Illustra

Illustra Pro Gen4 2MP, 4MP, 5MP & 8MP Indoor / Outdoor Domes, Corner Dome, Compact Dome, Bullet, LPR Dome and Bullet cameras

Installation and Configuration Guide




Johnson
Controls

Notice

Please read this manual thoroughly and save it for future use before attempting to connect or operate this unit.

The information in this manual was current when published. The manufacturer reserves the right to revise and improve its products. All specifications are therefore subject to change without notice.

Copyright

© 2025 Johnson Controls. All rights reserved.

JOHNSON CONTROLS, TYCO and ILLUSTRA are trademarks and/or registered trademarks. Unauthorized use is strictly prohibited.

Tyco Security Products

6600 Congress Avenue

Boca Raton, FL 33487 U.S.A.

Customer Service

Thank you for using Illustra products. We support our products through an extensive worldwide network of dealers. The dealer through whom you originally purchased this product is your point of contact if you need service or support. Our dealers are empowered to provide the very best in customer service and support. Dealers in North America should contact Illustra at (800) 507-6268 (dial Option 1) or (800) 392-2873 (dial Option 2). For other regions, please visit www.illustracameras.com.

Tyco Illustra Cameras

Tyco Illustra is a leading video surveillance specialist. Our domestic & commercial options give high-performance with affordability. Browse our products.

Camera Firmware Upgrade

The camera can be upgraded via the web GUI using firmware provided by Illustra which can be found on www.illustracameras.com. The firmware can also be upgraded using the Illustra Connect tool (windows based) or Illustra Tools (mobile app) or victor/VideoEdge, which also provides bulk firmware upgrade capability. Please refer to the respective application documents for further information.

Trademarks

The trademarks, logos, and service marks displayed on this document are registered in the United States [or other countries]. Any misuse of the trademarks is strictly prohibited and Tyco Security Products will aggressively enforce its intellectual property rights to the fullest extent of the law, including pursuit of criminal prosecution wherever necessary. All trademarks not owned by Tyco Security Products are the property of their respective owners, and are used with permission or allowed under applicable laws.

Product offerings and specifications are subject to change without notice. Actual products may vary from photos. Not all products include all features. Availability varies by region; contact your sales representative.

Table of Contents

Overview **9**

Illustra PG4 Series 2MP, 4MP, 5MP LPR and 8MP Indoor / Outdoor Dome Cameras **11**

Product overview 11

Installation 12

Illustra PG4 Series 2MP, 4MP, 5MP LPR and 8MP Indoor / Outdoor Bullet Cameras **27**

Product overview 27

Installation 28

Illustra PG4 Series 5MP Corner Dome Camera **39**

Product overview 39

Installation 39

Illustra PG4 Series 2MP, 4MP and 8MP Indoor / Outdoor Compact Cameras **50**

Product overview 50

Installation 51

Network Topology **57**

Network Connection **58**

Default IP Address 58

DHCP 59

Managing cameras with the Illustra Connect tool 60

Configuration **62**

Live menu 65

Quick Start Menu 67

Basic Configuration 67

Video Menu 85

Streams 85

Picture Settings 87

Date / Time / OSD 100

Privacy Zones 103

AI Privacy Mask 104

Region of Interest (ROI) 105

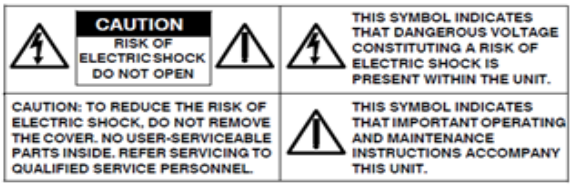
Events and Actions Menu 107
Event Settings 107
Event Actions 112
Alarm I / O 113
LED 115
Periodic Events 116
Event Logs 117
Analytics 120
Face Detection 120
Motion Detection 121
Artificial Intelligence Object Classification 122
Person Counting 128
Tamper Detection 131
Blur Detection 131
Audio Detection 132
Illustra 5MP LPR Camera License Plate Recognition 133
Applications 140
Applications 140
License 141
Security 142
Security Status 142
Security Status 145
Users 146
Password Protection 148
HTTP / HTTPS 149
IEEE 802.1x 150
Firewall 151
Remote Access 154
Session Timeout 157
Generate CSR 157
DAI 158
Network Menu 161

TCP/IP 162
Hostname 163
Multicast 163
FTP 164
SMTP 166
SNMP 167
Heartbeat 167
CIFS 168
Dynamic DNS 169
SIP 170
Wi-Fi 172
QoS 172
Traffic control 174
MTU 174
System 175
Maintenance 175
Firmware upgrade 179
Date / Time 181
Audio 182
HDMI Video 184
Streaming Mode 185
Health Monitor 185
Logs 186
About 187
Edge Recording 189
Micro SD Card Management 189
Encrypted SD card storage 191
Record Settings 193
Event Download 194
Appendix A: Using Media Player to View RTSP Streaming 195
Appendix B: Stream Tables 196
Appendix C:Technical Specifications 203

END USER LICENSE AGREEMENT (EULA) **268**

Warning

- Installation and service should be performed only by qualified and experienced technicians and comply with all local codes and rules to maintain your warranty.
- Wipe the camera with a dry soft cloth. For tough stains, slightly apply with diluted neutral detergent and wipe with a dry soft cloth.
- Do not apply benzene or thinner to the camera, which may cause the surface of the unit to be melted or lens to be fogged.
- To meet EU EMC immunity requirements for security equipment the mains power for equipment powering this unit should be backed up by an uninterruptible power supply.
- Avoid operating or storing the unit in the following locations:
  - Near fluorescent lamps or objects with reflections.
  - Under unstable or flickering light sources.





WEEE (Waste Electrical and Electronic Equipment). Correct disposal of this product (applicable in the European Union and other European countries with separate collection systems). This product should be disposed of, at the end of its useful life, as per applicable local laws, regulations, and procedures.

Overview

This Illustra Pro Installation and Configuration Guide is a user manual which provides physical properties, installation, and configuration information of the cameras in Table 1 on Page 9.

Table 1 Product codes

Product Code	Model Name	Description
IPS02-D12-OI04	Illustra Pro Gen 4, 2MP Indoor / Outdoor Dome	Illustra Pro Gen4 2MP MiniDome, 2.7-13.5mm, Indoor/Outdoor, IP67, IK10, TDN w/IR, TWDR
IPS02-D17-OI04	Illustra Pro Gen 4, 2MP Indoor / Outdoor Dome	Illustra Pro Gen4 2MP MiniDome, 7-22mm, Indoor/Outdoor, IP67, IK10, TDN w/IR, TWDR
IPS02-B12-OIA4	Illustra Pro Gen 4, 2MP Bullet	Illustra Pro Gen4 2MP Standard Bullet, indoor/outdoor, white, TDN w/IR, TWDR
IPS02-B15-OIA4	Illustra Pro Gen 4, 2MP Bullet	Illustra Pro Gen4 2MP Standard Bullet, indoor/outdoor, white, TDN w/IR, TWDR
IPS02-C10-OIA4	Illustra Pro Gen 4 2mp Compact	Illustra Pro 2MP Compact, 2.8mm Fixed, IP66/67 IK10, TDN w/IR, WDR
IPS04-D12-OI04	Illustra Pro Gen 4, 4MP Indoor / Outdoor Dome	Illustra Pro Gen4 4MP MiniDome, 2.7-13.5mm, Indoor/Outdoor, IP67, IK10, TDN w/IR, TWDR
IPS04-D14-OI04	Illustra Pro Gen 4, 4MP Indoor / Outdoor Dome	Illustra Pro Gen4 4MP MiniDome, 6-22mm, Indoor/Outdoor, IP67, IK10, TDN w/IR, TWDR
IPS04-B12-OIA4	Illustra Pro Gen 4, 4MP Bullet	Illustra Pro Gen4 4MP Standard Bullet, indoor/outdoor, white, TDN w/IR, TWDR
IPS04-B12-OTA4	Illustra Pro Gen 4, 4MP Bullet	Illustra Pro Gen4 4MP Standard Bullet, indoor/outdoor, white, TDN, TWDR
IPS04-B16-OIA4	Illustra Pro Gen 4, 4MP Bullet	Illustra Pro Gen4 4MP Tele Bullet, indoor/outdoor, white, TDN w/IR, TWDR
IPS04-C10-OIA4	Illustra Pro Gen 4 4mp Compact	Illustra Pro 4MP Compact, 2.8mm Fixed, IP66/67 IK10, TDN w/IR, WDR
IPS05-R10-OIA4	Illustra Pro Gen 4, 5MP Corner	Illustra Pro Gen4 5MP Corner, TDN w/IR, WDR
IPS08-D13-OI04	Illustra Pro Gen 4, 8MP Indoor / Outdoor Dome	Illustra Pro Gen4 8MP MiniDome, 3.6-11mm, Indoor/Outdoor, IP67, IK10, TDN w/IR, TWDR
IPS08-D14-OI04	Illustra Pro Gen 4, 8MP Indoor / Outdoor Dome	Illustra Pro Gen4 8MP MiniDome, 6-22mm, Indoor/Outdoor, IP67, IK10, TDN w/IR, TWDR

Product Code	Model Name	Description
IPS08-B13-OIA4	Illustra Pro Gen 4, 8MP Bullet	Illustra Pro Gen4 8MP Standard Bullet, indoor/outdoor, white, TDN w/IR, TWDR
IPS08-B16-OIA4	Illustra Pro Gen 4, 8MP Bullet	Illustra Pro Gen4 8MP Tele Bullet, indoor/outdoor, white, TDN w/IR, TWDR
IPS08-C10-OIA4	Illustra Pro Gen 4 8mp Compact	Illustra Pro 8MP Compact, 2.8mm Fixed, IP66/67 IK10, TDN w/IR, WDR
IPS05-D12-LPR4	Illustra Pro Gen 4, 5MP LPR Dome	Illustra Pro Gen4 5MP LPR Mini Dome, 2.7-13.5mm, Indoor/Outdoor, IP67, IK10, TDN w/IR, TWDR
IPS05-B12-LPR4	Illustra Pro Gen 4, 5MP LPR Bullet	Illustra Pro Gen4 5MP LPR Bullet, indoor/outdoor, white, TDN w/IR, TWDR
IPS05-B16-LPR4	Illustra Pro Gen 4 5MP LPR Bullet	Illustra Pro4 5MP LPR Bullet, indoor/outdoor, 13-55mm, AI, TDN w/IR, TWDR

The first portion of this guide contains information pertaining specifically to the aforementioned cameras.

The second portion of this guide contains information regarding the Illustra User Web Interface and the web configuration of the aforementioned cameras. Refer to Configuration on page 62 for procedural information pertaining to camera configuration.

Note: Please visit illustracameras.com for access to firmware updates that include new features, cyber-security enhancements and bug fixes.

Illustra PG4 Series 2MP, 4MP, 5MP LPR and 8MP Indoor / Outdoor Dome Cameras

This chapter provides product features, installation procedures, and connection information regarding the Illustra Pro Gen 4 Series 2MP, 4MP, 5MP LPR and 8MP Indoor / Outdoor Dome cameras.

Product overview

This chapter explains the features and installation of the PG4 Dome cameras. Product codes and descriptions of the cameras are provided in the table below.

Table 2 Product code and description of the PG4 Dome cameras

Product Code	Description
IPS02-D12-OI04	Illustra Pro Gen4 2MP MiniDome, 2.7-13.5mm, Indoor/Outdoor, IP67, IK10, TDN w/IR, TWDR
IPS02-D17-OI04	Illustra Pro Gen4 2MP MiniDome, 7-22mm, Indoor/Outdoor, IP67, IK10, TDN w/IR, TWDR
IPS04-D12-OI04	Illustra Pro Gen4 4MP MiniDome, 2.7-13.5mm, Indoor/Outdoor, IP67, IK10, TDN w/IR, TWDR
IPS04-D14-OI04	Illustra Pro Gen4 4MP MiniDome, 6-22mm, Indoor/Outdoor, IP67, IK10, TDN w/IR, TWDR
IPS08-D13-OI04	Illustra Pro Gen4 8MP MiniDome, 3.6-11mm, Indoor/Outdoor, IP67, IK10, TDN w/IR, TWDR
IPS08-D14-OI04	Illustra Pro Gen4 8MP MiniDome, 6-22mm, Indoor/Outdoor, IP67, IK10, TDN w/IR, TWDR
IPS05-D12-LPR4	Illustra Pro Gen4 5MP LPR Mini Dome, 2.7-13.5mm, Indoor/Outdoor, IP67, IK10, TDN w/IR, TWDR

Note: The following relates to the 5MP LPR camera only. Correct camera installation and configuration are required to achieve optimal performance of the License Plate Recognition solution. Please ensure the LPR Best Practice Guide is reviewed in this manual prior to installation.

Installation

In the box

Check everything in the packing box matches to the order form and the packing slip. In addition to this guide, items below are included in the packing box:

- 1 x Camera
- 1 x T20 Security Key
- 4 x TP4 32mm screws & 4 x Plastic screw anchors
- 1 x Water proof rubber (1 hole)
- 1 x Water proof rubber (3 holes)
- 1 x RJ45 Grommet insertion tool
- 1 x Water proof rubber insert tool
- 1 x Printed Regulatory Document
- 1 x Printed QSG
- 1 x Camera bottom base (use in a wall mount installation)
- 1 x Camera bottom base cable hole cover
- 1 x Mounting template (use with the bottom case / wall mount installation)
- 1 x Mounting template (use in an in-ceiling mount installation)
- 1 x Metal cover
- 1 x Trim Ring
- 1 x Ethernet cable

Contact your dealer if any item is missing.

Installation tools

The following tools assist with installation:

- 1 x Screw driver
- 1 x Drill
- 1 x Wire cutters

Quick Reference

- Default IP: 192.168.1.168 (DHCP enabled)
- Default Username / Password: admin / admin
- Power: PoE Class 3 or 24V AC

Note: The pre-fitted ethernet cable that comes with the camera can be removed if the installation requires the use of an existing network cable, or if additional cables are required. You must use the supplied rubber grommet with the cable to maintain the IP rating.

Figure 3 PG4 Indoor / Outdoor IR Dome camera parts

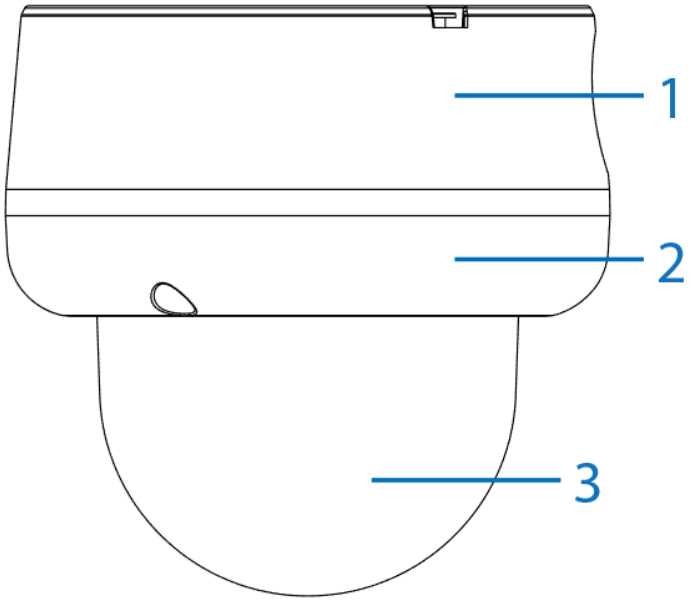


Table 4 Camera Interface - Bubble Assembly side

Number	Description
1	Camera bottom base
2	Dome cover
3	Dome

Figure 5 Camera Interface - Bubble Assembly side

Note: Use the T20 security key to remove the three screws on the dome cover (2) (Figure 3) to access the interior buttons and USB connection.

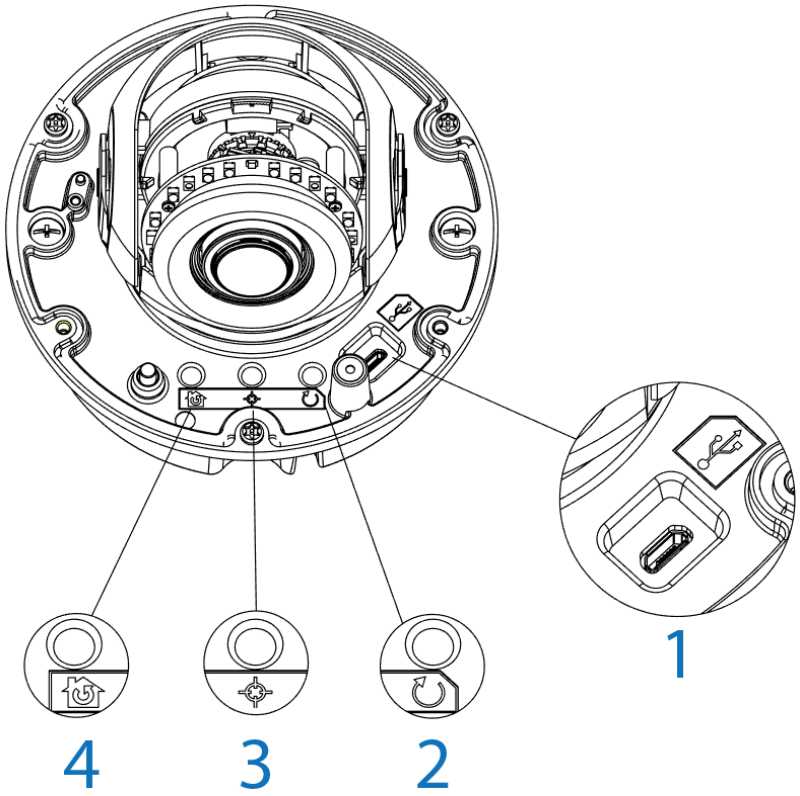


Table 6 Camera Interface - Bubble assembly side

Number	Description
1	Micro USB port connection
2	Reboot button
3	Auto focus (Set the camera focus during installation)
4	Reset to factory default but preserve IP Address (Hold for 5 seconds) Reset to factory default (Hold for 20 seconds)

Figure 7 Camera Interface - Base assembly side

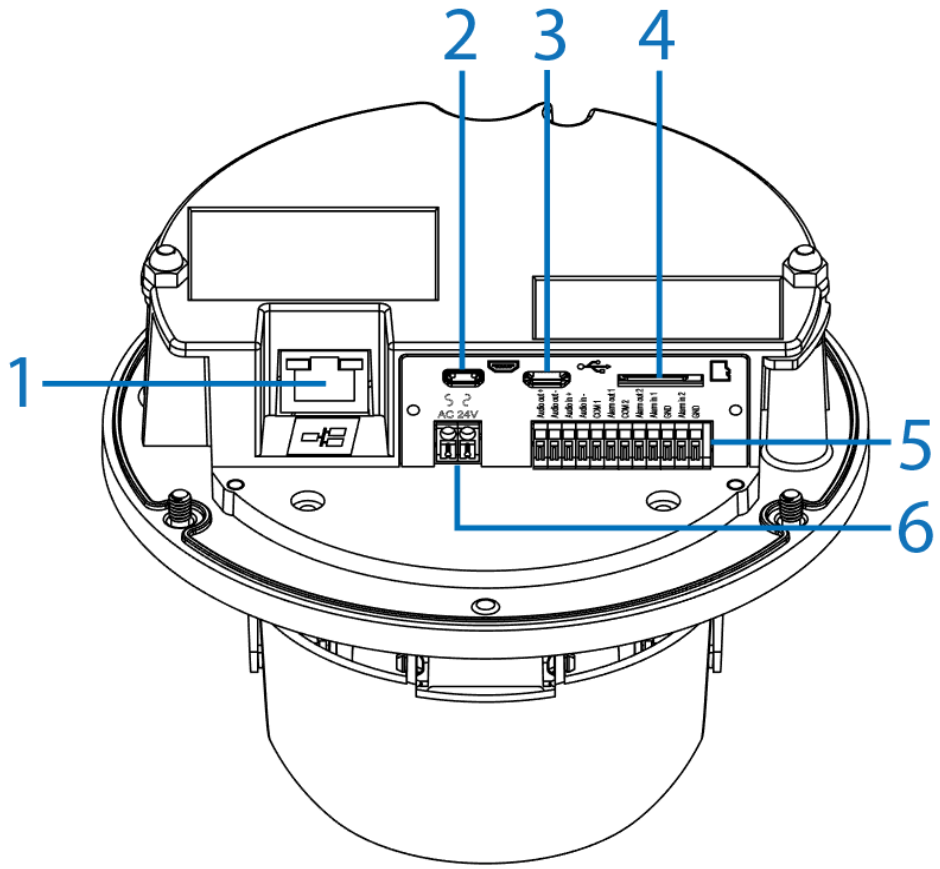


Table 8 Camera interior connections descriptions

Number	Description
1	Ethernet port
2	Micro HDMI cable port
3	Micro USB cable port
4	Micro SD card slot
5	Audio and alarm pins
6	Power connector

Procedure 1 Mounting the camera

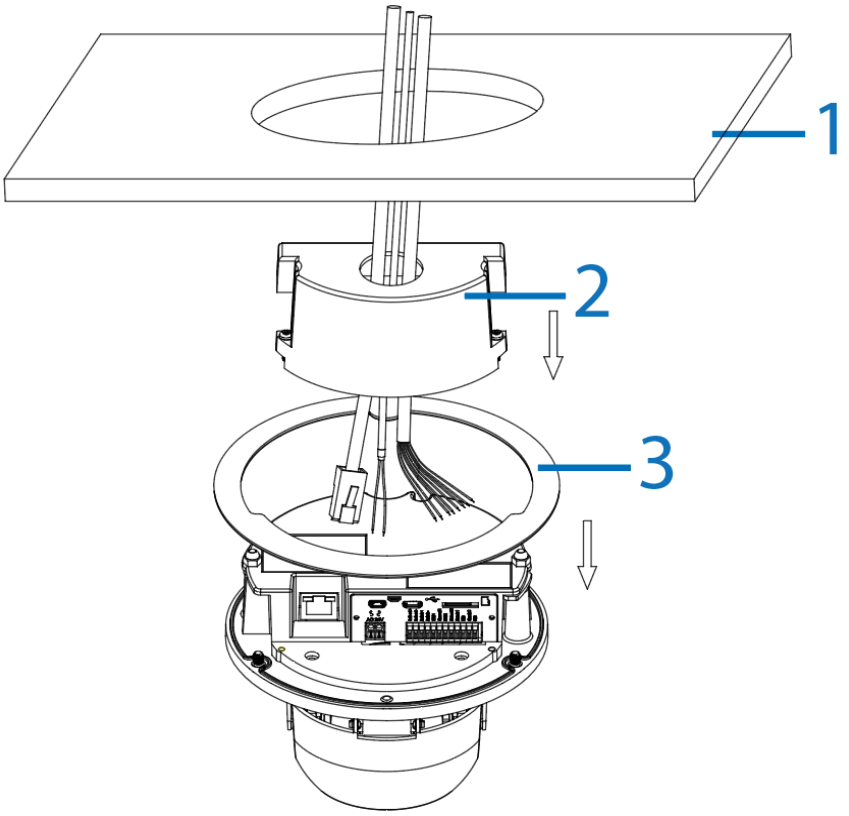
Refer to the Illustra mounting accessories webpage https://www.illustracameras.com/products/accessories/mounts for assistance. The following mount accessory part numbers are applicable with the Illustra Pro Gen4 2MP, 4MP and 8MP IR Indoor / Outdoor Dome cameras: ADCi6DPCAPOW, ADLOMARM, ADCDMCRNRO, ADCDMPOLE and IBJB-P-ISWB-0.

- End -

Procedure 2 Installing the camera into a recess ceiling

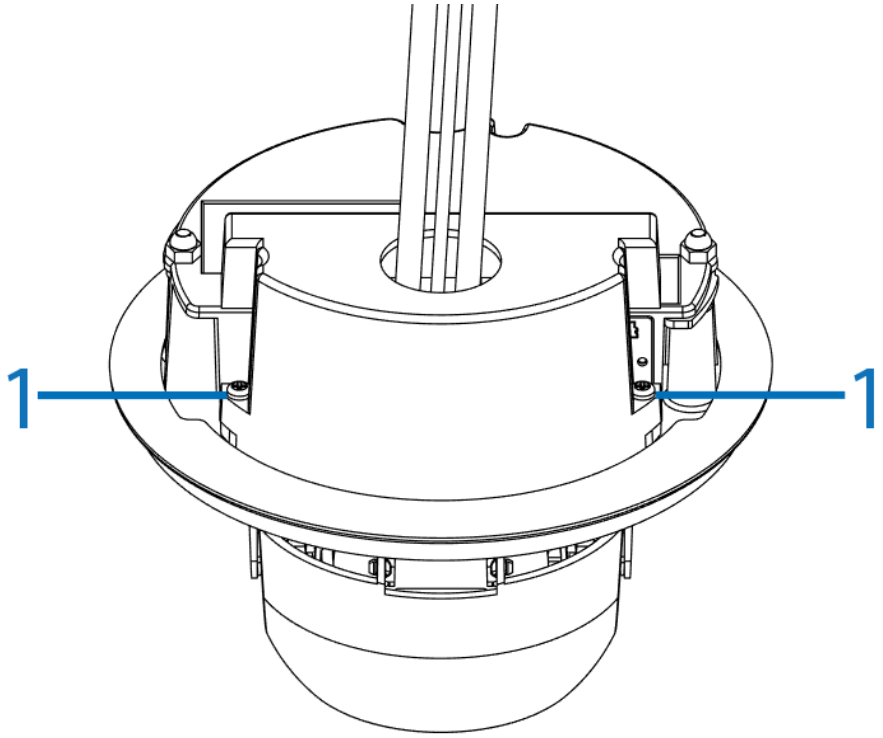
Step	Action
1	Hold the guide pattern sticker up to the ceiling (1) (Figure 9) and cut out a 125mm hole.
2	Use the T20 security key to remove the three screws on the dome cover (2) (Figure 3).
3	Use a screw driver to remove the safety lanyard screw that is connecting the dome cover to the camera.
	Note: The dome cover is now completely disconnected from the camera.
4	Place the camera cables through the hole in the ceiling, the metal cover (2) (Figure 9) and the trim plate (3) (Figure 9).

Figure 9 Installing the camera into a ceiling



5	Connect the cables to their respective ports on the camera and align the two screws on the metal cover (2) (Figure 9) with the holes on the camera and use a screw driver to securely attach the metal cover to the camera.
6	Ensure that the trim plate is positioned correctly around the camera.

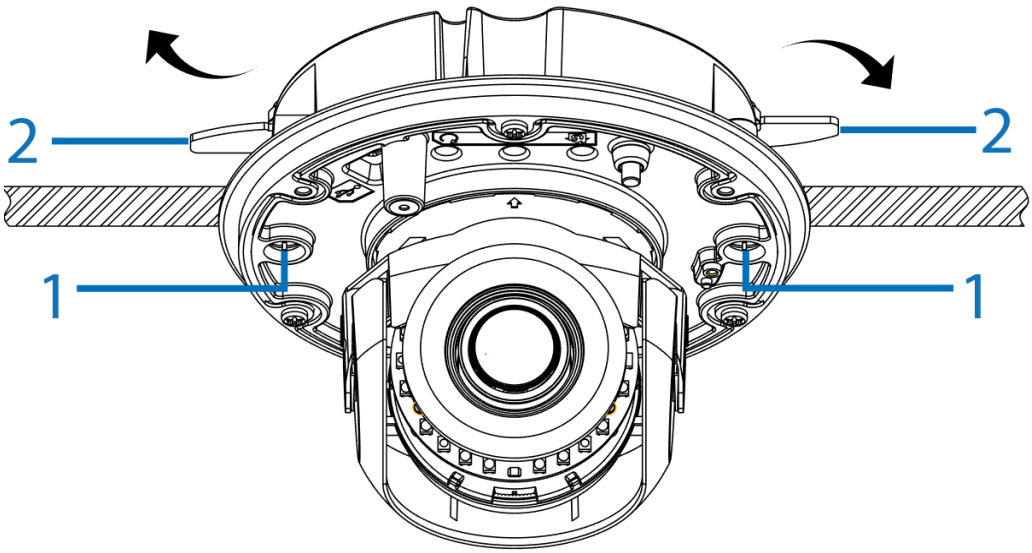
Figure 10 Metal cover attached to the camera



7 Push the camera cable back into the hole in the ceiling and hold the camera up to the hole in the ceiling.

8 Use a cross screw driver and turn both captive screws (1) (Figure 11) on the camera clockwise to extend out the locking arms (2) (Figure 11), then rotate the two captive screws anti-clockwise until the locking arms sit securely to the ceiling.

Figure 11 Ceiling locking springs



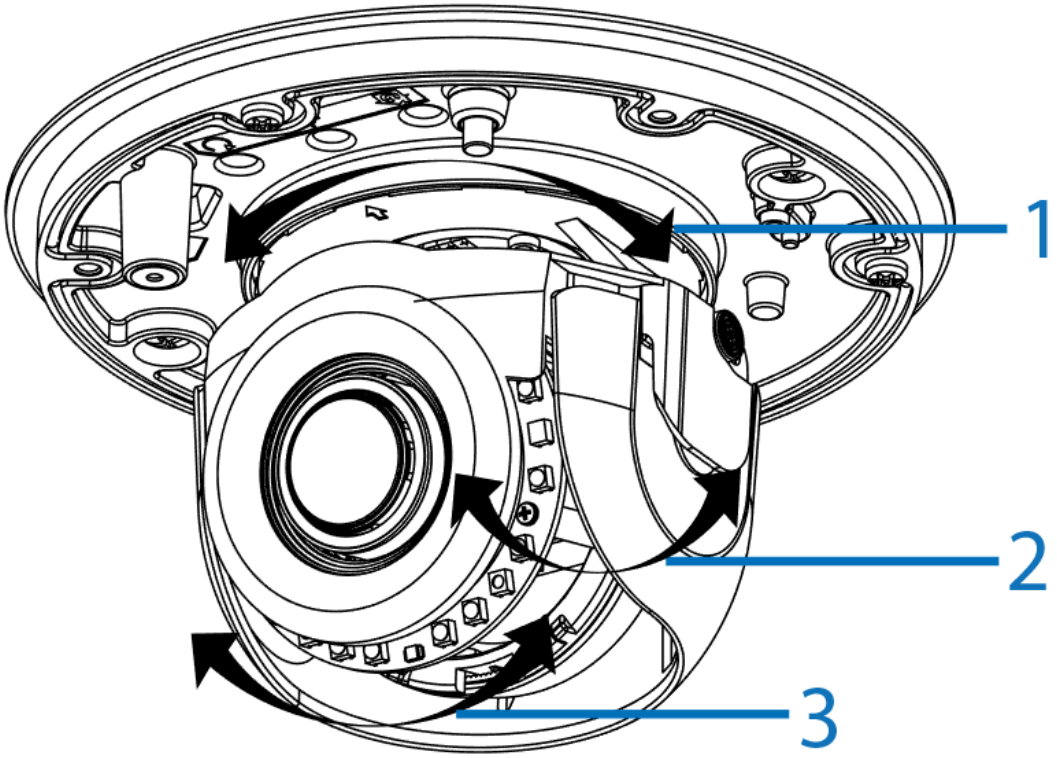
9 Adjust the camera lens position as follows. See Figure 12.

- Pan Adjustment (1): Rotate the lens base until you are satisfied with the field of view.
- Tilt Adjustment (2): Tilt the eyeball assembly as needed.
- Rotate Adjustment (3): Rotate the 3D assembly in the camera base.

Limitations for the three axis positions:

- Pan range = ±380°
- Tilt range = 15°～ 90°
- Rotation range (lens) = Motorized +/- 175°

Figure 12 Camera pan, tilt and rotation



10 Insert the dome cover safety lanyard screw into the camera and securely attach the dome cover to the camera.

11 Hold the dome cover up to the camera and align the three screws in the dome cover with the three holes on the camera.

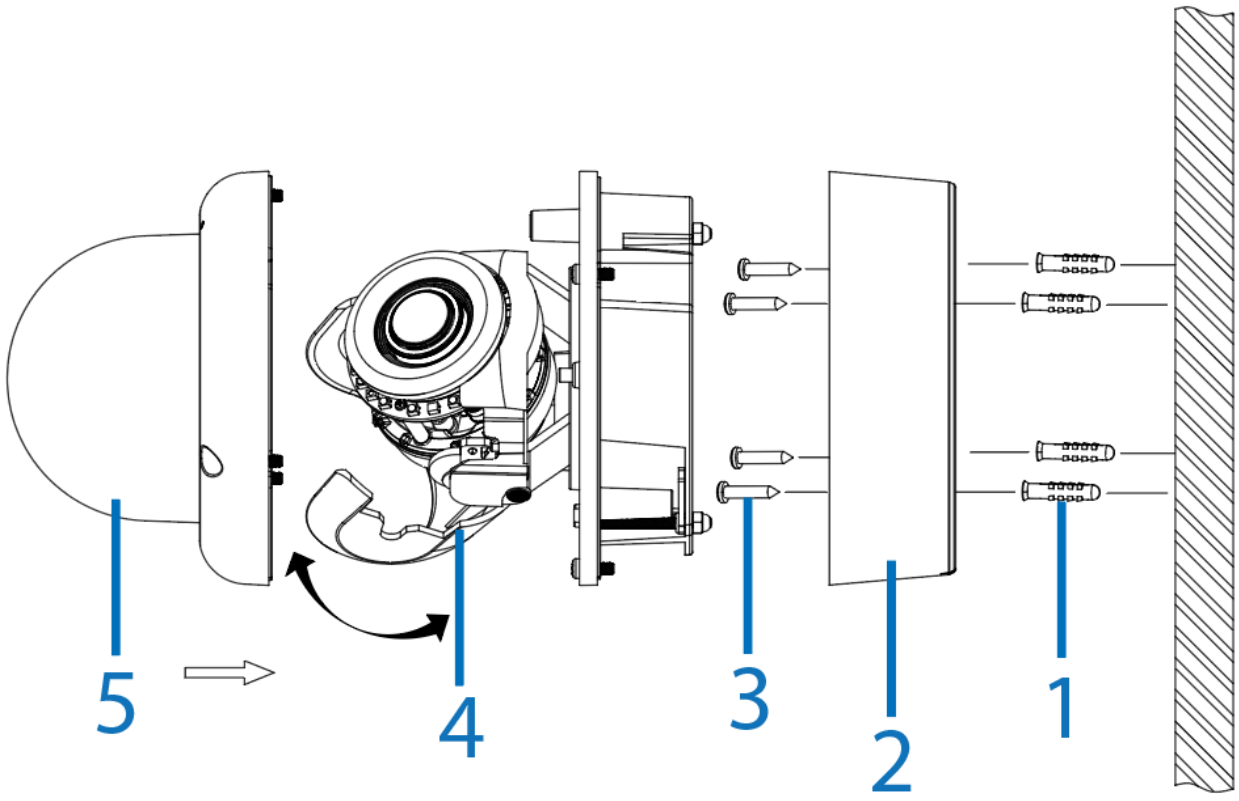
12 Use the T20 security key to securely attach the three screws to the camera.

- End -

Procedure 3 Installing the camera onto a wall or ceiling

Step	Action
1	Use the T20 security key to remove the three screws on the dome cover (2) (Figure 3).
2	Use a screw driver to remove the safety lanyard screw that is connecting the dome cover to the camera. **Note:** The dome cover is now completely disconnected from the camera.
3	Insert the cables through one of the waterproof rubbers: a if you are using the three hole waterproof rubber then pierce three holes as per the three circles on the rubber, insert the cable through the three rubber holes and then terminate the cable. OR a if you are using the one hole waterproof rubber then pull the rubber pin to make the cable hole, insert the terminated cable into the insert tool and then .pull the insert tool through the hole.
4	Hold the guide pattern sticker up to the surface and drill four 6mm holes and if you are not using the cable side entry hole on the bottom case then cut out a cable entry hole on the surface as per the guide pattern. **Note:**If you are not using the cable side entry hole then insert the cable cover.
5	Use a hammer to insert the four screw anchors (1) (Figure 13) into the holes
6	Hold the camera bottom case (2) (Figure 13) up to the surface and align the four 6mm holes on the surface with the four holes in the bottom case (remove the rubber inserts in the bottom case first).
7	Insert the four TP4, 32mm screws (3) (Figure 13) and securely attach the bottom case to the surface.
8	Pull the camera power cables through the cable hole on the surface or the side entry hole on the bottom case.
9	Hold the camera (4) (Figure 13) up to the bottom case and connect the cables to their respective ports on the camera.
10	Insert the camera into the bottom case and use a T20 security key to securely attach the camera to the bottom base with the three T20 screws.
11	Adjust the camera lens position as per step 9 in the Installing the camera in to a recess ceiling procedure.
12	Screw the safety lanyard screw into the camera so that the dome cover is attached to the camera.
13	Hold the dome cover (5) (Figure 13) up to the camera and align the three screws in the dome cover with the three holes on the camera.
14	Use the T20 security key to securely attach the three screws to the camera.

Figure 13 Mounting the camera onto a surface

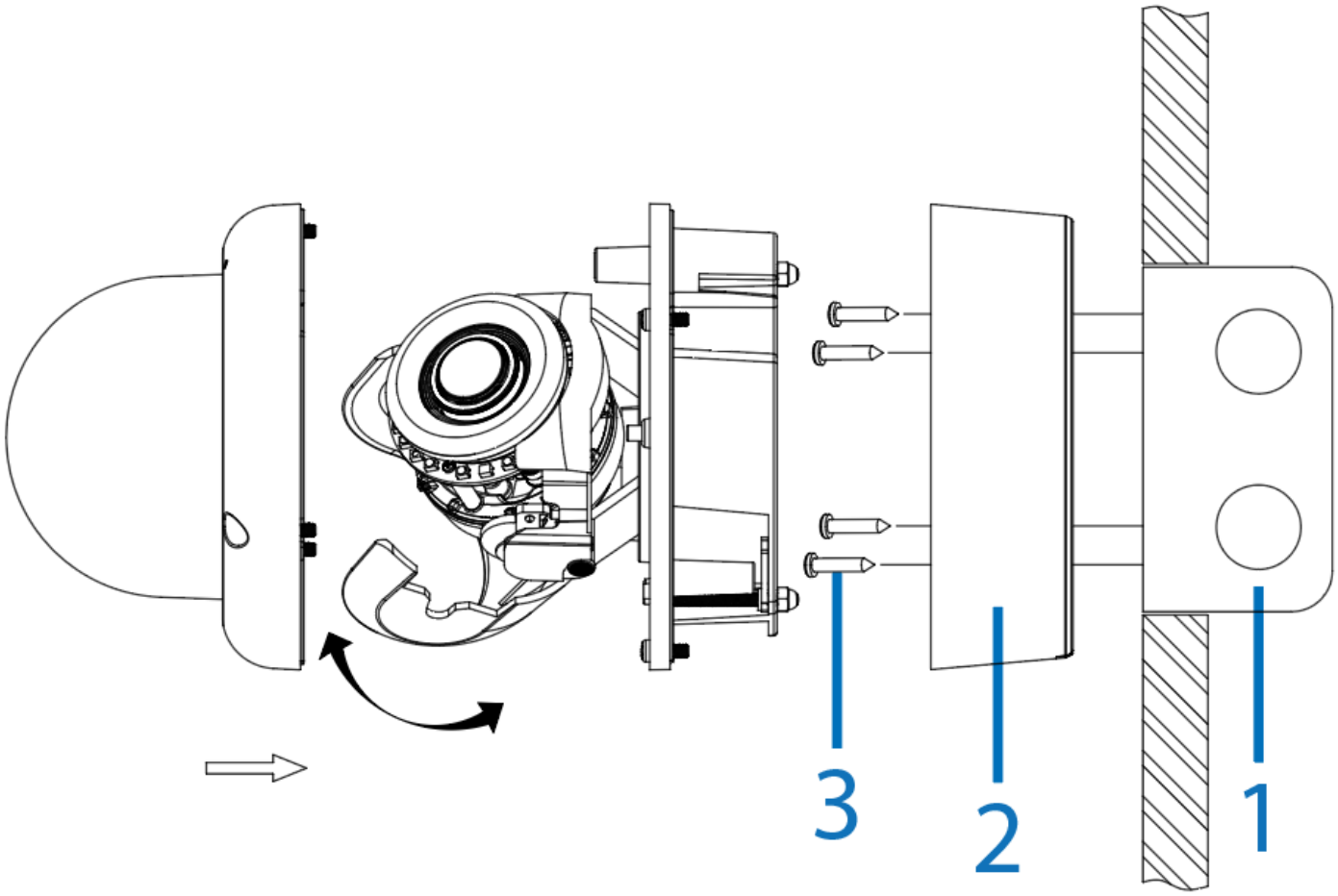


- End -

Procedure 4 Installing the camera onto a surface with a recessed junction box

Step	Action
1	See steps 1, 2, and 3 in the Installing the camera onto a wall or ceiling procedure.
2	Remove the four screws from the junction box.
3	Insert the four screws anchors onto the four holes on the junction box (1) (Figure 14).
4	Hold the camera bottom case (2) (Figure 14) up to the junction box and align the four holes on the camera bottom case with the four holes on the junction box
5	Insert the four screws and securely attach the bottom case to the junction box.

Figure 14 Installing the camera onto a surface with a recessed junction box



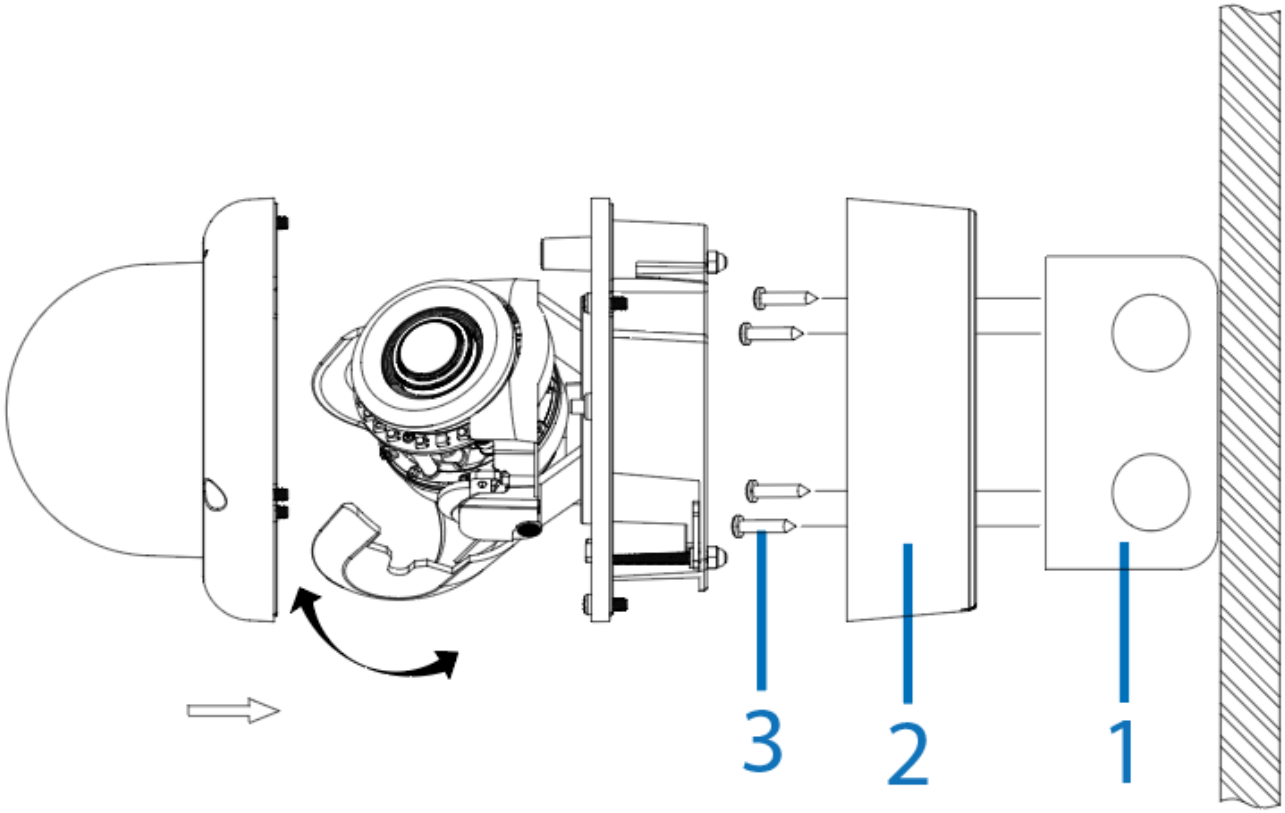
6 See steps 8 to 14 in the Installing the camera onto a wall or ceiling procedure to complete the installation.

- End -

Procedure 5 Installing the camera onto a surface with a junction box

Step	Action
1	See steps 1, 2, and 3 in the Installing the camera onto a wall or ceiling procedure.
2	Remove the four screws from the junction box.
3	Hold the camera bottom case (2) (Figure 15) up to the junction box (1) (Figure 15) and align the four holes on the camera bottom case with the four holes on the junction box
4	Insert the four screws and securely attach the bottom case to the junction box.

Figure 15 Installing the camera onto a surface with a junction box



5 See steps 8 to 14 in the Installing the camera onto a wall or ceiling procedure to complete the installation.

- End -

Weather shield cover (SOLD SEPARATELY) box contents:

- 1 x weather hood bracket
- 1 x weather shield cover (Part Number = IA-CAP-WH-P4D)
- 2 x M4 6mm screws
- 2 x M4 captive screws

The following tools assist with the installation procedure below:

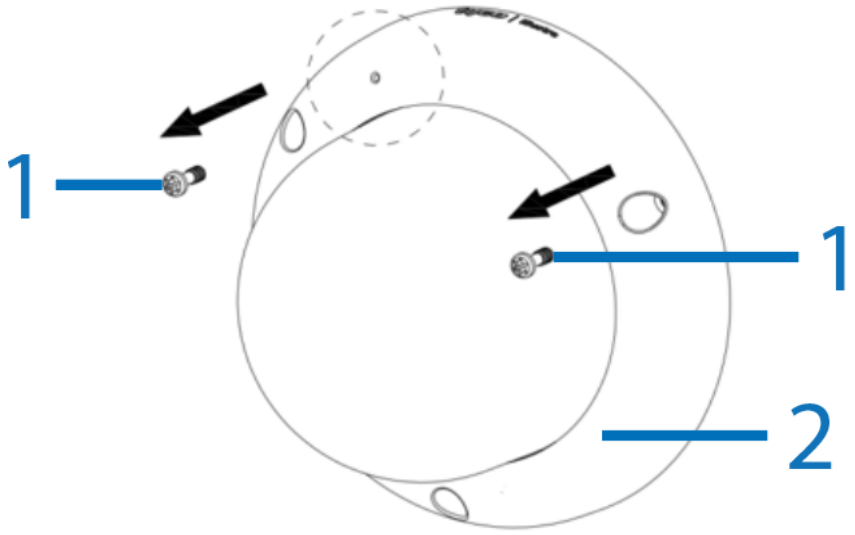
- T20 screwdriver

Procedure 6 Attaching the weather shield cover to the camera

Step	Action
1	Use the T20 screwdriver and remove the two M4 captive screws (1) (Figure 16) on the camera top cover (2) (Figure 16).

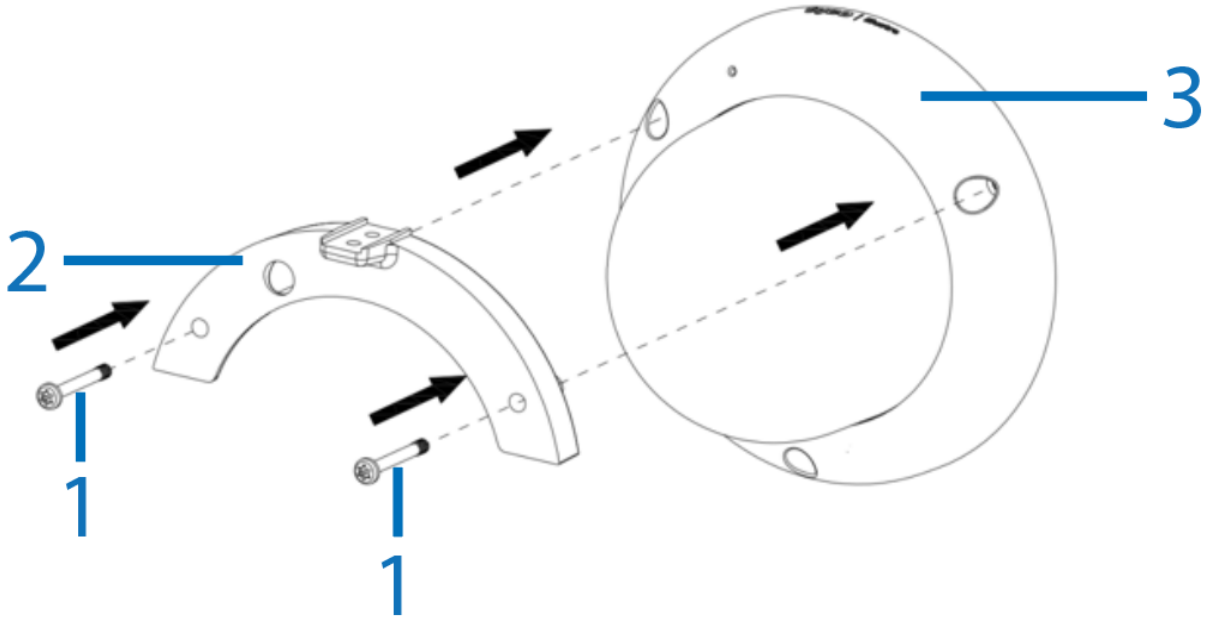
Note: The two screws are located either side of the 'Illustra' logo on the camera.

Figure 16 M4 Captive screws



2	Hold the bracket (2) (Figure 17) up to the camera dome cover (3) (Figure 17) and align the two holes on the bracket with the two holes on the camera dome.

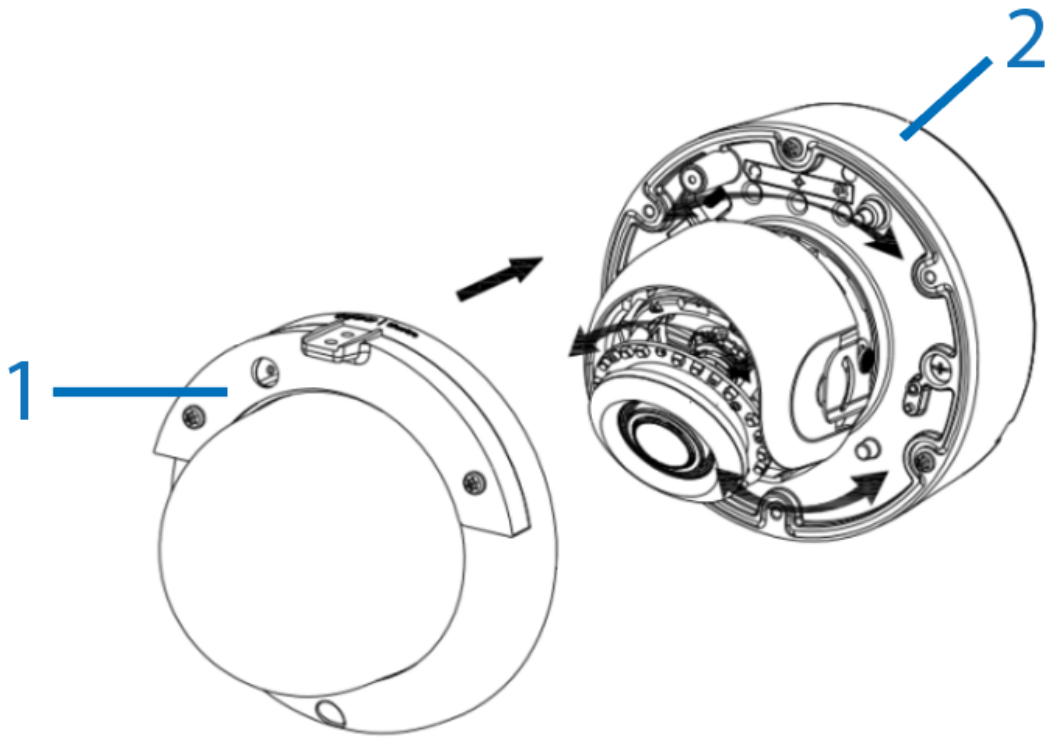
Figure 17 Bracket and screws



3 Insert the two new screws (1) (Figure 17) fully into the two-holes on the bracket and camera dome cover.

4 Hold the bracket and camera dome cover (1) (Figure 18) up to the camera base (2) (Figure 18) and align the two M4 screws on the bracket with the two holes on the camera base.

Figure 18 Bracket and Dome cover

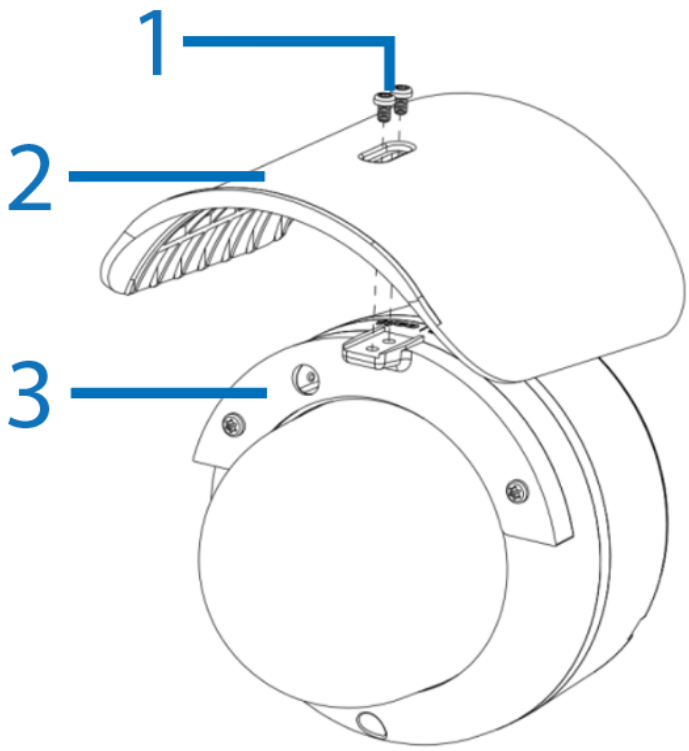


5 Use the T20 screwdriver and securely insert the two M4 screws on the bracket into the two holes on the camera base.

6 Use the T20 screwdriver and securely attach the remaining third screw on the camera dome.

7 Place the weather shield cover (2) (Figure 19) onto the bracket (3) (Figure 19) and align the two holes on both.

Figure 19 Weathershield cover and screws



8 Use the Phillips screwdriver and securely insert the two M4 6mm screws (1) (Figure 19) to securely attach the weather shield cover to the bracket.

Note: For additional installation and configuration recommendations, please refer to the new Illustra LPR Best Practice Guide at Tyco Illustra Cameras | Beyond Security.

Warnings

1 Installation and service should be performed only by qualified and experienced technicians and comply with all local codes and rules to maintain your warranty.

2 Wipe the camera with a dry soft cloth. For tough stains, slightly apply with diluted neutral detergent and wipe with a dry soft cloth.

3 Do not apply benzene or thinner to the camera, which may cause the surface of the unit to be melted or lens to be fogged.

4 To Meet EU EMC immunity requirements for security equipment the mains power for equipment powering this unit should be backed up by an uninterruptible power supply.

5 Avoid operating or storing the unit in the following locations:

- Near fluorescent lamps or objects with reflections.
- Under unstable or flickering light sources.

	Mounting, that includes climbing ladders, installing communications, power, etc. can be hazardous. Only skilled person(s) should install this device This camera can be mounted at a distance greater than 2 meters (6.6 feet) from the floor, there is a risk of Injury if the camera falls, ensure the camera is securely mounted.

Note: See IA-KIT-WD-UUA | Illustra (illustracameras.com) for more information on the USB cable mentioned in Table 8. IA-KIT-WD-UUA together with the Illustra Tools application lets users install, configure, and maintain cameras. Scan one of the QR codes below to access the application.

iOS

Android

Illustra PG4 Series 2MP, 4MP, 5MP LPR and 8MP Indoor / Outdoor Bullet Cameras

This chapter provides product features, installation procedures, and connection information regarding the Illustra Pro Gen 4 Series 2MP, 4MP, 5MP LPR and 8MP Indoor / Outdoor Bullet cameras.

Product overview

This chapter explains the features and installation of the PG4 Bullet cameras. Product codes and descriptions of the cameras are provided in the table below.

Table 20 Product code and description of the PG4 Bullet cameras

Product Code	Description
IPS02-B12-OIA4	Illustra Pro Gen4 2MP Standard Bullet, indoor/outdoor, white, TDN w/IR, TWDR
IPS02-B15-OIA4	Illustra Pro Gen4 2MP Standard Bullet, indoor/outdoor, white, TDN w/IR, TWDR
IPS04-B12-OIA4	Illustra Pro Gen4 4MP Standard Bullet, indoor/outdoor, white, TDN w/IR, TWDR
IPS04-B12-OTA4	Illustra Pro Gen4 4MP Standard Bullet, indoor/outdoor, white, TDN, TWDR
IPS04-B16-OIA4	Illustra Pro Gen4 4MP Tele Bullet, indoor/outdoor, white, TDN w/IR, TWDR
IPS08-B13-OIA4	Illustra Pro Gen4 8MP Standard Bullet, indoor/outdoor, white, TDN w/IR, TWDR
IPS08-B16-OIA4	Illustra Pro Gen4 8MP Tele Bullet, indoor/outdoor, white, TDN w/IR, TWDR
IPS05-B12-LPR4	Illustra Pro Gen4 5MP LPR Bullet, indoor/outdoor, white, TDN w/IR, TWDR
IPS05-B16-LPR4	Illustra Pro4 5MP LPR Bullet, indoor/outdoor, 13-55mm, AI, TDN w/IR, TWDR

Note: The following relates to the 5MP LPR camera only. Correct camera installation and configuration are required to achieve optimal performance of the License Plate Recognition solution. Please ensure the LPR Best Practice Guide is reviewed in this manual prior to installation.

Installation

In the box

Check everything in the packing box matches to the order form and the packing slip. In addition to this guide, items below are included in the packing box:

- 4 x plastic screw anchors (use on masonry walls and wood)
- 4 x Phillips pan head tapered screw TP6x32mm (use on masonry wall and wood)
- 1 x Printed Quick Start Guide
- 1 x Printed regulatory document
- 1 x RJ45 Connector
- 1 x Terminal block
- 1 x Mounting arm
- 1 x Mounting template
- 1 x Desiccant bag
- 4 x Toggle screw (Expansion Bolt)
- 1 x T10 security Torx wrench
- 1 x Pendant / pole mount adaptor
- 1 x rubber plug (with two holes) and 1 rubber pin
- 1 x rubber plug (with no holes)
- 1 x 4mm Allen key
- 1 x Reset Pin

Contact your dealer if any item is missing.

Installation tools

The following tools assist with installation:

- 1 x Phillips Screw driver
- 1 x Drill
- 1 x T10 security Torx wrench

Quick Reference

- Default IP: 192.168.1.168 (DHCP enabled)
- Default Username / Password: admin / admin
- Power: 24V AC, 50/60Hz, 1.27A or PoE 48V DC 0.53A.

Note: The camera will support PoE+ power detection to enable additional IR range (50m (PoE), 70m (PoE+).

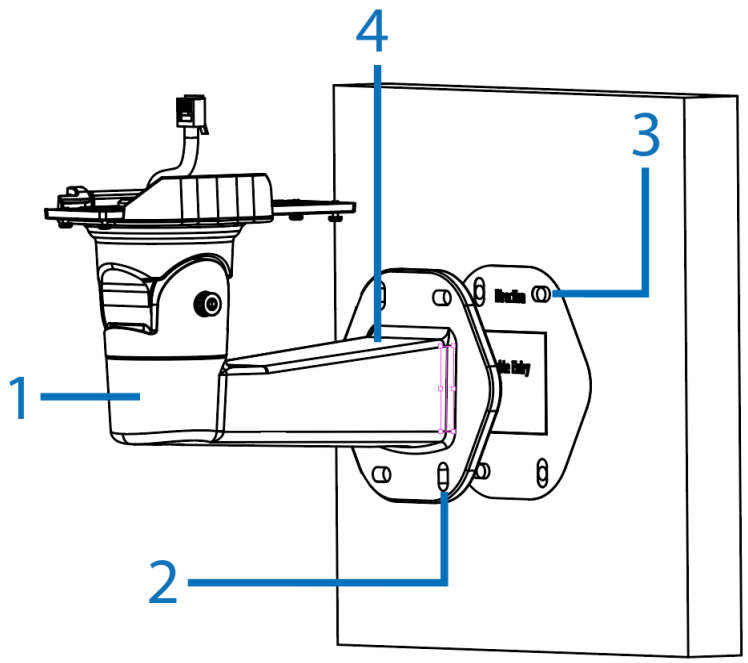
Note: You can attach the camera to a surface or directly to a pendant or pole 1 ½ '' Male NPT pipe using the pendant / pole mount adaptor. (The pendant / pole mount adaptor can be attached to a standard 1 ½'' NTP pipe using threads or set screws).

Note: To ensure optimal lens performance, JCI recommends using the automated lens calibration feature within the web GUI following initial camera installation.

Procedure 7 Attaching the mounting arm to a surface

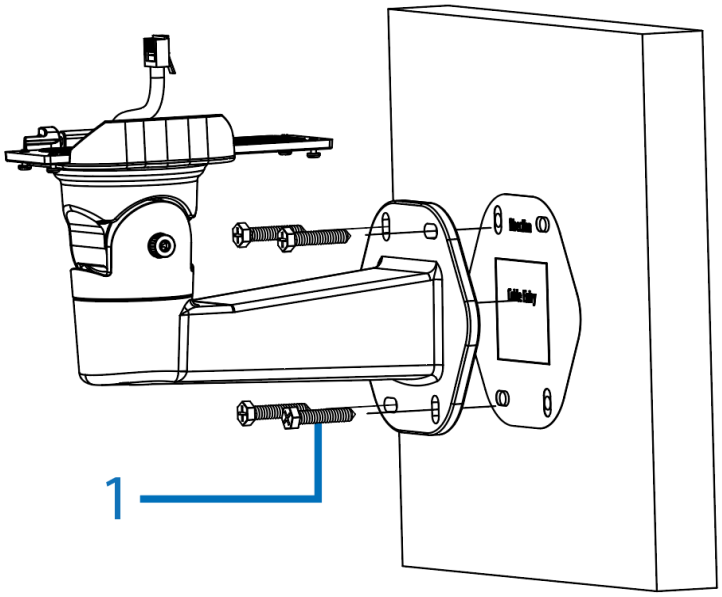
Step	Action
1	Place the mounting template provided on the surface and drill four 8mm (0.314inch) holes.
2	Insert the four screw anchors into the four holes on the surface.
3	After passing all required cabling through the mounting arm, place the mounting arm (1) (Figure 21) on the surface and align the four holes on the mounting arm (2) (Figure 21) with the four screw anchors or expansion bolts on the surface (3) (Figure 21).

Figure 21 Mounting arm and surface



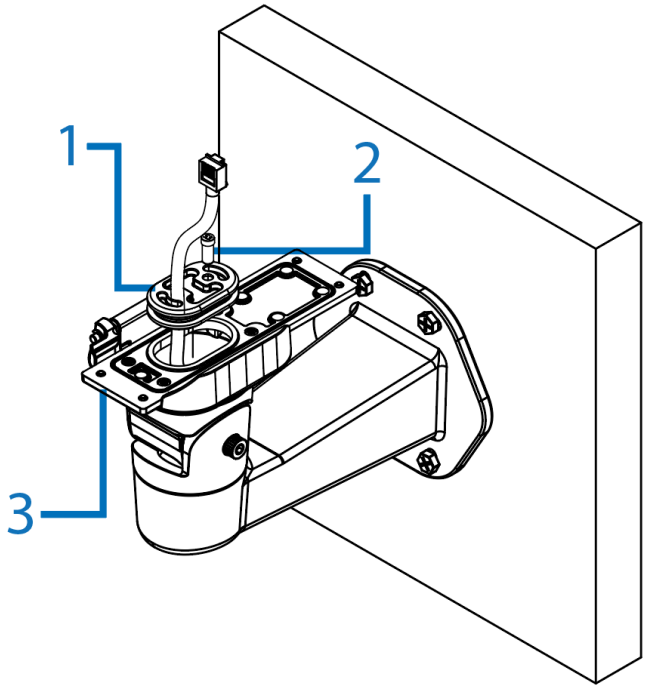
4	Insert the rubber plug into the top hole on the mounting arm (4) (Figure 21) to prevent water from entering the mounting arm.
5	Securely attach the mounting arm to the surface with the four TP6x32mm screws (1) (Figure 22).

Figure 22 Mounting arm screws



6 Insert the Ethernet cable through the waterproof rubber (1) (Figure 23) and if not using both grommet holes insert the rubber pin (2) (Figure 23) into the waterproof rubber.

Figure 23 Inserting the waterproof rubber insert



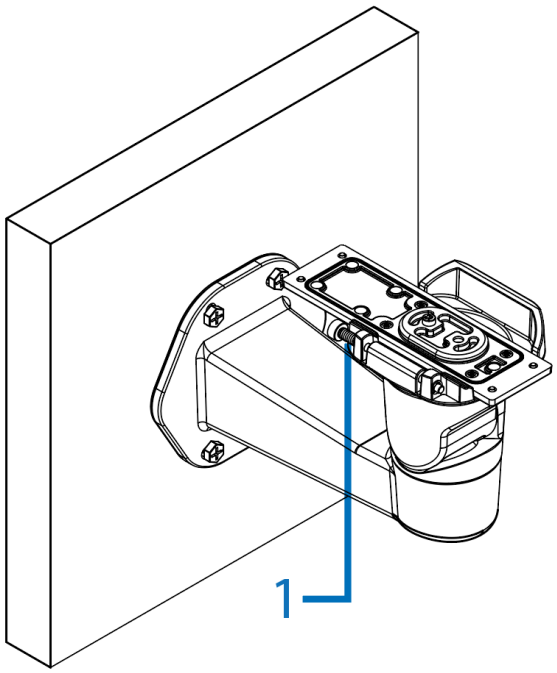
7 Insert the waterproof rubber onto the mounting arm plate. (3) (Figure 23).

- End -

Procedure 8 Attaching the camera to the mounting arm

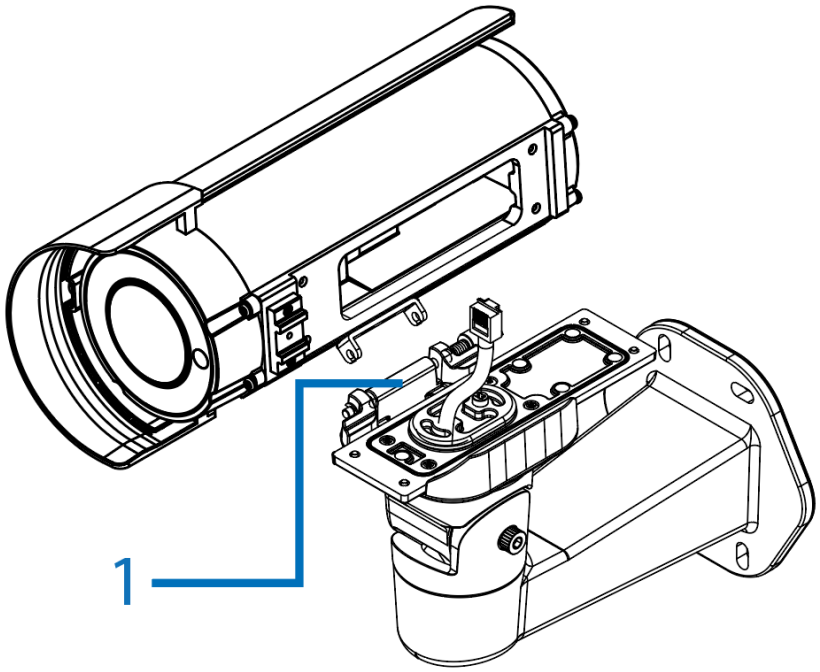
Step	Action
1	Push the pin (1) (Figure 24) from the mounting arm hinge.

Figure 24 Mounting arm pin



2	Place the camera onto the hinge (1) (Figure 25) and release the pin so that the camera is attached to the mounting arm plate.

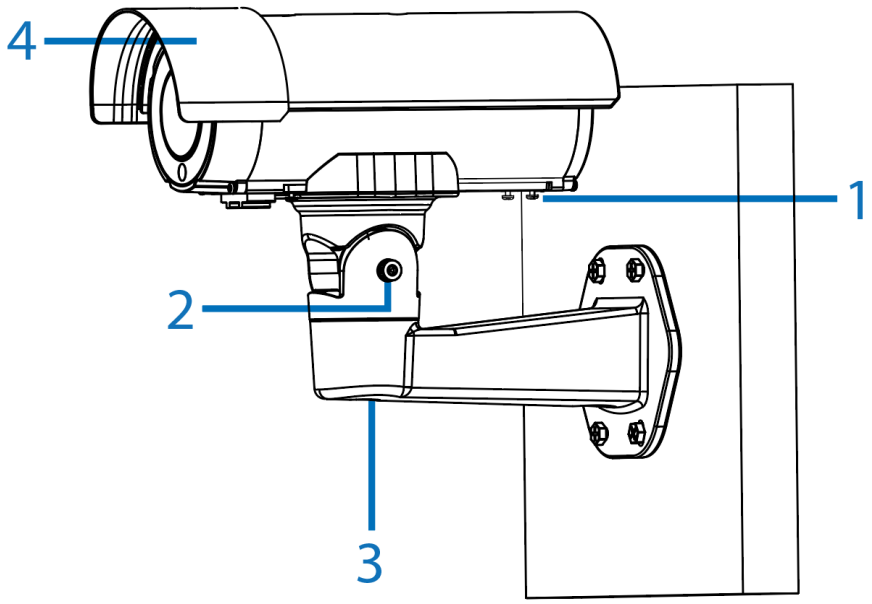
Figure 25 Mounting arm hinge



3 See the *Connecting the power cable to the power plugs* procedure and then continue at step 4.

4 Flip the camera so that it sits properly on the mounting arm plate and secure it to the mounting arm plate with the four T10 screws (1) (Figure 26).

Figure 26 T10 screws

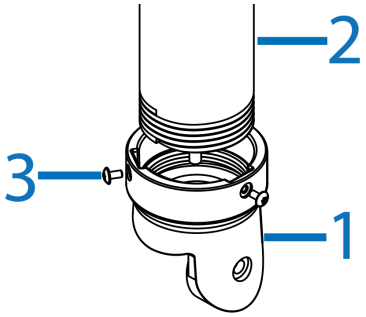


- End -

Procedure 9 Attaching the camera to a pendant or pole 1 ½ '' NTP pipe

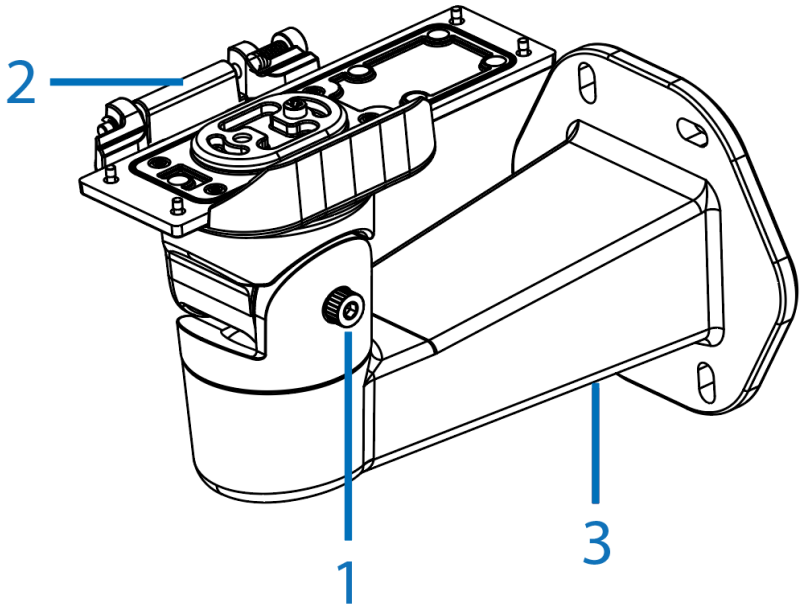
Step	Action
1	Place the pendant/pole mount adaptor (1) (Figure 27) around a standard 1 ½'' Male NPT threaded water pipe (2) (Figure 27) and securely attach the two M3x0.5P (L = 6mm) screws (3) (Figure 27) on the pendant mount adaptor with the T10 security Torx wrench.

Figure 27 NTP Pipe



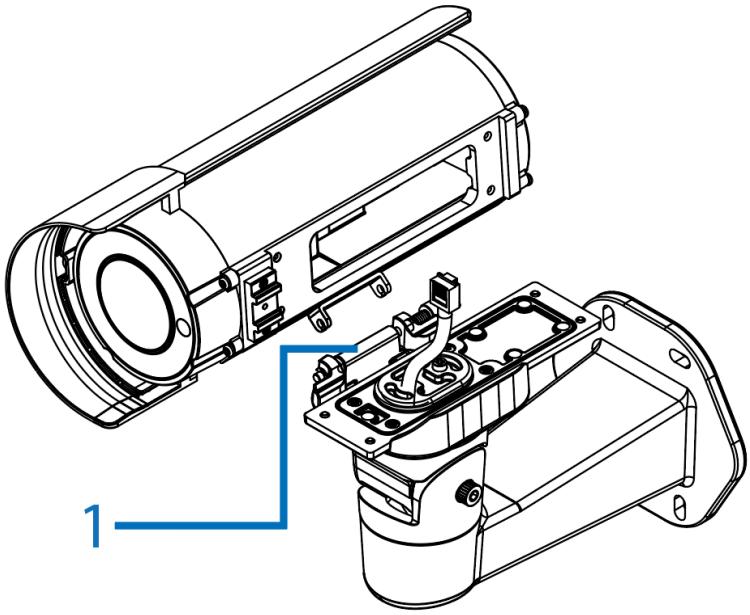
2	Unscrew the M5 Hex socket cap screw (1) (Figure 28) to remove the mounting arm plate (2) (Figure 28) from the mounting arm (3) (Figure 28).

Figure 28 Mounting arm plate



3	Push the pin (1) (Figure 29) and place the camera onto the hinge and release the pin so that the camera is attached to the mounting arm plate.

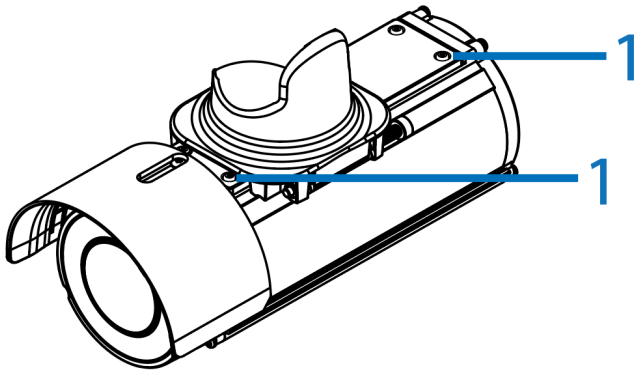
Figure 29 Mounting arm plate pin



4 See the *Connecting the power cable to the power plugs* procedure and then continue at step 5.

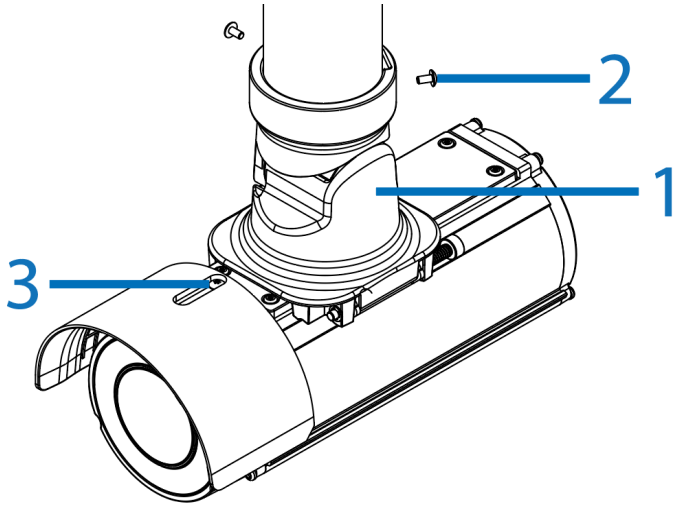
5 Securely attach the mounting arm plate to the camera with the four T10 screws (1) (Figure 30) on the mounting arm plate.

Figure 30 T10 screws



6 Place the mounting plate arm and camera into the pendant mount adaptor (1) (Figure 31) and securely attach the two M3x0.5P (L = 6mm) screws (2) (Figure 31) with the T10 security Torx wrench.

Figure 31 Pendant mount adaptor and camera



- End -

Procedure 10 Connecting the power cable to the power plugs

Step	Action
1	Connect the power cable to the power plugs with one of the following options: • AC 24V: Connect 24V cables to terminals AC 24V. • OR • PoE: Connect the RJ45 jack to a PoE compatible network device that supplies power through the Ethernet cable.

- End -

Procedure 11 Adjusting the camera position

Step	Action
1	Use the T10 security Torx wrench to adjust the bracket Tilt angle (2) (Figure 26) and to adjust the bracket Pan angle (3) (Figure 26).

- End -

Procedure 12 Adjusting the sun shield hood

Step	Action
1	Move the sun shield hood (4) (Figure 26) forward and backward to adjust the position of the sunshade. **Note:**When the camera is mounted inverted to a pendant 1 ½ '' NTP pipe you must remove the sun shield hood by unscrewing the M3x0.5P (L = 8mm) screw with the T10 security Torx wrench (3) (Figure 31) and relocate the sun shield with screw as per the sun shield hood located in Figure 26. **CAUTION:** Extending the sun shield hood forward could obstruct the field of view (FOV) when the camera lens is set to 'Wide'.

- End -

Procedure 13 Location of camera buttons, connections, and Desiccant bag

The figure below indicates the location of the camera buttons and connections (1) (Figure 32) and Desiccant bag (2) (Figure 32) on the camera.

Figure 32 Location of camera buttons, connections and desiccant bag

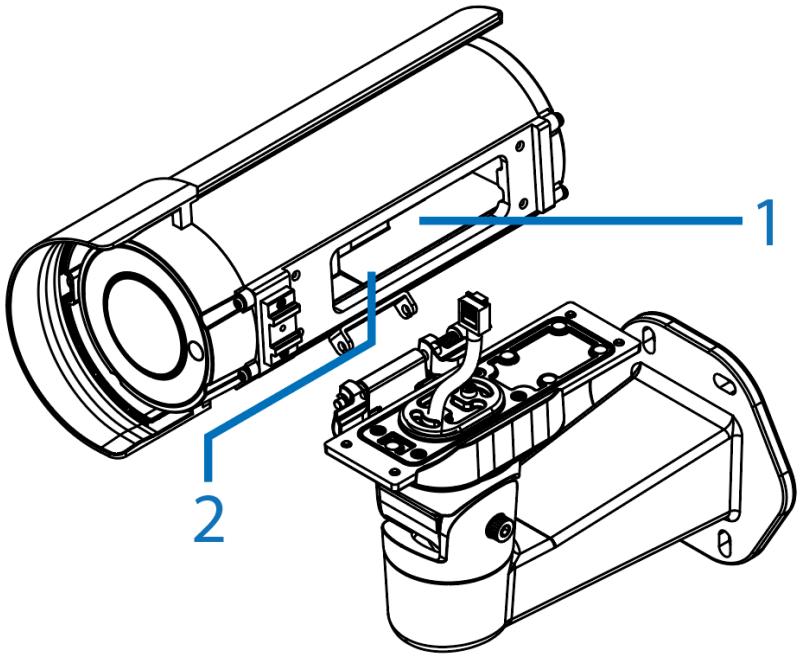
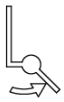


Table 33 Camera buttons / connections

Button / connections	Description
	Alarm in 1
	Alarm in 2
	Alarm out
	COM
	Audio line in
	Audio line out
	Ground
HDMI	HDMI Cable connection
	Micro SD card slot
AC 24V	AC power connection
	USB cable connection (Note: Insert the Micro USB On-The-Go (OTG) Adapter Cable with USB Wireless Network Adapter. See note and QR codes on the next page).
	Reboot button (Press and release to reboot the camera)
	Reset to Factory default but preserve IP Address (Hold for 5 seconds) Reset to factory default (Hold for 20 seconds)
	One push AF

Note: For additional installation and configuration recommendations, please refer to the new Illustra LPR Best Practice Guide at Tyco Illustra Cameras | Beyond Security.

Warnings

1. Installation and servicing shall be performed by qualified service personal only.
2. The mains power adaptor equipment should be marked LPS (Limited Current Source) or PS2 and rated according to 60C, 24VAC, 1.27A min or PoE IEEE802.3at type 2 Class 4, 48VDC, 0.53A min.
3. To meet security immunity requirements, use an uninterruptable PSU to supply power to the mains adaptor or POE mid/end span.
4. The mounting high above ground level shall be more than 3 meters from wall mount height.
5. If a Class I PoE adapter or switch is used to provided power, be sure that the power cord is firmly plugged into the socket and confirm the main earth connection.
6. Interconnecting cables for PoE is intended to be supplied by a UL Listed type CL3P, CL3R or CL3X, marked "SUNLIGHT RESISTANT", "SUN. RES." or "SR." and "water resistant" or "W"

	Mounting, that includes climbing ladders, installing communications, power, etc. can be hazardous. Only skilled person(s) should install this device This camera can be mounted at a distance greater than 2 meters (6.6 feet) from the floor, there is a risk of Injury if the camera falls, ensure the camera is securely mounted.

Note: See IA-KIT-WD-UUA | Illustra (illustracameras.com) for more information on the USB cable mentioned in Table 38. IA-KIT-WD-UUA together with the Illustra Tools application lets users install, configure, and maintain cameras. Scan one of the QR codes below to access the application.

iOS

Android

Illustra PG4 Series 5MP Corner Dome Camera

This chapter provides product features, installation procedures, and connection information regarding the Illustra Pro Gen 4 Series 5MP Corner Dome camera.

Product overview

This chapter explains the features and installation of the PG4 Corner cameras. Product codes and descriptions of the cameras are provided in the table below.

Table 34 Product code and description of the PG4 Corner camera

Product Code	Description
IPS05-R10-OIA4	Illustra Pro Gen4 5MP Corner, TDN w/IR, WDR

Installation

In the box

Check everything in the packing box matches to the order form and the packing slip. In addition to this guide, items below are included in the packing box:

- 1 x 8 pin terminal block
- 1 x 2 pin terminal block
- 3 x Plastic screw anchors
- 3 x Self-tapping screws TP4x30mm
- 2 x Desiccant bag
- 1 x Rubber with 3 holes
- 1 x Rubber with 1 hole
- 1 x RJ45 Cap
- 3 x Top rubber cap
- 1 x Security Torx Wrench (T20)
- 1 x QSG
- 1 x Regulatory Document

Contact your dealer if any item is missing.

Installation tools

The following tools assist with installation:

- 1 x Drill
- 1 x T20 Torx wrench
- 1 x Phillips screwdriver
- 1 x Wire cutters

Quick Reference

- Default IP: 192.168.1.168 (DHCP enabled)
- Default Username / Password: admin / admin
- Power: 12Vdc, 1.4A min. or 24VAC, 50/60Hz, 1A min. or PoE 48Vdc, 0.34A min., Tma=60 degree C

Note: The product is intended to be supplied by a UL Listed Power Unit marked "L.P.S." (or "Limited Power Source") and is rated output 12Vdc, 1.4A min. or 24VAC, 50/60Hz, 1A min. or PoE 48Vdc, 0.34A min., Tma=60-degree C. If need further assistance with purchasing the power source, please to Manufacturer for further information.

Figure 35 Product overview (Units in mm)

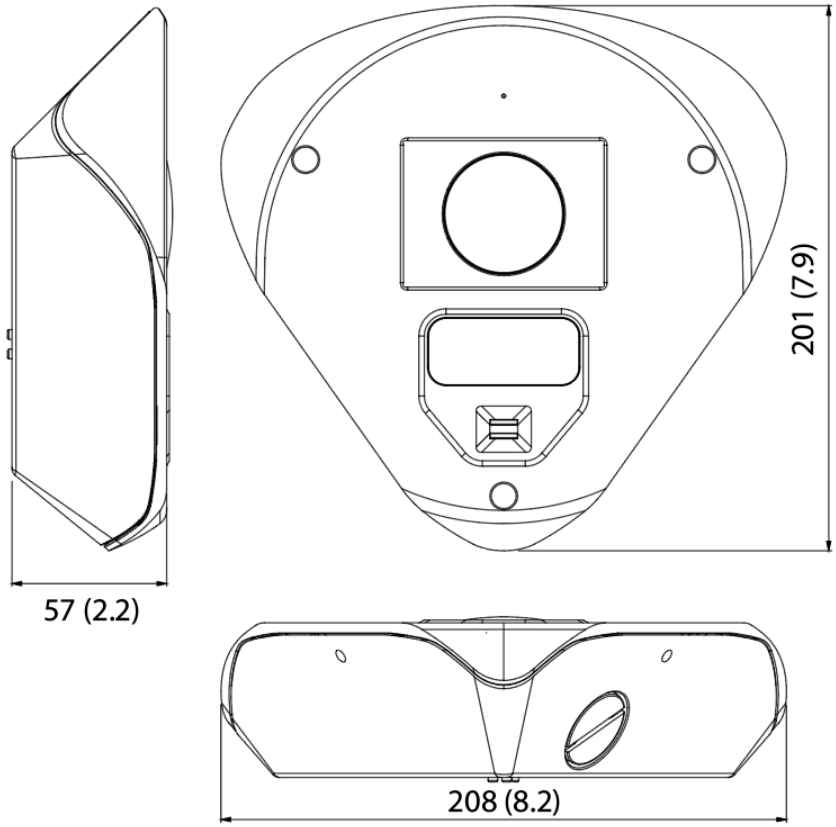
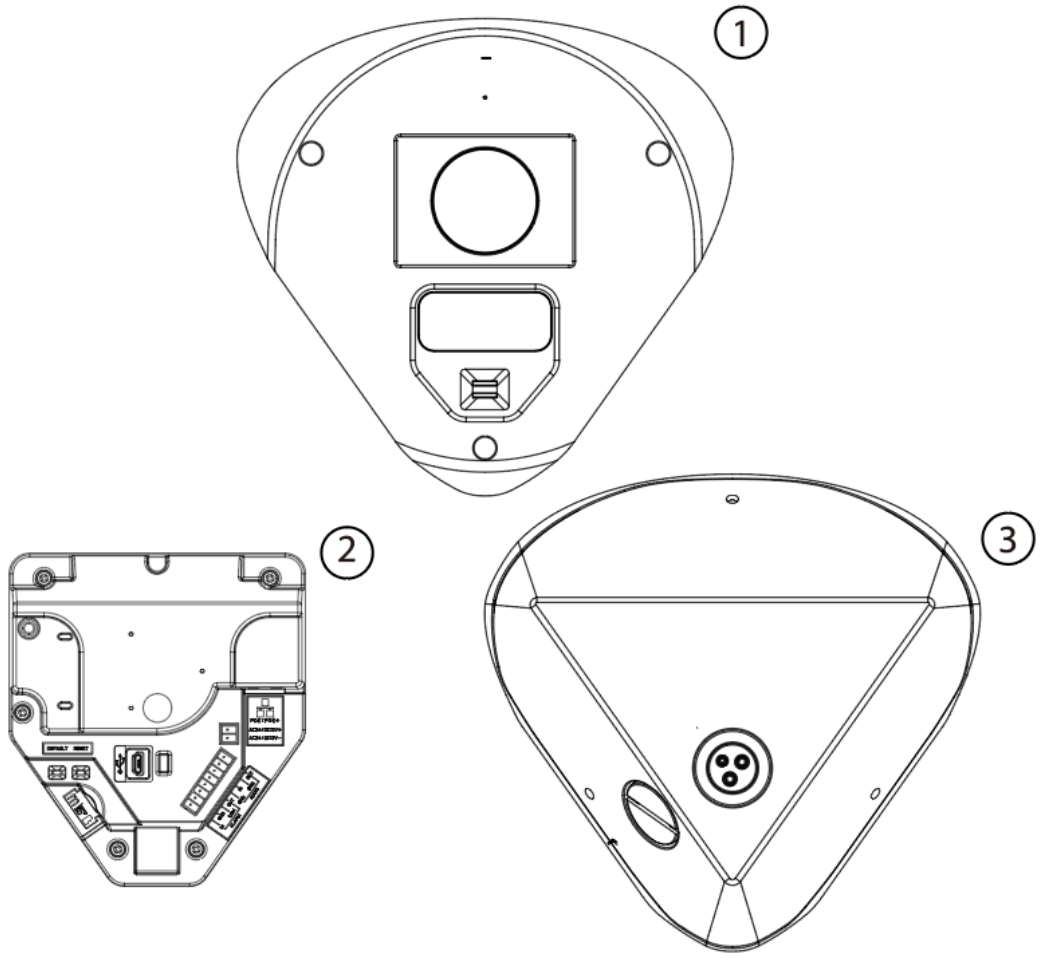


Figure 36 Camera parts

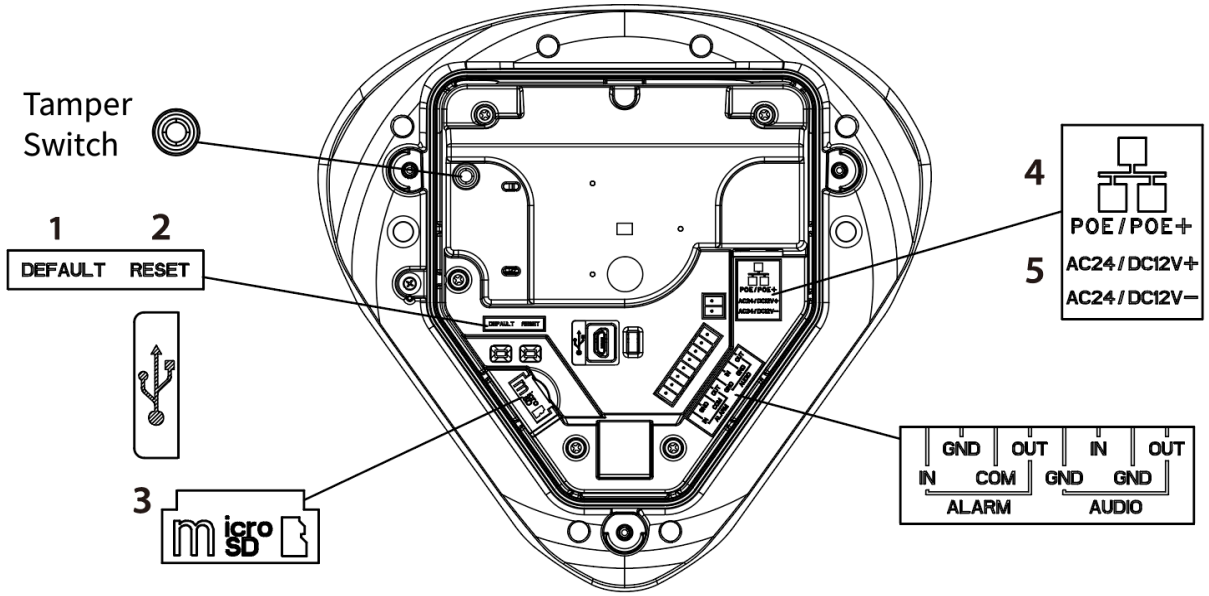


See Table 37 for a description of each part in Figure 36.

Table 37 Camera part descriptions

Number	Description
1	Camera top cover
2	Camera module
3	Bottom case

Figure 38 Camera buttons, ports and SD card location

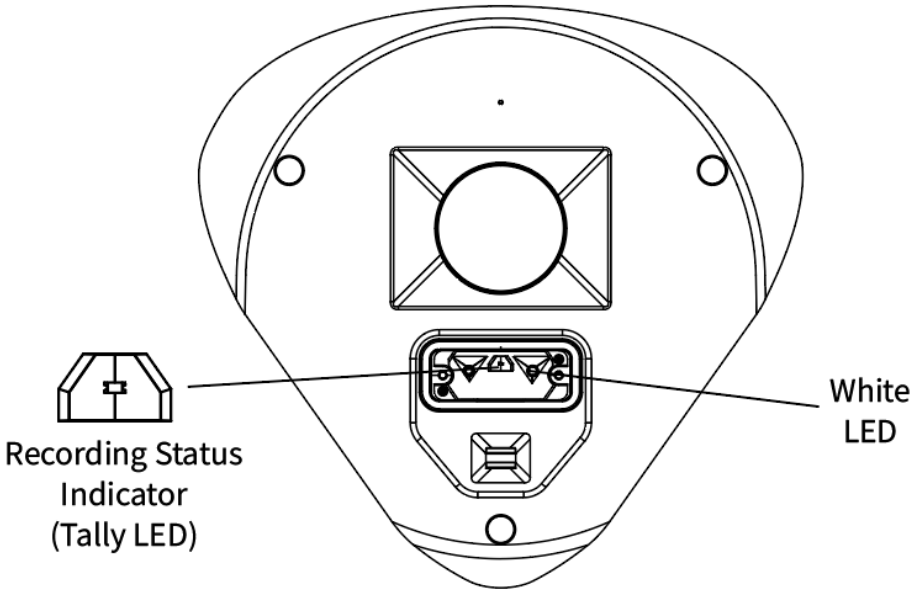


See Table 39 for a description of each part in Figure 38.

Table 39 Camera buttons, ports and SD card location descriptions

Number	Name	Description
1	Default	Reset to factory default but reserve IP address. (Hold for 5 seconds). Reset to default factory (Hold for 20 seconds).
2	Reset Button	Reset: Press the button for approximately 1 second to reboot the camera
3	USB cable port	Insert the Micro USB On-The-Go (OTG) Adapter Cable with USB Wireless Network Adapter. See note and QR codes on the next page for information.
4	Micro SD	Micro SD Port
5	RJ-45 Network Port	Connect the RJ-45 connector to this port with a PoE (IEEE 802.3af Class3) / PoE+(IEEE 802.3at Class4) compatible network device that supplies power through the Ethernet cable.
6	Power terminal	The port is used to connect with external 24VAC/12 VDC power supply.
7	DI/DO Port	DI/DO (Digital Input/Output) ports are equipped for external devices, e.g., smoke detector, siren, microphone. • Alarm In: Via “GND” and “Alarm In” ports, connect to external device that can trigger alarm input signals. • Alarm Out: Via “COM” and “Alarm Out” ports, connect to external device to be triggered through alarm output signals. • Audio In: Via “GND” and “Audio In” ports, connect to external device such as microphone that receives sound for the camera. • Audio Out: Via “GND” and “Audio Out” ports, connect to device such as speaker to be triggered through alarm output signals.

Figure 40 LED indicator location



See Table 41 for a description of each LED status.

Table 41 Recording status indicator LED descriptions

Status	Description
Always On (Default)	The tally LED is always on (flashing), even if no video or audio stream is being pulled from the device or recorded to the edge storage (SD card)
Always Off	The tally LED is always off, even if a video or audio stream is being pull from the device or recorded to the edge storage (SD card)
Auto	The tally LED is automatic on (flashing) when a video or audio stream is being pull from the device or recorded to the edge storage (SD card)

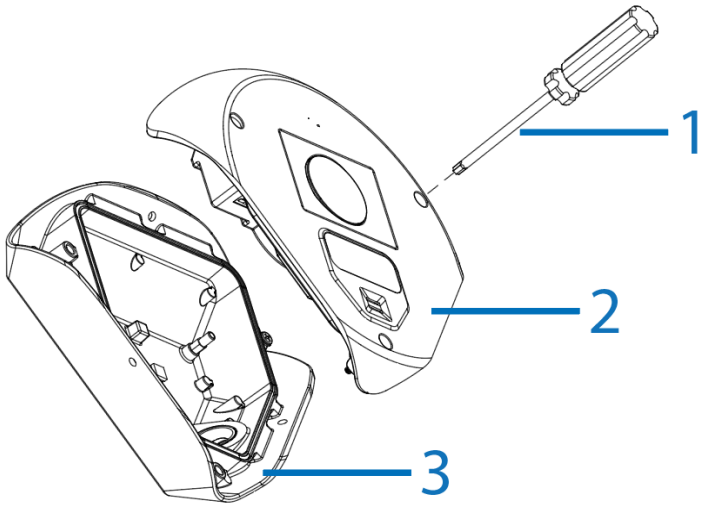
Table 42 White LED indicator descriptions

Status	Description
On	Permanently on
Auto	Automatically enables when linked to an event action
Off	Set Illuminator LED to never illuminate

Procedure 14 Installing the camera onto a wall

Step	Action
1	Use the T20 Torx wrench (1) (Figure 43) and loosen the three T20 screws located on the camera top cover (2) (Figure 43), and then remove the camera cover from the camera base (3) (Figure 43).

Figure 43 Camera top cover, base and screws



Note: You can route the power cables through the ceiling or wall.

2 Cut out a 25mm cable hole on the ceiling, close to the corner and pull all power cables through the ceiling hole, and then remove the power cable rubber insert (2) (Figure 44) on the camera base.

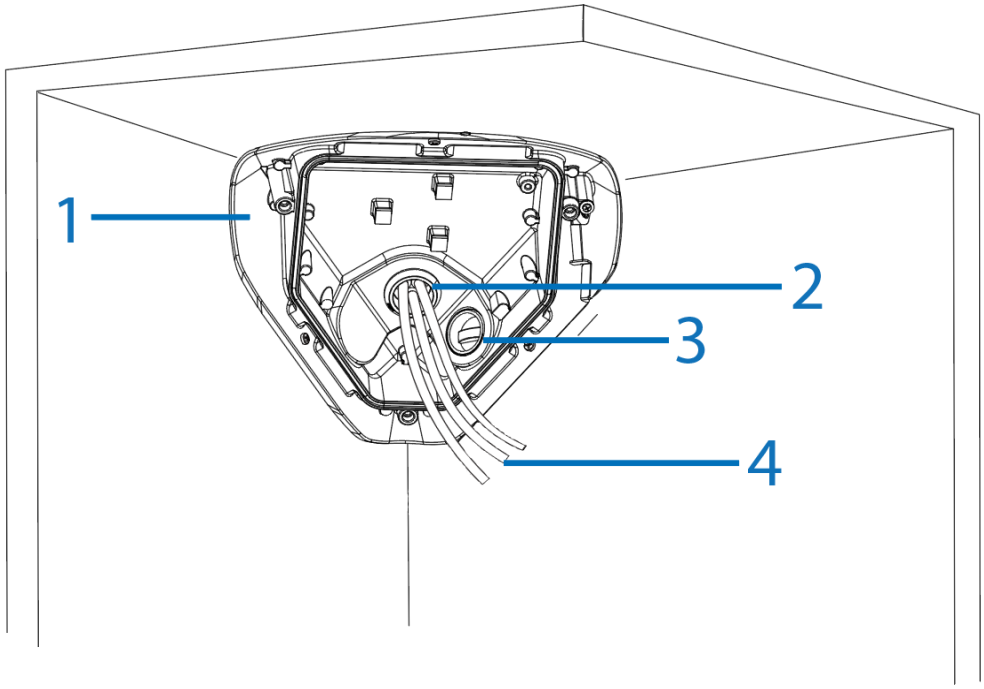
OR

Remove the cable side entry insert (3) (Figure 44) on the camera base if you are routing the cables through the wall.

3 Place the camera base (1) (Figure 44) fully into the wall / ceiling corner and using a pen / pencil, add two markings on the walls and one on the ceiling as per the three holes on the camera base.

Note: If you are routing the cables through the cable side entry hole on the camera base then also mark this out on the wall.

Figure 44 Camera base in a corner



4 Remove the camera base and drill three 7mm holes, and if you are routing the cables through the wall, then cut out a 25mm cable hole and pull the power cables through the hole on the wall.

5 Insert the three plastic screw anchors into the three holes.

6 Insert the camera base (1) (Figure 44) up to the corner:

a if the power cables are routed through the ceiling, then insert the cables (4) (Figure 44) through the rubber insert cable hole (2) (Figure 44).

OR

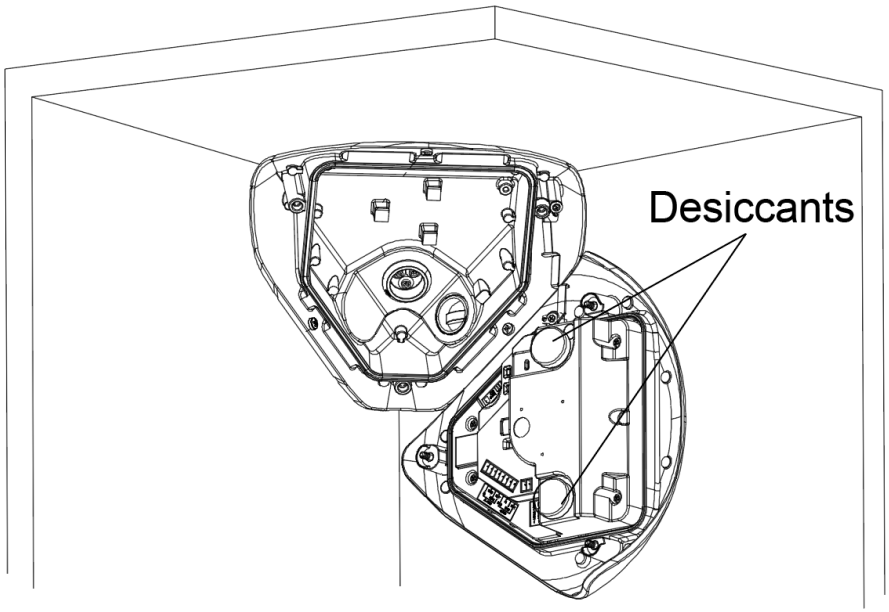
a If the cables are routed through the wall, then insert the cables through the cable side entry hole (3) (Figure 44) on the camera base.

7 Align the three holes on the camera bottom base with the three holes on the wall / ceiling.

8 Insert the three TP4x30mm screws into the three holes and use a screwdriver to securely attach the camera base to the wall.

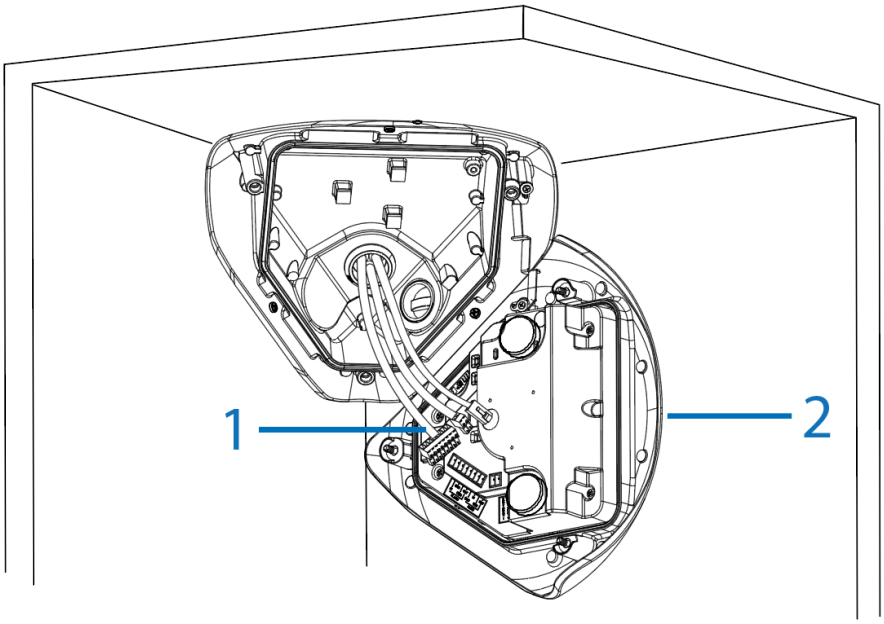
9 Insert the two desiccant bags (Figure 45) into the two slots on the camera top cover.

Figure 45 Desiccant bags



10 Hold the camera top cover (2) (Figure 46) up to the camera base and insert the power cables (1) (Figure 46) to their respective ports on the camera top cover.

Figure 46 Camera top cover

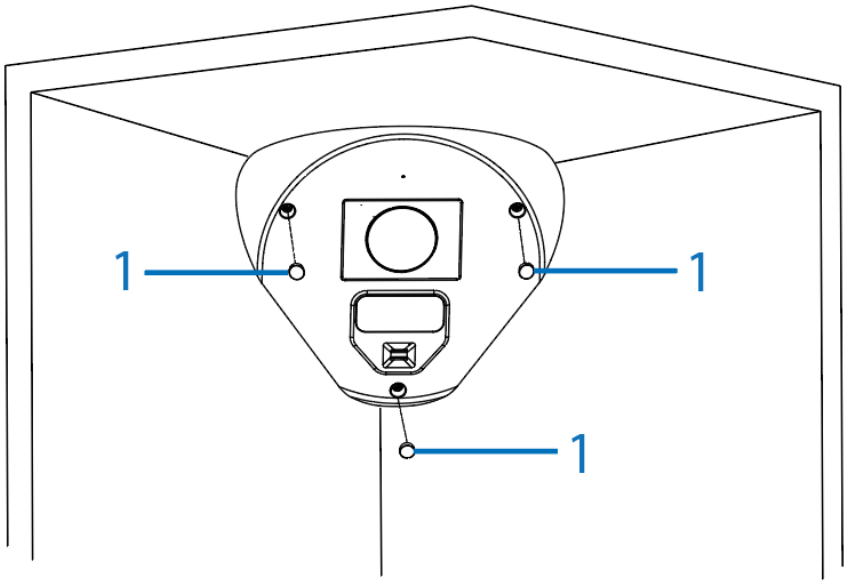


11 Place the camera top cover onto the camera base and align the three captive screws on the camera top cover with the three holes on the camera base.

12 Use the Torx wrench to securely attach the three camera top cover screws into the camera base.

13 Insert the three rubber inserts (1) (Figure 47) into the three screw holes on the camera top cover to complete the installation.

Figure 47 Rubber inserts



- End -

Procedure 15 Removing the SD card

Step	Action
1	Use the T20 Torx wrench (1) (Figure 43) and loosen the three T20 screws located on the camera top cover (2) (Figure 43), and then remove the camera cover from the camera base (3) (Figure 43).
2	Carefully pull open the micro-SD card cover (4) (Figure 38), and then insert or remove the micro-SD card into or from the camera. **Note:** It is advised that you reboot the camera after inserting the micro SD card.

- End -

Warnings

	Mounting, that includes climbing ladders, installing communications, power, etc. can be hazardous. Only skilled person(s) should install this device This camera can be mounted at a distance greater than 2 meters (6.6 feet) from the floor, there is a risk of Injury if the camera falls, ensure the camera is securely mounted.

Note: The recording status indicator is set to 'Always On' regardless of any recording or streaming activity in place or not. This can be changed to 'Auto' to reflect actual recording or streaming activity in place or set to 'Always Off' to not show recording status.

Note: Choice of power determines the cameras Operating Temperature -20°C ~ 60°C = PoE & DC12V and -40°C ~ 60°C = PoE+ & AC24V

Note: See IA-KIT-WD-UUA | Illustra (illustracameras.com) for more information on the USB cable mentioned in Table 39. IA-KIT-WD-UUA together with the Illustra Tools application lets users install, configure, and maintain cameras. Scan one of the QR codes below to access the application.

iOS

Android

Illustra PG4 Series 2MP, 4MP and 8MP Indoor / Outdoor Compact Cameras

This chapter provides product features, installation procedures, and connection information regarding the Illustra Pro Gen 4 Series 2MP, 4MP and 8MP Indoor / Outdoor Compact cameras.

Product overview

This chapter explains the features and installation of the PG4 Compact cameras. Product codes and descriptions of the cameras are provided in the table below.

Table 48 Product code and description of the PG4 Compact cameras

Product Code	Description
IPS02-C10-OIA4	Illustra Pro 2MP Compact, 2.8mm Fixed, IP66/67 IK10, TDN w/IR, WDR
IPS04-C10-OIA4	Illustra Pro 4MP Compact, 2.8mm Fixed, IP66/67 IK10, TDN w/IR, WDR
IPS08-C10-OIA4	Illustra Pro 8MP Compact, 2.8mm Fixed, IP66/67 IK10, TDN w/IR, WDR

Installation

In the box

Check everything in the packing box matches to the order form and the packing slip. In addition to this guide, items below are included in the packing box:

- 1 x Printed Quick Start Guide
- 1 x Printed regulatory document
- 3 x Plastic screw anchors
- 1 x Mounting template
- 1 x Desiccant bag
- 1 x T20 security Torx wrench
- 3 x Self-tapping TP2.6*22mm screws
- 3 x Rubber for topcover screws cover
- 1 x Adaptor plate

Contact your dealer if any item is missing.

Installation tools

The following tools assist with installation:

- 1 x Phillips Screw driver
- 1 x Drill
- 1 x T20 security Torx wrench

Quick Reference

- Default IP: 192.168.1.168 (DHCP enabled)
- Default Username / Password: admin / admin
- Power: 24V AC, 50/60Hz, 1.27A or PoE 48V DC 0.53A.

Note: The camera will support PoE+ power detection to enable additional IR range (50m (PoE), 70m (PoE+).

Note: You can attach the camera to a surface or directly to a pendant or pole 1 ½ '' Male NPT pipe using the pendant / pole mount adaptor. (The pendant / pole mount adaptor can be attached to a standard 1 ½'' NTP pipe using threads or set screws).

Note: To ensure optimal lens performance, JCI recommends using the automated lens calibration feature within the web GUI following initial camera installation.

Procedure 16 Installing the camera onto a wall or ceiling

Figure 49 Installing the camera onto a wall or ceiling

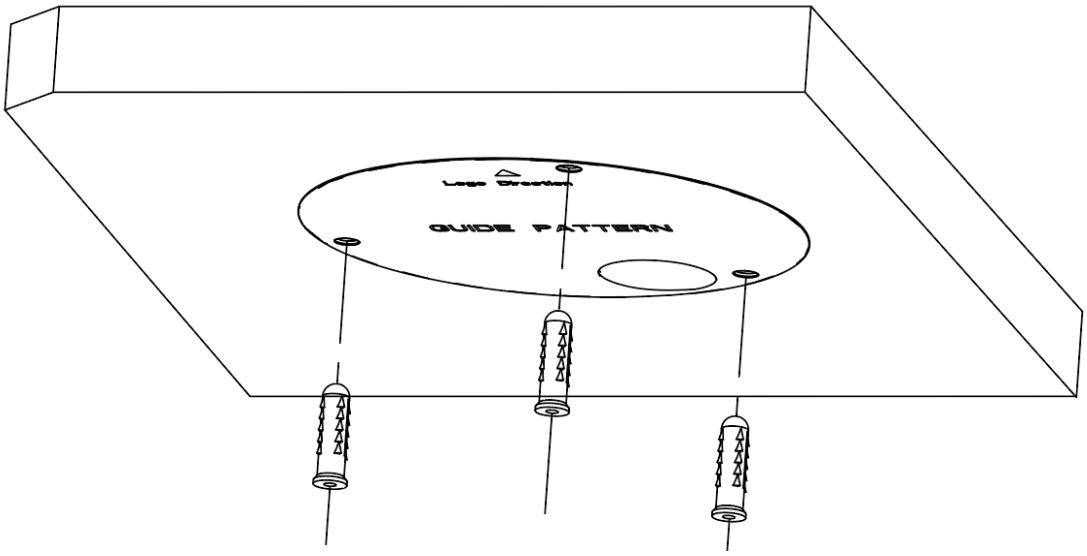


Figure 50 Installing the camera onto a wall or ceiling (continued)

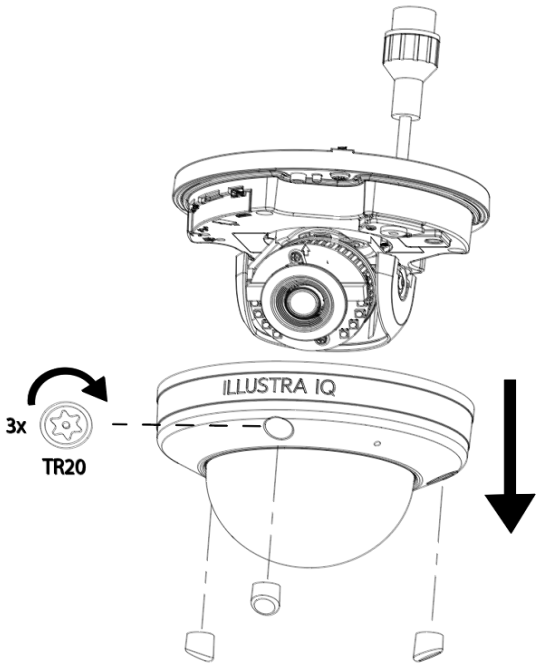


Figure 51 Installing the camera onto a wall or ceiling (continued)

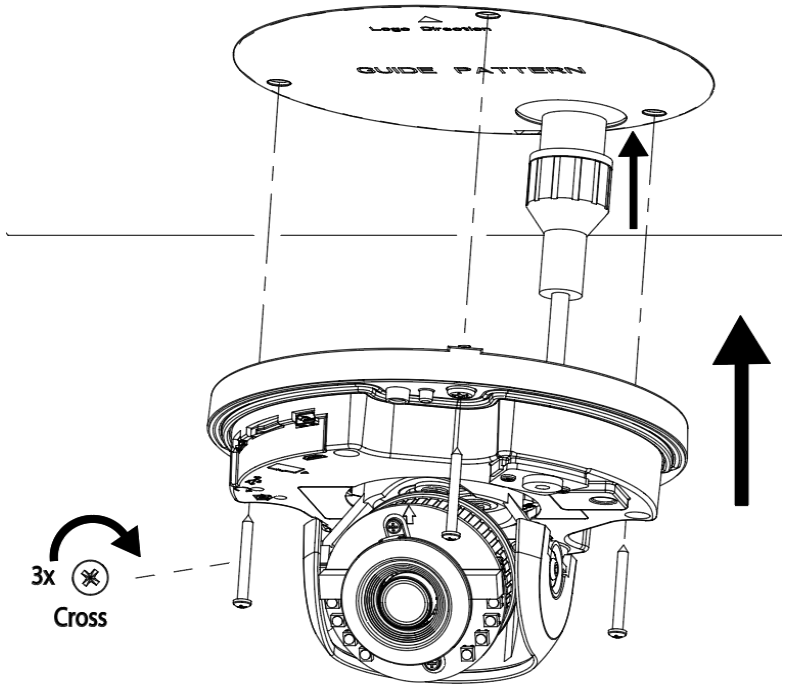
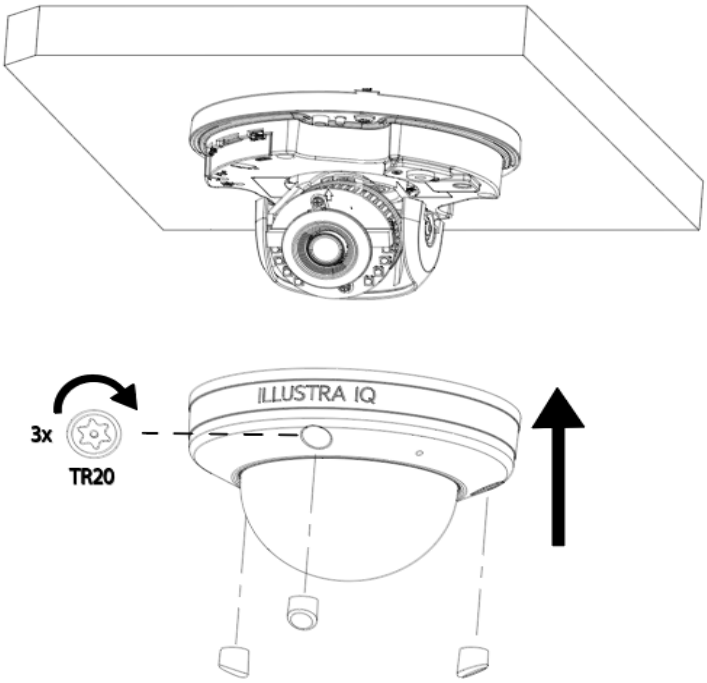


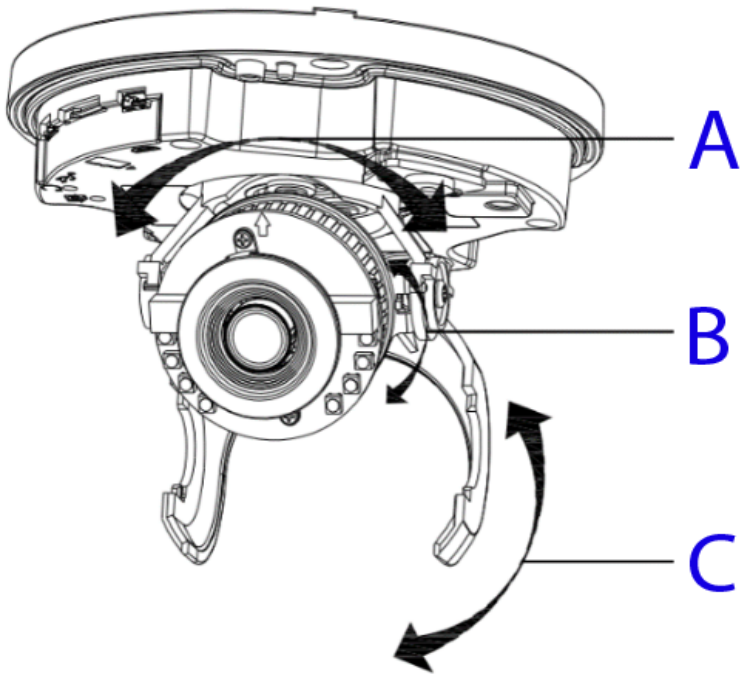
Figure 52 Installing the camera onto a wall or ceiling (continued)



- End -

Procedure 17 Pan, Tilt, and Zoom.

Figure 53 Pan, Tilt, and Zoom



Pan Adjustment (A): Rotate the lens base until you are satisfied with the field of view.

Tilt Adjustment (B): Tilt the eye-ball assembly as needed.

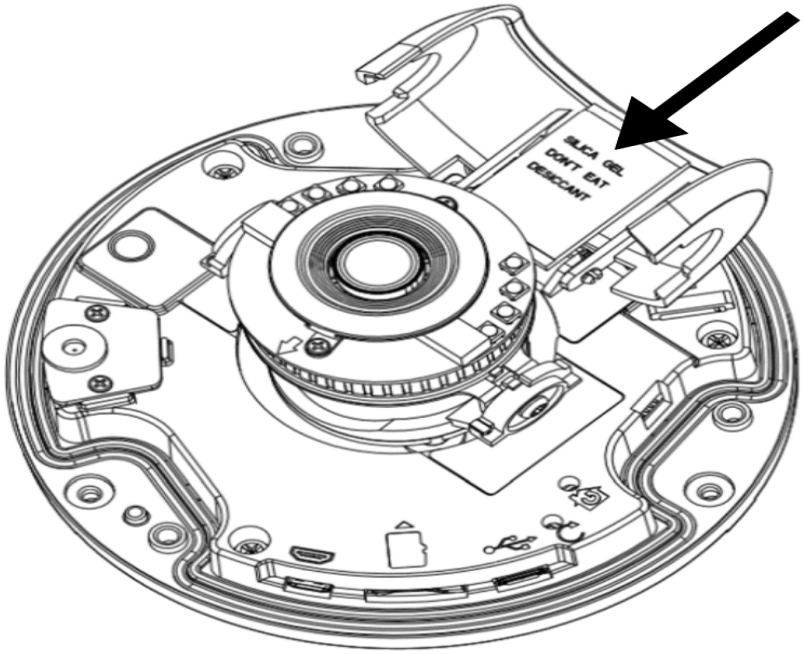
Rotate Adjustment (C): Rotate the 3D assembly in the camera base.

- End -

Procedure 18 Location of camera buttons, connections, and Desiccant bag

The figure below indicates the location of the Desiccant bag on the camera.

Figure 54 Location of desiccant bag



Warnings

1. Installation and servicing shall be performed by qualified service personal only.
2. The mains power adaptor equipment should be marked LPS (Limited Current Source) or PS2 and rated according to 60C, 24VAC, 1.27A min or PoE IEEE802.3at type 2 Class 4, 48VDC, 0.53A min.
3. To meet security immunity requirements, use an uninterruptable PSU to supply power to the mains adaptor or POE mid/end span.
4. The mounting high above ground level shall be more than 3 meters from wall mount height.
5. If a Class I PoE adapter or switch is used to provided power, be sure that the power cord is firmly plugged into the socket and confirm the main earth connection.
6. Interconnecting cables for PoE is intended to be supplied by a UL Listed type CL3P, CL3R or CL3X, marked "SUNLIGHT RESISTANT", "SUN. RES." or "SR." and "water resistant" or "W"

	Mounting, that includes climbing ladders, installing communications, power, etc. can be hazardous. Only skilled person(s) should install this device This camera can be mounted at a distance greater than 2 meters (6.6 feet) from the floor, there is a risk of Injury if the camera falls, ensure the camera is securely mounted.

Note: See IA-KIT-WD-UUA | Illustra (illustracameras.com) for more information on the USB cable applicable with the camera. IA-KIT-WD-UUA together with the Illustra Tools application lets users install, configure, and maintain cameras. Scan one of the QR codes below to access the application.

iOS

Android

Network Topology

The Illustra PG4 cameras deliver video images and audio in real-time using the internet and intranet. It is equipped with an Ethernet RJ-45 network interface.

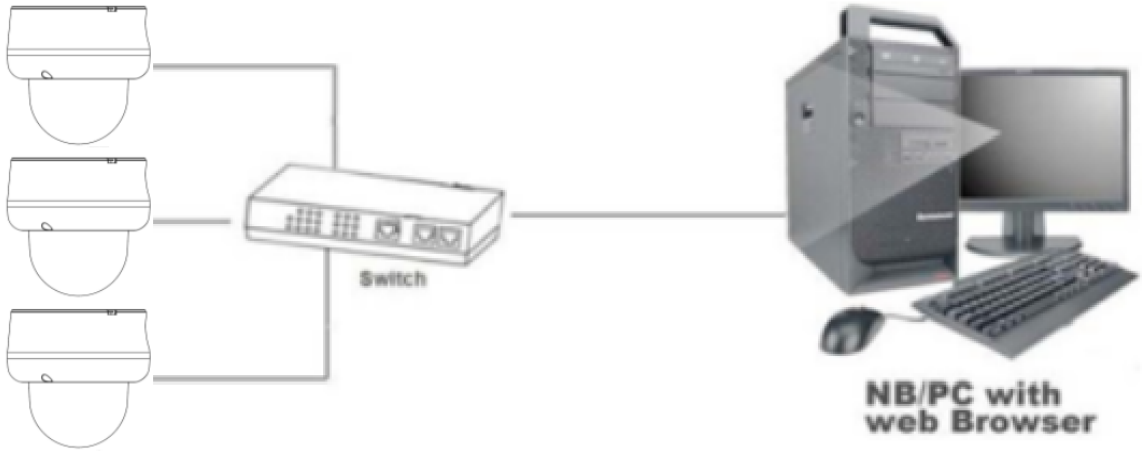
The following images illustate the network topologies of the cameras. (Using the Dome camera as an example).

PG4 Dome Camera Topology

Figure 55 Dome Cameras Network Topology Type I.



Figure 56 Dome Cameras Network Topology Type II



Network Connection

Default IP Address

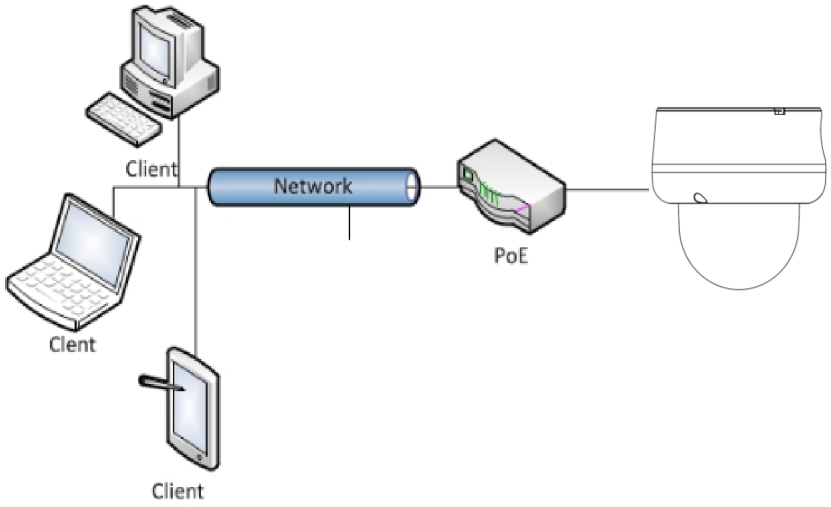
Since this is a network-based unit, an IP address must be assigned at the very first bootup. The default IP address of the unit is 192.168.1.168 and sub mask is 255.255.255.0.

However, if you have a DHCP server in your network, the unit obtains an IP address automatically from the DHCP server so that you do not need to change the IP address of the camera.

Note: If you assign the camera a Static IP address prior to DHCP being enabled, the camera first reboots for approximately 30 seconds and then remains accessible at its Static IP until it connects to a DHCP server.

- Connect to a PC directly: Directly connect the camera to a PC using a standard Ethernet cable. This requires POE switch or injector.
- Connecting a camera to a Local Area Network (LAN): To add the camera to an existing LAN, connect the camera to the POE hub or switch on your network.

Figure 57 Network connection diagram



Default camera settings

The following table describes the default camera settings.

Network Settings	Defaults
DHCP	Enabled
Static IP Address	192.168.1.168
Default Username	admin
Default Password	admin

Note: At first login the user is prompted to change the default username and password.

Procedure 19 Connecting from a computer

Step	Action
1	Ensure the camera and your computer are in the same subnet.
2	Check whether if the network is available between the unit and the computer by pinging the default IP address. a Start a command prompt. b Type “Ping 192.168.1.168”. If the message “Reply from…” appears, it means the connection is available.
3	Start Internet Explorer and enter IP address: 192.168.1.168. A login window appears. In the window, enter the default user name: admin and password: admin to log in.

- End -

DHCP

On initial camera startup, and after a hardware factory reset, Dynamic Host Configuration Protocol (DHCP) is enabled by default and remains enabled until the camera receives either a DHCP address or is assigned a Static IP address.

Procedure 20 Enable DHCP

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **TCP/IP** tab in the **Basic Configuration** menu.
3	Select the **Enable DHCP** check box to enable DHCP and disable manual settings.
4	Select **Apply** to save the settings.

The camera searches for a DHCP server. If one is found it connects to that server. If no connection is made to a DHCP server within two minutes, the camera goes to the default IP address 192.168.1.168, but continues to search for a DHCP address.

Note: If you assign the camera a Static IP address prior to DHCP being enabled, the camera first reboots for approximately 30 seconds and then remains accessible at its Static IP until it connects to a DHCP server.

- End -

Procedure 21 Disable DHCP

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **TCP/IP** tab in the **Basic Configuration** menu.
3	Clear the **Enable DHCP** check box to disable DHCP and allow manual settings to be entered. The default setting is ‘Enabled’.
4	If Enable DHCP has been disabled:

a Enter the IPv4 Address in the **IPv4 Address** text box in the form xxx.xxx.xxx.xxx.The default setting is '192.168.1.168'

b Enter the Network Mask in the **Network Mask** text box xxx.xxx.xxx.xxx. The default setting is '255.255.255.0'

c Enter the Gateway IP address in **Gateway** text box xxx.xxx.xxx.xxx.

d Enter the Primary DNS Server in the **Primary DNS Server** text box xxx.xxx.xxx.xxx.

5 Select **Apply** to save the settings.

- End -

Managing cameras with the Illustra Connect tool

In addition to using the IE browser to access your camera, you can alternatively use the provided tool, Illustra Connect.

Illustra Connect is a management tool designed to manage your network cameras on the LAN. It can:

- help you find multiple network cameras
- set the IP addresses
- show connection status
- manage firmware upgrades
- bulk configuration

Refer to Configuration on page 62 for further information regarding using the Illustra Connect tool for configuring the cameras.

Procedure 22 Connecting to the camera using Illustra Connect

Note:
Illustra Connect can only discover devices on the same subnet as its host computer. Therefore, the camera and the computer being used to configure it must be on the same subnet.

Step	Action
1	Using a computer which is connected to the same network and subnet, install the Illustra Connect software. The Illustra Connect software and the Illustra Connect manual are available to download on www.illustracameras.com
2	When the installation is complete, run Illustra Connect. It searches the network and displays all compliant devices.
3	Select the camera you want to configure, locating it by its unique MAC address.
4	Right-click the camera and select Launch Web GUI Configuration. The camera Web User Interface displays.

- End -

Procedure 23 Connecting to the camera using the static IP address

Step	Action
1	The camera attempts to obtain an IP Address from the DHCP Server. When no DHCP Server is available the camera is assigned a Static IP address of 192.168.1.168.
2	Open Microsoft Internet Explorer and enter the URL of the camera as 192.168.1.168. The camera sign in page displays.

Note:
The computer you use to configure the camera must have an IP address on the same subnet.

- End -

Procedure 24 Logging on to the camera web user interface

Step	Action
1	When you select the camera, the sign in page displays. Select your preferred language from the drop-down menu.
2	Enter the username in the **Username** text box. The default username is admin.
3	Enter the password in the **Password** text box. The default password is admin.
4	Select **Log in**.

Note: The first time that you access the camera or after a factory reset the following two pop up windows are visible: A pop up window that requests the user to **Define a Host ID** and a pop up window that requests the user to select a **Security Type**. Please refer to the user manual for further information on this.

5	The Live view page is visible. This displays the current view of the camera.

Note:
At first login the user is prompted to change the default username and password.

- End -

Procedure 25 Enabling the correct video orientation for a wall mounted camera

Step	Action
1	Log on to the camera web user interface.
2	Select **Setup** on the camera web user interface banner to display the setup menus.
3	Select the **Picture Basic** tab from the **Basic Configuration** menu.
4	Select the required **Orientation** setting: • **Mirror** • **Flip**
5	The video pane updates to display the new settings.

- End -

Configuration

The following sections explain the how you can configure Illustra Pro Gen 4 cameras using the Web User Interface.

Security Mode Profiles for First Time Connection

The Illustra Pro Gen 4 cameras have features that allow for operation in a Standard Security mode or in an Enhanced Security mode.

The Enhanced Security mode of operation is used to control changes to the camera communication protocols HTTP, HTTPS, FTP, and SMTP. When the camera is in Enhanced Security mode, you require a complex seven character Administrator password to make changes to these protocols.

Refer to Summary of Security Modes on page 63 for further information regarding the differences between Standard and Enhanced Security modes.

Accessing the Illustra Pro Gen 4 Series Camera Web User Interface

Use the following procedure to access the camera Web User Interface.

Procedure 26 Logging in to the Camera

Step	Action
1	Refer to Network Connection on page 58 for details on how to connect the camera to your network or computer.
2	When you select the camera, the sign in page displays.
3	Select your preferred language from the drop-down menu. The default language is English.
4	Enter the default username and password when prompted - Username: admin, Password: admin.
5	Click **Log in**. The camera Web User Interface displays. The first time that you access the camera, or after a factory reset, you are prompted to **Define a Host ID** and **Select a Security Type**. • **Define a Host ID**: The admin user must enter a 6 character code for the Host ID that includes both letters and/or numbers. This unique password can be used to access the operating system files. The HostID is not stored on the camera for security reasons and must be presented to Illustra Technical Support when remote access to the operating system is required. • **Select a Security Type**: Standard Security or Enhanced Security.

Note:A security prompt allows for the security to be rescheduled at the next camera reboot. When the camera has not completed the security configuration it displays a video Overlay “SECURITY NOT CONFIGURED”.

6	If you select the Standard Security option, password change is mandatory.

Note: Password complexity is set to require a minimum of 5 characters, 'admin' cant be used.

7 If you select the Enhanced Security option, a default admin username and password change is mandatory.

Note: The password must meet the following requirements:
Be a minimum of eight characters long.
Have at least one character from each of the following character groups:
• Upper-case letters - ABCDEFGHIJKLMNOPQRSTUVWXYZ
• Lower-case letters - abcdefghijklmnopqrstuvwxyz
• Numeric characters - 0123456789
• Special characters - @ % + \ / ‘ ! # $ ^ ? : , ( ) { } [ ] ~ - _ `

Note: Once the above steps are complete, the Live view page is visible. This displays the current view of the camera.

- End -

Summary of Security Modes

Standard Security:

- A default admin password change is mandatory.
- Changes to communication protocols are available to all users with appropriate privileges.
- Passwords complexity is set to require minimum of any 5 characters, 'admin' cant be used.
- Authentication method is set to basic by default.

Enhanced Security:

- Unsecure Protocols are disabled by default until enabled by a user.
- When you select enhanced security you must change the default 'admin' username and password.
- Discovery protocols are disabled by default until enabled by a user.
- Changes in the protocols are only be available to a user with administrative privileges and require that user to reenter their password.
- Authentication method is set to Digest by default.
- HTTPS protocol is enabled by default.
- Passwords for all accounts will meet the following password complexity requirements:
  - Minimum characters: 8
  - The password cannot contain the username (case sensitive)
  - Have at least one character from each of the following character groups:
  - Upper-case letters - ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - Lower-case letters - abcdefghijklmnopqrstuvwxyz
  - Numeric characters - 0123456789
  - Special characters - @ % + \ / ‘ ! # $ ^ ? : , ( ) { } [ ] ~ - _ `
  - Changing protocols require an administrator to re-enter their password

- Authentication method is set to Digest by default.

Changing the Camera Web User Interface Language

Use the following procedure to change the language used in the camera Web User Interface.

Procedure 27 Change the Camera Web User Interface Language

Step	Action
1	Open the camera sign in page. If you are already logged in to the Web User Interface, select Log Off to display the sign in page.
2	Select your preferred language from the drop-down menu: • English • Arabic • Czech • Danish • German • Spanish • French • Hungarian • Italian • Japanese • Korean • Dutch • Polish • Portuguese • Swedish • Turkish • Chinese Simplified • Chinese Traditional • Russian The default language is English.
3	Enter the Username.
4	Enter the Password.
5	Select Log in.

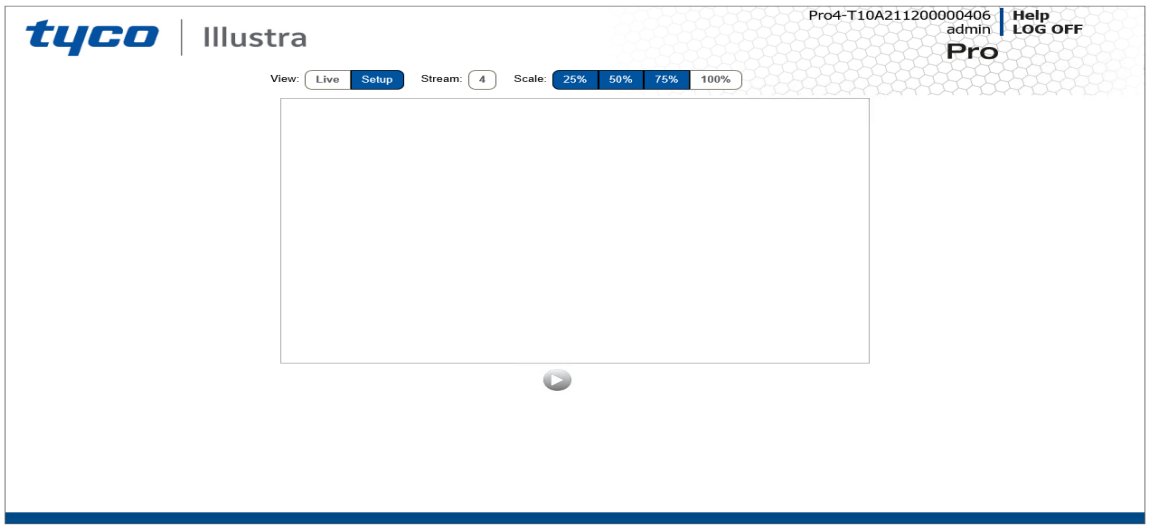
The camera web User Interface displays in the selected language.

- End -

Live menu

When you log in to the Illustra Web User Interface, the **Live** menu appears, as seen in Figure 58 on page 65.

Figure 58 Live menu page



Displaying the Live View Page

Display the live camera view page.

Procedure 28 Display Live View Page

Step	Action
1	Select **Live** in the Web User Interface banner. The Live view page displays.
2	Select a video stream from **Stream** to view.
3	Select a percentage from **Scale** to change the display size of the video pane: • 25% • 50% • 75% • 100% The default setting is 50%.
	- End -

Accessing the Setup Menus from Live View

Setup menus within the Web User Interface are restricted by user account access levels.

Procedure 29 Access Setup Menus from Live View

Step	Action
1	On the **Live** menu, click the **Setup** tab.

Note: When an admin user logs in for the first time the Liven menu displays. After this, on each login the Stream page on the Video menu displays.

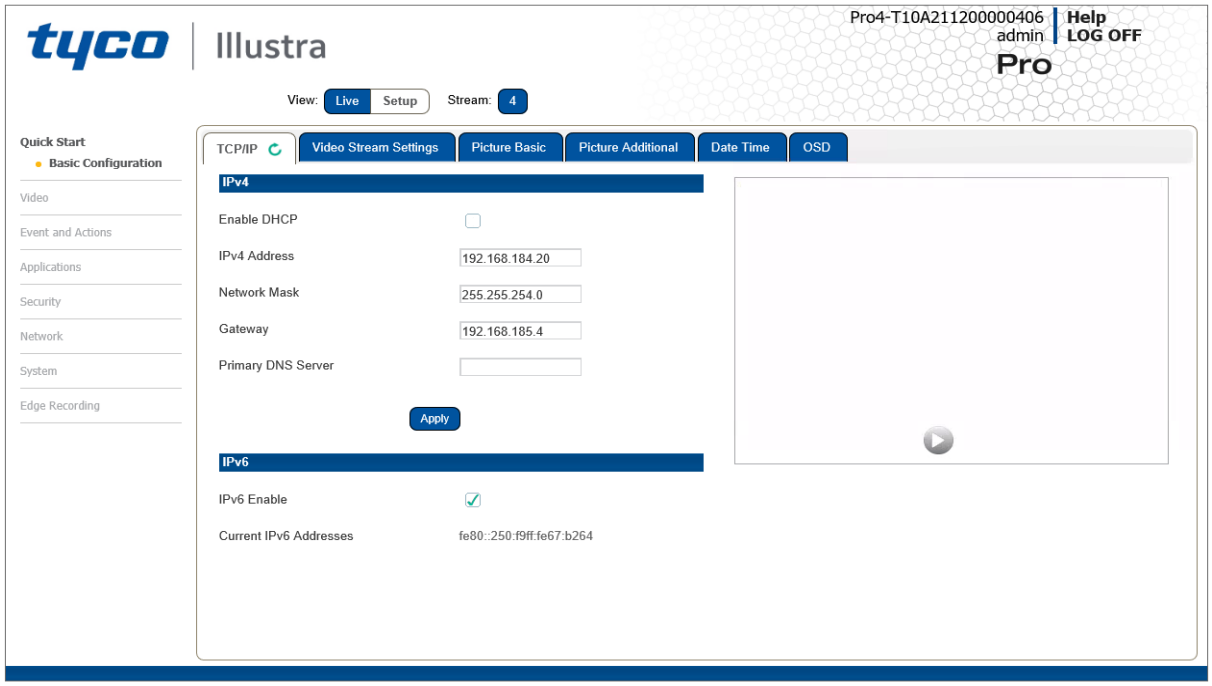
- End -

Quick Start Menu

When you select the Quick Start menu, the Basic Configuration Page displays, as shown in Figure 59 on page 67.

Note: When an admin user logs in for the first time the Basic Configuration page displays. After this, on each login the Video > Streams page displays.

Figure 59 Basic Configuration Menu



Basic Configuration

The **Basic Configuration** menu provides access to the most common features required when setting up a camera for the first time and is only available to an ‘admin’ user. The following tabs are displayed:

- TCP/IP
- Video Stream Settings
- Picture Basic
- Picture Additional
- Date Time
- OSD

TCP/IP

Configure the IPv4 and IPv6 network settings on the camera.

Note: When you perform a factory reset or reboot the unit searches for the last known IP address. If this is not available it reverts to the default IP address of 192.168.1.168. This could result in duplicate IP addresses. Refer to Quick Start Menu on page 67 for more information.

DHCP

On initial camera startup, and after a hardware factory reset, Dynamic Host Configuration Protocol (DHCP) is enabled by default and remains enabled until the camera receives either a DHCP address or is assigned a Static IP address.

Procedure 30 Enable DHCP

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Quick Start**.
2	Select the **TCP/IP** tab in the **Basic Configuration** menu.
3	Select the **Enable DHCP** check box to enable DHCP and disable manual settings.
4	Select **Apply** to save the settings.

The camera searches for a DHCP server. If one is found it connects to that server. If no connection is made to a DHCP server within two minutes, the camera goes to the default IP address 192.168.1.168, but continues to search for a DHCP address.

Note: If you assign the camera a Static IP address prior to DHCP being enabled, the camera first reboots for approximately 30 seconds and then remains accessible at its Static IP until it connects to a DHCP server.

- End -

Procedure 31 Disable DHCP

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Quick Start**.
2	Select the **TCP/IP** tab in the **Basic Configuration** menu.
3	Clear the **Enable DHCP** check box to disable DHCP and allow manual settings to be entered. The default setting is ‘Enabled’.
4	If Enable DHCP has been disabled: a Enter the IPv4 Address in the **IPv4 Address** text box in the form xxx.xxx.xxx.xxx.The default setting is ‘192.168.1.168’ b Enter the Network Mask in the **Network Mask** text box xxx.xxx.xxx.xxx. The default setting is ‘255.255.255.0’ c Enter the Gateway IP address in **Gateway** text box xxx.xxx.xxx.xxx. d Enter the Primary DNS Server in the **Primary DNS Server** text box xxx.xxx.xxx.xxx.

5 Select **Apply** to save the settings.

- End -

IPv4

Configure the IPv4 network settings for the camera.

Procedure 32 Configure the IPv4 Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Quick Start**.
2	Select the **TCP/IP** tab in the **Basic Configuration** menu.
3	Select the **Enable DHCP** check box to enable DHCP and disable manual settings. OR Clear **Enable DHCP** to disable DHCP and allow manual settings to be entered. The default setting is 'Enabled'.
4	If Enable DHCP has been disabled: a Enter the **IPv4 Address** in the IPv4 Address text box in the form xxx.xxx.xxx.xxx. The default setting is '192.168.1.168' b Enter the **Network Mask** in the Network Mask text box xxx.xxx.xxx.xxx. The default setting is '255.255.255.0' c Enter the **Gateway** IP address in Gateway text box xxx.xxx.xxx.xxx. d Enter the **Primary DNS Server** in the Primary DNS Server text box xxx.xxx.xxx.xxx.
5	Select **Apply** to save the settings.

- End -

IPv6

Enable or disable IPv6 on the camera.

Procedure 33 Enable/Disable IPv6

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Quick Start**.
2	Select the **TCP/IP** tab in the **Basic Configuration** menu.
3	Select the **IPv6 Enable** check box to enable IPv6 on the camera. OR Clear the **IPv6 Enable** check box to disable IPv6 on the camera. The default setting is 'Enabled'. If IPv6 is enabled the Link Local and DHCP address display beside 'Current IPv6 Addresses' if available.

- End -

Video Stream Settings

You can configure three video streams on the camera: Stream 1, Stream 2, and Stream 3.

Configuring the Web Video Stream

Adjust the settings for each video stream.

Procedure 34 Configure the Video Stream settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Quick Start**.
2	Select the **Video Streams Settings** tab in the **Basic Configuration** menu.
3	Select either **Stream 1**, **2, 3 or 4** from the **Stream Number** drop-down menu.
4	Select the required **Codec** from the drop-down list: • **H264** • **H264 IntelliZip** • **H265** • **H265 IntelliZip** • **MJPEG** The default setting is 'H264'.
	Note: When you select H264 or H264 IntelliZip you can set the Profile. If you do not select either of these options then contiune at step 6 below.
5	Select the required **Profile** from the drop-down list: • **Main** • **High** The default setting is 'Main'.
6	Select the required **Resolution** from the drop-down menu. The resolutions available depend on the Image Source selected.
	Note: See Stream Tables combinations in Appendix B.
7	Use the slider bar to select the **Frame Rate (fps)**.
	Note:FPS varies depending on other features - See Stream Tables combinations in Appendix B.
8	Use the slider bar to select the **GOP**.
9	If MJPEG has been selected, MJPEG Quality is enabled. Use the slider bar to select the **MJPEG Quality**. The default setting is 50. OR
10	If H264 has been selected in step 4, Rate Control is enabled. Select the required **Rate Control** by selecting the radio buttons: • **VBR (Variable Bit Rate)**

- **CBR (Constant Bit Rate)**
- **CVBR (Constrained Variable Bit Rate)**

The default setting is 'CVBR'.

a If you select VBR, VBR Quality is enabled. Select the required **VBR Quality** from the drop-down menu. The default setting is High.

- **Highest**
- **High**
- **Medium**
- **Low**
- **Lowest**

OR

b If you select CBR , Bit Rate is enabled. Use the slider bar to select the **Bit Rate**. The default setting is 1000.

OR

c If you select CVBR, Max Bit Rate is enabled. Use the slider bar to select the **Max Bit Rate**. The default setting is 4000.

- End -

Procedure 35 Configuring IntelliZip Max GOP

This feature only applies to H264+ IntelliZip or H265+ IntelliZip codec.

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Quick Start**.
2	Select the **Video Stream Settings** tab in the **Basic Configuration** menu.
3	Use the slider bar to select the **Max GOP** range. Range available is 1-180.

- End -

Picture Basic

You can configure the Picture rotation, zoom / focus and exposure.

Picture Rotation

Configure the orientation and corridor mode settings. Both settings are optional.

Focus/Zoom

The Focus is manually configured on initial setup. The **One Touch** button can be used to automatically focus the area of view. The plus and minus arrows are used to manually fine tune the image. The Zoom slider bar is used to manually zoom in and out to manually configure to picture. The table below describes the features supported by each camera.

Exposure

Configure the exposure settings for the camera.

Procedure 36 Configure Orientation Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Quick Start**.
2	Select the **Picture Basic** tab from the **Basic Configuration** menu.
3	Select the required **Orientation** setting: • **Mirror** • **Flip** Mirror and Flip settings are not selected by default. The video pane updates to display the new settings. **Note:**When wall mounting the camera you should select Flip to correct the lens orientation.

- End -

Corridor Mode

Provides a better perspective when viewing a long corridor.

Procedure 37 Configure Corridor Mode Settings

Step	Action
1	Select Setup on the Web User Interface banner to display the setup menus and then select **Quick Start**.
2	Select the **Picture Basic** tab from the **Basic Configuration** menu.
3	Select the Play button to start the video stream if it is not already active.
4	Select the required Corridor Mode setting: • Off • -90° • +90° The camera requires a reboot to set the new corridor mode. Once rebooted the video pane updates to display the new settings.

- End -

Procedure 38 Adjust Camera Focus / Zoom

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Quick Start**.
2	Select the **Picture Basic** tab from the **Basic Configuration** menu.
3	Select  to start the video stream if it is not already active.
4	Use the arrows to manually configure the focus and the slider bar to adjust zoom settings until the image in clear. The video pane updates to display the new settings.

- End -

Procedure 39 Adjust Camera Focus using OneTouch Autofocus

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Quick Start**.
2	Select the **Picture Basic** tab from the **Basic Configuration** menu.
3	Select  to start the video stream if it is not already active.
4	Select the **One Touch** button. The camera refocuses to the zoom level selected for the image. The video pane updates to display the new settings.

- End -

Procedure 40 Configure Exposure Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Quick Start**.
2	Select the **Picture Basic** tab from the **Basic Configuration** menu.
3	Select  to start the video stream if it is not already active.
4	Select the **Exposure Profiles** from the drop-down menu: See Exposure Profile descriptions below: **Demo** • Bitrate controller VBR • Quality highest • Set max exposure and min exposure allowed • Set max gain value allowed • Auto exposure selects shutter speed (between min and max exposure values) and gain (between 0db and max gain selection) to adjust exposure if light level or scene changes • Use case: Out of the box configuration for optimal video and image quality **Note:** • Demo Mode VBR Highest is the default out of the box (or after a factory reset) • Exposure default buttons will default Exposure profile to Auto (it will not apply any bitrate changes) • Demo mode will only revert back to VBR Highest on a Factory reset • Demo mode to other values will change the bitrate to CVBR Max Bitrate 4000 • Other to Demo does not change the bitrate under any circumstance

- Other to Other does not change the bitrate under any circumstance
- When Exposure profiles sets new bitrate values, they will not automatically restart active stream to update to the new settings. Manual restart is required.

Auto

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 4000
- Set any iris position
- Set Max exposure and Min exposure allowed
- Set max gain value allowed
- Auto Exposure selects shutter speed (between min and max exposure values) and gain (between 0db and max gain selection) to adjust exposure if light level or scene changes
- Use case: To select a required depth of focus.. Selecting a high iris value will give a larger depth of focus so that objects close to and far from the camera can be in focus at the same time. Caution: With a high iris value the camera is not able to produce a bright image in very low light levels

Outdoor

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 4000
- Set max gain allowed
- Set max exposure allowed
- Set min exposure allowed
- Auto Exposure selects shutter speed (between min and max exposure values), gain (between 0db and max gain selection) and iris position to adjust exposure if light level or scene changes
- Iris operation tailored to give larger depth of focus if conditions are bright enough
- Use case: Outdoor operation with or without IR illumination enabled

Note:

- Demo Mode VBR Highest is the default out of the box (or after a factory reset)
- Exposure default buttons will default Exposure profile to Auto (it will not apply any bitrate changes)
- Demo mode will only revert back to VBR Highest on a Factory reset
- Demo mode to other values will change the bitrate to CVBR Max Bitrate 4000
- Other to Demo does not change the bitrate under any circumstance
- Other to Other does not change the bitrate under any circumstance

- When Exposure profiles sets new bitrate values, they will not automatically restart active stream to update to the new settings. Manual restart is required.

Indoor

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 4000
- Set max gain allowed
- Set max exposure allowed
- Set min exposure allowed
- Auto Exposure selects shutter speed (between min and max exposure values), gain (between 0db and max gain selection) and iris position to adjust exposure if light level or scene changes
- Use case: Office environment where light levels can change quickly

Gaming

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 4000
- Set Stream 1 Framerate to 30 (if lower than)
- Set max gain value allowed
- Set min exposure allowed
- Set max exposure no slower than 1/30s (NTSC/60Hz) or 1/25s (PAL/50Hz)
- Use case: Casinos or other situations where Frame Rate must be no slower than 30fps (NTSC/60Hz) or 25fps (PAL/50Hz)

License Plate Recognition (LPR) low, mid and high

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 4000
- Set max gain value allowed
- Set min exposure allowed
- Low vs mid vs high, set slower or faster max exposure values
- Auto exposure selects iris position, shutter speed and gain to adjust exposure if light level or scene changes
- Use case: License Plate Recognition such as parking garages or other moving vehicle scenario where a fast shutter speed must be maintained to give sharper images, while the vehicle or object is moving, to help License Plate Recognition software.

Shutter Priority

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 4000
- Set any shutter speed
- Set max gain value allowed

- Auto Exposure selects gain (between 0db and max gain selection) and iris position to adjust exposure if light level or scene changes
- Use case: Typically for use in scenes with motion, e.g. overlooking traffic.. Caution: The illumination required for this configuration would need to be quite consistent.

Iris Priority

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 4000
- Set any Iris position
- Set Max exposure and Min exposure allowed
- Set max gain value allowed
- Auto Exposure selects shutter speed (between min and max exposure values) and gain (between 0db and max gain selection) to adjust exposure if light level or scene changes
- Use case: To select a required depth of focus. Selecting a high iris valus gives a larger depth of focus so that objects close to and far from the camera can be in focus at the same time. Caution: With a high iris value the camera is not able to produce a bright image in very low light levels

Manual

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 4000
- Set any shutter speed, gain value and iris position
- Fixed exposure
- Does not auto adjust if light level or scene changes
- Use case: Fixed conditions where illumination and scene will not change. If the lighting or scene changes the apparent brightness of the image will change.

5 Select the **Exposure Method** from the drop-down menu:

- **Full Picture Weighted**
- **Upper**
- **Lower**
- **Center Weighted**
- **Spot**
- **Left**
- **Right**
- **Object Defined**
- **Person Defined**
- **Face Defined**

Note: Default AE mode will prioritise change from Center Weighted to Person Defined. This new mode will automatically adjust AE region to prioritise an AI detected person.

6 Select the **Min Exposure** from the drop-down menu.
The default setting is 1/10000s.

7 Select the **Max Exposure** from the drop-down menu.
The default setting is 1/8s.

8 Select the **Exposure Offset (F-Stops)** from the drop-down menu.
The default setting is 0.

9 Select the **Max Gain** from the drop-down menu.
The default setting is 51db.

10 Select the **Iris Level** from the drop-down menu.
The default setting is 1.

Note: The Iris Level differs depending on the camera.

11 Select the **Exposure (sec)** from the drop-down menu.
The default setting is 1/8s.

12 Select the **Manual Gain (dB)** from the drop-down menu.
The default setting is 0db.

13 Select the **Frequency** radio button for either **50Hz** or **60Hz**.
The default setting is 60Hz.

14 Select or clear the check box for **Flickerless Mode**.
This feature is not selected by default.

- When you select **Flickerless Mode**, the minimum and maximum exposure times are locked to 1/100 and 1/50 respectively (PAL) or 1/120 and 1/60 respectively (NTSC). This applies to all cameras referenced in this guide.

- End -

Procedure 41 Restore Exposure Defaults

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Quick Start**.
2	Select the **Picture Basic** tab from the **Basic Configuration** menu.
3	Select  to start the video stream if it is not already active.
4	Select **Exposure Defaults** to restore the default settings.

- End -

Picture Additional

Configure Wide Dynamic Range, Day Night Mode, Picture Adjustments, defog and White Balance.

Wide Dynamic Range

Wide Dynamic Range (WDR) is a feature that supports the viewing of high contrast scenes that include both bright and low light areas in the same field of view (FOV).

WDR Level allows you to adjust the WDR level to favor a underexposed or overexposed image. By selecting the lower end of the control, the image is underexposed which provides more detail in areas of bright but less details in areas of darkness. Selecting the higher end of the control, the image is overexposed which provides more detail in the dark areas but less details in the bright areas.

A typical use for this feature would be viewing a scene with both indoor and outdoor lighting conditions simultaneously, for example, in a warehouse area with an open bay door.

Procedure 42 Disable/Enable Wide Dynamic Range (WDR)

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Quick Start**.
2	Select the **Picture Additional** tab from the **Basic Configuration** menu.
3	Select the required WDR from the drop-down list: • **Off:** WDR is off • **Smart WDR:** Digital wide dynamic range, enhancing detail in darker areas • **True WDR:** Two shutter wide dynamic range, to compensate for bright and dark areas in the scene. • **True WDR3x:** Three shutter wide dynamic range, to compensate for bright and dark areas in the scene. **Note:**TrueWDR3x does not apply to 8MP models. The default setting is OFF.

- End -

Defog

Defog lets you automatically control and help reduce the effects of mist or fog on image quality. When enabled, continuous image analysis adjusts the amount of defog effect applied within the range of the strength.

Note: Defog has some limitation and may not be available when used with Certain Dynamic Range Controls.

Procedure 43 Disable/Enable Defog

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Quick Start**.
2	Select the **Picture Additional** tab from the **Basic Configuration** menu.
3	Select the **Enable Defog** drop-down menu and one of the following options: • **Off** • **Low**

- **Mid**
- **High**

The default setting is Low for outdoor cameras and Off for indoor cameras.

- End -

Day Night Mode

IR/DayNight Mode utilizes a series of specific camera functions to dramatically enhance low light performance.

When needed, the True TDN mechanism removes an IR Cut Filter (IRCF) from in front of the images allowing the camera to see in black and white (BW) and utilize additional near-infrared energy found in many lighting sources like halogen, moonlight, etc.

This, along with slowing down another function, the shutter speed, significantly improves low light performance rendering clear images where none could be viewed previously.

IR Illuminator

When the camera is in B/W mode it can utilize or see near-IR illumination; something the human eye cannot do. This can be extremely powerful when the dome is paired with 850~950nm IR illuminators. With this combination a scene can be well lit with IR light that the dome can see but people cannot. This is great for areas where externally lighting is not allowed or there is a need for covert security.

Procedure 44 Enable / Disable IR Illuminator

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Quick Start**.
2	Select the **Picture Additional** from the **Basic Configuration** menu.
3	Select the **Enable IR Illuminator** check box to enable IR Illuminator. OR Clear the **Enable IR Illuminator**check box to disable **IR Illuminator**. The default setting is 'Enabled'.

- End -

Day Night Mode

The dome provides a black-and-white (B/W) mode to improve camera performance when the light level falls below certain thresholds. This allows clear images to be obtained under low-light conditions.

Procedure 45 Configure Day Night Mode

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Quick Start**.
2	Select the **Picture Additional** from the **Basic Configuration** menu.
3	Select a **Day Night Mode** setting from the drop-down menu: • **Forced Color** - enable full-time color mode.

- **Forced B&W** - enable full-time black and white mode.
- **Auto Low** - camera will adjust between BW and Color depending on light levels.
- **Auto Mid** - camera give a good balance of Color and BW depending on the scene.
- **Auto High** - increases the chance of switching to BW mode as light levels drop.
- **Manual** - a slider bar will display, the user can adjust the setting to suit the environment.

The default setting is 'Auto Mid'.

- End -

Picture Adjustment

Adjust contrast, saturation, and sharpness of the image displayed on the video pane.

Procedure 46 Adjust the Contrast, Saturation, and Sharpness

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Quick Start**.
2	Select the **Picture Additional** tab from the **Basic Configuration** menu.
3	Select  to start the video stream if it is not already active. The video pane will display the current camera view.
4	Use the slider bars to adjust: • **Contrast** • **Saturation** • **Sharpness** The values range from 1% to 100%. The video pane updates to display the new settings.

- End -

Procedure 47 Restore Picture Balance Defaults

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Quick Start**.
2	Select the **Picture Settings** tab from the **Basic Configuration** menu.
3	Select **Defaults** to restore the default settings. The default values are: • **Contrast:** 50% • **Saturation:** 50% • **Sharpness:** 50%

- End -

White Balance

White balance, the ability to keep whites looking white, is normally compensated for automatically using the default Auto White Balance setting.

Manual White Balance is available when specific color temperature settings want to be set and preserved. This can be done using the red and blue slider adjustments set for optimal viewing.

Procedure 48 Configure Auto White Balance

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Quick Start**.
2	Select the **Picture Additional** tab from the **Basic Configuration** menu.
3	Select  to start the video stream if it is not already active. The video pane displays the current camera view.
4	Select the required **White Balance** from the drop-down menu: • **Auto Normal:** Suitable for a normal range of lighting conditions • **Manual:** Adjustable red and blue balance sliders • **Auto Wide:** Suitable for a wider than normal range of lighting conditions The default setting is 'Auto Normal'.

- End -

Procedure 49 Manually Select White Balance

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Quick Start**.
2	Select the **Picture Additional** tab from the **Basic Configuration** menu.
3	Select  to start the video stream if it is not already active. The video pane displays the current camera view.
4	Select **Manual** from the White Balance drop-down menu. The Red and Blue slider bars display.
5	Use the slider bars to adjust the **Red** and **Blue** balance. The live video pane updates to display the new settings. The red and blue values range from 1% to 100%. If you change the configuration to **Manual**, the slider bar reads the real-time setting of the FOV.

- End -

Date Time

You can change the camera name and set the date and time.

Procedure 50 Change the Camera Name

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Quick Start**.
2	Select the **Date Time** tab in the **Basic Configuration** menu.
3	Enter the name of the camera in the **Camera Friendly Name** text box.

- End -

Procedure 51 Configuring the Date and Time

Step	Action
4	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Quick Start**.
5	Select the **Date Time** tab from the **Basic Configuration** menu.
6	Select the **Time 24-hour** check box to enable the 24-hour clock. Or Deselect the **Time 24-hour** check box to enable the 12-hour clock. The default setting is '24-hour'.
7	Select the **Date Display Format** from the drop-down menu: • **DD/MM/YYYY** • **MM/DD/YYYY** • **YYYY/MM/DD** The default setting is 'YYYY/MM/DD'.
8	Select the **Time Zone** from the drop-down menu. The default setting is '(GMT-05:00) Eastern Time (US & Canada)
9	Select the **Set Time** setting by selecting the radio buttons: • **Manually** • **via NTP** The default setting is 'Manually'.
10	If you select Manually in step 5: a Select the Date **(DD/MM/YYYY)** using the drop-down menus. b Select the Time **(HH:MM:SS)** using the drop-down menus.
11	If you select via NTP in step 5: a Enter the **NTP Server Name** in the text box.

- End -

On-Screen Display (OSD)

You can enable or disable on screen display information.

Procedure 52 Changing the on screen camera text size

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Quick Start**.
2	Select the **OSD** tab in the **Basic Configuration** menu.
3	In the **Text Size** section, select **Normal** to display the text in a normal size. OR In the **Text Size** section, select **Large** to display the text in a larger size. The default setting is 'Normal'.

- End -

Procedure 53 Display or Hide the Camera Name

Step	Action
4	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Quick Start**.
5	Select the **OSD** tab in the **Basic Configuration** menu.
6	In the **Camera Name** section, select the **Enable** check box to display the camera name in the OSD. OR In the **Camera Name** section, clear the **Enable** check box to hide the camera name in the OSD. The default setting is 'Disabled'.

- End -

Procedure 54 Display or Hide the Camera Time

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Quick Start**.
2	Select the **OSD** tab in the **Basic Configuration** menu.
3	In the **Date Time** section, select the **Enable** check box to display the camera name in the OSD. OR In the **Date Time** section, clear the **Enable** check box to hide the camera name in the OSD. The default setting is 'Disabled'.

- End -

Procedure 55 Display or Hide the User Defined

Step	Action
1	Select Setup on the Web User Interface banner to display the setup menus and then select **Quick Start**.
2	Select the **OSD** tab in the **Basic Configuration** menu.
3	In the **User Defined** section, select the **Enable** check box to display the camera name in the OSD. OR In the **User Defined** section, clear the **Enable** check box to hide the camera name in the OSD. The default setting is 'Disabled'.
4	Select a **Location** from the drop-down menu.

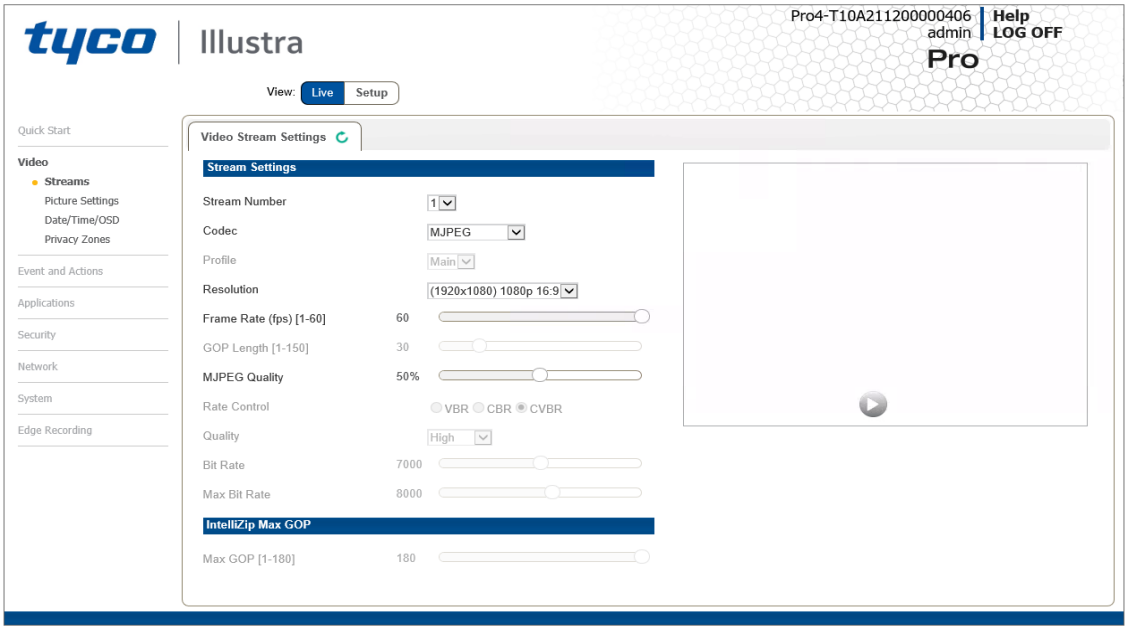
5	Enter a name in the **Name** field.
	The OSD User Defined fields must comply with the following validation criteria:
	• 0 - 24 characters
	• Cannot begin or end with:
	  • . (dot)
	  • - (hyphen)
	  • _ (underscore)
	  • \ (backslash)
	  • " (quotes)

- End -

Video Menu

When you select the **Video** menu, the **Streams** page displays, as seen in Figure 60 on page 85.

Figure 60 Video Menu



The **Video** Menu provides access to the following camera settings and functions:

- Streams
- Picture Settings
- Date / Time / OSD
- Privacy Zones
- AI Privacy Mask
- Region of Interest

Streams

You can configure up to three independent video streams on the camera: Stream 1, Stream 2, Stream 3 and Stream 4.

Video displaying on the video pane reflects the settings configured in the stream selected from the drop-down menu, either Stream 1 or Stream 2 or Stream 3 or Stream 4.

Note: The Web User Interface uses Stream 3.

Alarm Video

Edge Recording

Camera can directly record specific events (MD, DIO and Face detection) directly to Micro SD card. User can chose either Stream 1, 2, 3 or 4 to be recorded. When setting up motion detection on the camera, both streams can be used. Alarm Video is configured in the Edge Recording > Record Settings menu.

Integration with other Illustra API Clients

You can configure the 4 video streams through the Web User Interface, as detailed here, or through the Illustra API interface. Changes made to the streams through either method are applied and the video displays according to the configuration.

Opening the Web User Interface live video allows the stream to be shared with the Illustra API and will minimize the impact on camera resources.

Configuring the Video Stream

Adjust the settings for each video stream.

Procedure 56 Configure the Video Stream settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.
2	Select the **Streams** tab in the **Video** menu.
3	Select either **Stream 1**, **2, 3 or 4** from the **Stream Number** drop-down menu.
4	Select the required **Codec** from the drop-down list: • **H264** • **H264 IntelliZip** • **H265** • **H265 IntelliZip** • **MJPEG** The default setting is 'H264'.

Note: When you select H264 or H264 IntelliZip you can set the Profile. If you do not select either of these options then contiune at step 6 below.

5	Select the required **Profile** from the drop-down list: • **Main** • **High** The default setting is 'Main'.
6	Select the required **Resolution** from the drop-down menu. The resolutions available depend on the Image Source selected.

Note: See Stream Tables combinations in Appendix B.

7	Use the slider bar to select the **Frame Rate (fps)**.

Note:FPS varies depending on other features - See Stream Tables combinations in Appendix B.

8	Use the slider bar to select the **GOP**.

9 If MJPEG has been selected, MJPEG Quality is enabled. Use the slider bar to select the **MJPEG Quality**.

The default setting is 50.

OR

10 If H264 has been selected in step 4, Rate Control is enabled. Select the required **Rate Control** by selecting the radio buttons:

- **VBR (Variable Bit Rate)**
- **CBR (Constant Bit Rate)**
- **CVBR (Constrained Variable Bit Rate)**

The default setting is 'CVBR'.

a If you select VBR, VBR Quality is enabled. Select the required **VBR Quality** from the drop-down menu. The default setting is High.

- **Highest**
- **High**
- **Medium**
- **Low**
- **Lowest**

OR

b If you select CBR , Bit Rate is enabled. Use the slider bar to select the **Bit Rate**. The default setting is 1000.

OR

c If you select CVBR, Max Bit Rate is enabled. Use the slider bar to select the **Max Bit Rate**. The default setting is 4000.

- End -

Procedure 57 Configuring IntelliZip Max GOP

This feature only applies to H264+ IntelliZip or H265+ IntelliZip codec.

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.
2	Select the **Streams** tab in the **Video** menu.
3	Use the slider bar to select the **Max GOP** range. Range available is 1-180.

- End -

Picture Settings

Picture Basic

You can configure the Picture rotation, zoom / focus and exposure.

Picture Additional

Configure Wide Dynamic Range, Day Night Mode, Picture Adjustments and White Balance.

Image Profiles

The Image Profiles feature enables users to capture, export and restore selected picture settings configurations from a previously saved data file. The data file can be saved to a specified location and used to restore the camera picture settings configuration.

Image Stabilization

Electronic Image Stabilization (EIS) is a process where image stability is controlled through electronic processing procedures. Once EIS is enabled, image Field-of-View (FoV) is cropped. If the EIS device detects camera shake in pitch / yaw / roll directions, EIS responds by moving the cropped image offset and applying warp operation, so the image can remain in the position close to the original place as much as possible. There are 2 EIS modes, Low and High, where each mode will crop the image FoV by a percentage. Low crops the image FoV by 10% where High crops the image by 25%. In mode High, EIS will attempt to stabilize a greater vibration amplitude that Low mode.

Lens Calibration

Use the lens calibration process to recover focus and zoom after motor stalling has occurred. Motor step stalling is rare, but it can occur during shipping or through mishandling of the camera. If the One Touch focus at Wide or Tele is not working through the zoom range, the camera requires lens calibration. The lens calibration tool uses infinity focus curves to align the camera lens and correct problems focusing at Wide or Tele.

Procedure 58 Configure Orientation Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.
2	Select **Picture Settings** to view the **Picture Basic** tab.
3	Select the required **Orientation** setting: • **Mirror** • **Flip** Mirror and Flip settings are not selected by default. The video pane updates to display the new settings. **Note:**When wall mounting the camera you should select Flip to correct the lens orientation.

- End -

Corridor Mode

Provides a better perspective when viewing a long corridor.

Procedure 59 Configure Corridor Mode Settings

Step	Action

1 Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.

2 Select **Picture Settings** to view the **Picture Basic** tab.

3 Select the Play button to start the video stream if it is not already active.

4 Select the required Corridor Mode setting:

- Off
- -90°
- +90°

The camera requires a reboot to set the new corridor mode. Once rebooted the video pane updates to display the new settings.

- End -

Procedure 60 Adjust Camera Focus / Zoom

Step	Action

1 Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.

2 Select **Picture Settings** to view the **Picture Basic** tab.

3 Select  to start the video stream if it is not already active.

4 Use the arrows to manually configure the focus and the slider bar to adjust zoom settings until the image in clear. The video pane updates to display the new settings.

- End -

Procedure 61 Adjust Camera Focus using OneTouch Autofocus

Step	Action

1 Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.

2 Select **Picture Settings** to view the **Picture Basic** tab.

3 Select  to start the video stream if it is not already active.

4 Select the **One Touch** button. The camera refocuses to the zoom level selected for the image. The video pane updates to display the new settings.

- End -

Procedure 62 Configure Exposure Settings

Step	Action

1 Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.

2 Select **Picture Settings** to view the **Picture Basic** tab.

3 Select  to start the video stream if it is not already active.

4 Select the **Exposure Profiles** from the drop-down menu:

See Exposure Profile descriptions below:

Demo

- Bitrate controller VBR
- Quality highest
- Set max exposure and min exposure allowed
- Set max gain value allowed
- Auto exposure selects shutter speed (between min and max exposure values) and gain (between 0db and max gain selection) to adjust exposure if light level or scene changes
- Use case: Out of the box configuration for optimal video and image quality

Note:

- Demo Mode VBR Highest is the default out of the box (or after a factory reset)
- Exposure default buttons will default Exposure profile to Auto (it will not apply any bitrate changes)
- Demo mode will only revert back to VBR Highest on a Factory reset
- Demo mode to other values will change the bitrate to CVBR Max Bitrate 4000
- Other to Demo does not change the bitrate under any circumstance
- Other to Other does not change the bitrate under any circumstance
- When Exposure profiles sets new bitrate values, they will not automatically restart active stream to update to the new settings. Manual restart is required.

Auto

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 4000
- Set any iris position
- Set Max exposure and Min exposure allowed
- Set max gain value allowed
- Auto Exposure selects shutter speed (between min and max exposure values) and gain (between 0db and max gain selection) to adjust exposure if light level or scene changes
- Use case: To select a required depth of focus.. Selecting a high iris value will give a larger depth of focus so that objects close to and far from the camera can be in focus at the same time. Caution: With a high iris value the camera is not able to produce a bright image in very low light levels

Outdoor

- Set camera Bitrate controller to CVBR

- Set Max Bitrate to 4000
- Set max gain allowed
- Set max exposure allowed
- Set min exposure allowed
- Auto Exposure selects shutter speed (between min and max exposure values), gain (between 0db and max gain selection) and iris position to adjust exposure if light level or scene changes
- Iris operation tailored to give larger depth of focus if conditions are bright enough
- Use case: Outdoor operation with or without IR illumination enabled

Note:

- Demo Mode VBR Highest is the default out of the box (or after a factory reset)
- Exposure default buttons will default Exposure profile to Auto (it will not apply any bitrate changes)
- Demo mode will only revert back to VBR Highest on a Factory reset
- Demo mode to other values will change the bitrate to CVBR Max Bitrate 4000
- Other to Demo does not change the bitrate under any circumstance
- Other to Other does not change the bitrate under any circumstance
- When Exposure profiles sets new bitrate values, they will not automatically restart active stream to update to the new settings. Manual restart is required.

Indoor

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 4000
- Set max gain allowed
- Set max exposure allowed
- Set min exposure allowed
- Auto Exposure selects shutter speed (between min and max exposure values), gain (between 0db and max gain selection) and iris position to adjust exposure if light level or scene changes
- Use case: Office environment where light levels can change quickly

Gaming

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 4000
- Set Stream 1 Framerate to 30 (if lower than)
- Set max gain value allowed
- Set min exposure allowed

- Set max exposure no slower than 1/30s (NTSC/60Hz) or 1/25s (PAL/50Hz)
- Use case: Casinos or other situations where Frame Rate must be no slower than 30fps (NTSC/60Hz) or 25fps (PAL/50Hz)

License Plate Recognition (LPR) low, mid and high

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 4000
- Set max gain value allowed
- Set min exposure allowed
- Low vs mid vs high, set slower or faster max exposure values
- Auto exposure selects iris position, shutter speed and gain to adjust exposure if light level or scene changes
- Use case: License Plate Recognition such as parking garages or other moving vehicle scenario where a fast shutter speed must be maintained to give sharper images, while the vehicle or object is moving, to help License Plate Recognition software.

Shutter Priority

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 4000
- Set any shutter speed
- Set max gain value allowed
- Auto Exposure selects gain (between 0db and max gain selection) and iris position to adjust exposure if light level or scene changes
- Use case: Typically for use in scenes with motion, e.g. overlooking traffic.. Caution: The illumination required for this configuration would need to be quite consistent.

Iris Priority

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 4000
- Set any Iris position
- Set Max exposure and Min exposure allowed
- Set max gain value allowed
- Auto Exposure selects shutter speed (between min and max exposure values) and gain (between 0db and max gain selection) to adjust exposure if light level or scene changes
- Use case: To select a required depth of focus. Selecting a high iris valus gives a larger depth of focus so that objects close to and far from the camera can be in focus at the same time. Caution: With a high iris value the camera is not able to produce a bright image in very low light levels

Manual

- Set camera Bitrate controller to CVBR

- Set Max Bitrate to 4000
- Set any shutter speed, gain value and iris position
- Fixed exposure
- Does not auto adjust if light level or scene changes
- Use case: Fixed conditions where illumination and scene will not change. If the lighting or scene changes the apparent brightness of the image will change.

5 Select the **Exposure Method** from the drop-down menu:

- **Full Picture Weighted**
- **Upper**
- **Lower**
- **Center Weighted**
- **Spot**
- **Left**
- **Right**
- **Object Defined**
- **Person Defined**
- **Face Defined**

Note: Default AE mode will prioritise change from Center Weighted to Person Defined. This new mode will automatically adjust AE region to prioritise an AI detected person.

---

6 Select the **Min Exposure** from the drop-down menu.
The default setting is 1/10000s.

7 Select the **Max Exposure** from the drop-down menu.
The default setting is 1/8s.

8 Select the **Exposure Offset (F-Stops)** from the drop-down menu.
The default setting is 0.

9 Select the **Max Gain** from the drop-down menu.
The default setting is 51db.

10 Select the **Iris Level** from the drop-down menu.
The default setting is 1.

Note: The Iris Level differs depending on the camera.

---

11 Select the **Exposure (sec)** from the drop-down menu.
The default setting is 1/8s.

12 Select the **Manual Gain (dB)** from the drop-down menu.
The default setting is 0db.

13 Select the **Frequency** radio button for either **50Hz** or **60Hz**.
The default setting is 60Hz.

14 Select or clear the check box for **Flickerless Mode**.
This feature is not selected by default.

- When you select **Flickerless Mode**, the minimum and maximum exposure times are locked to 1/100 and 1/50 respectively (PAL) or 1/120 and 1/60 respectively (NTSC). This applies to all cameras referenced in this guide.

- End -

Procedure 63 Restore Exposure Defaults

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.
2	Select **Picture Settings** to view the **Picture Basic** tab.
3	Select  to start the video stream if it is not already active.
4	Select **Exposure Defaults** to restore the default settings.

- End -

Picture Additional

Configure Wide Dynamic Range, Day Night Mode, Picture Adjustments and White Balance.

Wide Dynamic Range

Wide Dynamic Range (WDR) is a feature that supports the viewing of high contrast scenes that include both bright and low light areas in the same field of view (FOV).

WDR Level allows you to adjust the WDR level to favor a underexposed or overexposed image. By selecting the lower end of the control, the image is underexposed which provides more detail in areas of bright but less details in areas of darkness. Selecting the higher end of the control, the image is overexposed which provides more detail in the dark areas but less details in the bright areas.

A typical use for this feature would be viewing a scene with both indoor and outdoor lighting conditions simultaneously, for example, in a warehouse area with an open bay door.

Procedure 64 Disable/Enable Wide Dynamic Range (WDR)

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.
2	Select **Picture Settings** and then select the **Picture Additional** tab.
3	Select the required WDR from the drop-down list: • **Off:** WDR is off • **Smart WDR:** Digital wide dynamic range, enhancing detail in darker areas • **True WDR:** Two shutter wide dynamic range, to compensate for bright and dark areas in the scene • **True WDR3x:** Three shutter wide dynamic range, to compensate for bright and dark areas in the scene

Note: TrueWDR3x does not apply to 8MP models.

The default setting is OFF.

- End -

Defog

Defog lets you automatically control and help reduce the effects of mist or fog on image quality. When enabled, continuous image analysis adjusts the amount of defog effect applied within the range of the strength.

Note: Defog has some limitation and may not be available when used with Certain Dynamic Range Controls.

Procedure 65 Disable/Enable Defog

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.
2	Select **Picture Settings** and then select the **Picture Additional** tab.
3	Select the **Enable Defog** drop-down menu and one of the following options: • **Off** • **Low** • **Mid** • **High** The default setting is Low for outdoor cameras and Off for indoor cameras.

- End -

Day Night Mode

IR/DayNight Mode utilizes a series of specific camera functions to dramatically enhance low light performance.

When needed, the True TDN mechanism removes an IR Cut Filter (IRCF) from in front of the images allowing the camera to see in black and white (BW) and utilize additional near-infrared energy found in many lighting sources like halogen, moonlight, etc.

This, along with slowing down another function, the shutter speed, significantly improves low light performance rendering clear images where none could be viewed previously.

IR Illuminator

When the camera is in B/W mode it can utilize or see near-IR illumination; something the human eye cannot do. This can be extremely powerful when the dome is paired with 850~950nm IR illuminators. With this combination a scene can be well lit with IR light that the dome can see but people cannot. This is great for areas where externally lighting is not allowed or there is a need for covert security.

Procedure 66 Enable / Disable IR Illuminator

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.
2	Select **Picture Settings** and then select the **Picture Additional** tab.
3	Select the **Enable IR Illuminator** check box to enable IR Illuminator.

OR

Clear the **Enable IR Illuminator**check box to disable **IR Illuminator**.

The default setting is 'Enabled'.

- End -

Day Night Mode

The dome provides a black-and-white (B/W) mode to improve camera performance when the light level falls below certain thresholds. This allows clear images to be obtained under low-light conditions.

Procedure 67 Configure Day Night Mode

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.
2	Select **Picture Settings** and then select the **Picture Additional** tab.
3	Select a **Day Night Mode** setting from the drop-down menu: • **Forced Color** - enable full-time color mode. • **Forced B&W** - enable full-time black and white mode. • **Auto Low** - camera will adjust between BW and Color depending on light levels. • **Auto Mid** - camera give a good balance of Color and BW depending on the scene. • **Auto High** - increases the chance of switching to BW mode as light levels drop. • **Manual** - a slider bar will display, the user can adjust the setting to suit the environment. The default setting is 'Auto Mid'.

- End -

Picture Adjustment

Adjust contrast, saturation, and sharpness of the image displayed on the video pane.

Procedure 68 Adjust the Contrast, Saturation, and Sharpness

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.
2	Select **Picture Settings** and then select the **Picture Additional** tab.
3	Select  to start the video stream if it is not already active. The video pane will display the current camera view.
4	Use the slider bars to adjust: • **Contrast**

- **Saturation**
- **Sharpness**

The values range from 1% to 100%. The video pane updates to display the new settings.

- End -

Procedure 69 Restore Picture Balance Defaults

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.
2	Select **Picture Settings** and then select the **Picture Additional** tab.
3	Select **Defaults** to restore the default settings. The default values are: • **Contrast:** 50% • **Saturation:** 50% • **Sharpness:** 50%

- End -

White Balance

White balance, the ability to keep whites looking white, is normally compensated for automatically using the default Auto White Balance setting.

Manual White Balance is available when specific color temperature settings want to be set and preserved. This can be done using the red and blue slider adjustments set for optimal viewing.

Procedure 70 Configure Auto White Balance

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.
2	Select **Picture Settings** and then select the **Picture Additional** tab.
3	Select  to start the video stream if it is not already active. The video pane displays the current camera view.
4	Select the required **White Balance** from the drop-down menu: • **Auto Normal:** Suitable for a normal range of lighting conditions • **Manual:** Adjustable red and blue balance sliders • **Auto Wide:** Suitable for a wider than normal range of lighting conditions The default setting is 'Auto Normal'.

- End -

Procedure 71 Manually Select White Balance

Step	Action

1 Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.

2 Select **Picture Settings** and then select the **Picture Additional** tab.

3 Select  to start the video stream if it is not already active.

The video pane displays the current camera view.

4 Select **Manual** from the White Balance drop-down menu.

The Red and Blue slider bars display.

5 Use the slider bars to adjust the **Red** and **Blue** balance.

The live video pane updates to display the new settings.

The red and blue values range from 1% to 100%.

If you change the configuration to **Manual**, the slider bar reads the real-time setting of the FOV.

- End -

Image Profiles

The Image Profiles feature enables users to capture, export and restore selected picture settings configurations from a previously saved data file. The data file can be saved to a specified location and used to restore the camera picture settings configuration.

Procedure 72 Capturing a profile

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.
2	Select **Picture Settings** and then select the **Image Profiles** tab.
3	Configure the required settings. **Note:**Frequency and Wide Dynamic Range settings are not supported.
4	Select **Save** in the **Capture Profile** section. The user is prompted to choose a location to save the file.

- End -

Procedure 73 Uploading a profile

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.
2	Select **Picture Settings** and then select the **Image Profiles** tab.
3	Select **Browse** in the **Upload Profile** section and navigate to saved data file.
4	Select **Upload**.
5	If the upload is successful, the profile is automatically applied to the camera and will be visible in the **Image Profiles** drop down list.

- End -

Procedure 74 Applying a profile

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.
2	Select **Picture Settings** and then select the **Image Profiles** tab.
3	Select uploaded profile from the **Image Profiles** drop down menu.
4	Select **Set**.

- End -

Procedure 75 Deleting a profile

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.
2	Select **Picture Settings** and then select the **Image Profiles** tab.
3	Select a profile from the list available.
4	Select **Delete**.

- End -

Image Stabilization

Electronic Image Stabilization (EIS) is a process where image stability is controlled through electronic processing procedures. Once EIS is enabled, image Field-of-View (FoV) is cropped. If the EIS device detects camera shake in pitch / yaw / roll directions, EIS responds by moving the cropped image offset and applying warp operation, so the image can remain in the position close to the original place as much as possible. There are 2 EIS modes, Low and High, where each mode will crop the image FoV by a percentage. Low crops the image FoV by 10% where High crops the image by 25%. In mode High, EIS will attempt to stabilize a greater vibration amplitude that Low mode.

Procedure 76 Setting the image stabilization

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.
2	Select **Picture Settings** and then select the **Image Stabilization** tab.
3	Select the **Image Stabilization Level** drop down icon and then one of the following: • **High** • **Low** • **Off** **Note:** The deafault setting is OFF.

- End -

Lens Calibration

Use the lens calibration process to recover focus and zoom after motor stalling has occurred. Motor step stalling is rare, but it can occur during shipping or through mishandling of the camera. If the One Touch focus at Wide or Tele is not working through the zoom range, the camera requires lens calibration. The lens calibration tool uses infinity focus curves to align the camera lens and correct problems focusing at Wide or Tele.

Lens calibration is automatic and you can run it from the **Lens Calibration** tab.

Procedure 77 Run a Lens Calibration

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.
2	Select **Picture Settings** and then select the **Lens Calibration** tab.
3	Select **Start Calibration** and wait for the camera lens initialization to complete.
4	To confirm the success of the lens calibration, select the **Picture Basic** tab from the **Picture Settings** menu and verify that the image is in focus through the zoom range. Use the **OneTouch** button to automatically focus the area.

- End -

Date / Time / OSD

Change the Camera Name, Date and Time and enable On-Screen Display (OSD).

Date Time

You can change the camera name and set the date and time.

Procedure 78 Change the Camera Name

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.
2	Select **Date/Time/OSD** to view the **Date Time** tab.
3	Enter the name of the camera in the **Camera Friendly Name** text box.

- End -

Procedure 79 Configuring the Date and Time

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.
2	Select **Date/Time/OSD** to view the **Date Time** tab.
3	Select the **Time 24-hour** check box to enable the 24-hour clock. Or

Deselect the **Time 24-hour** check box to enable the 12-hour clock.

The default setting is '24-hour'.

4 Select the **Date Display Format** from the drop-down menu:

- **DD/MM/YYYY**
- **MM/DD/YYYY**
- **YYYY/MM/DD**

The default setting is 'YYYY/MM/DD'.

5 Select the **Time Zone** from the drop-down menu.

The default setting is '(GMT-05:00) Eastern Time (US & Canada)

6 Select the **Set Time** setting by selecting the radio buttons:

- **Manually**
- **via NTP**

The default setting is 'Manually'.

7 If you select Manually in step 5:

a Select the Date **(DD/MM/YYYY)** using the drop-down menus.

b Select the Time **(HH:MM:SS)** using the drop-down menus.

8 If you select via NTP in step 5:

a Enter the **NTP Server Name** in the text box.

- End -

On-Screen Display (OSD)

You can enable or disable on screen display information.

Procedure 80 Changing the on screen camera text size

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.
2	Select **Date/Time/OSD** and then select the **OSD** tab.
3	In the **Text Size** section, select **Normal** to display the text in a normal size. OR In the **Text Size** section, select **Large** to display the text in a larger size. The default setting is 'Normal'.

- End -

Procedure 81 Display or Hide the Camera Name

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.

2 Select **Date/Time/OSD** and then select the **OSD** tab.

3 In the **Camera Name** section, select the **Enable** check box to display the camera name in the OSD.

OR

In the **Camera Name** section, clear the **Enable** check box to hide the camera name in the OSD.

The default setting is 'Disabled'.

- End -

Procedure 82 Display or Hide the Camera Time

Step	Action

1 Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.

2 Select **Date/Time/OSD** and then select the **OSD** tab.

3 In the **Date Time** section, select the **Enable** check box to display the camera name in the OSD.

OR

In the **Date Time** section, clear the **Enable** check box to hide the camera name in the OSD.

The default setting is 'Disabled'.

- End -

Procedure 83 Display or Hide the User Defined

Step	Action

1 Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.

2 Select **Date/Time/OSD** and then select the **OSD** tab.

3 In the **User Defined** section, select the **Enable** check box to display the camera name in the OSD.

OR

In the **User Defined** section, clear the **Enable** check box to hide the camera name in the OSD.

The default setting is 'Disabled'.

4 Select a **Location** from the drop-down menu.

5 Enter a name in the **Name** field.

The OSD User Defined fields must comply with the following validation criteria:

- 0 - 24 characters
- Cannot begin or end with:
  - . (dot)
  - - (hyphen)
  - _ (underscore)

- \ (backslash)
- " (quotes)

- End -

Privacy Zones

Privacy Zones are “masked” sections of the camera’s viewing area. These masks prevent operators of the surveillance system who do not have access to the camera password from viewing these designated zones. Each zone has four sides, and the zones may overlap to form irregular shapes.

The apparent size of the Privacy Zone adjusts automatically as the zoom level is adjusted. Privacy Zones are useful for high security areas. For example, you might establish a privacy Zone around a safe’s combination, but still view people approaching or opening the safe.

Up to 10 rectangular privacy zones can be used on the camera.

Defining a Privacy Zone

Create a privacy zone on the camera.

Procedure 84 Define a Privacy Zone

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.
2	Select **Privacy Zones** to view the Privacy Zones tab.
3	Select  to start the video stream if it is not already active. The video pane displays the current camera view. **Note:**Navigate to the centre of the camera field of view to create a privacy zone.
4	Click on the edit pencil button. Click and drag on the camera picture to define an area for the privacy zone. You must click and drag from the centre of the camera field of view.
5	Release the mouse button. The selected privacy area will turn yellow.
6	Select **Add** to save the current privacy zone.
7	To reselect an alternative area for the privacy zone select **Cancel** and repeat from step 4. **Note:**When a new privacy zone is created it is automatically enabled.

- End -

Enabling or Disabling a Privacy Zone

Select a privacy zone to hide or display on the camera.

Procedure 85 Enable/Disable a Privacy Zone

Step	Action

1 Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.

2 Select **Privacy Zones** to view the Privacy Zones tab.

3 Select  to start the video stream if it is not already active.

The video pane displays the current camera view.

4 Select the corresponding **Enabled** check box to enable the privacy zone.

OR
Clear the corresponding **Enabled** check box to disable the privacy zone.

- End -

Deleting a Privacy Zone

Delete a privacy zone from the camera.

Procedure 86 Delete a Privacy Zone

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Video**.
2	Select **Privacy Zones** to view the Privacy Zones tab.
3	Select the corresponding **Delete** check box to mark the privacy zone for deletion.
4	Select **Delete** to delete the selected privacy zones.
5	You are prompted to confirm the deletion.
6	Select **OK** to confirm the deletion. OR Select **Cancel**.

- End -

AI Privacy Mask

Unlike the traditional fixed-positioned privacy box that may unexpectedly filter-out critical details on a live video, AI Privacy Mask provides an AI-enabled dynamic privacy masking over each live AI Person object. AI Privacy Mask allows only what matters the most and the privacy of individual persons are masked per the need of GDPR or end-customer premises, and leave the details of the scene clean and visible in recorded videos.

Individually applicable to Stream 1 (e.g. recording, no masking) and/or Stream 2 (e.g. 1080p liveview masked) for flexible use cases.

Note: The masking will not be visible on GUI stream.

Procedure 87 Enabling AI Privacy Mask on Stream 1 and Stream 2

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **AI Privacy Mask** from the **Video** menu.

3 Select the **Redaction Class** drop-down icon and select one of the following options:

- **Person** blurs the entire person.
- **Face**: blurs the person's face only.

4 Adjust the **Minimum Confidence (40-99%)** slider bar and set a value.

5 Under the **Stream 1 AI Privacy Mask** heading, select the **Enable** check box to enable AI Privacy Mask for Stream 1.

6 Select the **Strength** drop down list and select one of the following options:

- Light:Level of bluriness set on a person.
- Medium: Level of bluriness set on a person.
- Strong: Level of bluriness set on a person.

OPTIONAL: You can also enable AI Privacy Mask for Stream 2.

7 Under the **Stream 2 AI Privacy Mask** heading, select the **Enable** check box to enable AI Privacy Mask for Stream 2.

8 Select the **Strength** drop down list and select one of the following options:

- Light:Level of bluriness set on a person.
- Medium: Level of bluriness set on a person.
- Strong: Level of bluriness set on a person.

- End -

Procedure 88 Disabling AI Privacy Mask on Stream 1 and Stream 2

Step	Action

1 Select **Setup** on the Web User Interface banner to display the setup menus.

2 Select **AI Privacy Mask** from the **Video** menu.

3 Under the **Stream 1 AI Privacy Mask** heading, select the**Enable** check box to remove the 'tick' and disable AI Privacy Mask for Stream 1.

OPTIONAL: You can also enable AI Privacy Mask for Stream 2.

4 Under the **Stream 2 AI Privacy Mask** heading, select the**Enable** check box to remove the 'tick' and disable AI Privacy Mask for Stream 2.

- End -

Region of Interest (ROI)

A region of interest is a defined area of the camera view which considered to be higher priority than areas of non-interest. For example, in secure environments, areas of potential activity could be a specific door or window. They are specified by drawing a rectangular overlay on the video stream. The overlay is highlighted in green and an OSD is displayed outlining the size % for the x and y axis. Up to five regions of interest can be configured, all of which can be enabled / disabled.

Procedure 89 Configure a Region of Interest

Step	Action

1 Select **Setup** on the Web User Interface banner to display the setup menus.

2 Select **ROI** from the **Video** menu.

3 Use the drawing tools to draw the region of interest overlay on the video stream.

4 Enter the name of the region of interest in the **Name** text box.

5 Select the **Enabled** check box to enable the region of interest.

OR

Clear the **Enabled** check box to disable the region of interest.

6 Click **Add**. The region of interest is configured.

- End -

Procedure 90 Delete a Region of Interest

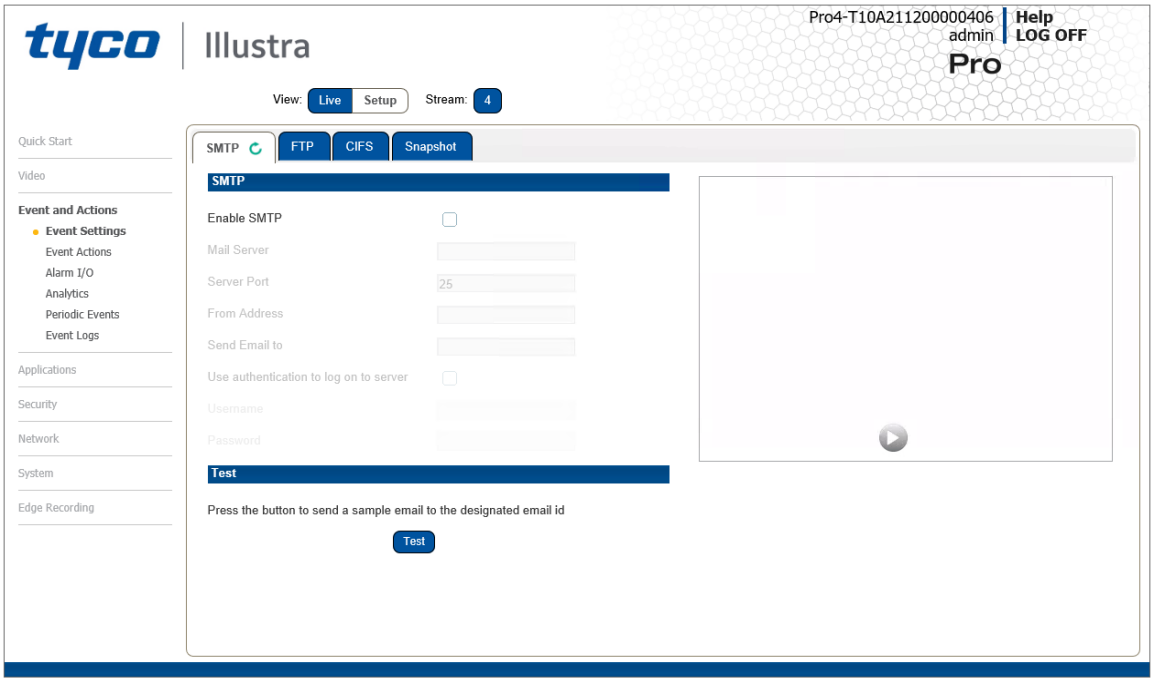
Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **ROI** from the **Video** menu.
3	Select  to delete the corresponding region of interest.

- End -

Events and Actions Menu

When you select the Events and Actions menu the Event Settings page displays, as seen in Figure 61 on page 107.

Figure 61 Events and Actions Menu



The Event Menu provides access to the following camera settings and functions:

- Event Settings
- Event Actions
- Alarms I / O
- Periodic Events
- Events Logs

Event Settings

Configure the SMTP, FTP, CIFS and Snapshot details required when setting Event Actions for analytic alerts.

SMTP

Configure the SMTP settings to allow e-mail alerts to be sent from the camera when an analytic alert is triggered. SMTP settings must be configured to enable email alerts when using analytics.

Procedure 91 Configure SMTP Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Events and Actions**.
2	Select **Event Settings** and then select the **SMTP** tab.
3	Select the **Enable SMTP** check box to enable SMTP. Fields on the tab become available for entry of information. OR Clear the **Enable SMTP** check box to disable SMTP. The default setting is 'Disabled'. **Note:**When in Enhanced Security mode, enabling SMTP requires the admin account password.
4	Enter the IP Address of the mail server in the **Mail Server** text box.
5	Enter the server port in the **Server Port** text box. The default setting is ‘25’.
6	Enter the from email address in the **From Address** text box.
7	Enter the email address to send email alerts to in the **Send Email to** text box.
8	Select the **Use authentication to log on to server** check box to allow authentication details to be entered. OR Clear the **Use authentication to log on to server** to disable authentication. The default setting is ‘Disabled’.
9	If ‘Use authentication to log on to server’ check box has been selected: a Enter the username for the SMTP account in the **Username** text box. b Enter the password for the SMTP account in the **Password** text box.

- End -

Test SMTP Settings

Test that the SMTP settings are configured correctly.

Procedure 92 Test the SMTP Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Events and Actions**.
2	Select **Event Settings** and then select the **SMTP** tab.
3	Select **Test** to send a sample email to the designated email id.

- End -

FTP

Configure the FTP settings for the FTP server. This is required to send video files from triggered analytic alerts. FTP must be configured to enable FTP video alerts when using analytics. You can configure FTP settings through the **Network** menu.

Procedure 93 Configure FTP Server Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Events and Actions**.
2	Select **Event Settings** and then select the **FTP** tab.
3	Select the **Enable FTP** check box to enable FTP. OR Clear the **Enable FTP** check box to disable FTP. The default setting is 'Enabled'.
4	If required, select the **Secure FTP** checkbox. The default setting is 'Disabled'. **Note:**When in Enhanced Security mode, enabling FTP requires the admin account password.
5	Enter the IP address of the FTP Server in the **FTP Server** text box.
6	Enter the FTP username in the **Username** text box.
7	Enter the FTP password in the **Password** text box.
8	Enter the FTP upload path in the **Upload Path** text box. **Note:** Refer Test the SMTP Settings on page 109 to confirm that the FTP settings are working as expected.

- End -

File Transfer Rate

You can limit the File Transfer Rate and assign a max transfer rate to manage the amount of FTP bandwidth used.

Procedure 94 Configure the FTP Transfer Rate

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Events and Actions**.
2	Select **Event Settings** and then select the **FTP** tab.
3	Select the **Limit Transfer Rate** check box to limited the FTP transfer rate. OR Deselect the **Limit Tranfer Rate** check box to disable limited FTP transfer. The default setting is 'Enabled'.
4	Enter the Max Transfer Rate in the **Max Transfer Rate** (Kbps) textbox.

- End -

Test FTP Settings

Test that the FTP settings are configured corretly.

Procedure 95 Test the FTP Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Events and Actions**.
2	Select **Event Settings** and then select the **FTP** tab.
3	Select **Test**. A sample text file is sent to the specified FTP destination to confirm that FTP settings are correct.

- End -

CIFS

The CIFS feature permits files generated from the camera such as alarm related video to be directed to network attached file storage through the Common Internet File System protocol. This supplements existing distribution methods such as FTP, SFTP and email.

Procedure 96 Configure CIFS Server Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Events and Actions**.
2	Select **Event Settings** and then select the **CIFS** tab.
3	Select the **Enable** check box to enable CIFS. OR

Clear the **Enable** check box to disable CIFS.

The default setting is 'Enabled'.

4 Enter the network path in the **Network Path** text box.

5 Enter the domain name in the **Domain Name** text box.

6 Enter the username in the **Username** text box.

7 Enter the password h in the **Password** text box.

- End -

Test CIFS Settings

Test that the CIFS settings are configured corretly.

Procedure 97 Test the CIFS Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Events and Actions**.
2	Select **Event Settings** and then select the **CIFS** tab.
3	Select **Test**. A sample text file is sent to the specified CIFS destination to confirm that CIFS settings are correct.

- End -

Snapshot

Snapshot is an image still of the current camera view saved in JPG file format. Snapshot can be generated without the need of an SD card.

Procedure 98 Enable a snapshot

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Events and Actions**.
2	Select **Event Settings** and then select the **Snapshot** tab.
3	Select the **Enable** check box to enable Snapshot. OR Clear the **Enable** check box to disable Snapshot. The default setting is 'Disabled'.
4	Select the **Record Source** stream from the drop down menu.

- End -

Event Actions

The camera can be commanded to carry out a specified operation when an analytic alert is triggered which are defined using event actions. Up to 5 event actions can be configured on the camera.

The event action can be used to configure any combination of the following actions:

- Record a clip to micro SD Card.
- Send an external alarm via email that includes alarm detail, where to retrieve the AVI video file and one JPEG picture of the event if recording MJPEG to micro SD Card. If MJPEG is not being recorded on micro SD Card, then no JPEG picture is sent.
- Send an AVI video file to a pre-configured external FTP or CIFS server. The video file contains pre and post alarm video buffer.
- Trigger alarm out.
- Audio Playback: Playback and Audio clip from the camera speakers when triggered.

Note:A micro SD Card must be inserted to enable recording and so that the camera can send FTP, CIFS, and SMTP events. SMTP e-mails are sent without inserting a micro SD card but do not include snapshot images of the event trigger. Micro SD cards are also required for audio clip storage on the camera.

Creating an Event Action

Configure an event action which can be triggered by an analytic alert.

Procedure 99 Create an Event Action

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Events and Actions**.
2	Select **Event Actions** to view the event actions tab.
3	Select an entry on the event actions list and enter an event action name in the **Name** text box.
4	Select the **Output** check box to enable an alarm output.
5	Select the **Record** check box to enable the Record Settings.
6	Select the **Snapshot** check box to enable the snapshot.
7	Select the **Email** check box to send an e-mail to the email address configured in the Configure SMTP Settings procedure.
8	Select the **FTP** check box to send a video file to the FTP details configured in the Configure FTP Server Settings procedure.
9	Select the **CIFS** check box to send a video file to the SFTP details configured in the Configure CIFS Server Settings procedure.

Note:
1. If you select Record, the AVI clip is saved to the micro SD card and it has to be removed from the camera to view the video file.
2. AVI clips can only be sent through FTP if a micro SD card has been installed and FTP and CIFS has been selected.

3. The selected pre and post event duration buffer is included in any video clips sent through FTP and CIFS.

10 Select the **SIP Call** check box and enter the extension in the text box to enable the camera to make an SIP call when the event has triggered.

11 Select the **Audio Playback** option from the drop-down menu.

- End -

Editing a Event Action

Modify the details of an existing event action.

Procedure 100 Edit an Event Action

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Events and Actions**.
2	Select **Event Actions** to view the event actions tab.
3	Select an entry on the event actions list, you can edit the following: • **Name** • **Output** - Enable/Disable • **Record** - Enable/Disable • **Snapshot** - Enable/Disable • **Email** - Enable/Disable • **FTP** - Enable/Disable • **CIFS** - Enable/Disable • **SIP Call** - Enable/Disable • **Audio Playback** - select the required audio clip

- End -

Alarm I / O

The cameras provide one alarm input. By connecting alarm devices, such as smoke alarms, twilight sensors, or motion sensors to these inputs you can enhance the usability of your video surveillance system.

For 15 seconds after being triggered, any additional individual input changes on that alarm source are logged and do not generate any other action. This is to reduce the effect that any oscillating alarm source, such as if a door is simply vibrating in the wind, causing a series of alarms to be generated.

Input alarms are triggered upon change of state. Either from opened to closed or from closed to open. The camera reports the current state of each input alarms (open or closed) as well as an active or inactive status in the alarm configuration page. Active alarms are also be visible in the current faults page.

The triggering of any input alarm affects scheduled tasks and delay them until at least 30 seconds has passed since the last digital alarm input was triggered.

Alarm Actions

Upon triggering each alarm input can be configured to trigger a faulty action:

- Activate the digital output contact. This stays active until the alarm is acknowledged and cleared by an operator.
- Send an external alarm WS-Event that includes alarm details
- Send an external alarm through email that includes alarm detail, where to retrieve the AVI video file and one JPEG picture of the event if recording MJPEG to local storage. If MJPEG is not being recorded on local storage, then no JPEG picture is sent.
- Send an audio file through the unit. If a speaker has been connected to the audio output on the unit the file can be played as the alarm is triggered.
- Send an AVI video file to a pre-configured external FTP server. The video file contains pre and post alarm video buffer and audio if enabled and supported, as outlined above.

Note:
1. An active internal alarm only resets when the input state changes to “normal.” A manual reset is not available.
2. A micro SD Card must be inserted to send an SMTP email, video files, audio and images from triggered alarms.

Procedure 101 Configure an Alarm

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Event and Actions**.
2	Select **Alarm I/O** to view the alarm I/O tab.
3	Enter the alarm name in the **Name** text box.
4	Select the **Enabled** check box to enable the alarm. OR Clear the **Enabled** check box to disable to alarm.
5	Select when the alarm is required to be activated from the **Normal** drop-down menu. i.e. when the dry contact is open or closed.
6	Select the required configured fault action from the **Action** drop down menu.

- End -

Procedure 102 Enable/Disable an Alarm

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Event and Actions**.
2	Select **Alarm I/O** to view the alarm I/O tab.
3	Select the **Enabled** check box to enable the corresponding alarm. OR Clear the **Enabled** check box to disable the corresponding alarm.

- End -

Enable or Disable Alarm Output

Alarm Output allows the alarm to activate a digital output as an action. For example, this digital output could be linked to an electrical device, i.e. a security light or siren.

Procedure 103 Enable/Disable Alarm Output

Step	Action
1	Select **Alarm I/O** from the **Event and Actions** menu.
2	Select the **Output** check box to enable alarm output. OR Clear the **Output** check box to disable alarm output.
3	Select the **Output Type** drop-down menu icon and then select one of the following: • **Latching:** Alarm out will stay active until the user manually clears it via the GUI. • **Momentary:** Alarm out will trigger for a short period (0.5 sec) before resetting (default). • **Timed:** Alarm out will trigger for a user defined period (1- 60sec) before resetting. Select the **Duration (seconds)** text box and enter a number beween 1 - 60 to set the duration.

- End -

Procedure 104 Clearing Alarm Output

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Event and Actions**.
2	Select **Alarm I/O** to view the alarm I/O tab.
3	Under **Alarm Output**, select the **Apply** button to Clear Active Output. The Alarm Output is cleared.

- End -

LED

The LED menu is specific to the Illustra Pro 4 Corner camera, the menu will offer use configuration of the LED present on this camera.The Tally LED has a function of Recording indicator, while the White LED has a function of Illuminator/Deterrent.

Procedure 105 Configure Tally (Red) LED

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Event and Actions**.
2	Select **LED** to view the alarm LED tab.
3	Select from the following options in the drop down for Tally LED:

Always On (default setting)	The tally LED is always on (flashing*), even if no video or audio stream is being pull from the device or recorded to the edge storage (SD card)
Always Off	The tally LED is always off, even if a video or audio stream is being pull from the device or recorded to the edge storage (SD card)
Auto	The tally LED is automatic on (flashing*) when a video or audio stream is being pull from the device or recorded to the edge storage (SD card)

- End -

Procedure 106 Configure White LED

Step	Action

1 Select **Setup** on the Web User Interface banner to display the setup menus and then select **Event and Actions**.

2 Select **LED** to view the alarm LED tab.

3 Select from the following options in the drop down for White LED:

Off (default)	White LED off
On	White LED permanently on
Auto	Event Action linked - White LED on for 10 seconds
Flashing	Event Action linked - White LED Flashing for 10 seconds

4 Use the White Intensity slider to adjust the intensity of the white LED when it is on.

- End -

Periodic Events

The camera can generate a scheduled event with an associated event action. The event can be set to trigger between 5 to 60 minute interval. You can name the event, enable or disable it, set the time and associate the event action.

Procedure 107 Configure a Periodic Event

Step	Action

1 Select **Setup** on the Web User Interface banner to display the setup menus and then select **Event and Actions**.

2 Select **Analytics** and then select the **Periodic Events** tab.

3 Enter the name of the periodic event in the **Name** text box.

4 Select the **Enabled** check box to enable the Periodic Event.

OR

Clear the **Enabled** check box to disable the Periodic Event.

5 Select the **Periodic Time (min)** drop-down menu to select a value for the periodic time.

6 Select the **Action** drop-down menu to select a fault action.

- End -

Event Logs

Event Log

When events are triggered the resulting alarms are displayed in the Event Log with the following information:

- **No.** - details the event index.
- **Event** - this is listed as 'MotionDetected'.
- **Date created** - the time and date when the motion detection was triggered.
- **Component** - internal software component that raised the fault for a motion detection alert. This is listed as ANALYTICS.
- **Severity** - indicates how serious the fault is. Motion detection alerts list as 'Warning'.
- **Detail** - extra information that supplements the motion detection alert.
- **Delete** - remove the motion detection alert notification from the fault table.

Procedure 108 Display Event Log

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Event and Actions**.
2	Select **Event Logs** to view the Event Log tab.
3	The Event Log tab displays. Triggered motion detection alerts display.

- End -

Procedure 109 Delete Current Events

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Event and Actions**.
2	Select **Event Logs** to view the Event Log tab.
3	Select the corresponding **Delete** check box to mark the motion detection alert for deletion. OR Clear the corresponding **Delete** check box to keep the motion detection alert. **Note:**You can select the **Select All** check box to mark all motion detection alerts displayed in the list for deletion.
4	Select **Delete** to delete the selected motion detection alerts. You are prompted to confirm the deletion.

5	Select **OK** to confirm the deletion. OR Select **Cancel**.

- End -

Fault Log

Any system or environmental faults experienced by the camera are displayed in the Fault Log with the following:

- **#** - details the fault index.
- **Fault** - a description of the fault.
- **Date created** - the time and date when the fault occurred.
- **Component** - internal software component that raised the fault.
- **Severity** - indicates how serious the fault is. The following are supported, in increasing order of severity, Clear, Warning, Critical and Error.
- **Detail** - extra information that supplements the fault description.
- **Delete** -remove the fault from the fault table.

System Faults

The following system faults may be raised:

- **DiskUsage(Warning)** - this warning is raised when the disk utilisation rises above the threshold value “threshold2” held in SYSM.conf. Once an alarm is generated and the disk utilization decreases 1% below the threshold value, the fault is then automatically cleared. The default threshold value is 80%.

Environmental Monitor (ENVM) Component

The following environmental faults can be raised by the ENVM (Environmental Monitor) component:

- **TemperatureTooHigh (Warning)** - this fault is raised when the internal temperature of the enclosure is equal to or exceeds the value MAX_TEMPERATURE held in ENVM.conf. Once an alarm is generated and the temperature drops to a level 1 degree below the MAX_ TEMPERATURE value the fault is then automatically cleared. This is to avoid transient changes in temperature around the threshold.
- **TemperatureTooLow (Warning)** - a fault is raised when the internal temperature of the enclosure is equal to or is below the value MIN_TEMPERATURE held in ENVM.conf. Once an alarm is generated and the temperature drops to a level 1 degree above the MIN_ TEMPERATURE value the fault is then automatically cleared. This is to avoid transient changes in temperature around the threshold.

Procedure 110 Display Current Faults

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Event and Actions**.
2	Select **Event Logs** and then select the **Fault Log** tab.

- End -

Procedure 111 Delete Current Faults

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Event and Actions**.
2	Select **Event Logs** and then select the **Fault Log** tab.
3	Select the corresponding **Delete** check box to mark the fault for deletion. OR Clear the corresponding **Delete** check box to keep the fault. **Note:**You can select the **Select All** check box to mark all faults displayed in the list for deletion.
4	Select **Delete** to delete the selected faults. You are prompted to confirm the deletion.
5	Select **OK** to confirm the deletion. OR Select **Cancel**.

- End -

Analytics

Video analytics is a technology used in security cameras to analyse video in order to identify changes in the scene or detect objects, and raises specific events in response. As well as Motion Detection, Blur and Tamper which analyse the pixel change in the Field Of View, Illustra cameras offer advanced AI Intelligence which allows configuration of specific rules to identify specific object classes.

Note: WebGUI AI Overlay Detections shows all analytic objects and not just those specific to the configured Events / Rules.

Face Detection

Face Detection works by detecting human faces and ignoring other objects, such as trees or buildings. This feature can be enabled or disabled and the required face orientation selected.

Note: Face detection is subject to a free licence request in order to enable the feature.

Procedure 112 Enable / Disable Face Detection

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Analytics**
2	Select the **Face Detection** tab.
3	To enable Face Detection on the camera: a Select the **Enable Face Detection** checkbox. b Select the **Highlight Faces** checkbox to enable OR Deselect the **Highlight Faces** checkbox to disable. c Select the **Enhances Faces** checkbox to enable. OR Deselect the **Enhances Faces** checkbox to disable. d Select the **Face Orientation** from the drop-down menu. • **Up** • **Left** • **Right** OR Deselect the **Enable Face Detection** checkbox to disable Face Detection on the camera.
4	Select the required pre-configured action to be taken if a face is detected from the **Action** drop down menu.

- End -

Motion Detection

Motion detection enables you to define a region of interest in the camera's field of view which can be used to trigger an Event Action. Multiple areas of interest can be selected in the field of view but only one Event Action may be triggered.

Motion Detection Best Practices

To ensure you get the highest quality results when using Motion Detection on the camera it is recommended that you adhere to the following:

- An object exhibiting motion needs to be at least 8x8 pixels in size to be detected.
- The color of the object (in gray scale) should be approximately 10-15% different than the background.
- Exclude the Time Stamp region from motion detection, because the time stamp changes constantly and could register as motion.
- Try not to point cameras into sunlight, because high brightness prevents detection of movement of bright objects such as a person with a white shirt.
- Avoid areas with persistent motion, such as trees, blinking lights, or spinning signs, by using an appropriate region of interest.

Motion Detection Configuration Pane

The regions of interest within the camera's field of view are defined using the Motion Detection Configuration Pane. The regions of interest are set by drawing/highlighting an area on the pane. This is done by using the drawing tools on the Motion Detection Configuration Pane.

Creating a Motion Detection Alert

Create a motion detection alert on the camera.

The Motion Detection Alert feature supports up to three profiles in a Field of View (FOV). You can configure each profile with an individual sensitivity level and an event action.

Note:

1 If the motion detection video stream is changed after the region of interest has been drawn it is necessary to re-draw a new region.

2 If the stream settings are modified the motion detection is disabled and it is necessary to enable motion detection again if required.

3 Motion detection can only be enabled on a video stream that uses H.264 with a resolution on 1920x1440 or lower.

Procedure 113 Create a Motion Detection Alert

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Analytics**
2	Select the **Motion Detection** tab.
3	Select the **Enable motion detection** check box to enable Motion Detection on the camera. OR Clear the **Enable motion detection** check box to disable Motion Detection on the camera.

4 Select the zone for detection in the **Motion zone** drop-down list.

5 Select the **Enable motion zone** check box to enable the zone for motion detection.

6 Select **Edit** in the **Region configuration** field.

7 Use the drawing tools on the Motion Detection Configuration Pane to draw the region of interest on the pane. Multiple selections can be made.

8 Select the sensitivity from the **Sensitivity** drop-down menu:

- **Highest**
- **High**
- **Medium**
- **Low**
- **Lowest**

9 Select the fault action from the **Action** drop-down menu.

This fault action activates when motion is detected in the selected region of interest.

Refer to the Create a Fault Action procedure if a fault action has not yet been defined.

10 Select **Apply** to save the changes.

- End -

Enable or Disable a Motion Detection Alert

Motion detection can be turned on and turned off when required.

Procedure 114 Enable or Disable a Motion Detection Alert

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Analytics**
2	Select the **Motion Detection** tab.
3	Select the **Enable motion detection** checkbox to enable Motion Detection on the camera. OR Clear the **Enable motion detection** checkbox to disable Motion Detection on the camera.
4	Select **Apply** to save.

- End -

Artificial Intelligence Object Classification

Artificial Intelligence Object Classification Camera Alarms

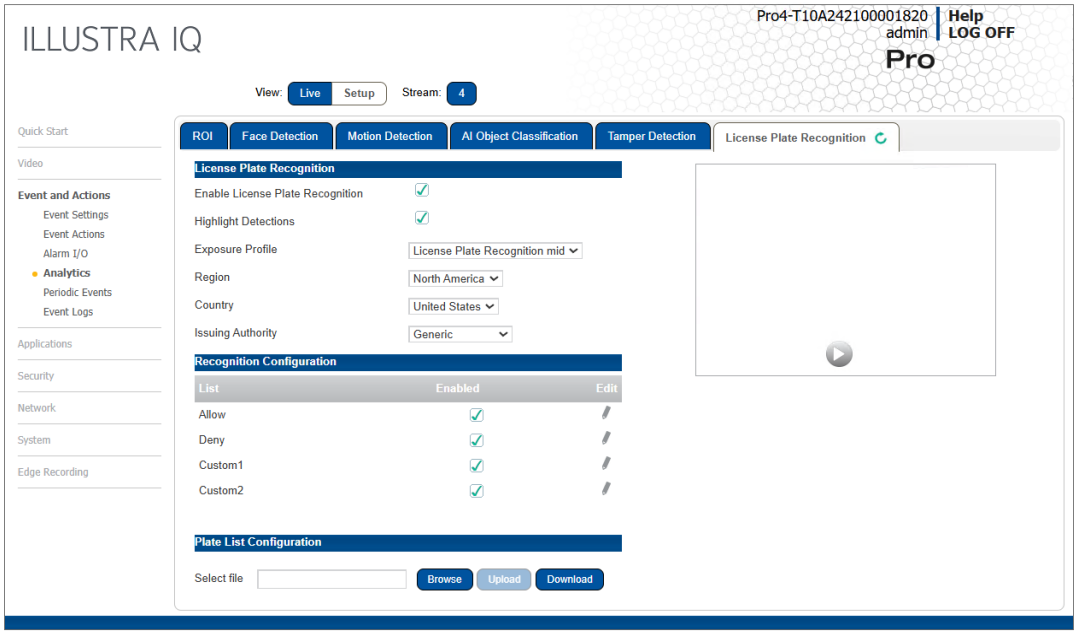
After enabling Artificial Intelligence Object Classification on a camera, you can define alarm rules that trigger an event.

Each camera can have any number of independent Artificial Intelligence Object Classification rules. In each rule you can define the areas in the cameras view that you want to monitor. You can name each alarm rule. It is best to use descriptive names like ‘Back Door’ or ‘Conference Room’, as these

names make it easier to identify the alarm rule in the alerts log better than an abstract name. You can choose the Artificial Intelligence Object Classification or Deep Intelligence type for the rule.

The areas that you want to monitor in a cameras view are configured in the Camera Alarm Configuration drawing window, a live display of the camera view. To determine the areas of the camera view that you want monitored, you need to draw on the window. Use the drawing tools to draw on the Camera Alarm Configuration window.

Figure 62 Artificial Intelligence Object Classification Tab



Artificial Intelligence Object Classification Best Practices

To ensure you get the highest quality results when using Artificial Intelligence Object Classification on the NVR, it is recommended that you adhere to the following:

- An object exhibiting movement or a change in the scene background must be large enough to be detected, i.e. it must be around 1/25 of the image size.
- The color of the object (in grayscale) should be approximately 10-15% different than the background.
- The frame rate of the video should be high enough to capture the object in one or more captured frames.
- Artificial Intelligence Object Classification events create entries in the victor Application Server database. It is important to ensure that the Artificial Intelligence Object Classification parameters are accurate to avoid generating false log entries.
- Try not to point cameras into sunlight, because high brightness will prevent detection of movement of bright objects such as a person with a white shirt.
- Avoid areas with persistent motion, such as trees, blinking lights, or spinning signs, by using an appropriate region of interest.
- Choose your Artificial Intelligence Object Classification alarms selectively. You do not want to create alarms that will trigger a high number of alerts, making the important alerts more difficult to identify.
- Situate cameras to provide the best possible views of the areas of interest, objects and people. It is best to ensure camera views separate objects from people, ensure objects and people take up a larger portion of the camera view, and keep the entire region of interest within the camera's view.
- Use staff to help identify regions of interest to monitor based on their observations, for example, of missing merchandise or missing fixtures.Artificial Intelligence Object Classification alarms can therefore be configured to monitor areas of potential activity.
- Use searches frequently and watch activity leading up to an alarm being triggered. This may give an indication of suspicious activity and other areas to monitor.
- Tune your alarms regularly to ensure the alarms reflect changes to the environment, for example, objects being rearranged or replaced. Monitoring these changes and re-tuning your alarms will ensure maximum effectiveness of the Artificial Intelligence Object Classification alarms and searches.
- Use the new information that Artificial Intelligence Object Classification provides to learn and adapt. Use it to implement changes that will improve surveillance and reduce losses, for example, eliminate blind spots, make staff aware of suspicious behavior, or re-design the environment and alarms

Artificial Intelligence Object Classification

In this section you can confirgure 'smarter' alerts or events, for example an alert for when a vehicle is in a pedestrian area, or when a person is in a scene . This eliminates 'false' alerts from standard motion detection because trees are blowing or an animal crosses a scene.

Note: WebGUI AI Overlay Detections shows all analytics objects and not just those specific to the configured Events / Rules

Creating an Artificial Intelligence Object Classification Camera Alarm

To create an AI Object Classification camera alarm you must have AI Object Classification enabled on the camera.

Procedure 115 Enable/Disable AI Object Classification

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Analytics.**
2	Select the **AI Object Classification** tab.
3	Select the **Enable AI Object Classification** check box to enable AI Object Classification on the camera. OR Deselect the **Enable AI Object Classification** check box to disable AI Object Classification on the camera. **Optional** - Highlight Detections. a Select the **Highlight Detections** check box to enable Highlight Detections on the camera. OR a Deselect the **Highlight Detections** check box to disable Highlight Detections on the camera.
4	Use the **Engine Minimum Confidence** slider bar to set the minimum confidence of the overall engine to generate continuous metadata and alarms, this range is from 40% to 100%. The default is 40%. **Note:**Changing this value will Affect AI rules and other AI based applications like AI Person Counting and AI Privacy Mask. Please make sure AI rules are the same, equal or above the minimum AI Object classification setting.

- End -

Procedure 116 Creating a Analytic Rule in AI Object Classification

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Analytics.**
2	Select the **AI Object Classification** tab.
3	Select the **Enable AI Object Classification** check box to enable AI Object Classification on the camera.
4	Select **New Rule.**
5	Type a **Rule Name** for your rule definition in the field provided.
6	Select a fault action from the **Action** drop-down menu. This fault action is activated when the parameters of the analytics rule are met.
7	Select a rule type from the **Rule Type** drop-down menu:

a **Object Detection** - Used to detect people or objects moving into a region of interest. This alarm is similar to a motion alarm, but only detects people or objects the first time they enter the region of interest. A separate event is generated for each object that enters the region, even if the objects move into the region at the same time, unlike motion detection that generates one event.

b **Abandoned / Removed** - Used to find changes to the background of a scene in a region of interest, for example, use it to detect when a stationary object was placed, moved or removed. Draw the region of interest that contains all of the area you want to search for changes.

c **Direction** - Used to detect objects moving in a certain direction through a region of interest, for example, a car traveling the wrong way on a road. It is best to use a thin region of interest to detect the direction of an object.

d **Linger** - Used to detect objects loitering in a region of interest. An object is lingering if it remains in the region of interest. The minimum amount of time an object must linger before being included in the results can be defined and you can draw a region in the area where you want to detect objects lingering. Use a higher Overlap setting to avoid detecting objects lingering nearby.

e **Dwell**: Used to detect objects lagging or tarrying in a region of interest. An object is dwelling if it is mostly stationary. The minimum amount of time an object must dwell before being included in the results can be defined. Draw a region in the area where you want to detect objects dwelling. Use a higher Overlap setting to avoid detecting objects dwelling nearby.

f **Enter** - Used to detect objects entering a camera view through a region of interest, for example, a doorway or threshold. It is best to draw the region of interest around the doorway or threshold to include areas in which the door can move or objects can be seen, for example, glass. This will exclude objects that can be seen in the region of interest but does not pass through it.

g **Exit** - Used to detect objects exiting a camera view through a region of interest, for example, a doorway or threshold. It is best to draw the region of interest around the doorway or threshold to include areas in which the door can move or objects can be seen, for example, glass. This will exclude objects that can be seen in the region of interest but does not pass through it.

h **Crowd Formation**: Used to detect and raise an alarm when a crowd forms in a specified region of interest. A minimum crowd size can be specified to trigger alarms only when the specified size is reached. For example if a particular region should not have more than 2 people at any given time the minimum crowd size should be set to 3.

i **Queue Analysis**: Used to monitor length of queues, for example, in a point of sale environment or highway tollbooth. Alarms can be triggered for when a queue grows beyond or falls below a specified threshold.

j **Perimeter**: Used to detect when objects enter a protected area through a perimeter area, or detect when an object is in the perimeter area for too long. Draw regions of interest to define the perimeter area and the protected area. You must also draw regions of interest to define the minimum size and the maximum size of objects that can trigger the perimeter alarm.

k **Tripwire**: AI Object classification is used to trigger when people cross a region of interest, usually a straight line or a combination of 2 lines forming an angle. People can be triggered going left, right of the line or both direction. Draw a tripwire and select the direction you want the alert to trigger.

8 Select the **Object Class** drop down and one of the following options:

- **Any Class**
- **Bicycle**
- **Bus**
- **Car**
- **Motorbike**
- **Person**
- **Train**
- **Truck**
- **Cart**
- **Backpack**
- **Handbag**
- **Suitcase**

9 Use the **Overlap** slider bar to increase or decrease the percentage of overlap.

10 Select **Save** to save your changes.

The rule name and type that you have created appears in the **Analytics Rules** table.

Note: When rule type is selected , extra configuration items appear for some rule types. See the section on Artificial Intelligence Object Classification above for information on the extra configuration options for each rule type.

Object Detection - Overlap (%) - The amount of a detected object that must be in the region of interest before an alarm is triggered. Use a higher setting to detect objects that are mostly inside the region, and use a lower value to find objects that just brush the edge of the region.

Linger

Overlap (%) - The amount of detected object that must be in the region of interest while lingering for an alarm to be triggered. Use a higher setting to avoid detecting objects lingering nearby.

Linger Time - The minimum amount of time an object lingers before the alarm is triggered.

Dwell

Overlap (%) - The amount of a detected object that must dwell in the region of interest for an alarm to be triggered.

Dwell Time - This is the minimum amount of time that an object must dwell in the region of interest before the alarm is triggered.

Perimeter

Select Area - Additional tools display when using perimeter to highlight zones of interest. Use these tools to define the zones of interest for the protected area and the perimeter area. Each selection is highlighted via a different color (perimeter area = green, protected area = yellow).

Linger Time - The minimum amount of time an object lingers before the alarm is triggered.

- End -

Procedure 117 Enable/Disable an Analytics Rule in AI Object Classification

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Analytics.**
2	Select the **AI Object Classification** tab.
3	From the Analytics Rules table, select the check box of the target Analytics Rule to enable the analytics rule OR Deselect the check box of the target Analytics Rule to disable the analytics rule.
	- End -

Procedure 118 Edit an Analytics Rule

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Analytics.**
2	Select the **AI Object Classification** tab.
3	From the Analytics Rules table, select the edit icon across from the analytics rule that you want to edit.
4	Edit the settings in the Rule Definition until you are happy with your changes.
5	Select **Save** to save your changes.
	- End -

Procedure 119 Delete an Analytics Rule

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Analytics.**
2	Select the **AI Object Classification** tab.
3	From the **Analytics Rules** table, select the delete icon across from the analytics rule that you want to delete.
4	Select **OK** when you are asked to confirm your action.
5	Select **Save** to save your changes.
	- End -

Person Counting

This AI application is designed to assist the improvement of building management efficiency by providing business intelligence of human traffic into a premise and its concurrent occupancy rate.

Illustra Pro AI is significantly more accurate than traditional person counting because a person must be classified as an AI Person object first then it must cross over an AI Tripwire rule.

Procedure 120 Enabling and configuring person counting

Step	Action

1 Select **Setup** on the Web User Interface banner to display the setup menus.

2 Select **Person Counting** from the Analytics menu.

3 Select the **Enable Person Counting** check box to enable person counting.

4 Select the **New Rule** button to view the Rule Definition settings.

5 Select the **Rule Name** text box and enter a name.

6 Select the **Action** drop down list and select a Fault Action.

7 Select the **Minimum Confidence (40-99%)** slider bar to the desired percentage.

8 Select the **Count Type** drop down list and select one of the following options:

- **In: Keep count of people crossing the line in the direction of the yellow arrow**
- **Out: Keep count of people crossing the line in the direction of the green arrow**
- **In and Out: Keep count of people crossing the line in the direction of the both the yellow and green arrow**

9 Select one of the **Line Style** options under the video pane and then click on the video pane to draw a line.

OPTIONAL 1: Select the **Clear** button to remove all line styles from rule definition and start fresh.

OPTIONAL 2: Select the **Swap Direction** button to set the desired direction for the IN and/or OUT rule.

10 Select the **Save** button to save all settings.

Note: The Person count feature will offer no Stream OSD or visual information on camera UI, this feature is designed for Integration with vVE and Exacq.

- End -

Procedure 121 Disabling person counting

Step	Action

1 Select **Setup** on the Web User Interface banner to display the setup menus.

2 Select **Person Counting** from the Analytics menu.

3 Select the**Enable Person Counting** check box to disable person counting.

- End -

Procedure 122 Editing configured rules

Step	Action

1 Select **Setup** on the Web User Interface banner to display the setup menus.

2 Select **Person Counting** from the Analytics menu.

3 Under the Configured Rules heading, select the  icon to edit any of the configured rules in the list.

4 Select the **New Rule** button to view the Rule Definition settings.

5 Select the **Rule Name** text box and enter a name.

6 Select the **Action** drop down list and select a Fault Action.

7 Select the **Minimum Confidence (40-99%)** slider bar to the desired percentage.

8 Select the **Count Type** drop down list and select one of the following options:

- **In: Keep count of people crossing the line in the direction of the yellow arrow**
- **Out: Keep count of people crossing the line in the direction of the green arrow**
- **In and Out: Keep count of people crossing the line in the direction of the both the yellow and green arrow**

9 Select one of the **Line Style** options under the video pane and then click on the video pane to draw a line.

OPTIONAL: Select the **Clear** button to remove all line styles on the video pane.

OPTIONAL: Select the **Swap Direction** button to swap the direction of the line styles on the video pane.

10 Select the **Save** button to save all settings.

- End -

Procedure 123 Deleting configured rules

Step	Action

1 Select **Setup** on the Web User Interface banner to display the setup menus.

2 Select **Person Counting** from the Analytics menu.

3 Under the Configured Rules heading, select the  icon to delete any of the configured rules in the list.

4 Select the**OK** button to delete the configured rules.

- End -

Procedure 124 Resetting the person counter

Step	Action

1 Select **Setup** on the Web User Interface banner to display the setup menus.

2 Select **Person Counting** from the **Analytics** menu.

a Select the **Reset Time (HH:MM)** drop down list to enter a specific time when the person counter should rest.

OR

a Select the Manual Reset **Reset** button to reset the person counter.

- End -

Tamper Detection

A Tamper Detection event can be created when the screen is blocked or camera position is changed. Option to detect image being affected by Blackout or Brightness can also be enabled.

Procedure 125 Enable Tamper Detection

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Event and Actions**.
2	Select **Analytics** and then select the **Tamper Detection** tab.
3	Select the **Enable Tamper Detection** check box to enable Tamper Detection.
4	Select the **Action** drop-down list and select an option.
5	Use the slider bar to select the **Threshold**.
6	Use the slider bar to select the **Duration (seconds)**.
7	Select the **Image Too Dark Alarms** check box to enable or disable detection when the image is obscured.
8	Use the slider bar to select the **Dark Alarm Threshold (%)**. **Note:**100% is full image blackout.
9	Select the **Image Too Bright Alarms** check box to enable or disable detection when the image is obscured.
10	Use the slider bar to select the **Bright Alarm Threshold (%)**. **Note:**100% is full image blackout.

- End -

Procedure 126 Disable Tamper Detection

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Event and Actions**.
2	Select **Analytics** and then select the **Tamper Detection** tab.
3	Uncheck the **Enable Tamper Detection** check box to disable Tamper Detection.

- End -

Blur Detection

The camera generates an alarm and then takes the action you specified during configuration when the Blur Detection feature is enabled and the camera detects incidents that make the video image blur, such as: redirection, blocking, or defocusing.

When you enable Blur detection, it has a polling period of roughly 1 minute.

A Blur Detection start fault is raised when blur has been detected at 60 successive polling periods of 1 second (up to 1 minute).

Procedure 127 Enable Blur Detection

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Event and Actions**.
2	Select **Analytics** and then select the **Tamper Detection** tab.
3	Select the **Enable Blur Detection** check box to enable Blur Detection.
4	Select the **Action** drop-down list and select an option.
5	Select the **Sensitivity** drop-down list and select an option.
6	Use the slider bar to select the **Duration (seconds)**.

- End -

Procedure 128 Disable Blur Detection

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Event and Actions**.
2	Select **Analytics** and then select the **Tamper Detection** tab.
3	Uncheck the Enable Blur Detection check box to disable Blur Detection.

- End -

Audio Detection

An Audio Detection event can be created when the camera detects a sound that falls into one of the following pre-determined rules.

- Loud abnormal Sound Alert
- Glass Break Alert
- Fire/Smoke Alarm Alert
- Low Pitch Alert
- Scream Alert

Procedure 129 Configuring Audio Detection rules

You can enable, edit and delete the following 5 audio detection rules; Loud Abnormal Sound, Glass breaking, Fire/Smoke Alarm, Low Pitch Abnormal Sound and Scream.

Step	Action
1	Select **Setup** and then Analytics to view the **Audio Detection** tab.
2	Make sure that the correct audio input is connected and configured then select the **Enable Audio Detection** check box to enable Audio Detection.
3	Select the **Edit Advanced Audio AI Settings** check box to edit the Audio Detection settings. a Select the **RMS Onset Sensitivity** drop-down menu and select one of the following options

- Highest
- High
- Medium
- Low
- Lowest

Note:RMS Onset Sensitivity controls the rule's response to ambient noise. For example, in a very quiet office, set RMS Onset Sensitivity to Highest or High, and in a noisy place like a school, set RMS Onset Sensitivity to Low or Lowest.

b Select the **RMS Loud Sensitivity** drop-down menu and select one of the following options

- Highest
- High
- Medium
- Low
- Lowest

Note:RMS Loud Sensitivity controls how much noise triggers the event. For example, in a very quiet office, set RMS Loud Sensitivity to High or Medium, and in a noisy place like a school, set RMS Loud Sensitivity to Lowest.

4 Select the **Apply** button and then select **OK** to save the settings.

Note: All 5 Audio Detection Rules are visible under the Audio Detection Rules heading and all 5 are enabled by default.

5 To **Disable** an Audio Detection Rule, uncheck the respective Enabled check box and then select **OK**.

6 To **Edit** an Audio Detection Rule, select the respective icon to view the Rule Definition options

a Select the **Rule Name** text box to enter a new rule name.

b Select the **Action** drop down icon and then a Fault Action.

c Select the **Minimum Confidence (40-99%)** slider bar to adjust the minimum confidence.

Note: For Loud Abnormal Sound, confidence is set at 99% and cannot be changed.

- End -

Illustra 5MP LPR Camera License Plate Recognition

Illustra LPR analytics is designated for lower-to-moderate speed parking access and security of parking management projects.

Our analytics can recognize plate numbers and country/state of issue.

Cameras allow you to configure four predefined lists to raise alerts, each with a unique Event Action association (e.g.[Allow] can trigger the I/O to open the parking gate).

For more setup information and illustrations regarding license plate recognition please see the License Plate Recognition Best Practice Guide at https://illustracameras.com/

License Plate Recognition Best Practices

Physical Installation; For optimal performance and accurate results using Illustra LPR, capturing appropriate and suitable images of license plates for recognition is important. When using Illustra LPR, consider the following best practices:

- Use a camera dedicated to the purpose of LPR. If an overview of the area/vehicle is desired, use a second camera (without LPR) for that purpose.
- Use a zoom position that delivers a field of view not more than 6 ft to 8 ft wide to capture the plate.
- Mount the camera 15 ft to 50 ft away from the vehicle/plate.
- Mount the camera 3 ft to 15 ft high, with no more than a 30-degree vertical angle to the vehicle/plate, ideally above the height of vehicle headlights.
- Position the camera with no more than a 15-degree horizontal angle off center.
- Ensure that the license plate is between 25 pixels and 60 pixels in height & that the stroke width of the letters and numbers in the license plate is at least 4 pixels. Use Stream 1 (2560x1440) for this measurement.
- Mount and rotate the camera so that a horizontal line can be drawn which crosses both the left edge and right edge of the license plate.
- Position the camera to avoid any undesired objects in the image that could obscure the license plate.
- Position the camera so that the plate appears in the centre of the image. Plates close to the edge of the image may not be recognized.
- Position the camera away from direct sunlight to avoid obscuring the license plate.
- Position the camera so that the license plate will not reflect direct sunlight back at the camera, as this could obscure the plate.
- At the point where the license plate can be recognised (between 25 pixels and 60 pixels), ensure the camera is not positioned directly in line with the vehicle headlights, as this can cause the field of view to be whited out. Position the camera so that the lights are not shining directly into the camera.
- If Day-time light level is below 500 Lux, it is recommended that supplemental lighting be used.
- If night-time operation is required, the use of an external IR illuminator or white light source is highly recommended. This device should be located at least 20-degree angle from the camera location, and such that the IR is not reflected directly towards the camera, or create any shadowing on the plate.
- If coverage of multiple lanes is required, deploy additional Illustra LPR cameras for each lane.
- As environmental conditions (snow, rain, fog, etc.) can have a negative impact on LPR performance; please consider methods to mitigate, such as Weather Hoods.

Camera Configuration

- If deploying for 'Free Flow' applications; to minimize motion blur, ensure you have selected one of the LPR mode settings, or manually select an appropriate shutter speed, 1/500 sec or faster is preferred.
- Note that higher shutter speeds will reduce the performance in low light scenarios. For deployments with slower moving vehicles the use can lower the shutter speed to increase recognition time & low light performance.
- If deploying for 'Stop & Go' style applications, shutter speeds as low as 1/120 sec can be selected.
- Ensure that the camera is focused at a point which is central to depth of the region in which you plan to recognize plates.
- If the image exposure is being negatively affected by external lighting (e.g. car headlights), adjusting the 'Exposure Method' to a region (e.g. Spot) that is not affected by the lighting is recommended.

Recommended Settings:

1 TrueWDR: Disabled (Default).

2 SmartWDR: Disabled

3 Smart Defog: Disabled.

4 Flickerless Mode: Disabled (Default)

5 Day-Night Mode: Auto Mid (Default)

6 Max Gain: 51db (Default)

Procedure 130 Enabling License Plate Recognition

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Event and Actions**.
2	Select **Analytics** and then select the **License Plate Recognition** tab.
3	Select the **Enable License Plate Recognition** check box to enable License Plate Recogntion.
4	Select the **Highlights Detections** check box to enable the detection GUI overlay.
5	Select the **Exposure Profile** drop-down list. **Note:**The LRP camera is automatically defaulted to the recommended LPR medium profile, with selected option and dropdown being a mirror of the Exposure Profile under Picture setting.
6	Select the **Region** drop-down list and select one of the following regions: • **North America** • **Europe**
7	Select the **Country** drop-down list and then select a country from the list. • **United States:** Available when the Region is set to North America in step 6. • **Canada:** Available when the Region is set to North America in step 6.

- One of the 44 European countries below when the Region is set to Europe in step 6. **Generic European, Albania, Andorra, Austria, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Faroe Islands, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Kosovo, Latvia, Lichtenstein, Lithuania, Luxembourg, Macedonia, Malta, Moldova, Monaco, Montenegro, Netherlands, Norway, Poland, Romania, Portugal, Serbia, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Ukraine, United Kingdom**.

Note: Step 8 is only available when you select North America is step 6.

8 Select the **State / Province** drop-down list and then select one of the following Canadian provinces or United States states:

- Canada (14): **Generic Canadian, Alberta, British Columbia, Manitoba, Ontario, Quebec, New Brunswick, Newfoundland, Nova Scotia, Northwest Territories, Nunavut, Prince Edward Island, Saskatchewan, Yukon.**.
- United States (53): **Generic American, Alabama, Alaska, Arizona, Arkansas, California, Colorado,Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, Wyoming, Washington DC, US Government**

9 The above procedure will allow EDGE continuous metadata creation for VMS integration only - for camera based Event alarms continue with follow up procedure.

- End -

Procedure 131 Enabling and configuring camera License Plate Recognition events

Step	Action
1	Repeat all steps in procedure 117.
2	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Event and Actions**.
3	Select **Analytics** and then select the **License Plate Recognition** tab.
4	Under the **Recognition Configuration** heading, select from the following options: • **Allow:** To enable the "Allow" list rule and linked eventing. • **Deny:** To disable the "Allow" list rule and linked eventing. • **Custom 1:** To enable the "Custom 1" list rule and linked eventing. • **Custom 2:** To enable the "Custom 2" list rule and linked eventing.

5 Under the **Recognition Configuration** heading, select the  icon for the configuration of each list Detection rule and event linkage.

6 Select the **Field** drop-down list and select an option from the list.

7 Adjust the **Minimum Confidence (40-99%)** slider bar to your desired level.

8 Select the **Action** drop-down list and select an event fault action from the list.

9 You can now highlight a specifc area on the camera pane by drawing a highlighted area of interest on the camera pane.

a Under the **Draw Style** heading select one of the three available styles.

b Under the **Draw Mode** heading select the pencil icon to free draw a shape on the camera pane.

a Move your computer mouse next to the area on the camera pane that you want to highlight, click and hold down the button on your mouse and then move the mouse to fully cover the area on the camera pane. Release the button on your mouse to insert the new highlighted zone on camera pane.

Note: To remove all highlighted zones, select the highlighted zone on the camera pane and then select the rubber icon.

10 Select the **Save** button to save all settings.

11 Select the **Browse** button and navigate to the file that you want to upload.

12 Select the **Upload** button to upload CSV file.

Note: When fully uploaded, the CSV file can be downloaded by selecting the **Download** button for additional editing or the CSV file can be overwritten by a new file upload.

- End -

Procedure 132 Disabling License Plate Recognition

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Event and Actions**.
2	Select **Analytics** and then select the **License Plate Recognition** tab.
3	Select the **Enable License Plate Recognition** check box to disable License Plate Recogntion.

- End -

Procedure 133 Editing a configured License Plate Recognition list

Step	Action
1	Repeat all steps in procedures 117 and 118.
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Event and Actions**.
2	Select **Analytics** and then select the **License Plate Recognition** tab.

3 Under the **Recognition Configuration** heading, select the icon for the configuration of each list Detection rule and event linkage.

4 Select the **Field** drop-down list and select an option from the list.

5 Adjust the **Minimum Confidence (40-99%)** slider bar to your desired level.

6 Select the **Action** drop-down list and select an event fault action from the list.

7 You can now highlight a specifc area on the camera pane by drawing a highlighted area of interest on the camera pane.

a Under the **Draw Style** heading select one of the three available styles.

b Under the **Draw Mode** heading select the pencil icon to free draw a shape on the camera pane.

a Move your computer mouse next to the area on the camera pane that you want to highlight, click and hold down the button on your mouse and then move the mouse to fully cover the area on the camera pane. Release the button on your mouse to insert the new highlighted zone on camera pane.

Note: To remove all highlighted zones, select the highlighted zone on the camera pane and then select the rubber icon.

8 Select the **Save** button to save all settings.

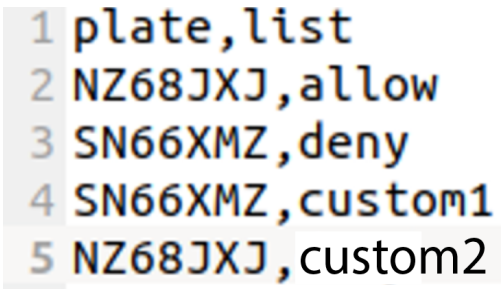
- End -

Procedure 134 Uploading a License Plate list

Plate list configuration lets the user upload a file which includes number plates and associated list in order to generate camera alarms and Actions.

When first configuring, the Download icon enables the user to download a template to populate. Once a new file is uploaded it can always be downloaded for editing or replaced with a new file upload. Please take note of CSV format below, noting that “plate,list“ cannot be edited/changed as this will corrupt the functionality of the list.

Figure 63 CSV Format



Step	Action

1 Repeat **all** steps in Procedures 117, 118 and 120.

2 Select **Setup** on the Web User Interface banner to display the setup menus and then select **Event and Actions**.

3 Select **Analytics** and then select the **License Plate Recognition** tab.

4 Select the **Browse** button and navigate to the file that you want to upload.

5 Select the **Upload** button to upload CSV file.

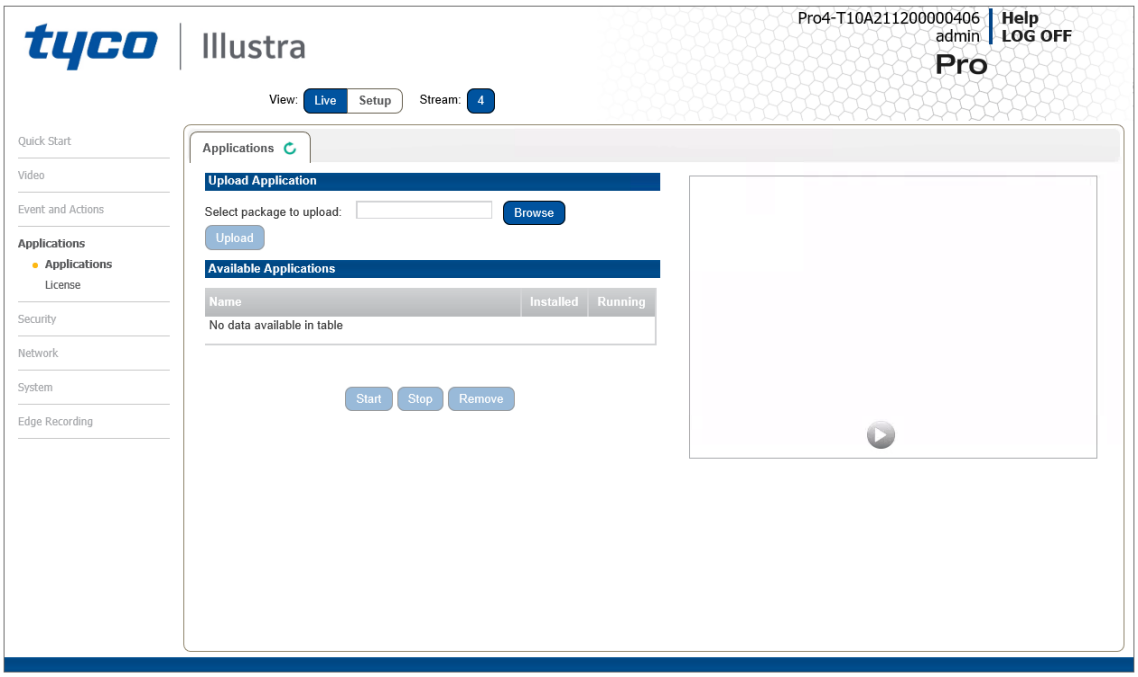
Note: When fully uploaded, the CSV file can be downloaded by selecting the **Download** button for additional editing or the CSV file can be overwritten by a new file upload.

- End -

Applications

When you select the Applications menu the Applications page displays, as seen in on page 140.

Figure 64 Applications Menu



Applications support allow for the upload of binary files that add custom functionality and value to the camera. Applications are uploaded through the Web User Interface.

These applications are licensed by Tyco Security Products using a licensing facility.

Note: This application is not available on the LPR cameras.

Applications

Procedure 135 Upload an Application

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Applications** to view the Applications tab.
2	Select **Browse**. The Choose file dialog is displayed.
3	Navigate to the location where the application has been saved.
4	Select the application file then select the **Open** button.
5	Select **Upload**. The upload process begins.

- End -

Available Applications

A list of applications currently installed and running are displayed. Each can be started, stopped and removed.

Procedure 136 Start, Stop or Remove an Application

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Applications** to view the Applications tab.
2	Select the corresponding **Application** checkbox to Start, Stop or Remove.
3	Select one of the following options: a **Start** to start the application running. b **Stop** to stop the application running. c **Remove** to remove the application.

- End -

License

License files for applications are uploaded using the licensing webpage. Available licenses are listed displaying their application ID and their license expiry date.

Procedure 137 Upload a License File

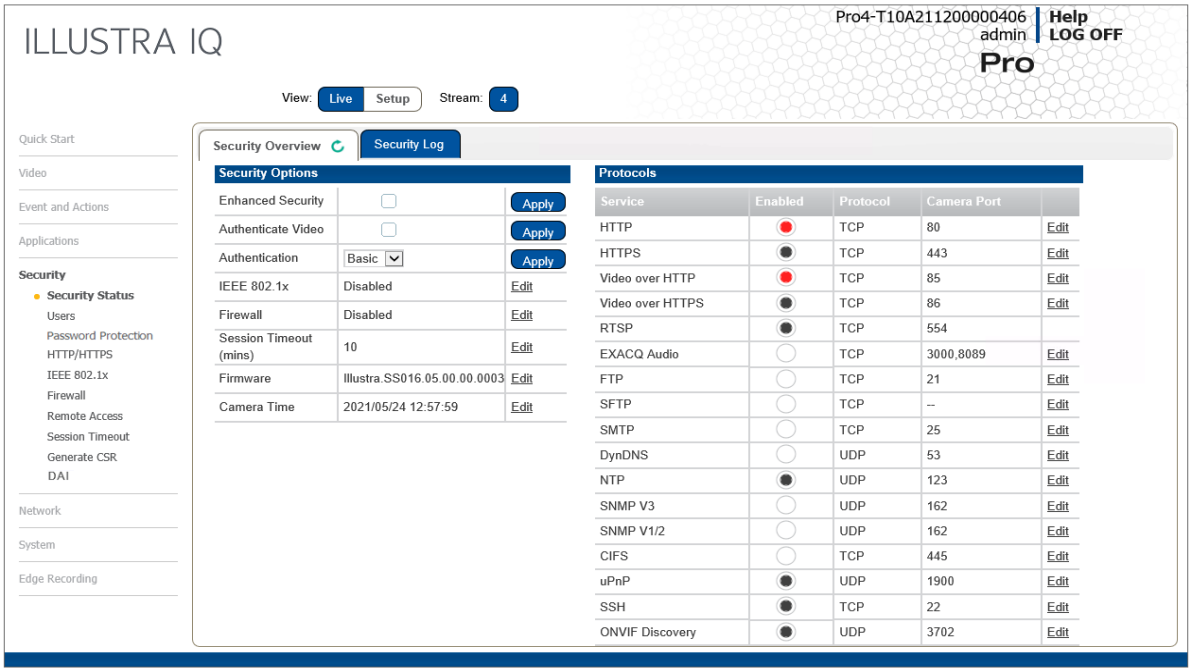
Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Applications.**
2	Select **License** to view the License tab.
3	Select **Browse**. The Choose file dialog is displayed.
4	Navigate to the location where the license file has been saved.
5	Select the license file then select the **Open** button.
6	Select **Upload**. The upload process begins.

- End -

Security

When you select the **Security** menu, the **Security Status** page appears, as seen in Figure 65 on page 142.

Figure 65 Security menu



The Event Menu provides access to the following camera settings and functions:

- Security Status
- Users
- Password Protection
- HTTP/HTTPS
- IEEE 802.1x
- Firewall
- Remote Access
- Session Timeout
- Generate CSR
- DAI

Security Status

This section explains how to configure security features for the camera and modify the communication protocols that are used.

Note: Any changes in the Security section, either changes to the Security Mode or to an individual protocol, are logged in the Security Log.

Enhanced Security

When you first log in to the Web User Interface, an overlay over the Live menu tab appears prompting you to choose either Standard or Enhanced Security mode. For more information regarding the requirements for Enhanced Security mode, refer to Summary of Security Modes on page 63.

Admin users can change the Security Mode of the camera from Standard Security to Enhanced Security.

Procedure 138 Enable Enhanced Security

Step	Action
1	Select **Setup**→ **Security**→ **Security Status**.
2	Select the **Security Overview** tab.
3	Check the **Enable Enhanced Security** check box to enable enhanced security. A prompt appears asking you for your current password and the new password for the Enhanced Security feature. Your password must adhere to the minimum requirements for an Enhanced Security password as seen below. OR Clear the **Enable Enhanced Security** check box to disable enhanced security. Enhanced Security is disabled by default. The Security Warning dialog appears.
4	Enter the current password in the **Current Password** text box.
5	Enter the new password in the **New Password** text box. The password for enhanced security must meet the following requirements: • Be a minimum of eight characters long • Have at least one character from one of the following character groups: Upper-case letters Lower-case letters Numeric characters Special characters
6	Re-enter the new password in the **Confirm Password** text box.
7	Click **Apply**. **Note:**Any changes to the Security Mode are logged in the Security Log.

- End -

Procedure 139 Disable Enhanced Security Mode

Step	Action
1	Select **Setup**→ **Security**→ **Security Status**.
2	Select the **Security Overview** tab.
	Note: When in Enhanced Security mode, changing the security mode requires the admin account password.
3	Click **Apply**.
	Note: Any changes to the Security mode are logged in the Security Log.

- End -

Security Status

This section summarizes the communication protocols that are used and their status. The following communication protocols can be enabled: CIFS, Dyn DNS, EXACQ Audio, FTP, HTTP, HTTPS, NTP, ONVIF Discovery, RTSP, SFTP, SMTP, SNMP V1/2, SNMP V3, SSH, uPNP, Video over HTTP, Video over HTTPS.

Security Overview

Procedure 140 Enable/Disable Communication Protocols

Step	Action
1	Select **Setup**→ **Security**→ **Security Status**.
2	Select the **Security Overview** tab.
3	Select or clear the **Protocols** check box to enable or disable that protocol.
4	Click **Apply** to save your settings.
	Note: When in Enhanced Security, enabling/disabling individual protocols requires the admin account password. Any changes to individual protocol settings are logged in the Security Log.

- End -

Security Log

The security log records any changes made to the security mode or to an individual protocol.

Procedure 141 Display Security Log

Step	Action
1	Select **Setup**→ **Security**→ **Security Status**.
2	Select the **Security Log** tab.
3	Select **Refresh** to refresh the log for the most up-to-date information.

- End -

Procedure 142 Filter the Security Log

Step	Action
1	Select **Setup**→ **Security**→ **Security Status**.
2	Select the **Security Log** tab.
3	Enter the number of lines of the log file you would like to view in the **Lines (from the end of the log file)** text box.
4	Enter the word or phrase that you would like to search for in the **Filter (only lines containing text)** text box.
5	Select **Refresh** to refresh the log for the most up-to-date information that meets the filter parameters.
6	Select **Clear** to empty the log of its current entries. You will be required to enter your password to do this.

- End -

Users

In this section you are able to add a user, change a user password and a delete user account. There are three levels of access: admin, operator and user.

Note: The default Username is **admin** and the default Password is **admin**. To maintain security the password on the admin account should be changed.

View Current User Accounts

View a list of the current user accounts assigned to the camera.

Procedure 143 View User Accounts

Step	Action
1	Select **Setup**→ **Security**→ **Users**. The current user accounts assigned to the camera display.

- End -

Add User

Add a new user account to allow access to the camera.

Procedure 144 Add a User

Step	Action
1	Select **Setup**→ **Security**→ **Users**.
2	Select the **Add User** tab.
3	Enter a User Name in the **Name** text box. The username must start with a letter and can be followed by any alphanumeric values (a-z, A-Z, 0-9) and the following special characters, underscore(_), dash(-), or dot(.)
4	Select a **Role**: • admin • operator • user

5	Enter a password in the **Password** text box.
	The password for Standard Security must start with an alphanumeric character and is case sensitive, it can contain alphanumeric characters with a length of between 5 and 32 characters.
	The password for enhanced security must meet the following requirements:
	• Be a minimum of seven characters long.
	• Have at least one character from at least three of the following character groups:
	  • Upper-case letters
	  • Lower-case letters
	  • Numeric characters
	  • Special characters

6	Enter the same password in the **Confirm Password** text box.
7	Select **Apply** to save the settings. The new user account appears in the Users list on the **Users** tab.
	- End -

Changing the User Accounts Password

Change the password of an existing user account.

Procedure 145 Change User Password

Step	Action
1	Select **Setup**→ **Security**→ **Users**.
2	Select the **Change Password** tab.
3	Select the user account from the **Name** drop-down menu.
4	Enter the current password for the user account in the **Current Password** text box.
5	Enter the new password for the user account in the **New Password** text box. The password is case sensitive and can contain alphanumeric characters with a length of between 5 and 32 characters.
6	Enter the same new password in the **Confirm New Password** text box.
7	Select **Apply** to save the settings.

- End -

Delete a User Account

Delete a user account from the camera.

Note: The default 'admin' account cannot be deleted.

Procedure 146 Delete a User Account

Step	Action
1	Select **Setup**→ **Security**→ **Users**. The Users tab displays.
2	Select  to delete the corresponding user account. You will be prompted to confirm the deletion.
3	Select **OK** to delete. OR
4	Select **Cancel**.

- End -

Password Protection

Users can configure additional rules to protect the camera. Users can also configure the system to track logins, notify admin users of logins, and store the data in Access Logs.

Procedure 147 Configuring Brute Force Protection

Step	Action
1	Select **Setup**→ **Security**→ **Password Protection**.
2	Use the **Max Attempts** slider to select a value from one to 1000. This sets the number of times a user can enter an incorrect password until the user is locked out.

3 Use the **Attempts Expiration Time**slider to select a value from one to 1000. This sets the number of seconds the system retains an incorrect password attempt.

4 Use the **Account Lockout Time** slider to select a value from three to 1000. This sets the number of seconds a user is locked out for.

The default settings for password protection are as follows:

- Enable password protection: **On**
- Max attempts: **5**
- Attempt expiry time: **60 seconds**
- Account lockout time: **60 seconds**

- End -

Procedure 148 Configuring GUI login notification

Step	Action

1 Select **Setup**→ **Security**→ **Password Protection**.

2 Select the **Notify on new user login** check box to enable the service, and clear the check box to stop the service.

Admin users see a GUI overlay that informs them when another user logs in and when a log is registered in **System>Logs>Access Logs**.

Note: Service is enabled by default.

- End -

HTTP / HTTPS

User can select the option to use HTTP, HTTPS or both. The camera automatically creates an SSL certificate file to use for HTTPS. It is possible to upload a custom SSL certificate if validation is required.

Procedure 149 Specify HTTP Method

Step	Action
1	Select **Setup**→ **Security**→ **HTTP/HTTPS**.
2	Select the **HTTP Method** using the radio buttons • **HTTP** • **HTTPS** • **Both**

- End -

Procedure 150 Add a HTTPS Certificate

Step	Action
1	Select **Setup**→ **Security**→ **HTTP/HTTPS**.
2	Click on the **Upload** button and navigate to the certificate location.
3	Select the file and select **Open**.

Note: The camera only accepts .pem format certificates. The certificate must have the server certificate and private key combined and the private key must not be password protected.

After the certificate has been uploaded the camera must be rebooted to take affect.

- End -

Delete a HTTPS Certificate

If you delete the existing certificate it will be replaced by a temporary substitute. The current browser session will be lost and you will be required to log back in to the camera Web User Interface.

Procedure 151 Delete a HTTPS Certificate

Step	Action
1	Select **Setup**→**Security**→**HTTP/HTTPS**→**Delete**. The camera displays a “Restarting HTTPS Service” page with a progress bar showing the deletion progress.
2	When complete, the camera returns to the log in page.

- End -

IEEE 802.1x

The IEEE 802.1x security feature provides port based network access control i.e. securing corporate networks from the attachment of unauthorized devices.

Authentication is carried out through use of the Extensible Authentication Protocol or EAP. Both PEAP and TLS methods are supported.

Procedure 152 Configure IEEE 802.1x Security

Step	Action
1	Select **Setup→Security→IEEE 802.1x**. The **EAP Settings** tab displays.
2	Select the **Enable IEEE802.1x** check box to enable IEEE802.1x security . OR Clear the **Enable IEEE802.1x** check box to disable IEEE802.1x security.
3	Select the **EAPOL Version** from the drop-down menu.
4	Select the **EAP Method** using the radio buttons.
5	Enter the EAP identity name in the **EAP Identify** textbox.
6	Select **Upload** to navigate to the **CA Certificate** location.The Choose file dialog displays.
7	Navigate to the location where the certificate has been saved. Select the file and select **Open**.
8	Select **Upload**. The upload process starts.
9	If **PEAP** is selected: a Enter the required PEAP **Password.** OR If **TLS** is selected - a Select **Upload** to navigate to the **Client Certificate** location. The Choose file dialog will be displayed. b Navigate to the location where the certificate has been saved. c Select the file and select **Open**. d Select **Upload**. The upload process starts. e Enter the required **Private Key Password**.
	- End -

Firewall

Configure the Basic Filtering and Address Filtering for the firewall.

Basic Filtering

Enable or disable basic filtering for the camera this includes:

- ICMP (Internet Control Message Protocol) Blocking
- RP (Reverse Path) Filtering
- SYN Cookie Verification.

Procedure 153 Enable/Disable Basic Filtering

Step	Action
1	Select **Setup→Security→Firewall**. The **Basic Filtering** tab displays.
2	Select the **ICMP Blocking** check box to enable ICMP blocking. OR Clear the **ICMP Blocking** check box to disable ICMP blocking. The default setting is 'Disabled'.
3	Select the **RP Filtering** check box to enable the RP filtering. OR Deselect the **RP Filtering** check box to disable. The default setting is 'Disabled'.
4	Select **SYN Cookie Certification** check box to enable SYN cookie certification. OR Deselect the **SYN Cookie Certification** check box to disable. The default setting is 'Disabled'.

- End -

Address Filtering

Configure the IP or MAC addresses which are denied access to the camera.

Procedure 154 Enable/Disable and configure Address Filtering

Step	Action
1	Select **Setup→Security→Firewall**.
2	Select the **Address Filtering** tab.
3	Select **Off** to disable address filtering completely. OR Select **Allow** to allow address filtering for specified addresses OR Select **Deny** to deny address filtering for specific addresses. The default setting is 'Off'.
4	If address filtering has been set to **Allow** or **Deny**:

a Enter an IP or MAC Address to allow / deny in the **IP or MAC Address** text box in the following format xxx.xxx.xxx.xxx.

Note:CIDR (Classless Inter-Domain Routing) is supported when using address filtering. If using a CIDR address use the following format xxx.xxx.xxx.xxx/xx.

b Select **Add**.

5 Select **Apply** to save the settings.

- End -

Editing an Address Filter

Edit an existing address filter.

Procedure 155 Edit an Address Filter

Step	Action
1	Select **Setup**→ **Security**→**Firewall**.
2	Select the **Address Filtering** tab.
3	Edit the IP or MAC Address in the **IP or MAC Address** text box.
4	Select **Add** to save the changes.

- End -

Deleting an Address Filter

Delete an existing address filter.

Procedure 156 Delete an Address Filter

Step	Action
1	Select **Setup**→ **Security**→**Firewall**.
2	Select the **Address Filtering** tab.
3	Select to  delete the corresponding address filter.

- End -

Remote Access

SSH Enable

Enables Secure Shell access into the camera, if remote access is permitted by the camera network. This will also enable Tyco Security Products Level 3 Technical Support to diagnose any problems on the camera.

Note: It is recommended to keep SSH Enable disabled. This function should only be enabled this when it is requested by Tyco Security Products Level 3 Technical Support.

Procedure 157 Configure SSH

Step	Action
1	Select **Setup**→ **Security**→**Remote Access**.
	The **Remote Access** tab displays.
2	Select the **SSH Enable** check box to enable SSH.
	OR
	Deselect **SSH Enable** check box to disable SSH.
	The default setting is 'Disabled'.

- End -

ONVIF

The Web User Interface allows ONVIF functionality to be managed at a high level. ONVIF Discovery Mode and User Authentication can be enabled or disabled.

- ONVIF Discovery Mode allows enabling or disabling discovery of the camera via ONVIF.
- ONVIF User Authentication allows the camera to accept ONVIF commands from all users or only authenticated users. Enabling User Authentication ensures the camera will only execute commands from authenticated users.

The separation of Discovery Mode and User Authentication allows the camera to be set up in a configuration that suits requirements for the network and users. The preferred discovery method for the camera is Illustra Connect, and this utilizes ONVIF discovery. It is therefore recommended that ONVIF Discovery Mode is always enabled.

ONVIF Discovery Mode

Enable or disable ONVIF discovery on the camera.

Procedure 158 Enable/Disable ONVIF Discovery Mode

Step	Action
1	Select **Setup**→ **Security**→**Remote Access**.
	The **Remote Access** tab displays.
2	Select the **ONVIF Discovery Mode** check box to enable ONVIF Discovery Mode.
	OR
	Deselect **ONVIF Discovery Mode** check box to disable ONVIF Discovery Mode.

The default setting is ‘Enabled’.

- End -

ONVIF User Authentication

To utilize ONVIF User Authentication, there must be at least one admin level user in the ONVIF service.

Note: When in Enhanced Security mode, editing ONVIF User Authentication requires the admin account password.

Procedure 159 Enable/Disable ONVIF User Authentication

Step	Action
1	Select **Setup**→ **Security**→**Remote Access**. The **Remote Access** tab displays.
2	Select the **ONVIF User Authentication** check box to enable ONVIF User Authentication. OR Deselect **ONVIF User Authentication** check box to disable ONVIF User Authentication. The default setting is ‘Enabled’.

- End -

Video over HTTP

Enable or disable video or steam metadata over HTTP on the camera.

Procedure 160 Enable/Disable Video over HTTP

Step	Action
1	Select **Setup**→ **Security**→**Remote Access**. The **Remote Access** tab displays.
2	Select the **Video over HTTP** check box to enable Video over HTTP. OR Deselect **Video over HTTP** check box to disable Video over HTTP. The default setting is ‘Enabled’.

- End -

Video over HTTPS

Enable or disable video or steam metadata over HTTPS on the camera.

Procedure 161 Enable/Disable Video over HTTPS

Step	Action
1	Select **Setup**→ **Security**→**Remote Access**. The **Remote Access** tab displays.
2	Select the **Video over HTTPS** check box to enable Video over HTTPS. OR Deselect **Video over HTTPS** check box to disable Video over HTTPS. The default setting is 'Enabled'.
	- End -

UPnP Discovery

Enable or disable UPnP Discovery on the camera.

Procedure 162 Enable/Disable UPnP Discovery

Step	Action
1	Select **Setup**→ **Security**→**Remote Access**. The **Remote Access** tab displays.
2	Select the **UPnP Discovery** check box to enable UPnP Discovery. OR Deselect **UPnP Discovery**check box to disable UPnP Discovery. The default setting is 'Enabled'.
	- End -

ExacqVision Server Audio

Enable or disable audio ports used for ExacqVision bidirectional audio integration.

Procedure 163 Enable/Disable EXACQ Audio

Step	Action
1	Select **Setup**→ **Security**→**Remote Access**. The **Remote Access** tab displays.
2	Select the **EXACQ Audio** check box to enable EXACQ Audio. OR Deselect **EXACQ Audio** check box to disable EXACQ Audio. The default setting is 'Enabled'.
	- End -

Session Timeout

Session timeout specifies the number of minutes that a web session can remain idle before it is automatically terminated.

Procedure 164 Set a Session Timeout time

Step	Action
1	Select **Setup→Security→Session Timeout**.
2	The **Session Timeout** tab displays.
3	Use the slider bar to select the **Session Timeout (mins)**. The default setting is 15 minutes.

- End -

Generate CSR

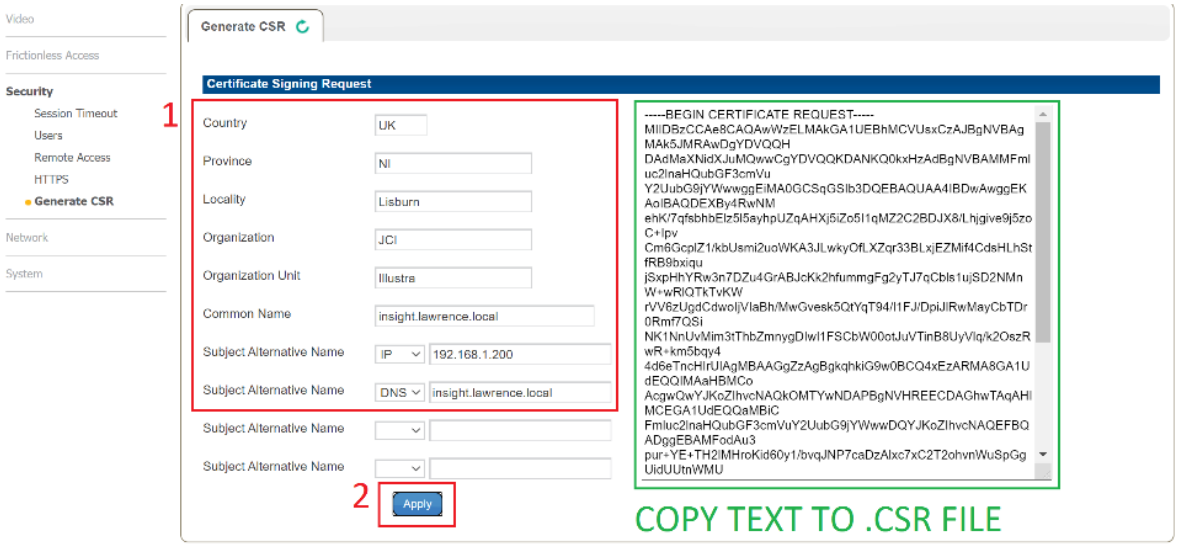
When accessing a camera web GUI via HTTPS, the browser shows an insecure / not secure browser warning. This warning is due to the camera having a 'self-signed certificate'; which offers communication encryption but cannot be used for authentication. Introduction of the Certificate Signing Request (CSR) feature, which allows the user to generate a certificate signing request that can be used by a certificate authority to create an SSL certificate specifically for the individual camera.

Note:SSL certificates can only be used for a single device.

Procedure 165 Generate a .csr file

Step	Action
1	Select **Setup→Security→Generate CSR**.
2	Enter information into the Request form and select Apply, Items 1 & 2 in Figure 66 on Page 158.

Figure 66 .CSR file tab



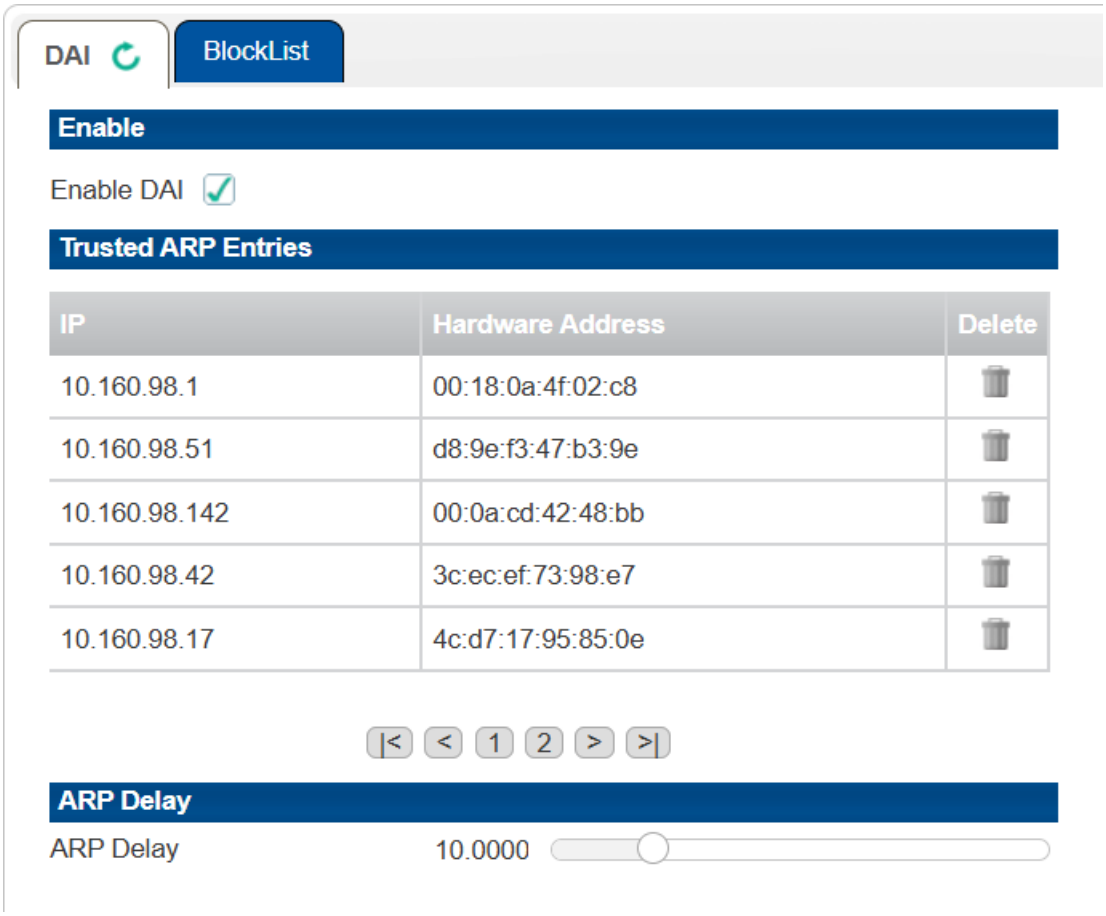
3 Copy the text shown in Green above & paste into a text file with .csr file extension.

- End -

DAI

Dynamic ARP Inspection (DAI) helps prevent Distributed Denial of Service (DDoS) and Man-in-the-Middle (MITM) attacks.

Figure 67 DAI tab



Procedure 166 View current and recent connections to the camera

Step	Action
1	Select **Setup→Security→DAI**.
2	Select the **DAI**tab.
3	Check **Enable DAI**.
4	View the IP address and MAC address of all current and recent connections to the camera.

- End -

Procedure 167 Change the ARP delay

This feature helps to prevent DDOS attacks.

Step	Action
1	Select **Setup→Security→DAI**.
2	Select the **DAI**tab.
3	Use the slider bar to set the number of messages per second that the camera can receive. • Default: 10 messages per second

- Range: 5 — 30 messages per second

- End -

Procedure 168 Add or remove addresses from the blocklist

Duplicate MAC and IP addresses are a primary indicator of a MITM attack. If two or more duplicate IP or MAC addresses are connected to the camera the most recently connected device's MAC will be blocked and a pop-up window shows on the camera. An IP or MAC address which is on the blocklist cannot access the camera. A blocked MAC can be removed from the blocklist.

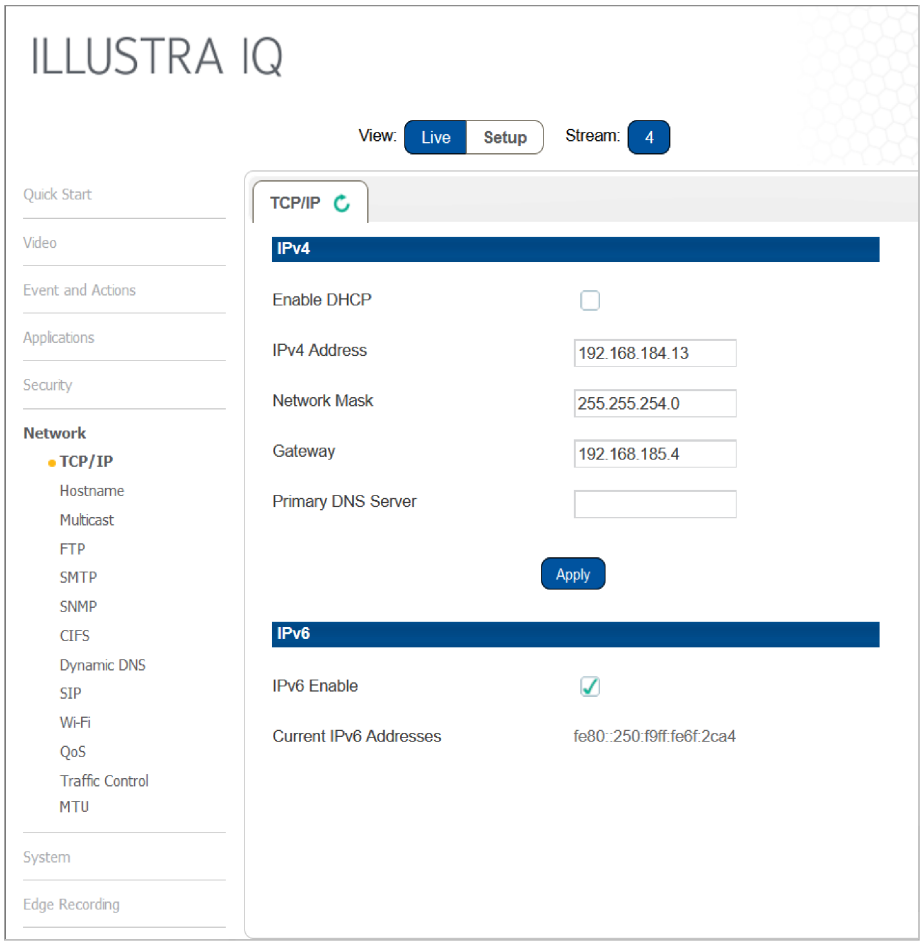
Step	Action
1	Select **Setup**→**Security**→**DAI**.
2	Select the **Blocklist** tab.
3	Add and remove IP and MAC addresses as necessary.

- End -

Network Menu

When you select the **Network** menu, the **TCP/IP** page displays, as seen in Figure 68 on page 161.

Figure 68 Network Menu



The Network Menu provides access to the following camera settings and functions:

- TCP/IP
- Hostname
- Multicast
- FTP
- SMTP
- SNMP
- CIFS
- Dynamic DNS
- SIP
- Wi-Fi
- QoS

- Traffic Control
- MTU

TCP/IP

Configure the IPv4 and IPv6 settings on the camera.

IPv4

Configure the IPv4 settings for the camera.

Note: When you perform a factory reset or reboot the unit searches for the last known IP address. If this is not available it reverts to the default IP address of 192.168.1.168. This could result duplicate IP addresses. Refer to Network Menu on page 161 for more information.

Procedure 169 Configure the IPv4 Settings

Step	Action
1	Select **Setup→Network→TCP/IP**.
2	Select the **Enable DHCP** check box to enable DHCP and disable manual settings. OR Deselect **Enable DHCP** to disable DHCP and allow manual settings to be entered. The default setting is 'Disabled'.
3	If Enable DHCP has been disabled: a Enter the **IPv4 Address** in the IPv4 Address text box in the form xxx.xxx.xxx.xxx. The default setting is '192.168.1.168' b Enter the **Network Mask** in the Network Mask text box xxx.xxx.xxx.xxx. The default setting is '255.255.255.0' c Enter the **Gateway** IP address in Gateway text box xxx.xxx.xxx.xxx. d Enter the **Primary DNS Server** in the Primary DNS Server text box xxx.xxx.xxx.xxx. e Enter the **Secondary DNS Server** in the Secondary DNS Server text box xxx.xxx.xxx.xxx.
4	Select **Apply** to save the settings.
	- End -

IPv6

Enable IPv6 on the camera.

Procedure 170 Enable/Disable IPv6

Step	Action
1	Select **Setup→Network→TCP/IP**.
2	Select the **IPv6 Enable** check box to enable IPv6 on the camera. OR Deselect the **IPv6 Enable** check box to disable IPv6 on the camera.

The default setting is ‘Enabled’.

If IPv6 is enabled the Link Local and DHCP address displays beside ‘Current IPv6 Addresses’ if available.

- End -

Hostname

The hostname is a device's name on a network and is used to distinguish devices from each other. You can use the hostname to find a camera and exchange data. Hostnames are used on the internet as part of the fully qualified domain name (FQDN).

Procedure 171 Change the Hostname Value

Step	Action
1	Select **Setup→Network→Hostmane**.
2	In the **Hostname** text box, enter the new hostname, then click **OK**.
3	Accept the prompt to reboot the camera.

When the reboot is complete, the change propagates to the network devices and DHCP server and the camera's FQDN appears on the network.

- End -

Multicast

Multicast streaming is a one-to-many relationship between a camera and the clients receiving the stream. With a multicast stream, the server streams to a multicast IP address on the network, and clients receive the stream by subscribing to the IP address.

Procedure 172 Configure Multicast Streaming

Step	Action
1	Select **Setup→Network→Multicast**.
2	Select the **Stream Number** from the drop-down list you want to configure.

3	In the **Video Address** field, enter a valid IP address for the Multicast broadcasting. The valid range for the IP address is:
	`224.xxx.xxx.xxx`
	`232.xxx.xxx.xxx`
	`234.xxx.xxx.xxx`
	`239.xxx.xxx.xxx`

Multicast stream addresses must be unique to the stream and cameras.

4	In the **Port** field, enter a port for the Multicast broadcasting. The Multicast stream port must be unique to stream cameras. The approved port range is: 0-65535.
5	In the **Time to live** field, enter a value.

Example of correct Multicast configuration:

```
Stream.1.Multicast.IPAddress=224.16.18.2
Stream.1.Multicast.Port=1032
Stream.2.Multicast.IPAddress=224.16.18.2
Stream.2.Multicast.Port=1030
Stream.3.Multicast.IPAddress=0.0.0.0
Stream.3.Multicast.Port=0
```

- End -

FTP

Configure the FTP settings for the FTP server. This is required to send video files from triggered analytic alerts. FTP must be configured to enable FTP video alerts when using analytics.

Note:FTP settings can also be configured in the **Network** menu.

Procedure 173 Configure FTP Server Settings

Step	Action
1	Select **Setup→Network→FTP**.
2	Select the **Enable** check box to enable FTP. OR Deselect the **Enable** check box to disable FTP. The default setting is 'Enabled'. **Note:**When in Enhanced Security mode, enabling FTP requires the admin account password.
3	If required, select the **Secure FTP** checkbox. The default setting is 'Disabled'.
4	Enter the IP address of the FTP Server in the **FTP Server** text box.
5	Enter the FTP port in the **FTP Port** text box. The default setting is 21.
6	Enter the FTP username in the **Username** text box.
7	Enter the FTP password in the **Password** text box.
8	Enter the FTP upload path in the **Upload Path** text box. **Note:**When entering the upload path the following format should be used '//<name of ftp directory>/<folder>'

- End -

File Transfer Rate

You can limit the File Transfer Rate and assign a max transfer rate assigned to manage the amount of FTP bandwidth used.

Procedure 174 Configure the FTP Transfer Rate

Step	Action
1	Select **Setup→ Network→FTP**.
2	Select the **FTP** tab.
3	Select the **Limit Transfer Rate** check box to limit the FTP transfer rate. OR Clear the **Limit Transfer Rate** check box to disable limited FTP transfer. The default setting is 'Enabled'.
4	Enter the Max Transfer Rate in the **Max Transfer Rate** (Kbps) textbox. The default setting is 50.

- End -

Test FTP Settings

Test the FTP settings that have been configured correctly.

Procedure 175 Test the FTP Settings

Step	Action
1	Select **Setup→ Network→FTP**.
2	Select the **FTP** tab.
3	Select **Test**. A sample text file will be sent to the specified FTP destination to confirm that FTP settings are correct.

- End -

SMTP

Configure the SMTP settings to allow e-mail alerts to be sent from the camera when an analytic alert is triggered.

Note:SMTP settings must be configured to enable email alerts when using analytics.

Procedure 176 Configure SMTP Settings

Step	Action
1	Select **Setup→ Network→SMTP**.
2	Check the **Enable SMTP** check box to enable SMTP. Text boxes on the tab become available for entry. **Note:**When in Enhanced Security mode, enabling SMTP requires the admin account password.
3	Enter the IP Address of the mail server in the **Mail Server** text box.
4	Enter the server port in the **Server Port** text box. The default setting is '25'.
5	Enter the from email address in the **From Address** text box.
6	Enter the email address to send email alerts to in the **Send Email to** text box.
7	Select the **Use authentication to log on to server** check box to allow authentication details to be entered. OR Clear the **Use authentication to log on to server** to disable authentication. The default setting is 'Disabled'.
8	If 'Use authentication to log on to server' check box has been selected: a Enter the username for the SMTP account in the **Username** text box. b Enter the password for the SMTP account in the **Password** text box.
9	Select **Apply** to save the settings.

- End -

SNMP

The camera introduces support for the Simple Network Management Protocol making it easier to manage on an IP network.

The SNMP support includes support for V2 and V3. Using V2 means no authentication is required to access the data and results are unencrypted. V3 offers enhanced encryption and authentication security features.

Procedure 177 Configure SNMP Settings

Step	Action
1	Select **Setup→ Network→SNMP**.
2	Enter a location reference in the **Location** text box.
3	Enter an SNMP managing contact reference in the **Contact** text box.
4	If using **V2**: a Select the **Enable V2** checkbox. b Enter the authorized ID for reading SNMP data in the **Read Community** text box. c Enter the **Trap Community**. d Enter the **Trap Address**. e Select **Apply**. OR If using **V3**: a Select the **Enable V3** checkbox. b Enter the **Read User**. c Select the **Security Level** from the drop down menu: **noauth:** No authentication / no encryption. **auth:** Authentication / no encryption. A user password is required. It is symmetrically encrypted using either MD5 or SHA. **priv**: Authentication / encryption. A user password is required as is symmetrically encrypted using either MD5 or SHA. A data encryption password is required as is symmetrically encrypted using either DES or AES. d Select the **Authentication Type** using the radio buttons. e Enter the Authentication Password f Select the **EncryptionType** using the radio buttons. g Enter the **Encryption** Password h Select **Apply**.

- End -

Heartbeat

Procedure 178 Enable/Disable Heartbeat

Step	Action

1 Select **Setup→ Network→SNMP→Heartbeat**.

2 Select the **Heartbeat** tab.

3 Select the **Enable Heartbeat** check box to enable Heartbeat.

OR

Deselect the **Enable Heartbeat** check box to disable Heartbeat.

The default setting is 'Disabled'.

- End -

Procedure 179 Enable select Heartbeat intervals

Step	Action
1	Select **Setup→ Network→SNMP→Heartbeat**.
2	Select the **Heartbeat** tab.
3	Select the **Enable Heartbeat** check box to enable Heartbeat.
4	Use the slider bar to select the **Heartbeat Interval (secs)**.
5	The default setting is '60' seconds. The seconds range from 5 to 500.

- End -

CIFS

The CIFS feature permits files generated from the camera such as alarm related video to be directed to network attached file storage via the Common Internet File System protocol. This supplements existing distribution methods such as FTP, SFTP and email.

Procedure 180 Configure CIFS Server Settings

Step	Action
1	Select **Setup→Network→CIFS**.
2	Select the **Enable** check box to enable CIFS. OR Deselect the **Enable** check box to disable CIFS. The default setting is 'Disabled'. **Note:**When in Enhanced Security mode, enabling CIFS requires the admin account password.
3	Enter the network path in the **Network Path** text box. **Note:**When entering the network path the following format should be used '//<IP Address>/<folder name>'
4	Enter the domain name in the **Domain Name** in the text box.
5	Enter the username in the **Username** text box.
6	Enter the password in the **Password** text box.

- End -

Test CIFS Settings

Test that the CIFS settings are configured correctly.

Procedure 181 Test the CIFS Settings

Step	Action
1	Select **Setup→Network→CIFS**.
2	Select the **CIFS** tab.
3	Select **Test**. A sample text file is sent to the specified CIFS destination to confirm that CIFS settings are correct.

- End -

Dynamic DNS

Dynamic DNS is supported for updating, in real time a changing IP address on the Internet to provide a persistent domain name for a resource that may change location on the network. RFC 2136 Dynamic Updates in the Domain Name System. In this situation the camera talks only to the DHCP server and the DHCP server is responsible for updating the DNS server. The camera sends its hostname to the DHCP server when requesting a new lease and the DHCP server updates the DNS records accordingly. This is suitable for an intranet style configuration where there is an internal DHCP and DNS service and the user wants only to access their camera within their own network.

By default, when making a DHCP request the camera transmits its hostname as part of the DHCP request. This option is not user configurable. The camera's hostname matches the configurable parameter "camera name" on the Web User Interface. Any DHCP request contains the camera's

hostname for use of the DHCP server to forward to an appropriate DNS server.

Dynamic DNS

Configure the Dynamic DNS settings for the camera.

Procedure 182 Configure Dynamic DNS

Step	Action
1	Select **Setup→ Network→Dynamic DNS**.
2	Select the **Service Enable** check box to enable Dynamic DNS. OR Deselect **Service Enable** check box to disable Dynamic DNS. The default setting is 'Disabled'.
3	If Service Enable has been enabled: a Enter the Camera Alias in the text box. b Select a Service Provider from the drop-down list: • **dyndns.org** • **easydns.com** • **no-ip.com** • **zerigo.com** • **dynsip.org** • **tzo.com** c Enter a **Username** in the text box. d Enter a **Password** in the text box. e Enter **Service Data** in the text box.
4	Select **Apply** to save the settings.

- End -

SIP

The Session Initiation Protocol (SIP) feature enables the camera to be configured as a SIP User Agent that can register with a SIP server to make and receive audio calls to another SIP device, for example, a SIP IP phone or softphone. The camera can operate as a SIP phone if it is equipped with an external microphone and speaker. The camera can also be configured to monitor the audio from a SIP call and make this available as an RTSP/RTP stream.

Note: Only the SIP incoming audio is recorded in the RTSP stream.

Note: Cameras that do not support audio will not offer SIP configuration.

Procedure 183 Enable/Disable SIP

Step	Action

1 Select **Setup→Network→SIP**.

2 Check the **Enabled** check box to enable SIP

OR

Clear the **Enabled** check box to disable SIP.

The default setting is 'Disabled'.

3 Click **Apply** to save your settings.

Note: After you enable SIP, the camera reboots automatically.

- End -

Procedure 184 Configure the SIP Server Settings

Step	Action

1 Select **Setup→Network→SIP**.

2 Check the **Enabled** check box to enable SIP.

3 Enter the IP address of the SIP Server in the **Domain** text box.

4 Enter the SIP account username in the **Username** text box.

5 Enter the SIP account password in the **Password** text box.

6 From the **Audio Source** dropdown menu, select the Audio Source for calls:

- **Mic** - only external microphones are currently supported.

7 From the **Audio Output** dropdown menu, select an audio output:

- **Speaker -** the SIP call audio is output to the external speaker.
- **Network Stream -** the SIP call audio can be streamed using an RTSP Audio Stream.

8 Click **Apply** to save your settings.

Note: After you enable SIP, the camera reboots automatically.

- End -

Procedure 185 Place a SIP call

Step	Action
1	Select **Setup→Network→SIP**.
2	Enter the SIP Extension number in the **Extension** text box.
3	Click **Dial** to activate the call.
4	Click **Hang up** to end the call.

Note: The Status Log, located below the Dial and Hang up buttons, reports the status of SIP connection and active calls.

- End -

Wi-Fi

The Wi-Fi option allows wireless configuration of the camera at the point of install in conjunction with the Illustra Tools app (Illustra Wi-Fi dongle required).

Note: The Illustra Tools App is available on Android and IOS App stores.

Procedure 186 Enable wireless configuration of the camera

Step	Action
1	Select **Setup→Network→Wi-Fi**.
2	Check the **Enable USB** check box to enable WIFI configuration.

Note: The Illustra Tools app can now connect to the camera using the IP address 10.181.182.1 or by scanning the QR code shown or on the product packaging.

Note:USB will be enabled for 1 hour after the camera is powered from a factory reset. After 1hr, Wi-Fi will be disabled and will require a factory reset to re-enable. Illustra Wi-Fi dongle must inserted in camera for Wi-Fi access.

- End -

QoS

Quality of Service (QoS) is a network capability that allows the prioritisation of different types and sources of network traffic, in relation to throughput, transmission delay and reliability. Traffic packets originating from a source with quality of service will be handled through each hop in the network according to their quality of service value.

In the event of one or more network hops saturating, packets with higher priority will be transmitted in favour of those with lower priority.

For example, if the video stream for a specific camera is of critical priority, it's quality of service setting may be set to 46 (expedited forwarding). This means that if the network hop saturates, other network traffic will be dropped or delayed to ensure that this video traffic is transmitted.

QoS settings require all open stream sessions to be closed, before new settings take effect.

Special values (options in step 3)

- **0 - CS0:** Best effort - lowest priority - first packets to be delayed and dropped when network overloads.
- **46 - EF:** Expedited forwarding - highest priority - low loss & low latency.

Grouped values (options in step 3)

- **AF:** assured forwarding, higher priority than "best effort" but lower than "expedited forwarding". AF1x - IP precedence - Priority AF2x - IP precedence - Immediate AF3x - IP precedence - Flash AFx1 - low drop probability AFx2 - medium drop probability AFx3 - high drop probability
- **CS:** class selector - backward compatible with devices using IP presedence field to mark priority traffic. Higher CS numbers result in higher priority.

Procedure 187 Configuring quality of service settings

Step	Action
1	Select **Setup→Network→QoS**.
2	Select the **Audio** drop-down menu and select one of the following options: • **0 - CS0 (Best Effort)** • **8 - CS1** • **10 - AF11** • **12 - AF11** • **14 - AF13** • **16 - CS2** • **18 - AF21** • **20 - AF22** • **22 - AF23** • **24 - CF3** • **26 - AF31** • **28 - AF32** • **30 - AF33** • **32 - CS2** • **34 - AF41** • **36 - AF42** • **38 - AF43** • **40 - CS5** • **46 - EF (Expedited Forwarding)** • **48 - CS6** • **56 - CS7**
3	Select the **Metadata** drop-down menu and select one of the options.
4	Select the **Video** drop-down menu and select one of the options.

- End -

Traffic control

Traffic control allows throttling and shaping of data transmission from the camera. Rate limiting may be utilised to set a hard limit to the maximum bandwidth sent per second, however, it also adds a smoothing element which operates down to the millisecond.

For example, setting the "Max Rate (kB/S)" to 20000 results in a maximum transmission rate of all data types to 20,000kB/S. It will also shape data so the maximum amount of data sent per second is 20kB. Excess data will be queued up, and transmitted as soon as possible.

Procedure 188 Enabling traffic control

Step	Action
1	Select **Setup→Network→Traffic Control**.
2	Check the **Enable Traffic Control** check box to enable traffic control configuration.
3	Select the **Max Peak Rate (mBit/s)** text box and enter a value.
4	**Status** is a dynamic icon showing the status of the outbound packet buffer. Green indicates that the outbound packet buffer is idle, Amber indicates that it is filling up but not yet full, Red indicates that its completely saturated.

- End -

MTU

Maximum Transmission Unit (MTU) is the maximum size (in bytes) of a packet that a network device can handle in a single transmission. It is a crucial network setting that determines the largest data packet that can be sent without fragmentation (which might affect network performance).

Procedure 189 Configure the MTU settings

Step	Action
1	Select **Setup→Network→MTU**.
2	Use the slider bar to set the MTU. a IPv6 enabled (default configuration) • Default: 1500 bytes • Range: 1250 — 8000 bytes b IPv6 disabled (must be manually disabled on UI) • Default: 1500 bytes • Range: 500 — 8000 bytes

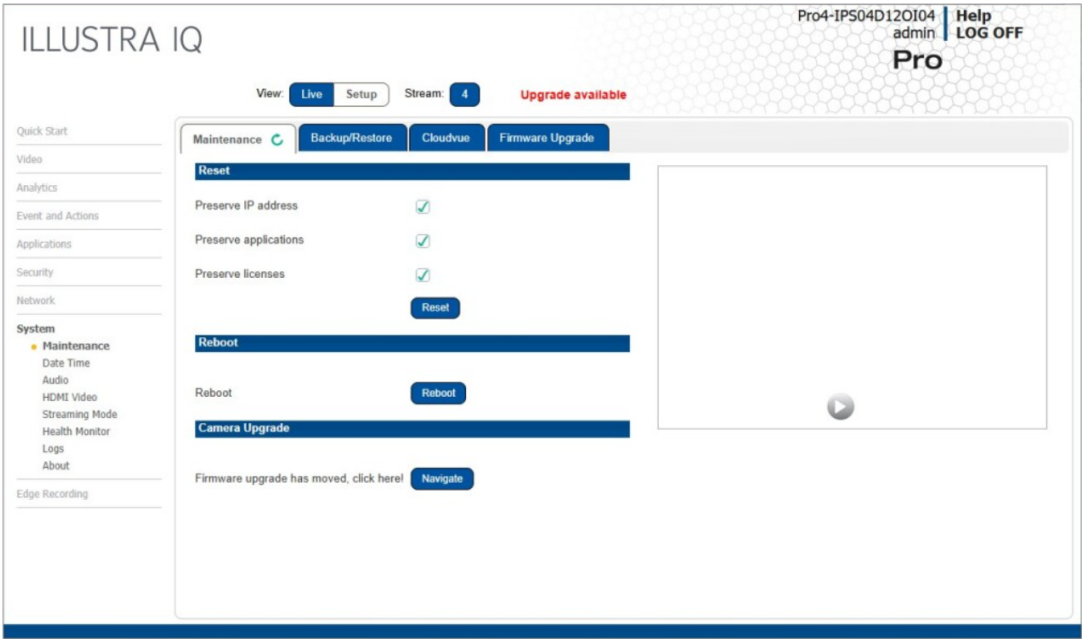
Note: When IPv6 is enabled, MTU can reach a minimum of 1250. To select a lower value, you must disable IPv6.

- End -

System

When you open the **System** menu, the **Maintenance** page appears, as seen in Figure 69 on page 175.

Figure 69 System Menu



The System Menu provides access to the following camera settings and functions:

- Maintenance
- Date Time
- Audio
- HDMI Video
- Streaming Mode
- Health Monitor
- Logs
- About

Maintenance

The Maintenance menu allows you to restore the camera settings to factory default, reboot the camera and apply a firmware upgrade.

Reset

To perform a physical reset of the camera, refer to the chapter regarding your camera model in this guide.

Note: Network settings can be retained if required.

Procedure 190 Resetting the Camera

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **System**.
2	Select **Maintenance** from the **System** menu.
3	Select the **Preserve IP address** check box to retain the current network settings during the camera reset. OR Deselect the **Preserve IP address** check box to restore the default networking settings. The default setting is 'Enabled'.
4	Select **Reset.** You will be prompted to confirm the camera reset. • Select **OK** to confirm. The Web User Interface will display a "Camera Resetting" page with a progress bar showing the reboot progress. • When the camera is restarted it will take 2 - 3 minutes until it is online and ready to be accessed and controlled. OR Select **Cancel**.
5	The Log in page displays.

- End -

Reboot

To perform a physical reset of the camera, refer to the chapter regarding your camera model in this guide.

Procedure 191 Reboot the Camera

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **System**.
2	Select **Maintenance** from the **System** menu.
3	Select **Reboot**. You will be prompted to confirm the camera reboot.
4	Select **OK** to confirm. The Web User Interface will display a "Camera Rebooting" page with a progress bar showing the reboot progress.

When the camera is restarted it will take 2 - 3 minutes until it is online and ready to be accessed and controlled.

OR

Select **Cancel**.

5 The Log in page displays.

- End -

Backup/Restore

Backup camera data and restore from a previously saved data file. The data file can be saved to a specified location and used to restore the camera configuration.

Note:A saved backup data file created on a camera is camera specific and cannot be used to restore the settings on a different camera.

Procedure 192 Backup Camera Data

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **System**.
2	Select **Maintenance** from the **System** menu.
3	Select the **Backup/Restore** tab.
4	Select **Backup**. You are prompted to save the backup file.
5	Select **Save**.

- End -

Procedure 193 Restore Camera from Backup

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **System**.
2	Select **Maintenance** from the **System** menu.
3	Select the **Backup/Restore** tab.
4	Select **Browse**. The Choose file to Upload dialog displays.
5	Navigate to the location where the firmware file has been saved.
6	Select the firmware file then select the **Open** button.
7	Select **Upload**. The file transfer begins. Do not disconnect power to the camera during the upgrade process. The camera restarts automatically after the updates have been completed, this can take from 1 to 10 minutes. The Log in page displays.

- End -

Cloudvue

The Cloudvue feature implements Illustra Cameras to Cloud (C2C) from Cloudvue to provide a secure, scalable, cloud-based storage solution. Before you enable this feature, you need to install the mobile application. You can download the app from either the iOS App Store or the Google Play Store and then you can complete the registration using the app.

Procedure 194 Enabling Cloudvue integration

Note: If a Cloudvue server is not setup when enabling the Cloudvue feature then the camera may become inaccessible.

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **System**.
2	Select **Maintenance** from the **System** menu.

3 Select the **Cloudvue** tab.

4 Select **Apply**.

5 Enter an administrator password to validate the request.

- If the camera detects an Internet connection, it continues with th Cloud-vue integration request. If an Internet connection is not detected an error displays and the request is rejected.

Note: If an Internet connection is detected, a factory reset begins. This clears all previous user defined configurations including user management settings.
The camera boots in Cloudvue mode and is only accessible using HTTPS.
The password changes to a string of characters determined by the Cloudvue.

6 Refer to Cloudvue documentation and follow the procedure to add a camera to regain access.

- End -

Procedure 195 Resetting the camera to normal operation

Note: There are two procedures for resetting the camera, please select one.

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **System**.
2	Select **Maintenance** from the **System** menu.
3	Select the **Maintenance** tab. This page displays two types of factory reset: a **Factory Reset**: Resets the camera and boots the camera in Illustra mode. b **Cloudvue Reset**: Resets the camera and boots the camera in Cloudvue mode.
4	If you do not have the credentials to perform a reset, you can perform a factory reset on the hardware itself by using the hardware reset button as detailed in the Product Overview of each camera.

- End -

Firmware upgrade

View the current firmware, manually upgrade to new firmware, and schedule automatic updates.

Note: The procedures that follow require the camera to have access to Illustra Online Cloud Firmware repository.

Procedure 196 Upgrading the camera firmware

Step	Action
1	Select **Setup** and then **System** to view the Maintenance tab.
2	Select the **Firmware Upgrade** tab to view the camera firmware option.

Note: The firmware that is currently installed is visible under the **Firmware Version Status** heading.

Note: When the **New Version** is set to **Up-to-date** then the camera has the latest firmware installed and no upgrade is currently available.

Current Status: This confirms that the Over The Air (OTA) process is running or when a new firmware is downloading.

- **Optional:** Select PDF icon to view the most recent firmware release note information.
- **Optional:** Select the **Download URL** button to save link to firmware then download directly via browser
- **Optional:** Select the **Weekly check** check box to enable or disable the camera to automatically check for a new firmware on a weekly basis.
- **Optional:** Select the **Check for Updates** button to see if a new camera firmware upgrade is available now.

3 Select the **Update Now** button and then select **Yes** to start the upgrade.

Note: The camera begins an upgrade when a new firmware is available.

Note: The Current Status changes to Downloading when you begin the upgrade.

- End -

Procedure 197 Scheduling a weekly camera firmware upgrade

Step	Action
1	Select **Setup** and then **System** to view the Maintenance tab.
2	Select the **Firmware Upgrade** tab to view the camera firmware option.
3	Under the **Firmware Scheduler** heading, select the **Auto Apply Upgrades** to view the **Upgrade Automatically Upon Availability** window. a Select any day from under the **Select Day(s)** heading. b Enter the **hour**, **minute** and **am** or **pm** for when the upgrade should start. **Note:** Select the **Time 24-hour** check box to show the time in 24-hour format.
4	Select the **Save** button to save all upgrade settings.

- End -

Procedure 198 Scheduling a camera firmware upgrade

Step	Action
1	Select **Setup** and then **System** to view the Maintenance tab.
2	Select the **Firmware Upgrade** tab to view the camera firmware option.
3	Under the **Firmware Scheduler** heading, select the **Set** button to view the **Date Time** window. a Select the **Date** text box and then select a date.

b Enter the **hour**, **minute** and **am** or **pm** for when the upgrade should start.

Note: Select the **Time 24-hour** check box to show the time in 24-hour format.

4 Select the **Save** button to save all upgrade settings.

- End -

Procedure 199 Manually install a specific firmware version

Use this procedure to install a firmware that is not the latest version.

Step	Action
1	Select **Setup** and then **System** to view the Maintenance tab.
2	Select the **Firmware Upgrade** tab to view the camera firmware option.
3	Under the **Manual Firmware Upgrade** heading, select the **Browse** button and select the firmware that you want to use.
4	Select the **Upload** button to begin the upgrade.

- End -

Date / Time

Set the date and time on the camera.

Note: Date and Time can also be configured in the **Quick Start** menu.

Procedure 200 Configuring the Date and Time

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **System**.
2	Select the **Date Time** from the **System** menu.
3	Select the **Time 24-hour** check box to enable the 24-hour clock. Or Deselect the **Time 24-hour** check box to enable the 12-hour clock. The default setting is '24-hour'.
4	Select the **Date Display Format** from the drop-down menu: • **DD/MM/YYYY** • **MM/DD/YYYY** • **YYYY/MM/DD** The default setting is 'YYYY/MM/DD'.
5	Select the **Time Zone** from the drop-down menu. The default setting is '(GMT-05:00) Eastern Time (US & Canada)
6	Select the **Set Time** setting by selecting the radio buttons: • **Manually**

- **via NTP**

The default setting is 'Manually'.

7 If you select Manually in step 5:

c Select the Date **(DD/MM/YYYY)** using the drop-down menus.

d Select the Time **(HH:MM:SS)** using the drop-down menus.

8 If you select via NTP in step 5:

a Enter the **NTP Server Name** in the text box.

- End -

Audio

You can configure the audio input, output, upload audio and stored audio clips, as well as configure Audio Video Synchronization on this tab.

The cameras internal microphone is identified by number 2 in Figure 5.

Procedure 201 Configure Audio Input

Step	Action

1 Select **Setup** on the Web User Interface banner to display the setup menus and then select **System**.

2 Select the **Input Source** drop-down and select one of the following options:

- **Internal**
- **External**

3 Select the **Audio** from the **System** menu.

4 Select the **Input Enable** check box to enable the audio input settings.

Or

Clear the **Input Enable** check box to disable audio input settings.

The default setting is 'Disabled'.

5 Use the slider bar to select the **Input Volume**.

Values range from 1 to 100.

The default setting is 72.

- End -

Procedure 202 Configuring Audio Output

Step	Action

1 Select **Setup** on the Web User Interface banner to display the setup menus and then select **System**.

2 Select the **Audio** from the **System** menu.

3 Select the **Output Enable** check box to enable the audio output settings.

Or

Deselect the **Output Enable** check box to disable audio input settings.

The default setting is 'Disabled'.

4 If Output Enable has been enabled, use the slider bar to select the Output Volume.

Values range from 1 to 100.

The default setting is 50.

- End -

Configuring Stored Audio

When connected to an appropriate device, the unit is capable of playing back stored audio when an alarm has been triggered. A maximum of five audio files can be uploaded to the unit.

Note: Audio clips can only be used if a micro SD Card has been installed. Refer to the relevant Quick Reference Guide for information on installing the micro SD Card.

When uploading an audio file it must meet the following requirements:

- The filename cannot contain spaces.
- It must be a 'wav' file with a '.wav' extension.
- A single channel mono file with a bit depth of 16kHz.
- The sample rate must be 8kHz.
- The duration must be no longer than 20 seconds.

Procedure 203 Play Stored Audio

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **System**.
2	Select the **Audio** from the **System** menu.
3	Select the **Audio Clips** tab.
4	Select to play back the corresponding audio file.

- End -

Procedure 204 Upload an Audio File

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **System**.
2	Select the **Audio** from the **System** menu.
3	Select the **Audio Clips** tab.
4	Select **Browse**. The Choose file dialog displays.
5	Navigate to the location where the audio file has been saved. Select the audio file then select the **Open** button.

When uploading an audio file it must meet the following requirements:

- The filename cannot contain spaces.
- It must be a 'wav' file with a '.wav' extension.
- A single channel mono file with a bit depth of 16kHz.
- The sample rate must be 8kHz.
- The duration must be no longer than 20 seconds.

6 Select **Upload**.

7 You will be prompted to confirm that you would like to upload the audio file.

Select **OK** to confirm the upload.

Or

Select **Cancel**.

- End -

Procedure 205 Delete a Stored Audio file

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **System**.
2	Select the **Audio** from the **System** menu.
3	Select the **Audio Clips** tab.
4	Select the corresponding **Delete** check box to mark the audio file for deletion. Or Deselect the corresponding **Delete** check box to keep the audio file.
5	Select the **Select All** check box to mark all audio files for deletion.
6	Select **Delete** to delete the selected audio files. You will be prompted to confirm the deletion.
7	Select **OK** to confirm the deletion. Or Select **Cancel**.

- End -

HDMI Video

The camera can output to a HDMI monitor through the micro HDMI cable port.

Procedure 206 Enable or disable HDMI Video

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **System**.
2	Select the **HDMI Video** from the **System** menu.

3 Select the **Enable HDMI** check box to enable HDMI video.

Or

Deselect the **Enable HDMI** check box to enable HDMI video.

The default setting is 'Disabled'.

- End -

Streaming Mode

On some cameras the user can change the stream performance by selecting additional modes.

Note: This application is not available on the LPR cameras.

Procedure 207 Change Camera Streaming Mode

Step	Action

1 Select **Setup** on the Web User Interface banner to display the setup menus and then select **System**.

2 Select **Streaming Mode** to view the Streaming Mode tab.

3 Select from the following options in the drop down for Streaming Mode:

Default (default setting)	Legacy Stream table supported up until now
DualFullHDmode	Adds additional stream 2 resolutions: 1664x936, 1920x1080. Enabling this Stream option will impact some legacy functionality. Please refer to stream table for limitations

4 Reboot the camera to apply the new streaming mode

- End -

Health Monitor

The Health Monitor function provides visibility on the health status of popular device parameters. Each parameter can be enabled or disabled. The refresh frequency of the health monitor can be determined by selecting a duration from the Reporting Period drop-down menu.

Procedure 208 Configure Health Monitor Settings

Step	Action

1 Select **Setup** on the Web User Interface banner to display the setup menus and then select **System**.

2 Select the **Health Monitor** from the **System** menu.

3 Select the **Recording Period** from the drop-down menu.

4 Select the corresponding check box to enable health monitoring on a parameter.

OR

Clear the corresponding check box to disable health monitoring on a parameter.

The default setting for all parameters is Enabled.

- End -

Logs

Information is provided on system and boot logs created by the camera.

System Log

The system log gives the most recent messages from the unix/var/log/messages file. Information will include the following:

- Messages about system behavior such as process startup/shutdown.
- Warnings about recoverable problems that processes encounter.
- Error messages where processes encounter problems they cannot fix; note that this does not mean that the process will not continue to work, only that it encountered an issue it could do nothing about.

Procedure 209 Display System Log

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **System**.
2	Select the **Logs** from the **System** menu. The System Log tab displays.
3	Select **Refresh** to refresh the log for the most up-to-date information.

- End -

Procedure 210 System Log Filter

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **System**.
2	Select the **Logs** from the **System** menu. The System Log tab displays.
3	Enter the number of lines of the log file you would like to view in the **Lines** text box.
4	Enter the word or phrase that you would like to search for in the **Filter** text box.
5	Select **Refresh** to refresh the log for the most up-to-date information.

- End -

Boot Log

The Boot log is a log of the Linux operating system boot processes and will only be useful to Tyco Security Products support engineers who require additional information on the device.

Procedure 211 Display Boot Log

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **System**.
2	Select the **Logs** from the **System** menu.
3	Select the **Boot Log** tab.
4	Select **Refresh** to refresh the log for the most up-to-date information.

- End -

Procedure 212 Boot Log Filter

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **System**.
2	Select the **Logs** from the **System** menu.
3	Select the **Boot Log** tab.
4	Enter the number of lines of the log file you would like to view in the **Lines** text box.
5	Enter the word or phrase that you would like to search for in the **Filter** text box.
6	Select **Refresh** to refresh the log for the most up-to-date information.

- End -

Audit Log

The Audit Log will log details obtained when anything is logged are source, class, result, user and a description of the change.all changes that have been made in the following areas of the Web User Interface as outlined below:

- Changes in FTP, CIFS, SMTP, IPV4, IPV6, DNS and SNMP are logged under class NETWORK.
- Changes in Stream are logged under class VIDEO.
- Changes in Reboot, Reset and Upgrade are logged under class MAINTENANCE.
- Changes in DIO and ROI are logged under EVENT.

About

The About menu provides the following camera information:

- Camera Name
- Model
- Product Code
- Manufacturing Date
- Serial Number
- MAC Address

- Firmware Version
- Hardware Version
- iAPI Version

Procedure 213 Display Model Information

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **System**.
2	Select **About** from the **System** menu. The model tab displays.

- End -

Procedure 214 Edit Camera Name

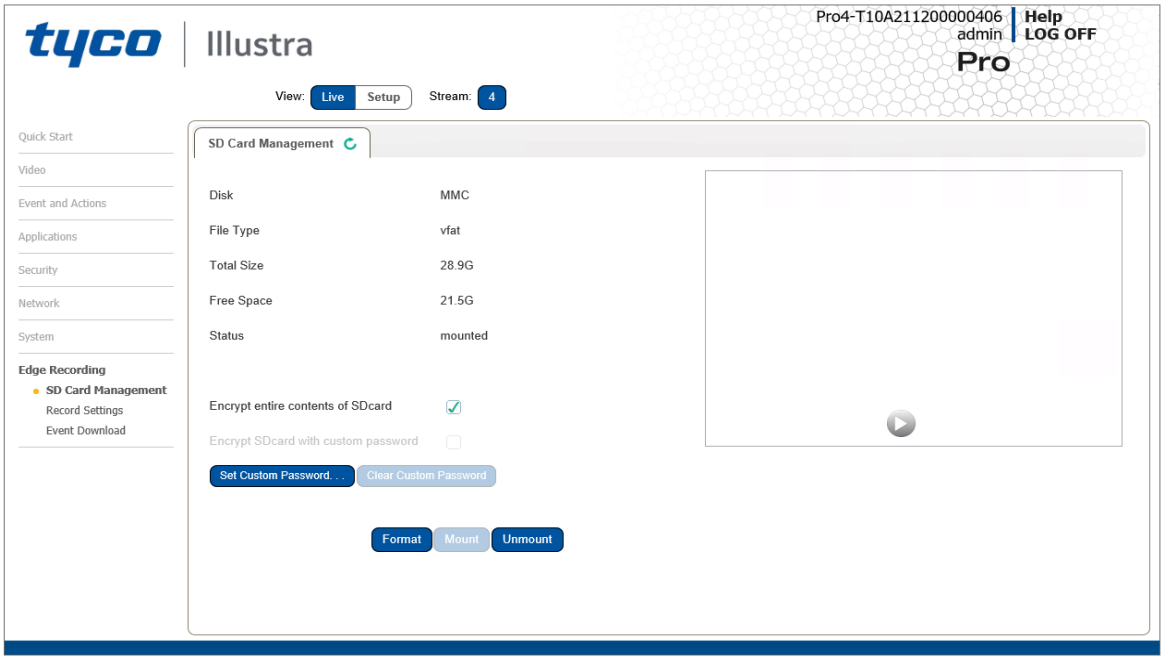
Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **System**.
2	Select **About** from the **System** menu. The model tab displays.
3	Edit the name in the **Camera Name** textbox.

- End -

Edge Recording

When you select the **Edge Recording** menu, the **Micro SD Card Management** page appears, as seen in Figure 70 on page 189.

Figure 70 Edge Recording Menu



The Edge Recording Menu provides access to the following camera settings and functions:

- SD Card Management
- Record Settings
- Event Download

Micro SD Card Management

Edge recording provides the ability to save recorded video to a Micro SD Card. Video can be configured to be recorded based on an event. Without a Micro SD Card current faults notifications displayed on camera if an alarm is triggered. Using a Micro SD Card enables the following:

- Current faults notifications displayed on camera if an alarm is triggered.
- Video/Audio and screen shot are saved to the SD card.
- SMTP notifications can be sent.
- FTP and CIFS uploads of video can be sent.
- Audio can be played via the Audio Out port.

Inserting the Micro SD Card

When inserting a Micro SD Card it is essential that the camera is rebooted. The Micro SD Card should be mounted and unmounted through the Web User Interface. If you receive a 'Device is Busy' model you should wait and try again in a few minutes. If this does not work then it may be necessary to disable Motion Detection, FTP or any other process which may be using the Micro SD Card.

Note: Refer to the Quick Reference Guide supplied with the product for details on how to remove the housing assembly and gain access to the camera.

Procedure 215 Insert the Micro SD Card by powering down the Camera

Step	Action
1	Turn off the camera by disconnecting the power supply.
2	Insert the Micro SD card into the camera.
3	Reconnect the power supply and power up the camera.

- End -

Procedure 216 Mount the Micro SD Card through the Web User Interface to reboot the Camera

Step	Action
1	Insert the Micro SD card into the camera.
2	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Edge Recording**.
3	Select **SD Card Management** from the **Edge Recording** menu.
4	Select **Mount**.

- End -

Removing the Micro SD Card

If at any stage you need to remove the Micro SD card from the camera one of the following two procedures should be used:

- Remove the Micro SD Card by powering down the camera - Use this procedure if you do not have access to the Web User Interface and are unable to unmount the Micro SD card before removal.
- Unmount the Micro SD Card for Removal - Use this procedure when you are unable to access the power supply to the camera.

Note: Refer to the Quick Reference Guide supplied with the product for details on how to remove the housing assembly and gain access to the camera.

Procedure 217 Remove the Micro SD Card by powering down the Camera

Step	Action
1	Turn off the camera by disconnecting the power supply.
2	Remove the Micro SD card from the camera. **Note:**AVI clips are not available on the camera until the Micro SD card has been inserted and the camera rebooted.
3	Reconnect the power supply and power up the camera.

- End -

Procedure 218 Unmount the Micro SD Card for Removal

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Edge Recording**.
2	Select **SD Card Management** from the **Edge Recording** menu.
3	Select **Unmount**. You are prompted to confirm the unmounting.
4	Select **OK** to confirm. OR
5	Select **Cancel**. Remove the Micro SD card from the camera. AVI clips are not available on the camera until the Micro SD card has been inserted and mounted.

- End -

Encrypted SD card storage

Introduction of the Encrypted SD Card storage feature which offers encryption for the entire contents of their SD card. When SD card Encryption is enabled the contents of the SD Card will only be accessible through the Camera Web GUI, unless a Custom Password has been set which allows password protected access to the SD card when mounted elsewhere. Currently this mounting is only supported on Linux systems.

NOTE: The user can disable Encrypted SD Card storage to revert to being able to access the SD card via Windows based systems, without a Password.

Disabling SD card encryption is not recommended.

Procedure 219 Encrypting the contents on the SD card

Step	Action
1	Insert the SD card into camera.
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Edge Recording**.

2 Select **SD Card Management** from the **Edge Recording** menu.

Note: The SD card will show as unmounted with encryption enabled.

Note: Encryption is always enabled by default after the camera has been reset. The user may disable encryption mode but any change to the encryption status requires the SD card to be formatted.

3 Format the SD card by selecting **Format** and select **Mount** to mount the encrypted SD card.

Note: The SD card will fail to mount until it has been formatted. The user now has the option to encrypt SD card with a custom password.

The Custom Password is only required when the SD card is accessed independently from the camera. It will not affect SD card functionality while it is being used by the camera.

4 Log in to the camera Web GUI and select **SD Card Management** from the **Edge Recording** menu.

5 Select 'Encrypt SD card with custom password'.

6 Enter the custom password into both password fields and select **Save.**

Note: Once the Custom Password has been set, it can be edited or cleared at any time in the SD Card Management tab under the Edge Recording menu.

The Custom Password will remain set after a firmware upgrade. The Custom Password will be cleared after a reset.

The SD Card Encryption can be disabled at any time by unticking 'Encrypt entire contents of SD card'. However any changes to the encryption status requires the SD card to be formatted.

- End -

Procedure 220 Resetting a camera

Step	Action

Note: The SD card encryption is always enabled by default after a camera reset

1 Select **Setup** on the Web User Interface banner to display the setup menus and then select **System**.

2 Select **Maintenance** from the **System** menu.

3 Select **Reset** and **OK**.

Note: Wait for the Reset process to complete.

4 Log in to the camera Web GUI and run through the initial setup.

5 Select **SD Card Management** from the Edge Recording menu.

- If SD card Encryption was enabled before reset and the same HostID is used after reset, the SD card will show as mounted and Encryption will be enabled.
- If SD card Encryption was enabled before reset and a different HostID is used, the SD card will show as unmounted and Encryption will be

enabled. SD card will need to be formatted before it can be mounted by the camera.

- If SD card Encryption was disabled before reset, the SD card will show as unmounted and Encryption will be enabled. SD card will need to be formatted before it can be mounted by the camera.

- End -

Record Settings

Select which video stream to use for alarm video and configure pre and post event durations for the playable video clip. The camera can record video generated from MD, face detection and DIO events.

Procedure 221 Configure Record Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Edge Recording**.
2	Select **Record Settings** from the **Edge Recording** menu.
3	Select **Enable Record** to allow the camera to create a playable video clip. OR Deselect **Enable Record** to disable the feature.
4	If **Enable Record** has been enabled: a Select the required video stream from the Video drop-down menu. Refer to Procedure 5-1 Configure the Video Stream Settings. b Select the Pre Event (secs) in seconds from the drop-down menu. Values range from 0 to 10. The default setting is 5 seconds. c Select the Post Event (secs) in seconds from the drop-down menu. Values range from 0 to 10. The default setting is 5 seconds.
5	Select **Apply** to save.

- End -

Offline Record Settings

When you configure the Offline Record Settings feature and once it detects a loss of connection with the recorder, it sends the video stream to the Micro SD card within the unit. This satisfies the loss of video and continues recording. Once the recorder is back online the camera initiates sending recorded video from the Micro SD card to the recorder. The maximum time recording during the outage depends on the Micro SD card and the recorded stream you selected. If the Micro SD reaches full capacity, it deletes video from earliest recording to latest recording. This feature integrates with the VE NVR 5.0 Trickle Stor.

Procedure 222 Configure Offline Recording Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Edge Recording**.
2	Select **Record Settings** from the **Edge Recording** menu.
3	Select the **Offline Record Settings** tab.
4	In the **Recorder IP Address** field, enter the IP address of the recorder the camera is connected to.
5	In the **Pre event (secs)** field, enter a time in seconds of the amount of time you want recorded before the offline event.
6	In the **Post event (secs)** field, enter a time in seconds of the amount of time you wants recorded after the offline event.

- End -

Event Download

If an event action has record mode enabled, when triggered, the associated video is logged in the event download table where it can later be downloaded from an Micro SD Card using the specified upload protocol.

Note: An event action must have record mode enabled to be logged and downloaded. This is configured in **Event Actions** under the **Events and Actions** menu.

Appendix A: Using Media Player to View RTSP Streaming

Note: This appendix is provided for user instruction only. Tyco Security Products does not support or is not responsible for any error caused during the use of third party software used for RTSP playback.

Procedure 223 Viewing RTSP Stream through Media Player

Step	Action

You can use Media Player to view live video and audio in real time from the camera.

1 Select **Media** then **Open Network Stream**.

2 Enter the IP address of the camera stream in the **Network URL** text box in the following format to view Stream 1 and 2:

- **Stream 1:** rtsp://cameraip:554/videoStreamId=1
- **Stream 2:** rtsp://cameraip:554/audioStreamId=1

For example: rtsp://192.168.1.168:554/videoStreamId=1

OR

rtsp://192.168.1.168:554/videoStreamId=1&audioStreamId=1

3 Select **Play**.The live video stream displays.

- End -

Appendix B: Stream Tables

Pro Gen 4 - 2MP, 4MP, 5MP and 8MP Streaming Combinations

Table 71 2MP Dome, Bullet, and Compact Camera Stream Set (all resolution, codes and frame rate combinations of Stream 1, 2, 3 and 4 are valid)

		Normal Mode				
		Resolution	Description	Max FPS		
				TWDR Off	TWDR 2x	TWDR 3x
Stream 1	H.264, H.265, H.264+, H.265+, MJPEG	1920x1080 1664x936 1280x720	(1080p) 16:9 (HD+) 16:9 (720P) 16:9	60 60 60	30 30 30	15 15 15
Stream 2	H.264, H.265, H.264+, H.265+, MJPEG	1920x1080** 1664x936** 1280x720 1024x576 960x544 816x464 640x360 480x272	(1080p) 16:9 (HD+) 16:9 (720p) 16:9 (PAL+) 16:9 (qHD) 16:9 16:9 (nHD) 16:9 16:9	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	15 15 15 15 15 15 15 15
Stream 3	H.264, H.265, H.264+, H.265+, MJPEG	640x360 480x272	16:9 16:9	30 30	30 30	15 15
Stream 4	MJPEG	640x368	16:9	7	7	7

Note:**Available via Streaming Mode selection: DualFullHDMode. Limitations: Analogue/HDMI options removed from stream.

Note:A maximum of 5 concurrent streams are supported by each camera, this includes shared streams.

Table 72 2MP Dome, Bullet, and Compact Camera Stream Set (all resolution, codes and frame rate combinations of Stream 1, 2, 3 and 4 are valid)

		Corridor Mode				
		Resolution	Description	Max FPS		
				TWDR Off	TWDR 2x	TWDR 3x
Stream 1	H.264, H.265, H.264+, H.265+, MJPEG	1920x1080 1664x936 1280x720	(1080p) 16:9 (HD+) 16:9 (720P) 16:9	30 30 30	30 30 30	15 15 15
Stream 2	H.264, H.265, H.264+, H.265+, MJPEG	1920x1080** 1664x936** 1280x720 1024x576 960x544 816x464 640x360 480x272	(1080p) 16:9 (HD+) 16:9 (720p) 16:9 (PAL+) 16:9 (qHD) 16:9 16:9 (nHD) 16:9 16:9	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	15 15 15 15 15 15 15 15
Stream 3	H.264, H.265, H.264+, H.265+, MJPEG	640x360 480x272	16:9 16:9	30 30	30 30	15 15
Stream 4	MJPEG	640x368	16:9	7	7	7

Note:**Available via Streaming Mode selection: DualFullHDMode. Limitations: Analogue/HDMI options removed from stream.

Note:A maximum of 5 concurrent streams are supported by each camera, this includes shared streams.

Table 73 4MP Dome, Bullet, Compact Cameras and 5MP LPR Dome and 5MP LPR Bullet Cameras Stream Set (all resolution, codes and frame rate combinations of Stream 1, 2, 3 and 4 are valid)

		Normal Mode				
		Resolution	Description	Max FPS		
				TWDR Off	TWDR 2x	TWDR 3x
Stream 1	H.264, H.265, H.264+, H.265+,	2560x1920 2560x1440 *1	4:3 16:9	30 30	30 30	15 15
	H.264, H.265, H.264+, H.265+, MJPEG	2048 x 1536*** 1920x1080 1664x936 1280x720	(3MP) 4:3 (1080p) 16:9 (HD+) 16:9 (720P) 16:9	30 60 60 60	30 30 30 30	15 15 15 15
Stream 2	H.264, H.265, H.264+, H.265+, MJPEG	1920x1080** 1664x936** 1280x720 1024x576 960x544 816x464 640x480 640x360 480x272	(1080p) 16:9 (HD+) 16:9 (720p) 16:9 (PAL+) 16:9 (qHD) 16:9 16:9 16:9 (nHD) 16:9 16:9	30 30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30 30	15 15 15 15 15 15 15 15 15
Stream 3	H.264, H.265, H.264+, H.265+, MJPEG	640x360 640x480 480x360 480x272	16:9 (VGA) 4:3 4:3 16:9	30 30 30 30	30 30 30 30	15 15 15 15
Stream 4	MJPEG	640x368	16:9	7	7	7

Note: *1 = The default resolution of stream 1 will be 2560x1440.

Note: ** Available via Streaming Mode selection: DualFullHDmode. Limitations: Analogue/HDMI option removed from stream.

Note: ***Available on 24.03 release

Note: A maximum of 5 concurrent streams are supported by each camera, this includes shared streams.

Table 74 4MP Dome, Bullet, Compact Cameras and 5MP LPR Dome and 5MP LPR Bullet Cameras Stream Set (all resolution, codes and frame rate combinations of Stream 1, 2, 3 and 4 are valid)

		Corridor Mode				
		Resolution	Description	Max FPS		
				TWDR Off	TWDR 2x	TWDR 3x
Stream 1	H.264, H.265, H.264+, H.265+	2560x1920 2560x1440 *1	4:3 16:9	30 30	30 30	15 15
	H.264, H.265, H.264+, H.265+, MJPEG	2048 x 1536*** 1920x1080 1664x936 1280x720	(3MP) 4:3 (1080p) 16:9 (HD+) 16:9 (720P) 16:9	30 30 30 30	25 30 30 30	15 15 15 15
Stream 2	H.264, H.265, H.264+, H.265+, MJPEG	1920x1080** 1664x936** 1280x720 1024x576 960x544 816x464 640x480 640x360 480x272	(1080p) 16:9 (HD+) 16:9 (720p) 16:9 (PAL+) 16:9 (qHD) 16:9 16:9 16:9 (nHD) 16:9 16:9	30 30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30 30	15 15 15 15 15 15 15 15 15
Stream 3	H.264, H.265, H.264+, H.265+, MJPEG	640x360 640x480 480x360 480x272	16:9 (VGA) 4:3 4:3 16:9	30 30 30 30	30 30 30 30	15 15 15 15
Stream 4	MJPEG	640x368	16:9	7	7	7

Note:*1 = The default resolution of stream 1 will be 2560x1440.

Note:** Available via Streaming Mode selection: DualFullHDmode. Limitations: Analogue/HDMI option removed from stream.

Note:***Available on 24.03 release

Note:A maximum of 5 concurrent streams are supported by each camera, this includes shared streams.

Table 75 5MP Corner Dome Camera Stream Set (all resolution, codes and frame rate combinations of Stream 1, 2, 3 and 4 are valid)

		Normal Mode				
		Resolution	Description	Max FPS		
				TWDR Off	TWDR 2x	TWDR 3x
Stream 1	H.264, H.265, H.264+, H.265+,	2560x1920	5MP 4:3	30	30	15
	H.264, H.265, H.264+, H.265+, MJPEG	2048x1536*** 1280x960	3MP 4:3 1.2MP 16:9	30 60	30 30	15 15
Stream 2	H.264, H.265, H.264+, H.265+, MJPEG	1440x1080** 800x600 640x480 480x360	(QHD) 4:3 (SVGA) 4:3 4:3 4:3	30 30 30 30	30 30 30 30	15 15 15 15
Stream 3	H.264, H.265, H.264+, H.265+, MJPEG	640x480	4:3	30	30	15
Stream 4	MJPEG	800x600	4:3	7	7	7

Note:** Available via Streaming Mode selection: DualFullHDmode. Limitations: Analogue/HDMI option removed from stream.

Note:*** Available on 24.03 release

Note:A maximum of 5 concurrent streams are supported by each camera, this includes shared streams.

Note: Use cases for this camera should not include 4:3 resolutions

Table 76 8MP Dome, Bullet, and Compact Camera Stream Set (all resolution, codes and frame rate combinations of Stream 1, 2, 3 and 4 are valid)

		Normal Mode				
		Resolution	Description	Max FPS		
				TWDR Off	TWDR 2x	TWDR 3x
Stream 1	H.264, H.265, H.264+, H.265+,	3840x2160 3264x1840 2688x1520	(4K) 16:9 16:9 16:9	30 30 30	25 25 25	15 15 15
	H.264, H.265, H.264+, H.265+, MJPEG	1920x1080 1664x936 1280x720	(1080p) 16:9 (HD+) 16:9 (720P) 16:9	30 30 60	25 25 25	15 15 15
Stream 2	H.264, H.265, H.264+, H.265+, MJPEG	1920x1080** 1664 x 936** 1280x720 1024x576 960x544 816x464 640x360 480x272	(1080p) 16:9 (HD+) 16:9 (720p) 16:9 (PAL+) 16:9 (qHD) 16:9 16:9 (nHD) 16:9 16:9	30 30 30 *1 30 *1 30 *1 30 *1 30 *1 30 *1	25 *1 25 *1 25 *1 25 *1 25 *1 25 *1 25 *1 25 *1	15 15 15 15 15 15 15 15
Stream 3	H.264, H.265, H.264+, H.265+, MJPEG	640x360 480x272	16:9 16:9	30 *2 30 *2	25 *2 25 *2	15 15
Stream 4	MJPEG	640x368	16:9	7	7	7

Note:*1 = Stream 2 is restricted to 15 FPS when Stream 1 resolution is greater than 1920x1080.

Note:*2 = Stream 3 is restricted to 10 FPS when Stream 1 resolution is greater than 1920x1080.

Note: Enabling TWDR on the 8MP camera requires Analog Video to be disabled

Note: Enabling TWDR will retrict the frame rate of Stream 1 to 25 FPS for any resolution.

Note:A maximum of 5 concurrent streams are supported by each camera, this includes shared streams.

Note:**Available via Streaming Mode selection: DualFullHD mode. Limitations: Analog/HDMI option removed from stream.

Table 77 8MP Dome, Bullet, and Compact Camera Stream Set (all resolution, codes and frame rate combinations of Stream 1, 2, 3 and 4 are valid)

		Corridor Mode				
		Resolution	Description	Max FPS		
				TWDR Off	TWDR 2x	TWDR 3x
Stream 1	H.264, H.265, H.264+, H.265+,	3840x2160 3264x1840 2688x1520	(4K) 16:9 16:9 16:9	30 30 30	25 25 25	15 15 15
	H.264, H.265, H.264+, H.265+, MJPEG	1920x1080 1664x936 1280x720	(1080p) 16:9 (HD+) 16:9 (720P) 16:9	30 30 30	25 25 25	15 15 15
Stream 2	H.264, H.265, H.264+, H.265+, MJPEG	1920x1080** 1664 x 936** 1280x720 1024x576 960x544 816x464 640x360 480x272	(1080p) 16:9 (HD+) 16:9 (720p) 16:9 (PAL+) 16:9 (qHD) 16:9 16:9 (nHD) 16:9 16:9	30 30 30 *1 30 *1 30 *1 30 *1 30 *1 30 *1	25 *1 25 *1 25 *1 25 *1 25 *1 25 *1 25 *1 25 *1	15 15 15 15 15 15 15 15
Stream 3	H.264, H.265, H.264+, H.265+, MJPEG	640x360 480x272	16:9 16:9	30 *2 30 *2	25 *2 25 *2	15 15
Stream 4	MJPEG	640x368	16:9	7	7	7

Note:*1 = Stream 2 is restricted to 15 FPS when Stream 1 resolution is greater than 1920x1080.

Note:*2 = Stream 3 is restricted to 10 FPS when Stream 1 resolution is greater than 1920x1080.

Note: Enabling TWDR on the 8MP camera will require Analogue Video to be disabled.

Note: Enabling TWDR will restrict the frame rate of Stream 1 to 25 FPS for any resolution.

Note:A maximum of 5 concurrent streams are supported by each camera, this includes shared streams.

Note:** Available via Streaming Mode selection: DualFullHDmode. Limitations: Analogue/HDMI option removed from stream.

Appendix C:Technical Specifications

The table below lists technical specifications of the PG4 2MP Dome cameras.

Camera Part Number	IPS02-D12-OI04	IPS02-D17-OI04
Camera Features		
Imager	Sony Colour CMOS IMX327, 1/2.8"	Sony Colour CMOS IMX327, 1/2.8"
Sensor Matrix (effective pixel)	Approx 2,0703,600 pixels	Approx 2,0703,600 pixels
Memory	RAM: LPDDR 2GB ROM: eMMC 4GB	RAM: LPDDR 2GB ROM: eMMC 4GB
Lens Spec	Motorised lens (4Mp optics), f 2.7-13.5mm, F1.4~2.8	Motorised lens (4Mp optics), f 7-22mm, F1.7~2.8
Optical Zoom	5x	3x
FOV	Wide: 107°(H) 56°(V) Tele : 34°(H) 10°(V)	Wide: 38°(H) 20°(V) Tele : 17°(H) 10°(V)
Iris Control	P-Iris (manual, auto)	P-Iris (manual, auto)
Focus Control	One Touch auto focus with user select-able target ROI area, manual, and auto-matic focus with zoom. Physical AF button on Dome.	One Touch auto focus with user select-able target ROI area, manual, and auto-matic focus with zoom. Physical AF button on Dome.
Min. Illumination	color = 0.01 lux B&W = 0.005 lux	color = 0.03 lux B&W = 0.01 lux
Day / Night control	Mechanical ICR	Mechanical ICR
Day / Night Switch control	Mode: Auto, colour, BW D/N switch sensitivity D/N switch time	Mode: Auto, colour, BW D/N switch sensitivity D/N switch time
IR Distance	Up to 50m	Up to 50m
IR Mode	On, off	On, off
Adaptive IR	Yes	Yes
Smart IR	No	No
Video Output	Micro HDMI Female connector on cam-era	Micro HDMI Female connector on cam-era
S/N Ratio	>50dB	>50dB
Image		
Exposure Profiles	Demo, Auto, Indoor, Outdoor,Shutter Priority, Iris priority, Gaming, License plate recognition (LPR) High, LPR Medium, LPR low, manual	Demo, Auto, Indoor, Outdoor,Shutter Priority, Iris priority, Gaming, License plate recognition (LPR) High, LPR Medium, LPR low, manual

WDR	True WDR 126 dB Technologies	True WDR 126 dB Technologies
Video		
Video Compression	H264, H264 Intellizip, H265, H265 Intellizip, MJPEG	H264, H264 Intellizip, H265, H265 Intellizip
Maximum Frame Rate	2MP@60 fps	2MP@60 fps
Resolution & Frame Rate	1920x1080 @ 30fps (H.264/H.265)	1920x1080 @ 30fps (H.264/H.265)
Video Imaging		
AEC weighting method	Full|Upper|Lower|Center|Spot|Left|Right|User Defined | AI Object | AI Person | AI Face	
Exposure compensation offset range	-2 to +2 f-stops	
Exposure range	1/32000| 1/20000| 1/12500| 1/10000| 1/8000| 1/4000| 1/2500| 1/2000| 1/1000| 1/800| 1/500| 1/400| 1/250| 1/200| 1/120|1/60 1/30 1/15|1/8|1/4|	
Default maximum exposure	1/8 sec.	
Default minimum exposure	1/32,000 sec.	
White balance	Auto Normal / Manual / Auto Wide	
Dynamic range method	Off/ Smart WDR/ True WDR2x /TrueWDR3x/	
Dynamic Range (Sensor Theoretical)	True multi shutter WDR up to 120dB	
Noise Reduction	Digital Noise Reduction 2D and 3D	
Defog	Yes	
Image stabilization EIS	Yes	
Flicker less	50/60 Hz or OFF	
Corridor mode (rotate 90º)	Yes	
Text overlay	Camera Name / Date Time / User Defined Test in one of 4 locations	
Privacy zones	10 user definable rectangular zones	
Audio		
Compression Format	G.711	G.711
Audio Input / Output / Interface	Built in Microphone Terminal block for Line in & audio Out	Built in Microphone Terminal block for Line in & audio Out
Built in Microphone	Yes	Yes
Alarm		

Alarm Input	2 x Alarm in	2 x Alarm in
Alarm Output	2 x Relay out (1A/80V)	2 x Relay out (1A/80V)
Alarm Interface	Terminal block	Terminal block
System Integrations		
USB Interface	Yes, Micro-USB in pan-base & rear. Not for simultaneous use	Yes, Micro-USB in pan-base & rear. Not for simultaneous use
Edge Storage		
On Board Storage	Micro SD/SDHC/SDXC card slot. Up to 2TB. ENCRYPTED STORAGE (card not incl)	Micro SD/SDHC/SDXC card slot. Up to 2TB. ENCRYPTED STORAGE (card not incl)
General		
Ethernet	IEEE 802.3, 10/100 Base-T/TX, auto sensing, 1 x RJ45	IEEE 802.3, 10/100 Base-T/TX, auto sensing, 1 x RJ45
Reset / Default Button	2 Buttons (Hardware Reset & Factory Reset)	2 Buttons (Hardware Reset & Factory Reset)
Mechanical		
Casing	Bubble: PC, clear /smoke Dome Body: Aluminium Dome Base: Aluminium Pigtail: No Colour: White RAL 9003	Bubble: PC, clear /smoke Dome Body: Aluminium Dome Base: Aluminium Pigtail: No Colour: White RAL 9003
Weathering Resistance	IP67	IP67
Vandal Resistance	IK10	IK10
Dimension (HxWxD)	Ø138 x 143 mm	Ø138 x 143 mm
Weight	1.2kg (approx)	1.2kg (approx)
Electrical		
Power Source	Power over Ethernet (PoE) IEEE 802.3af Type 1 Class 3; 24 VAC	Power over Ethernet (PoE) IEEE 802.3af Type 1 Class 3; 24 VAC
Environmental		
Operating Temperature	-50°C to 65°C (1) IR LEDs will operate at 50% power if the temperature is between 49°C and 65°C.	-50°C to 65°C (1) IR LEDs will operate at 50% power if the temperature is between 49°C and 65°C.
Cold Start Temperature	-40°C	-40°C
Storage Temperature	-40°C to +60°C	-40°C to +60°C
Storage Humidity	90%, non-condensing	90%, non-condensing

RTC	Up to 24 hours	Up to 24 hours
Certification		
CE/FCC	Class A under 3 dB	Class A under 3 dB
RoHS	Yes	Yes
UL	UL62368/UL60950-22 62368/60950-22 CSA 22.2 No. 62368 CE: EN62368 / EN60950-22 IEC 62471 (IR LED)	UL62368/UL60950-22 62368/60950-22 CSA 22.2 No. 62368 CE: EN62368 / EN60950-22 IEC 62471 (IR LED)

The table below lists technical specifications of the PG4 4MP Dome cameras.

Camera Part Number	IPS04-D12-OI04	IPS04-D14-OI04
Camera Features		
Imager	Sony Colour CMOS IMX335, 1/2.8"	Sony Colour CMOS IMX335, 1/2.8"
Sensor Matrix (effective pixel)	Approx 5,040,000 pixels	Approx 5,040,000 pixels
Memory	RAM: LPDDR 2GB ROM: eMMC 4GB	RAM: LPDDR 2GB ROM: eMMC 4GB
Lens Spec	Motorised lens (6Mp optics), f 2.7-13.5mm, F1.4~2.8	Motorised lens (8Mp optics), f 6-22mm, F1.6
Optical Zoom	5x	3.5x
FOV	Wide: 101°(H) 54°(V) Tele : 32°(H) 18°(V)	Wide: 39°(H) 21°(V) Tele : 16°(H) 10°(V)
Iris Control	P-Iris (manual, auto)	P-Iris (manual, auto)
Focus Control	One Touch auto focus with user select-able target ROI area, manual, and auto-matic focus with zoom. Physical AF button on Dome.	One Touch auto focus with user select-able target ROI area, manual, and auto-matic focus with zoom. Physical AF button on Dome.
Min. Illumination	color = 0.12 lux B&W = 0.05 lux	color = 0.1 lux B&W = 0.04 lux
Day / Night control	Mechanical ICR	Mechanical ICR
Day / Night Switch control	Mode: Auto, colour, BW D/N switch sensitivity D/N switch time	Mode: Auto, colour, BW D/N switch sensitivity D/N switch time
IR Distance	Up to 50m	Up to 50m
IR Mode	On, off	On, off
Adaptive IR	Yes	Yes
Smart IR	No	No
Video Output	Micro HDMI Female connector on cam-era	Micro HDMI Female connector on cam-era
S/N Ratio	>50dB	>50dB
Image		
Exposure Profiles	Demo, Auto, Indoor, Outdoor,Shutter Priority, Iris priority, Gaming, License plate recognition (LPR) High, LPR Medium, LPR low, manual	Demo, Auto, Indoor, Outdoor,Shutter Priority, Iris priority, Gaming, License plate recognition (LPR) High, LPR Medium, LPR low, manual

WDR	True WDR 126 dB Technologies	True WDR 126 dB Technologies
Video		
Video Compression	H264, H264 Intellizip, H265, H265 Intellizip, MJPEG	MJPEG, H264, H264 Intellizip, H265, H265 Intellizip
Maximum Frame Rate	4MP @30 fps 2MP@60 fps	4MP @30 fps 2MP@60 fps
Resolution & Frame Rate	2688 x 1520@ 30fps (H.264/H.265)	2688 x 1520@ 30fps (H.264/H.265)
Video Imaging		
AEC weighting method	Full|Upper|Lower|Center|Spot|Left|Right|User Defined | AI Object | AI Person | AI Face	
Exposure compensation offset range	-2 to +2 f-stops	
Exposure range	1/32000| 1/20000| 1/12500| 1/10000| 1/8000| 1/4000| 1/2500| 1/2000| 1/1000| 1/800| 1/500| 1/400| 1/250| 1/200| 1/120|1/60 1/30 1/15|1/8|1/4|	
Default maximum exposure	1/8 sec.	
Default minimum exposure	1/32,000 sec.	
White balance	Auto Normal / Manual / Auto Wide	
Dynamic range method	Off/ Smart WDR/ True WDR2x /TrueWDR3x/	
Dynamic Range (Sensor Theoretical)	True multi shutter WDR up to 120dB	
Noise Reduction	Digital Noise Reduction 2D and 3D	
Defog	Yes	
Image stabilization EIS	Yes	
Flicker less	50/60 Hz or OFF	
Corridor mode (rotate 90º)	Yes	
Text overlay	Camera Name / Date Time / User Defined Test in one of 4 locations	
Privacy zones	10 user definable rectangular zones	
Audio		
Compression Format	G.711	G.711
Audio Input / Output / Interface	Built in Microphone Terminal block for Line in & audio Out	Built in Microphone Terminal block for Line in & audio Out
Built in Microphone	Yes	Yes
Alarm		

Alarm Input	2 x Alarm in	2 x Alarm in
Alarm Output	2 x Relay out (1A/80V)	2 x Relay out (1A/80V)
Alarm Interface	Terminal block	Terminal block
System Integrations		
USB Interface	Yes, Micro-USB in pan-base & rear. Not for simultaneous use	Yes, Micro-USB in pan-base & rear. Not for simultaneous use
Edge Storage		
On Board Storage	Micro SD/SDHC/SDXC card slot. Up to 2TB. ENCRYPTED STORAGE (card not incl)	Micro SD/SDHC/SDXC card slot. Up to 2TB. ENCRYPTED STORAGE (card not incl)
General		
Ethernet	IEEE 802.3, 10/100/1000 Base-T/TX, auto sensing, 1 x RJ45	IEEE 802.3, 10/100 Base-T/TX, auto sensing, 1 x RJ45
Reset / Default Button	2 Buttons (Hardware Reset & Factory Reset)	2 Buttons (Hardware Reset & Factory Reset)
Mechanical		
Casing	Bubble: PC, clear /smoke Dome Body: Aluminium Dome Base: Aluminium Pigtail: No Colour: White RAL 9003	Bubble: PC, clear /smoke Dome Body: Aluminium Dome Base: Aluminium Pigtail: No Colour: White RAL 9003
Weathering Resistance	IP67	IP67
Vandal Resistance	IK10	IK10
Dimension (HxWxD)	Ø138 x 143 mm	Ø138 x 143 mm
Weight	1.2kg (approx)	1.2kg (approx)
Electrical		
Power Source	Power over Ethernet (PoE) IEEE 802.3af Type 1 Class 3; 24 VAC	Power over Ethernet (PoE) IEEE 802.3af Type 1 Class 3; 24 VAC
Environmental		
Operating Temperature	-50°C to 65°C (1) IR LEDs will operate at 50% power if the temperature is between 49°C and 65°C.	-50°C to 65°C (1) IR LEDs will operate at 50% power if the temperature is between 49°C and 65°C.
Cold Start Temperature	-40°C	-40°C
Storage Temperature	-40°C to +60°C	-40°C to +60°C
Storage Humidity	90%, non-condensing	90%, non-condensing

RTC	Up to 24 hours	Up to 24 hours
Certification		
CE/FCC	Class A under 3 dB	Class A under 3 dB
RoHS	Yes	Yes
UL	UL62368/UL60950-22 62368/60950-22 CSA 22.2 No. 62368 CE: EN62368 / EN60950-22 IEC 62471 (IR LED)	UL62368/UL60950-22 62368/60950-22 CSA 22.2 No. 62368 CE: EN62368 / EN60950-22 IEC 62471 (IR LED)

The table below lists technical specifications of the PG4 8MP Dome cameras.

Camera Part Number	IPS08-D13-OI04	IPS08-D14-OI04
Camera Features		
Imager	Sony Colour CMOS IMX334, 1/1.8"	Sony Colour CMOS IMX334, 1/1.8"
Sensor Matrix (effective pixel)	Approx 8,290,000 pixels	Approx 8,290,000 pixels
Memory	RAM: LPDDR 2GB ROM: eMMC 4GB	RAM: LPDDR 2GB ROM: eMMC 4GB
Lens Spec	Motorised lens (all-new 4K optics), f3.6-11mm, F1.5-2.8	Motorised lens (8Mp optics), f6-22mm, F1.6
Optical Zoom	3x	3.5x
FOV	Wide: 102°(H) 56°(V) Tele: 46°(H) 26°(V)	Wide: 59°(H) 32°(V) Tele: 25°(H) 14°(V)
Iris Control	P-Iris (manual, auto)	P-Iris (manual, auto)
Focus Control	One Touch auto focus with user select-able target ROI area, manual, and auto-matic focus with zoom. Physical AF button on Dome.	One Touch auto focus with user select-able target ROI area, manual, and auto-matic focus with zoom. Physical AF button on Dome.
Min. Illumination	color = 0.22 lux B&W = 0.1 lux	color = 0.17 lux B&W = 0.08 lux
Day / Night control	Mechanical ICR	Mechanical ICR
Day / Night Switch control	Mode: Auto, colour, BW D/N switch sensitivity D/N switch time	Mode: Auto, colour, BW D/N switch sensitivity D/N switch time
IR Distance	Up to 50m	Up to 50m
IR Mode	On, off	On, off
Adaptive IR	Yes	Yes
Smart IR	No	No
Video Output	Micro HDMI Female connector on cam-era	Micro HDMI Female connector on cam-era
S/N Ratio	>50dB	>50dB
Image		
Exposure Profiles	Demo, Auto, Indoor, Outdoor,Shutter Priority, Iris priority, Gaming, License plate recognition (LPR) High, LPR Medium, LPR low, manual	Demo, Auto, Indoor, Outdoor,Shutter Priority, Iris priority, Gaming, License plate recognition (LPR) High, LPR Medium, LPR low, manual

WDR	True WDR 126 dB Technologies	True WDR 126 dB Technologies
Video		
Video Compression	H264, H264 Intellizip, H265, H265 Intellizip, MJPEG	H264, H264 Intellizip, H265, H265 Intellizip
Maximum Frame Rate	8MP @30 fps 2MP@60 fps	8MP @30 fps 2MP@60 fps
Resolution & Frame Rate	3840x2160 @ 30fps (H.264/H.265)	3840x2160 @ 30fps (H.264/H.265)
Video Imaging		
AEC weighting method	Full|Upper|Lower|Center|Spot|Left|Right|User Defined | AI Object | AI Person | AI Face	
Exposure compensation offset range	-2 to +2 f-stops	
Exposure range	1/32000| 1/20000| 1/12500| 1/10000| 1/8000| 1/4000| 1/2500| 1/2000| 1/1000| 1/800| 1/500| 1/400| 1/250| 1/200| 1/120|1/60 1/30 1/15|1/8|1/4|	
Default maximum exposure	1/8 sec.	
Default minimum exposure	1/32,000 sec.	
White balance	Auto Normal / Manual / Auto Wide	
Dynamic range method	Off/ Smart WDR/ True WDR2x /TrueWDR3x/	
Dynamic Range (Sensor Theoretical)	True multi shutter WDR up to 120dB	
Noise Reduction	Digital Noise Reduction 2D and 3D	
Defog	Yes	
Image stabilization EIS	Yes	
Flicker less	50/60 Hz or OFF	
Corridor mode (rotate 90º)	Yes	
Text overlay	Camera Name / Date Time / User Defined Test in one of 4 locations	
Privacy zones	10 user definable rectangular zones	
Audio		
Compression Format	G.711	G.711
Audio Input / Output / Interface	Built in Microphone Terminal block for Line in & audio Out	Built in Microphone Terminal block for Line in & audio Out
Built in Microphone	Yes	Yes
Alarm		

Alarm Input	2 x Alarm in	2 x Alarm in
Alarm Output	2 x Relay out (1A/80V)	2 x Relay out (1A/80V)
Alarm Interface	Terminal block	Terminal block
System Integrations		
USB Interface	Yes, Micro-USB in pan-base & rear. Not for simultaneous use	Yes, Micro-USB in pan-base & rear. Not for simultaneous use
Edge Storage		
On Board Storage	Micro SD/SDHC/SDXC card slot. Up to 2TB. ENCRYPTED STORAGE (card not incl)	Micro SD/SDHC/SDXC card slot. Up to 2TB. ENCRYPTED STORAGE (card not incl)
General		
Ethernet	IEEE 802.3, 10/100 Base-T/TX, auto sensing, 1 x RJ45	IEEE 802.3, 10/100 Base-T/TX, auto sensing, 1 x RJ45
Reset / Default Button	2 Buttons (Hardware Reset & Factory Reset)	2 Buttons (Hardware Reset & Factory Reset)
Mechanical		
Casing	Bubble: PC, clear /smoke Dome Body: Aluminium Dome Base: Aluminium Pigtail: No Colour: White RAL 9003	Bubble: PC, clear /smoke Dome Body: Aluminium Dome Base: Aluminium Pigtail: No Colour: White RAL 9003
Weathering Resistance	IP67	IP67
Vandal Resistance	IK10	IK10
Dimension (HxWxD)	Ø138 x 143 mm	Ø138 x 143 mm
Weight	1.2kg (approx)	1.2kg (approx)
Electrical		
Power Source	Power over Ethernet (PoE) IEEE 802.3af Type 1 Class 3; 24 VAC	Power over Ethernet (PoE) IEEE 802.3af Type 1 Class 3; 24 VAC
Environmental		
Operating Temperature	-50°C to 65°C (1) IR LEDs will operate at 50% power if the temperature is between 49°C and 65°C.	-50°C to 65°C (1) IR LEDs will operate at 50% power if the temperature is between 49°C and 65°C.
Cold Start Temperature	-40°C	-40°C
Storage Temperature	-40°C to +60°C	-40°C to +60°C
Storage Humidity	90%, non-condensing	90%, non-condensing

RTC	Up to 24 hours	Up to 24 hours
Certification		
CE/FCC	Class A under 3 dB	Class A under 3 dB
RoHS	Yes	Yes
UL	UL62368/UL60950-22 62368/60950-22 CSA 22.2 No. 62368 CE: EN62368 / EN60950-22 IEC 62471 (IR LED)	UL62368/UL60950-22 62368/60950-22 CSA 22.2 No. 62368 CE: EN62368 / EN60950-22 IEC 62471 (IR LED)

The table below lists technical specifications of the PG4 5MP Corner Dome camera.

Camera Part Number	IPS05-R10-OI04
General Features	
Sales description	Illustra Pro 5MP Corner, 2.3mm Fixed, IP66/67/68 IK11, TDN w/IR, WDR
Model name (ONVIF & iAPI3) 1	Pro4 5mp Corner
Camera body color	White RAL 9003
Bubble color	NA
Indoor/outdoor	Indoor/outdoor
Max. resolution	2560 x 1920 4:3
Lens	
Aperture Range	F/2.3
Focal length range	2.3 mm
Focal means	Fixed (factory focused at 1 m for DOF of .38 m to ∞)
Focal type	Fixed Manual
Focus type	Factory Focused
Auto focus	Fixed
Iris type	Fixed -Iris
Day/night	TDN
Horizontal angle of view	130°
Vertical angle of view	95°
Illuminator	
IR Distance	10m
Smart IR	No
Adaptive IR	N/A
Video Imaging	
AEC weighting method	Full|Upper|Lower|Center|Spot|Left|Right|User Defined | AI Object | AI Person | AI Face
Exposure compensation offset range	-2 to +2 f-stops
Exposure range	1/32000| 1/20000| 1/12500| 1/10000| 1/8000| 1/4000| 1/2500| 1/2000| 1/1000| 1/800| 1/500| 1/400| 1/250| 1/200| 1/120|1/60 1/30 1/15|1/8|1/4|
Default maximum exposure	1/8 sec.

Default minimum exposure	1/32,000 sec.
White balance	Auto Normal / Manual / Auto Wide
Dynamic range method	Off/ Smart WDR/ True WDR2x /TrueWDR3x/
Dynamic Range (Sensor Theoretical)	True multi shutter WDR up to 120dB
Noise Reduction	Digital Noise Reduction 2D and 3D
Defog	Yes
Image stabilization EIS	Yes
Flicker less	50/60 Hz or OFF
Corridor mode (rotate 90º)	Yes
Text overlay	Camera Name / Date Time / User Defined Test in one of 4 locations
Privacy zones	10 user definable rectangular zones
Video Codecs	
Configurable Streams	4 Streams
Frame rate range	1-60
Max resolution & rate	5MP @ 30ips / 2MP @60 fps
Resolutions available	2560 x 1920, 2048 x 1536, 1280 x 960, 800 x 600, 640 x 480, 480 x 360
Stream sharing	5 Streams
H.264	
Profile	High / Main
Smart Codec	IntelliZip® Selectable setting reduces BW automatically based on scene activity provided BW savings for uses having times of scene inactivity.
GOP range	1 - 180
GOP default	30
Rate control	(CBR/VBR/CVBR)
VBR quality settings	Highest, High, Med, Low, Lowest
CBR bit rate range	16 - 14,000
CVBR settings	Max Bitrate
H.265	
Profile	High
Smart Codec	IntelliZip® Selectable setting reduces BW automatically based on scene activity

	provided BW savings for uses having times of scene inactivity.
GOP range	1 - 150
GOP default	30
Rate control	(CBR/VBR/CVBR)
VBR quality settings	Highest, High, Med, Low, Lowest
CBR bit rate range	16 - 14,000
CVBR settings	500 - 14,000
MJPEG	
Quality	1 - 100
Video latency	<200ms
Audio	
Audio Features	Streaming Output, Streaming Input, Stored Audio Clips with Replay
Encoding method	G.711 u-law
Standard compliance	G711
Sampling rate	8khz
Sampling bits	16bit
Frequency response range	100 to 3,600 Hz
Input type	SE/Line/MIC
Input impedance	20K/attenuation = 0 dB
Maximum input level	2V p-p
Input connector	Terminal Block
Output type	Line, Speaker
Output type impedance	Hi impedance
Maximum output	2V p-p
Output connector	Terminal Block
Client interfaces	
Browsers supported & version	MS Edge, Firefox, Chrome, Safari
IP Network	
Ethernet NIC	IEEE 802.3, 10/100Base-T Ethernet, RJ45, auto sensing
Supported Protocols	TCP/IP, IPv4, IPv6, TCP, UDP, HTTP, FTP, DHCP, WS-Discovery, DNS, DDNS, RTP,

	RTCP, RTSP, TLS, Unicast, Multicast, NTP, ICMP, IGMP, SMTP, WS-Security, IEEE 802.1x, PEAP, EAP-TLS, EAPoL, SSH, HTTPS, SOAP, WSAddressing, CIFS, SNMP, UPNP, RTSP, LLDP
Base protocol	TCP/IP - RFC4614
Internet layer addressing	IPv4 - RFC791 IPv6 - RFC2460
Transport layer	TCP - RFC973 UDP - RFC768
Data transmission	HTTP - RFC2616 FTP - RFC959 SFTP
Network address configuration	DHCP - RFC2131 Zeroconf - RFC3927 Static IP address LLDP
Network name resolution	DNS - RFC5395 DDNS - RFC 2136
Discovery	WS-discovery (ONVIF and Illustra Connect), UPnP, mDNS
Streaming	RTP - RFC3550 RTCP - RFC3550 RTSP - RFC2326 Unicast Streaming Multicast Streaming - RFC1112 level 1
Time synchronization	NTP - RFC1305
Time synchronization poll rate	1 / minute
E-mail	SMTP - RFC5321 Authenticated SMTP - RFC4954
Authentication and security	TLS - RFC5246 v1.2 HTTPS (HTTP over TLS) - RFC2818 WS-Security Certificate Management Multi-level password protection IP address filtering HTTPS encryption Enhanced Security Feature Supports: One-Click Security Hardening, User Access Log, Validate Complex Credentials, Disabling Unused Protocols IEEE 802.1x including: PEAP, EAP-TLS, EAPoL
Users	5 simultaneous users
Firmware upgrade	ONVIF / browser / illustra Connect / Tyco Illustra mobile app
External Interface Protocol	AD illustra API 3.4.5 / SOAP - SOAP 1.2 / ONVIF Profile SGTM / WS-Addressing / WS-Eventing
Network management	SNMP v2c / v3
Special features	
Motion detection	Yes
Higher compression quality ROI	Yes
Tamper & Blur Detection	Yes
License plate detection	No
AI Person Counting	Yes

AI Privacy Mask	Yes
Higher compression quality ROI	Yes
Video Intelligence	No
AI Object classification	Yes
Defog	Yes
TWDR (multi exposure)	Yes
Local storage	Micro SD & SDXC slot up to 2TB; Class 10 or higher; Card not included.
User account access levels	Virtually unlimited user accounts, with Admin, Operator, and User levels
Enhanced Security	Enhanced Security Feature Provides: One-Click Security Hardening, User Access Log, Validates Complex Credentials, Disables Unused Protocols, Video Over HTTPS
IntelliZip®	Advanced H.264 & H.265 modes
Offline recording	Yes
Micro USB - Wifi configuration	Yes
Event alarms	
Event triggers	Motion Detection, Tamper &Blur Detection, , Face Detection, AI Object classification, Alarm Input, Tamper Switch, Network Loss, Temperature
Pre-alarm recording	Pre & Post Buffer 1-10 Sec
Event actions	Record to SD card / Snapshot / SMTP e-mail file transfer / FTP file transfer / CIFS / Auxiliary output / Audio clip playback / SIP Call / LED Illuminator
Alarm input	Two; Max 6V (High)/0.6V(LOW)
Auxiliary output	30V (Peak AC)/1A,NC/NO; PotoMOS Relay
Tamper switch	Yes (Alarm input 2)
IO Interfaces	
SD card	Micro SD/SDHC/SDXC slot up to 2TB; Class 10 or higher; Card not included.
Alarm inputs	1 + 1 Tamper Switch
Auxiliary outputs	1
Video output	No
IP Connector	RJ45
LED indicators	Red: Recording Status Indicator White: Illuminator or Warning Indicator
Reset buttons	2 Recessed reset pushbutton, 1 for reboot & 1 factory reset

I/O Connector	Inside enclosure: - RJ-45 IP connector - 2 pin terminal block 12Vdc / 24Vac I/O connector - 8 pin terminal block audio and Alarm I/O connector - Micro SD SDXC card slot - Recessed pushbutton for reboot - Recessed pushbutton for factory reset - Micro-USB
Power supply	
PoE	
Type	POE 802.3af Type 1 / POE+ 802.3at Type 2
PoE class	POE Class 3 / POE+ Class 4
Current draw amps	0.34A
Wattage	12.95W / 25.5W
12VDC	
Voltage range	DC12V+20/-10%
Current draw amps	1.4A
Power wattage	16.8W
24VAC	
Voltage range	AC24V+20/-10%
Line frequency range	50/ 60Hz
Current draw amps	1A
Power wattage	16.5W
Connector	2pin Mini type 3.5mm
Inrush current	26.3A (peak)
Design tolerance	24VAC (21.6 ~ 28.8VAC)
Mechanical	
Dimensions	208.29(W)x200.91(H)x57(D)mm (8.2(W)0x7.91(H)x2.24(D)in)
Weight	1.6 kg
Shipping weight	1.8Kg
Vandal rating	IK11
Environmental	
Operating Temperature	-20°C to +60°C @PoE and DC 12V '-40°C to +60°C @PoE+ and AC 24
Extended Temperature:	Yes
Operating humidity range	Up to 90% non-condensing

Storage temp. range	-40°C ~ +65°C
Water/dust intrusion	IP66/67/IP68, NEMA 4X
Regulatory	
Safety	UL60950-1; CAN/CSA-C22.2 No. 60950-1, BIS IS13252 Part 1:2010
Emissions	FCC Part 15 Class A; EN55032 Class A; AS/NZS CISPR 32 Class A; ICES-003/NMB-003 Class A
Immunity	EN 50130-4
Environmental	RoHS; WEEE, REACH

The table below lists the technical specifications of the Pro Gen 4 Indoor / Outdoor Bullet cameras.

	IPS02-B12-OIA4 = 2MP Standard Bullet **IPS04-B12-OIA4 = 4MP Standard Bullet** **IPS04-B13-OTA4 = 4MP Standard Bullet w/o IR** **IPS08-B13-OIA4 = 4MP Standard Bullet**
General	
Bubble color	White RAL 9003
Bubble color	NA
Indoor / Outdoor	Indoor/outdoor
Max resolution	IPS02-B12-OIA4 = 1920x1080 1080p 16:9 IPS04-B12-OIA4 = 2560x1920 IPS04-B13-OTA4 = 2560x1920 IPS08-B13-OIA4 = (3840 x 21600) 4K
Lens	
Aperture Range	IPS02-B12-OIA4 = F/1.4(W) ~ F/2.8(T) IPS04-B12-OIA4 = F/1.4(W) ~ F/2.8(T) IPS04-B13-OTA4 = F/1.4(W) ~ F/2.8(T) IPS08-B13-OIA4 = F/1.5(W) ~ F/2.8(T)
Focal length range	IPS02-B12-OIA4 = 3.13-9.77 mm IPS04-B12-OIA4 = 3.13-9.77 mm IPS04-B13-OTA4 = 3.13-9.77 mm IPS08-B13-OIA4 = 4.16- 9.41mm
Focal means	Gear Focus
Focal type	Gear
Focus type	One Touch auto focus , manual, and automatic focus with zoom.
Auto focus	Physical AF button
Iris type	P-Iris with Renesas control
Day / Night	TDN
Horizontal angle of view	IPS02-B12-OIA4 = 103.8°~33.8° IPS04-B12-OIA4 = 101°~31.8° IPS04-B13-OTA4 = 101°~31.8° IPS08-B13-OIA4 = 102°~47.8°

Vertical angle of view	IPS02-B12-OIA4 = 55°~19° IPS04-B12-OIA4 = 54°~18° IPS04-B13-OTA4 = 54°~18° IPS08-B13-OIA4 = 57.8°~27.8°
Illuminator	
IR Distance	IPS02-B12-OIA4 = 40M PoE 70M PoE+ IPS04-B12-OIA4 = 40M PoE 70M PoE+ IPS04-B13-OTA4 = N/A IPS08-B13-OIA4 = 40M PoE 70M PoE+
Smart IR	IPS02-B12-OIA4 = No IPS04-B12-OIA4 = No IPS04-B13-OTA4 = N/A IPS08-B13-OIA4 = No
Adaptive IR	IPS02-B12-OIA4 = Yes IPS04-B12-OIA4 = Yes IPS04-B13-OTA4 = N/A IPS08-B13-OIA4 = Yes
Video Imaging	
AEC weighting method	Full|Upper|Lower|Center|Spot|Left|Right|User Defined | AI Object | AI Person | AI Face
Exposure compensation offset range	-2 to +2 f-stops
Exposure range	1/32000| 1/20000| 1/12500| 1/10000| 1/8000| 1/4000| 1/2500| 1/2000| 1/1000| 1/800| 1/500| 1/400| 1/250| 1/200| 1/120|1/60 1/30 1/15|1/8|1/4|
Default maximum exposure	1/8 sec.
Default minimum exposure	1/32,000 sec.
White balance	Auto Normal / Manual / Auto Wide
Dynamic range method	Off/ Smart WDR/ True WDR2x /TrueWDR3x/
Dynamic Range (Sensor Theoretical)	True multi shutter WDR up to 120dB
Noise Reduction	Digital Noise Reduction 2D and 3D

Defog	Yes
Image stabilization EIS	Yes
Flicker less	50/60 Hz or None
Corridor mode (rotate 90º)	Yes
Text overlay	Camera Name / Date Time / User Defined Test in one of 4 locations
Privacy zones	10 user definable rectangular zones
Video Codecs	
Configurable Streams	4 streams
Frame rate range	1 to 60 ips
Max resolution & rate	IPS02-B12-OIA4 = 2MP @ 60ips IPS04-B12-OIA4 = 2MP @ 60ips, 4MP @ 30ips IPS04-B13-OTA4 = 2MP @ 60ips, 4MP @ 30ips IPS08-B13-OIA4 = 2MP @ 60ips, 4K @ 30ips
Resolutions available	See Appendix B - Stream Tables section
Stream sharing	5 streams
H.264	
Profile	High / Main
Smart Codec	IntelliZip® Selectable setting reduces BW automatically based on scene activity provided BW savings for uses having times of scene inactivity.
GOP range	1 - 180
GOP default	30
Rate control	(CBR/VBR/CVBR)
VBR quality settings	Highest, High, Med, Low, Lowest
CBR bit rate range	16 - 14,000
CVBR settings	Max Bitrate
H.265	

Profile	High
Smart Codec	IntelliZip® Selectable setting reduces BW automatically based on scene activity provided BW savings for uses having times of scene inactivity
GOP range	IPS02-B12-OIA4 = 150 IPS04-B12-OIA4 = 150 IPS04-B13-OTA4 = 150 IPS08-B13-OIA4 = 180
GOP default	30
Rate control	(CBR/VBR/CVBR)
VBR quality settings	Highest, High, Med, Low, Lowest
CBR bit rate range	16 - 14,000
CVBR settings	IPS02-B12-OIA4 = 500- 14,000 IPS04-B12-OIA4 = 500- 14,000 IPS04-B13-OTA4 = 500- 14,000 IPS08-B13-OIA4 = Max Bitrate
MJPEG	
Quality	1 - 100
Video latency	<200ms
Audio	
Audio Features	Streaming Output, Streaming Input, Stored Audio Clips with Replay
Encoding method	G.711 u-law & a-law
Standard compliance	G711
Sampling rate	8khz
Sampling bits	16bit
Frequency response range	100 to 3,600 Hz
Input type	SE/Line/MIC
Input impedance	20K/attenuation = 0 dB
Maximum input	2V p-p

level	
Input connector	Terminal Block
Output type impedance	Hi impedance
Maximum output	2V p-p
Output connector	Terminal Block
Client interfaces	
Browsers supported & version	MS Edge , Firefox, Chrome, Safari
IP Network	
Ethernet NIC	IEEE 802.3, 10/100Base-T Ethernet, RJ45, auto sensing
Supported Protocols	TCP/IP, IPv4, IPv6, TCP, UDP, HTTP, FTP, DHCP, WS-Discovery, DNS, DDNS, RTP, RTCP, RTSP, TLS, Unicast, Multicast, NTP, ICMP, IGMP, SMTP, WS-Security, IEEE 802.1x, PEAP, EAP-TLS, EAPoL, SSH, HTTPS, SOAP, WSAddressing, CIFS, SNMP, UPNP, RTSP, LLDP
Base protocol	TCP/IP - RFC4614
Internet layer addressing	IPv4 - RFC791 IPv6 - RFC2460
Transport layer	TCP - RFC973 UDP - RFC768
Data transmission	HTTP - RFC2616 FTP - RFC959 SFTP
Network address configuration	DHCP - RFC2131 Zeroconf - RFC3927 Static IP address LLDP
Network name resolution	DNS - RFC5395 DDNS - RFC 2136
Discovery	WS-discovery (ONVIF and Illustra Connect), UPnP, mDNS
Streaming	RTP - RFC3550 RTCP - RFC3550 RTSP - RFC2326

	Unicast Streaming Multicast Streaming - RFC1112 level 1
Time synchronization	NTP - RFC1305
Time synchronization poll rate	1 / minute
E-mail	SMTP - RFC5321 Authenticated SMTP - RFC4954
Authentication and security	TLS - RFC5246 v1.2 HTTPS (HTTP over TLS) - RFC2818 WS-Security Certificate Management Multi-level password protection IP address filtering HTTPS encryption Enhanced Security Feature Supports: One-Click Security Hardening, User Access Log, Validate Complex Credentials, Disabling Unused Protocols IEEE 802.1x including: PEAP, EAP-TLS, EAPoL
Users	5 simultaneous users
Firmware upgrade	ONVIF / browser / illustra Connect
External Interface Protocol	AD illustra API 3.4.5 SOAP - SOAP 1.2 ONVIF Profile SGTM WS-Addressing WS-Eventing
Network management	SNMP v2c / v3
Special features	
Motion detection	Yes
Face Detection	Yes
License plate detection	No
AI Person	Yes

Counting	
AI Privacy Mask	Yes
Higher compression quality ROI	Yes
Tamper & Blur detection	Yes
Video Intelligence	No
AI Object classification	Yes
Defog	Yes
TWDR (multi exposure)	Yes
Local storage	Micro SD & SDXC slot up to 2TB; Class 10 or higher; Card not included.
User account access levels	Virtually unlimited user accounts, with Admin, Operator, and User levels
Enhanced Security	Enhanced Security Feature Provides: One-Click Security Hardening, User Access Log, Validates Complex Credentials, Disables Unused Protocols
IntelliZip®	Advanced H.264 & H.265 modes
VideoEdge® TrickleStor	Yes
Event alarms	
Event triggers	Motion Detection, Tamper & Blur Detection, Face Detectiom , AI Object classification, Alarm Input, Network Loss, Temperature
Pre-alarm recording	1-10 Sec
Event actions	Record to SD card Snapshot SMTP e-mail file transfer FTP file transfer CIFS Auxiliary output Audio clip playback SIP Call
Alarm input	Two; Max 6V (High)/0.6V(LOW)

Auxiliary output	Two 30V (Peak AC)/1A,NC/NO; PotoMOS Relay
I/O Interfaces	
SD card	Micro SD/SDHC/SDXC slot up to 512GB; Class 10 or higher; Card not included.
Alarm inputs	2
Auxiliary out-puts	2
Video output	Yes (micro HDMI)
IP Connector	RJ45 connector
LED indicators	NA
Reset buttons	Recessed reset pushbutton for reboot & factory reset
I/O Connector	Inside enclosure: - RJ-45 IP connector - 8 pin push pin audio and I/O connector - Micro SD SDXC card slot - Recessed pushbutton for reboot - Recessed button for factory reset - MicroHDMI video output port (Required a optional accessory cable) -Micro-USB in PAN Base (Not for simultaneous use)
Power supply	
PoE	
Type	IEEE 802.3af Type 1 / IEEE 802.3at Type 2
PoE class	Class 4
Current draw amps	IPS02-B12-OIA4 = 0.27A / 0.39A IPS04-B12-OIA4 = 0.27A / 0.39A IPS04-B13-OTA4 = 0.2A IPS08-B13-OIA4 = 0.27A / 0.39A
Wattage	IPS02-B12-OIA4 = 12.95W / 18.72W IPS04-B12-OIA4 = 12.95W / 18.72W IPS04-B13-OTA4 = 9.55W EE IPS08-B13-OIA4 = 12.95W / 18.72W
24 VAC	
Voltage range	22 to 30 VAC, Class 2 LP EE
Current draw amps	IPS02-B12-OIA4 = 1.27A EE IPS04-B12-OIA4 = 1.27A EE IPS04-B13-OTA4 = 0.95A EE IPS08-B13-OIA4 = 1.27A EE
Power wattage	IPS02-B12-OIA4 = 21W EE IPS04-B12-OIA4 = 21W EE

	IPS04-B13-OTA4 = 16W EE IPS08-B13-OIA4 = 21W EE
Connector	2 pin mini type 3.5 mm push pin
In rush current	19.8A (peak)
Design tolerance	24VAC (22 to 30 VAC)
Environmental	
Operating temp. range	-50ºC to 60ºC (-58ºF to 140ºF)
Start up temp. range	IPS02-B12-OIA4 = -40ºC to 60ºC (-40ºF to 140ºF) IPS04-B12-OIA4 = -40ºC to 60ºC (-40ºF to 140ºF) IPS04-B13-OTA4 = -40ºC to 60ºC (-40ºF to 140ºF) IPS08-B13-OIA4 = -10ºC to 60ºC (14ºF to 140ºF)
Extended Temperature:	Yes
Operating humidity range	Up to 90% non-condensing
Storage temp. range	-40°C ~ +65°C
Water/dust intrusion	IP66/67, NEMA 4X
Mechanical	
Dimensions	Ø79.9x205mm(Ø3.15inx8.07in)
Weight	1.2KG
Shipping weight	3.2KG
Pan rotation angle	270°
Tilt angle	90°
Z-axis rotation	N/A
Vandal rating	IK10
Regulatory	
Safety	UL60950-1; CAN/CSA-C22.2 No. 60950-1, BIS IS13252 Part 1:2010
Emissions	FCC Part 15 Class A; EN55032 Class A; AS/NZS CISPR 32 Class A; ICES-003/NMB-003 Class A
Immunity	EN50130-4

Environmental	RoHS; WEEE, REACH

The table below lists the technical specifications of the Pro Gen 4 Indoor / Outdoor Bullet cameras.

	IPS02-B15-OIA4 = 2MP Tele Bullet **IPS04-B16-OIA4 = 4MP Tele Bullet** **IPS08-B16-OIA4 = 8MP Tele Bullet**
General	
Bubble color	White RAL 9003
Bubble color	NA
Indoor / Outdoor	Indoor/outdoor
Max resolution	IPS02-B15-OIA4 = 1920x1080 1080p 16:9 IPS04-B16-OIA4 = 2560x1920 IPS08-B16-OTA4 = (3840 x 21600) 4K
Lens	
Aperture Range	IPS02-B15-OIA4 = F/1.4(W) ~ F/2.8(T) IPS04-B16-OIA4 = F/1.5(W) ~ F/2.8(T) IPS04-B16-OTA4 = F/1.5(W) ~ F/2.8(T)
Focal length range	IPS02-B15-OIA4 = 3.13-9.77 mm IPS04-B15-OIA4 = 4.16-9.41 mm IPS04-B16-OTA4 = 4.16-9.41 mm
Focal means	Screw Focus
Focal type	Screw
Focus type	One Touch auto focus , manual, and automatic focus with zoom.
Auto focus	Physical AF button
Iris type	P-Iris with Renesas control
Day / Night	TDN
Horizontal angle of view	IPS02-B15-OIA4 = 65°~7° IPS04-B15-OIA4 = 21.8°~5.6° IPS04-B16-OTA4 = 34.2°~8.3°
Vertical angle of view	IPS02-B15-OIA4 = 39°~4° IPS04-B15-OIA4 = 16.2°~4.3° IPS04-B16-OTA4 = 20°~5.6°
Illuminator	
IR Distance	40M PoE

	70M PoE+
Smart IR	No
Adaptive IR	Yes
Video Imaging	
AEC weighting method	Full|Upper|Lower|Center|Spot|Left|Right|User Defined | AI Object | AI Person | AI Face
Exposure compensation offset range	-2 to +2 f-stops
Exposure range	1/32000| 1/20000| 1/12500| 1/10000| 1/8000| 1/4000| 1/2500| 1/2000| 1/1000| 1/800| 1/500| 1/400| 1/250| 1/200| 1/120|1/60 1/30 1/15|1/8|1/4|
Default maximum exposure	1/8 sec.
Default minimum exposure	1/32,000 sec.
White balance	Auto Normal / Manual / Auto Wide
Dynamic range method	Off/ Smart WDR/ True WDR2x /TrueWDR3x/
Dynamic Range (Sensor Theoretical)	True multi shutter WDR up to 120dB
Noise Reduction	Digital Noise Reduction 2D and 3D
Defog	Yes
Image stabilization EIS	Yes
Flicker less	50/60 Hz or OFF
Corridor mode (rotate 90º)	Yes
Text overlay	Camera Name / Date Time / User Defined Test in one of 4 locations
Privacy zones	10 user definable rectangular zones
Video Codecs	
Configurable Streams	4 streams
Frame rate range	1-60
Max resolution & rate	IPS02-B15-OIA4 = 2MP @ 60ips

	IPS04-B15-OIA4 = 2MP @ 60ips, 4MP @ IPS04-B16-OTA4 = 2MP @ 60ips, 4MP @ 30 ips
Resolutions available	See Appendix B - Stream Tables section
Stream sharing	5 Streams
H.264	
Profile	High / Main
Smart Codec	IntelliZip® Selectable setting reduces BW automatically based on scene activity provided BW savings for uses having times of scene inactivity.
GOP range	1 - 180
GOP default	30
Rate control	(CBR/VBR/CVBR)
VBR quality settings	Highest, High, Med, Low, Lowest
CBR bit rate range	16 - 14,000
CVBR settings	Max Bitrate
H.265	
Profile	High
Smart Codec	IntelliZip® Selectable setting reduces BW automatically based on scene activity provided BW savings for uses having times of scene inactivity
GOP range	1 - 180
GOP default	30
Rate control	(CBR/VBR/CVBR)
VBR quality settings	Highest, High, Med, Low, Lowest
CBR bit rate range	16 - 14,000
CVBR settings	Max Bitrate
MJPEG	
Quality	1 - 100
Video latency	<200ms

Audio	
Audio Features	Streaming Output, Streaming Input, Stored Audio Clips with Replay
Encoding method	G.711 u-law & a-law
Standard compliance	G711
Sampling rate	8khz
Sampling bits	16bit
Frequency response range	100 to 3,600 Hz
Input type	SE/Line/MIC
Input impedance	20K/attenuation = 0 dB
Maximum input level	2V p-p
Input connector	Terminal Block
Output type impedance	Hi impedance
Maximum output	2V p-p
Output connector	Terminal Block
Client interfaces	
Browsers supported & version	MS Edge , Firefox, Chrome, Safari
IP Network	
Ethernet NIC	IEEE 802.3, 10/100Base-T Ethernet, RJ45, auto sensing
Supported Protocols	TCP/IP, IPv4, IPv6, TCP, UDP, HTTP, FTP, DHCP, WS-Discovery, DNS, DDNS, RTP, RTCP, RTSP, TLS, Unicast, Multicast, NTP, ICMP, IGMP, SMTP, WS-Security, IEEE 802.1x, PEAP, EAP-TLS, EAPoL, SSH, HTTPS, SOAP, WSAddressing, CIFS, SNMP, UPNP, RTSP, LLDP
Base protocol	TCP/IP - RFC4614
Internet layer addressing	IPv4 - RFC791 IPv6 - RFC2460
Transport layer	TCP - RFC973 UDP - RFC768

Data transmission	HTTP - RFC2616 FTP - RFC959 SFTP
Network address configuration	DHCP - RFC2131 Zeroconf - RFC3927 Static IP address LLDP
Network name resolution	DNS - RFC5395 DDNS - RFC 2136
Discovery	WS-discovery (ONVIF and Illustra Connect), UPnP, mDNS
Streaming	RTP - RFC3550 RTCP - RFC3550 RTSP - RFC2326 Unicast Streaming Multicast Streaming - RFC1112 level 1
Time synchronization	NTP - RFC1305
Time synchronization poll rate	1 / minute
E-mail	SMTP - RFC5321 Authenticated SMTP - RFC4954
Authentication and security	TLS - RFC5246 v1.2 HTTPS (HTTP over TLS) - RFC2818 WS-Security Certificate Management Multi-level password protection IP address filtering HTTPS encryption Enhanced Security Feature Supports: One-Click Security Hardening, User Access Log, Validate Complex Credentials, Disabling Unused Protocols IEEE 802.1x including: PEAP, EAP-TLS, EAPoL
Users	5 simultaneous users
Firmware upgrade	ONVIF / browser / illustra Connect

External Interface Protocol	AD illustra API 3.4.5 SOAP - SOAP 1.2 ONVIF Profile SGTM WS-Addressing WS-Eventing
Network management	SNMP v2c / v3
Special features	
Motion detection	Yes
Face Detection	Yes
License plate detection	No
AI Person Counting	Yes
AI Privacy Mask	Yes
Higher compression quality ROI	No
Tamper & Blur detection	Yes
Video Intelligence	No
AI Object classification	Yes
Defog	Yes
TWDR (multi exposure)	Yes
Local storage	Micro SD & SDXC slot up to 512GB; Class 10 or higher; Card not included.
User account access levels	Virtually unlimited user accounts, with Admin, Operator, and User levels
Enhanced Security	Enhanced Security Feature Provides: One-Click Security Hardening, User Access Log, Validates Complex Credentials, Disables Unused Protocols
IntelliZip®	Advanced H.264 & H.265 modes
TrickleStor	Yes
Event alarms	
Event triggers	Motion Detection, Tamper & Blur Detection, Face Detectiom , AI Object classification, Alarm

	Input, Network Loss, Temperature
Pre-alarm recording	1-10 Sec
Event actions	Record to SD card Snapshot SMTP e-mail file transfer FTP file transfer CIFS Auxiliary output Audio clip playback SIP Call
Alarm input	Two; Max 6V (High)/0.6V(LOW)
Auxiliary output	Two 30V (Peak AC)/1A,NC/NO; PotoMOS Relay
I/O Interfaces	
SD card	Micro SD/SDHC/SDXC slot up to 512GB; Class 10 or higher; Card not included.
Alarm inputs	2
Auxiliary out-puts	2
Video output	Yes (micro HDMI)
IP Connector	RJ45 connector
LED indicators	NA
Reset buttons	Recessed reset pushbutton for reboot & factory reset
I/O Connector	Inside enclosure: - RJ-45 IP connector - 8 pin push pin audio and I/O connector - Micro SD SDXC card slot - Recessed pushbutton for reboot - Recessed button for factory reset - MicroHDMI video output port (Required a optional accessory cable) -Micro-USB in PAN Base (Not for simultaneous use)
Power supply	
PoE	
Type	IEEE 802.3af / IEEE 802.3at Type 2
PoE class	Class 4
Current draw amps	0.27A / 0.39A
Wattage	12.95W / 18.72W
24 VAC	

Voltage range	22 to 30 VAC, Class 2 LP EE
Current draw amps	1.27A EE
Power wattage	21W EE
Connector	2 pin mini type 3.5 mm push pin
In rush current	17.5A (peak)
Design tolerance	24VAC (22 to 30 VAC)
Environmental	
Operating temp. range	-50ºC to 60ºC (-58ºF to 140ºF)
Start up temp. range	-40ºC to 60ºC (-40ºF to 140ºF)
Extended Temperature:	Yes
Operating humidity range	Up to 90% non-condensing
Storage temp. range	-40°C ~ +65°C
Water/dust intrusion	IP66/67, NEMA 4X
Mechanical	
Dimensions	IPS02-B15-OIA4 = Ø79.9x217mm(Ø3.15inx8.54in) IPS04-B15-OIA4 = Ø79.9x235.5mm(Ø3.15inx9.27in) IPS04-B16-OTA4 = Ø79.9x235.5mm(Ø3.15inx9.27in)
Weight	IPS02-B15-OIA4 = 1.3KG IPS04-B15-OIA4 = 1.4KG IPS04-B16-OTA4 = 1.4KG
Shipping weight	3.3KG
Vandal rating	IK10
Regulatory	
Safety	UL60950-1; CAN/CSA-C22.2 No. 60950-1, BIS IS13252 Part 1:2010
Emissions	FCC Part 15 Class A; EN55032 Class A; AS/NZS CISPR 32 Class A; ICES-003/NMB-003 Class A

Immunity	EN50130-4
Environmental	RoHS; WEEE, REACH

The table below lists the technical specifications of the Pro Gen 4 Indoor / Outdoor Compact cameras.

	IPS02-C10-OIA4 = 2MP Compact **IPS04-c10-OIA4 = 4MP Compact** **IPS08-c10-OIA4 = 8MP Compact**
General	
Body color	White RAL 9003
Bubble color	NA
Indoor / Outdoor	Indoor/outdoor
Max resolution	IPS02-C10-OIA4 = 1920x1080 1080p 16:9 IPS04-C10-OIA4 = 2560x1920 4:3 IPS08-C10-OIA4 = (3840 x 21600) 4K 16:9
Lens	
Aperture Range	IPS02-C10-OIA4 = F/1.6 IPS04-C10-OIA4 = F/2.0 IPS08-C10-OTA4 = F/1.65
Focal length range	IPS02-C10-OIA4 = 3.03 mm IPS04-C10-OIA4 = 2.99 mm IPS08-C10-OTA4 = 4.46 mm
Focal means	IPS02-C10-OIA4 = Fixed (factory focused at 1 m for DOF of .50 m to ∞) IPS04-C10-OIA4 = Fixed (factory focused at 2 m for DOF of .72 m to ∞) IPS08-C10-OTA4 = Fixed (factory focused at 3 m for DOF of 1.50 m to ∞)
Focal type	Fixed Manual
Focus type	Factory Focused
Auto focus	Fixed
Iris type	Fixed -Iris
Day / Night	TDN
Horizontal angle of view	IPS02-C10-OIA4 = 105.3° IPS04-C10-OIA4 = 100.8° IPS08-C10-OTA4 = 109.9°
Vertical angle of view	IPS02-C10-OIA4 = 58.9° IPS04-C10-OIA4 = 74.7°

	IPS04-C10-OTA4 = 56.7°
Illuminator	
IR Distance	20m
Smart IR	No
Adaptive IR	N/A
Video Imaging	
AEC weighting method	Full|Upper|Lower|Center|Spot|Left|Right|User Defined | AI Object | AI Person | AI Face
Exposure compensation offset range	-2 to +2 f-stops
Exposure range	1/32000| 1/20000| 1/12500| 1/10000| 1/8000| 1/4000| 1/2500| 1/2000| 1/1000| 1/800| 1/500| 1/400| 1/250| 1/200| 1/120|1/60 1/30 1/15|1/8|1/4|
Default maximum exposure	1/8 sec.
Default minimum exposure	1/32,000 sec.
White balance	Auto Normal / Manual / Auto Wide
Dynamic range method	Off/ Smart WDR/ True WDR2x /TrueWDR3x/
Dynamic Range (Sensor Theoretical)	True multi shutter WDR up to 120dB
Noise Reduction	Digital Noise Reduction 2D and 3D
Defog	N/A
Image stabilization EIS	Yes
Flicker less	50/60 Hz or OFF
Corridor mode (rotate 90º)	Yes
Text overlay	Camera Name / Date Time / User Defined Test in one of 4 locations
Privacy zones	8 user definable rectangular zones
Video Codecs	
Configurable Streams	4 streams
Frame rate	1-60

range	
Max resolution & rate	IPS02-C10-OIA4 = 2MP @ 60ips IPS04-C10-OIA4 = 4MP @ 30ips & 2MP @60ips IPS08-C10-OTA4 = 8MP @ 30ips & 2MP @60ips
Resolutions available	See Appendix B - Stream Tables section
Stream sharing	5 Streams
H.264	
Profile	High / Main
Smart Codec	IntelliZip® Selectable setting reduces BW automatically based on scene activity provided BW savings for uses having times of scene inactivity.
GOP range	1 - 180
GOP default	30
Rate control	(CBR/VBR/CVBR)
VBR quality settings	Highest, High, Med, Low, Lowest
CBR bit rate range	16 - 14,000
CVBR settings	Max Bitrate
H.265	
Profile	High
Smart Codec	IntelliZip® Selectable setting reduces BW automatically based on scene activity provided BW savings for uses having times of scene inactivity
GOP range	1 - 150
GOP default	30
Rate control	(CBR/VBR/CVBR)
VBR quality settings	Highest, High, Med, Low, Lowest
CBR bit rate range	16 - 14,000
CVBR settings	500 - 14,000
MJPEG	

Quality	1 - 100
Video latency	<200ms
Audio	
Audio Features	Streaming Output, Streaming Input, Stored Audio Clips with Replay streaming input
Encoding method	G.711 u
Standard compliance	G711
Sampling rate	8khz
Sampling bits	24bit
Frequency response range	100 to 3,600 Hz
Input type	MIC
Input connector	No
Client interfaces	
Browsers supported & version	MS Edge , Firefox, Chrome, Safari
IP Network	
Ethernet NIC	IEEE 802.3, 10/100Base-T Ethernet, RJ45, auto sensing
Supported Protocols	TCP/IP, IPv4, IPv6, TCP, UDP, HTTP, FTP, DHCP, WS-Discovery, DNS, DDNS, RTP, RTCP, RTSP, TLS, Unicast, Multicast, NTP, ICMP, IGMP, SMTP, WS-Security, IEEE 802.1x, PEAP, EAP-TLS, EAPoL, SSH, HTTPS, SOAP, WSAddressing, CIFS, SNMP, UPNP, RTSP, LLDP
Base protocol	TCP/IP - RFC4614
Internet layer addressing	IPv4 - RFC791 IPv6 - RFC2460
Transport layer	TCP - RFC973 UDP - RFC768
Data transmission	HTTP - RFC2616 FTP - RFC959 SFTP
Network address configuration	DHCP - RFC2131 Zeroconf - RFC3927 Static IP address LLDP

Network name resolution	DNS - RFC5395 DDNS - RFC 2136
Discovery	WS-discovery (ONVIF and Illustra Connect), UPnP, mDNS
Streaming	RTP - RFC3550 RTCP - RFC3550 RTSP - RFC2326 Unicast Streaming Multicast Streaming - RFC1112 level 1
Time synchronization	NTP - RFC1305
Time synchronization poll rate	1 / minute
E-mail	SMTP - RFC5321 Authenticated SMTP - RFC4954
Authentication and security	TLS - RFC5246 v1.2 HTTPS (HTTP over TLS) - RFC2818 WS-Security Certificate Management Multi-level password protection IP address filtering HTTPS encryption Enhanced Security Feature Supports: One-Click Security Hardening, User Access Log, Validate Complex Credentials, Disabling Unused Protocols IEEE 802.1x including: PEAP, EAP-TLS, EAPoL
Users	5 simultaneous users
Firmware upgrade	ONVIF / browser / illustra Connect
External Interface Protocol	AD illustra API 3.4.5 SOAP - SOAP 1.2 ONVIF Profile SGTM WS-Addressing WS-Eventing
Network management	SNMP v2c / v3

Special features	
Motion detection	Yes
Face Detection	Yes
License plate detection	No
AI Person Counting	Yes
AI Privacy Mask	Yes
Higher compression quality ROI	Yes
Tamper & Blur detection	Yes
Video Intelligence	No
AI Object classification	Yes
Defog	Yes
TWDR (multi exposure)	Yes
Local storage	Micro SD & SDXC slot up to 512GB; Class 10 or higher; Card not included.
User account access levels	Virtually unlimited user accounts, with Admin, Operator, and User levels
Enhanced Security	Enhanced Security Feature Provides: One-Click Security Hardening, User Access Log, Validates Complex Credentials, Disables Unused Protocols
IntelliZip®	Advanced H.264 & H.265 modes
TrickleStor	Yes
Event alarms	
Event triggers	Motion Detection, Tamper & Blur Detection, Face Detectiom , AI Object classification, Alarm Input, Network Loss, Temperature
Pre-alarm recording	Pre & Post Buffer 1-10 Sec
Event actions	Record to SD card Snapshot SMTP e-mail file transfer FTP file transfer

	CIFS
Alarm input	No
Auxiliary output	No
I/O Interfaces	
SD card	Micro SD/SDHC/SDXC slot up to 2TB; Class 10 or higher; Card not included.
Alarm inputs	No
Auxiliary outputs	No
Video output	Yes (micro HDMI)
IP Connector	RJ45 connector
LED indicators	No
Reset buttons	Recessed reset pushbutton for reboot & factory reset
I/O Connector	Inside enclosure: - RJ-45 IP connector - Micro SD SDXC card slot - Recessed pushbutton for reboot - Recessed button for factory reset - Micro-USB - Debug port
Power supply	
PoE	
Type	POE 802.3af Type 1
PoE class	POE Class 3
Current draw amps	0.27A
Wattage	12.95W
Environmental	
Operating temp. range	-40°C to +60°C @PoE
Start up temp. range	-40ºC to 60ºC (-40ºF to 140ºF)
Extended Temperature:	Yes
Operating humidity range	Up to 90% non-condensing
Storage temp. range	-40°C ~ +60°C
Water/dust intrusion	IP66/67, NEMA 4X
Mechanical	

Dimensions	Ø121x78(H) mm Ø4.76x3.07(H) inch
Weight	0.55 kg
Shipping weight	7.2 kg
Vandal rating	IK10
Regulatory	
Safety	CB/UL/NEMA 4X/BIS
Emissions	CE/FCC/RCM
Immunity	EN50121-4
Environmental	RoHS; WEEE, REACH

The table below lists technical specifications of the PG4 5MP LPR Dome camera.

Camera Part Number	**IPS05-D12-LPR4**
Camera Features	
Imager	Sony Colour CMOS IMX335, 1/2.8"
Sensor Matrix (effective pixel)	Approx 5,040,000 pixels
Memory	RAM: LPDDR 2GB ROM: eMMC 4GB
Lens Spec	Motorised lens (6Mp optics), f 2.7-13.5mm, F1.4~2.8
Optical Zoom	5x
FOV	Wide: 101°(H) 54°(V) Tele : 32°(H) 18°(V)
Iris Control	P-Iris (manual, auto)
Focus Control	One Touch auto focus with user selectable target ROI area, manual, and automatic focus with zoom. Physical AF button on Dome.
Min. Illumination	color = 0.12 lux B&W = 0.05 lux
Day / Night control	Mechanical ICR
Day / Night Switch control	Mode: Auto, colour, BW D/N switch sensitivity D/N switch time
IR Distance	Up to 50m
IR Mode	On, off
Adaptive IR	Yes
Smart IR	Yes
Video Output	Micro HDMI Female connector on camera
S/N Ratio	>50dB
Image	
Exposure Profiles	Demo, Auto, Indoor, Outdoor,Shutter Priority, Iris priority, Gaming, License plate recognition (LPR) High, LPR Medium, LPR low, manual
WDR	True WDR 126 dB Technologies
Video	
Video Compression	H264, H264 Intellizip, H265, H265 Intellizip
Maximum Frame Rate	5MP @30 fps 2MP@60 fps

Resolution & Frame Rate	2688 x 1520@ 30fps (H.264/H.265)
Audio	
Compression Format	G.711
Audio Input / Output / Interface	Built in Microphone Terminal block for Line in & audio Out
Built in Microphone	Yes
Alarm	
Alarm Input	2 x Alarm in
Alarm Output	2 x Relay out (1A/80V)
Alarm Interface	Terminal block
System Integrations	
USB Interface	Yes, Micro-USB in pan-base & rear. Not for simultaneous use
Edge Storage	
On Board Storage	Micro SD/SDHC/SDXC card slot. Up to 512GB. ENCRYPTED STORAGE (card not incl)
General	
Ethernet	IEEE 802.3, 10/100/1000 Base-T/TX, auto sensing, 1 x RJ45
Reset / Default Button	2 Buttons (Hardware Reset & Factory Reset)
Mechanical	
Casing	Bubble: PC, clear /smoke Dome Body: Aluminium Dome Base: Aluminium Pigtail: No Colour: White RAL 9003
Weathering Resistance	IP67
Vandal Resistance	IK10
Dimension (HxWxD)	Ø138 x 143 mm
Weight	1.2kg (approx)
Electrical	
Power Source	Power over Ethernet (PoE) IEEE 802.3af Type 1 Class 3; 24 VAC
Environmental	

Operating Temperature	-50°C to 65°C (1) IR LEDs will operate at 50% power if the temperature is between 49°C and 65°C.
Cold Start Temperature	-40°C
Storage Temperature	-40°C to +60°C
Storage Humidity	90%, non-condensing
RTC	Up to 24 hours
Certification	
CE/FCC	Class A under 3 dB
RoHS	Yes
UL	UL62368/UL60950-22 62368/60950-22 CSA 22.2 No. 62368 CE: EN62368 / EN60950-22 IEC 62471 (IR LED)

The table below lists the technical specifications of the PG4 5MP LPR Bullet camera.

Camera Part Number	**IPS05-B12-LPR4**
General	
Bubble color	White RAL 9003
Bubble color	NA
Indoor / Outdoor	Indoor/outdoor
Max resolution	2560x1920
Lens	
Aperture Range	F/1.4(W) ~ F/2.8(T)
Focal length range	3.13-9.77 mm
Focal means	Gear Focus
Focal type	Gear
Focus type	One Touch auto focus , manual, and automatic focus with zoom.
Auto focus	Physical AF button
Iris type	P-Iris with Renesas control
Day / Night	TDN
Horizontal angle of view	101°~31.8°
Vertical angle of view	54°~18°
Illuminator	
IR Distance	40M PoE 70M PoE+
Smart IR	No
Adaptive IR	Yes
Video Imaging	
AEC weighting method	Full|Upper|Lower|Center|Spot|Left|Right|User Defined | AI Object | AI Person | AI Face
Exposure com-pensation offset range	-2 to +2 f-stops
Exposure range	1/32000| 1/20000| 1/12500| 1/10000| 1/8000| 1/4000| 1/2500| 1/2000| 1/1000| 1/800| 1/500| 1/400| 1/250| 1/200| 1/120|1/60 1/30 1/15|1/8|1/4|
Default max-	1/8 sec.

imum exposure	
Default min-imum exposure	1/32,000 sec.
White balance	Auto Normal / Manual / Auto Wide
Dynamic range method	Off/ Smart WDR/ True WDR2x /TrueWDR3x/
Dynamic Range (Sensor The-oretical)	True multi shutter WDR up to 120dB
Noise Reduc-tion	Digital Noise Reduction 2D and 3D
Defog	Yes
Image sta-bilization EIS	Yes
Flicker less	50/60 Hz or None
Corridor mode (rotate 90º)	Yes
Text overlay	Camera Name / Date Time / User Defined Test in one of 4 locations
Privacy zones	10 user definable rectangular zones
Video Codecs	
Configurable Streams	4 streams
Frame rate range	1 to 60 ips
Max resolution & rate	5MP @ 60ips, 4MP @ 30ips
Resolutions available	See Appendix B - Stream Tables section
Stream sharing	5 streams
H.264	
Profile	High / Main
Smart Codec	IntelliZip® Selectable setting reduces BW automatically based on scene activity provided BW savings for uses having times of scene inactivity.
GOP range	1 - 180
GOP default	30
Rate control	(CBR/VBR/CVBR)

VBR quality settings	Highest, High, Med, Low, Lowest
CBR bit rate range	16 - 14,000
CVBR settings	Max Bitrate
H.265	
Profile	High
Smart Codec	IntelliZip® Selectable setting reduces BW automatically based on scene activity provided BW savings for uses having times of scene inactivity
GOP range	150
GOP default	30
Rate control	(CBR/VBR/CVBR)
VBR quality settings	Highest, High, Med, Low, Lowest
CBR bit rate range	16 - 14,000
CVBR settings	500- 14,000
MJPEG	
Quality	1 - 100
Video latency	<200ms
Audio	
Audio Features	Streaming Output, Streaming Input, Stored Audio Clips with Replay
Encoding method	G.711 u-law & a-law
Standard compliance	G711
Sampling rate	8khz
Sampling bits	16bit
Frequency response range	100 to 3,600 Hz
Input type	SE/Line/MIC
Input impedance	20K/attenuation = 0 dB
Maximum input level	2V p-p

Input connector	Terminal Block
Output type impedance	Hi impedance
Maximum output	2V p-p
Output connector	Terminal Block
Client interfaces	
Browsers supported & version	MS Edge , Firefox, Chrome, Safari
IP Network	
Ethernet NIC	IEEE 802.3, 10/100Base-T Ethernet, RJ45, auto sensing
Supported Protocols	TCP/IP, IPv4, IPv6, TCP, UDP, HTTP, FTP, DHCP, WS-Discovery, DNS, DDNS, RTP, RTCP, RTSP, TLS, Unicast, Multicast, NTP, ICMP, IGMP, SMTP, WS-Security, IEEE 802.1x, PEAP, EAP-TLS, EAPoL, SSH, HTTPS, SOAP, WSAddressing, CIFS, SNMP, UPNP, RTSP, LLDP
Base protocol	TCP/IP - RFC4614
Internet layer addressing	IPv4 - RFC791 IPv6 - RFC2460
Transport layer	TCP - RFC973 UDP - RFC768
Data transmission	HTTP - RFC2616 FTP - RFC959 SFTP
Network address configuration	DHCP - RFC2131 Zeroconf - RFC3927 Static IP address LLDP
Network name resolution	DNS - RFC5395 DDNS - RFC 2136
Discovery	WS-discovery (ONVIF and Illustra Connect), UPnP, mDNS
Streaming	RTP - RFC3550 RTCP - RFC3550 RTSP - RFC2326 Unicast Streaming

	Multicast Streaming - RFC1112 level 1
Time synchronization	NTP - RFC1305
Time synchronization poll rate	1 / minute
E-mail	SMTP - RFC5321 Authenticated SMTP - RFC4954
Authentication and security	TLS - RFC5246 v1.2 HTTPS (HTTP over TLS) - RFC2818 WS-Security Certificate Management Multi-level password protection IP address filtering HTTPS encryption Enhanced Security Feature Supports: One-Click Security Hardening, User Access Log, Validate Complex Credentials, Disabling Unused Protocols IEEE 802.1x including: PEAP, EAP-TLS, EAPoL
Users	5 simultaneous users
Firmware upgrade	ONVIF / browser / illustra Connect
External Interface Protocol	AD illustra API 3.4.5 SOAP - SOAP 1.2 ONVIF Profile SGTM WS-Addressing WS-Eventing
Network management	SNMP v2c / v3
Special features	
Motion detection	Yes
Face Detection	Yes
License plate detection	No
AI Person Counting	Yes

AI Privacy Mask	Yes
Higher compression quality ROI	Yes
Tamper & Blur detection	Yes
Video Intelligence	No
AI Object classification	Yes
Defog	Yes
TWDR (multi exposure)	Yes
Local storage	Micro SD & SDXC slot up to 2TB; Class 10 or higher; Card not included.
User account access levels	Virtually unlimited user accounts, with Admin, Operator, and User levels
Enhanced Security	Enhanced Security Feature Provides: One-Click Security Hardening, User Access Log, Validates Complex Credentials, Disables Unused Protocols
IntelliZip®	Advanced H.264 & H.265 modes
VideoEdge® TrickleStor	Yes
Event alarms	
Event triggers	Motion Detection, Tamper & Blur Detection, Face Detection, AI Object classification, Alarm Input, Network Loss, Temperature
Pre-alarm recording	1-10 Sec
Event actions	Record to SD card Snapshot SMTP e-mail file transfer FTP file transfer CIFS Auxiliary output Audio clip playback SIP Call
Alarm input	Two; Max 6V (High)/0.6V(LOW)
Auxiliary output	Two 30V (Peak AC)/1A,NC/NO; PotoMOS Relay

I/O Interfaces	
SD card	Micro SD/SDHC/SDXC slot up to 512GB; Class 10 or higher; Card not included.
Alarm inputs	2
Auxiliary outputs	2
Video output	Yes (micro HDMI)
IP Connector	RJ45 connector
LED indicators	NA
Reset buttons	Recessed reset pushbutton for reboot & factory reset
I/O Connector	Inside enclosure: - RJ-45 IP connector - 8 pin push pin audio and I/O connector - Micro SD SDXC card slot - Recessed pushbutton for reboot - Recessed button for factory reset - MicroHDMI video output port (Required a optional accessory cable) -Micro-USB in PAN Base (Not for simultaneous use)
Power supply	
PoE	
Type	IEEE 802.3af Type 1 / IEEE 802.3at Type 2
PoE class	Class 4
Current draw amps	0.27A / 0.39A
Wattage	12.95W / 18.72W
24 VAC	
Voltage range	22 to 30 VAC, Class 2 LP EE
Current draw amps	1.27A EE
Power wattage	21W EE
Connector	2 pin mini type 3.5 mm push pin
In rush current	19.8A (peak)
Design tolerance	24VAC (22 to 30 VAC)
Environmental	
Operating temp. range	-50ºC to 60ºC (-58ºF to 140ºF)
Start up temp. range	-40ºC to 60ºC (-40ºF to 140ºF)
Extended Tem-	Yes

perature:	
Operating humidity range	Up to 90% non-condensing
Storage temp. range	-40°C ~ +65°C
Water/dust intrusion	IP66/67, NEMA 4X
Mechanical	
Dimensions	Ø79.9x205mm(Ø3.15inx8.07in)
Weight	1.2KG
Shipping weight	3.2KG
Pan rotation angle	270°
Tilt angle	90°
Z-axis rotation	N/A
Vandal rating	IK10
Regulatory	
Safety	UL60950-1; CAN/CSA-C22.2 No. 60950-1, BIS IS13252 Part 1:2010
Emissions	FCC Part 15 Class A; EN55032 Class A; AS/NZS CISPR 32 Class A; ICES-003/NMB-003 Class A
Immunity	EN50130-4
Environmental	RoHS; WEEE, REACH

The table below lists the technical specifications of the PG4 5MP LPR Tele Bullet camera.

Camera Part Number	**IPS05-B16-LPR4**
General	
Bubble color	White RAL 9003
Bubble color	NA
Indoor / Outdoor	Indoor/outdoor
Max resolution	2560x1920
Lens	
Aperture Range	F/1.5(W) ~ F/2.8(T)
Focal length range	13-55 mm
Focal means	Gear Focus
Focal type	Gear
Focus type	One Touch auto focus , manual, and automatic focus with zoom.
Auto focus	Physical AF button
Iris type	P-Iris with Renesas control
Day / Night	TDN
Horizontal angle of view	21.8°~5.6°
Vertical angle of view	16.2°~4.3°
Illuminator	
IR Distance	40M PoE 70M PoE+
Smart IR	No
Adaptive IR	Yes
Video Imaging	
AEC weighting method	Full|Upper|Lower|Center|Spot|Left|Right|User Defined | AI Object | AI Person | AI Face
Exposure com-pensation offset range	-2 to +2 f-stops
Exposure range	1/32000| 1/20000| 1/12500| 1/10000| 1/8000| 1/4000| 1/2500| 1/2000| 1/1000| 1/800| 1/500| 1/400| 1/250| 1/200| 1/120|1/60 1/30 1/15|1/8|1/4|
Default max-	1/8 sec.

imum exposure	
Default min-imum exposure	1/32,000 sec.
White balance	Auto Normal / Manual / Auto Wide
Dynamic range method	Off/ Smart WDR/ True WDR2x /TrueWDR3x/
Dynamic Range (Sensor The-oretical)	True multi shutter WDR up to 120dB
Noise Reduc-tion	Digital Noise Reduction 2D and 3D
Defog	Yes
Image sta-bilization EIS	Yes
Flicker less	50/60 Hz or None
Corridor mode (rotate 90º)	Yes
Text overlay	Camera Name / Date Time / User Defined Test in one of 4 locations
Privacy zones	10 user definable rectangular zones
Video Codecs	
Configurable Streams	4 streams
Frame rate range	1 to 60 ips
Max resolution & rate	5MP @ 60ips, 4MP @ 30ips
Resolutions available	See Appendix B - Stream Tables section
Stream sharing	5 streams
H.264	
Profile	High / Main
Smart Codec	IntelliZip® Selectable setting reduces BW automatically based on scene activity provided BW savings for uses having times of scene inactivity.
GOP range	1 - 180
GOP default	30
Rate control	(CBR/VBR/CVBR)

VBR quality settings	Highest, High, Med, Low, Lowest
CBR bit rate range	16 - 14,000
CVBR settings	Max Bitrate
H.265	
Profile	High
Smart Codec	IntelliZip® Selectable setting reduces BW automatically based on scene activity provided BW savings for uses having times of scene inactivity
GOP range	150
GOP default	30
Rate control	(CBR/VBR/CVBR)
VBR quality settings	Highest, High, Med, Low, Lowest
CBR bit rate range	16 - 14,000
CVBR settings	500- 14,000
MJPEG	
Quality	1 - 100
Video latency	<200ms
Audio	
Audio Features	Streaming Output, Streaming Input, Stored Audio Clips with Replay
Encoding method	G.711 u-law & a-law
Standard compliance	G711
Sampling rate	8khz
Sampling bits	16bit
Frequency response range	100 to 3,600 Hz
Input type	SE/Line/MIC
Input impedance	20K/attenuation = 0 dB
Maximum input level	2V p-p

Input connector	Terminal Block
Output type impedance	Hi impedance
Maximum output	2V p-p
Output connector	Terminal Block
Client interfaces	
Browsers supported & version	MS Edge , Firefox, Chrome, Safari
IP Network	
Ethernet NIC	IEEE 802.3, 10/100Base-T Ethernet, RJ45, auto sensing
Supported Protocols	TCP/IP, IPv4, IPv6, TCP, UDP, HTTP, FTP, DHCP, WS-Discovery, DNS, DDNS, RTP, RTCP, RTSP, TLS, Unicast, Multicast, NTP, ICMP, IGMP, SMTP, WS-Security, IEEE 802.1x, PEAP, EAP-TLS, EAPoL, SSH, HTTPS, SOAP, WSAddressing, CIFS, SNMP, UPNP, RTSP, LLDP
Base protocol	TCP/IP - RFC4614
Internet layer addressing	IPv4 - RFC791 IPv6 - RFC2460
Transport layer	TCP - RFC973 UDP - RFC768
Data transmission	HTTP - RFC2616 FTP - RFC959 SFTP
Network address configuration	DHCP - RFC2131 Zeroconf - RFC3927 Static IP address LLDP
Network name resolution	DNS - RFC5395 DDNS - RFC 2136
Discovery	WS-discovery (ONVIF and Illustra Connect), UPnP, mDNS
Streaming	RTP - RFC3550 RTCP - RFC3550 RTSP - RFC2326 Unicast Streaming

	Multicast Streaming - RFC1112 level 1
Time synchronization	NTP - RFC1305
Time synchronization poll rate	1 / minute
E-mail	SMTP - RFC5321 Authenticated SMTP - RFC4954
Authentication and security	TLS - RFC5246 v1.2 HTTPS (HTTP over TLS) - RFC2818 WS-Security Certificate Management Multi-level password protection IP address filtering HTTPS encryption Enhanced Security Feature Supports: One-Click Security Hardening, User Access Log, Validate Complex Credentials, Disabling Unused Protocols IEEE 802.1x including: PEAP, EAP-TLS, EAPoL
Users	5 simultaneous users
Firmware upgrade	ONVIF / browser / illustra Connect
External Interface Protocol	AD illustra API 3.4.5 SOAP - SOAP 1.2 ONVIF Profile SGTM WS-Addressing WS-Eventing
Network management	SNMP v2c / v3
Special features	
Motion detection	Yes
Face Detection	Yes
License plate detection	No
AI Person Counting	Yes

AI Privacy Mask	Yes
Higher compression quality ROI	Yes
Tamper & Blur detection	Yes
Video Intelligence	No
AI Object classification	Yes
Defog	Yes
TWDR (multi exposure)	Yes
Local storage	Micro SD & SDXC slot up to 2TB; Class 10 or higher; Card not included.
User account access levels	Virtually unlimited user accounts, with Admin, Operator, and User levels
Enhanced Security	Enhanced Security Feature Provides: One-Click Security Hardening, User Access Log, Validates Complex Credentials, Disables Unused Protocols
IntelliZip®	Advanced H.264 & H.265 modes
VideoEdge® TrickleStor	Yes
Event alarms	
Event triggers	Motion Detection, Tamper & Blur Detection, Face Detection , AI Object classification, Alarm Input, Network Loss, Temperature
Pre-alarm recording	1-10 Sec
Event actions	Record to SD card Snapshot SMTP e-mail file transfer FTP file transfer CIFS Auxiliary output Audio clip playback SIP Call
Alarm input	Two; Max 6V (High)/0.6V(LOW)
Auxiliary output	Two 30V (Peak AC)/1A,NC/NO; PotoMOS Relay

I/O Interfaces	
SD card	Micro SD/SDHC/SDXC slot up to 512GB; Class 10 or higher; Card not included.
Alarm inputs	2
Auxiliary outputs	2
Video output	Yes (micro HDMI)
IP Connector	RJ45 connector
LED indicators	NA
Reset buttons	Recessed reset pushbutton for reboot & factory reset
I/O Connector	Inside enclosure: - RJ-45 IP connector - 8 pin push pin audio and I/O connector - Micro SD SDXC card slot - Recessed pushbutton for reboot - Recessed button for factory reset - MicroHDMI video output port (Required a optional accessory cable) -Micro-USB in PAN Base (Not for simultaneous use)
Power supply	
PoE	
Type	IEEE 802.3af Type 1 / IEEE 802.3at Type 2
PoE class	Class 4
Current draw amps	0.27A / 0.39A
Wattage	12.95W / 18.72W
24 VAC	
Voltage range	22 to 30 VAC, Class 2 LP EE
Current draw amps	1.27A EE
Power wattage	21W EE
Connector	2 pin mini type 3.5 mm push pin
In rush current	19.8A (peak)
Design tolerance	24VAC (22 to 30 VAC)
Environmental	
Operating temp. range	-50ºC to 60ºC (-58ºF to 140ºF)
Start up temp. range	-40ºC to 60ºC (-40ºF to 140ºF)
Extended Tem-	Yes

perature:	
Operating humidity range	Up to 90% non-condensing
Storage temp. range	-40°C ~ +65°C
Water/dust intrusion	IP66/67, NEMA 4X
Mechanical	
Dimensions	Ø79.9x205mm(Ø3.15inx8.07in)
Weight	1.2KG
Shipping weight	3.2KG
Pan rotation angle	270°
Tilt angle	90°
Z-axis rotation	N/A
Vandal rating	IK10
Regulatory	
Safety	UL60950-1; CAN/CSA-C22.2 No. 60950-1, BIS IS13252 Part 1:2010
Emissions	FCC Part 15 Class A; EN55032 Class A; AS/NZS CISPR 32 Class A; ICES-003/NMB-003 Class A
Immunity	EN50130-4
Environmental	RoHS; WEEE, REACH

END USER LICENSE AGREEMENT (EULA)

IMPORTANT NOTICE: This End User License Agreement ("Agreement") is a binding legal contract between you ("you") and Johnson Controls International plc. (including its Affiliates such as Johnson Controls, Inc.) with a corporate address at 507 E. Michigan St., Milwaukee, WI ("JCI", "we", or "us"). By downloading, installing, accessing or using the accompanying software (the "Software") you will be bound by the terms of this Agreement. If you do not agree to the terms of this Agreement, JCI is not willing to grant you any right to use or access the Software. In such event, you may not download, install, access, use or copy the Software. If this agreement is being agreed to by a company or other legal entity, then the person agreeing to this agreement on behalf of that company or entity represents and warrants that he or she is authorized and lawfully able to bind that company or entity to this agreement. You should print and retain a copy of this agreement for your records. Unless a separate agreement is provided, other JCI application software distributed by this Software will also be subject to the terms of this agreement.

PLEASE READ THE FOLLOWING TERMS AND CONDITIONS CAREFULLY BEFORE DOWNLOADING, INSTALLING, ACCESSING OR USING THE SOFTWARE.

Agreement Structure. This Agreement includes Part 1 – General Terms and Part 2 – Country Specific Terms, as applicable. The terms of Part 2 may replace or modify those of Part 1. In the event of a conflict between the terms of any or all of Part 1 and Part 2, the terms of Part 2 shall prevail over Part 1.

PART 1 – General Terms

1. Grant of License. During the term of this Agreement, JCI grants you and your individual employees a revocable, non-transferable, non-sublicensable, nonexclusive license to use the object code version of the Software and any Documentation for your internal use only, subject to all Scope Restrictions. The order document under which you have licensed the Software may contain additional terms limiting the scope your license, including, but not limited to, a specified number of users or specific systems, licensed facilities, geographic areas, etc. (collectively, "Scope Restrictions"). In the event the Software is furnished for use in connection with a particular JCI system or hardware product, it may only be used in conjunction with that JCI system or hardware product. If the Software is furnished embedded in a JCI system or hardware product, the Software may not be extracted or used separately from that system or product. "Documentation" means JCI then current generally available documentation for use and operation of the Software. Documentation is deemed included in the definition of Software. The term "Software" will be deemed to include any updates, bug fixes, and versions (collectively, "Enhancements") that JCI may, in its discretion, make available to you. You are responsible for ensuring your employees comply with all relevant terms of this Agreement and any failure to comply will constitute a breach by you. The Software is licensed, not sold. Except for the limited license granted above, JCI and its licensors retain all right, title and interest in the Software, all copies thereof, and all proprietary rights in the Software, including copyrights, patents, trademarks and trade secret rights.

2. Restrictions. Your use of the Software must be in accordance with the Documentation. You will be solely responsible for ensuring your use of the Software is in compliance with all applicable foreign, federal, state and local laws, rules and regulations. You may not (i) copy or distribute the Software except to the extent that copying is necessary to use the Software for purposes set forth herein; provided you may make a single copy of the Software for backup and archival purposes; (ii) modify or create derivative works of the Software; (iii) decompile, disassemble, reverse engineer, or otherwise attempt to derive the trade secrets embodied in the Software, except and only to the extent that such activity may be expressly permitted, notwithstanding this limitation or another limitation contained in this agreement, either by applicable law or, in the case of open source software, the

applicable open source license; (iv) use the Software for purposes of developing a competing product or service; (v) remove any copyright, trademark, proprietary rights, disclaimer, or warning notice included on or embedded in any part of the Documentation and Software; (v) assign, sublicense, rent, timeshare, loan, lease or otherwise transfer the Software, or directly or indirectly permit any third party to use or copy the Software. Under no circumstances will JCI be liable or responsible for any use, or any results obtained by the use, of the services in conjunction with any services, software, or hardware that are not provided by JCI. All such use will be at your sole risk and liability.

3. Third Party Software. To the extent any software licensed from third parties, including open source software, (collectively, “Third Party Software”) is provided with or incorporated into the Software, you will comply with the terms and conditions of the applicable third party licenses associated with the Third Party Software, in addition to the terms and restrictions contained in this Agreement. All relevant licenses for the Third Party Software are provided at www.johnsoncontrols.com/buildings/legal/digital. By using the Software you are also agreeing to be bound to the terms of such third party licenses. If provided for in the applicable third party license, you may have a right to reverse engineer such open source software or receive open source code for such open source software for use and distribution in any program that you create, so long as you in turn agree to be bound to the terms of the applicable third party license, and your programs are distributed under the terms of that license. If applicable, a copy of such open source code may be obtained free of charge by contacting your Johnson Controls representative. JCI MAKES NO WARRANTY OF ANY KIND, WHETHER EXPRESS OR IMPLIED, WITH REGARD TO ANY THIRD PARTY SOFTWARE. ALL THIRD PARTY SOFTWARE IS PROVIDED "AS-IS," WITHOUT WARRANTIES OF ANY KIND. IN NO EVENT WILL JCI BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY DIRECT, INDIRECT, PUNITIVE, EXEMPLARY, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE THIRD PARTY SOFTWARE, EVEN IF JCI HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSSES.

4. Metering Devices. The Software may contain technology based metering devices and passive restraints to regulate usage. For example, the Software may contain a license file limiting use to the licensed number of concurrent users or named users or may temporarily restrict usage until license and other fees have been paid in full. You acknowledge that such restraints and metering devices are a reasonable method to ensure compliance with the license and have been factored into the license and other fees and the Agreement as a whole. You agree that You will not circumvent, override, or otherwise bypass such metering devices and restraints that regulate the use of the Software.

5. Term and Termination. Unless provided otherwise in an accompanying order document, this Agreement will commence on the earlier of the date you first download, install, access or use the Software (the “Effective Date”) and continue in effect for the term specified in the order document or, if no term is specified, until it is terminated (the “Term”) as provided in this Section. Either party may terminate this Agreement on written notice to the other party if the other party is in material breach of its obligations hereunder and fails to cure the breach within thirty (30) days of such written notice. In addition, either party may, in its sole discretion, elect to terminate this Agreement on written notice to the other party upon the bankruptcy or insolvency of the other party or upon the bankruptcy or insolvency of the other party upon the commencement of any voluntary or involuntary winding up, or upon the filing of any petition seeking the winding up of the other party. In the event of any claim of infringement relating to the Software, JCI may terminate this Agreement on written notice to you and, as your sole and exclusive remedy, refund the license fees paid, if any, hereunder (less depreciation calculated on a three (3)-year straight-line basis commencing on the date of initial delivery to you). Sections 9 and 10 shall remain unaffected. Upon any termination or expiration of this Agreement, the license granted in Section 1 will automatically terminate and you will have no further right to possess or use the Software. On JCI’s request, you will provide JCI with a signed written statement confirming that the Software has been permanently removed from your systems.

6. Fees; Taxes. You will pay the fees, if any, associated with the Software. All amounts due hereunder shall be paid within thirty (30) days of the date of the invoice. Payments not made within such time period shall be subject to late charges equal to the lesser of (i) one and one-half percent (1.5%) per month of the overdue amount or (ii) the maximum amount permitted under applicable law. If the license granted to You is a term or subscription license: then, unless set forth in your applicable ordering document, any renewal of such license shall be at then-current JCI list price and any such license shall automatically terminate upon nonpayment of amounts due hereunder. All taxes, duties, fees and other governmental charges of any kind (including sales and use taxes, but excluding taxes based on the gross revenues or net income of JCI) that are imposed by or under the authority of any government or any political subdivision thereof on the fees for the Software shall be borne solely by you, unless you can evidence tax exemption and shall not be considered a part of a deduction from or an offset against such fees. If you lose tax exempt status, you will pay any taxes due as part of any renewal or payment. You will promptly notify JCI if your tax status changes. You will pay all court costs, fees, expenses and reasonable attorneys' fees incurred by JCI in collecting delinquent fees.

7. Limited Warranty; Disclaimer. JCI warrants that (i) for a period of thirty (30) days from delivery initial delivery to you (the "Warranty Period"), the Software will operate in substantial conformity with its Documentation; and (ii) it shall use screening software to scan the Software prior to delivery for viruses, Trojan horses, and other malicious code. If, during the Warranty Period, you notify JCI of any non-compliance with the foregoing warranties, JCI will, in its discretion: (a) use commercially reasonable efforts to provide the programming services necessary to correct any verifiable non-compliance with the foregoing warranties; or (b) replace any non-conforming Software; or if neither of foregoing options is reasonably available to JCI, (c) terminate this Agreement in whole or in part, and refund to You the fees, if any, paid for the non-conforming Software (less depreciation calculated on a three (3)-year straight-line basis commencing on the date of initial delivery to you). JCI shall not be liable for failures caused by third party hardware and software (including your own systems), misuse of the Software, or your negligence or willful misconduct. EXCEPT AS PROVIDED IN THIS SECTION, THE SOFTWARE IS PROVIDED ON AN "AS AVAILABLE," "AS IS" BASIS. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JCI AND ITS AFFILIATES, AND THEIR RESPECTIVE SUPPLIERS AND VENDORS DISCLAIM ALL OTHER WARRANTIES WITH RESPECT TO THE SOFTWARE, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, TITLE, MERCHANTABILITY, QUIET ENJOYMENT, QUALITY OF INFORMATION, AND FITNESS FOR A PARTICULAR PURPOSE. JCI AND ITS AFFILIATES AND THEIR RESPECTIVE SUPPLIERS AND VENDORS DO NOT WARRANT THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS, OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE SOFTWARE WILL BE CORRECTED. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY JCI OR ANY OF ITS PERSONNEL OR AGENTS SHALL CREATE ANY ADDITIONAL JCI WARRANTIES OR IN ANY WAY INCREASE THE SCOPE OF JCI'S OBLIGATIONS HEREUNDER.

8. Indemnities. JCI will indemnify, defend, and hold you harmless from any claim, demand, action, proceeding, judgment, or liability arising out of a claim by a third-party that your use of the Software in conformance with the terms of this Agreement infringes a United States patent, copyright, or trade secret of that third party. The foregoing indemnification obligation of JCI is contingent upon you promptly notifying JCI in writing of such claim, permitting JCI sole authority to control the defense or settlement of such claim, and providing JCI reasonable assistance in connection therewith. If a claim of infringement under this Section occurs, or if JCI determines a claim is likely to occur, JCI will have the right, in its sole discretion, to either: (i) procure for you the right or license to continue to use the Software free of the infringement claim; or (ii) modify the Software to make it non-infringing, without loss of material functionality. If either of these remedies is not reasonably available to JCI, JCI may, in its sole discretion, immediately terminate this Agreement and return the license fees paid by you for the Software, prorated on a three (3)-year straight-line basis commencing on the date of initial delivery to you. Notwithstanding the foregoing, JCI shall have no obligation with respect to any claim

of infringement that is based upon or arises out of (the “Excluded Claims”): (i) the use or combination of the Software with any third party hardware, software, products, data or other materials, including your own systems and data; (ii) modification or alteration of the Software by anyone other than JCI; (iii) your use of the Software in excess of the rights granted in this Agreement; or (iv) any Third Party Software. The provisions of this Section state the sole and exclusive obligations and liability of JCI and its JCIs and suppliers for any claim of intellectual property infringement arising out of or relating to the Software and/or this Agreement and are in lieu of any implied warranties of non-infringement, all of which are expressly disclaimed. Section 9 shall remain unaffected. You will, subject to your culpability, indemnify, defend, and hold JCI harmless from any claim, demand, action, proceeding, judgment, or liability from a third-party claim arising out of an Excluded Claim. JCI must promptly notify you in writing of any such claim, permit you sole authority to control the defense or settlement of the claim, and provide you reasonable assistance in connection therewith.

9. Limitation of Liability. TO THE MAXIMUM EXTENT PERMITTED BY LAW, IN NO EVENT SHALL JCI AND ITS AFFILIATES AND THEIR RESPECTIVE SUPPLIERS AND VENDORS BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE, OR INDIRECT DAMAGES, WHICH SHALL INCLUDE, WITHOUT LIMITATION, DAMAGES FOR PERSONAL INJURY, LOST PROFITS, LOST DATA AND BUSINESS INTERRUPTION, ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE, EVEN IF THEY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ANY CASE, THE ENTIRE AGGREGATE LIABILITY OF JCI AND ITS AFFILIATES AND THEIR RESPECTIVE SUPPLIERS AND VENDORS UNDER THIS AGREEMENT FOR ALL DAMAGES, LOSSES, AND CAUSES OF ACTION (WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE) SHALL BE LIMITED TO FEES PAID BY YOU FOR THE SOFTWARE, IF ANY, DURING THE THREE (3) MONTHS IMMEDIATELY PRECEDING THE FIRST EVENT GIVING RISE TO LIABILITY.

10. Confidentiality. You acknowledge that the ideas, methods, techniques, and expressions thereof contained in the Software (collectively, “JCI Confidential Information”) constitute confidential and proprietary information of JCI, the unauthorized use or disclosure of which would be damaging to JCI. You agree to hold the Software and JCI Confidential Information in strictest confidence, disclosing information only to permitted individual employees who are required to have access in order to perform under this Agreement and to use such information only for the purposes authorized by this Agreement. You are responsible for and agree to take all reasonable precautions, by instruction, agreement or otherwise, to ensure that your employees who are required to have access to such information in order to perform under this Agreement, are informed that the Software and JCI Confidential Information are confidential proprietary information belonging to JCI and to ensure that they make no unauthorized use or disclosure of such information. You may disclose JCI Confidential Information if you are required to do so pursuant to a governmental agency, a court of law or to any other competent authority so long as you provide JCI with written notice of such request prior to such disclosure and cooperate with JCI to obtain a protective order. Prior to disposing of any media reflecting or on which is stored or placed any Software, you will ensure any Software contained on the media has been securely erased or otherwise destroyed. You recognize and agree a remedy at law for damages will not be adequate to fully compensate JCI for the breach of Sections 1, 2, or 10. Therefore, JCI will be entitled to temporary injunctive relief against you without the necessity of proving actual damages and without posting bond or other security. Injunctive relief will in no way limit any other remedies JCI may have as a result of breach by You of the foregoing Sections or any other provision of this Agreement.

11. Data Collection and Use. You acknowledge and agree that the Software and/or hardware used in connection with the Software may collect data resulting from or otherwise relating to your use of the Software and/or hardware (“Data”) for purposes of providing you with service/product recommendations, benchmarking, energy monitoring, and maintenance and support. JCI shall be the exclusive owner of all Data. JCI shall have the right to de-identify your Data so that it does not identify you directly or by inference (the “De-Identified Data”). JCI shall have the right and ability to

use the De-Identified Data for its business purposes, including improvement of the Software, research, product development, product improvement and provision of products and services to JCI's other customers (collectively, "JCI's Business Purposes". In the event JCI does not own or is unable to own the De-Identified Data as a result of applicable law, or contractual commitments or obligations, you grant JCI a non-exclusive, perpetual, irrevocable, fully-paid-up, royalty free license to use, copy, distribute, and otherwise exploit statistical and other data derived from your use of the De-Identified Data for JCI's Business Purposes.

12. Feedback. You may provide suggestions, comments, or other feedback (collectively, "Feedback") to JCI with respect to its products and services, including the Software. Feedback is voluntary and JCI is not required to hold it in confidence. JCI may use Feedback for any purpose without obligation of any kind. To the extent a license is required under your intellectual property rights to make use of the Feedback, you grant JCI an irrevocable, non-exclusive, perpetual, world-wide, royalty-free license to use the Feedback in connection with JCI's business, including enhancement of the Software, and the provision of products and services to JCI's customers.

13. Governing Law and Jurisdiction.

13.1Governing Law. This Agreement is governed by and construed in accordance with the laws of the State of Wisconsin, as applied to agreements entered into and wholly performed within Wisconsin between Wisconsin residents. In the event the foregoing sentence is determined by a court of competent jurisdiction to not be enforceable or applicable to an action or proceeding brought by either party relating to or under this Agreement, the parties agree to the application of the laws of the country in which you entered into this Agreement to govern, interpret, and enforce all of your and JCI's respective rights, duties, and obligations arising from, or relating in any manner to, the subject matter of this Agreement, without regard to conflict of law principles. The United Nations Convention on Contracts for the International Sale of Goods does not apply to any such action or proceeding.

13.2Jurisdiction. Any action or proceeding brought by either party hereto shall be brought only in a state or federal court of competent jurisdiction located in Milwaukee, Wisconsin and the parties submit to the in personam jurisdiction of such courts for purposes of any action or proceeding. In the event the foregoing sentence is determined by a court of competent jurisdiction to not be enforceable or applicable to an action or proceeding brought by either party relating to or under this Agreement, the parties agree all rights, duties, and obligations of the parties are subject to the courts of the country in which You entered into this Agreement.

14. General. This Agreement constitutes the entire understanding and agreement between the parties with respect to the transactions contemplated in this Agreement and supersedes all prior or contemporaneous oral or written communications with respect to the subject matter of this Agreement, all of which are merged in this Agreement. This Agreement shall not be modified, amended or in any way altered except by an instrument in writing signed by authorized representatives of both parties. In the event that any provision of this Agreement is found invalid or unenforceable pursuant to judicial decree, the remainder of this Agreement shall remain valid and enforceable according to its terms. Any failure by JCI to strictly enforce any provision of this Agreement will not operate as a waiver of that provision or any subsequent breach of that provision. The following provisions shall survive any termination or expiration of this Agreement: Sections 2 (Restrictions), 4 (Term and Termination), 6 (Fees and Taxes) (to the extent of any fees accrued prior to the date of termination), 9 (Limitation of Liability), 10 (Confidentiality), 11 (Feedback), 13 (Governing Law), 14 (General), and 16 (U.S. Government Rights). JCI may assign any of its rights or obligations hereunder as it deems appropriate. **IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT IN THE EVENT ANY REMEDY HEREUNDER IS DETERMINED TO HAVE FAILED OF ITS ESSENTIAL PURPOSE, ALL LIMITATIONS OF LIABILITY AND EXCLUSIONS OF DAMAGES SET FORTH HEREIN SHALL REMAIN IN EFFECT.**

15. Export/Import. The Software is licensed for use in the specific country authorized by JCI. You may not export or import the Software to another country without JCI's written permission and

payment of any applicable country specific surcharges. You agree to comply fully with all relevant and applicable export and import laws and regulations of the United States and foreign nations in which the Software will be used ("Export/Import Laws") to ensure that neither the Software nor any direct product thereof are (a) exported or imported, directly or indirectly, in violation of any Export/Import Laws; or (b) are intended to be used for any purposes prohibited by the Export/Import Laws. Without limiting the foregoing, you will not export or re-export or import the Software: (a) to any country to which the United States or European Union has embargoed or restricted the export of goods or services or to any national of any such country, wherever located, who intends to transmit or transport the Software back to such country; (b) to any user who you know or have reason to know will utilize the Software in the design, development or production of nuclear, chemical or biological weapons; or (c) to any user who has been prohibited from participating in export transactions by any federal or national agency of the U.S. government or European Union. You will defend, indemnify, and hold harmless JCI and its affiliates and their respective licensors and suppliers from and against any and all damages, fines, penalties, assessments, liabilities, costs and expenses (including attorneys' fees and expenses) arising out of any your breach of this Section.

16. U.S. Government Rights. The Software is a "commercial item" as that term is defined at 48 CFR 2.101 (October 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 CFR 12.212 (September 1995), and is provided to the U.S. Government only as a commercial end item. Consistent with 48 CFR 12.212 and 48 CFR 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire the Software with only those rights set forth herein.

17. Electronic Acceptance. This Agreement may be accepted in electronic form (e.g., by an electronic or other means of demonstrating assent) and your acceptance will be deemed binding between the parties. Neither party may contest the validity or enforceability of this Agreement, including under any applicable statute of frauds, because it was accepted or signed in electronic form. Electronically maintained records when produced in hard copy form shall constitute business records and shall have the same validity as any other generally recognized business records.

PART 2 - Country Specific Terms

For licenses granted in the countries specified below, the following terms replace or modify the referenced terms in Part 1 and Part 3. All terms in Part 1 and Part 3 that are not changed by these amendments remain unchanged and in effect. This Part 2 is organized as follows:

13.1 Governing Law The phrase "the laws of the country in which You entered into this Agreement" in Section 13.1 (Governing Law) is replaced by the following language as it applies to the countries identified below:

Americas

Canada: the laws in the Province of Ontario;

Mexico: the federal laws of the Republic of Mexico;

United States, Anguilla, Antigua/Barbuda, Aruba, British Virgin Islands, Cayman Islands, Dominica, Grenada, Guyana, Saint Kitts and Nevis, Saint Lucia, Saint Maarten, and Saint Vincent and the Grenadines: the laws of the State of Wisconsin, United States;

Venezuela: the laws of the Bolivarian Republic of Venezuela;

Asia Pacific

Cambodia and Laos: the laws of the State of Wisconsin, United States;

Australia: the laws of the State or Territory in which the transaction is performed;

Hong Kong SAR and Macau SAR: the laws of Hong Kong Special Administrative Region ("SAR");

Taiwan: the laws of Taiwan;

Europe, Middle East, and Africa

Albania, Armenia, Azerbaijan, Belarus, Bosnia-Herzegovina, Bulgaria, Croatia, Former Yugoslav Republic of Macedonia, Georgia, Hungary, Kazakhstan, Kyrgyzstan, Moldova, Montenegro, Poland, Romania, Russia, Serbia, Slovakia, Tajikistan, Turkmenistan, Ukraine, and Uzbekistan: the laws of Austria;

Algeria, Andorra, Benin, Burkina Faso, Cameroon, Cape Verde, Central African Republic, Chad, Comoros, Congo Republic, Djibouti, Democratic Republic of Congo, Equatorial Guinea, French Guiana, French Polynesia, Gabon, Gambia, Guinea, Guinea-Bissau, Ivory Coast, Lebanon, Madagascar, Mali, Mauritania, Mauritius,

Mayotte, Morocco, New Caledonia, Niger, Reunion, Senegal, Seychelles, Togo, Tunisia, Vanuatu, and Wallis and Futuna: the laws of France;

Estonia, Latvia, and Lithuania: the laws of Finland;

Angola, Bahrain, Botswana, Burundi, Egypt, Eritrea, Ethiopia, Ghana, Jordan, Kenya, Kuwait, Liberia, Malawi, Malta, Mozambique, Nigeria, Oman, Pakistan, Qatar, Rwanda, Sao Tome and Principe, Saudi Arabia, Sierra Leone, Somalia, Tanzania, Uganda, United Arab Emirates, the United Kingdom, West Bank/Gaza, Yemen, Zambia, and Zimbabwe: the laws of England and Wales; and South Africa, Namibia, Lesotho, and Swaziland: the laws of the Republic of South Africa.

1**3.2 Jurisdiction** The following provisions replace Section 13.2 (Jurisdiction) as it applies for those countries identified below: All rights, duties, and obligations are subject to the courts of the country in which You entered into this Agreement except that in the countries identified below all claims or proceedings arising out of or related to this Agreement, including summary proceedings, will be brought before and subject to the exclusive jurisdiction of the following courts of competent jurisdiction:

Americas

Argentina: the Ordinary Commercial Court of the city of Buenos Aires;

Brazil: the court of Rio de Janeiro, RJ;

Chile: the Civil Courts of Justice of Santiago;

Ecuador: the civil judges of Quito for executory or summary proceedings (as applicable);

Mexico: the courts located in Mexico City, Federal District;

Peru: the judges and tribunals of the judicial district of Lima, Cercado;

Uruguay: the courts of the city of Montevideo;

Venezuela: the courts of the metropolitan area of the city of Caracas;

Europe, Middle East, and Africa

Austria: the court of law in Vienna, Austria (Inner-City);

Algeria, Andorra, Benin, Burkina Faso, Cameroon, Cape Verde, Central African Republic, Chad, Comoros, Congo Republic, Djibouti, Democratic Republic of Congo, Equatorial Guinea, France, French Guiana, French Polynesia, Gabon, Gambia, Guinea, Guinea-Bissau, Ivory Coast, Lebanon, Madagascar, Mali, Mauritania, Mauritius, Mayotte, Monaco, Morocco, New Caledonia, Niger, Reunion, Senegal, Seychelles, Togo, Tunisia, Vanuatu, and Wallis and Futuna: the Commercial Court of Paris;

Angola, Bahrain, Botswana, Burundi, Egypt, Eritrea, Ethiopia, Ghana, Jordan, Kenya, Kuwait, Liberia, Malawi, Malta, Mozambique, Nigeria, Oman, Pakistan, Qatar, Rwanda, Sao Tome and Principe, Saudi Arabia, Sierra Leone, Somalia, Tanzania, Uganda, United Arab Emirates, the United Kingdom, West Bank/Gaza, Yemen, Zambia, and Zimbabwe: the courts of England and Wales;

South Africa, Namibia, Lesotho, and Swaziland: the High Court in Johannesburg;

Greece: the competent court of Athens;

Israel: the courts of Tel Aviv-Jaffa;

Italy: the courts of Milan;

Portugal: the courts of Lisbon;

Spain: the courts of Madrid; and

Turkey: the Istanbul Central Courts and Execution Directorates of Istanbul, the Republic of Turkey

13.3 Arbitration The following paragraph is added as a new Subsection 13.3 (Arbitration) as it applies for those countries identified below. The provisions of this Subsection 13.3 prevail over those of Subsection 13.2 (Jurisdiction) to the extent permitted by the applicable governing law and rules of procedure:

Asia Pacific

A. **In Cambodia, India, Laos, Philippines, and Vietnam:**

Disputes arising out of or in connection with this Agreement will be finally settled by arbitration which will be held in Singapore in accordance with the Arbitration Rules of Singapore International Arbitration Center ("SIAC Rules") then in effect. The arbitration award will be final and binding for the parties without appeal and will be in writing and set forth the findings of fact and the conclusions of law.

The number of arbitrators will be three, with each side to the dispute being entitled to appoint one arbitrator. The two arbitrators appointed by the parties will appoint a third arbitrator who will act as chairman of the proceedings. Vacancies in the post of chairman will be filled by the president of the SIAC. Other vacancies will be filled by the respective nominating party. Proceedings will continue from the stage they were at when the vacancy occurred.

If one of the parties refuses or otherwise fails to appoint an arbitrator within 30 days of the date the other party appoints its, the first appointed arbitrator will be the sole arbitrator, provided that the arbitrator was validly and properly appointed.

All proceedings will be conducted, including all documents presented in such proceedings, in the English language. The English language version of this Agreement prevails over any other language version.

B. **In the People's Republic of China:**

In case no settlement can be reached, the disputes will be submitted to China International Economic and Trade Arbitration Commission for arbitration according to the then effective rules of the said Arbitration Commission. The arbitration will take place in Beijing and be conducted in Chinese. The arbitration award will be final and binding on both parties. During the course of arbitration, this agreement will continue to be performed except for the part which the parties are disputing and which is undergoing arbitration.

C. **In Indonesia:**

Each party will allow the other reasonable opportunity to comply before it claims that the other has not met its obligations under this Agreement. The parties will attempt in good faith to resolve all

disputes, disagreements, or claims between the parties relating to this Agreement. Unless otherwise required by applicable law without the possibility of contractual waiver or limitation, i) neither party will bring a legal action, regardless of form, arising out of or related to this Agreement or any transaction under it more than two years after the cause of action arose; and ii) after such time limit, any legal action arising out of this Agreement or any transaction under it and all respective rights related to any such action lapse.

Disputes arising out of or in connection with this Agreement shall be finally settled by arbitration that shall be held in Jakarta, Indonesia in accordance with the rules of Board of the Indonesian National Board of Arbitration (Badan Arbitrase Nasional Indonesia or ″BANI″) then in effect. The arbitration award shall be final and binding for the parties without appeal and shall be in writing and set forth the findings of fact and the conclusions of law.

The number of arbitrators shall be three, with each side to the dispute being entitled to appoint one arbitrator. The two arbitrators appointed by the parties shall appoint a third arbitrator who shall act as chairman of the proceedings. Vacancies in the post of chairman shall be filled by the chairman of the BANI. Other vacancies shall be filled by the respective nominating party. Proceedings shall continue from the stage they were at when the vacancy occurred.

If one of the parties refuses or otherwise fails to appoint an arbitrator within 30 days of the date the other party appoints its, the first appointed arbitrator shall be the sole arbitrator, provided that the arbitrator was validly and properly appointed.

All proceedings shall be conducted, including all documents presented in such proceedings, in the English and/or Indonesian language.

Europe, Middle East, And Africa

D. **In Albania, Armenia, Azerbaijan, Belarus, Bosnia-Herzegovina, Bulgaria, Croatia, Former Yugoslav Republic of Macedonia, Georgia, Hungary, Kazakhstan, Kyrgyzstan, Moldova, Montenegro, Poland, Romania, Russia, Serbia, Slovakia, Tajikistan, Turkmenistan, Ukraine, and Uzbekistan:**

All disputes arising out of this Agreement or related to its violation, termination or nullity will be finally settled under the Rules of Arbitration and Conciliation of the International Arbitral Center of the Federal Economic Chamber in Vienna (Vienna Rules) by three arbitrators appointed in accordance with these rules. The arbitration will be held in Vienna, Austria, and the official language of the proceedings will be English. The decision of the arbitrators will be final and binding upon both parties. Therefore, pursuant to paragraph 598 (2) of the Austrian Code of Civil Procedure, the parties expressly waive the application of paragraph 595 (1) figure 7 of the Code. JCI may, however, institute proceedings in a competent court in the country of installation.

E. **In Estonia, Latvia, and Lithuania:** All disputes arising in connection with this Agreement will be finally settled in arbitration that will be held in Helsinki, Finland in accordance with the arbitration laws of Finland then in effect. Each party will appoint one arbitrator. The arbitrators will then jointly appoint the chairman. If arbitrators cannot agree on the chairman, then the Central Chamber of Commerce in Helsinki will appoint the chairman.

Additional Country Specific Amendments

Canada

The following is added as a new Section 18:

For purposes of this Section 18, ″Personal Data″ refers to information relating to an identified or identifiable individual made available by one of the parties, its personnel or any other individual to the other in connection with this Agreement. The following provisions apply in the event that one party makes Personal Data available to the other:

a. General

i. Each party is responsible for complying with any obligations applying to it under applicable Canadian data privacy laws and regulations ("Laws").

ii. Neither party will request Personal Data beyond what is necessary to fulfill the purpose(s) for which it is requested. The purpose(s) for requesting Personal Data must be reasonable. Each party will agree in advance as to the type of Personal Data that is required to be made available.

b. Security Safeguards

i. Each party acknowledges that it is solely responsible for determining and communicating to the other the appropriate technological, physical and organizational security measures required to protect Personal Data.

ii. Each party will ensure that Personal Data is protected in accordance with the security safeguards communicated and agreed to by the other.

iii. Each party will ensure that any third party to whom Personal Data is transferred is bound by the applicable terms of this section.

iv. Additional or different services required to comply with the Laws will be deemed a request for new services.

c. Use

Each party agrees that Personal Data will only be used, accessed, managed, transferred, disclosed to third parties or otherwise processed to fulfill the purpose(s) for which it was made available.

d. Access Requests

i. Each party agrees to reasonably cooperate with the other in connection with requests to access or amend Personal Data.

ii. Each party agrees to reimburse the other for any reasonable charges incurred in providing each other assistance.

iii. Each party agrees to amend Personal Data only upon receiving instructions to do so from the other party or its personnel.

e. Retention

Each party will promptly return to the other or destroy all Personal Data that is no longer necessary to fulfill the purpose(s) for which it was made available, unless otherwise instructed by the other or its personnel or required by law.

f. Public Bodies Who Are Subject to Public Sector Privacy Legislation

If you are a public body subject to public sector privacy legislation, this Section 18 applies only to Personal Data made available to you in connection with this Agreement, and the obligations in this section apply only to ** you **, except that: 1) section (b)(i) applies only to JCI; 2) sections (a)(i) and (d)(i) apply to both parties; and 3) section (d)(ii) and the last sentence in (a)(ii) do not apply.

Peru

9. **Limitation of Liability**

The following is added to the end of this Section 9 (Limitation of Liability):

Except as expressly required by law without the possibility of contractual waiver, you and JCI intend that the limitation of liability in this Section 9 (Limitation of Liability) applies to damages caused by all types of claims and causes of action. If any limitation on or exclusion from liability in this section is held by a court of competent jurisdiction to be unenforceable with respect to a particular claim or

cause of action, the parties intend that it nonetheless apply to the maximum extent permitted by applicable law to all other claims and causes of action. Additionally, in accordance with Article 1328 of the Peruvian Civil Code, the limitations and exclusions specified in this section will not apply to damages caused by JCI's willful misconduct ("dolo") or gross negligence ("culpa inexcusable").

United States of America

6. **Fees; Taxes**

The following is added to the end of Section 6 (Fees; Taxes)

For Software delivered electronically in the United States for which you claim a state sales and use tax exemption, you agree not to receive any tangible personal property (e.g., media and publications) associated with the electronic program. You agree to be responsible for any sales and use tax liabilities that may arise as a result of your subsequent redistribution of the Software after delivery by JCI.

14. **General**

The following is added to the end of Section 14 (General):

Each party waives any right to a jury trial in any proceeding arising out of or related to this Agreement.

Australia

6. **Fees; Taxes**

The following is added to the end of Section 6 (Fees; Taxes)

Notwithstanding the foregoing, if any government or authority imposes a duty, tax (other than income tax), levy, or fee, on this Agreement or on the Software itself, that is not otherwise provided for in the amount payable, you agree to pay it when JCI invoices you. If the rate of GST changes, you may adjust the charge or other amount payable to take into account that change from the date the change becomes effective.

7. **Limited Warranty; Disclaimer**

The following is added to the first paragraph of Section 7 (Limited Warranty; Disclaimer): Although JCI disclaims certain warranties, you may have certain rights under the Competition and Consumer Act 2010 or other legislation and are only limited to the extent permitted by the applicable legislation. If JCI is in breach of a condition or warranty implied by the Competition and Consumer Act 2010, JCI's liability is limited to the repair or replacement of the goods, or the supply of equivalent goods. Where that condition or warranty relates to right to sell, quiet possession or clear title, or the goods are of a kind ordinarily obtained for personal, domestic or household use or consumption, then none of the limitations in this paragraph apply.

Hong Kong Sar, Macau Sar, and Taiwan

For licenses obtained in Taiwan and the special administrative regions, phrases throughout this Agreement containing the word "country" (for example, " the country in which you entered into this Agreement") are replaced with the following:

a. **In Hong Kong SAR:** "Hong Kong SAR"

b. In **Macau SAR:** "Macau SAR" except in the Governing Law clause (Section 11.1)

c. In **Taiwan:** "Taiwan."

India

14. **General**

The following is added to the end of Section 14 (General):

If no suit or other legal action is brought, within three years after the cause of action arose, in respect of any claim that either party may have against the other, the rights of the concerned party in respect of such claim will be forfeited and the other party will stand released from its obligations in respect of such claim.

Indonesia

5. **Term and Termination**

The following is added to the end of Section 5 (Term and Termination):

Both parties waive the provision of article 1266 of the Indonesian Civil Code, to the extent the article provision requires such court decree for the termination of an agreement creating mutual obligations.

Japan

14. **General**

The following is added to the end of Section 14 (General):

Any doubts concerning this Agreement will be initially resolved between us in good faith and in accordance with the principle of mutual trust.

Malaysia

7. **Limited Warranty; Disclaimer**

The word ″SPECIAL″ in Section 7 is deleted.

New Zealand

7. **Limited Warranty; Disclaimer**

The following is added to the first paragraph of Section 7 (Limited Warranty; Disclaimer): Although JCI disclaims certain warranties, you may have certain rights under the Consumer Guarantees Act 1993 or other legislation which cannot be excluded or limited. The Consumer Guarantees Act 1993 will not apply in respect of any goods which JCI provides, if you require the goods for the purposes of a business as defined in that Act.

9. **Limitation of Liability**

The following is added to Section 9 (Limitation of Liability):

Where the Software is not obtained for the purposes of a business as defined in the Consumer Guarantees Act 1993, the limitations in this Section are subject to the limitations in that Act.

People's Republic of China

6. **Fees; Taxes**

The following is added to the end of Section 6 (Fees; Taxes)

All banking charges incurred in the People's Republic of China will be borne by you and those incurred outside the People's Republic of China will be borne by JCI.

9. **Limitation of Liability**

The following is added to the end of Section 9 (Limitation of Liability)

nothing in these Terms shall exclude any liability of JCI: (i) for the death of or injury to any person; (ii) for damage to property caused by wilful misconduct and/or gross negligence of JCI; (iii) for fraud or

fraudulent misrepresentation; or (iv) for any matter which it would be illegal for JCI to exclude or limit or attempt to exclude or limit its liability under PRC law.

Philippines

9. **Limitation of Liability**

The following replaces the first sentence of Section 9 (Limitation of Liability):

TO THE MAXIMUM EXTENT PERMITTED BY LAW, IN NO EVENT SHALL JCI AND AFFILIATES AND THEIR RESPECTIVE ITS SUPPLIERS AND VENDORS BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY SPECIAL, (INCLUDING NOMINAL AND EXEMPLARY DAMAGES), INCIDENTAL, CONSEQUENTIAL, PUNITIVE, INDIRECT DAMAGES, MORAL, INCIDENTAL, OR INDIRECT DAMAGES OR FOR ANY ECONOMIC CONSEQUENTIAL DAMAGES WHICH SHALL INCLUDE, WITHOUT LIMITATION, DAMAGES FOR PERSONAL INJURY, LOST PROFITS, LOST DATA AND BUSINESS INTERRUPTION, ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE, EVEN IF THEY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Singapore

11. **Data Collection and Use.**

The following is added to the end of Section 11 (Data Collection and Use):

You have the right to request access to your personal information in the possession or under the control of JCI, and to request for corrections to be made on any errors in your personal information. Where possible, JCI will validate personal information provided using generally accepted practices and guidelines, for example, validating such personal information against pre-existing data held by JCI, or request to see supporting documentation before the personal information may be updated.

JCI will retain personal information we process on behalf of our customers for as long as needed to provide services to our customers. JCI may further retain and use this personal information as necessary to comply with our legal obligations, resolve disputes, maintain accurate accounting, financial and other operational records and enforce our agreements. You consent and authorize JCI to collect, use and retain information relating to your use of the Software and/or hardware in the manner set out above.

14. **General**

The following is added to the end of Section 14 (General):

Subject to the rights provided to JCI's suppliers and vendors provided in Section 9 (Limitation of Liability), a person who is not a party to this Agreement will have no right under the Contracts (Right of Third Parties) Act (Cap. 53B) to enforce any of its terms.

Taiwan

9. **Limitation of Liability**

The following is added to the end of Section 9 (Limitation of Liability):

To the extent required by applicable law, the words "AND THEIR RESPECTIVE SUPPLIERS AND VENDORS" are deleted.

European Union Member States

7. **Limited Warranty; Disclaimer**

The following is added to Section 7 (Limited Warranty; Disclaimer):

In the European Union (″EU″), consumers have legal rights under applicable national legislation governing the sale of consumer goods. Such rights are not affected by the provisions set out in this Section 7 (Limited Warranty; Disclaimer).

EU Member States And The Following Identified Countries

Iceland, Liechtenstein, Norway, Switzerland, Turkey, and any other European country that has enacted local data privacy or protection legislation similar to the EU model.

14. **General**

The following is added to the end of Section 14 (General): In the European Union (″EU″), consumers have legal rights under applicable national legislation governing the sale of consumer goods. Nothing in this Agreement shall in anyway whatsoever be intended to affect or in any way limit such rights, which remain in full force and effect.

A. **Definitions** – For the purposes of this Section 14 (General), the following additional definitions apply:

(1) **Business Contact Information** – business-related contact information disclosed by you to JCI, including names, job titles, business addresses, telephone numbers and email addresses of your employees and contractors. For Austria, Italy and Switzerland, Business Contact Information also includes information about you and your contractors as legal entities (for example, your revenue data and other transactional information).

(2) **Business Contact Personnel** – Your employees and contractors to whom the Business Contact Information related

(3) **Data Protection Authority** – The authority established by the Data Protection and Electronic Communications Legislation in the applicable country or, for non-EU countries, the authority responsible for supervising the protection of personal data in that country, or (for any of the foregoing) any duly appointed successor entity thereto.

(4) **Data Protection & Electronic Communications Legislation** – (i) the applicable local legislation and regulations in force implementing EU Directive 95/46/EC (on the protection of individuals with regard to the processing of personal data and on the free movement of such data) and of EU Directive 2002/58/EC (concerning the processing of personal data and the protection of privacy in the electronic communications sector), as amended or replaced from time to time (such as the General Data Protection Regulation, when and as applicable); or (ii) for non-EU countries, the legislation and/or regulations passed in the applicable country relating to the protection of personal data and the regulation of electronic communications involving personal data, including (for any of the foregoing) any statutory replacement or modification thereof.

JCI Group – Johnson Controls International, Plc, including Johnson Controls, Inc., its subsidiaries, and their respective Business Partners and subcontractors.

B. You authorize JCI:

(1) to process and use Business Contact Information within JCI Group in support of you and your business including the provision of support services, and for the purpose of furthering the business relationship between you and JCI Group, including, without limitation, contacting Business Contact Personnel (by email or otherwise) and marketing JCI Group products and services (the ″Specified Purpose″); and

(2) to disclose Business Contact Information to other members of JCI Group in pursuit of the Specified Purpose only.

C. JCI agrees that all Business Contact Information will be processed in accordance with the Data Protection & Electronic Communications Legislation and will be used only for the Specified Purpose.

(1) To the extent required by the Data Protection & Electronic Communications Legislation, you represent that (a) you have obtained (or will obtain) any consents from (and has issued (or will issue) any notices to) the Business Contact Personnel as are necessary in order to enable JCI Group to process and use the Business Contact Information for the Specified Purpose.

(2) You authorize JCI to transfer Business Contact Information outside the European Economic Area, provided that the transfer is made on contractual terms approved by the Data Protection Authority or the transfer is otherwise permitted under the Data Protection & Electronic Communications Legislation.

Austria

9. **Limitation of Liability**

The following is added to the beginning of Section 9 (Limitation of Liability):

THE FOLLOWING LIMITATIONS AND EXCLUSIONS OF JCI'S LIABILITY DO NOT APPLY FOR DAMAGES CAUSED BY GROSS NEGLIGENCE OR WILLFUL MISCONDUCT. CIRCUMSTANCES MAY ARISE WHERE, BECAUSE OF A DEFAULT BY JCI IN THE PERFORMANCE OF ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHER LIABILITY, YOU ARE ENTITLED TO RECOVER DAMAGES FROM JCI.

The following is added to the end of Section 9 (Limitation of Liability):

THE LIMITATIONS AND EXCLUSIONS OF JCI'S LIABILITY DO NOT APPLY FOR DAMAGES CAUSED BY GROSS NEGLIGENCE OR WILLFUL MISCONDUCT.

The following words are deleted from Section 9 (Limitation of Liability): "(WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE)"

The following replaces the first sentence (second sentence after the above amendment) of Section 9 (Limitation of Liability):

"TO THE MAXIMUM EXTENT PERMITTED BY LAW, IN NO EVENT SHALL JCI AND AFFILIATES AND THEIR RESPECTIVE ITS SUPPLIERS AND VENDORS BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INDIRECT DAMAGES OR CONSEQUENTIAL DAMAGES, WHICH SHALL INCLUDE, WITHOUT LIMITATION, DAMAGES FOR PERSONAL INJURY, LOST PROFITS, LOST DATA AND BUSINESS INTERRUPTION, ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE, EVEN IF THEY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES."

Belgium, France and Luxembourg

9. **Limitation of Liability**

The following replaces the Section 9 (Limitation of Liability) in its entirety:

"EXCEPT AS OTHERWISE PROVIDED BY MANDATORY LAW, JCI'S ENTIRE LIABILITY FOR ALL CLAIMS IN THE AGGREGATE FOR ANY DAMAGES AND LOSSES THAT MAY ARISE AS A CONSEQUENCE OF THE FULFILLMENT OF ITS OBLIGATIONS UNDER OR IN CONNECTION WITH THIS AGREEMENT OR DUE TO ANY OTHER CAUSE RELATED TO THIS AGREEMENT IS LIMITED TO THE COMPENSATION OF ONLY THOSE DAMAGES AND LOSSES PROVED AND ACTUALLY ARISING AS AN IMMEDIATE AND DIRECT CONSEQUENCE OF THE NON-FULFILLMENT OF SUCH OBLIGATIONS (IF JCI IS AT FAULT) OR OF SUCH CAUSE, FOR A MAXIMUM OF EUR 500,000 (FIVE HUNDRED THOUSAND EURO). THE ABOVE LIMITATION WILL NOT APPLY TO DAMAGES FOR BODILY INJURIES (INCLUDING DEATH) AND DAMAGES TO REAL PROPERTY AND TANGIBLE PERSONAL PROPERTY FOR WHICH JCI IS LEGALLY LIABLE. UNDER NO CIRCUMSTANCES IS JCI OR ANY OF ITS SUPPLIERS OR VENDORS LIABLE FOR ANY OF THE FOLLOWING, EVEN IF INFORMED OF THEIR POSSIBILITY:

1) LOSS OF, OR DAMAGE TO, DATA; 2) INCIDENTAL, EXEMPLARY OR INDIRECT DAMAGES, OR FOR ANY ECONOMIC CONSEQUENTIAL DAMAGES; AND / OR 3) LOST PROFITS, BUSINESS, REVENUE, GOODWILL, OR ANTICIPATED SAVINGS, EVEN IF THEY ARISE AS AN IMMEDIATE CONSEQUENCE OF THE EVENT THAT GENERATED THE DAMAGES.

THE LIMITATION AND EXCLUSION OF LIABILITY HEREIN AGREED APPLIES NOT ONLY TO THE ACTIVITIES PERFORMED BY JCI BUT ALSO TO THE ACTIVITIES PERFORMED BY ITS SUPPLIERS AND VENDORS, AND REPRESENTS THE MAXIMUM AMOUNT FOR WHICH JCI AS WELL AS ITS SUPPLIERS AND VENDORS ARE COLLECTIVELY RESPONSIBLE.

France

6. **Fee; Taxes**

The following replaces the Section 6 (Fee; Taxes) in its entirety:

You will pay the fees, if any, associated with the Software. All amounts due hereunder shall be paid within thirty (30) days of the date of the invoice. Pursuant to article L. 441-6 of the French Commercial Code, late payment penalties as well as a fixed compensation for recovery costs of the amount of 40 Euros (forty Euros) are due in the event that the amounts due are paid after the due date, and this without the necessity of a reminder without prejudice to damages and other expenses that JCI has the right to claim. The late penalties due to, under the mentioned legislation, will be claimed by JCI at the rate equal to the interest rate applied by the European Central Bank to its most recent refinancing operation plus 10 percentage points.

All taxes, duties, fees and other governmental charges of any kind (including sales and use taxes, but excluding taxes based on the gross revenues or net income of JCI) that are imposed by or under the authority of any government or any political subdivision thereof on the fees for the Software shall be borne solely by you, unless you can evidence tax exemption and shall not be considered a part of a deduction from or an offset against such fees. If you lose tax exempt status, you will pay any taxes due as part of any renewal or payment.

You will promptly notify JCI if your tax status changes. You will pay all court costs, fees, expenses and reasonable attorneys' fees incurred by JCI in collecting delinquent fees.

11. **Data Collection and Use**

The following replaces the Section 11 (Data Collection and Use) in its entirety:

A. Definitions – For the purposes of this Section 11 (Data Collection and Use), the following additional definitions apply:

(1) **Data** – Data resulting from or otherwise relating to your use of the Software and/or hardware used in connection with the Software.

(2) **Data Protection Authority** – The authority established by the Data Protection and Electronic Communications Legislation in the applicable country or, for non-EU countries, the authority responsible for supervising the protection of personal data in that country, or (for any of the foregoing) any duly appointed successor entity thereto.

(3) **Data Protection & Electronic Communications Legislation** – (i) the applicable local legislation and regulations in force implementing the requirements of EU Directive 95/46/EC (on the protection of individuals with regard to the processing of personal data and on the free movement of such data) and of EU Directive 2002/58/EC (concerning the processing of personal data and the protection of privacy in the electronic communications sector), as amended or replaced from time to time; or (ii) for non-EU countries, the legislation and/or regulations passed in the applicable country relating to the protection of personal data and the regulation of electronic communications involving personal data, including (for any of the foregoing) any statutory replacement or modification thereof.

JCI Group – Johnson Controls International, Plc., including Johnson Controls, Inc., its subsidiaries, and their respective Business Partners and subcontractors.

B. You authorize JCI:

(1) to process and use your Data within JCI Group for purposes of providing you with service/product recommendations, benchmarking, energy monitoring, and maintenance and support (the ″Specified Purpose″);

(2) to disclose your Data to other members of JCI Group in pursuit of the Specified Purpose only;

(3) to de-identify your Data so that it does not identify you directly or by inference (the “De-Identified Data”);

(4) to use the De-Identified Data for its business purposes, including improvement of the Software, research, product development, product improvement and provision of products and services to JCI’s other customers (collectively, “JCI’s Business Purposes”);

(5) to use, copy, distribute, and otherwise exploit statistical and other data derived from your use of the De-Identified Data for JCI’s Business Purposes.

C. JCI agrees that all Data will be processed in accordance with the Data Protection & Electronic Communications Legislation and will be used only for the Specified Purpose.

D. You authorize JCI to transfer Data outside the European Economic Area, provided that the transfer is made on contractual terms approved by the Data Protection Authority or the transfer is otherwise permitted under the Data Protection & Electronic Communications Legislation.

E. According to the Data Protection Act of January 6th, 1978, you have at any time, a right of access to and rectification of all of your personal data. If you wish to exercise this right and gain access to your personal data, please write to us via https://www.johnsoncontrols.com/contact-us. You may also oppose, for legitimate reasons, the processing of your personal data."

Italy

4. **Metering devices**

The following is added to Section 4 (Metering devices): The metering devices and passive restraints mentioned in this Section are those specified in the accompanying order document.

5. **Term and termination**

The following paragraph is deleted in its entirety from Section 5:

“In addition, either party may, in its sole discretion, elect to terminate this Agreement on written notice to the other party upon the bankruptcy or insolvency of the other party or upon the commencement of any voluntary or involuntary winding up, or upon the filing of any petition seeking the winding up of the other party.”

The following wording is added to Section 5 (Term and termination): Without prejudice to the above, if no term is specified, either party shall have the right to terminate the Agreement at any time by giving the other Party a six months prior written notice.

11 **Data Collection and Use**

The following replaces the Section 11 (Data Collection and Use) in its entirety:

You acknowledge and agree the Software and/or hardware used in connection with the Software may collect data resulting from or otherwise relating to your use of the Software and/or hardware (“Data”) for purposes of providing you with service/product recommendations, benchmarking, energy monitoring, and maintenance and support. JCI shall have the right and ability to use the De-Identified Data for its business purposes, including improvement of the Software, research, product

development, product improvement and provision of products and services to JCI's other customers (collectively, "JCI's Business Purposes"). JCI shall have the right to use the Data provided that: (i) the Data have been De-Identified by JCI, so that JCI does not identify You directly or by inference; the Data, as De-Identified, will be used in compliance with the applicable local legislation and regulations in force.

9. **Limitation of Liability**

The following replaces the Section 9 (Limitation of Liability) in its entirety:

"TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, JCI'S ENTIRE LIABILITY FOR ALL CLAIMS IN THE AGGREGATE FOR ANY DAMAGES AND LOSSES THAT MAY ARISE IN CONNECTION WITH THE FULFILLMENT OF ITS OBLIGATIONS UNDER OR IN CONNECTION WITH THIS AGREEMENT OR DUE TO ANY OTHER CAUSE RELATED TO THIS AGREEMENT IS LIMITED TO THE COMPENSATION OF ONLY THOSE DAMAGES AND LOSSES PROVED AND ACTUALLY ARISING AS AN IMMEDIATE AND DIRECT CONSEQUENCE OF THE NON-FULFILLMENT OF SUCH OBLIGATIONS (IF JCI IS AT FAULT) OR OF SUCH CAUSE, FOR A MAXIMUM OF EUR 500,000 (FIVE HUNDRED THOUSAND EURO). THE ABOVE LIMITATION WILL NOT APPLY TO DAMAGES FOR BODILY INJURIES (INCLUDING DEATH) AND DAMAGES TO REAL PROPERTY AND TANGIBLE PERSONAL PROPERTY FOR WHICH JCI IS LEGALLY LIABLE. SAVE IN CASE OF GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, UNDER NO CIRCUMSTANCES JCI OR ANY OF ITS SUPPLIERS OR VENDORS LIABLE FOR ANY OF THE FOLLOWING, EVEN IF INFORMED OF THEIR POSSIBILITY:

1) LOSS OF, OR DAMAGE TO, DATA; 2) INCIDENTAL, EXEMPLARY OR INDIRECT DAMAGES, OR FOR ANY ECONOMIC CONSEQUENTIAL DAMAGES; AND / OR 3) LOST PROFITS, BUSINESS, REVENUE, GOODWILL, OR ANTICIPATED SAVINGS, EVEN IF THEY ARISE AS AN IMMEDIATE CONSEQUENCE OF THE EVENT THAT GENERATED THE DAMAGES.

THE LIMITATION AND EXCLUSION OF LIABILITY HEREIN AGREED APPLIES NOT ONLY TO THE ACTIVITIES PERFORMED BY JCI BUT ALSO TO THE ACTIVITIES PERFORMED BY ITS SUPPLIERS AND VENDORS, AND REPRESENTS THE MAXIMUM AMOUNT FOR WHICH JCI AS WELL AS ITS SUPPLIERS AND VENDORS ARE COLLECTIVELY RESPONSIBLE.

Germany

9. **Limitation of Liability**

The following replaces the Section 9 (Limitation of Liability) in its entirety:

1. JCI WILL BE LIABLE WITHOUT LIMIT FOR 1) LOSS OR DAMAGE CAUSED BY A BREACH OF AN EXPRESS GUARANTEE; 2) DAMAGES OR LOSSES RESULTING IN BODILY INJURY (INCLUDING DEATH); 3) DAMAGES CAUSED INTENTIONALLY OR BY GROSS NEGLIGENCE; AND 4) claims pursuant to the German Product Liability Act (Produkthaftungsgesetz, ProdHaftG)..

2. IN THE EVENT OF LOSS, DAMAGE AND FRUSTRATED EXPENDITURES CAUSED BY SLIGHT NEGLIGENCE OR IN BREACH OF ESSENTIAL CONTRACTUAL OBLIGATIONS (I.E. an obligation which must be fulfilled to enable a due performance of the AGREEMENT and on whose fulfilment YOU generally relY and may rely ON), JCI WILL BE LIABLE, REGARDLESS OF THE BASIS ON WHICH YOU ARE ENTITLED TO CLAIM DAMAGES FROM JCI (INCLUDING FUNDAMENTAL BREACH, NEGLIGENCE, MISREPRESENTATION, OR OTHER CONTRACT OR TORT CLAIM), PER CLAIM ONLY UP TO 500,000 EURO FOR THE PROGRAM THAT CAUSED THE LOSS OR DAMAGE. A NUMBER OF DEFAULTS WHICH TOGETHER RESULT IN, OR CONTRIBUTE TO, SUBSTANTIALLY THE SAME LOSS OR DAMAGE WILL BE TREATED AS ONE DEFAULT.

3. IN THE EVENT OF LOSS, DAMAGE AND FRUSTRATED EXPENDITURES CAUSED BY SLIGHT NEGLIGENCE, JCI WILL NOT BE LIABLE FOR INDIRECT OR CONSEQUENTIAL DAMAGES, EVEN IF JCI WAS INFORMED ABOUT THE POSSIBILITY OF SUCH LOSS OR DAMAGE. THIS LIMITATION SHALL NOT APPLY WHERE THE LOSS, DAMAGE AND FRUSTRATED EXPENDITURES WAS CAUSED BY A SLIGHT NEGLIGENT BREACH OF ESSENTIAL CONTRACTUAL OBLIGATIONS.

4. IN CASE OF DELAY ON JCI'S PART: 1) JCI WILL PAY TO YOU AN AMOUNT NOT EXCEEDING THE LOSS OR DAMAGE CAUSED BY JCI'S DELAY AND 2) JCI WILL BE LIABLE ONLY IN RESPECT OF THE RESULTING DAMAGES THAT YOU SUFFER, SUBJECT TO THE PROVISIONS OF ITEMS A AND B ABOVE.

14**. General**

The following is added to the end of Section 14 (General):

Any claims resulting from this Agreement are subject to a limitation period of three years, except as stated in Section 7 (Limited Warranty; Disclaimer) of this Agreement.

Ireland

7. **Limited Warranty; Disclaimer**

The following is added to Section 7 (Limited Warranty; Disclaimer):

Except as expressly provided in these terms and conditions, or Section 12 of the Sale of Goods Act 1893 as amended by the Sale of Goods and Supply of Services Act, 1980 (the ″1980 Act″), all conditions or warranties (express or implied, statutory or otherwise) are hereby excluded including, without limitation, any warranties implied by the Sale of Goods Act 1893 as amended by the 1980 Act (including, for the avoidance of doubt, Section 39 of the 1980 Act).

United Kingdom

Agreement Structure

The following sentence is added:

Nothing in this paragraph shall be interpreted or construed as excluding or limiting the liability of any person for fraud or fraudulent misrepresentation.

2. **Restrictions**

The following is added at the end of point (iii):

(if it is necessary for You to decompile the Software, to obtain the information necessary to create an independent program which can be operated with the Software, You will inform JCI that this is the case and will allow JCI a reasonable opportunity to provide such information to You so that it is no longer necessary for You to carry out that decompilation)

9. **Limitation of Liability**

The following replaces the Section 9 (Limitation of Liability) in its entirety:

FOR THE PURPOSES OF THIS SECTION, A ″DEFAULT″ MEANS ANY ACT, STATEMENT, OMISSION OR NEGLIGENCE ON THE PART OF JCI IN CONNECTION WITH, OR IN RELATION TO, THE SUBJECT MATTER OF AN AGREEMENT IN RESPECT OF WHICH JCI IS LEGALLY LIABLE TO YOU, WHETHER IN CONTRACT OR IN TORT. A NUMBER OF DEFAULTS WHICH TOGETHER RESULT IN, OR CONTRIBUTE TO, SUBSTANTIALLY THE SAME LOSS OR DAMAGE WILL BE TREATED AS ONE DEFAULT. TO THE MAXIMUM EXTENT PERMITTED BY LAW, IN NO EVENT SHALL JCI AND AFFILIATES AND THEIR RESPECTIVE ITS SUPPLIERS AND VENDORS BE LIABLE TO YOU OR ANY THIRD PARTY

FOR ANY SPECIAL, CONSEQUENTIAL, OR INDIRECT DAMAGES; OR WASTED MANAGEMENT TIME OR LOST PROFITS, BUSINESS, REVENUE, GOODWILL, OR ANTICIPATED SAVINGS, WHICH SHALL INCLUDE, WITHOUT LIMITATION, DAMAGES FOR LOST PROFITS, LOST DATA AND BUSINESS INTERRUPTION, ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE, EVEN IF THEY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.. CIRCUMSTANCES MAY ARISE WHERE, BECAUSE OF A DEFAULT BY JCI IN THE PERFORMANCE OF ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHER LIABILITY, YOU ARE ENTITLED TO RECOVER DAMAGES FROM JCI. REGARDLESS OF THE BASIS ON WHICH YOU ARE ENTITLED TO CLAIM DAMAGES FROM JCI AND EXCEPT AS EXPRESSLY REQUIRED BY LAW WITHOUT THE POSSIBILITY OF CONTRACTUAL WAIVER, JCI'S ENTIRE LIABILITY FOR ANY ONE DEFAULT WILL NOT EXCEED THE AMOUNT OF ANY DIRECT DAMAGES, TO THE EXTENT ACTUALLY SUFFERED BY YOU AS AN IMMEDIATE AND DIRECT CONSEQUENCE OF THE DEFAULT, UP TO 500,000 EURO (OR THE EQUIVALENT IN THEN-PREVAILING LOCAL CURRENCY) FOR THE PROGRAM THAT IS THE SUBJECT OF THE CLAIM.

NOTWITHSTANDING THE ABOVE, NOTHING IN THIS AGREEMENT WILL OPERATE TO EXCLUDE OR RESTRICT A PARTY'S LIABILITY (IF ANY) TO THE OTHER: (i) FOR DEATH OR PERSONAL INJURY; (ii) FOR FRAUD OR FRAUDULENT MISREPRESENTATION; (iii) FOR BREACH OF ITS OBLIGATIONS ARISING UNDER SECTION 12 SALE OF GOODS ACT 1979; (iii) FOR BREACH OF ITS OBLIGATIONS ARISING UNDER SECTION 2 SUPPLY OF GOODS AND SERVICES ACT 1982; (iv) FOR BREACH OF ITS OBLIGATIONS ARISING UNDER SECTION 8 SUPPLY OF GOODS (IMPLIED TERMS) ACT 1973; OR (v) FOR ANY MATTER FOR WHICH IT IS NOT PERMITTED BY LAW TO EXCLUDE OR LIMIT, OR TO ATTEMPT TO EXCLUDE OR LIMIT, ITS LIABILITY.

Additional Country Specific Amendments

Spain

7. **Limited Warranty; Disclaimer**

Section 7 (limited warranty; disclaimer) is replaced with the following:

JCI warrants that (i) for a period of thirty (30) days from delivery initial delivery to you (the "Warranty Period"), the Software will operate in substantial conformity with its Documentation; and (ii) it shall use screening software to scan the Software prior to delivery for viruses, Trojan horses, and other malicious code. If, during the Warranty Period, you notify JCI of any non-compliance with the foregoing warranties, JCI will, in its discretion: (a) use commercially reasonable efforts to provide the programming services necessary to correct any verifiable non-compliance with the foregoing warranties; or (b) replace any non-conforming Software; or if neither of foregoing options is reasonably available to JCI, (c) terminate this Agreement in whole or in part, and refund to You the fees, if any, paid for the non-conforming Software (less depreciation calculated on a three (3)-year straight-line basis commencing on the date of initial delivery to you. JCI shall not be liable for failures caused by third party hardware and software (including your own systems), misuse of the Software, or your negligence or willful misconduct. EXCEPT AS PROVIDED IN THIS SECTION, THE SOFTWARE IS PROVIDED ON AN "AS AVAILABLE," "AS IS" BASIS. THIS WITHOUT PREJUDICE THAT JCI WILL BE LIABLE FOR ANY HIDDEN FAULTS OF THE PRODUCTS PROVIDED, AS WELL AS ANY DAMAGES ARISED AS A RESULT OF PROVIDING A PRODUCT THAT DO NOT CONFORM WITH JCI'S DESCRIPTION, AND/OR THAT IT IS USELESS FOR THE PURPOSES OF THIS AGREEMENT. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JCI AND ITS AFFILIATES, AND THEIR RESPECTIVE SUPPLIERS AND VENDORS DISCLAIM ALL OTHER WARRANTIES WITH RESPECT TO THE SOFTWARE, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, TITLE, MERCHANTABILITY, QUITE ENJOYMENT, QUALITY OF INFORMATION, AND FITNESS FOR A PARTICULAR PURPOSE. JCI AND AFFILIATES AND THEIR RESPECTIVE

ITS SUPPLIERS AND VENDORS DO NOT WARRANT THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS, OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE SOFTWARE WILL BE CORRECTED. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY JCI OR ANY OF ITS PERSONNEL OR AGENTS SHALL CREATE ANY ADDITIONAL JCI WARRANTIES OR IN ANY WAY INCREASE THE SCOPE OF JCI'S OBLIGATIONS HEREUNDER.

9. **Limitation of liability**

The following is added to the end of this section 9 (limitation of liability):

NOTHING IN THIS AGREEMENT SHALL EXCLUDE OR LIMIT EITHER PARTY'S LIABILITY FOR: (I) DEATH OR PERSONAL INJURY CAUSED BY NEGLIGENCE; (II) FRAUD OR DECEIT; (III) WILLFULLY COSTS DAMAGES OR (IV) ANY OTHER LIABILITY THAT CANNOT BE EXCLUDED BY APPLICABLE LAW.

11. **Data Collection and Use**

Section 11 (data collection and use) is modified in the following terms:

You acknowledge and agree that the Software and/or hardware used in connection with the Software may collect data resulting from or otherwise relating to your use of the Software and/or hardware ("Data"). You hereby agree that your Data will be incorporated into a data file controlled by JCI, for the purposes of providing you with service/product recommendations, benchmarking, energy monitoring, maintenance and support, as well as for any purposes related to the execution of this agreement. You may exercise your rights of access, rectification, cancellation and opposition by writing to JCI corporate address stated above, or by contacting us at https://www.johnsoncontrols.com/contact-us, accompanying the request with a copy of an official identifying document. JCI shall be the exclusive owner of all Data. JCI shall have the right to de-identify your Data so that it does not identify you directly or by inference (the "De-Identified Data"). JCI shall have the right and ability to use the De-Identified Data for its business purposes, including improvement of the Software, research, product development, product improvement and provision of products and services to JCI's other customers (collectively, "JCI's Business Purposes".

© 2025 Johnson Controls. All rights reserved.

JOHNSON CONTROLS, TYCO and ILLUSTRA are trademarks and/or registered trademarks. Unauthorized use is strictly prohibited.