### CM-6308-P1-I User and Installation Guide

**Lens**

<table>
<thead>
<tr>
<th>Lens Type</th>
<th>F2.0, 3.6mm, fixed-focus lens</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing Angle (HFOV)</td>
<td>92°</td>
</tr>
</tbody>
</table>

**IR Illuminator**

<table>
<thead>
<tr>
<th>IR Range</th>
<th>Up to 25m (82 feet)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Angle of illumination</td>
<td>60°</td>
</tr>
<tr>
<td>LED Type</td>
<td>High-efficiency SMD</td>
</tr>
<tr>
<td>Peak Emission Wavelength (nm)</td>
<td>850</td>
</tr>
</tbody>
</table>

**Operation**

<table>
<thead>
<tr>
<th>Exposure Control</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gain Control</td>
<td>Yes</td>
</tr>
<tr>
<td>Backlight Compensation</td>
<td>Yes</td>
</tr>
<tr>
<td>Gamma Correction</td>
<td>0.45, 1</td>
</tr>
<tr>
<td>Brightness</td>
<td>Manual</td>
</tr>
<tr>
<td>Contrast</td>
<td>Manual</td>
</tr>
<tr>
<td>Saturation</td>
<td>Manual</td>
</tr>
<tr>
<td>Hue</td>
<td>Manual</td>
</tr>
<tr>
<td>Sharpness</td>
<td>Manual (0-100)</td>
</tr>
<tr>
<td>White Balance</td>
<td>ATW/Auto/Manual/One Push</td>
</tr>
<tr>
<td>Wide Dynamic Range (WDR)</td>
<td>Digital WDR and Shutter WDR</td>
</tr>
<tr>
<td>3D Noise Reduction</td>
<td>Manual (0-100)</td>
</tr>
</tbody>
</table>
### Operation

<table>
<thead>
<tr>
<th>Image Settings</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Zones</td>
<td>Yes (8 zones)</td>
</tr>
<tr>
<td>Regions of Interest</td>
<td>Yes (two regions)</td>
</tr>
<tr>
<td>Orientation</td>
<td>0°, 180°</td>
</tr>
<tr>
<td>True Day/Night</td>
<td>Removable Mechanical IR Cut Filter</td>
</tr>
<tr>
<td>IR Control</td>
<td>Yes (adjustable LED brightness)</td>
</tr>
<tr>
<td>Sensitivity</td>
<td>Yes (enables switching between Day and Night modes)</td>
</tr>
<tr>
<td>Mirror Flip</td>
<td>Flip/Mirror/Both/Off</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Audio</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>G.711 (µ-LAW and ALAW) and AAC Audio Compression</td>
<td>Audio Intensity Detection</td>
</tr>
<tr>
<td>1x Audio-in/1x Audio-out</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alarm</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1x Alarm-in/1x Alarm-out</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Languages</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>English, Arabic, Czech, Simplified Chinese, Traditional Chinese, French, German, Hungarian, Italian, Japanese, Polish, Portuguese, Russian, Spanish</td>
<td></td>
</tr>
</tbody>
</table>

| MicroSD Card Recording      | Up to 128GB microSDXC, Class 10 (card not included) |

<table>
<thead>
<tr>
<th>Analytics</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Motion Detection</td>
<td>When the unit detects motion, a corresponding action is triggered. On/Off, by zone, object size, sensitivity level, and schedule.</td>
</tr>
<tr>
<td>Tampering Alarm</td>
<td>When the unit detects tampering, a corresponding action is triggered. On/Off, on-event notification, sensitivity level, schedule, recording to SD card, and more are supported as events in Latitude.</td>
</tr>
</tbody>
</table>
## Network

<table>
<thead>
<tr>
<th>Interface</th>
<th>1 x 10/100 Mbps Ethernet RJ45 interface (IEEE 802.3/802.3u)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services and Protocols</td>
<td>IPv4, IPv6 (including IPv6 addressing, IPv6 router advertisement, IPv6 DHCP, and IPv6 web support), TCP, UDP, IGMP, ICMP, DHCP, DNS, DDNS, RTP, RTSP, RTCP, NTP, SMTP, HTTP, HTTPS, FTP, PPPoE, QoS, SNMPv1/v2c/v3 (MIB-II), UPnP, ONVIF® Profile S &amp; G, LDAP</td>
</tr>
<tr>
<td>Video Streaming</td>
<td>RTSP/RTP</td>
</tr>
<tr>
<td>Event Notification</td>
<td>HTTP event query, HTTP event client pulling, SMTP, FTP</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>802.1X (EAP-MD5, EAP-TTLS, EAP-PEAP), IP address filtering, SSL, SNMPv3 (AES, DES, MD5, and SHA)</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 Server 2003, Windows Server 2008 (32-bit version); Windows 7, 8, 8.1, and 10 (all 64-bit versions)</td>
</tr>
<tr>
<td>Internet Browser</td>
<td>Microsoft Internet Explorer 10 (32-bit version) and above; Microsoft Edge 38 and above; Chrome v.55 and above; Firefox v.50 and above</td>
</tr>
</tbody>
</table>
## Power

<table>
<thead>
<tr>
<th>Power Consumption</th>
<th>24.9W with heater and IR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>802.3at PoE+ (Minimum Rating 30W), 24VAC</td>
</tr>
<tr>
<td>Power Input (PoE+)</td>
<td>45-57V</td>
</tr>
<tr>
<td>Power Output</td>
<td>PoE+: &gt;0.52A; 24VAC: &gt;1.42A</td>
</tr>
<tr>
<td>Power Connection</td>
<td>PoE+: RJ45; 24VAC: 2-pin terminal block connector</td>
</tr>
</tbody>
</table>

### Physical

<table>
<thead>
<tr>
<th>Dimensions (Ø x H)</th>
<th>190 x 130mm (7.5 x 5.1&quot;)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weight</td>
<td>1.56kg (3.44 lbs.)</td>
</tr>
<tr>
<td>Ingress Protection</td>
<td>IP67</td>
</tr>
<tr>
<td>Vandal-Proof Protection</td>
<td>IK10</td>
</tr>
<tr>
<td>Tilt</td>
<td>360° (Ceiling) Mode: 63°; 180° (Wall) Mode: 45°</td>
</tr>
<tr>
<td>Bubble F-Stop</td>
<td>F1.0 Smoked Bubble</td>
</tr>
</tbody>
</table>

### Environmental Specifications

<table>
<thead>
<tr>
<th>Storage Temperature</th>
<th>-40° to 60°C (-40° to 140°F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Temperature</td>
<td>-40° to 50°C (-40° to 122°F)</td>
</tr>
<tr>
<td>Operating Humidity</td>
<td>Up to 90% relative humidity (non-condensing)</td>
</tr>
</tbody>
</table>

### Certifications

<table>
<thead>
<tr>
<th>Safety</th>
<th>AS/NZS CISPR22 (Class B); EN50130-4; EN61000-3-2/3; EN61000-4-2/3/4/5/6/8/11;EN61000-6-3 (Class B); UL 60950-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environmental</td>
<td>RoHS 2011_65_EU, excluding Pb in 2LI (lead on second level interconnect); WEEE Directive 2012/19/EU; REACH</td>
</tr>
</tbody>
</table>
5.2 Internet Security Settings on Internet Explorer

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

To set the default Internet security level

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

![Command Bar Toolbar – Select Internet Options]

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

![Internet Options > Security Tab]

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

Configuring ActiveX Controls and Plug-in Settings

To create a custom level

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

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.

### 5.3 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.
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.

   ![Windows Services (Local) Dialog Box](image)

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.
5.4 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](image)

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](image)

5.5 Installing and Deleting the Web Player

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

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

Installing the Web Player with Internet Explorer

If your browser is Internet Explorer, a message is displayed, requesting you to install a plug-in.
To install the Web Player

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

   ![Run Ariel Player Plug-in Information Bar]

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

   ![Web Player Installation Wizard]
3. Click **Next** to install the Ariel Player plug-in on your PC.

4. Click **Close** when the **Installation Complete** dialog box is displayed.
5. Click Close. Ariel Player is displayed in the Programs and Features window.

![Programs and Features Window](image)

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

![Ariel Player Plug-in Download Completed Information Bar](image)

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

![Ariel Player Restart System Dialog Box](image)

a. Click Yes. The computer reboots and the Rebooting Completed message appears.

b. Click OK. The Live View screen is displayed.

Deleting the Web Player

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

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

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

![Programs and Features](image)

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

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

**To delete an existing Web Player file on Windows 10**

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

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

**To clear your computer’s cache memory**

1. In the Control Panel, click **Internet Options**. The **Internet Properties** dialog box opens.
2. From the Browsing History section, click **Delete**. The **Delete Browsing History** dialog box opens.

![Delete Browsing History Dialog Box](image)

3. From the **Delete Browsing History** dialog box, check **Preserve Favorites website data**, **Temporary Internet files and website files**, **Cookies and website data**, **History**, **Download History**, **Form data**, **Passwords**, **Preserve Favorite websites**, **Cookies and website data**, and **Tracking Protection**, **ActiveX Filtering** and **Do Not Track**.

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

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

6. Follow instructions above to install the Web Player.
## 5.6 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></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>
## 5.7 Troubleshooting

This section provides useful information and remedies for common situations.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Solution</th>
</tr>
</thead>
</table>
| No network connection                             | **Hardware issues:**  
  - Check that the network is working and the unit is powered on.  
  - Check that the network (Ethernet) cable is properly attached to the unit.
  - Confirm that the network cables are not damaged and replace if necessary.  
  **IP Address issues:**  
  - Change the default IP address/addresses of the unit.  
  - From the PC running the web browser, ping the unit IP address and confirm that it can be reached.  
  - Confirm that the network settings/firewalls are set according to the requirements.  
  - The camera might be located on a different subnet. Contact your IT administrator to get the IP address of the camera. |
| How do I find IP address of my unit?              | • Check the network DHCP server IP address assignments and lease.  
  • Alternatively, move the camera to an isolated network and make sure camera gets DHCP address and is accessible. Move the camera back to the network and test it. If you still have issues, reset the camera physically by pressing the reset button on the rear of the camera and test the camera again. This will ensure the camera releases the IP address. |
| The IP address responds to a ping on the network from the workstation but does not show in the Discovery List | • Disconnect the unit's Ethernet 10/100 port or turn the power to unit off, and then ping the IP address again. If the IP address responds, there is another device using the IP address. Consult with your network administrator to resolve the conflict.  
  • Check the network port and ensure that it is working OK.  
  • Ensure that the switch ports provide the necessary power. |
| The unit IP address is in use by another computer (collision) | • Check the DHCP settings. Obtain a new IP address using DHCP. Ensure this is a unique IP address.  
  • Alternatively, change the unit IP address after connecting to it directly (not through the system network). |
<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cannot login to the camera</td>
<td>• Check the login user ID of the user or admin.</td>
</tr>
<tr>
<td></td>
<td>• Check the login password of the user or admin.</td>
</tr>
<tr>
<td>No video image displayed on the main menu or the view menu of the web interface</td>
<td>• Reset the browser security settings to the default value.</td>
</tr>
<tr>
<td></td>
<td>• Check that the correct port was configured. The default port is 554.</td>
</tr>
<tr>
<td>Bad output video quality</td>
<td>• Check that the network cable is connected securely.</td>
</tr>
<tr>
<td></td>
<td>• Check that the camera settings are correct on the camera and in the unit.</td>
</tr>
<tr>
<td></td>
<td>• Check that the camera lens is clean and unobstructed.</td>
</tr>
<tr>
<td></td>
<td>• Check that the cable length is within specification.</td>
</tr>
<tr>
<td>Streaming video image is hanging (stopped)</td>
<td>• Confirm the unit’s video streaming settings.</td>
</tr>
<tr>
<td></td>
<td>• Refresh your browser screen (F5).</td>
</tr>
<tr>
<td></td>
<td>• Check that the bandwidth and bit rate settings of the network are set properly.</td>
</tr>
<tr>
<td></td>
<td>• Check that other processes and applications are not causing undue latency.</td>
</tr>
<tr>
<td></td>
<td>• Check that the firewall analysis or blocking is not interfering with the video stream and supports the required ports and communication protocols.</td>
</tr>
<tr>
<td>Bluish picture in an indoor scene (possibly mixing indoor and outdoor lighting)</td>
<td>Adjust the White balance configuration to Auto. If the lighting in the scene is fixed, manually adjust the White balance to an acceptable image.</td>
</tr>
<tr>
<td>Reddish picture and incorrect colors in the image</td>
<td>Check the PoE power supply and associated network cables. Connect directly to the PoE and compare the images. If the problem persists, contact support.</td>
</tr>
<tr>
<td>IR LEDs do not function</td>
<td>The cameras have a circuit protection mechanism that is activated if the cover is removed while the IR LEDs are on.</td>
</tr>
<tr>
<td></td>
<td>• Re-attach the cover (making sure that the IR contacts are in place)</td>
</tr>
<tr>
<td></td>
<td>• Make sure that the cover is closed properly</td>
</tr>
<tr>
<td></td>
<td>• Power cycle the camera.</td>
</tr>
</tbody>
</table>
### 5.8 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>
5.9  Fifth Imager - FLIR-CM-IMG5-63P

The Fifth Imager lens (FLIR-CM-IMG5-63P) is an add-on accessory for the CM-6308-P1-I. It allows for a fifth lens to be easily attached to the center of the camera to allow for additional coverage. See CM_IMG5_63P_QIG for reference.

Note: When the Fifth Imager lens is installed and the camera is being used in FLIR UVMS, it will show two scenes for the unit. The first scene includes all 4 scenes from the CM-6308-P1-I and the second scene is shown from the Fifth Imager.

Upgrading Firmware

Note when upgrading firmware.

Should it be necessary to upgrade the camera and the CM-IMG5-63P accessory firmware, the following steps should be followed:

1. Set the camera on 360 mode.
2. Attach the CM-IMG5-63P to the camera.
3. Upgrade the CM-IMG5-63P firmware through the camera’s web UI.
4. Upgrade the camera firmware.
5. Upgrade the FPGA, if needed.
5.10 Mounting Accessories

The following mounting accessories are available from FLIR for installation of your Quasar Gen III CM-6308 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></td>
<td>CM-CAPX-63P</td>
<td>Pendant Mount</td>
</tr>
</tbody>
</table>