Illustra

Illustra Pro 4 20MP & 32MP

Multisensor Dome 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

© 2023 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 **7**

Illustra Pro4 20MP and 32MP Multisensor Cameras (Phase 1) **8**

Product overview 8

Installation 9

Illustra Pro4 20MP and 32MP Multisensor Cameras (Phase 2) **19**

Product overview 19

Installation 20

Network Topology **31**

Network Connection **32**

Default IP Address 32

DHCP 33

Managing cameras with the Illustra Connect tool 34

Configuration **36**

Live menu 40

Quick Start Menu 43

Basic Configuration 43

Video Menu 61

Streams 61

Picture Settings 64

Date / Time / OSD 73

Privacy Zones 76

Events and Actions Menu 78

Event Settings 78

Event Actions 82

Alarm I / O 83

Analytics 86

Artificial Intelligence Object Classification 89

Periodic Events 96

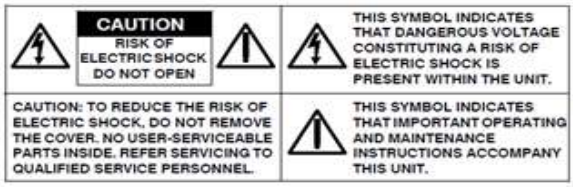
Event Logs 97

Applications 100
Applications 100
License 101
Security 102
Security Status 102
Security Status 104
Users 105
HTTP / HTTPS 107
IEEE 802.1x 108
Firewall 110
Remote Access 112
Session Timeout 115
Generate CSR 115
Network Menu 117
TCP/IP 117
Multicast 119
FTP 119
SMTP 121
SNMP 122
Heartbeat 123
CIFS 123
Dynamic DNS 124
SIP 125
Wi-Fi 126
QoS 127
Traffic control 128
System 129
Maintenance 129
Date / Time 132
Audio 133
Health Monitor 135
Logs 136

About 137
Edge Recording 139
Micro SD Card Management 139
Encrypted SD card storage 141
Record Settings 143
Event Download 144
Appendix A: Using Media Player to View RTSP Streaming 145
Appendix B: Stream Tables 146
Appendix C: Multisensor Cameras Technical Specifications 150
END USER LICENSE AGREEMENT (EULA) 160

Warning

- This camera operates at PoE BT Class8 (71.3W / 1920mA) or 24V AC (74W / 3.7A)
- Installation and service should be performed only by qualified and experienced technicians and comply with all local codes and rules to maintain your warranty.
- The warranty does not cover any damage arising either directly or indirectly from inappropriate installation which is not depicted within this documentation.
- 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 to be melted or lens fogged.
- Avoid aligning the lens with extremely bright objects (e.g., light fixtures) for long periods of time.
- Although this camera is waterproof and suitable for both indoor and outdoor usages, please do not sink the camera into water. Contact your dealer in case of sunk.
- Avoid operating or storing the camera in the following locations:
  - Close to sources of powerful radio or TV transmitters
  - Close to 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 Pro4 Multisensor Installation and Configuration Guide is a user manual which provides physical properties, installation, and configuration information of the cameras in Table 1 on Page 7.

Table 1 Product codes

Product Code	Model Name	Description
IPR20-M12-OI04	Illustra Pro 20MP (4x5MP) Motorised Multisensor PTR	Illustra Pro 20MP (4x5MP) Motorised Multisensor PTR, 2.7-13.5mm, Indoor/Outdoor, TDN w/IR, IK10, IP66
IPR32-M13-OI04	Illustra Pro 32MP (4x8MP) Motorised Multisensor PTR	Illustra Pro 32MP (4x8MP) Motorised Multisensor PTR, 3.6-11mm, Indoor/Outdoor, TDN w/IR, IK10, IP66
IPS20-M12-OIA4	Illustra Pro4 20MP Multisensor	Illustra Pro 20MP (4x5MP) Multisensor, 2.7-13.5mm, Indoor/Outdoor, TDN w/IR, IK10, IP66
IPS32-M13-OIA4	Illustra Pro4 32MP Multisensor	Illustra Pro 32MP (4x8MP) Multisensor, 3.6-11mm, Indoor/Outdoor, TDN w/IR, IK10, IP66
IPS20-M12-OTA4	Illustra Pro4 20MP Multisensor	Illustra Pro 20MP (4x5MP) Multisensor, 2.7-13.5mm, Indoor/Outdoor, TDN, IK10, IP66
IPS32-M13-OTA4	Illustra Pro4 32MP Multisensor	Illustra Pro 32MP (4x8MP) Multisensor, 3.6-11mm, Indoor/Outdoor, TDN, IK10, IP66

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 36 for procedural information pertaining to camera configuration.

Illustra Pro4 20MP and 32MP Multisensor Cameras (Phase 1)

This chapter provides product features, installation procedures, and connection information regarding the Illustra Pro4 20MP and 32MP Multisensor cameras.

Product overview

This chapter explains the features and installation of the Pro4 Multisensor cameras. Product code and description of the camera is provided in the table below.

Table 2 Product code and description of the Pro4 Multisensor cameras

Product Code	Description
IPR20-M12-OI04	Illustra Pro 20MP (4x5MP) Motorised Multisensor PTR, 2.7-13.5mm, Indoor/Outdoor, TDN w/IR, IK10, IP66
IPR32-M13-OI04	Illustra Pro 32MP (4x8MP) Motorised Multisensor PTR, 3.6-11mm, Indoor/Outdoor, TDN w/IR, IK10, IP66

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
- 2 x Rubber grommets
- 4 x Plastic screw anchors
- 1 x T20 Torx Wrench
- 4 x T4 Self-tapping screws
- 1 x Side Cover
- 1 x RJ45 Insert Tool
- 2 x T20 Screw for Side Cover
- 1 x Mounting Template
- 1 x 12-pin Terminal connector for I/O function
- 1 x 2-pin Terminal block
- 1 x Printed Quick Start Guide
- 1 x Printed Regulatory Document

Contact your dealer if any item is missing.

Installation tools

The following tools assist with installation:

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

Quick Reference

- Default IP: 192.168.1.168 (DHCP enabled)
- Default Username / Password: admin / admin
- Power: PoE 802.3bt Type 4 (90w) Class 8 (71.3W / 0.96A) or 24V AC (81W / 3.54A)

Figure 3 Pro4 Multisensor Dome camera parts

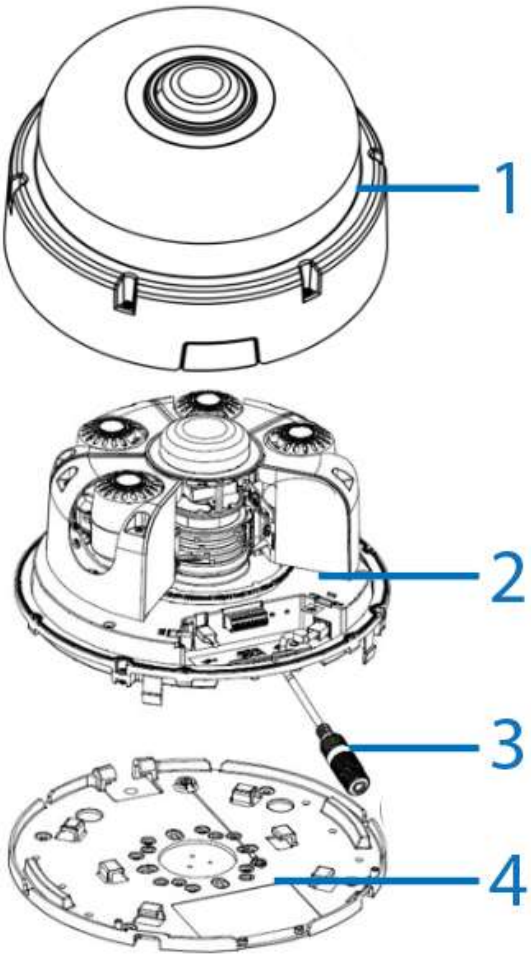


Table 4 Pro4 Multisensor Dome camera parts descriptions

Number	Description
1	Camera Top Cover with Bubble
2	Camera Lens Module
3	Pre-Fitted RJ45 cable
4	Mount Plate

Figure 5 Camera interior buttons / connections

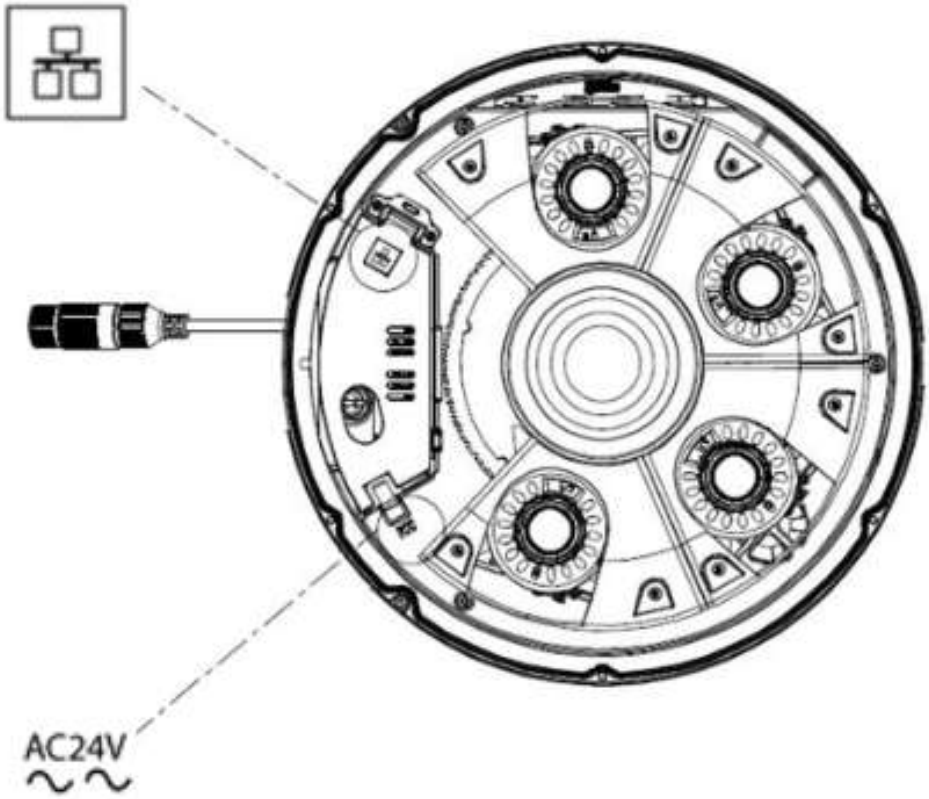
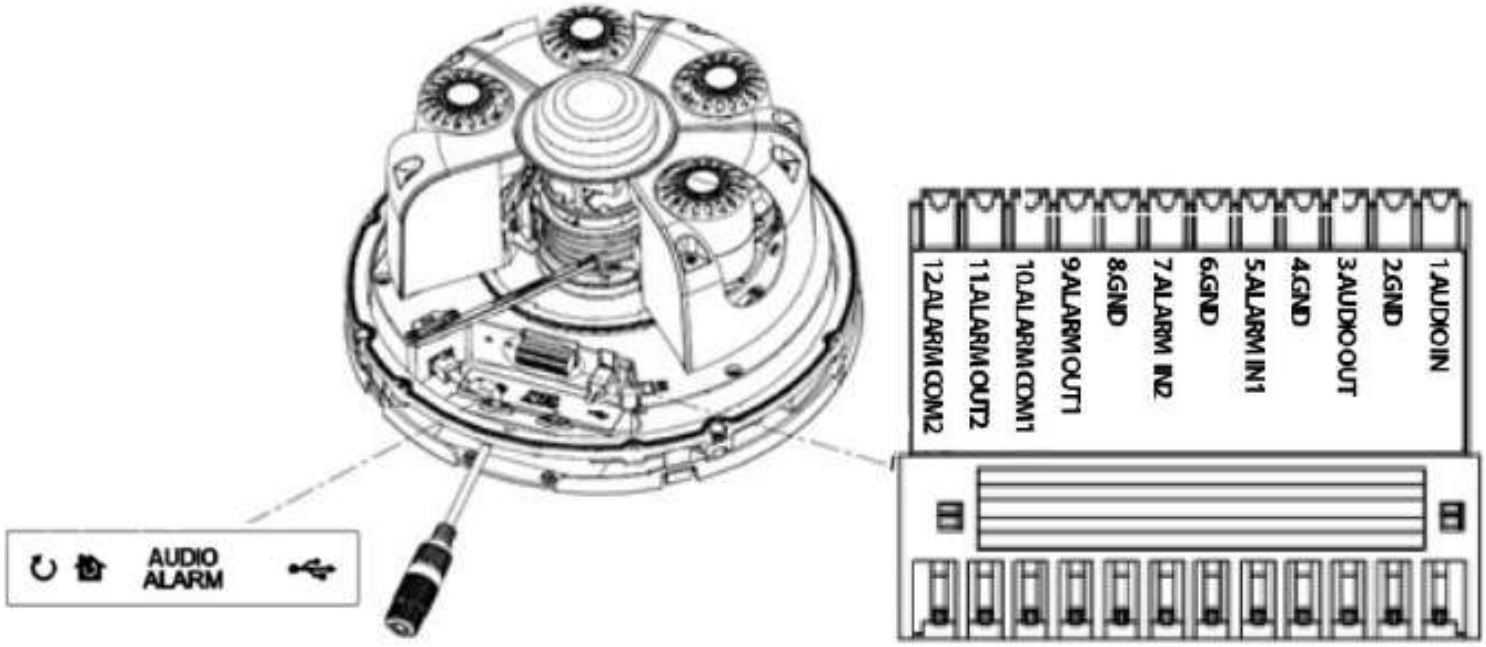


Figure 6 Camera interior buttons / connections



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.

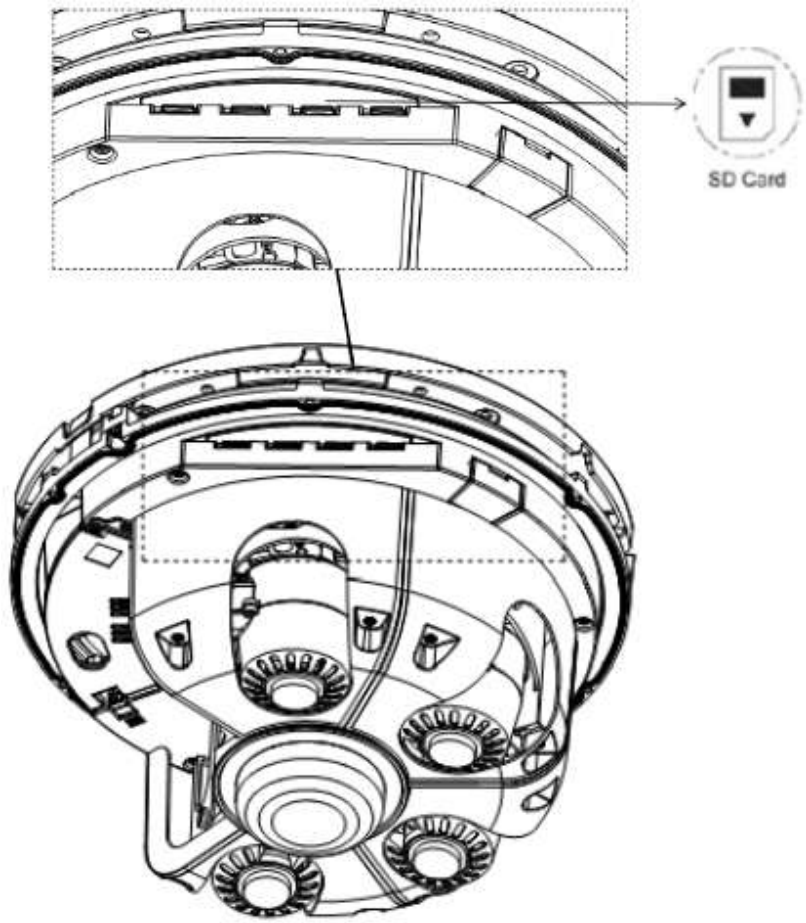
Table 7 Camera interior buttons / connections descriptions

Buttons / Connectors	Description
	PoE Ethernet port
	AC24V Power connector
	Reboots the camera (Press for 1 second)
	Reset to Factory default but preserve IP Address (Hold for 5 seconds) / Reset to factory default (Hold for 20 seconds)
AUDIO **ALARM**	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 camera. **Audio Out:** Via “GND” and “Audio Out” ports, connect to device such as speaker to be triggered through alarm output signals.
	Micro USB port

Procedure 1 Inserting or removing the SD card

Step	Action
1	Disassemble the camera as per steps 1 to 2 in ‘Disassembling the camera’ procedure and carefully insert or remove the micro-SD card (Figure 8) into or from the camera. **Note:**It is advised that you reboot the camera after inserting the micro-SD card.

Figure 8 SD Card cover

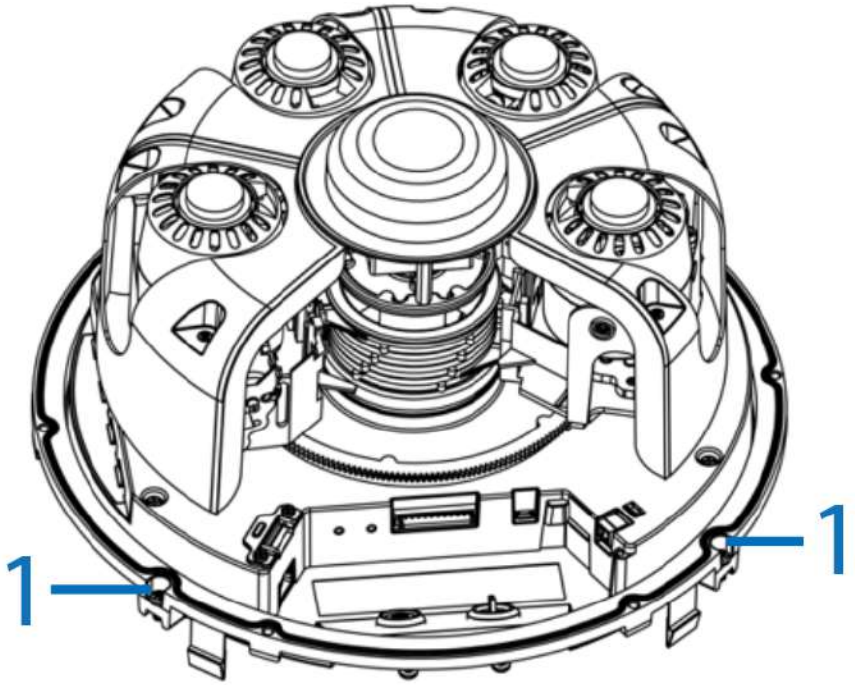


- End -

Procedure 2 Disassembling the camera

Step	Action
1	Use a T20 Torx wrench to remove the six screws located on the camera top cover (1) (Figure 3) and then remove the camera top cover. **Note:** The camera lens module (2) (Figure 3) is now exposed.
2	Use a T20 Torx wrench to remove the two screws (1) (Figure 9) on the camera lens module and remove the mounting plate (3) (Figure 3) from the camera lens module.

Figure 9 Camera lens module screws

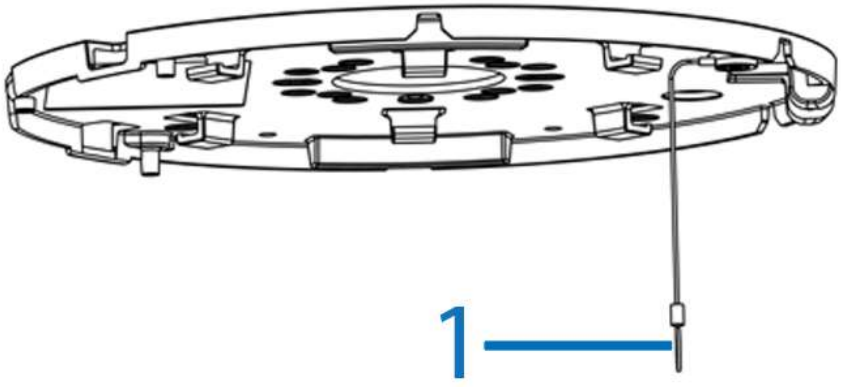


- End -

Procedure 3 Installing the camera onto a wall or ceiling

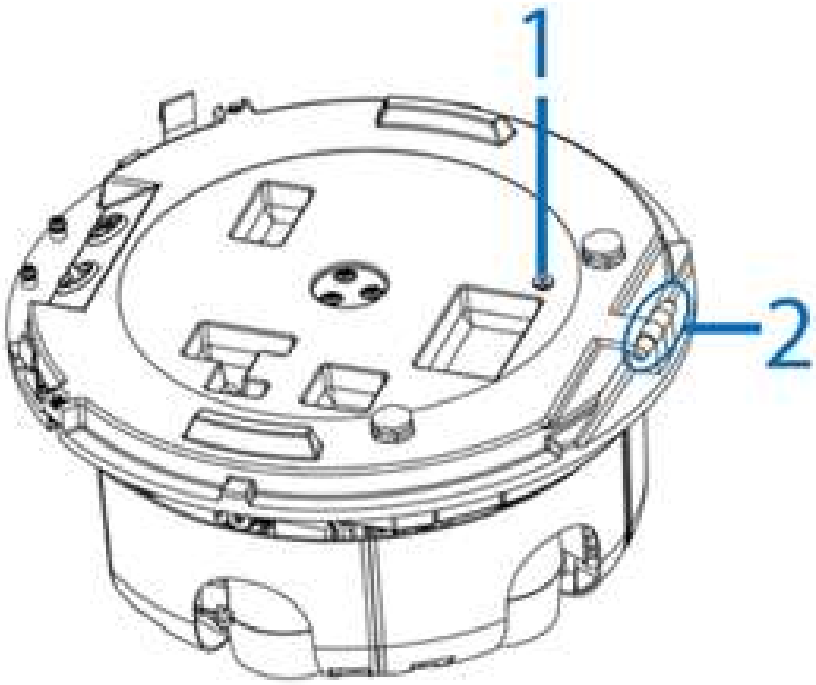
Step	Action
1	Disassemble the camera as per steps 1 to 2 in ‘Disassembling the camera’ procedure.
2	Hold the mounting template sticker up to the surface and mark out four holes as per the instructions on the template sticker.
3	Drill four holes on the surface and insert the four screw anchors into the four holes.
4	If you are not using the cable side entry hole on the mounting plate, then cut out a cable hole on the surface as per the instructions on the template sticker.
5	Hold the mounting plate (3) (Figure 3) up to the surface and align the four holes on the mounting plate with the four holes on the surface.
6	Insert the four TP4 self-tapping screws into the four holes and use the screwdriver to securely attach the mounting plate to the surface.
7	Hold the camera lens module up to the mounting plate and insert the ‘loop’ on the safety lanyard (1) (Figure 10) that is attached to the mounting template to the screw (1) (Figure 6) on the camera lens module.

Figure 10 Safety lanyard



8 Insert the ‘hinge pins’ (2) (Figure 11) on the camera module lens into the ‘hinge knuckle’ on the mounting plate. ‘3’ in Figure 13 identifies how the camera lens module and mounting plate attach together.

Figure 11 Safety lanyard screw and hinge pin



9 Pull all cables through the cable hole in the mounting plate.

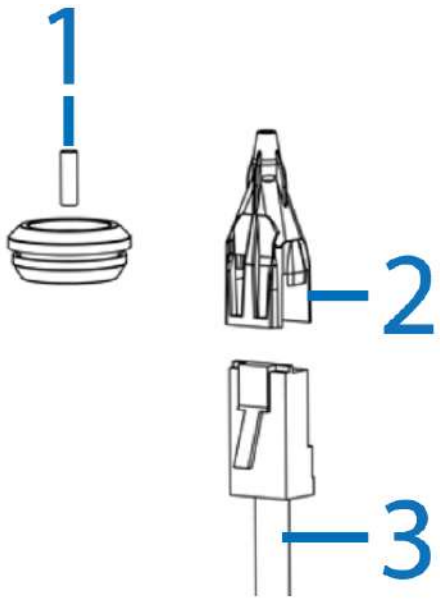
OR

If you are using the cable side entry on the mounting plate, remove the cable side entry cover screw and route all cables through the cable side entry.

10 Insert the RJ-45 cable (3) (Figure 12) into the insert tool (4) (Figure 12) remove the rubber grommet (2) (Figure 13) from the camera lens module.

11 Pierce the rubber grommet by passing the insert tool and cable through the center of the rubber grommet.

Figure 12 Grommet and RJ45 cable insert tool



12 Pass the insert tool and cable (1) (Figure 13) through the rubber grommet hole (2) (Figure 13) on the camera lens module.

13 Remove the insert tool, connect the RJ 45 cable to the camera lens module ethernet connector, and insert the rubber grommet into the camera lens module hole to prevent water/dust ingress.

14 Snap the camera lens module into the mounting plate and secure the two screws on the camera lens module into the two holes on the mounting plate using the T20 Torx wrench.

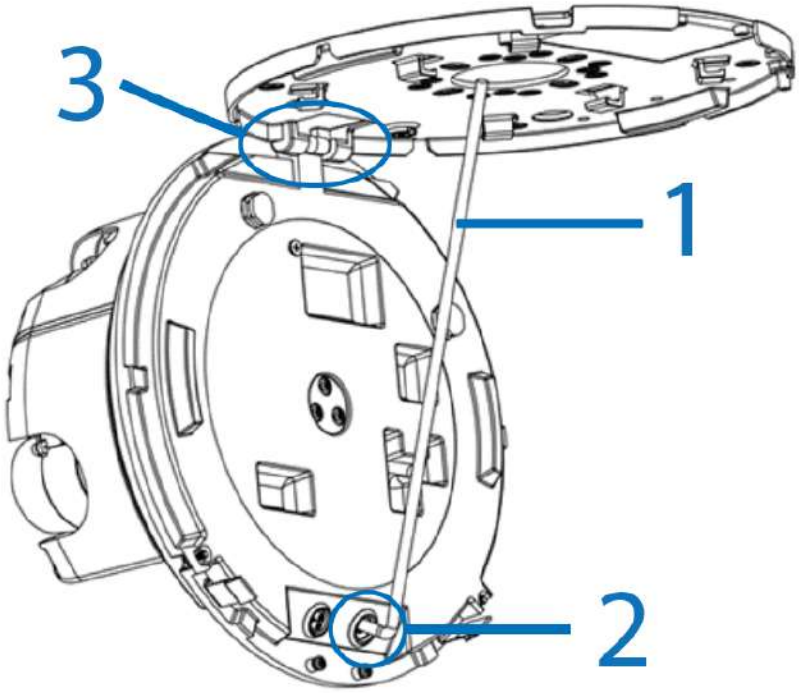
15 Based on your needs, connect the power cable to the power port through one of the following options.

- **PoE 802.3bt Type 4 (90w) Class 8 (71.3W / 0.96A):** Connect an Ethernet cable terminated with a RJ-45 connector to the PoE RJ-45 port for both power supply and network connectivity purposes simultaneously.
- **24V AC (81W / 3.54A):** Connect a power cable that supplies 24V AC power source to the power terminal.

OPTIONAL: Insert audio in / out cables and alarm in / out cables to the corresponding terminals on the camera if required and plug in a micro-USB device to the USB port.

Note: It is recommended to connect external microphones to ground (GND) on the digital I/O connector.

Figure 13 Cable inserted through the grommet



16 Hold the camera top cover (1) (Figure 3) up to the camera lens module and align the six holes on the camera top cover with the six holes on the camera lens module.

17 Insert the six screws and securely attached the camera top cover to the camera lens module.

- End -

Illustra Pro4 20MP and 32MP Multisensor Cameras (Phase 2)

This chapter provides product features, installation procedures, and connection information regarding the Illustra Pro4 20MP and 32MP Multisensor cameras.

Product overview

This chapter explains the features and installation of the Pro4 Multisensor cameras. Product code and description of the camera is provided in the table below.

Table 14 Product code and description of the Pro4 Multisensor cameras

Product Code	Description
IPS20-M12-OIA4	Illustra Pro 20MP (4x5MP) Multisensor, 2.7-13.5mm, Indoor/Outdoor, TDN w/IR, IK10, IP66
IPS32-M13-OIA4	Illustra Pro 32MP (4x8MP) Multisensor, 3.6-11mm, Indoor/Outdoor, TDN w/IR, IK10, IP66
IPS20-M12-OTA4	Illustra Pro 20MP (4x5MP) Multisensor, 2.7-13.5mm, Indoor/Outdoor, TDN, IK10, IP66
PS32-M13-OTA4	Illustra Pro 32MP (4x8MP) Multisensor, 3.6-11mm, Indoor/Outdoor, TDN, IK10, IP66

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
- 2 x Rubber grommets
- 4 x Plastic screw anchors
- 1 x T20 Torx Wrench
- 4 x T4 Self-tapping screws
- 1 x Side Cover
- 1 x RJ45 Insert Tool
- 2 x T20 Screw for Side Cover
- 1 x Mounting Template
- 1 x 12-pin Terminal connector for I/O function
- 1 x 2-pin Terminal block
- 1 x Printed Quick Start Guide
- 1 x Printed Regulatory Document

Contact your dealer if any item is missing.

Installation tools

The following tools assist with installation:

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

Quick Reference

- Default IP: 192.168.1.168 (DHCP enabled)
- Default Username / Password: admin / admin
- Power: PoE 802.3bt Type 4 (90w) Class 8 (71.3W / 0.96A) or 24V AC (81W / 3.54A)

Figure 15 Pro4 Multisensor Dome camera parts

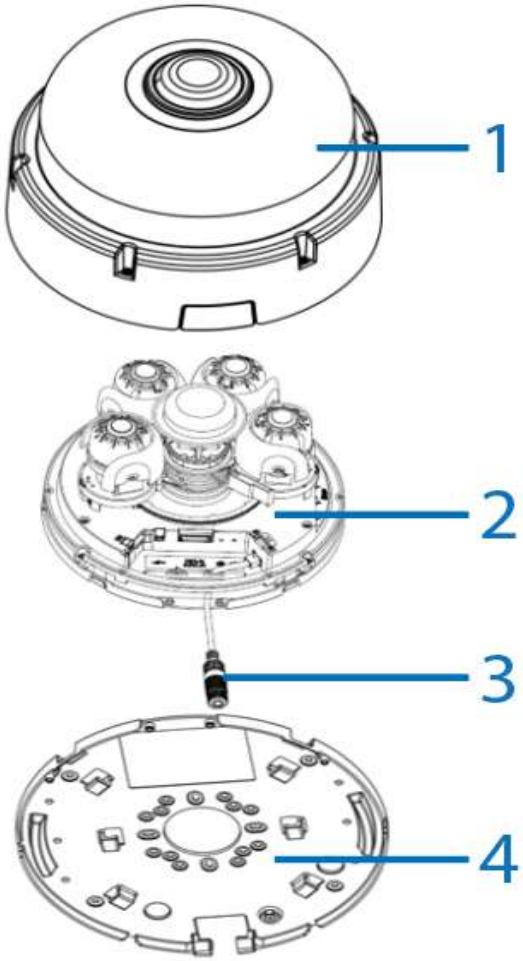


Table 16 Pro4 Multisensor Dome camera parts descriptions

Number	Description
1	Camera Top Cover with Bubble
2	Camera Lens Module
3	Pre-Fitted RJ45 cable
4	Mount Plate

Figure 17 Camera interior buttons / connections

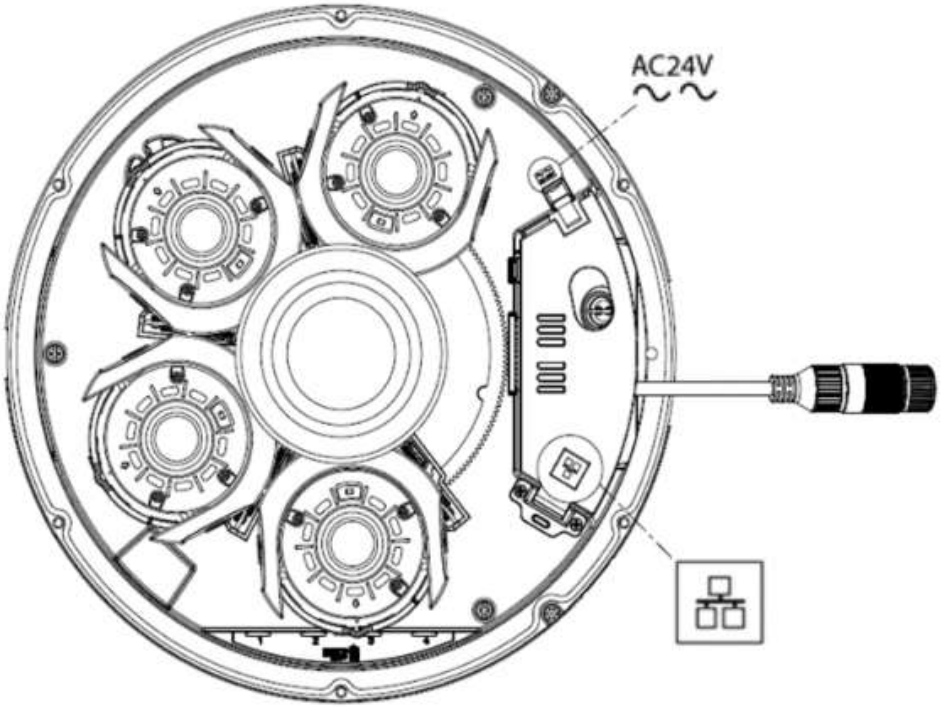
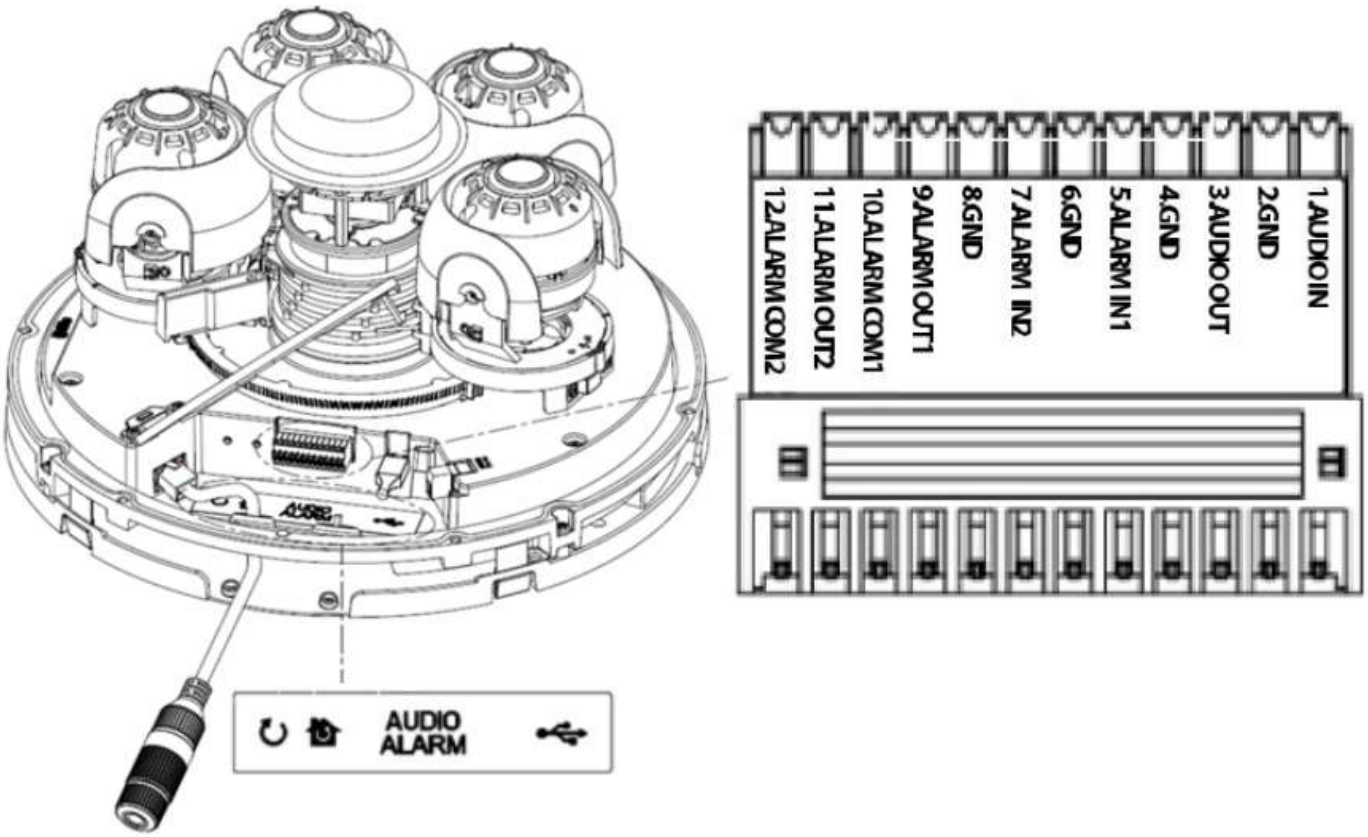


Figure 18 Camera interior buttons / connections



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.

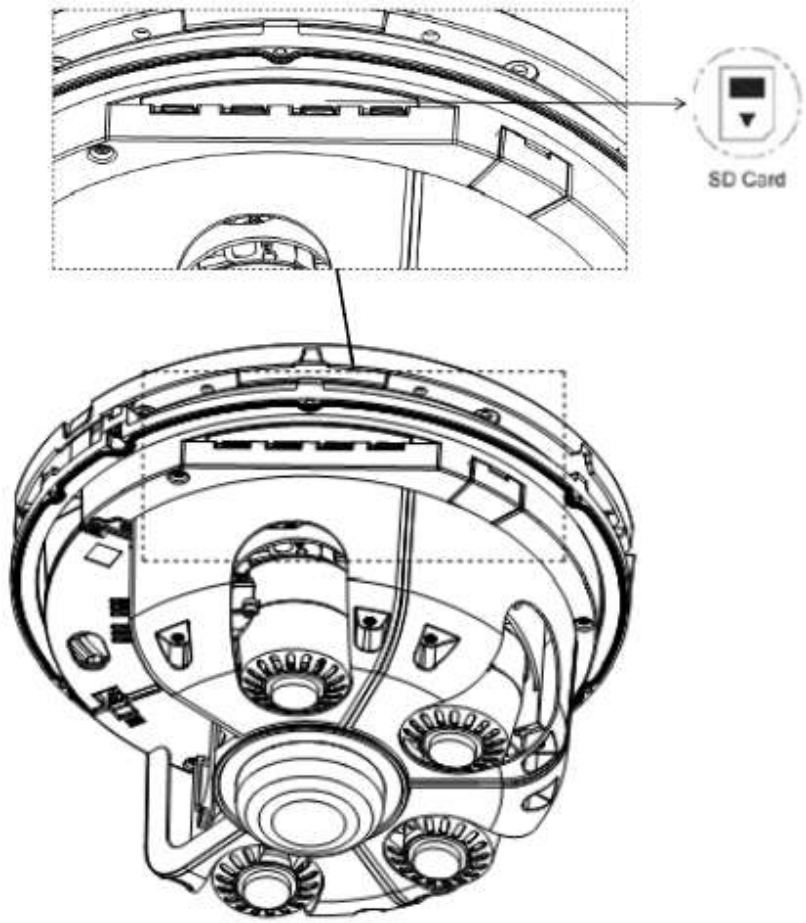
Table 19 Camera interior buttons / connections descriptions

Buttons / Connectors	Description
	PoE Ethernet port
	AC24V Power connector
	Reboots the camera (Press for 1 second)
	Reset to Factory default but preserve IP Address (Hold for 5 seconds) / Reset to factory default (Hold for 20 seconds)
AUDIO **ALARM**	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 camera. **Audio Out:** Via “GND” and “Audio Out” ports, connect to device such as speaker to be triggered through alarm output signals.
	Micro USB port

Procedure 4 Inserting or removing the SD card

Step	Action
1	Disassemble the camera as per steps 1 to 2 in ‘Disassembling the camera’ procedure and carefully insert or remove the micro-SD card (Figure 20) into or from the camera. **Note:**It is advised that you reboot the camera after inserting the micro-SD card.

Figure 20 SD Card cover

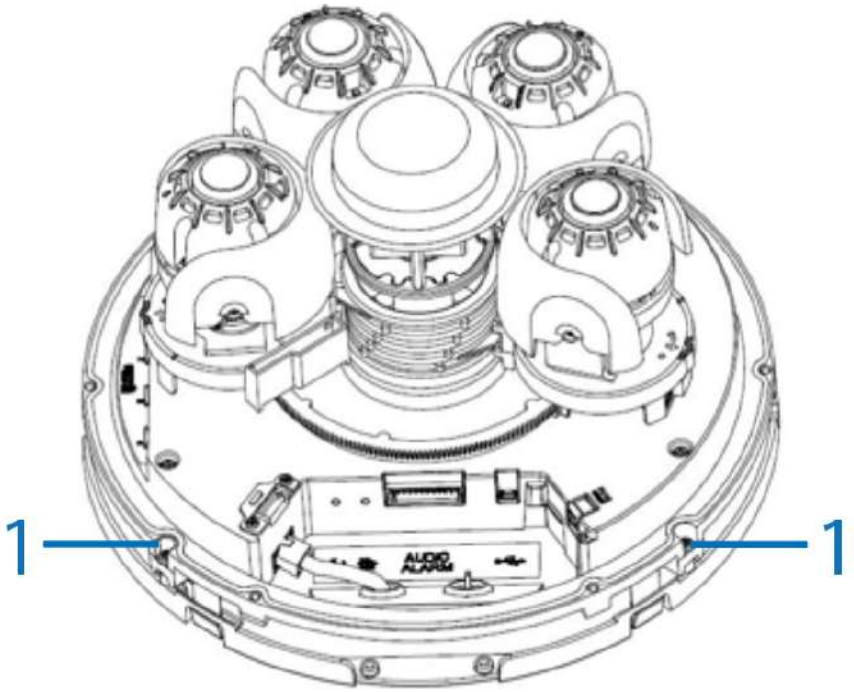


- End -

Procedure 5 Disassembling the camera

Step	Action
1	Use a T20 Torx wrench to remove the six screws located on the camera top cover (1) (Figure 15) and then remove the camera top cover. **Note:** The camera lens module (2) (Figure 15) is now exposed.
2	Use a T20 Torx wrench to remove the two screws (1) (Figure 21) on the camera lens module and remove the mounting plate (3) (Figure 15) from the camera lens module.

Figure 21 Camera lens module screws

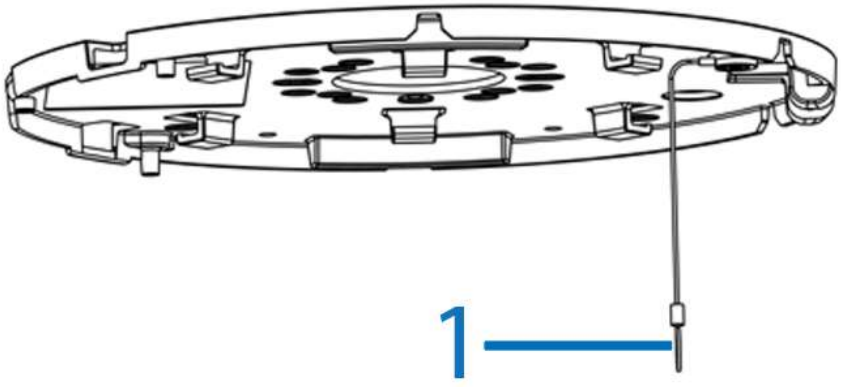


- End -

Procedure 6 Installing the camera onto a wall or ceiling

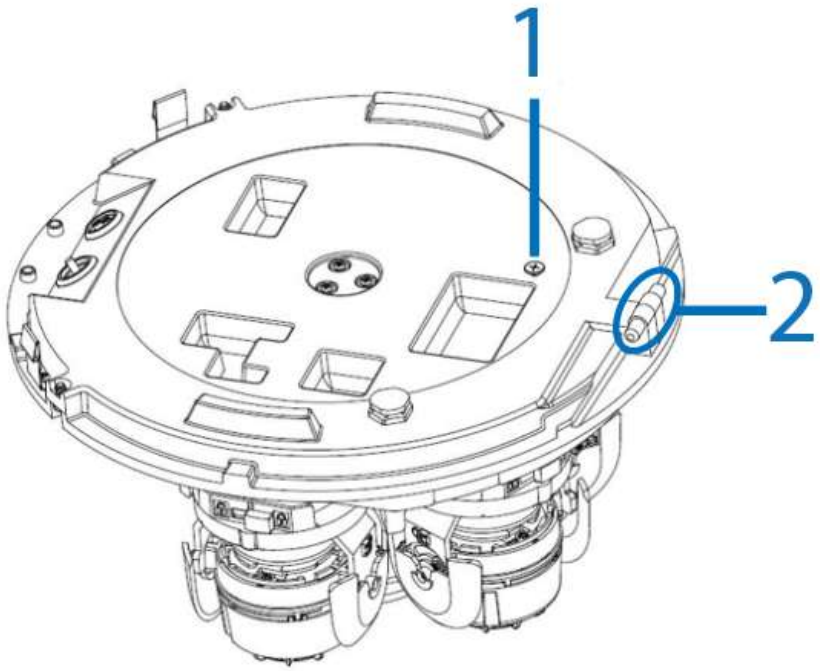
Step	Action
1	Disassemble the camera as per steps 1 to 2 in ‘Disassembling the camera’ procedure.
2	Hold the mounting template sticker up to the surface and mark out four holes as per the instructions on the template sticker.
3	Drill four holes on the surface and insert the four screw anchors into the four holes.
4	If you are not using the cable side entry hole on the mounting plate, then cut out a cable hole on the surface as per the instructions on the template sticker.
5	Hold the mounting plate (4) (Figure 15) up to the surface and align the four holes on the mounting plate with the four holes on the surface.
6	Insert the four TP4 self-tapping screws into the four holes and use the screwdriver to securely attach the mounting plate to the surface.
7	Hold the camera lens module up to the mounting plate and insert the ‘loop’ on the safety lanyard (1) (Figure 22) that is attached to the mounting template to the screw (1) (Figure 23) on the camera lens module.

Figure 22 Safety lanyard



8 Insert the ‘hinge pins’ (2) (Figure 23) on the camera module lens into the ‘hinge knuckle’ on the mounting plate. ‘1’ in Figure 25 identifies how the camera lens module and mounting plate attach together.

Figure 23 Safety lanyard screw and hinge pin



9 Pull all cables through the cable hole in the mounting plate.

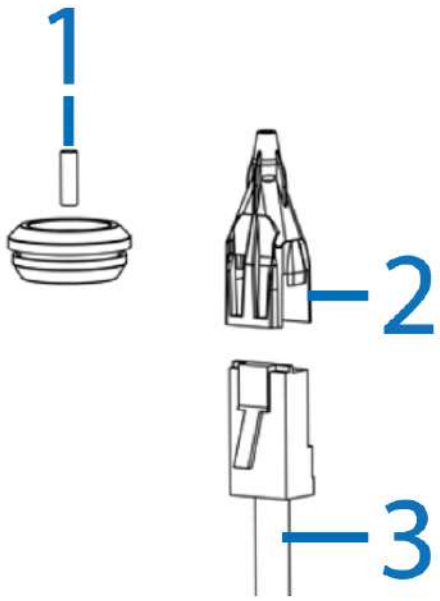
OR

If you are using the cable side entry on the mounting plate, remove the cable side entry cover screw and route all cables through the cable side entry.

10 Insert the RJ-45 cable (3) (Figure 24) into the insert tool (4) (Figure 24) and remove the rubber grommet (3) (Figure 25) from the camera lens module.

11 Pierce the rubber grommet by passing the insert tool and cable through the center of the rubber grommet.

Figure 24 Grommet and RJ45 cable insert tool



12 Pass the insert tool and cable (2) (Figure 25) through the rubber grommet hole (3) (Figure 25) on the camera lens module.

13 Remove the insert tool, connect the RJ 45 cable to the camera lens module ethernet connector, and insert the rubber grommet into the camera lens module hole to prevent water/dust ingress.

14 Snap the camera lens module into the mounting plate and secure the two screws on the camera lens module into the two holes on the mounting plate using the T20 Torx wrench.

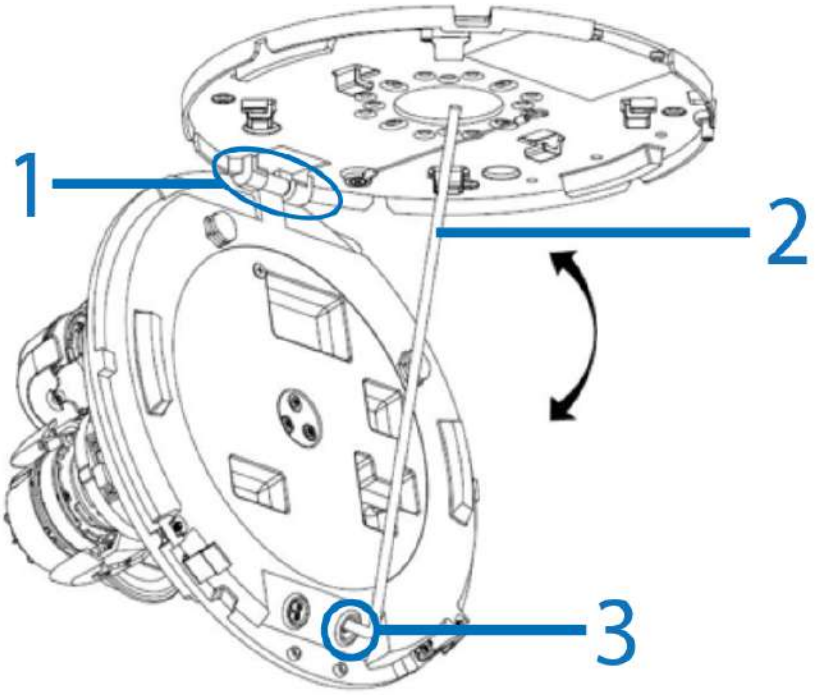
15 Based on your needs, connect the power cable to the power port through one of the following options.

- **PoE 802.3bt Type 4 (90w) Class 8 (71.3W / 0.96A):** Connect an Ethernet cable terminated with a RJ-45 connector to the PoE RJ-45 port for both power supply and network connectivity purposes simultaneously.
- **24V AC (81W / 3.54A):** Connect a power cable that supplies 24V AC power source to the power terminal.

OPTIONAL: Insert audio in / out cables and alarm in / out cables to the corresponding terminals on the camera if required and plug in a micro-USB device to the USB port.

Note: It is recommended to connect external microphones to ground (GND) on the digital I/O connector.

Figure 25 Cable inserted through the grommet



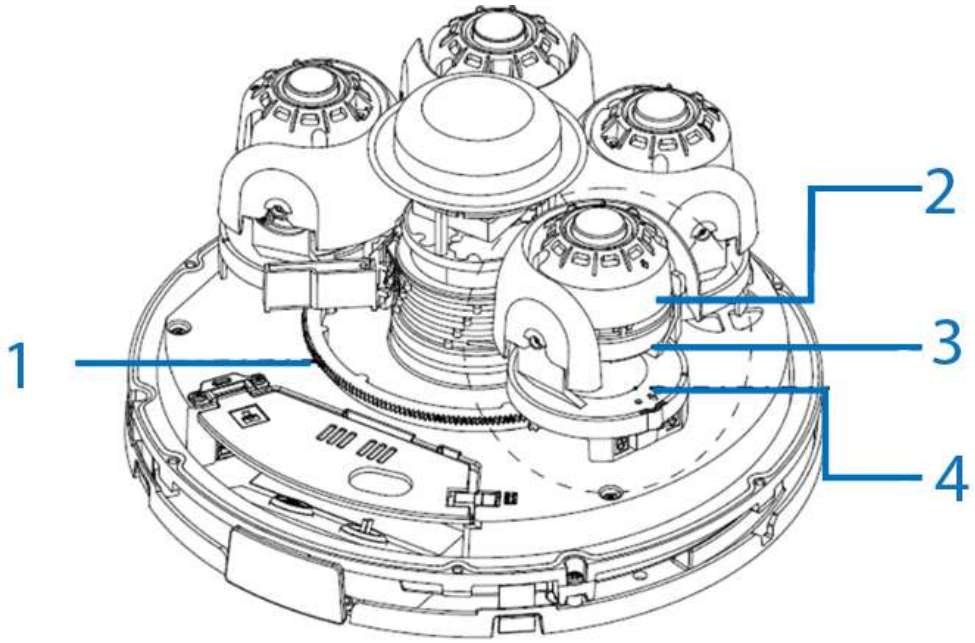
16 Hold the camera top cover (1) (Figure 15) up to the camera lens module and align the six holes on the camera top cover with the six holes on the camera lens module.

17 Insert the six screws and securely attached the camera top cover to the camera lens module.

- End -

Procedure 7 Adjusting the camera position

Figure 26 Adjusting the camera



1 Orbital pan: Pan range of the 4-axis gimbal is 0° to 360°.

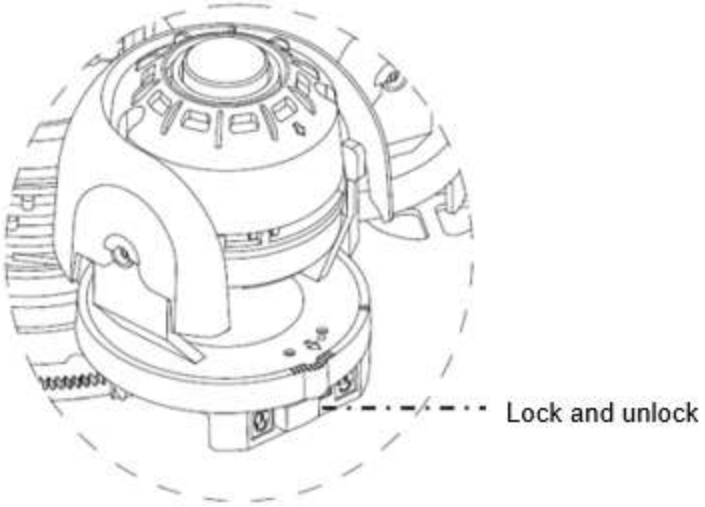
2 Rotate range: Rotate range of the 4-axis gimbal is 0° to 355°.

Note: Each camera lens has a lock and unlock mechanism. See Figure 27.

3 Tilt: Tilt range of the 4-axiz gimbal is 0° to 90°.

4 Individual Pan: Pan range of the 4-axiz gimbal is +/- 10°.

Figure 27 Lock and umlock mechanism



- End -

Network Topology

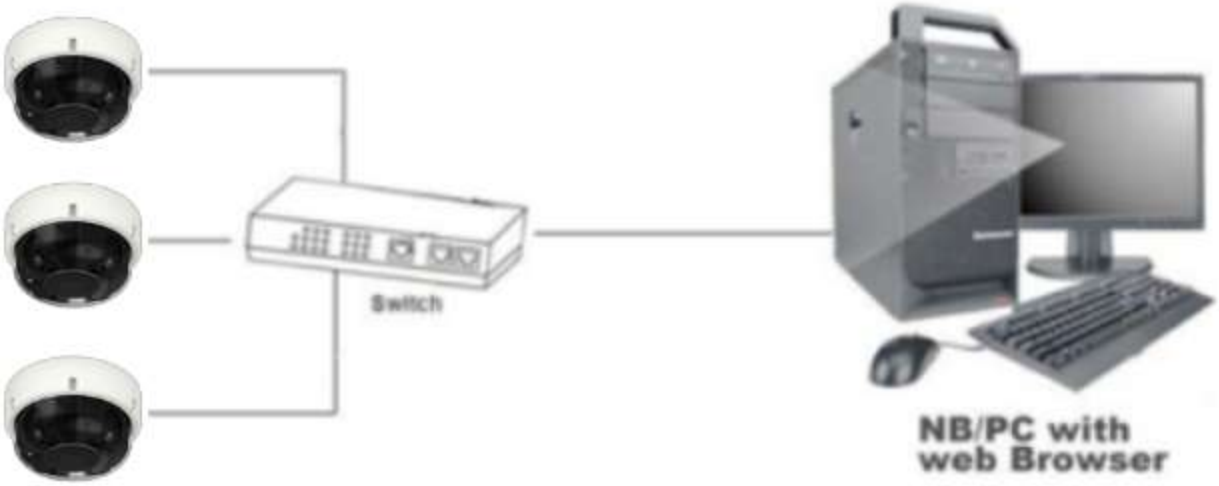
The Illustra Pro 4 Multisensor cameras deliver video images and audio in real-time using the internet and intranet. It is equipped with an Ethernet RJ-45 network interface.

The following images illustra the network topologies of the cameras.

Multisensor Dome Camera Topology

Figure 28 Dome Cameras Network Topology Type I.

Figure 29 Dome Cameras Network Topology Type II



Network Connection

Default IP Address

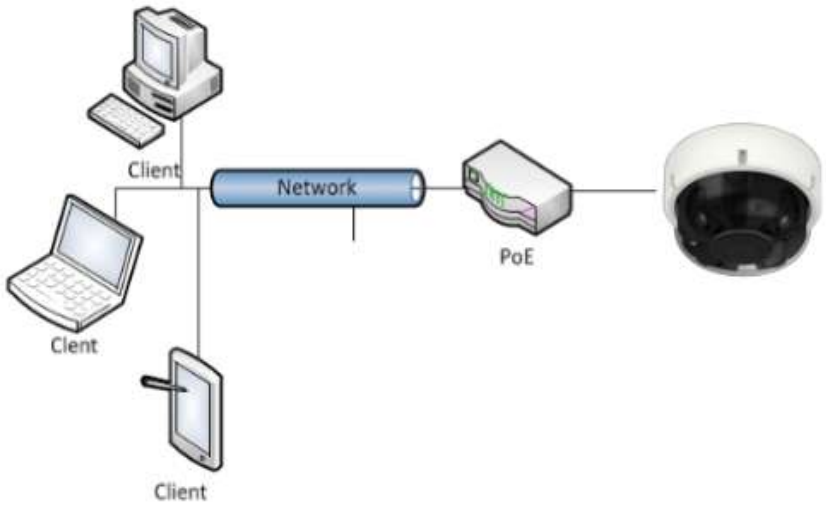
Since this is a network-based unit, an IP address must be assigned at the very first bootup. The default IP address of the unit is 192.168.1.168 and sub mask is 255.255.255.0.

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 30 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 8 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 9 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 10 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 36 for further information regarding using the Illustra Connect tool for configuring the cameras.

Procedure 11 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 12 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 13 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 14 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 Pro4 Multisensor cameras using the Web User Interface.

Note: The Pro4 Multi-sensor camera shares the GUI and functionality of the Pro4 dome camera series but with 4 individual camera sensors. This configuration requires some configuration settings to be applied globally (applied across the whole camera) and other configuration settings to be sensor specific. Any settings that are sensor specific will show the selected sensor at the top of the GUI and will be applied to that sensor only. For the purpose of the manual all instructions will be assumed to be global.

Figure 31 Sensors 1 to 4

Security Mode Profiles for First Time Connection

The Illustra Pro4 Multisensor 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 37 for further information regarding the differences between Standard and Enhanced Security modes.

Accessing the Illustra Pro4 Multisensor Camera Web User Interface

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

Procedure 15 Logging in to the Camera

Step	Action
1	Refer to Network Connection on page 32 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.

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 - @ % + \ / ‘ ! # $ ^ ? : , ( ) { } [ ] ~ - _ `

- The Multisensor camera offers an additional Wizard popup, this popup informs the user that on first boot a lens calibration is required. A question is then put to the end user if all packaging has been removed:

  a If all packaging is removed then select **Yes** to start the calibration for all sensors.

  OR

  a Select **No (skip)** if packaging is present to skip the process and not damage the lens but please note that a calibration will be required manually once packaging is removed.

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 16 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.

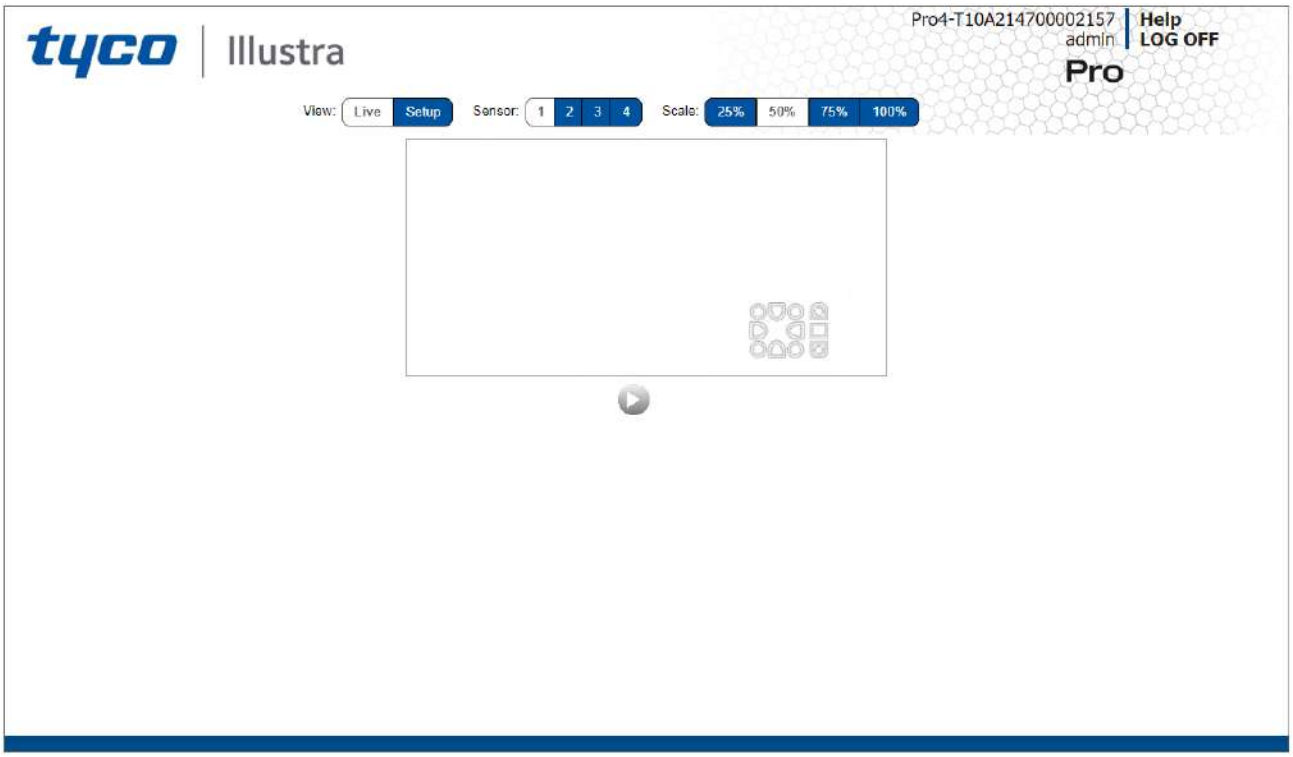
The camera web User Interface displays in the selected language.

- End -

Live menu

When you log in to the Illustra Web User Interface, the **Live** menu appears, as seen in Figure 32 on page 40.

Figure 32 Live menu page



Displaying the Live View Page

Display the live camera view page.

Procedure 17 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%.

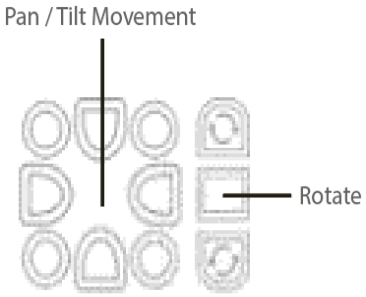
- End -

Controlling the PTR camera using camera controls.

The PTR camera can be controlled using the on-screen controls in the Live video pane.

GUI camera controls

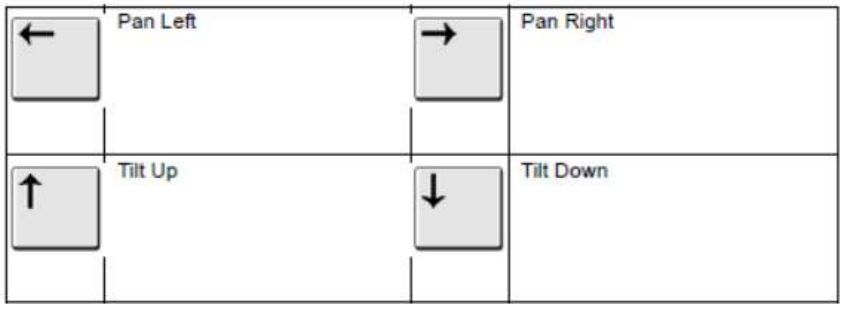
The following diagram provides information on the controls available for on-screen camera control. The camera control overlay is visible when video is displayed on the Live video pane.



Note: It is possible for two users to access live viewing at the same time. However, only one user may control the camera at any time. Camera control operates on a "last come, first served" basis. Therefore, when a new user logs into the camera from a different browser and starts a camera control session, the original user loses their camera control session.

Controlling the PTR Camera with the keyboard shortcuts

You can use the following keyboard shortcuts to control the camera.



Controlling the PTR camera with the camera controls

You can use the on-screen controls in the Live video pane to control the camera.

Procedure 18 Controlling the PTR Camera through the Live video pane

Step	Action
1	Select to start the live web video. The live video pane displays the current camera view.
2	Select the camera control item on the overlay to activate the control. Refer to GUI Camera Controls for information on specific camera controls.

- End -

Accessing the Setup Menus from Live View

Setup menus within the Web User Interface are restricted by user account access levels. Refer to Appendix A: User Account Access on page 1 for details on the features which are available to each role.

Procedure 19 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.

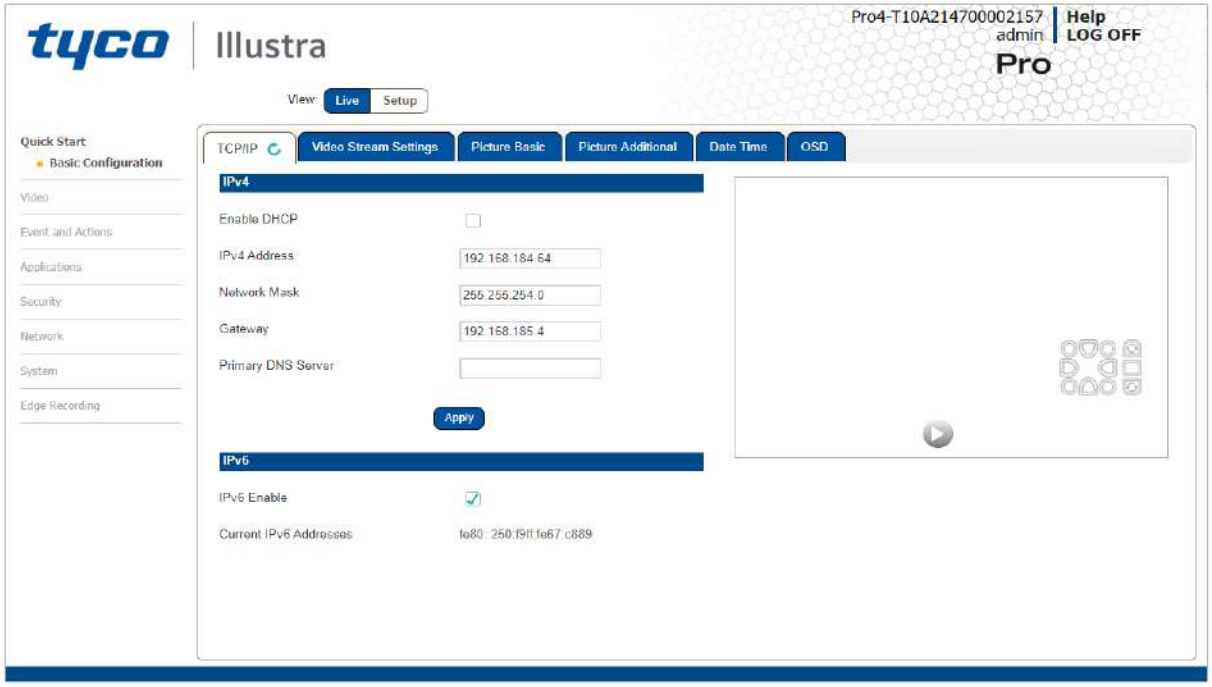
- End -

Quick Start Menu

When you select the Quick Start menu, the Basic Configuration Page displays, as shown in Figure 33 on page 43.

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 33 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 43 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 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 -

IPv4

Configure the IPv4 network settings for the camera.

Procedure 22 Configure the IPv4 Settings

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. 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 23 Enable/Disable IPv6

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 **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 four video streams per sensor on the camera: Stream 1, Stream 2, Stream 3 and Stream 4.

Configuring the Web Video Stream

Adjust the settings for each video stream.

Procedure 24 Configure the Video Stream settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
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	If MJPEG has been selected, MJPEG Quality is enabled. Use the slider bar to select the **MJPEG Quality**. The default setting is 50. OR
9	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 , CBR Bit Rate is enabled. Use the slider bar to select the **CBR 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 8000.

- End -

Procedure 25 Configuring IntelliZip Max GOP

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

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

- End -

Picture Basic

Configure the Auto Focus and Exposure settings on the camera.

When Auto Focus is enabled, the camera automatically compensates for scene changes that affect focal length (focus) and light levels (iris).

Setting Exposure

Configure the exposure settings for the camera. Automatic Gain Control (AGC) and Open Shutter provide additional functionality to help compensate for low-light scenes.

Max Gain

The Max Gain setting is an upper limit for how much gain can be increased when AGC is enabled. The trade-off between picture level (brightness) and noise may be adjusted by setting the Max Gain value. Lower values for Max Gain setting may result in a darker picture, but with less noise. Higher values for Max Gain setting may result in a brighter picture, but with more noise.

Exposure

Configure the exposure settings for the camera.

Procedure 26 Configure Exposure Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Picture Settings** 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 8000
- 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 8000
- 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

Manual

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 8000
- 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.

Shutter Priority

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 8000
- 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 8000
- 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

License Plate Recognition (LPR) low, mid and high

- Set camera Bitrate controller to CVBR

- Set Max Bitrate to 8000
- 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.

Gaming

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 8000
- 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)

Indoor

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 8000
- 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

Outdoor

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 8000
- 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 8000
- 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.

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

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

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

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

Note: The Iris Level differs depending on the camera.

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

13 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 -

Corridor Mode

Provides a better perspective when viewing a long corridor.

Procedure 27 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 28 Restore Exposure Defaults

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Picture Settings** 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 -

Setting Auto Focus

Enable or disable auto focus. **Auto Focus** is a camera feature that the user can use to control the camera auto-focusing on a static field of view. When auto-focus is on the camera focuses on the moving object.

Procedure 29 Enable/Disable Auto Focus

Step	Action
1	Select **Setup** on the GUI banner to display the setup menus.
2	Select the **Picture Basic** tab from the **Basic Configuration** menu.
3	Select the **Auto Focus** check box to enable auto focus. OR Deselect the **Auto Focus** check box to disable auto focus. The default setting is 'Enabled'.

- End -

Picture Additional

Configure Wide Dynamic Range, Day Night Mode, and Picture Adjustments including Brightness, Contrast, White Balance, Saturation and Sharpness which displays in the video pane.

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 30 Disable/Enable Wide Dynamic Range (WDR)

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Picture Additional** tab from the **Basic Configuration** menu.
3	Select the required WDR from the drop-down list: • **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 31 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.

- 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 32 Enable / Disable IR Illuminator

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
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 33 Configure Day Night Mode

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
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 brightness, contrast and saturation of the image displayed on the video pane.

Procedure 34 Adjust the Contrast, Saturation and Sharpness

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
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 35 Restore Picture Balance Defaults

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
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 36 Configure Auto White Balance

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
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
- **Indoor:**Suitable for indoor lighting conditions.
- **Outdoor:**Suitable for outdoor lighting conditions.

The default setting is ‘Auto Normal'.

- End -

Procedure 37 Manually Select White Balance

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
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 / OSD

Change the camera name, date and time and enable OSD.

Camera Name

The camera name displays on the Web User Interface banner and the on-screen display for the camera. This name also displays when using Illustra Connect or ONVIF.

Procedure 38 Changing the on screen camera text size

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
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 39 Change the Camera Name

Step	Action
1	Select **Setup** on the Web User Interface banner.
2	Select the **Date/Time/OSD** tab in the **Basic Configuration** menu.
3	Enter the name of the camera in the **Camera Friendly Name** text box.

- End -

Date / Time

Set the date and time on the camera.

Procedure 40 Configuring the Date and Time

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Date/Time/OSD** from the **Basic Configuration** 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: 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)

Within OSD you can set enable or disable camera name and time display.

Procedure 41 Display or Hide the Camera Name OSD

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **OSD** tab in the **Basic Configuration** menu.
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 42 Display or Hide the Camera Time OSD

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
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 43 Display or Hide the User Defined OSD

Step	Action
1	Select Setup on the Web User Interface banner to display the setup menus.
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)

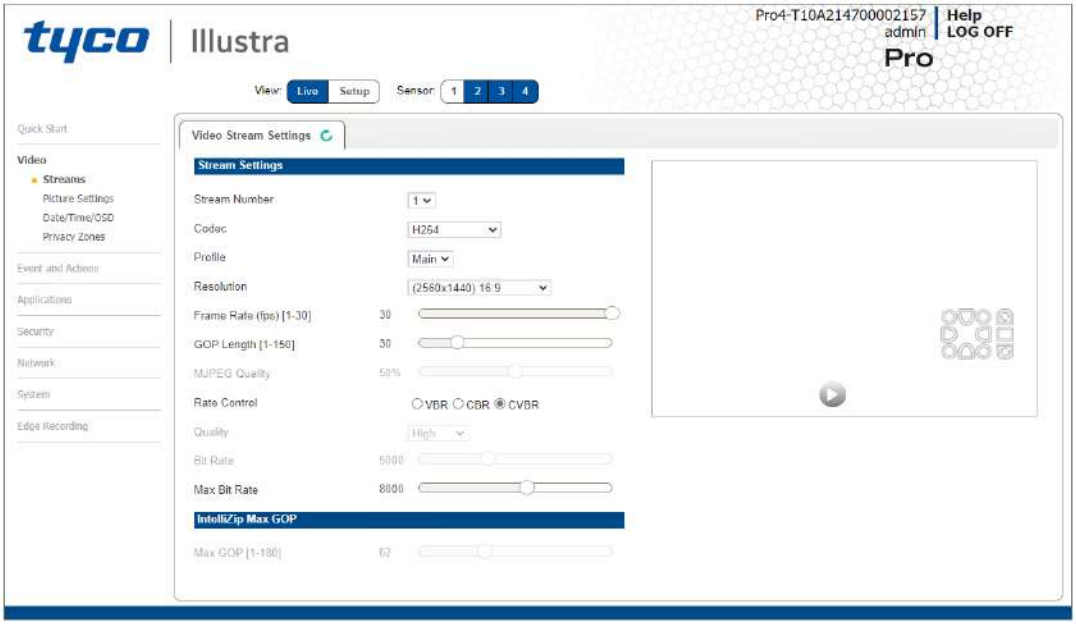
- End -

Video Menu

The camera is made up of four sensors. The selected sensor will be shown at the top of the GUI and any changes to video settings will apply to that sensor only with a few exceptions which are applied globally. When you select the **Video** menu, the **Streams** page displays, as seen in Figure 34 on page 61.

Figure 34 Sensors 1 to 4

Figure 35 Video Menu



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

- Streams
- Picture Settings
- Date / Time / OSD
- Privacy Zones

Streams

Four independent video streams can be configured per sensor.

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 4.

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 44 Configure the Video Stream settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Streams** tab in the **Video** menu.
3	Select **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 model 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 If MJPEG has been selected, MJPEG Quality enables. Use the slider bar to select the **MJPEG Quality**.

The default setting is 50.

OR

9 If H264 has been selected in step 4, Rate Control will be 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 VBR has been selected, 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 CBR has been selected, CBR Bit Rate will be enabled. Use the slider bar to select the **CBR 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 8000.

- End -

Procedure 45 Configuring IntelliZip Max GOP

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

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

The camera is made up of four sensors and you can configure the Auto Focus, Exposure, and Wide Dynamic Range (WDR) settings for each individual sensor.

Figure 36 Sensors 1 - 4

When Auto Focus is enabled, the camera automatically compensates for scene changes that affect focal length (focus) and light levels (iris).

Setting Exposure

Configure the exposure settings for the camera. Automatic Gain Control (AGC) and Open Shutter provide additional functionality to help compensate for low-light scenes.

Max Gain

The Max Gain setting is an upper limit for how much gain can be increased when AGC is enabled. The trade-off between picture level (brightness) and noise may be adjusted by setting the Max Gain value. Lower values for Max Gain setting may result in a darker picture, but with less noise. Higher values for Max Gain setting may result in a brighter picture, but with more noise.

Exposure

Configure the exposure settings for the camera.

Procedure 46 Configure Exposure Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Picture Settings** 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 8000
- 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 8000
- 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

Manual

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 8000
- 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.

Shutter Priority

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 8000

- 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 8000
- 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

License Plate Recognition (LPR) low, mid and high

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 8000
- 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.

Gaming

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 8000
- 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)

Indoor

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 8000
- 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

Outdoor

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 8000
- 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 8000
- 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.

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

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

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

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

Note: The Iris Level differs depending on the camera.

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

13 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 -

Corridor Mode

Provides a better perspective when viewing a long corridor.

Procedure 47 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 48 Restore Exposure Defaults

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Picture Settings** 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 -

Setting Auto Focus

Enable or disable auto focus. **Auto Focus** is a camera feature that the user can use to control the camera auto-focusing on a static field of view. When auto-focus is on the camera focuses on the moving object.

Procedure 49 Enable/Disable Auto Focus

Step	Action
1	Select **Setup** on the GUI banner to display the setup menus.
2	Select the **Picture Basic** tab from the **Basic Configuration** menu.
3	Select the **Auto Focus** check box to enable auto focus. OR Deselect the **Auto Focus** check box to disable auto focus. The default setting is 'Enabled'.

- End -

Picture Additional

Configure Wide Dynamic Range, Day Night Mode, Flicker Control and Picture Adjustments including Brightness, Contrast, White Balance, Saturation and Sharpness displayed in the video pane.

Wide Dynamic Range

Wide Dynamic Range (WDR) is a feature that allows 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 an 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 50 Disable/Enable Wide Dynamic Range (WDR)

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Picture Additional** tab from the **Picture Settings** menu.
3	Select the required WDR from the drop-down list: • **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 the 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 51 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 OFF.

- 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 52 Enable / Disable IR Illuminator

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
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 ‘Disabled’.

- 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 53 Configure Day Night Mode

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
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 displays, the user can adjust the setting to suit the environment.

The default setting is 'Auto Mid'.

- End -

Picture Adjustment

Adjust brightness, contrast, and saturation of the image displaying on the video pane.

Procedure 54 Adjust the Contrast, Saturation and Sharpness

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
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	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 55 Restore Picture Balance Defaults

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

- End -

White Balance

White balance, the ability to keep whites looking white, is normally compensated for automatically via 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 56 Configure Auto White Balance

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
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 Wide:** Suitable for a wider than normal range of lighting conditions • **Auto Normal:** Suitable for a normal range of lighting conditions • **Manual:** Adjustable red and blue balance The default setting is 'AutoNormal'.

- End -

Procedure 57 Manually Select White Balance

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
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 / OSD

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

Camera Name

The camera name will be displayed on the Web User Interface banner and the on-screen display for the camera. This name will also be displayed when using Illustra Connect or ONVIF.

Procedure 58 Changing the on screen camera text size

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
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 59 Change the Camera Name

Step	Action
1	Select **Setup** on the Web User Interface banner.
2	Select **Date/Time/OSD** from the **Video** menu.
3	Enter the name of the camera in the **Camera Friendly Name** text box.

- End -

Date / Time

Set the date and time on the camera.

Procedure 60 Configuring the Date and Time

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Date/Time/OSD** from the **Video** 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:

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)

Within OSD you can set enable or disable camera name and time display.

Procedure 61 Display or Hide the Camera Name

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Date/Time/OSD** tab in the **Basic Configuration** menu.
3	Select the **Camera Name** check box to display the camera name in the OSD. OR Deselect the **Camera Name** check box to hide the camera name in the OSD. The default setting is ‘Disabled’.

- End -

Procedure 62 Display or Hide the Camera Time

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Date/Time/OSD** tab in the **Basic Configuration** menu.
3	Select the **Time** check box to display the camera name in the OSD. OR Deselect the **Time** check box to hide the camera name in the OSD. The default setting is ‘Disabled’.

- End -

Procedure 63 Display or Hide the User Defined OSD

Step	Action
1	Select Setup on the Web User Interface banner to display the setup menus.
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 -

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 8 rectangular privacy zones can be used on the camera.

Defining a Privacy Zone

Create a privacy zone on the camera.

Procedure 64 Define a Privacy Zone

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Privacy Zones** from the **Video** menu.
3	Select to start the video stream if it is not already active. The video pane displays the current camera view.
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. **Note:**It is advised that you draw privacy zones larger than required to help ensure better coverage during the PTR operations. This compensates for privacy zone distortion and repositioning during Pan, Tilt and Rotate.
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 65 Enable/Disable a Privacy Zone

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Privacy Zones** from the **Video** menu. The **Privacy Zones** tab displays.
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 66 Delete a Privacy Zone

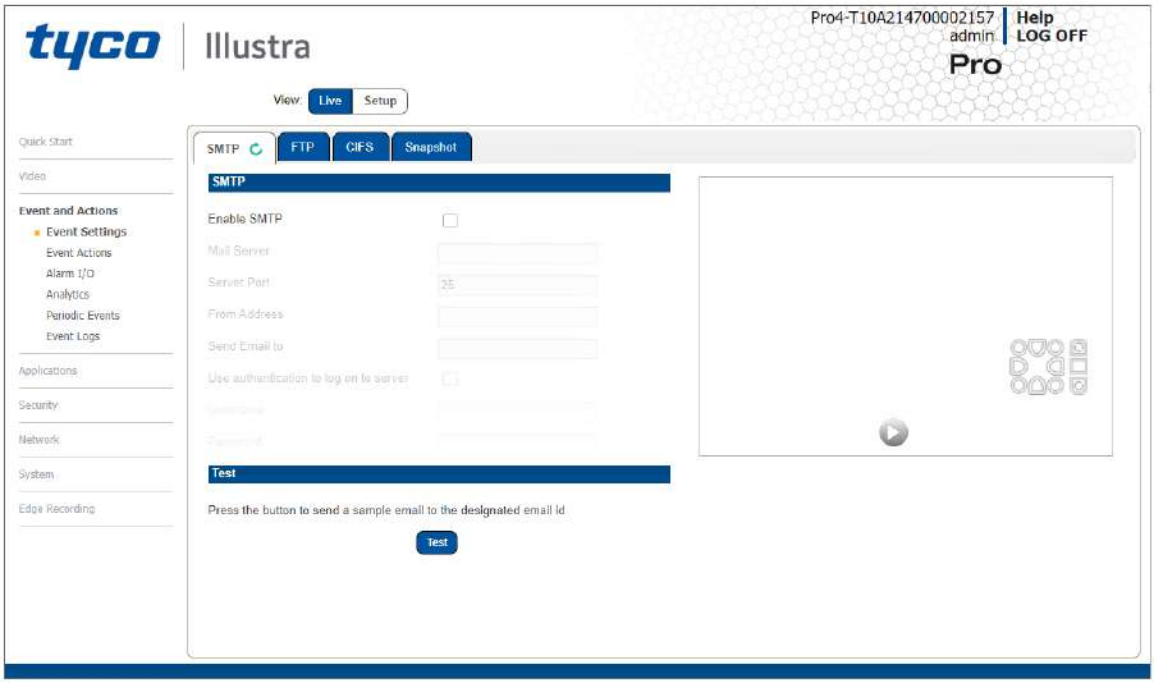
Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Privacy Zones** from the **Video** menu. The Privacy zones tab displays.
3	Select the corresponding **Delete** check box to mark the privacy zone for deletion.
4	Select **Delete** to delete the selected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

- End -

Events and Actions Menu

When you select the Events and Actions menu the Event Settings page displays, as seen in Figure 37 on page 78.

Figure 37 Events and Actions Menu



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

- Event Settings
- Event Actions
- Alarms I / O
- Analytics
- 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 67 Configure SMTP Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Event Settings** from the **Events and Actions** menu.
3	Select the **SMTP** tab.
4	Select the **Enable SMPT** check box to enable SMTP. Fields on the tab become available for entry of information. OR Clear the **Enable SMPT** check box to disable SMTP. The default setting is 'Disabled'. **Note:**When in Enhanced Security mode, enabling SMTP requires the admin account password.
5	Enter the IP Address of the mail server in the **Mail Server** text box.
6	Enter the server port in the **Server Port** text box. The default setting is ‘25’.
7	Enter the from email address in the **From Address** text box.
8	Enter the email address to send email alerts to in the **Send Email to** text box.
9	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’.
10	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 -

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 68 Configure FTP Server Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Event Settings** from the **Events and Actions** menu.
3	Select the **FTP** tab.
4	Select the **Enable FTP** check box to enable FTP. OR Clear the **Enable FTP** check box to disable FTP. The default setting is 'Enabled'.
5	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.
6	Enter the IP address of the FTP Server in the **FTP Server** text box.
7	Enter the FTP username in the **Username** text box.
8	Enter the FTP password in the **Password** text box.
9	Enter the FTP upload path in the **Upload Path** text box. **Note:** Refer Test the FTP Settings on page 81 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 69 Configure the FTP Transfer Rate

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Event Settings** from the **Events and Actions** menu.
3	Select the **FTP** tab.
4	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'.
5	Enter the Max Transfer Rate in the **Max Transfer Rate** (Kbps) textbox.

- End -

Test FTP Settings

Test the SMTP settings that have been configured in Procedure 7-4 Configure FTP Server Settings.

Procedure 70 Test the FTP Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Event Settings** from the **Events and Actions** menu.
3	Select the **FTP** tab.
4	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 71 Configure CIFS Server Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Event Settings** from the **Events and Actions** menu.
3	Select the **CIFS** tab.
4	Select the **Enable** check box to enable CIFS.
	OR
	Clear the **Enable** check box to disable CIFS.
	The default setting is ‘Enabled’.
5	Enter the network path in the **Network Path** text box.
6	Enter the domain name in the **Domain Name** in the text box.
7	Enter the username in the **Username** text box.
8	Enter the password h in the **Password** text box.

- 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 72 Enable a snapshot

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Event Settings** from the **Events and Actions** menu.
3	Select the **Snapshot** tab.
4	Select the **Enable** check box to enable Snapshot. OR Clear the **Enable** check box to disable Snapshot. The default setting is 'Disabled'.
5	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 73 Create an Event Action

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Event Actions** from the **Events and Actions** menu.
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 **Email** check box to send an e-mail to the email address configured in the Configure SMTP Settings procedure.

7 Select the **FTP** check box to send a video file to the FTP details configured in the Configure FTP Server Settings procedure.

8 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.

9 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.

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

- End -

Editing a Event Action

Modify the details of an existing event action.

Procedure 74 Edit an Event Action

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Event Actions** from the Events and Actions menu.
3	Select an entry on the event actions list, you can edit the following: • **Name** • **Output** - Enable/Disable • **Record** - 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 75 Configure an Alarm

Step	Action
1	Select **Alarm I/O** from the **Event and Actions** menu.
2	Enter the alarm name in the **Name** text box.
3	Select the **Enabled** check box to enable the alarm. OR Clear the **Enabled** check box to disable to alarm.
4	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.
5	Select the required configured fault action from the **Action** drop down menu.

- End -

Procedure 76 Enable/Disable an Alarm

Step	Action
1	Select **Alarm I/O** from the **Event and Actions** menu.
2	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 77 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 -

- End -

Procedure 78 Clearing Alarm Output

Step	Action
1	Select **Alarm I/O** from the **Event and Actions** menu.
2	Under **Alarm Output**, select the **Apply** button to Clear Active Output. The Alarm Output is cleared.

- End -

Analytics

Analytics is a feature which detects and tracks objects in video. Analytics supported are Region of Interest, Motion Detection, and Blur Detection.

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 79 Configure a Region of Interest

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Analytics** from the **Events and Actions** menu. The **ROI** tab displays.
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 80 Delete a Region of Interest

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Analytics** from the **Events and Actions** menu. The **ROI** tab is displays.
3	Select to delete the corresponding region of interest.

- End -

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 reques in order to enable the feature.

Procedure 81 Enable / Disable Face Detection

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Analytics** from the **Events and Actions** menu. The ROI tab is displayed.
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. • **Top** • **Left** • **Right** OR Deselect the **Enable Face Detection** checkbox to disable Face Detection on the camera.
4	Select the required preconfigured 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 82 Create a Motion Detection Alert

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Analytics** from the **Events and Actions** menu.
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 83 Enable or Disable a Motion Detection Alert

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Analytics** from the **Events and Actions** menu.
3	Select the **Motion Detection** tab. The Motion Detection Configuration pane displays.
4	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.
5	Select **Apply** to save.

- End -

Artificial Intelligence Object Classification

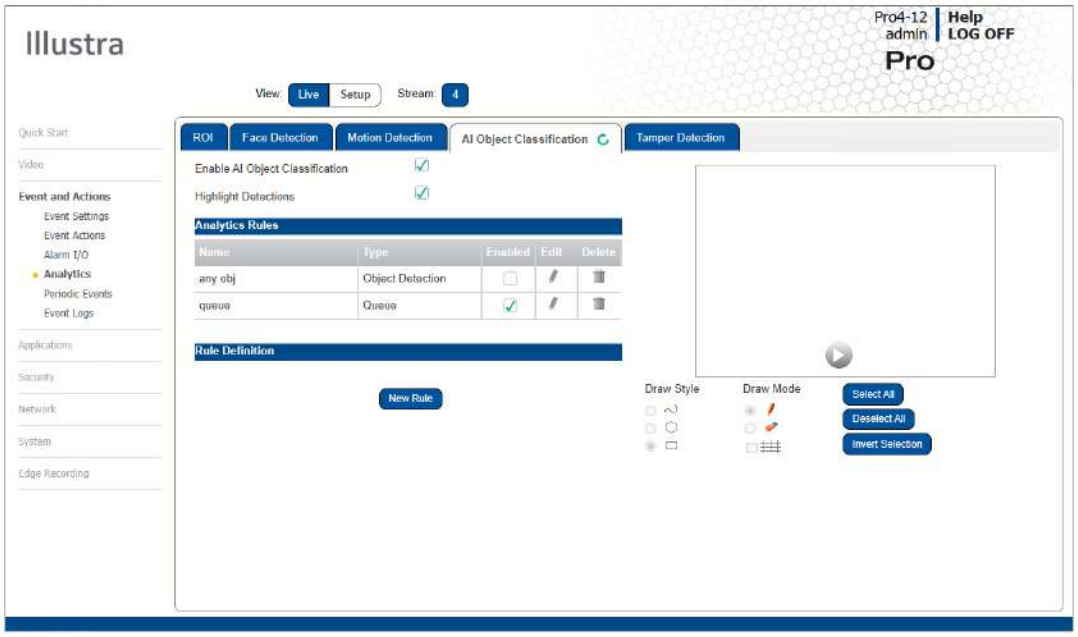
Artificial Intelligence Object Classification Camera Alarms

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 38 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

Artifical Intelligence Object Classification

In this section you can configure '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 84 Enable/Disable AI Object Classification

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Analytics** from the **Events and Actions** menu.
3	Select the **AI Object Classification** tab.
4	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. e 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.

- End -

Procedure 85 Creating a Analytic Rule in AI Object Classification

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Analytics** from the Events and Actions menu.
3	Select the **AI Object Classification** tab.
4	Select the **Enable AI Object Classification** check box to enable AI Object Classification on the camera.
5	Select **New Rule.**
6	Type a **Rule Name** for your rule definition in the field provided.
7	Select a fault action from the **Action** drop-down menu. This fault action is activated when the parameters of the analytics rule are met.
8	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.

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

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

10 Use the **Minimum Confidence** slider bar to increase or decrease the percentage of confidence.

11 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.

Minimum Confidence level - Minimum confidence is the minimum percentage of confidence required to trigger an event.

- End -

Procedure 86 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.
2	Select **Analytics** from the Events and Actions menu.
3	Select the **AI Object Classification** tab.
4	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 87 Edit an Analytics Rule

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

- End -

Procedure 88 Delete an Analytics Rule

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Analytics** from the **Events and Actions** menu.

3 Select the **AI Object Classification** tab.

4 From the **Analytics Rules** table, select the delete icon across from the analytics rule that you want to delete.

5 Select **OK** when you are asked to confirm your action.

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

- 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 89 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 90 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 91 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 92 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 -

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 93 Configure a Periodic Event

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Periodic Events** from the **Events and Actions** menu. The **Periodic Events** tab displays.
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 94 Display Event Log

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

- End -

Procedure 95 Delete Current Events

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Event Logs** from the **Event and Actions** menu. The Event Logtab displays.
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 96 Display Current Faults

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

- End -

Procedure 97 Delete Current Faults

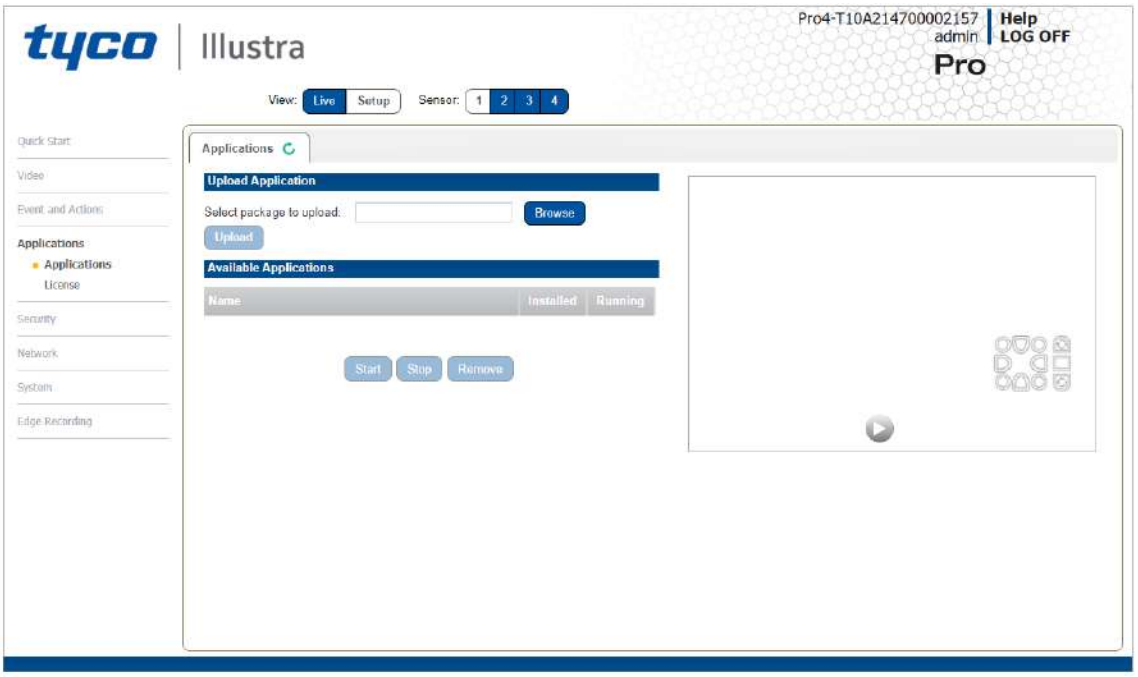
Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Event Logs** from the **Events and Actions** menu.
3	Select the **Fault Log** tab.
4	Select the corresponding **Delete** check box to mark the fault for deletion. OR Clear the corresponding **Delete** 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.
5	Select **Delete** to delete the selected faults. You are prompted to confirm the deletion.
6	Select **OK** to confirm the deletion. OR Select **Cancel**.

- End -

Applications

When you select the Applications menu the Applications page displays, as seen in on page 100.

Figure 39 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.

Applications

Procedure 98 Upload an Application

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Applications** menu. The Applications tab displays.
3	Select **Browse**. The Choose file dialog is displayed.
4	Navigate to the location where the application has been saved.
5	Select the application file then select the **Open** button.
6	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 99 Start, Stop or Remove an Application

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Applications** menu. The Applications tab displays.
3	Select the corresponding **Application** checkbox to Start, Stop or Remove.
4	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 100 Upload a License File

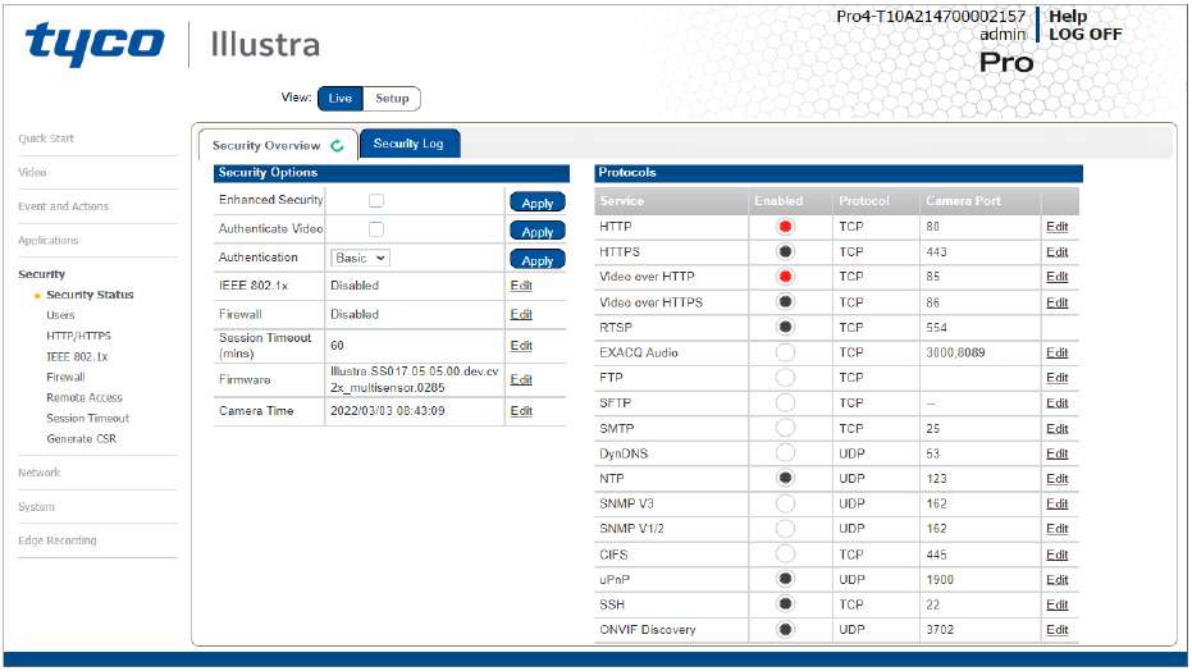
Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **License** from the **Applications** menu.
3	Select **Browse**. The Choose file dialog is displayed.
4	Navigate to the location where the license file has been saved.
5	Select the license file then select 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 40 on page 102.

Figure 40 Security menu



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

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

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 37.

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

Procedure 101 Enable Enhanced Security

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Security Status** from the **Security** menu.
3	Select the **Security Overview** tab.
4	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 Enchanced Security feature. Your password must adhere to the minimum requriments 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.
5	Enter the current password in the **Current Password** text box.
6	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
7	Re-enter the new password in the **Confirm Password** text box.
8	Click **Apply**. **Note:**Any changes to the Security Mode are logged in the Security Log.

- End -

Procedure 102 Disable Enhanced Security Mode

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Security Status** from the **Security** menu.
3	Select the **Security Overview** tab.
	Note: When in Enhanced Security mode, changing the security mode requires the admin account password.
4	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: HTTP, FTP, CIFS, Dyn DNS, SMTP, HTTPS, SNMP V1/2, SNMP V3, uPNP, and SFTP.

Security Overview

Procedure 103 Enable/Disable Communication Protocols

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Security Status** from the **Security** menu.
3	Select the **Security Overview** tab.
4	Select or clear the **Protocols** check box to enable or disable that protocol.
5	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.

Security Log

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

Procedure 104 Display Security Log

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Security Status** from the **Security** menu.
3	Select the **Security Log** tab.

4 Select **Refresh** to refresh the log for the most up-to-date information.

- End -

Procedure 105 Filter the Security Log

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Security Status** from the **Security** menu.
3	Select the **Security Log** tab.
4	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.
5	Enter the word or phrase that you would like to search for in the **Filter (only lines containing text)** text box.
6	Select **Refresh** to refresh the log for the most up-to-date information that meets the filter parameters.
7	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.

Refer to Appendix A: User Account Access on page 1 for details on the features which are available to each role.

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 106 View User Accounts

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Users** from the **Security** menu. The current user accounts assigned to the camera display.

- End -

Add User

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

Procedure 107 Add a User

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Users** from the **Security** menu.
3	Select the **Add User** tab.
4	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(.)
5	Select a **Role**: • admin • operator • user Refer to Appendix A: User Account Access for details on the features which are available to each role.

6	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

7	Enter the same password in the **Confirm Password** text box.
8	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 108 Change User Password

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Users** from the **Security** menu.
3	Select the **Change Password** tab.
4	Select the user account from the **Name** drop-down menu.
5	Enter the current password for the user account in the **Current Password** text box.
6	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.
7	Enter the same new password in the **Confirm New Password** text box.
8	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 109 Delete a User Account

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Users** from the **Security** menu. The Users tab displays.
3	Select to delete the corresponding user account. You will be prompted to confirm the deletion.
4	Select **OK** to delete. OR
5	Select **Cancel**.

- 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 110 Specify HTTP Method

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **HTTP/HTTPS** from the **Security** menu.
3	Select the **HTTP Method** using the radio buttons • **HTTP** • **HTTPS** • **Both**

- End -

Procedure 111 Add a HTTPS Certificate

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **HTTP/HTTPS** from the **Security** menu.
3	Click on the **Upload** button and navigate to the certificate location.
4	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 112 Delete a HTTPS Certificate

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **HTTP/HTTPS** from the **Security** menu.
3	Select **Delete**. The camera displays a “Restarting HTTPS Service” page with a progress bar showing the deletion progress.
4	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 113 Configure IEEE 802.1x Security

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **IEEE 802.1x** from the **Security** menu. The **EAP Settings** tab displays.
3	Select the **Enable IEEE802.1x** check box to enable IEEE802.1x security . OR
4	Clear the **Enable IEEE802.1x** check box to disable IEEE802.1x security.
5	Select the **EAPOL Version** from the drop-down menu.
6	Select the **EAP Method** using the radio buttons.
7	Enter the EAP identity name in the **EAP Identify** textbox.
8	Select **Upload** to navigate to the **CA Certificate** location.The Choose file dialog displays.
9	Navigate to the location where the certificate has been saved. Select the file and select **Open**.
10	Select **Upload**. The upload process starts.
11	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 114 Enable/Disable Basic Filtering

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Firewall** from the **Security** menu. The **Basic Filtering** tab displays.
3	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'.
4	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'.
5	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 115 Enable/Disable and configure Address Filtering

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Firewall** from the **Security** menu.
3	Select the **Address Filtering** tab.
4	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'.

5 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**.

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

- End -

Editing an Address Filter

Edit an existing address filter.

Procedure 116 Edit an Address Filter

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Firewall** from the **Security** menu.
3	Select the **Address Filtering** tab.
4	Edit the IP or MAC Address in the **IP or MAC Address** text box.
5	Select **Add** to save the changes.

- End -

Deleting an Address Filter

Delete an existing address filter.

Procedure 117 Delete an Address Filter

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Firewall** from the **Security** menu.
3	Select the **Address Filtering** tab.
4	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 118 Configure SSH

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Remote Access** from the **Security** menu. The **Remote Access** tab displays.
3	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 119 Enable/Disable ONVIF Discovery Mode

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Remote Access** from the **Security** menu. The Remote Access tab displays.
3	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 120 Enable/Disable ONVIF User Authentication

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Remote Access** from the **Security** menu. The Remote Access tab displays.
3	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 121 Enable/Disable Video over HTTP

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Remote Access** from the **Security** menu. The Remote Access tab displays.
3	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 122 Enable/Disable Video over HTTPS

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Remote Access** from the **Security** menu. The Remote Access tab displays.
3	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 123 Enable/Disable UPnP Discovery

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Remote Access** from the **Security** menu. The Remote Access tab displays.
3	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 124 Enable/Disable EXACQ Audio

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Remote Access** from the **Security** menu. The Remote Access tab displays.
3	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 125 Set a Session Timeout time

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Session Timeout** from the **Security** menu. 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

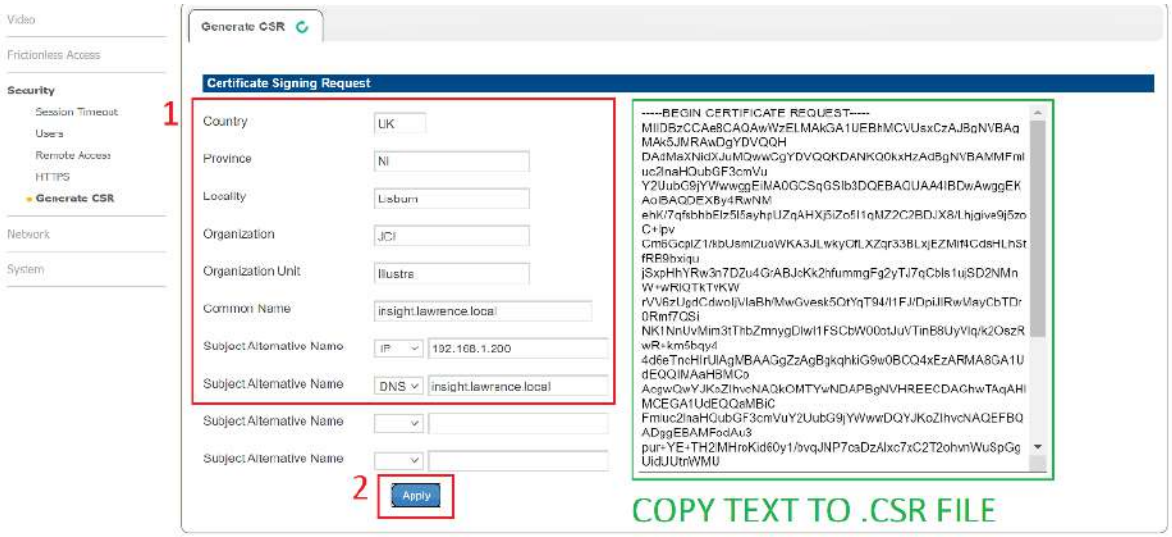
When accessing a camera web GUI via HTTPS, the browser shows an insecure / not secure browser warning. This warning is due to the camera having a 'self-signed certificate'; which offers communication encryption but cannot be used for authentication. Introduction of the Certificate Signing Request (CSR) 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 126 Generate a .csr file

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select Generate CSR from the Security menu.
3	Enter information into the Request form and select Apply, Items 1 & 2 in the image below.

Figure 41 .CSR file tab



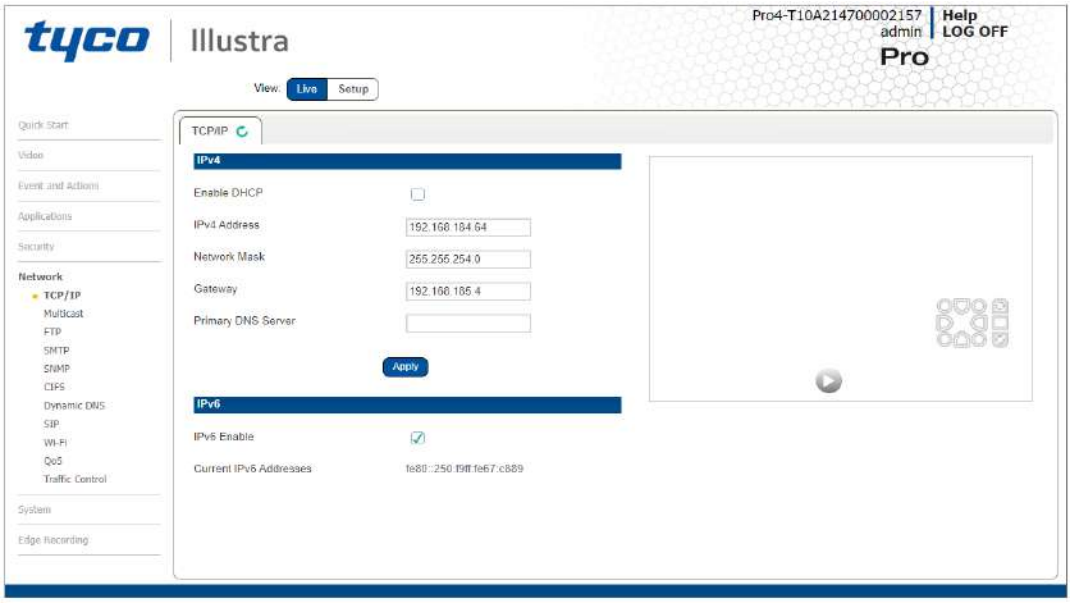
4 Copy the text shown in Green above & paste into a text file with .csr file extension.

- End -

Network Menu

When you select the **Network** menu, the **TCP/IP** page displays, as seen in Figure 42 on page 117.

Figure 42 Network Menu



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

- TCP/IP
- Multicast
- FTP
- SMTP
- SNTP
- CIFS
- Dynamic DNS
- SIP
- Wi-Fi
- QoS
- Traffic Control

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 117 for more information.

Procedure 127 Configure the IPv4 Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **TCP/IP** from the **Network** menu.
3	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'.
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. e Enter the **Secondary DNS Server** in the Secondary DNS Server text box xxx.xxx.xxx.xxx.
5	Select **Apply** to save the settings.

- End -

IPv6

Enable IPv6 on the camera.

Procedure 128 Enable/Disable IPv6

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **TCP/IP** from the **Network** menu.
3	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 -

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 129 Configure Multicast Streaming

Step	Action
1	Select **Network** on the Web User Interface to display the Network menu options and click the **Multicast** tab.
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 Mutlicast 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
```

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 130 Configure FTP Server Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **FTP** from the **Network** menu.
3	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.
4	If required, select the **Secure FTP** checkbox. The default setting is 'Disabled'.
5	Enter the IP address of the FTP Server in the **FTP Server** text box.
6	Enter the FTP port in the **FTP Port** text box. The default setting is 21.
7	Enter the FTP username in the **Username** text box.
8	Enter the FTP password in the **Password** text box.
9	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 131 Configure the FTP Transfer Rate

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Event Settings** from the **Events and Actions** menu.
3	Select the **FTP** tab.
4	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'.
5	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 132 Test the FTP Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **FTP** from the **Network** menu.
3	Select the **FTP** tab.
4	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 133 Configure SMTP Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **SMPT** from the **Network** menu. The **SMPT** tab displays.
3	Check the **Enable SMPT** check box to enable SMPT. Text boxes on the tab become available for entry. **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.

10 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 134 Configure SNMP Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **SNMP** from the **Network** menu.
3	Enter a location reference in the **Location** text box.
4	Enter an SNMP managing contact reference in the **Contact** text box.
5	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 135 Enable/Disable Heartbeat

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **SNMP** from the **Network** menu.
3	Select the **Heartbeat** tab.
4	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 136 Enable select Heartbeat intervals

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **SNMP** from the **Network** menu.
3	Select the **Heartbeat** tab.
4	Select the **Enable Heartbeat** check box to enable Heartbeat.
5	Use the slider bar to select the **Heartbeat Interval (secs)**.
6	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 137 Configure CIFS Server Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **CIFS** from the **Network** menu.
3	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.

4 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>'

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

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

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

- 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 cameras hostname matches the configurable parameter “camera name” on the Web User Interface. Any DHCP request contains the cameras 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 138 Configure Dynamic DNS

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Dynamic DNS** from the **Network** menu.
3	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’.
4	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.

5 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 the SIP incoming audio is recorded in the RTSP stream.

Procedure 139 Enable/Disable SIP

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **SIP** from the **Network** menu.
3	Check the **Enabled** check box to enable SIP OR Clear the **Enabled** check box to disable SIP. The default setting is 'Disabled'.
4	Click **Apply** to save your settings. **Note:** After you enable SIP, the camera reboots automatically.

- End -

Procedure 140 Configure the SIP Server Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **SIP** from the **Network** menu.
3	Check the **Enabled** check box to enable SIP.
4	Enter the IP address of the SIP Server in the **Domain** text box.
5	Enter the SIP account username in the **Username** text box.
6	Enter the SIP account password in the **Password** text box.

7 From the **Audio Source** dropdown menu, select the Audio Source for calls:

- **Mic** - only external microphones are currently supported.

8 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.

9 Click **Apply** to save your settings.

Note: After you enable SIP, the camera reboots automatically.

- End -

Procedure 141 Place a SIP call

Step	Action

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

2 Select **SIP** from the **Network** menu.

3 Enter the SIP Extension number in the **Extension** text box.

4 Click **Dial** to activate the call.

5 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: Illustra Tools App available on Android and IOS App stores.

Procedure 142 Enable wireless configuration of the camera

Step	Action

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

2 Select **Wi-Fi** from the **Network** menu.

3 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 143 Configuring quality of service settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Network**.
2	Select **QoS** from the **Network** menu.
3	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**

4 Select the **Metadata** drop-down menu and select one of the options.

5 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 144 Enabling traffic control

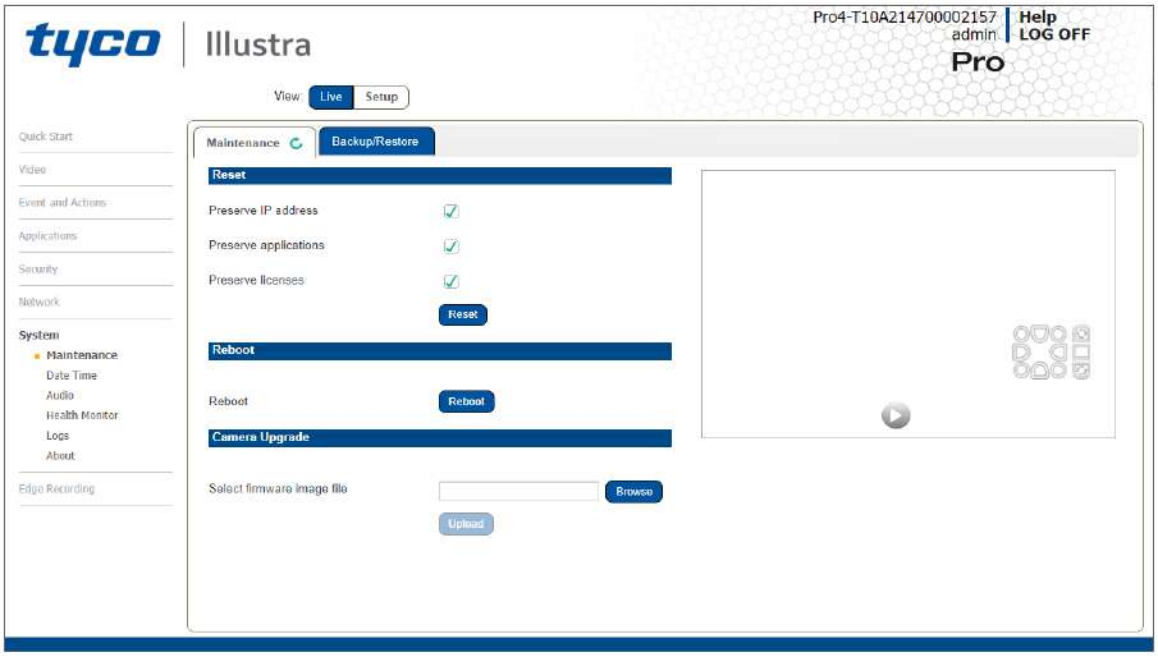
Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus and then select **Network**.
2	Select **Traffic Control** from the **Network** menu.
3	Check the **Enable Traffic Control** check box to enable traffic control configuration.
4	Select the **Max Peak Rate (mBit/s)** text box and enter a value.
5	**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 -

System

When you open the **System** menu, the **Maintenance** page appears, as seen in Figure 43 on page 129.

Figure 43 System Menu



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

- Maintenance
- Date Time
- Audio
- 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, presets, patterns and sequences can be retained if required.

Procedure 145 Resetting the Camera

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
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 146 Reboot the Camera

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

Camera Firmware Upgrade

The camera can be upgraded using firmware provided by Illustra. Alternatively, the camera can also be upgraded using Illustra Connect. Refer to the Illustra Connect User Guide for further information.

Note: All existing camera settings are maintained when the firmware is upgraded.

Caution

You should only use firmware that has been provided by Illustra. Using any other firmware may cause a malfunction and damage the camera.

Procedure 147 Upgrade Camera Firmware

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Maintenance** from the **System** menu.
3	Select **Browse**. The Choose file to Upload dialog displays.
4	Navigate to the location where the firmware file has been saved.
5	Select the firmware file then select the **Open** button.
6	Select **Upload**. The file transfer will begin. 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 -

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 148 Backup Camera Data

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
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 149 Restore Camera from Backup

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

Date / Time

Set the date and time on the camera.

Note:

Date and Time can also be configured in the **Quick Start** menu.

Procedure 150 Configuring the Date and Time

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

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 -

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 indoor cameras internal microphone is identified by number 4 in Figure 18.

Procedure 151 Configure Audio Input

Step	Action

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

2 Select **Audio** from the **System** menu. The Audio Input tab displays.

3 Select the **Input Source** drop-down and select one of the following options:

- **Internal**
- **External**

Note: The Outdoor camera does not include the 'Internal' option as no built in microphone is present in the unit.

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 152 Configuring Audio Output

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Audio** from the Camera Configuration 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 153 Play Stored Audio

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Audio** from the **System** menu.
3	Select the **Audio Clips** tab.
4	Select to play back the corresponding audio file.

- End -

Procedure 154 Upload an Audio File

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **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 155 Delete a Stored Audio file

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **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 -

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 156 Configure Health Monitor Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
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 157 Display System Log

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **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 158 System Log Filter

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **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 159 Display Boot Log

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **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 160 Boot Log Filter

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **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 161 Display Model Information

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **About** from the **System** menu. The model tab displays.

- End -

Procedure 162 Edit Camera Name

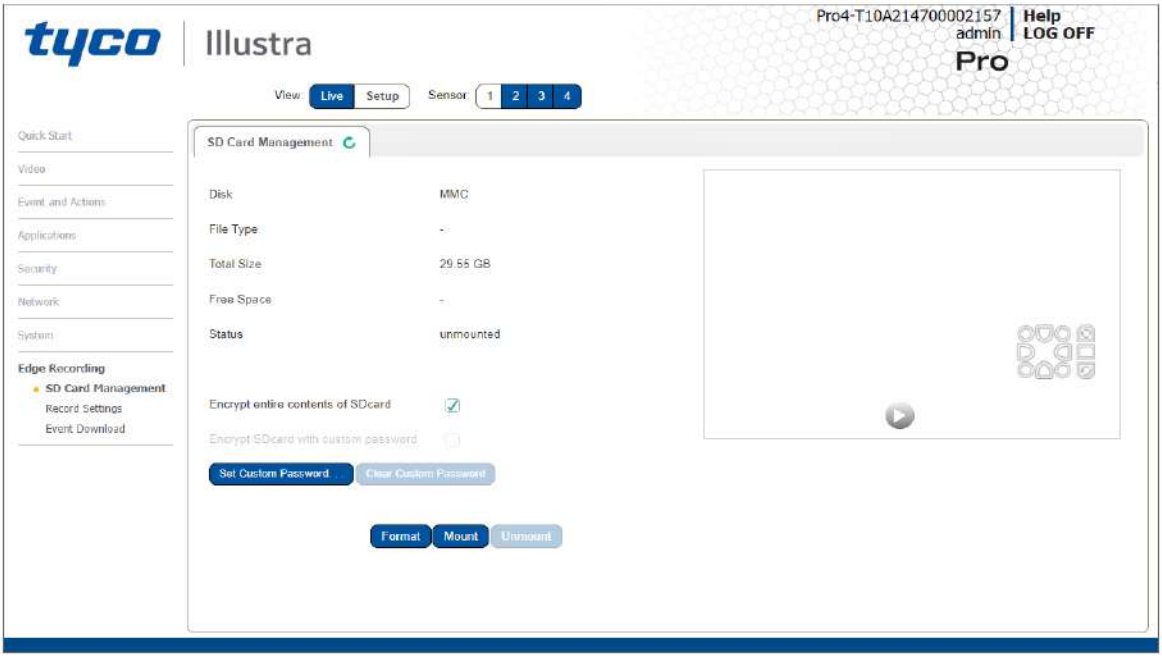
Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **About** from the **System** menu. The model tab displays.
3	Edit the name in the **Camera Name** textbox.

- End -

Edge Recording

When you select the **Edge Recording** menu, the **Micro SD Card Management** page appears, as seen in Figure 44 on page 139.

Figure 44 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 163 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 164 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.
3	Select **SD Card Management** menu 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 165 Remove the Micro SD Card by powering down the Camera

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 166 Unmount the Micro SD Card for Removal

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **SD Card Management** menu 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 167 Encrypting the contents on the SD card

Step	Action
1	Insert the SD card into camera.
2	Log in to the camera Web GUI and select **Setup** on the Web User Interface banner to display the setup menus.
3	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.
4	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.

5 Log in to the camera Web GUI and select **SD Card Management** from the **Edge Recording** menu.

6 Select 'Encrypt SD card with custom password'.

7 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 168 Resetting a camera

Step	Action

Note: The SD card encryption is always enabled by default after a camera reset

1 Log in to camera Web GUI and select **Setup** on the Web User Interface banner to display the setup menus.

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 169 Configure Record Settings

Step	Action
1	Select **Setup** on the Web User Interface Banner to display the setup menus.
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 6.0 Trickle Stor.

Procedure 170 Configure Offline Recording Settings

Step	Action
1	Select **Setup** on the Web User Interface Banner to display the setup menus.
2	Select **Record Settings** from the **Edge Recording** menu.
3	Select the **Offline Record Settings** tab.
4	In the **Video Edge IP Address** field, enter the IP address of the Video Edge 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 171 Viewing RTSP Stream through Media Player

You can use Media Player to view live video and audio in real time from the camera.

Step	Action
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: **Sensor 1:** • Video Stream: rtsp://<cameraip>:554/videoStreamId=<1-4> **Sensor 2:** • Video Stream: rtsp://<cameraip>:555/videoStreamId=<5-8> **Sensor 3:** • Video Stream: rtsp://<cameraip>:556/videoStreamId=<9-12> **Sensor 4:** • Video Stream: rtsp://<cameraip>:557/videoStreamId=<13-16> For example: rtsp://192.168.1.168:554/videoStreamId=1 OR **Audio** As audio is associated to Host Camera (sensor3) RTSP request will be formatted as follows **Audio only** • rtsp://<cameraip>:556/audioStreamId=1 **Video And audio** • rtsp://<cameraip>:556/videoStreamId=9&audioStreamId=1 **Note:**Audio is not available for individual sensors
3	Select **Play**.The live video stream displays.

- End -

Appendix B: Stream Tables

Pro4 - 20MP and 32MP Camera Streaming Combinations

Table 45 20MP 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 2560x1440 *1	4:3 16:9	30 30	30 30	15 15
	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	1280x720 1024x576 800x464 816x464 640x360 480x272	(720p) 16:9 (PAL+) 16:9 (SVGA) 4:3 16:9 (nHD) 16:9 16:9	30 30 30 30 30 30	30 30 30 30 30 30	15 15 15 15 15 15
Stream 3	H.264, H.265, H.264+, H.265+, MJPEG	640x360 480x360 480x272	16:9 4:3 16:9	30 30 30	30 30 30	15 15 15
Stream 4	MJPEG	640x368 *2	16:9	7	7	7

Note:*1 The default resolution of stream 1 will be 2560x1440

Note:*2 Stream 4 is used for analytics, supporting a second resolution (480x360) would require additional work in the analytics code.

Note:A maximum of 5 concurrent streams are supported by each camera, this includes shared streams.

Table 46 20MP 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+,	2560x1920 2560x1440 *1	4:3 16:9	30 30	30 30	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	30 30 30	15 15 15
Stream 2	H.264, H.265, H.264+, H.265+, MJPEG	1280x720 1024x576 800x464 816x464 640x360 480x272	(720p) 16:9 (PAL+) 16:9 (SVGA) 4:3 16:9 (nHD) 16:9 16:9	30 30 30 30 30 30	30 30 30 30 30 30	15 15 15 15 15 15
Stream 3	H.264, H.265, H.264+, H.265+, MJPEG	640x360 480x360 480x272	16:9 4:3 16:9	30 30 30	30 30 30	15 15 15
Stream 4	MJPEG	640x368 *2	16:9	7	7	7

Note:*1 The default resolution of stream 1 will be 2560x1440

Note:A maximum of 5 concurrent streams are supported by each camera, this includes shared streams.

Table 47 32MP 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	1920x1080 1664x936 1280x720	60 60 60	25 25 25	15 15 15
Stream 2	H.264, H.265, H.264+, H.265+, MJPEG	1280x720 1024x576 960x544 816x464 640x360 480x272	(720p) 16:9 (PAL+) 16:9 (qHD) 4:3 16:9 (nHD) 16:9 16:9	30 *1 30 *1 30 *1 30 *1 30 *1 30 *1	25 *1 25 *1 25 *1 25 *1 25 *1 25 *1	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 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.

Table 48 32MP 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	1920x1080 1664x936 1280x720	30 30 30	25 25 25	15 15 15
Stream 2	H.264, H.265, H.264+, H.265+, MJPEG	1280x720 1024x576 960x544 816x464 640x360 480x272	(720p) 16:9 (PAL+) 16:9 (qHD) 4:3 16:9 (nHD) 16:9 16:9	30 *1 30 *1 30 *1 30 *1 30 *1 30 *1	25 *1 25 *1 25 *1 25 *1 25 *1 25 *1	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 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.

Appendix C: Multisensor Cameras Technical Specifications

The table below lists the technical specifications of the PG4 20MP and 32MP Multisensor cameras.

General Features	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
Part number	IPR20-M12-OIA4	IPR32-M13-OIA4
Camera body color	White RAL 9003	White RAL 9003
Bubble color	N/A	N/A
Indoor / outdoor	Yes - both	Yes - both
Max. resolution	2560x1920	(3840 x 2160) 4K
Lens	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
Aperture Range	F/1.4(W) ~ F/2.8(T)	F/1.5(W) ~ F/2.8(T)
Focal length range	3.13mm ~ 9.77mm	4.16mm ~ 9.45mm
Focal means	Gear Focus	Gear Focus
Focal type	Gear	Gear
Focus type	Auto, Zoom trigger, Manual, One-Push AF	Auto, Zoom trigger, Manual, One-Push AF
Auto focus	One-Push AF	One-Push AF
Iris type	P Iris (Manual/Auto)	P Iris (Manual/Auto)
Day/night	True Day Night	True Day Night
Horizontal angle of view	100°~32°	104°~48°
Vertical angle of view	72°~24°	56°~27°
Illuminator	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
IR Distance	20m	20m
Smart IR	On,off	On,off
Adaptive IR	N/A	N/A
Video Imaging	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
AEC weighting method	Full / Upper / Lower / Center / Spot / Left / Right / ExposureBitMask	Full / Upper / Lower / Center / Spot / Left / Right / ExposureBitMask
Exposure compensation offset range	-2 to +2 f-stops	-2 to +2 f-stops

Exposure range	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|1/7.5|1/4	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|1/7.5|1/4|
Default maximum exposure	1/7.5 ~ 1/60sec.	1/7.5 ~ 1/60sec.
Default minimum exposure	1/120(100)~1/10000sec.	1/120(100)~1/10000sec.
White balance	Auto Normal / Manual / Auto Wide	Auto Normal / Manual / Auto Wide
Dynamic range method	Off/ Smart WDR/ True WDR2x /TrueWDR3x/	Off/ Smart WDR/ True WDR2x /TrueWDR3x/
Dynamic Range (Sensor Theoretical)	True multi shutter WDR up to 120dB	True multi shutter WDR up to 120dB
Noise Reduction	Digital Noise Reduction 2D and 3D	Digital Noise Reduction 2D and 3D
Defog	YES	YES
Flicker less	60(50) HZ	60(50) HZ
Corridor mode (rotate 90º)	Yes	Yes
Text overlay	Camera Name / Date Time / User Defined Test in one of 4 locations	Camera Name / Date Time / User Defined Test in one of 4 locations
Privacy zones	8 user definable rectangular zones	8 user definable rectangular zones
Min. scene illumination color	0.11 lux	0.2 lux
Min. scene illumination B/W	0.06 lux	0.11lux
Video Codecs	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
Configurable Streams	Quad Streaming	Quad Streaming
Frame rate range	1 to 30 ips (1-50 PAL)	1 to 30 ips (1-50 PAL)
Max resolution & rate	2MP @ 60ips, 4MP @ 30ips	2MP @ 60ips, 4K @ 30ips
Resolutions available	See the Stream Tables section for more information.	See the Stream Tables section for more information.
Stream sharing	A maximum of 12 concurrent shared streams	A maximum of 12 concurrent shared streams
Audio	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
Audio Features	Streaming Output, Streaming Input, Stored Audio Clips with Replay	Streaming Output, Streaming Input, Stored Audio Clips with Replay
Encoding method	G.711 9KHz/16 bits (A-Law/U-Law)	G.711 9KHz/16 bits (A-Law/U-Law)
Standard compliance	G711	G711
Sampling rate	9khz	9khz

Sampling bits	16bit	16bit
Frequency response range	100 to 3,600 Hz	100 to 3,600 Hz
Input type	SE/Line/MIC (TBC)	SE/Line/MIC (TBC)
Input impedance	20K/attenuation = 0 dB	20K/attenuation = 0 dB
Maximum input level	2V p-p	2V p-p
Input connector	Terminal Block	Terminal Block
Output type impedance	Hi impedance	Hi impedance
Maximum output	2V p-p	2V p-p
Output connector	Terminal Block	Terminal Block
Client Interfaces	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
Browsers supported & version	Mozilla Firefox, Chrome,Safari, Microsoft Edge	Mozilla Firefox, Chrome,Safari, Microsoft Edge
Special Features	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
Motion detection	Yes	Yes
Higher compression quality ROI	No	No
Blur and Tamper detection	Yes	Yes
AI Object classification	Yes	Yes
TWDR (multi exposure)	Yes	Yes
Local storage	Micro SD & SDXC slot up to 512GB; Class 10 or higher; Card not included.	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	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	Enhanced Security Feature Provides: One-Click Security Hardening, User Access Log, Validates Complex Credentials, Disables Unused Protocols
IntelliZip®	Advanced H.264 & H.265 modes	Advanced H.264 & H.265 modes
VideoEdge® TrickleStor	VideoEdge® TrickleStor technology for edge-based failover redundancy	VideoEdge® TrickleStor technology for edge-based failover redundancy
Event Alarms	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
Event triggers	Motion Detection, Blur Detection, AI Object classification, Alarm Input, Network Loss, Temperature	Motion Detection, Blur Detection, AI Object classification, Alarm Input, Network Loss, Temperature

Pre-alarm recording	10 sec.	10 sec.
Event actions	"Record to SD card Snapshot SMTP e-mail file transfer FTP file transfer CIFS Auxiliary output Audio clip play-back"	"Record to SD card Snapshot SMTP e-mail file transfer FTP file transfer CIFS Auxiliary output Audio clip play-back"
Alarm input	Two; Max 6V (High)/0.6V(LOW)	Two; Max 6V (High)/0.6V(LOW)
Auxiliary output	Two 30V (Peak AC)/1A,NC/NO; PotoMOS Relay	Two 30V (Peak AC)/1A,NC/NO; PotoMOS Relay
I/O Interfaces	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
SD card	Micro SD/SDHC/SDXC slot up to 512GB; Class 10 or higher; Card not included.	Micro SD/SDHC/SDXC slot up to 512GB; Class 10 or higher; Card not included.
Alarm inputs	2	2
Auxiliary outputs	2	2
IP Connector	RJ-45	RJ-45
LED indicators	Green Led indicates connected Yellow LED indicates active com-munication	Green Led indicates connected Yellow LED indicates active com-munication
Reset buttons	Recessed reset pushbutton for reboot & factory reset	Recessed reset pushbutton for reboot & factory reset
I/O Connector	Inside enclosure: - RJ-45 IP con-nector - 2 pin Euro-style terminal block power connector 24VAC - 12 pin audio and I/O connector (requires IO Accessory cable) - Micro SD SDXC card slot - Recessed reset pushbutton for reboot & factory reset -MicroUSB to support Illustra WiFi Accessory	Inside enclosure: - RJ-45 IP con-nector - 2 pin Euro-style terminal block power connector 24VAC - 12 pin audio and I/O connector (requires IO Accessory cable) - Micro SD SDXC card slot - Recessed reset pushbutton for reboot & factory reset -MicroUSB to support Illustra WiFi Accessory
Power Supply (PoE)	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
Type	IEEE 802.3bt	IEEE 802.3bt
Type	Class 8	Class 8
Current draw amps	0.96A	0.96A
Wattage	71.3W	71.3W
Power Supply (24VAC)	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
Voltage range	24Vac	24Vac
Current draw amps	3.54A	3.54A
Wattage	81W	81W

Environmental	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
Operating temp. range	-40°C ~ 55°C (-40ºF to 131ºF)	-40°C ~ 55°C (-40ºF to 131ºF)
Start up temp. range	-40°C(-40°F)	-40°C(-40°F)
Extended Temperature:	Yes	Yes
Operating humidity range	Up to 90% non-condensing	Up to 90% non-condensing
Storage temp. range	-40°C ~ +60°C	-40°C ~ +60°C
Water/dust intrusion	IP66/IK10	IP66/IK10
Mechanical	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
Dimensions	-40°C ~ 55°C (-40ºF to 131ºF)	-40°C ~ 55°C (-40ºF to 131ºF)
Weight	5.7 Kg	5.7 Kg
Shipping weight	6.7 Kg	6.7 Kg
Pan rotation angle	360°	360°
Tilt angle	0°~90°	0°~90°
Vandal rating	IK10	IK10
Regulatory	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
Safety	UL60950-1; CAN/CSA-C22.2 No. 60950-1, BIS IS13252 Part 1:2010	UL60950-1; CAN/CSA-C22.2 No. 60950-1, BIS IS13252 Part 1:2010
Emissions	FCC Part 15 Class A; EN55032 Class A; ICES-003/NMB-003 Class A	FCC Part 15 Class A; EN55032 Class A; ICES-003/NMB-003 Class A
Immunity	EN50130-4	EN50130-4
Environmental	RoHS; WEEE, REACH	RoHS; WEEE, REACH

The table below lists the technical specifications of the PG4 20MP and 32MP Multisensor cameras.

General Features	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
Part number	IPS20-M12-OTA4 / IPS20-M12-OIA4	IPS32-M13-OTA4 / IPS32-M13-OIA4
Camera body color	White RAL 9003	White RAL 9003
Bubble color	N/A	N/A
Indoor / outdoor	Yes - both	Yes - both
Max. resolution	2560x1920	(3840 x 2160) 4K
Lens	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
Aperture Range	F/1.4(W) ~ F/2.8(T)	F/1.5(W) ~ F/2.8(T)
Focal length range	3.13mm ~ 9.77mm	4.16mm ~ 9.45mm
Focal means	Gear Focus	Gear Focus
Focal type	Gear	Gear
Focus type	Auto, Zoom trigger, Manual, One-Push AF	Auto, Zoom trigger, Manual, One-Push AF
Auto focus	One-Push AF	One-Push AF
Iris type	P Iris (Manual/Auto)	P Iris (Manual/Auto)
Day/night	True Day Night	True Day Night
Horizontal angle of view	100°~32°	104°~48°
Vertical angle of view	72°~24°	56°~27°
Illuminator	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
IR Distance	IPS20-M12-OTA4 = N/A IPS20-M12-OIA4 = 20m	IPS32-M13-OTA4 = N/A IPS32-M13-OIA4 = 20m
Smart IR	On,off	On,off
Adaptive IR	N/A	N/A
Video Imaging	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
AEC weighting method	Full / Upper / Lower / Center / Spot / Left / Right / ExposureBitMask	Full / Upper / Lower / Center / Spot / Left / Right / ExposureBitMask
Exposure compensation offset range	-2 to +2 f-stops	-2 to +2 f-stops
Exposure range	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|1/7.5|1/4	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|1/7.5|1/4|

Default maximum exposure	1/7.5 ~ 1/60sec.	1/7.5 ~ 1/60sec.
Default minimum exposure	1/120(100)~1/10000sec.	1/120(100)~1/10000sec.
White balance	Auto Normal / Manual / Auto Wide	Auto Normal / Manual / Auto Wide
Dynamic range method	Off/ Smart WDR/ True WDR2x /TrueWDR3x/	Off/ Smart WDR/ True WDR2x /TrueWDR3x/
Dynamic Range (Sensor Theoretical)	True multi shutter WDR up to 120dB	True multi shutter WDR up to 120dB
Noise Reduction	Digital Noise Reduction 2D and 3D	Digital Noise Reduction 2D and 3D
Defog	YES	YES
Flicker less	60(50) HZ	60(50) HZ
Corridor mode (rotate 90º)	Yes	Yes
Text overlay	Camera Name / Date Time / User Defined Test in one of 4 locations	Camera Name / Date Time / User Defined Test in one of 4 locations
Privacy zones	8 user definable rectangular zones	8 user definable rectangular zones
Min. scene illumination color	0.11 lux	0.2 lux
Min. scene illumination B/W	0.06 lux	0.11lux
Video Codecs	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
Configurable Streams	Quad Streaming	Quad Streaming
Frame rate range	1 to 30 ips (1-50 PAL)	1 to 30 ips (1-50 PAL)
Max resolution & rate	2MP @ 60ips, 4MP @ 30ips	2MP @ 60ips, 4K @ 30ips
Resolutions available	See the Stream Tables section for more information.	See the Stream Tables section for more information.
Stream sharing	A maximum of 12 concurrent shared streams	A maximum of 12 concurrent shared streams
Audio	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
Audio Features	Streaming Output, Streaming Input, Stored Audio Clips with Replay	Streaming Output, Streaming Input, Stored Audio Clips with Replay
Encoding method	G.711 9KHz/16 bits (A-Law/U-Law)	G.711 9KHz/16 bits (A-Law/U-Law)
Standard compliance	G711	G711
Sampling rate	9khz	9khz
Sampling bits	16bit	16bit
Frequency response range	100 to 3,600 Hz	100 to 3,600 Hz

Input type	Line input	Line input
Input impedance	20K/attenuation = 0 dB	20K/attenuation = 0 dB
Maximum input level	1.8V p-p	1.8V p-p
Input connector	Terminal Block	Terminal Block
Output type impedance	Hi impedance	Hi impedance
Maximum output	1.8V p-p	1.8V p-p
Output connector	Terminal Block	Terminal Block
Client Interfaces	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
Browsers supported & version	Mozilla Firefox, Chrome,Safari, Microsoft Edge	Mozilla Firefox, Chrome,Safari, Microsoft Edge
Special Features	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
Motion detection	Yes	Yes
Higher compression quality ROI	No	No
Blur and Tamper detection	Yes	Yes
AI Object classification	Yes	Yes
TWDR (multi exposure)	Yes	Yes
Local storage	Micro SD & SDXC slot up to 512GB; Class 10 or higher; Card not included.	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	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	Enhanced Security Feature Provides: One-Click Security Hardening, User Access Log, Validates Complex Credentials, Disables Unused Protocols
IntelliZip®	Advanced H.264 & H.265 modes	Advanced H.264 & H.265 modes
VideoEdge® TrickleStor	VideoEdge® TrickleStor technology for edge-based failover redundancy	VideoEdge® TrickleStor technology for edge-based failover redundancy
Event Alarms	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
Event triggers	Motion Detection, Blur Detection, AI Object classification, Alarm Input, Network Loss, Temperature	Motion Detection, Blur Detection, AI Object classification, Alarm Input, Network Loss, Temperature
Pre-alarm recording	10 sec.	10 sec.
Event actions	Record to SD card	Record to SD card

Alarm input	Two; Max 6V (High)/0.6V(LOW)	Two; Max 6V (High)/0.6V(LOW)
Auxiliary output	Two 30V (Peak AC)/1A,NC/NO; PotoMOS Relay	Two 30V (Peak AC)/1A,NC/NO; PotoMOS Relay
I/O Interfaces	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
SD card	Micro SD/SDHC/SDXC slot up to 512GB; Class 10 or higher; Card not included.	Micro SD/SDHC/SDXC slot up to 512GB; Class 10 or higher; Card not included.
Alarm inputs	2	2
Auxiliary outputs	2	2
IP Connector	RJ-45	RJ-45
LED indicators	Green Led indicates connected Yellow LED indicates active communication	Green Led indicates connected Yellow LED indicates active communication
Reset buttons	Recessed reset pushbutton for reboot & factory reset	Recessed reset pushbutton for reboot & factory reset
I/O Connector	Inside enclosure: - RJ-45 IP connector - 2 pin Euro-style terminal block power connector 24VAC - 12 pin audio and I/O connector (requires IO Accessory cable) - Micro SD SDXC card slot - Recessed reset pushbutton for reboot & factory reset -MicroUSB to support Illustra WiFi Accessory	Inside enclosure: - RJ-45 IP connector - 2 pin Euro-style terminal block power connector 24VAC - 12 pin audio and I/O connector (requires IO Accessory cable) - Micro SD SDXC card slot - Recessed reset pushbutton for reboot & factory reset -MicroUSB to support Illustra WiFi Accessory
Power Supply (PoE)	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
Type	IEEE 802.3bt	IEEE 802.3bt
Type	Class 8	Class 8
Current draw amps	IPS20-M12-OTA4 = 1.2A IPS20-M12-OIA4 = 1.3A	IPS32-M13-OTA4 = 1.2A IPS32-M13-OIA4 = 1.3A
Wattage	IPS20-M12-OTA4 = 66W IPS20-M12-OIA4 = 71.3W	IPS32-M13-OTA4 = 66W IPS32-M13-OIA4 = 71.3W
Power Supply (24VAC)	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
Voltage range	24Vac	24Vac
Current draw amps	IPS20-M12-OTA4 = 2.9A IPS20-M12-OIA4 = 3.7A	IPS32-M13-OTA4 = 2.9W IPS32-M13-OIA4 = 3.7A
Wattage	IPS20-M12-OTA4 = 66W IPS20-M12-OIA4 = 81W	IPS32-M13-OTA4 = 66W IPS32-M13-OIA4 = 81W

Environmental	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
Operating temp. range	-40°C ~ 55°C (-40ºF to 131ºF)	-40°C ~ 55°C (-40ºF to 131ºF)
Start up temp. range	-40°C(-40°F)	-40°C(-40°F)
Extended Temperature:	Yes	Yes
Operating humidity range	Up to 90% non-condensing	Up to 90% non-condensing
Storage temp. range	-40°C ~ +60°C	-40°C ~ +60°C
Water/dust intrusion	IP66/IK10	IP66/IK10
Mechanical	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
Dimensions	-40°C ~ 55°C (-40ºF to 131ºF)	-40°C ~ 55°C (-40ºF to 131ºF)
Weight	5.7 Kg	5.7 Kg
Shipping weight	6.7 Kg	6.7 Kg
Pan rotation angle	360°	360°
Tilt angle	0°~90°	0°~90°
Vandal rating	IK10	IK10
Regulatory	**PG4 20MP Multisensor camera**	**PG4 32MP Multisensor camera**
Safety	UL60950-1; CAN/CSA-C22.2 No. 60950-1, BIS IS13252 Part 1:2010	UL60950-1; CAN/CSA-C22.2 No. 60950-1, BIS IS13252 Part 1:2010
Emissions	FCC Part 15 Class A; EN55032 Class A; ICES-003/NMB-003 Class A	FCC Part 15 Class A; EN55032 Class A; ICES-003/NMB-003 Class A
Immunity	EN50130-4	EN50130-4
Environmental	RoHS; WEEE, REACH	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".

© 2023 Johnson Controls. All rights reserved.

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