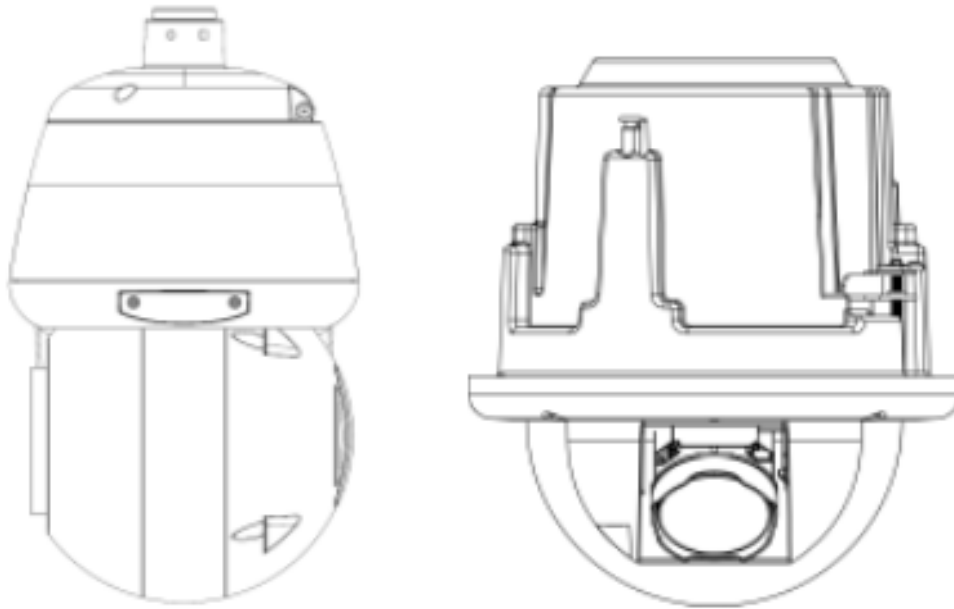


Illustra Pro Gen 4 2MP & 8MP Outdoor and Indoor PTZ Dome cameras Installation and Configuration Guide



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

© 2021 Johnson Controls. All rights reserved.

JOHNSON CONTROLS, TYCO and ILLUSTRATION 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 American Dynamics 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 should contact American Dynamics at (800) 507-6268 or (561) 912-6259 or on the Web at www.americandynamics.net.

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 PG4 Series 2MP and 8MP Outdoor PTZ Dome Cameras	8
Product overview	8
Installation	8
Illustra PG4 Series 2MP and 8MP Indoor PTZ Dome Cameras	17
Product overview	17
Installation	17
Network Topology	28
Network Connection	29
Default IP Address	29
DHCP	30
Managing cameras with the Illustra Connect tool	31
Configuration	33
Live menu	36
Quick Start Menu	41
Basic Configuration	41
Video Menu	58
Streams	58
Picture Settings	60
Date / Time / OSD	69
Privacy Zones	72
PTZ Settings Menu	74
PTZ Parameters	74
Shake and Dry	77
Intelligent Guard	77
Preset	78
Patterns	80
Scans	82
Sequences	84

Events and Actions Menu	87
Event Settings	87
Event Actions	91
Alarm I/O	93
Analytics	94
Video Intelligence	98
Periodic Events	108
Event Logs	108
Applications	111
Applications	111
License	112
Security	113
Security Status	113
Security Status	115
Users	116
HTTP/HTTPS	118
IEEE 802.1x	119
Firewall	121
Remote Access	123
Session Timeout	126
Generate CSR	126
Network Menu	128
TCP/IP	128
Multicast	130
FTP	130
SMTP	132
SNMP	133
Heartbeat	134
CIFS	134
Dynamic DNS	135
SIP	136
Wi-Fi	137

System	138
Maintenance	138
Date / Time	141
Audio	142
Analog Video	144
Health Monitor	144
PTZ Summary	145
Logs	145
About	147
Edge Recording	148
Micro SD Card Management	148
Encrypted SD card storage	150
Record Settings	152
Event Download	153
Appendix A: Using Media Player to View RTSP Streaming	154
Appendix B: Stream Tables	155
Appendix C: PTZ Dome Technical Specifications	157
End User License Agreement (EULA)	162

Warning

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

	CAUTION RISK OF ELECTRIC SHOCK DO NOT OPEN		THIS SYMBOL INDICATES THAT DANGEROUS VOLTAGE CONSTITUTING A RISK OF ELECTRIC SHOCK IS PRESENT WITHIN THE UNIT.
CAUTION: TO REDUCE THE RISK OF ELECTRIC SHOCK, DO NOT REMOVE THE COVER. NO USER-SERVICEABLE PARTS INSIDE. REFER SERVICING TO QUALIFIED SERVICE PERSONNEL.			THIS SYMBOL INDICATES THAT IMPORTANT OPERATING AND MAINTENANCE INSTRUCTIONS ACCOMPANY THIS UNIT.



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

Overview

This Illustra Pro Installation and Configuration Guide is a user manual which provides physical properties, installation, and configuration information of the cameras in Table 1 on Page 7.

Table 1 Product codes

Product Code	Model Name	Description
IPS02-P24-OI04	Illustra Pro Gen 4, 2MP PTZ Outdoor Dome	Gen 4, 2MP PTZ, 42x, outdoor, vandal, white, TDN w/IR, TWDR
IPS08-P25-OI04	Illustra Pro Gen 4, 8MP PTZ Outdoor Dome	Gen 4, 8MP PTZ, 22x, outdoor, vandal, white, TDN w/IR, TWDR
IPS02-P07-RT04	Illustra Pro Gen 4, 2MP PTZ Indoor Dome	Gen4 2MP PTZ, 30x, Indoor, Non-Vandal, Smoked, White, TDN, TWDR
IPS08-P25-RT04	Illustra Pro Gen 4, 8MP PTZ Indoor Dome	Gen4 8MP PTZ, 22x, Indoor, Non-Vandal, Smoked, White, TDN, TWDR

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

The second portion of this guide contains information regarding the Illustra User Web Interface and the web configuration of the aforementioned cameras. Refer to Configuration on page 33 for procedural information pertaining to camera configuration.

Illustra PG4 Series 2MP and 8MP Outdoor PTZ Dome Cameras

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

Product overview

This chapter explains the features and installation of the PG4 PTZ Dome cameras. Product code and description of the camera is provided in the table below.

Table 2 Product code and description of the PG4 PTZ cameras

Product Code	Description
IPS02-P24-OI04	Gen4 2MP PTZ, 30x, Outdoor, Non-Vandal, Smoked, White, TDN, TWDR
IPS08-P25-OI04	Gen4 8MP PTZ, 22x, Outdoor, Non-Vandal, Smoked, White, TDN, TWDR

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 Illustra IR PTZ Camera
- 1 x Printed Quick Start Guide
- 1 x Printed Regulatory Document
- 1 x NTSC/PAL output female BNC cable
- 1 x 2-pin European style terminal block
- 1 x Torx 20 security L-Key & 1 x Torx 10 security L-Key
- 1 x 12-pin terminal connector for I/O function
- 1 x Safety cable (Pre-attached to the camera)
- 1 x Mount adaptor
- 3 x ¼ 20 UNC security screws
- 1 x Rubber grommet
- 1 x RJ45 Insert tool

Contact your dealer if any item is missing.

Installation tools

The following tools assist with installation:

- 1 x Screw driver
- 1 x Torx 20 security L-Key
- 1 x Torx 10 security L-Key
- 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 90w or AC 24V

Note:As part of the start-up sequence the camera runs motor calibration, this includes a 15 second 'shake' procedure.

Figure 3 PG4 IR PTZ camera parts

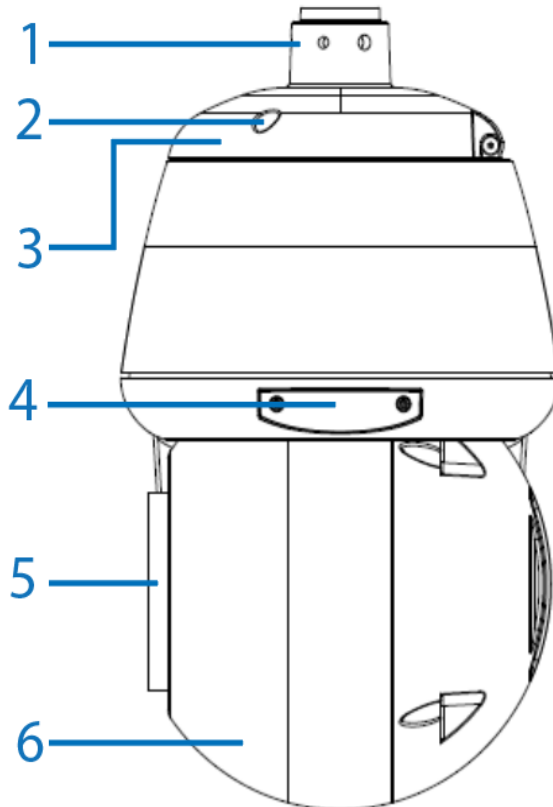


Table 4 Camera part descriptions

Number	Description
1	NPT Pendant Cap
2	Screw (x2) to open and lock the top cover
3	Top cover
4	SD Card Cover
5	Camera lens
6	Camera head

Procedure 1 Accessing the camera interior buttons / connections

Step	Action
1	Use the Torx security L-Key to remove the two screws on the camera top cover (1) (Figure 5).

Figure 5 Camera top cover



- End -

Table 6 Camera interior buttons / connections descriptions

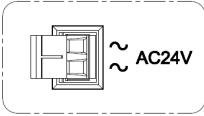
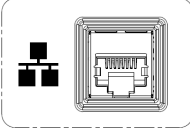
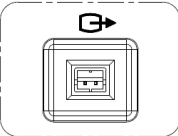
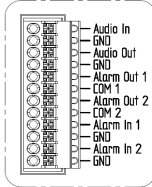



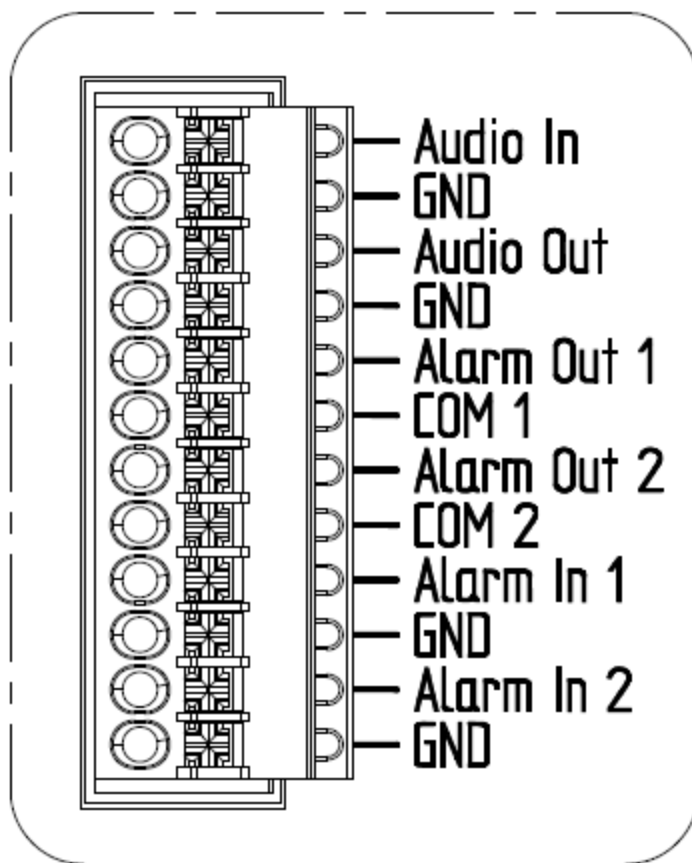
Buttons / Connectors	Description
	AC24V Power connector
	PoE Ethernet port
	Analog out port
	Audio and Alarm pins (See Figure 3 for descriptions)
	Reset to factory default (Hold for 5 seconds and then release)
	Power LED indicator
	Reboots the camera

Figure 7 Audio and alarm pin descriptions



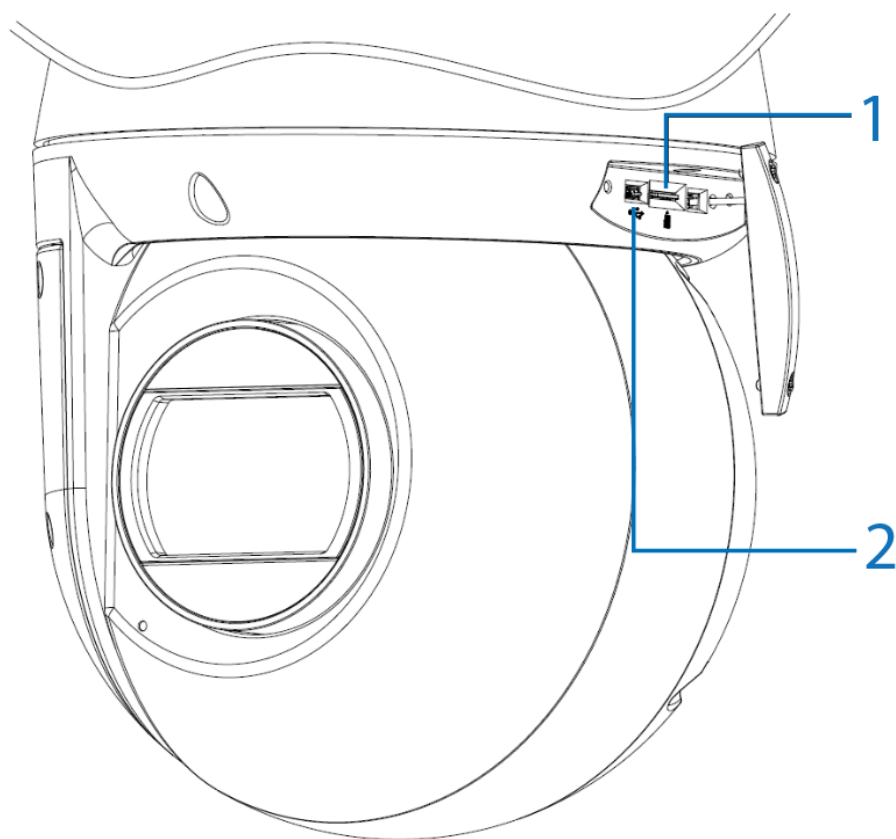
Procedure 2 Mounting the camera

Refer to the Illustra mounting accessories webpage <https://www.illustracameras.com/products/accessories/mounts> for assistance. The following mount accessory part numbers are applicable with the Illustra Pro Gen4 2MP and 8MP IR PTZ camera: RHOSW, RHOLW, RHOTR, ROTRF, RHOWCA, ROENDC.

Procedure 3 Inserting or removing the micro SD card

Step	Action
1	Remove the two screws located on the micro SD card cover (4) (Figure 8).

Figure 8 SD Card Cover



- 2 Carefully pull open the cover to access the SD card slot (1) (Figure 8) and insert (or remove) the micro SD card into (or from) the camera.

Note:It is advised that you reboot the camera after inserting the micro SD card.

- 3 Secure the two screws located on the micro SD card cover.

Note:The USB cable connection slot (2) (Figure 8) for Wi-Fi configuration is also located under the micro SD card cover.

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).

- End -

Procedure 4 Connecting the wires

Step	Action
------	--------

This unit supports one of the following options as power supply:

- 1 Connect a power source.
 - AC24V wired to connector and separate RJ45 Ethernet.

OR

- PoE through RJ45 connector. The Outdoor unit operates with IEEE 802.3at (30W).
- 2 Connect any optional audio or digital inputs or outputs.

Note:After connecting all cables ensure that the two screws on the top cover are securely attached to maintain the waterproof seal.

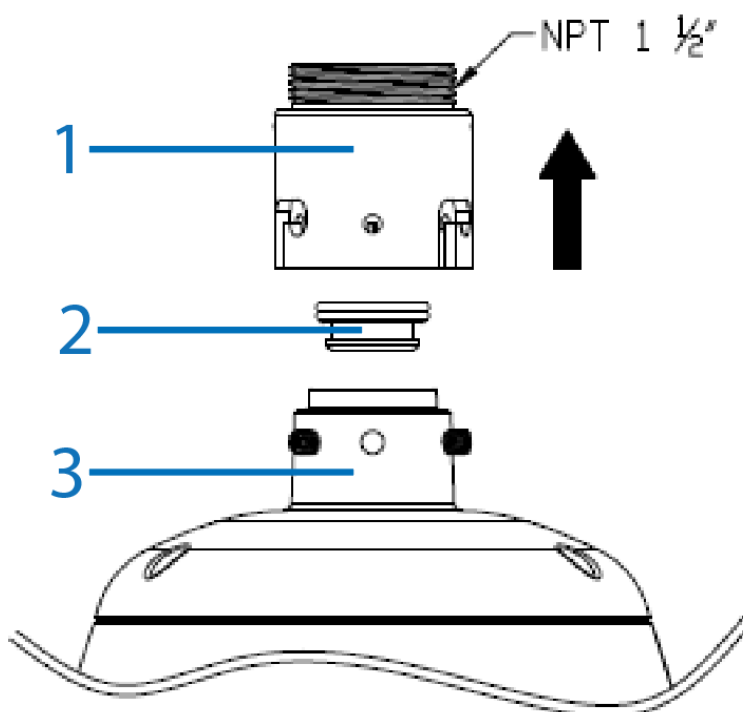
- End -

Procedure 5 Installing the rubber cable seal in to the NPT pendant cap

Step	Action
------	--------

- 1 Securely place the rubber cable seal (2) (Figure 9) into the pendant cap (3) (Figure 9).

Figure 9 NPT Pendant cap



- 2 Place the mount adaptor (1) (Figure 9) on to the NPT pendant cap (3) (Figure 9) and align the holes on the mount adaptor with the holes on the NPT pendant cap.
- 3 Insert the three security screws into the three holes and use the Torx security L-Key to securely attach the screws and the mount adaptor to the NPT cap.

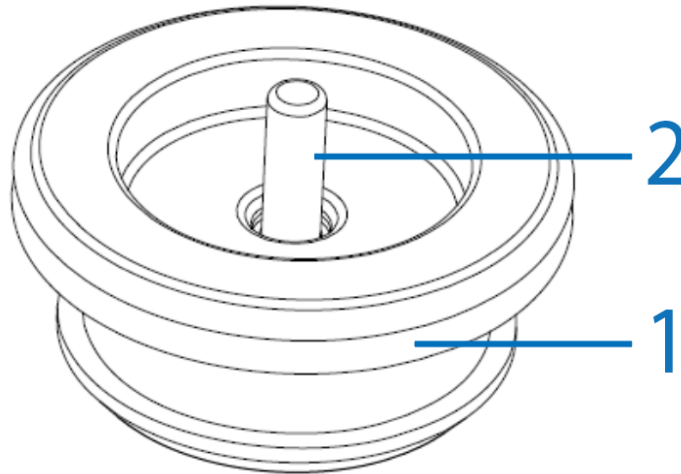
Note:To maintain the waterproof seal only pierce holes that are required for the installation.

- End -

Procedure 6 Passing the RJ45 connector through the grommet

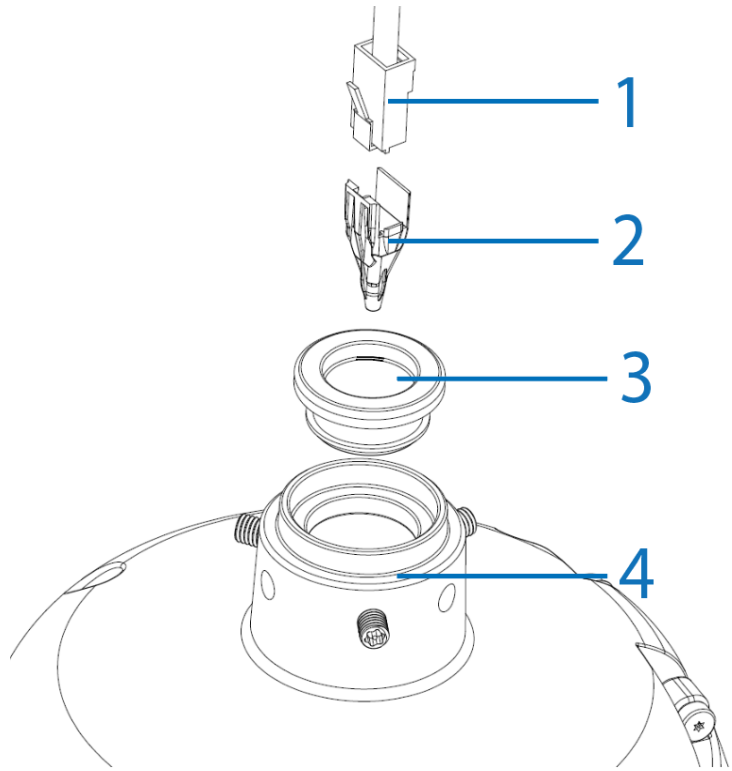
Step	Action
1	Remove the plug from the grommet (1) (Figure 10) by pulling the stub (2) (Figure 10) to create a hole in the grommet.

Figure 10 Grommet and stub



- 2 Insert the RJ45 cable connector (1) (Figure 11) into the insert tool (2) (Figure 11).
- 3 Push the insert tool and cable through the grommet hole (3) (Figure 11).
- 4 Remove the insert tool from the RJ45 connector and pass the cable through the NPT cap (4) (Figure 11).

Figure 11 Cable connector and insert tool



- End -

Illustra PG4 Series 2MP and 8MP Indoor PTZ Dome Cameras

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

Product overview

This chapter explains the features and installation of the PG4 PTZ Dome cameras. Product code and description of the camera is provided in the table below.

Table 12 Product code and description of the PG4 PTZ cameras

Product Code	Description
IPS02-P07-RT04	Gen4 2MP PTZ, 30x, Indoor, Non-Vandal, Smoked, White, TDN, TWDR
IPS08-P25-RT04	Gen4 8MP PTZ, 22x, Indoor, Non-Vandal, Smoked, White, TDN, TWDR

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 Indoor PTZ Camera
- 1 x Printed Quick Start Guide
- 1 x Mounting template sticker
- 1 x Printed Regulatory document
- 1 x BNC+ Connector cable (1000mm)
- 1 x Torx 20 Security L-Key
- 1 x 12-pin terminal connector
- 1 x Safety cable (Pre-attached to the camera)
- 1 x 2-pin terminal connector (2 pin tray 10x18x15mm L type)
- 1 x Waterproof connector (NPT 1/2)
- 2 x Stopper for Waterproof connector

Contact your dealer if any item is missing.

Installation tools

The following tools assist with installation:

- 1 x Screw driver

- 1 x Torx 20 security L-Key
- 1 x Drill
- 1 x Wire cutters

Quick Reference

- Default IP: 192.168.1.168 (DHCP enabled)
- Default Username / Password: admin / admin
- Power: 802.3at PoE+ Type 2 (30w) or AC 24V

Note:As part of the start-up sequence the camera runs motor calibration, this includes a 15 second 'shake' procedure.

Figure 13 PG4 IR PTZ camera parts

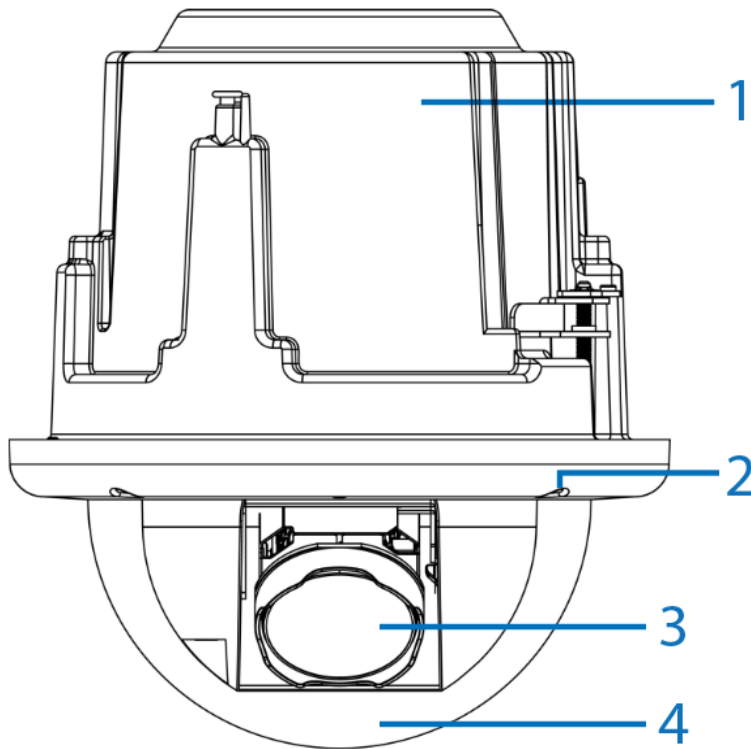


Table 14 Camera part descriptions

Number	Description
1	Recessed camera housing
2	Bubble assembly screws (x4)
3	Camera lens
4	Bubble assembly

Procedure 7 Removing the camera from the Recessed camera housing

Step	Action
------	--------

You can then access the cameras interior buttons and connections.

- 1 Place the Recessed camera housing on a flat surface so that the Bubble assembly (4) (Figure 13) is facing upward.

Note:The four Bubble assembly screws are now visible.

- 2 Use the Torx security L-Key to loosen the four screws (2) (Figure 13) on the camera Bubble assembly and remove the Bubble assembly.

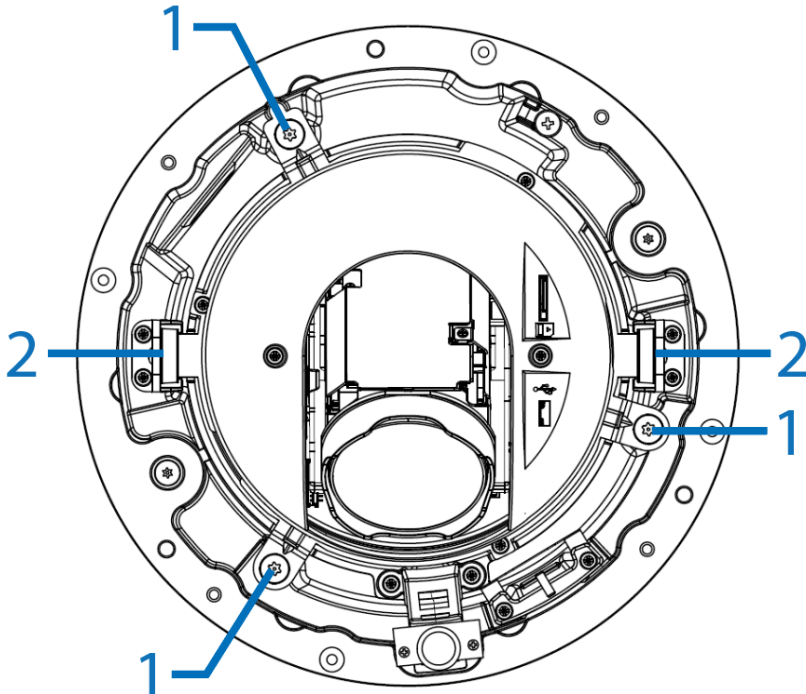
Note:As a safety precaution the Bubble assembly is attached to a safety wire. The camera lens (3) (Figure 13) is now visible.

- 3 Loosen the three captive fastener screws (1) (Figure 15) on the camera.

- 4 Gently push the two plastic clips (2) (Figure 15) located on the Recessed camera housing away from the camera and lift the camera away from Recessed camera housing.

Note:The camera interior buttons are located on the flat underside of the camera. See Table 16 for all symbols and descriptions.

Figure 15 Plastic clips and captive fastener screws



- End -

Table 16 Camera interior buttons / connections descriptions



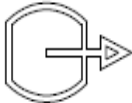
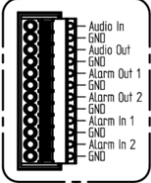



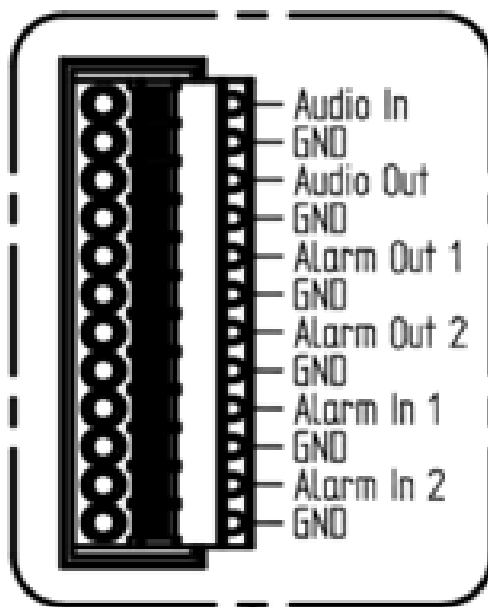
Buttons / Connectors	Description
	AC24V Power connector
	PoE Ethernet port
	Analog out port
	Audio and Alarm pins (See Figure 3 for descriptions)
	Reset to factory default (Hold for 5 seconds and then release)
	Power LED indicator
	Reboots the camera

Figure 17 Audio and alarm pin descriptions



Procedure 8 Mounting the camera

Refer to the Illustra mounting accessories webpage <https://www.illustracameras.com/products/accessories/mounts> for assistance. The following mount accessory part numbers are applicable with the Illustra Pro Gen4 Indoor 2MP and 8MP IR PTZ camera: RHOSW, RHOLW, RHOTR, ROTRF, RHOWCA, ROENDC and IAPN-P-IS12-0.

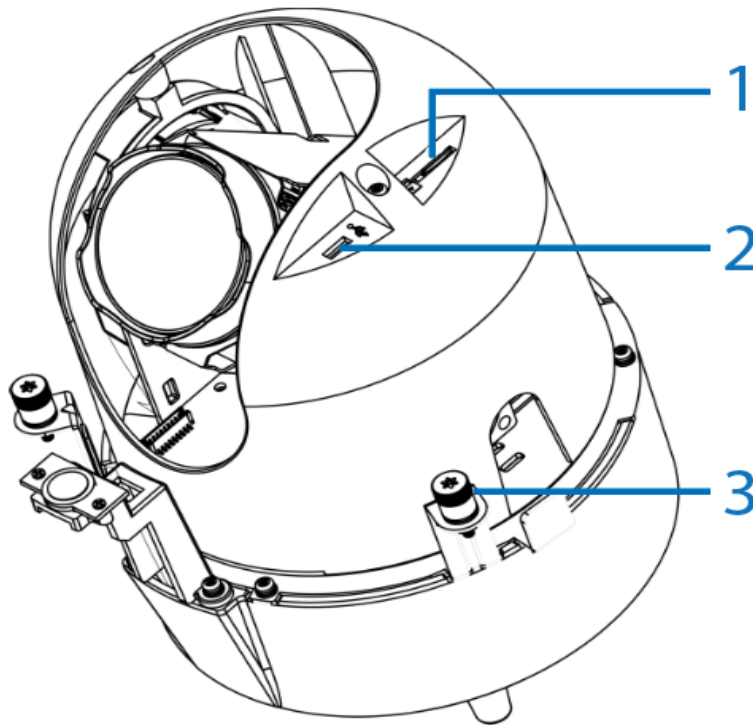
Procedure 9 Inserting or removing the micro SD card

Step	Action
------	--------

- Carefully insert (or remove) the micro SD card (1) (Figure 18) into (or from) the camera.

Note: It is advised that you reboot the camera after inserting the micro SD card.

Figure 18 SD Card slot



Note:The USB cable connection slot (2) (Figure 18) for Wi-Fi configuration is also located next to the micro SD card cover.

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).

- End -

Procedure 10 Connecting the wires

Step	Action
------	--------

This unit supports one of the following options as power supply:

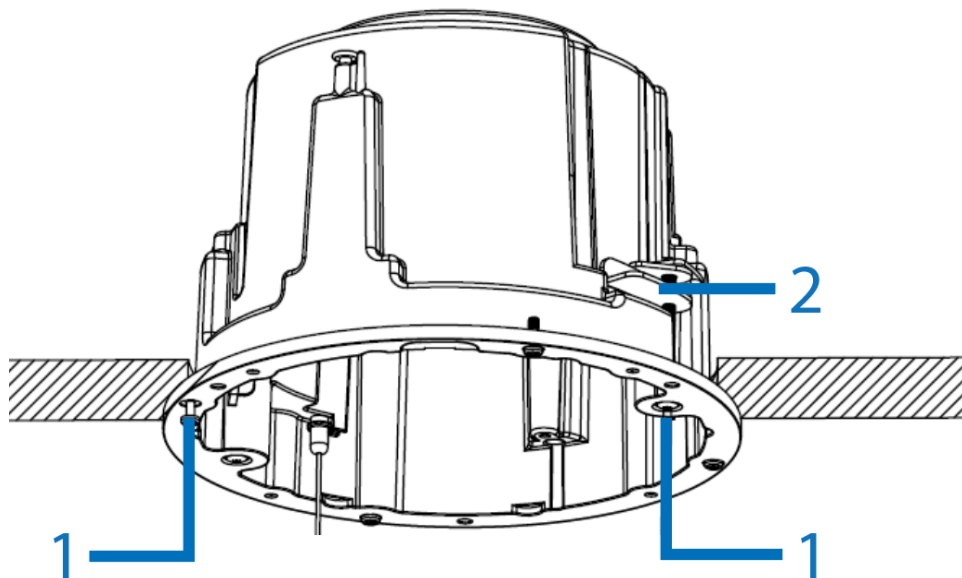
- 1 Connect a power source.
 - AC24V wired to connector and separate RJ45 Ethernet.
- OR
- PoE through RJ45 connector. The Outdoor unit operates with IEEE 802.3at (30W).
- 2 Connect any optional audio or digital inputs or outputs.

- End -

Procedure 11 Installing the camera into a ceiling

Step	Action
1	Remove the camera from the Recessed camera housing as per steps 1 to 4 in Removing the camera from the Recessed camera housing procedure.
2	Place the mounting template sticker onto the ceiling and cut out a cable hole as per the markings on the sticker.
3	Pull all power cables through hole on the ceiling.
4	Attach one end of a safety chain/cable (not supplied) to a secure structure within the roof and the other end to the 1/4-20 threaded hole on the top of the camera housing.
<p>Note:The safety chain/cable should be capable of supporting up to 7.3 kg (16 pounds).</p>	
5	Hold the Recessed camera housing up to the hole in the ceiling and pull all power cables through the hole in the camera housing.
6	Insert the Recessed camera housing into the hole in the ceiling and fasten the two screws (1) (Figure 19) with a screwdriver so that both locking springs paddles (2) (Figure 19) can slide out to secure the camera housing into the ceiling.
7	Hold the camera up to the camera housing and connect all power cables to the camera.
8	Ensure that the two metal 'clips' on the camera align with the two plastic 'tracks' in the camera housing.
9	Push the camera (1) (Figure 20) into the camera housing (2) (Figure 20) until it is temporarily secure in the camera housing.
10	Screw the three captive fasteners (3) (Figure 18) to fully secure the camera to the camera housing.

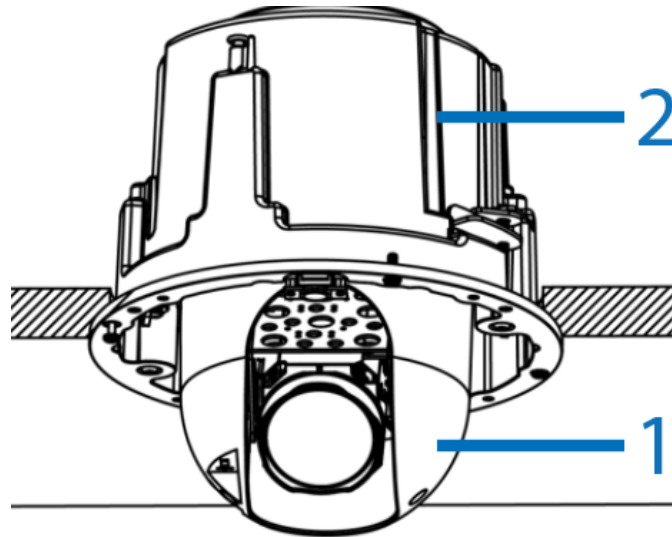
Figure 19 Ceiling screws and locking springs



- 11 Hold the Bubble assembly up to the camera housing and attach the Bubble safety lanyard on to the 'hook' located on the camera housing.

- 12 Align the four screws on the Bubble assembly with the four holes on the camera housing and attach the Bubble assembly to the camera housing.

Figure 20 Camera and camera housing



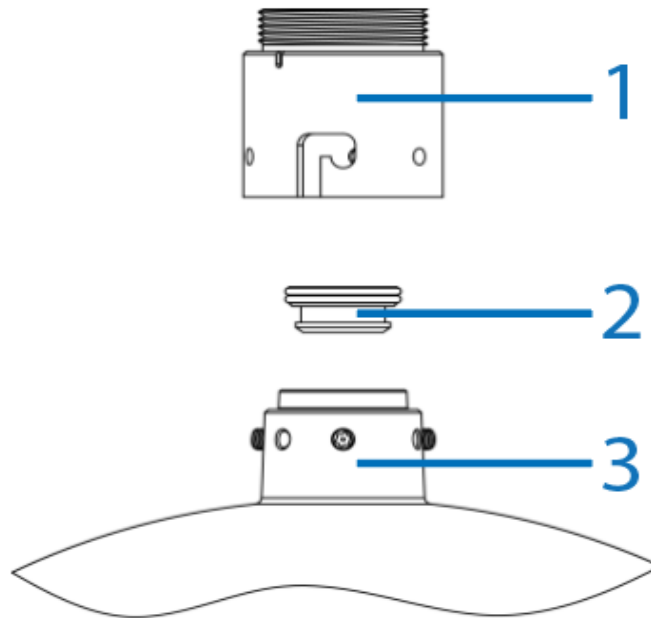
- End -

Procedure 12 Installing the camera into a pendant mount (sold separately)

Step	Action
1	Remove the camera from the Recessed camera housing as per steps 1 to 4 in Removing the camera from the Recessed camera housing procedure.
2	Once the pendant mount is installed then pull all power cables through the pendant mount arm.
3	Securely place the rubber cable seal (2) (Figure 21) into the pendant cap (3) (Figure 21).
4	Place the mount adaptor (1) (Figure 21) on to the NPT pendant cap (3) (Figure 21) and align the holes on the mount adaptor with the holes on the NPT pendant cap.
5	Insert the three security screws into the three holes and use the Torx security L-Key to securely attach the screws and the mount adaptor to the NPT cap.

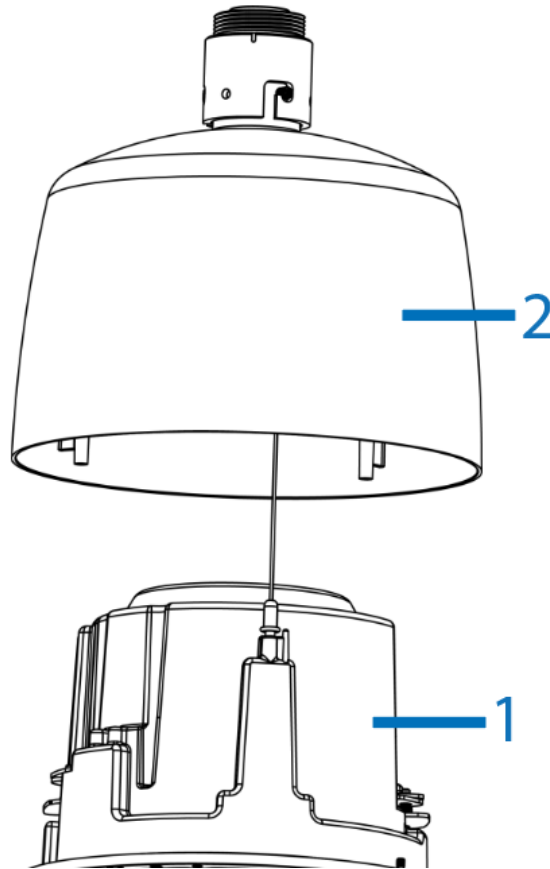
Note: To maintain the waterproof seal only pierce holes that are required for the installation.

Figure 21 NPT Pendant cap



- 6 Place the camera housing (1) (Figure 22) up into the pendant mount (2) (Figure 22) and pull the power cables through the hole in the camera housing.

Figure 22 Camera housing and pendant mount



- 7 Align the four holes on the camera housing with the four holes in the pendant mount and securely attach the camera housing to the pendant mount.
- 8 Push the camera into the camera housing until it is temporarily secure in the camera housing.
- 9 Screw the three captive fasteners (3) (Figure 18) to fully secure the camera to the camera housing.
- 10 Hold the Bubble assembly up to the camera housing and securely attach the Bubble assembly safety lanyard on to the 'hook' located on the camera housing.
- 11 Align the four screws on the Bubble assembly with the four holes on the camera housing and securely attach the Bubble assembly to the camera housing.

- End -

Network Topology

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

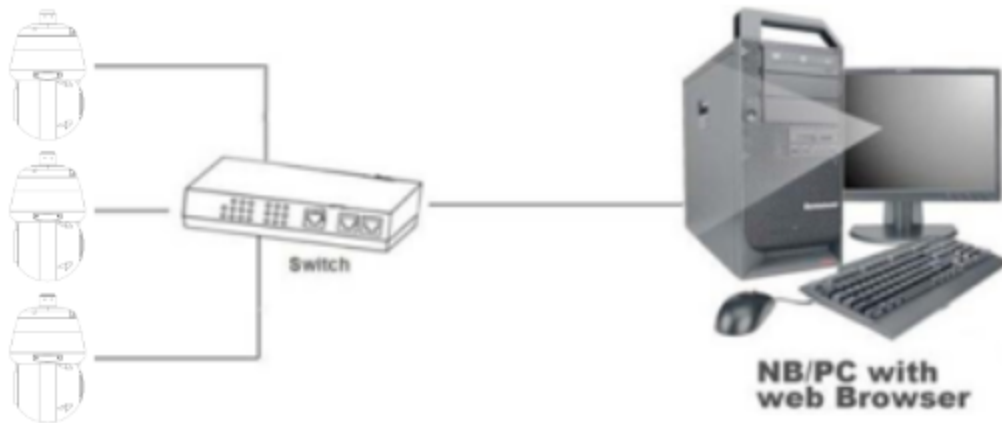
The following images illustrate the network topologies of the cameras.

Outdoor IR PTZ Dome Camera Topology

Figure 23 Dome Cameras Network Topology Type I.



Figure 24 Dome Cameras Network Topology Type II



Network Connection

Default IP Address

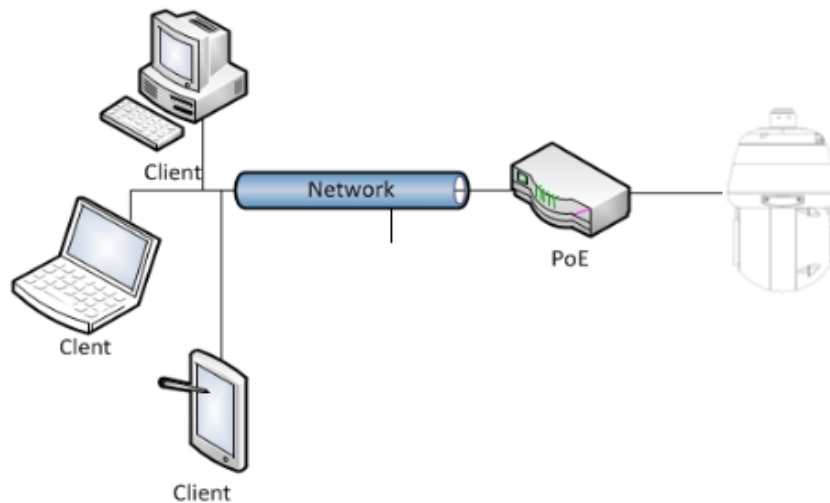
Since this is a network-based unit, an IP address must be assigned at the very first bootup. The default IP address of the unit is 192.168.1.168 and sub mask is 255.255.255.0.

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 25 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 13 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. <ol style="list-style-type: none"> 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 14 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 15 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 33 for further information regarding using the Illustra Connect tool for configuring the cameras.

Procedure 16 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 17 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 18 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 19 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: <ul style="list-style-type: none"> • Mirror • Flip
5	The video pane updates to display the new settings.

- End -

Configuration

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

Security Mode Profiles for First Time Connection

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

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

Refer to Summary of Security Modes on page 34 for further information regarding the differences between Standard and Enhanced Security modes.

Accessing the Illustra Pro Gen 4 Series Camera Web User Interface

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

Procedure 20 Logging in to the Camera

Step	Action
1	Refer to Network Connection on page 29 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 . <ul style="list-style-type: none">• Define a Host ID: The admin user must enter a 6 character code for the Host ID that includes both letters and/or numbers. This unique password can be used to access the operating system files. The HostID is not stored on the camera for security reasons and must be presented to Illustra Technical Support when remote access to the operating system is required.• Select a Security Type: Standard Security or Enhanced Security.

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

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

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

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

Note:The password must meet the following requirements:

Be a minimum of eight characters long.

Have at least one character from each of the following character groups:

- Upper-case letters - ABCDEFGHIJKLMNOPQRSTUVWXYZ
 - Lower-case letters - abcdefghijklmnopqrstuvwxyz
 - Numeric characters - 0123456789
 - Special characters - @ % + \ / ' ! # \$ ^ ? : , () { } [] ~ - _ `
-

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

- End -

Summary of Security Modes

Standard Security:

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

Enhanced Security:

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

- Authentication method is set to Digest by default.

Changing the Camera Web User Interface Language

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

Procedure 21 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: <ul style="list-style-type: none">• 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.

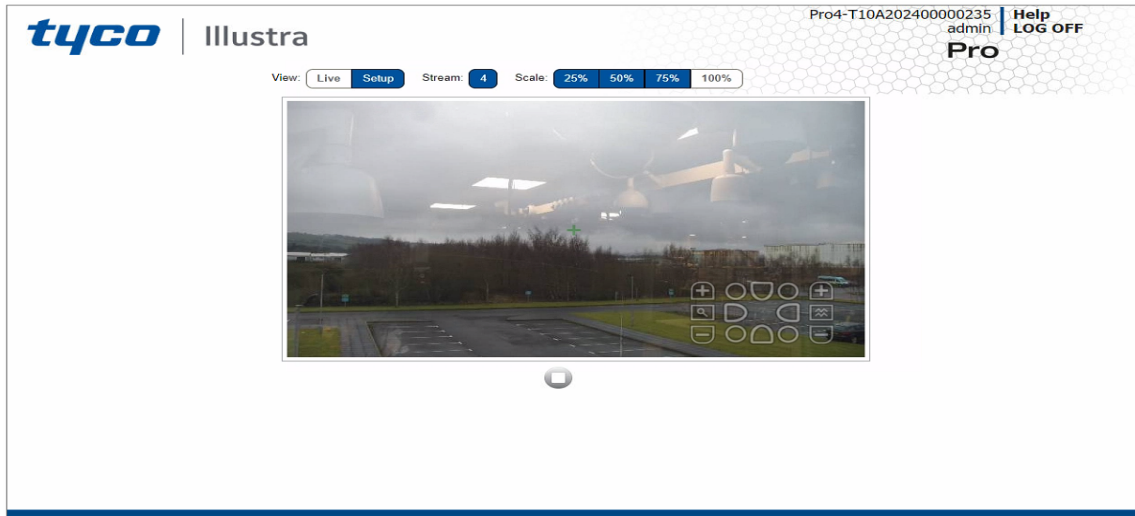
The camera web User Interface displays in the selected language.

- End -

Live menu

When you log in to the Illustra Web User Interface, the **Live** menu appears, as seen in Figure 26 on page 36.

Figure 26 Live menu page



Displaying the Live View Page

Display the live camera view page.

Procedure 22 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: <ul style="list-style-type: none">• 25%• 50%• 75%• 100% The default setting is 50%.

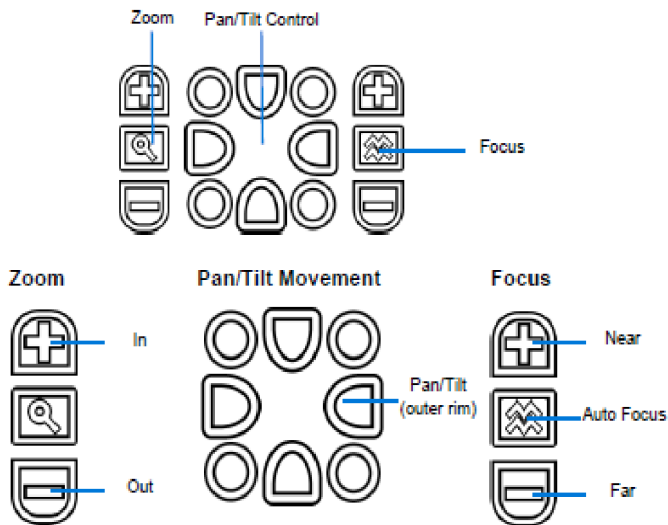
- End -

Controlling the PTZ camera using camera controls.

The PTZ 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 PTZ Camera with the keyboard shortcuts

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


	Pan Left		Pan Right
	Tilt Up		Tilt Down
	Zoom In		Zoom Out

Controlling the PTZ camera with the camera controls

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

Procedure 23 Controlling the PTZ 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 -

Controlling the Pan/Tilt Control through click and drag

You can use the mouse to control the camera, allowing slower camera movement and maximum accuracy.

Procedure 24 Controlling Pan/Tilt through click and drag using the Live video pane

Step	Action
------	--------

- | | |
|---|--|
| 1 | Select  to start the live web video.
The live video pane displays the current camera view. |
| 2 | Move the cursor to the pan and tilt quick control icon  in the center of the video pane control. |
| 3 | Click and drag the cursor to set the direction and speed of the camera. <ul style="list-style-type: none">• A red arrow is visible showing the direction of camera movement. |

- The camera's movement speed increases as the arrow is moved further from the cursor origin mark.


- End -

Zooming with the mouse scroll wheel

You can control the zoom function using a scroll wheel mouse.

Procedure 25 Zooming with the mouse scroll wheel using the Live Video Pane

Step	Action
------	--------

- | | |
|---|--|
| 1 | Select  to start the live web video.
The live video pane displays the current camera view. |
| 2 | Refer to Controlling the PTZ Camera with the Camera Controls or Controlling Pan/Tilt through click and drag using the Live video pane. |
| 3 | Scroll the mouse wheel upwards (zoom in) and downwards (zoom out). |


- End -

Double-click to center using the mouse

Click on the live video pane to automatically center the camera display.

Procedure 26 Activate double-click to center

Step	Action
------	--------

- | | |
|---|--|
| 1 | Select  to start the live web video.
The live video pane will display the current camera view. |
| 2 | Using the mouse, double-click on the area of interest in the live video pane.
The PTZ adjusts to display the area of interest in the center of the live video pane. |
| 3 | Repeat Step 2 to select a new area of interest. |


- End -

PTZ to a Selected Area Using the Mouse

Draw a rectangle on the live video pane to have the camera PTZ adjust to the selected area of interest.

Procedure 27 Activate PTZ to a selected area using the mouse

Step	Action
------	--------

- | | |
|---|--|
| 1 | Select  to start the live web video.
The live video pane displays the current camera view. |
| 2 | Click and drag on the live video pane to highlight the area to display. |

A red outline is visible identifying the selected area of interest.

3 Release the mouse button.

The PTZ adjusts to display the area of interest in the center of the live video pane.

4 Repeat Step 2 to select a new area of interest.

- 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 28 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.

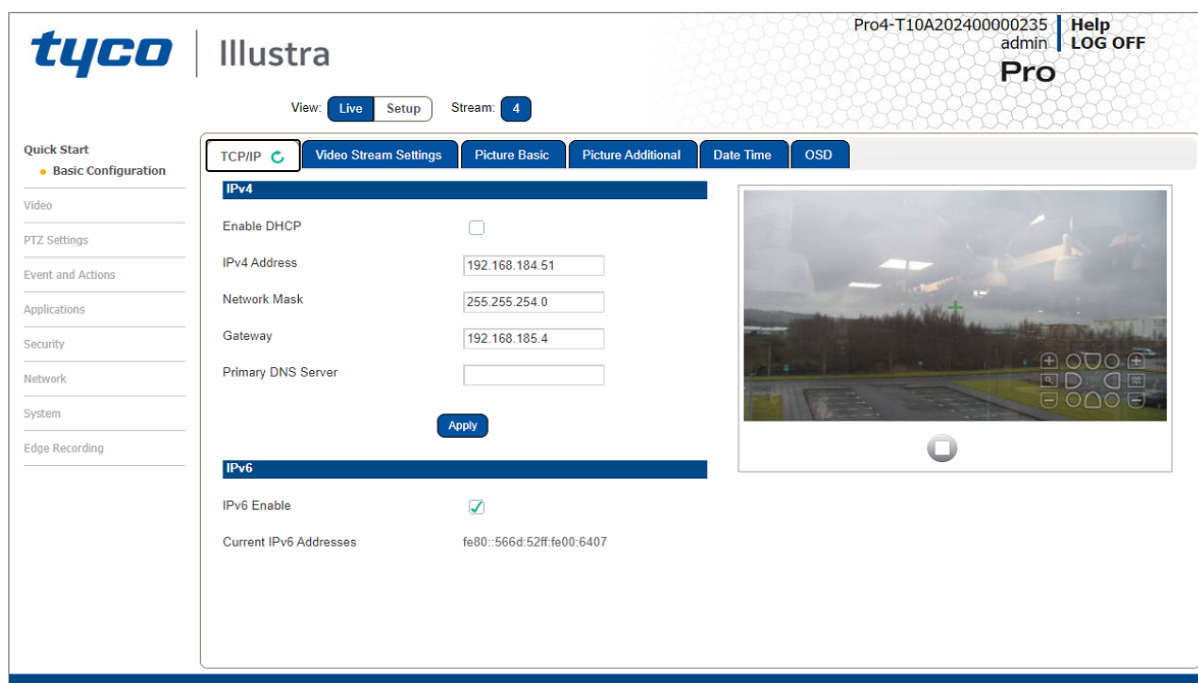
- End -

Quick Start Menu

When you select the Quick Start menu, the Basic Configuration Page displays, as shown in Figure 27 on page 41.

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 27 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 41 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 29 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 30 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: <ol style="list-style-type: none"> 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 31 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: <ol style="list-style-type: none">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'Enter the Network Mask in the Network Mask text box xxx.xxx.xxx.xxx. The default setting is '255.255.255.0'Enter the Gateway IP address in Gateway text box xxx.xxx.xxx.xxx.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 32 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 three video streams on the camera: Stream 1, Stream 2, and Stream 3.

Configuring the Web Video Stream

Adjust the settings for each video stream.

Procedure 33 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: <ul style="list-style-type: none"> • H264 • H264 IntelliZip • H265 • H265 IntelliZip • MJPEG <p>The default setting is 'H264'.</p>
<hr/> <p>Note:When you select H264 or H264 IntelliZip you can set the Profile. If you do not select either of these options then continue at step 6 below.</p> <hr/>	
5	Select the required Profile from the drop-down list: <ul style="list-style-type: none"> • Main • High <p>The default setting is 'Main'.</p>
6	Select the required Resolution from the drop-down menu. The resolutions available depend on the Image Source selected.
<hr/> <p>Note:See Stream Tables combinations in Appendix B.</p> <hr/>	
7	Use the slider bar to select the Frame Rate (fps) .
<hr/> <p>Note:FPS varies depending on other features - See Stream Tables combinations in Appendix B.</p> <hr/>	
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: <ul style="list-style-type: none"> • VBR (Variable Bit Rate) • CBR (Constant Bit Rate) • CVBR (Constrained Variable Bit Rate) <p>The default setting is 'CVBR'.</p>

- 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 34 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 35 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 value 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**

The default setting is center weighted.

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 -

Procedure 36 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 PTZ 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 37 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 38 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: <ul style="list-style-type: none">• 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 -

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 39 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 40 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: <ul style="list-style-type: none"> • 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. <p>The default setting is 'Auto Mid'.</p>
- End -	

Picture Adjustment

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

Procedure 41 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: <ul style="list-style-type: none"> • Contrast • Saturation • Sharpness <p>The values range from 1% to 100%. The video pane updates to display the new settings.</p>
- End -	

Procedure 42 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: <ul style="list-style-type: none">• 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 43 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: <ul style="list-style-type: none">• Auto Normal (or Auto if the PTZ camera is selected): 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' or 'Auto' when the PTZ camera is selected.

- End -

Procedure 44 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 -

Electronic Image Stabilization

All PTZ cameras now have the Electronic Image Stabilisation feature.

Procedure 45 Enable/Disable Electronic Image Stabilization

All PTZ cameras now have Electronic Image Stabilisation feature.

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 Electronic Image Stabilization check box to enable it.
OR
Clear the Electronic Image Stabilization check box to disable it. |
| 4 | The default setting is 'Enabled'. |

- 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 46 Changing the on screen camera text size

- 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 47 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 48 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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• Manually• via NTP The default setting is 'Manually'.
7	If you select Manually in step 5: <ol style="list-style-type: none">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: <ol style="list-style-type: none">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 49 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 50 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 51 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: <ul style="list-style-type: none"> • 0 - 24 characters • Cannot begin or end with: <ul style="list-style-type: none"> • . (dot)

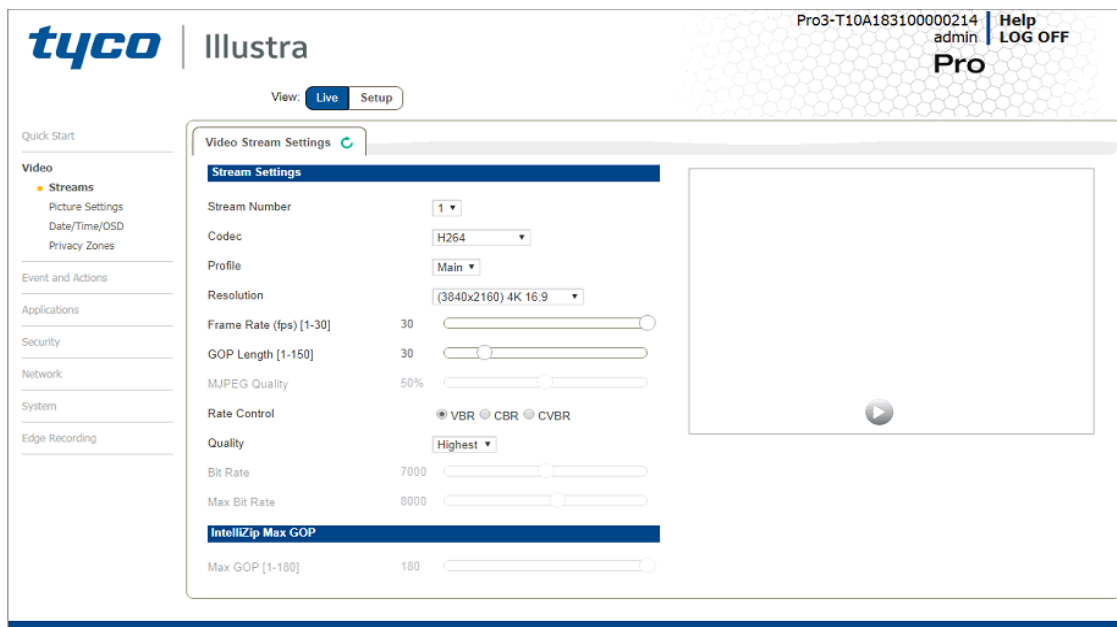
- - (hyphen)
- _ (underscore)
- \ (backslash)
- " (quotes)

- End -

Video Menu

When you select the **Video** menu, the **Streams** page displays, as seen in Figure 28 on page 58.

Figure 28 Video Menu



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

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

Streams

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

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

Note: The Web User Interface uses Stream 3.

Alarm Video

Edge Recording

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

Integration with other Illustra API Clients

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

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

Configuring the Video Stream

Adjust the settings for each video stream.

Procedure 52 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: <ul style="list-style-type: none"> • H264 • H264 IntelliZip • H265 • H265 IntelliZip • MJPEG <p>The default setting is 'H264'.</p>
<hr/> <p>Note:When you select H264 or H264 IntelliZip you can set the Profile. If you do not select either of these options then continue at step 6 below.</p> <hr/>	
5	Select the required Profile from the drop-down list: <ul style="list-style-type: none"> • Main • High <p>The default setting is 'Main'.</p>
6	Select the required Resolution from the drop-down menu. The resolutions available depend on the model selected:
<hr/> <p>Note:See Stream Tables combinations in Appendix B.</p> <hr/>	
7	Use the slider bar to select the Frame Rate (fps) .
<hr/> <p>Note:FPS varies depending on other features - See Stream Tables combinations in Appendix B.</p> <hr/>	
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 53 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

Configure the Auto Focus, Exposure, and Wide Dynamic Range (WDR) 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 54 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:
	<p>Demo</p> <ul style="list-style-type: none"> • 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 value 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**

The default setting is center weighted.

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 -

Procedure 55 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 PTZ 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 56 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 57 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: <ul style="list-style-type: none">• 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 -

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 58 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 59 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: <ul style="list-style-type: none"> • 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 60 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: <ul style="list-style-type: none"> • Contrast

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

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

- End -

Procedure 61 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 62 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: <ul style="list-style-type: none"> • 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 63 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 -

Electronic Image Stabilization

All PTZ cameras now have the Electronic Image Stabilisation feature.

Procedure 64 Enable/Disable Electronic Image Stabilization

All PTZ cameras now have Electronic Image Stabilisation feature.

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 Electronic Image Stabilization check box to enable it. OR Clear the Electronic Image Stabilization check box to disable it.
4	The default setting is 'Enabled'.

- 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 65 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 66 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 67 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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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 68 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 69 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 70 Display or Hide the User Defined OSD

- 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 71 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. <hr/> Note: Navigate to the centre of the camera field of view to create a privacy zone.
4	Click on the edit pencil button. Click and drag on the camera picture to define an area for the privacy zone. You must click and drag from the centre of the camera field of view. <hr/> Note: It is advised that you draw privacy zones larger than required to help ensure better coverage during the PTZ operations. This compensates for privacy zone distortion and repositioning during Pan, Tilt and Zoom.
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 72 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 73 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 -

PTZ Settings Menu

When the video menu is selected, Figure 29 on page 74 PTZ Settings Menu will be displayed.

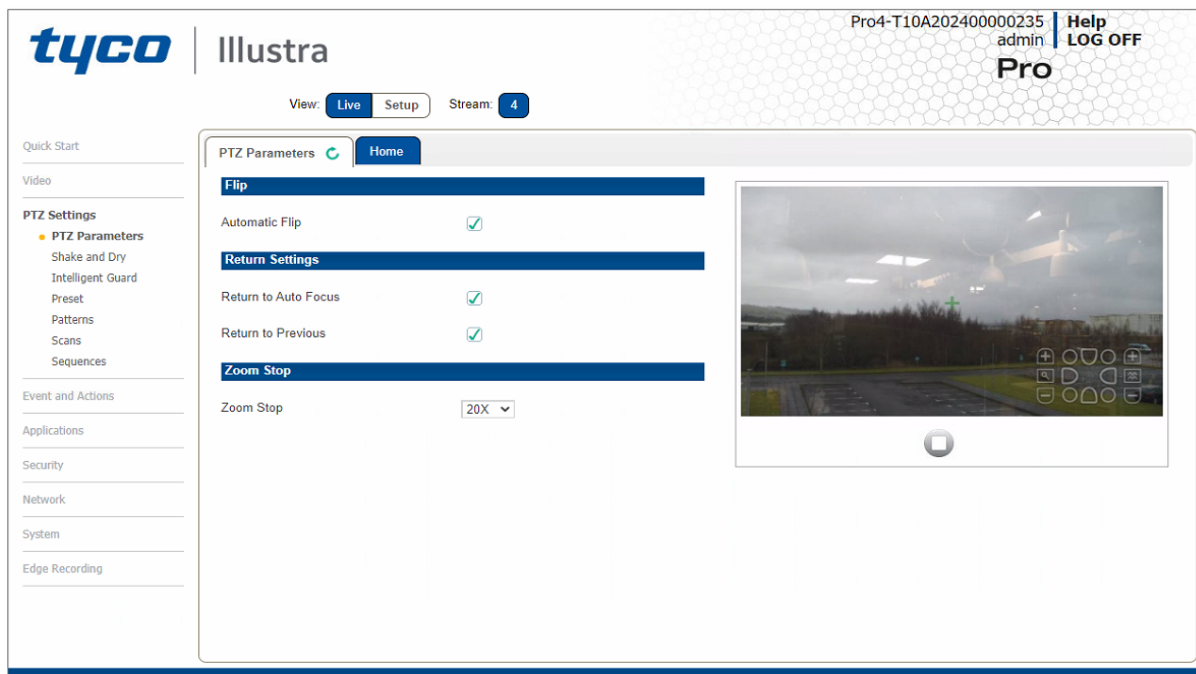


Figure 29 PTZ Settings Menu

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

- PTZ Parameters
- Shake and Dry
- Intelligent Guard
- Preset
- Patterns
- Scans
- Sequences

PTZ Parameters

PTZ Parameters allows you to adjust Automatic Flip, Return Settings, Zoom Stops, and Home Position Type.

Automatic Flip

Use the automatic (proportional) “flip” feature when you need to track someone who walks directly under the camera and continues on the other side. You start the flip by moving the tilt control to its lower limit and holding for a brief period. When the flip engages, the camera automatically rotates

180°. You may then continue to track the person as long as the tilt control stays in its lower limit. Once the tilt control is released, the camera resumes normal operation.

Procedure 74 Enable/Disable Automatic Flip

Step	Action
1	Select Setup on the Web User Interface banner to display the setup menus.
2	Select PTZ Parameters from the PTZ Settings menu.
3	Select the PTZ Parameters tab.
4	Select the Automatic Flip check box to enable automatic flip. OR Deselect the Automatic Flip check box to disable automatic flip. The default setting is 'Enabled'.
- End -	

Return Settings

When calling a Preset, the camera adopts the settings uniquely created for that Preset. When an operator moves the camera from its Preset position, the camera can return to global settings only if programmed to do so through the Return Settings page.

Procedure 75 Enable/Disable Return Settings

Step	Action
1	Select Setup on the Web User Interface banner to display the setup menus.
2	Select PTZ Parameters from the PTZ Settings menu.
3	Select the PTZ Parameters tab.
4	Select the corresponding check box to enable the return settings for: <ul style="list-style-type: none"> • Return to Auto Focus • Return to Previous OR Deselect the corresponding check box to disable the setting. The default setting is 'Enabled'.
- End -	

Zoom Stops

The Zoom Stops define how the digital zoom function is partitioned.

Note: The Zoom Stop will not be used if EIS is enabled.

The Illustra Pro PTZ camera has a 30x optical zoom with a 12X digital zoom resulting in a maximum possible zoom of 360X. The first zoom stop can be selected and is defaulted to 30x (end of Optional zoom). The last stop is 360x (but its not configurable). Pressing Zoom In continuously causes the zoom to stop at 30X. Renewing the zoom in command lets the user navigate to 360x.

Procedure 76 Setting the Zoom Stops

Step	Action
1	Select Setup on the Web User Interface banner to display the setup menus.
2	Select PTZ Parameters from the PTZ Settings menu.
3	In the Zoom Stops section use the drop box to change the First Zoom Stop setting. The default first zoom stop setting is 30X.

- End -

Home

Home allows you to adjust the Home Position Type. The home position is a preset, pattern or scan/sequence that automatically runs after a designated period of camera inactivity. Use this option if you want to keep a specific area under surveillance when the camera is not moving.

Procedure 77 Configure the Home Position

Step	Action
1	Select Setup on the Web User Interface banner to display the setup menus.
2	Select PTZ Parameters from the PTZ Settings menu.
3	Select the Home tab.
4	Select the Home Position Type : <ul style="list-style-type: none">• Preset• Pattern• Sequence• Scan• None The default is None. If an action is selected, chose the type of action to perform from the Parameter drop-down menu that is enabled.
5	Use the slider bar to select the Return Time (mins) . The default is 5.
6	Select Apply to save the settings.

- End -

Procedure 78 Clear the Home Position

1	Select Setup on the Web User Interface banner to display the setup menus.
2	Select PTZ Parameters from the PTZ Settings menu.
3	Select the Home tab.
4	Select None from Home Position Type .
5	Select Apply to save the settings.

- End -

Procedure 79 Selecting the Bubble Type

You can set the Bubble Type to either Smoked or Clear. Changing between the two bubble types selects different visual profiles to suit the bubble.

Step	Action
------	--------

- | | |
|---|--|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select PTZ Parameters from the PTZ Settings menu. |
| 3 | In the Bubble Options section use the drop box to change the Bubble Type. The default Bubble Type setting is Smoked. |

- End -

Shake and Dry

This feature helps remove rain water from the lens and dry the lens.

Procedure 80 Enable Shake and Dry

Step	Action
------	--------

- | | |
|---|--|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select Shake and Dry from the PTZ Settings menu. |
| 3 | Select the Apply button to enable the feature. |

- End -

Intelligent Guard

When selected, Intelligent Guard constantly analyzes a scene and once a target is identified (face or a person) then tracking is initiated. Tracking stops (and the camera reverts back to its position before tracking) 15 seconds after no target is identified.

Procedure 81 Enable an Intelligent Guard type

Step	Action
------	--------

- | | |
|---|---|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select Intelligent Guard from the PTZ Settings menu. |
| 3 | Select one of the following options: <ul style="list-style-type: none"> • Off • Face based • Person based |

- End -



Preset

A Preset is a pre-positioned camera scene that you program using the pan, tilt and zoom options. Up to 96 presets can be programmed on the camera.

Adding a new Preset

Create a new preset position on the camera.

Procedure 82 Add a Preset


Step	Action
1	Select Setup on the Web User Interface banner to display the setup menus.
2	Select Presets from the PTZ Settings menu. The Preset tab is displayed
3	Select  to start the video stream if it is not already active. The video pane will display the current camera view.
4	Adjust the camera view as required. <ul style="list-style-type: none">• Pan, Tilt and Zoom.• Focus Mode (Auto or Manual Focus points). Preset can also store additional Picture Settings when Exposure Mode: Shutter Priority is selected. In this case Preset can save Exposure Offset and Exposure settings. These will then be changed accordingly with a preset call up.
5	In a numbered slot on the preset table, select  to add the new preset.
6	Enter the preset name in the Preset Name text box.
7	Select Add to save the preset. OR Select Cancel .


- End -

Viewing a Preset

View an existing preset position.

Procedure 83 View a Preset

Step	Action
1	Select Setup on the Web User Interface banner to display the setup menus.
2	Select Preset from the PTZ Settings menu. The Preset tab displays.
3	Select  to start the video stream if it is not already active. The video pane will display the current camera view.




- 4 Select  to activate the corresponding preset.
The video pane will update to display the selected preset. The preset will display until interrupted by a camera command, pattern or scan.

- End -

Editing a Preset

Edit an existing preset position.

Procedure 84 Edit an existing Preset


Step	Action
1	Select Setup on the Web User Interface banner to display the setup menus.
2	Select Preset from the PTZ Settings menu. The Preset tab displays.
3	Select  to start the video stream if it is not already active. The video pane will display the current camera view.
4	Select  to activate the corresponding preset. The video pane will update to display the selected preset.
5	Select  to edit the corresponding preset.
6	Edit the preset name in the Preset Name text box if required.
7	Adjust the camera view as required. <ul style="list-style-type: none"> • Pan, Tilt and Zoom • Focus Mode and Iris Mode
8	The following camera controls can be saved as part of the preset and accessed via the Picture Settings menu: <ul style="list-style-type: none"> • White Balance • Picture Balance • Wide Dynamic Range (WDR) • IR/DayNight • Shutter Limit
9	Select Add to save the updated preset. You will be prompted to confirm the update.
10	Select OK to save the changes. OR Select Cancel .

- End -

Deleting a Preset

Delete an existing preset position from the camera.

Procedure 85 Delete a Preset

Step	Action
1	Select Setup on the Web User Interface banner to display the setup menus.
2	Select Preset from the PTZ Settings menu. The Preset tab displays.
3	Select  to delete the corresponding preset. You will be prompted to confirm the deletion.
Note: You cannot delete a preset while it is associated with another camera function. To remove the preset, refer to the associated camera function.	
4	Select OK to confirm the deletion. OR Select Cancel .
- End -	

Patterns

A pattern is a series of pan, tilt and zoom movements which can be saved to the camera. A maximum of 16 user programmable patterns can be programmed for the camera with an unlimited duration.

Note:The Illustra Pro PTZ provides Apple Peel, which is a predefined pattern stored on the camera by default that covers the entire viewing area. This pattern slowly pans 360° starting at the ceiling line. It then tilts 30° and pans 360° again, repeating until the entire viewing area is covered. The pattern will repeat continuously until interrupted by a camera command, preset, scan or alarm.

Note:There are two Apple Peel patterns on the camera by default. Apple Peel pattern one is read only and cannot be edited or deleted. Apple Peel pattern two can be edited and if necessary deleted from the camera.


Adding a Pattern

Create a new pattern.

Note:A 15 minute time-out period is implemented when adding a pattern. If no command is received within the time-out period, the Add a Pattern procedure will automatically terminate.

Procedure 86 Add a Pattern

Step	Action
1	Select Setup on the Web User Interface banner to display the setup menus.
2	Select Patterns from the PTZ Settings menu.



- 3 Select the **Record** tab.
The Record tab displays.
- 4 Select  to start the video stream if it is not already active.
The video pane will display the current camera view.
- 5 Enter the **Pattern Name**.
- 6 Select **Start**.
The Record page will update with an **Add** and **Cancel** button.
- 7 Adjust the camera view as required.
 - **Pan, Tilt and Zoom**
- 8 Select **Add** to save the pattern.
The pattern name is entered in the table on the Patterns tab.
Or
Select **Cancel**.

- End -

Running a Pattern

Activate an existing pattern.

Procedure 87 Run a Pattern

Step	Action
1	Select Setup on the Web User Interface banner to display the setup menus.
2	Select Patterns from the PTZ Settings menu. The Patterns tab displays.
3	Select  to start the video stream if it is not already active. The video pane will display the current camera view.
4	Select  to activate the corresponding pattern. The video pane will update to display the selected pattern. The pattern will run continuously until interrupted by a camera command, pattern, scan or alarm.

- End -


Deleting a Pattern

Delete an existing pattern.

Procedure 88 Delete a Pattern

Step	Action
1	Select Setup on the Web User Interface banner to display the setup menus.
2	Select Patterns from the PTZ Settings menu.

The Patterns tab displays.

- 3 Select  to delete the corresponding pattern.
You will be prompted to confirm the deletion.

Note: You cannot delete a pattern while it is associated with another camera function. To remove the pattern, refer to the associated camera function.

- 4 Select **OK** to confirm the deletion.
OR
Select **Cancel**.

- End -

Repeating a Pattern

Use this procedure to have a pattern repeat until interrupted by a camera command.

Procedure 89 Enable/Disable Repeat a Pattern

Step	Action
1	Select Setup on the Web User Interface banner to display the setup menus.
2	Select Patterns from the PTZ Settings menu.
3	Select the Repeat tab. The Repeat tab displays.
4	Select the Repeat Pattern check box to allow the selected pattern to repeat continuously. OR Deselect the Repeat Pattern check box to allow the selected pattern to run only once. The default setting is 'Enabled'.

- End -

Scans


A scan allows you to program left and right scan limits to automate surveillance activities. Once these scan limits are programmed, you can choose to run a smooth scan, stepped scan, or random scan. When active, the scan repeats until interrupted by a camera command, preset, pattern or alarm.

Setting Scan Limits

Set left and right scan limits on the camera.

Procedure 90 Set Scan Limits

Step	Action
1	Select Setup on the Web User Interface banner to display the setup menus.
2	Select Scans from the PTZ Settings menu. The Scans tab displays.

- 3 Select  to start the video stream if it is not already active.
The video pane will display the current camera view.
- 4 Adjust the camera view as required to locate the left scan limit.
- 5 Select **Set Left** to set the displayed position as the left limit.
- 6 Adjust the camera view as required to locate the right scan limit.
- 7 Select **Set Right** to set the displayed position as the right limit.
The scan limits have been set and the selected scan will now run within the scan limits set.
- 8 Select the pause time for a Stepped Scan from the **Pause** drop-down menu.
The settings are 2-10. The default is 2.

- End -

Set Scan Limits to Default Settings

Return the camera to the default scan settings.

Procedure 91 Set Scan Limits to Default Settings



Step	Action
1	Select Setup on the Web User Interface banner to display the setup menus.
2	Select Scans from the PTZ Settings menu.
3	Select the Scans tab. The Scans tab displays.
4	Select Defaults . The scan limits will default to Left: 0 and Right: 359.

- End -

Activating a Scan

Activate a scan on the camera, this will run using the scan limits saved in Setting Scan Limits.

Procedure 92 Activate a Scan

Step	Action
1	Select Setup on the Web User Interface banner to display the setup menus.
2	Select Scans from the PTZ Settings menu. The Scans tab displays.
3	Select  to start the video stream if it is not already active. The video pane will display the current camera view. (Before activating a scan, refer to the Set Scan Limits to Default Settings procedure).
4	Select  to activate the corresponding scan.

- **Smooth** -slowly pans between the left and right scan limits, starting at the left scan limit. When the right scan limit is reached, the scan reverses
- **Stepped** -pans slowly, pausing briefly every 10° between the left and right scan limits. Once the right scan limit is reached, the scan reverses.
- **Random** -pans randomly between the left and right scan limits. For example, the scan may start at 10°, then pan right 40° and pause, pan right 20° and pause, pan left 30° and pause, and pan right until it reaches the right scan limit.

- 5 The video pane will update to display the selected scan.
- 6 The scan will run continuously until interrupted by a camera command, pattern, preset or alarm.

- End -

Sequences

A Sequence is a sequential display of multiple camera Presets. Sequences provide a methodical and effective way to monitor multiple areas of interest by switching to different Presets automatically.

Sequences are created by identifying Preset views to include in the Sequence and specifying a dwell time that controls how long each Preset remains on-screen before switching to another Preset.

Up to 16 Sequences can be created, each with 16 steps (Presets)

Adding a Sequence

Create a new sequence on the camera using defined presets. Refer to Add a Preset on Page 123 if no presets have yet been added to the camera.

Procedure 93 Add a Sequence

Step	Action
1	Select Setup on the Web User Interface banner to display the setup menus. If no presets have been created, refer to Add a Preset on Page 123 before continuing to the next step.
2	Select Sequences from the PTZ Settings menu.
3	Select the Add Sequence tab.
4	Enter the Sequence Name .
5	Select a preset from the Preset Name drop-down menu.
6	Enter a dwell time in seconds in the Dwell Time (sec) text box. The settings are 10-500.
7	Select Add . The preset is now listed as part of the sequence.
8	Repeat steps 5 to 7 to add further presets to the sequence.

Note: Up to 16 presets can be added to a sequence.

- 9 Select **Apply** to save the sequence.



- End -

Activating a Sequence

Activate a selected sequence.

Procedure 94 Activate a Sequence

Step	Action
------	--------

- | | |
|---|--|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select Sequences from the PTZ Settings menu.
The Sequences tab displays. |
| 3 | Select  to start the video stream if it is not already active.
The video pane will display the current camera view. |
| 4 | Select  to activate the corresponding sequence.
The video pane will update to display the selected sequence. The sequence will run continuously until interrupted by a camera command, pattern, preset, scan or alarm. |



- End -

Editing a Sequence

Edit an existing sequence.

Procedure 95 Edit a Sequence

Step	Action
------	--------

- | | |
|---|--|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select Sequences from the PTZ Settings menu.
The Sequences tab displays. |
| 3 | Select  to edit the corresponding sequence.
The sequence will open in the Edit Sequence tab. |
| 4 | Edit the sequence name in the Sequence Name text box if required. |
| 5 | Select  to edit the corresponding preset. The following can be edited: <ul style="list-style-type: none"> • Preset Name: To add a new preset to the sequence, move to the next available free slot and select a preset from the Preset Name drop-down menu. • Dwell time |
| 6 | If required, select to remove the corresponding preset from the sequence. |
| 7 | Select Add to save the changes |
| | OR |

Select **Cancel**.


- 8 Select **Apply** to save the changes.

- End -

Deleting a Sequence

Delete an existing sequence.

Procedure 96 Delete a Sequence

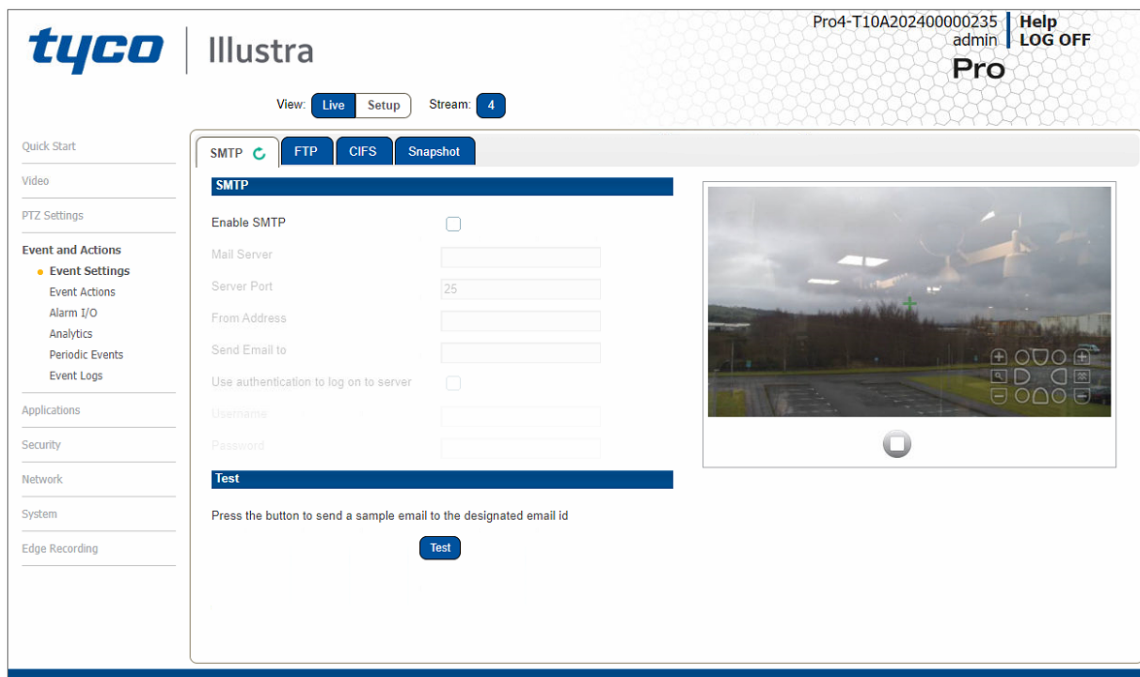
Step	Action
1	Select Setup on the Web User Interface banner to display the setup menus.
2	Select Sequences from the PTZ Settings menu. The Sequences tab displays.
3	Select  to delete the corresponding sequence. You will be prompted to confirm the deletion.
4	Select OK to delete the sequence. Or Select Cancel .

- End -

Events and Actions Menu

When you select the Events and Actions menu the Event Settings page displays, as seen in Figure 30 on page 87.

Figure 30 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 97 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'.
<hr/> <p>Note:When in Enhanced Security mode, enabling SMTP requires the admin account password.</p> <hr/>	
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: <ol style="list-style-type: none"> Enter the username for the SMTP account in the Username text box. 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 98 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 90 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 99 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 100 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 101 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 102 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.
- PTZ Action: Perform a stored preset, pattern, scan or sequence. The result of this PTZ action will continue until another PTZ or return home command is received. A PTZ command from the web GUI or ONVIF will be responded to immediately, possibly interrupting the programmed PTZ action. A PTZ action from a differemt digital input will also be done immediately.

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 103 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 **Audio Playback** option from the drop-down menu.
- 10 Select the **PTZ Action** option from the drop-down menu.
- 11 Select the **PTZ Parameter** option from the drop-down menu.

- End -

Editing a Event Action

Modify the details of an existing event action.

Procedure 104 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: <ul style="list-style-type: none"> • Name • Output - Enable/Disable • Record - Enable/Disable • Email - Enable/Disable • FTP - Enable/Disable • CIFS - Enable/Disable • Audio Playback - select the required audio clip • PTZ Action - select the required PTZ Action • PTZ Parameter - select the required PTZ Parameter |

- 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 105 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 106 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 107 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.

- End -

Procedure 108 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 109 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 110 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 111 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 112 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.

Note:The PTZ camera does not support the Motion Zones feature.

- 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 113 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 -

Video Intelligence

Video Intelligence Camera Alarms

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

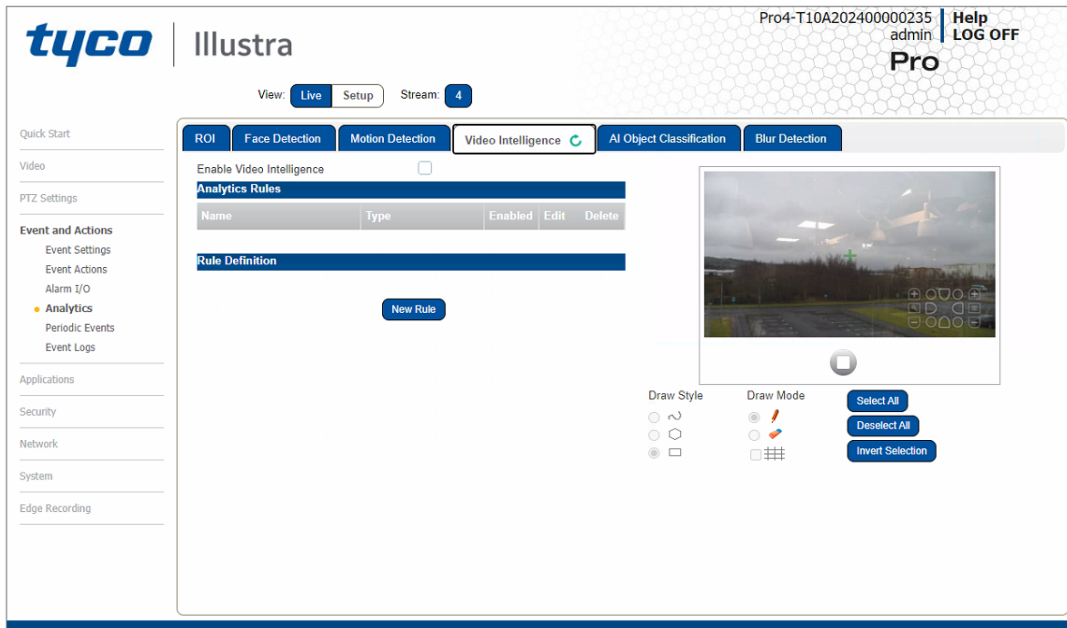
Each camera can have any number of independent Video Intelligence rules. In each rule you can define the areas in the cameras view that you want to monitor. You can name each alarm rule. It is best to use descriptive names like 'Back Door' or 'Conference Room', as these names make it easier to identify the alarm rule in the alerts log better than an abstract name. You can choose the Video Intelligence 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.

The status of each Video Intelligence alarm is highlighted in the **Status** field. There are three alarm states:

- **Red** - Alarm is disabled. The alarm can be disabled via the **Enabled** option button.
- **Yellow** - Alarm is enabled, however, the recording mode set for the camera does NOT support alarms so the alarms will not be generated. Supported modes are **Only Record on Alarm** or **Recording Always with Alarm On**.
- **Green** - Alarm is enabled and a supported recording mode is selected. Alarms will be generated.

Figure 31 Video Intelligence Tab



Video Intelligence Best Practices

To ensure you get the highest quality results when using Video Intelligence 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.
- Video Intelligence events create entries in the victor Application Server database. It is important to ensure that the Video Intelligence parameters are accurate to avoid generating false log entries.
- Exclude the Time Stamp region from the region of interest, because the time stamp changes constantly and could register as movement.
- 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 Video Intelligence 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. Video Intelligence 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 Video Intelligence alarms and searches.
- Use the new information that Video Intelligence 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

Creating a Video Intelligence Camera Alarm

To create a Video Intelligence camera alarm you must have Video Intelligence enabled on the camera.

Procedure 114 Enable/Disable Video Intelligence

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 Video Intelligence tab.
4	Select the Enable Video Intelligence check box to enable Video Intelligence on the camera. OR Deselect the Enable Video Intelligence check box to disable Video Intelligence on the camera.
5	Select Save to save your changes.

- End -

Procedure 115 Creating a Video Intelligence 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 Video Intelligence check box to enable Video Intelligence on the camera.
4	Use the drawing tools beneath the live video feed to create a Region of Interest
5	Type a Rule Name for your rule definition in the field provided.
6	Select a fault action from the Action drop-down menu. This fault action is activated when the parameters of the analytics rule are met.
7	Select a rule type from the Rule Type drop-down menu:

- a **Object Detection** - Used to detect people or objects moving into a region of interest. This alarm is similar to a motion alarm, but only detects people or objects the first time they enter the region of interest. A separate event is generated for each object that enters the region, even if the objects move into the region at the same time, unlike motion detection that generates one event.
 - b **Abandoned / Removed** - (Video Intelligence only) 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 **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.
 - g **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.
 - 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 **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.
 - j **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.
- 8 Use the **Overlap** slider bar to increase or decrease the percentage of overlap.
- 9 To apply a color filter over the Region of Interest, select one of the seven **Color Filter** check boxes.
- 10 Select **Save** to save your changes.

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

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

The Color Filters parameter allows you to limit your search results to the specified color(s) only. The color filters parameter is not available on Abandoned / Removed, Perimeter, Queue Analysis, or Crowd Formation. Leaving the color filter parameter blank has the equivalent function of 'ANY' color.

Object Detection

- a 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.

Abandoned / Removed

- a Overlap (%) - The amount of background change that must be in the region of interest before an alarm is triggered. Use a higher setting to avoid finding nearby changes or changes that are not completely in the region of interest.
- b Minimum Skip (secs) - This is the period of time after an alert, during which no further alerts are generated. A setting of 0 seconds triggers all alerts.
- c Fast Trigger - Enable Fast trigger to reduce the time required to assess if an object is abandoned or removed. As a result, alerts trigger more quickly, but the number of false alarms also increases.
- d Wipeout Amount Changed (%) - The percentage of the region of interest that must change before an alarm is triggered. Adjust to look for either a larger or smaller change in the region.
- e Wipeout Within (secs) - Time frame within which the change must occur in order to trigger the alarm. A setting of 0 seconds represents instantaneous change.

Direction

- a Overlap (%) - The amount of a detected object that must be in the region of interest while moving in the specified direction for an alarm to be triggered.
- b Direction - This is the general direction the object must move in to trigger an alarm. You can choose North, South, East or West.
- c Traversal Time- This is the maximum amount of time which an object can take to traverse most of the region before the alarm is triggered. This is to exclude objects that move too slow.

Linger

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

Dwell

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

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

Queue Analysis

- a Select Area - Additional tools display when using queue analysis to highlight zones of interest; Short, Medium and Long. Use these to define the zones of interest that must be occupied to form a short medium and long queue, all 3 zones must be defined, regardless of the queue length. Each selection is highlighted via a different color (Short = green, Medium = yellow and Long = purple).
- b Overlap (%) - The amount of detected object that must be in the region of interest to be identified as a person in a queue.
- c Queue Length - The required minimum length for an alarm to be generated. The following options are available:
 - **Empty**; this will generate an alarm when no objects are present in the designated regions of interest.
 - **Not Empty**; this will generate an alarm when an object(s) is present in the designated regions of interest.
 - **Short**; this will generate an alarm when objects are present in the short designated region of interest and meet the overlap requirements.
 - **Medium**; this will generate an alarm when objects are present in both the short and medium designated regions of interest and meet the overlap requirements.
 - **Long**; this will generate an alarm when objects are present in the short, medium and long designated regions of interest and meet the overlap requirements.

Perimeter

- a 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, the perimeter area, the minimum object size, and the maximum object size. Each selection is highlighted via a different color (perimeter area = green, protected area = yellow, minimum object size = purple, and maximum object size = red).
- b Linger Time- The minimum amount of time an object lingers before the alarm is triggered.

Crowd Formation

- a Overlap (%) - The amount of detected object that must be in the region of interest to be considered for determining the crowd size.
- b Minimum Crowd Size - The minimum number of people that must be present to generate an alarm. This can be between 2-50 people.

Exit

- a Overlap (%) - The amount of detected object that must be in the region of interest when the object leaves the scene for an alarm to be triggered. The object must appear in the scene while being outside the region of interest by the same amount. For best results select a higher overlap setting.

Enter

- a Overlap (%) - The amount of detected object that must be in the region of interest when it first appears in the camera view. The object must leave the region of interest by the

same amount before an alarm is triggered. For best results select a higher overlap setting.


- End -

Procedure 116 Enable/Disable 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 Video Intelligence 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 117 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 Video Intelligence 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 118 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 Video Intelligence 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 -

AI 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.

Creating an AI Object Classification Camera Alarm

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

Procedure 119 Enable/Disable 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.
b	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 120 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	Enter the Presets you want the rule to apply to in the Apply to which presets in the field provide or leave blank to apply to all presets

- 9 Select a rule type from the **Rule Type** drop-down menu:
Object Detection - Used to detect objects moving into a region of interest. This alarm is similar to a motion alarm, but only detects 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.
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.
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.
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.
- 10 Select **Object type** from the **Object Class** drop down
- 11 Use the **Overlap** slider bar to increase or decrease the percentage of overlap.
- 12 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 Video Intelligence above for information on the extra configuration options for each rule type.

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

Linger

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

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

Dwell

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

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

Perimeter

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

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

- End -

Procedure 121 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 122 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 123 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 -

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).

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 124 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 125 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 126 Delete Current Events

- 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 127 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 -	

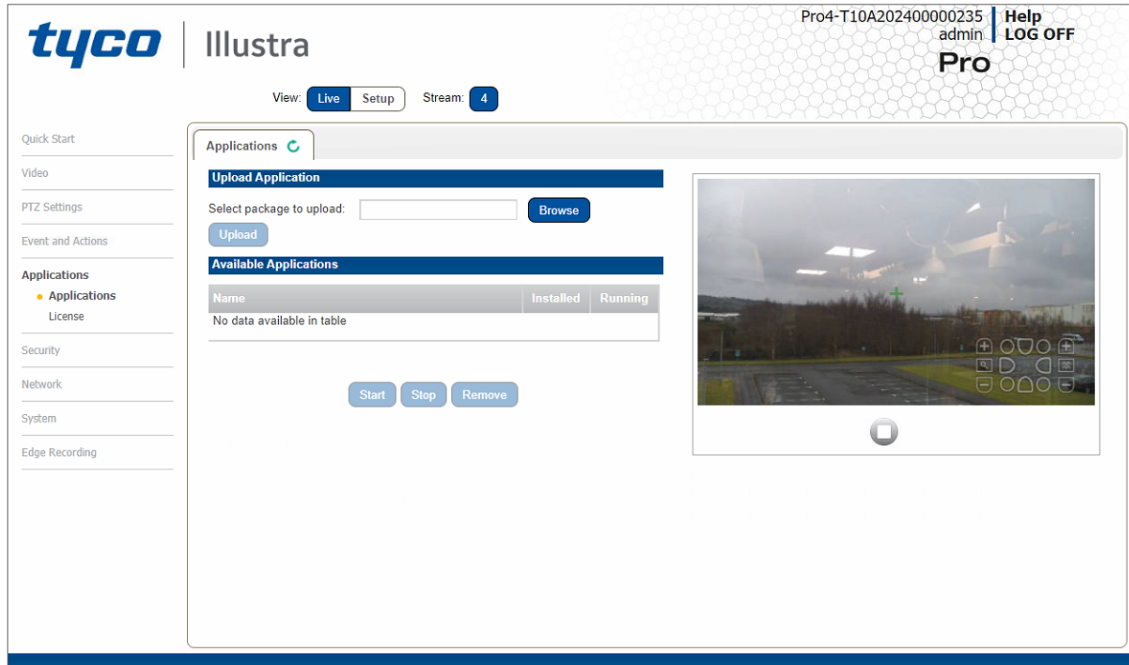
Procedure 128 Delete Current Faults

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.
<p>Note: You can select the Select All check box to mark all faults displayed in the list for deletion.</p>	
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 111.

Figure 32 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 129 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 130 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: <ul style="list-style-type: none"> 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 131 Upload a License File

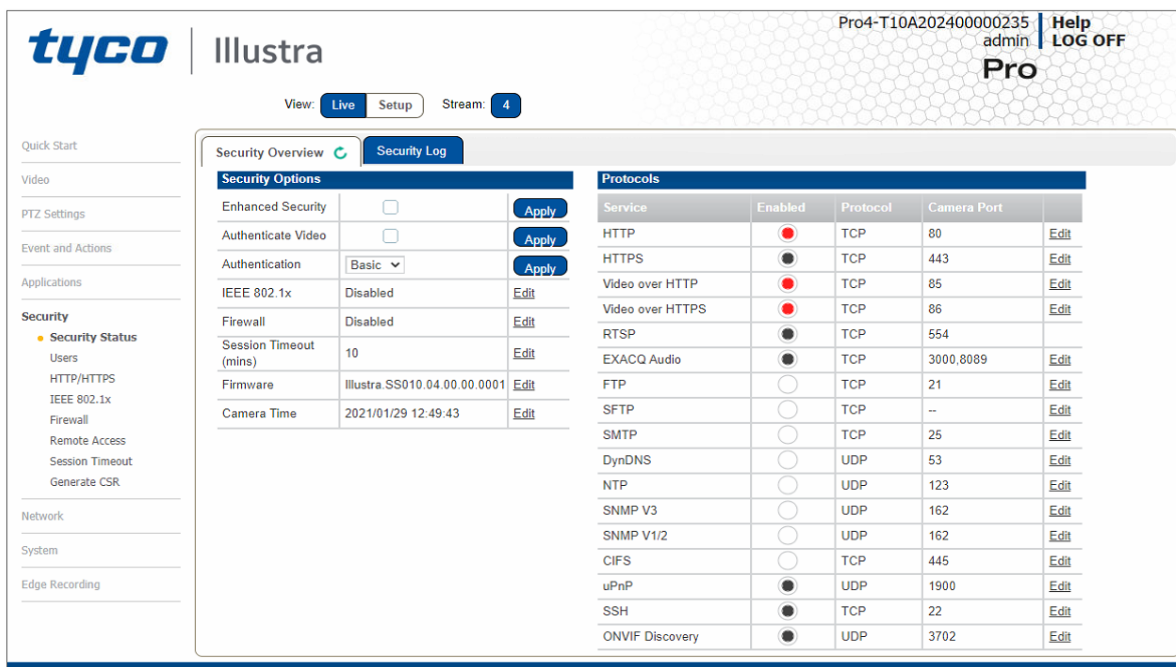
Step	Action
1	Select Setup on the Web User Interface banner to display the setup menus.
2	Select License from the Applications menu.
3	Select Browse . The Choose file dialog is displayed.
4	Navigate to the location where the license file has been saved.
5	Select the license file then select the Open 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 33 on page 113.

Figure 33 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 34.

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

Procedure 132 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 Enhanced Security feature. Your password must adhere to the minimum requirements for an Enhanced Security password as seen below. OR Clear the Enable Enhanced Security check box to disable enhanced security. Enhanced Security is disabled by default. The Security Warning dialog appears.
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: <ul style="list-style-type: none"> • Be a minimum of eight characters long • Have at least one character from one of the following character groups: <ul style="list-style-type: none"> 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 133 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 134 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 135 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 136 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 137 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 138 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 : <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• Be a minimum of seven characters long.• Have at least one character from at least three of the following character groups:<ul style="list-style-type: none">• 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 139 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 140 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 141 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 <ul style="list-style-type: none">• HTTP• HTTPS• Both
- End -	

Procedure 142 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 .
<hr/> 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. <hr/>	
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 143 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 144 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 145 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 146 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 147 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 148 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 149 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 150 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 151 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 152 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 153 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 154 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 155 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 156 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 157 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 34 .CSR file tab

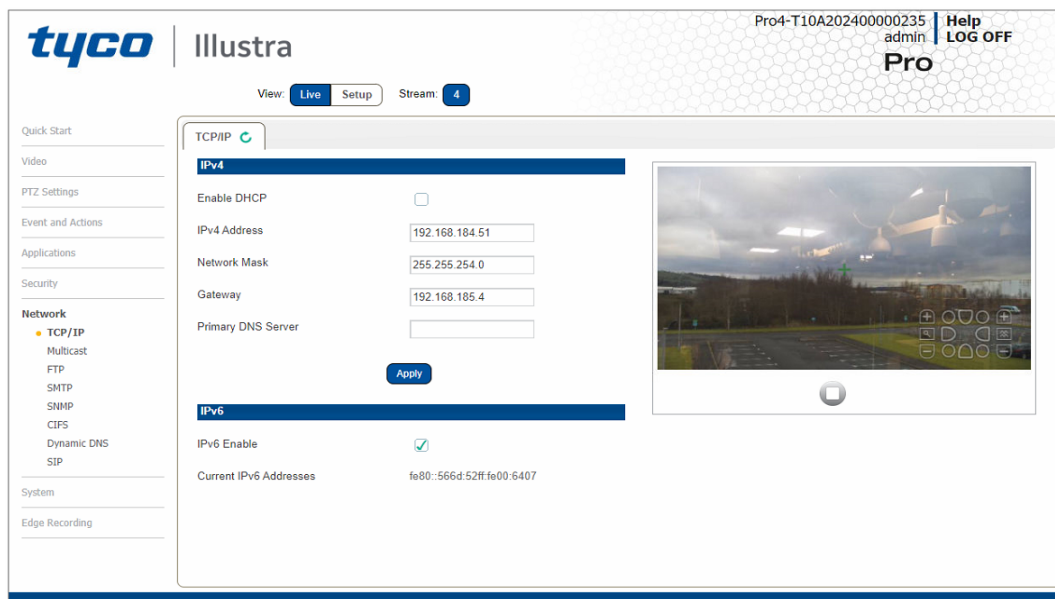
4 Copy the text shown in Green above & paste into a text file with .csr file extension.

- End -

Network Menu

When you select the **Network** menu, the **TCP/IP** page displays, as seen in Figure 35 on page 128.

Figure 35 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

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 128 for more information.

Procedure 158 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: <ol style="list-style-type: none"> 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' Enter the Network Mask in the Network Mask text box xxx.xxx.xxx.xxx. The default setting is '255.255.255.0' Enter the Gateway IP address in Gateway text box xxx.xxx.xxx.xxx. Enter the Primary DNS Server in the Primary DNS Server text box xxx.xxx.xxx.xxx. 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 159 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 160 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 Multicast configuration:

```
Stream.1.Multicast.IPAddress=224.16.18.2  
Stream.1.Multicast.Port=1032  
Stream.2.Multicast.IPAddress=224.16.18.2  
Stream.2.Multicast.Port=1030  
Stream.3.Multicast.IPAddress=0.0.0.0  
Stream.3.Multicast.Port=0
```

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 161 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 162 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 163 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 164 Configure SMTP Settings

Step	Action
1	Select Setup on the Web User Interface banner to display the setup menus.
2	Select SMTP from the Network menu. The SMTP tab displays.
3	Check the Enable SMTP check box to enable SMTP. Text boxes on the tab become available for entry.
<hr/> <p>Note:When in Enhanced Security mode, enabling SMTP requires the admin account password.</p> <hr/>	
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 165 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 : <ol style="list-style-type: none"> 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 : <ol style="list-style-type: none"> a Select the Enable V3 checkbox. b Enter the Read User. c Select the Security Level from the drop down menu: <ul style="list-style-type: none"> - 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 166 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 167 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 168 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 169 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: <ol style="list-style-type: none"> a Enter the Camera Alias in the text box. b Select a Service Provider from the drop-down list: <ul style="list-style-type: none"> • dyndns.org • easyns.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 170 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 171 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 172 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 173 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 on the product packaging.

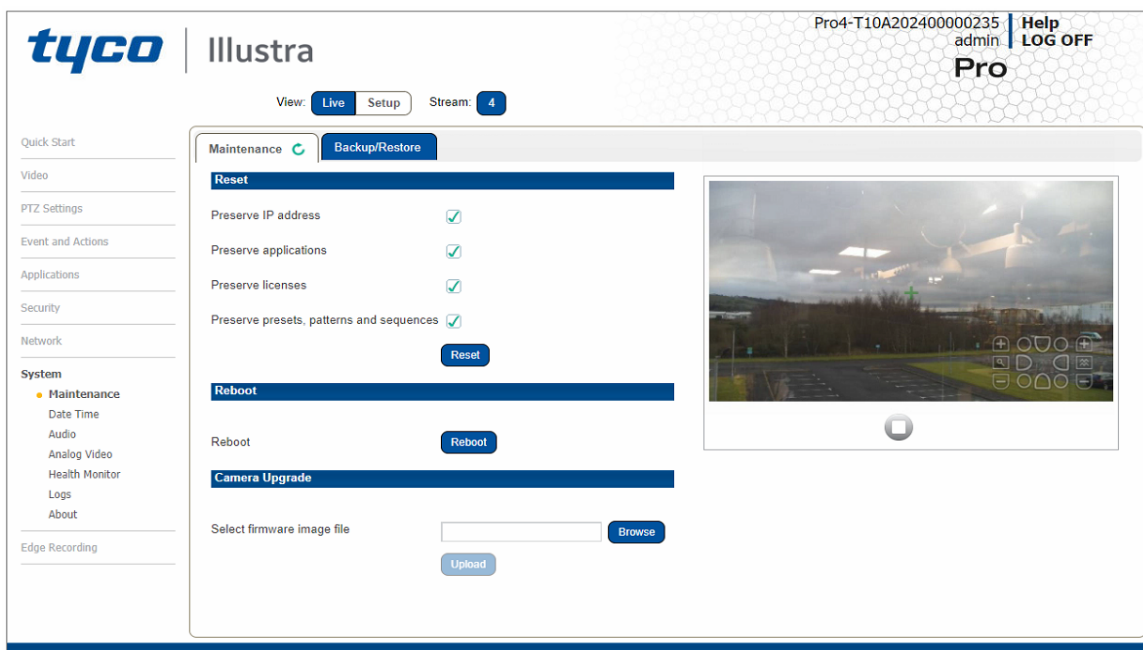
Note:USB will be enabled for 1 hour after the camera is powered from a factory reset. After 1hr, Wi-Fi will be disabled and will require a factory reset to re-enable. Illustra Wi-Fi dongle must inserted in camera for Wi-Fi access.

- End -

System

When you open the **System** menu, the **Maintenance** page appears, as seen in Figure 36 on page 138.

Figure 36 System Menu



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

- Maintenance
- Date Time
- Audio
- Analog Video
- 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 174 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. <ul style="list-style-type: none"> • 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 175 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 176 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 177 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 178 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 179 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: <ul style="list-style-type: none"> • 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.

Procedure 180 Configure Audio Input

Step	Action
1	Select Audio from the System menu. The Audio Input tab displays.
2	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'.
3	Use the slider bar to select the Input Volume . Values range from 1 to 100. The default setting is 72.

- End -

Procedure 181 Configuring Audio Output

Step	Action
1	Select Audio from the Camera Configuration menu.
2	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'.
3	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 182 Play Stored Audio

Step	Action
1	Select Audio from the System menu.
2	Select the Audio Clips tab.
3	Select to play back the corresponding audio file.
- End -	

Procedure 183 Upload an Audio File

Step	Action
1	Select Audio from the System menu.
2	Select the Audio Clips tab.
3	Select Browse . The Choose file dialog displays.
4	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: <ul style="list-style-type: none"> • 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.
5	Select Upload .
6	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 184 Delete a Stored Audio file

Step	Action
------	--------

- | | |
|---|---|
| 1 | Select Audio from the System menu. |
| 2 | Select the Audio Clips tab. |
| 3 | 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. |
| 4 | Select the Select All check box to mark all audio files for deletion. |
| 5 | Select Delete to delete the selected audio files.
You will be prompted to confirm the deletion. |
| 6 | Select OK to confirm the deletion.
Or
Select Cancel . |

- End -

Analog Video

You can select an Analog Video Source from the drop-down menu found in the **Analog Video** menu. You can manage output format of the analogue video by the dip switch located on the camera (default value) or through the Web User Interface page.

Available options are **PAL**, **NTSC** and **OFF**.

Note: Once PAL or NTSC are selected through the Web User Interface- the physical DIP Switch selection on camera will be obsolete.

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 185 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 -

PTZ Summary

The Health Monitor option displays the following PTZ statistics information:

- Pan Rights
- Pan Lefts
- Tilt Down
- Tilt Up
- Zoom Out
- Zoom In

Procedure 186 Display PTZ Summary Information

Step	Action
1	Select Setup on the GUI banner to display the setup menus.
2	Select Health Monitor from the System menu.
3	Select the PTZ Summary tab.

- 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 187 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 188 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 189 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 190 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 191 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 192 Edit Camera Name

Step	Action
------	--------

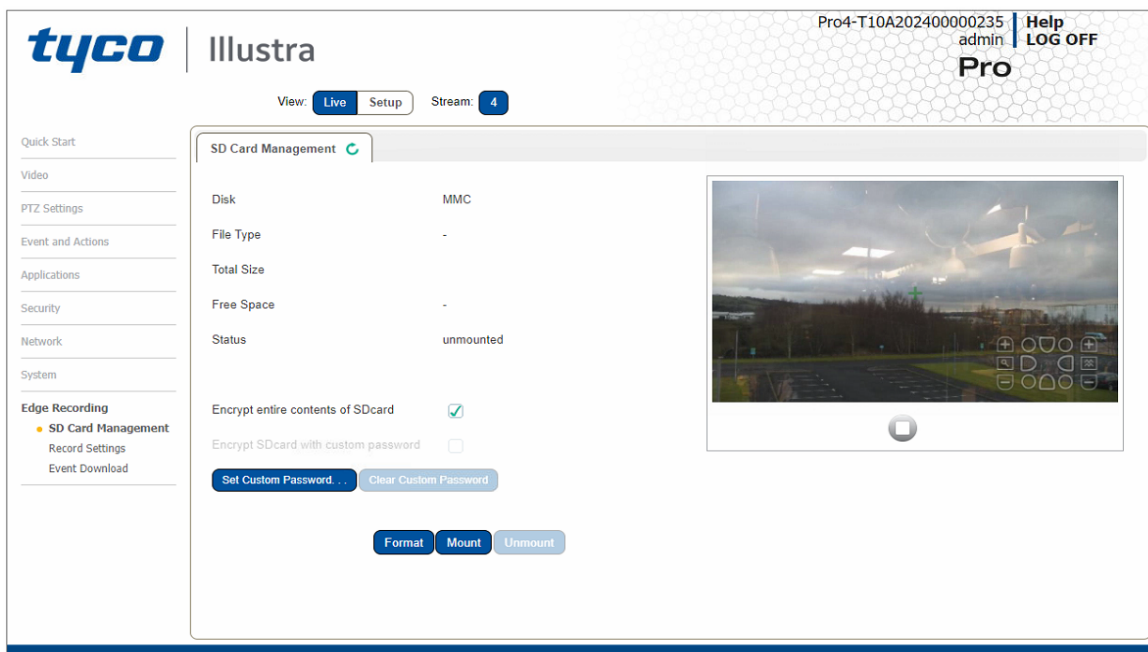
- | | |
|---|--|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select About from the System menu. The model tab displays. |
| 3 | Edit the name in the Camera Name textbox. |

- End -

Edge Recording

When you select the **Edge Recording** menu, the **Micro SD Card Management** page appears, as seen in Figure 37 on page 148.

Figure 37 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 193 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 194 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 195 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.
<hr/> <p>Note: AVI clips are not available on the camera until the Micro SD card has been inserted and the camera rebooted.</p> <hr/>	

- 3 Reconnect the power supply and power up the camera.

- End -

Procedure 196 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 197 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 198 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 199 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: <ol style="list-style-type: none">Select the required video stream from the Video drop-down menu. Refer to Procedure 5-1 Configure the Video Stream Settings.Select the Pre Event (secs) in seconds from the drop-down menu. Values range from 0 to 10. The default setting is 5 seconds.Select the Post Event (secs) in seconds from the drop-down menu. Values range from 0 to 10. The default setting is 5 seconds.
5	Select Apply to save.

- End -

Offline Record Settings

When you configure the Offline Record Settings feature and once it detects a loss of connection with the recorder, it sends the video stream to the Micro SD card within the unit. This satisfies the loss of video and continues recording. Once the recorder is back online the camera initiates sending recorded video from the Micro SD card to the recorder. The maximum time recording during the outage depends on the Micro SD card and the recorded stream you selected. If the Micro SD reaches full capacity, it deletes video from earliest recording to latest recording. This feature integrates with the VE NVR 5.0 Trickle Stor.

Procedure 200 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 want 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 a 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 201 Viewing RTSP Stream through Media Player

Step	Action
------	--------

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

- 1 Select **Media** then **Open Network Stream**.
- 2 Enter the IP address of the camera stream in the **Network URL** text box in the following format to view Stream 1 and 2:
 - **Stream 1:** rtsp://cameraip:554/videoStreamId=1
 - **Stream 2:** rtsp://cameraip:554/audioStreamId=1For example: rtsp://192.168.1.168:554/videoStreamId=1
OR
rtsp://192.168.1.168:554/videoStreamId=1&audioStreamId=1
- 3 Select **Play**. The live video stream displays.

- End -

Appendix B: Stream Tables

Pro Gen 4 - 2MP and 8MP Camera Streaming Combinations

Table 38 8MP 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,	3840x2160 3264x1840 2688x1520	(4K) 16:9 16:9 16:9	30 30 30	25 25 25	- - -
	H.264, H.265, H.264+, H.265+, MJPEG	1920x1080 1664x936 1280x720	(1080p) 16:9 (HD+) 16:9 (720p) 16:9	60 60 60	25 25 25	- - -
	H.264, H.265, H.264+, H.265+, MJPEG	1280x720 1024x576 960x444 816x464 640x360 480x272	(720p) 16:9 (PAL+) 16:9 (qHD) 16:9 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	- - - - -
	H.264, H.265, H.264+, H.265+, MJPEG	640x360 480x272	16:9 16:9	30*2 30*2	25 *2 25 *2	- -
	MJPEG	640x368	16:9	7	7	-

Note:*1 Stream 2 is restricted to 15 FPS when Stream 1 resolution is greater than 1920x1080.

Note:*2 Stream 3 is restricted to 10 FPS when Stream 1 resolution is greater than 1920x1080.

Note:Enabling TWDR on the 8MP camera will require Analogue Video to be disabled.

Note:Enabling TWDR will restrict the frame rate of Stream 1 to 25 FPS for any resolution.

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

Table 39 2MP 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,	1920x1080	(1080p) 16:9	60	30	15
	H.265,	1664x936	(HD+) 16:9	60	30	15
	H.264+, H.265+, MJPEG	1280x720	(720p) 16:9	60	30	15
Stream 2	H.264,	1280x720	(720p) 16:9	30	30	15
	H.265,	1024x576	(PAL+) 16:9	30	30	15
	H.264+,	960x544	(qHD) 16:9	30	30	15
	H.265+,	816x464	16:9	30	30	15
	MJPEG	640x360	(nHD) 16:9	30	30	15
		480x272	16:9	30	30	15
Stream 3	H.264,	640x360	16:9	30	30	15
	H.264+, H.265+, MJPEG	480x272	16:9	30	30	15
Stream 4	MJPEG	640x368	16:9	7	7	7

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

Appendix C: PTZ Dome Technical Specifications

The table below lists technical specifications of the PG4 2MP and 8MP Outdoor PTZ cameras.

General Features		
Model Type	2MP Outdoor PTZ camera	8MP Outdoor PTZ camera
Model No.	IPS02-P24-OI04	IPS08-P25-OI04
Optical zoom	42X	22X
Digital zoom	12X	12X
Megapixels	2MP (1080p)	8MP (4K)
Minimum illumination	< 0.1 Lux color 1/30s 0.01 Lux color 1/4s 0.001 Lux B/W 1/4s	< 0.1 Lux color 1/30s 0.01 Lux color 1/4s 0.001 Lux B/W 1/4s
IR Distance	≥ 150m	≥ 150m
Dynamic range	True multi shutter WDR 120db	True multi shutter WDR 120db
H.264 video latency	< 200 ms	< 200 ms
Smart codec	H.264+ & H.265+	H.264+ & H.265+
Noise reduction	2D & 3D	2D & 3D
Defog	Yes	Yes
Image stabilization EIS	Optical	Yes
flicker less	Yes	Yes
Video Out	USB Interface (micro USB) for installation & maintenance	USB Interface (micro USB) for installation & maintenance
PTZ Features		
Pan travel	360° continuous, no end stop	360° continuous, no end stop
Tilt travel	15° above horizon to straight down and auto flip	15° above horizon to straight down and auto flip
Drive Type	Direct Drive	Direct Drive
Pan & tilt accuracy	< +/- 0.2° with backlash compensation & north position automatic recentering	< +/- 0.2° with backlash compensation & north position automatic recentering
Zoom & focus accuracy	+/- 0.5%	+/- 0.5%
Manual P&T speed	< 0.25° to 100°/s scaled in proportion to zoom position	< 0.25° to 100°/s scaled in proportion to zoom position

Preset P&T speed	700° per Second Maximum	700° per Second Maximum
Smooth P&T	No noticeable stepping at full optical & 2X digital zoom	No noticeable stepping at full optical & 2X digital zoom
Special Features		
Motion detection	Yes	Yes
Face detection	Yes	Yes
License plate Recognition	Desired	Desired
Local storage	Micro SD/SDHC/SDXC card slot. Target up to 1TB, limited by card availability.	Micro SD/SDHC/SDXC card slot. Target up to 1TB, limited by card availability.
Audio	Bi-directional	Bi-directional
Digital I/O	2 input, 2 output	2 input, 2 output
Bubble	No	No
Vandal rating	IK10	IK10
Water/dust intrusion	IP66	IP66
Reboot time	< 30s	< 30s
RTC hold up time	≥ 10 days	≥ 10 days
PoE	UPoE 802.3bt (60W)	UPoE 802.3bt (60W)
Direct power	22 to 30 VAC, Class 2 LP	22 to 30 VAC, Class 2 LP
Operating Temperature	-40°C to 60°C	-40°C to 60°C
Start up temp. range	-40°C to 60°C	-40°C to 60°C
Storage Temperature	-40°C to 65°C	-40°C to 65°C
Dimensions	Ø190 x 305	Ø190 x 305

The table below lists technical specifications of the PG4 2MP and 8MP Indoor PTZ cameras.

General Features		
Model Type	2MP Indoor PTZ camera	8MP Indoor PTZ camera
Model No.	IPS02-P07-RT04	IPS08-P25-RT04
Optical zoom	30X	22X
Digital zoom	12X	12X
Megapixels	2MP (1080p)	8MP (4K)
Minimum illumination	< 0.1 Lux color 1/30s	< 0.1 Lux color 1/30s
IR Distance	N/A	N/A
Dynamic range	True multi shutter WDR 120db	True multi shutter WDR 120db
H.264 video latency	< 200 ms	< 200 ms
Smart codec	H.264+ & H.265+	H.264+ & H.265+
Noise reduction	2D & 3D	2D & 3D
Defog	Yes	Yes
Image stabilization EIS	Yes	Yes
flicker less	Yes	Yes
USB interface	MicroUSB to support Illustra WiFi Accessory	MicroUSB to support Illustra WiFi Accessory
Video Out	2 pin analog video out service port	2 pin analog video out service port
PTZ Features		
Pan travel	360° continuous, no end stop	360° continuous, no end stop
Tilt travel	0° to 90°	0° to 90°
Drive Type	Direct Drive	Direct Drive
Pan & tilt accuracy	< +/- 0.2° with backlash compensation & north position automatic recentering	< +/- 0.2° with backlash compensation & north position automatic recentering
Zoom & focus accuracy	+/- 0.5%	+/- 0.5%
Manual P&T speed	< 0.25° to 100°/s scaled in proportion to zoom position	< 0.25° to 100°/s scaled in proportion to zoom position
Preset P&T speed	Pan: 700°/Sec, Tilt: 400°/Sec(Max.)	Pan: 700°/Sec, Tilt: 400°/Sec(Max.)
Smooth P&T	No noticable stepping at full optical & 2X No noticable stepping at full optical & 2X digital	No noticable stepping at full optical & 2X digital zoomdigital zoom

	zoomdigital zoom	
Presets	256	256
Patterns	16	16
Scan (auto pan)	4	4
Sequences	16	16
Home position (idle motion)	Go to preset, pattern, scan or seq. after no PTZ activity	Go to preset, pattern, scan or seq. after no PTZ activity
Auto flip	Yes	Yes
Privacy zones	32	32
Special Features		
Motion detection	Yes	Yes
Face detection	Yes	Yes
License plate Recognition	Desired	Desired
Local storage	Micro SD/SDHC/SDXC card slot. Target up to 1TB, limited by card availability.	Micro SD/SDHC/SDXC card slot. Target up to 1TB, limited by card availability.
Audio	Bi-directional	Bi-directional
Digital I/O	2 input, 2 output	2 input, 2 output
Bubble	Yes (Tinted default) TBC Spherical or Hemisphere	Yes (Tinted default) TBC Spherical or Hemisphere
Vandal rating	IK10	IK10
Water/dust intrusion	IP66	IP66
Reboot time	< 30s	< 30s
RTC hold up time	2 days	2 days
PoE	802.3at PoE+ Type 2 (30w)	802.3at PoE+ Type 2 (30w)
Direct power	22 to 30 VAC, Class 2 LP	22 to 30 VAC, Class 2 LP
Operating Temperature	-10°C to 60°C	-10°C to 60°C
Start up temp. range	-10°C to 60°C	-10°C to 60°C
Storage Temperature	-40°C to 65°C	-40°C to 65°C

Dimensions	Ø210 x 280 (Pendant Mount) Ø230 x 255 (in-ceiling Mount)	Ø210 x 280 (Pendant Mount) Ø230 x 255 (in-ceiling Mount)
------------	--	--

End User License Agreement (EULA)

IMPORTANT - READ THIS END-USER LICENSE AGREEMENT ("EULA") CAREFULLY BEFORE OPENING THE DISK PACKAGE, DOWNLOADING THE SOFTWARE OR INSTALLING, COPYING OR OTHERWISE USING THE SOFTWARE. THIS EULA IS A LEGAL AGREEMENT BETWEEN YOU AND SENSORMATIC ELECTRONICS, LLC ("TYCO"), AND GOVERNS YOUR USE OF THE SOFTWARE AND/OR FIRMWARE ACCOMPANYING THIS EULA WHICH SOFTWARE MAY BE INCLUDED IN AN ASSOCIATED PRODUCT AND INCLUDES COMPUTER SOFTWARE AND MAY INCLUDE MEDIA, PRINTED MATERIALS, AND "ON-LINE" OR ELECTRONIC DOCUMENTATION (COLLECTIVELY, THE "SOFTWARE"). BY BREAKING THE SEAL ON THIS PACKAGE, DOWNLOADING THE SOFTWARE OR INSTALLING, COPYING OR OTHERWISE USING THE SOFTWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA. IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS EULA, DO NOT OPEN, DOWNLOAD, INSTALL, COPY OR OTHERWISE USE THE SOFTWARE.

1. SCOPE OF LICENSE. The Software may include computer code, program files and any associated media, hardware or software keys, printed material and electronic documentation. The Software may be provided to you pre-installed in a product or on a storage device (the media) as part of a computer system or other hardware or device ("System"). The Software is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. All title and intellectual property rights in and to the Software (including but not limited to any images, photographs, and text incorporated into the Software), the accompanying printed materials, and any copies of the Software, are owned by Tyco and/or its suppliers. The Software is licensed, not sold. All rights not expressly granted under this EULA are reserved by Tyco and its suppliers.

2. GRANT OF LICENSE. This EULA grants you the following rights on a non-exclusive basis:

a. General. This EULA permits you to use the Software for which you have purchased this EULA. If the Software is protected by a software or hardware key or other device, the Software may be used on any computer on which the key is installed. If the key locks the Software to a particular System, the Software may only be used on that System.

b. Locally Stored Components. The Software may include a software code component that may be stored and operated locally on one or more devices. Once you have paid the required license fees for these devices (as determined by Tyco in its sole discretion), you may install and/or use one copy of such component of the Software on each of the devices as licensed by Tyco. You may then use, access, display, run or otherwise interact with ("use") such component of the Software in connection with operating the device on which it is installed solely in the manner set forth in any accompanying documentation or, in the absence of such, solely in the manner contemplated by the nature of the Software.

c. Remotely Stored Components. The Software may also include a software code component for operating one or more devices remotely. You may install and/or use one copy of such component of the Software on a remote storage device on an internal network with all of the devices and may operate such component with each device over the internal network solely in the manner set forth in any accompanying documentation or, in the absence of such, solely in the manner contemplated by the nature of the Software; provided however, you must still acquire the required number of licenses for each of the devices with which such component is to be operated. d. Embedded

Software/Firmware. The Software may also include a software code component that is resident in a device as provided by Tyco for operating that device. You may use such component of the Software solely in connection with the use of that device, but may not retrieve, copy or otherwise transfer that software component to any other media or device without Tyco's express prior written authorization.

e. Backup Copy. You may make a back-up copy of the Software (other than embedded software) solely for archival purposes, which copy may only be used to replace a component of the Software for which you have current valid license. Except as expressly provided in this EULA, you may not otherwise make copies of the Software, including the printed materials.

3. OTHER RIGHTS AND LIMITATIONS. Your use of the Software is subject to the following additional limitations. Failure to comply with any of these restrictions will result in automatic termination of this EULA and will make available to Tyco other legal remedies.

a. Limitations on Reverse Engineering and Derivative Works. You may not reverse engineer, decompile, or disassemble the Software, and any attempt to do so shall immediately terminate this EULA - except and only to the extent that such activity may be expressly permitted, notwithstanding this limitation, either by applicable law or, in the case of open source software, the applicable open source license. You may not make any changes or modifications to any portion of the Software, or create any derivative works, without the written permission of an officer of Tyco (except as provided in Section 3(f) of this EULA with respect to "open source" software). You may not remove any proprietary notices, marks or labels from the Software. You shall institute reasonable measures to ensure compliance with the terms and conditions of this EULA by your personnel and agents.

b. Copyright Notices. You must maintain all copyright notices on all copies of the Software.

c. Transfer. You may only transfer your rights under this EULA (i) as part of a permanent sale or transfer of all of the devices for which the Software is licensed as applicable; (ii) if you transfer all of the Software (including all component parts, the media and printed materials, any upgrades and this EULA); (iii) if you do not retain any copies of any portion of the Software; (iv) if the recipient agrees to the terms of this EULA; and (v) if the Software is an upgrade, such transfer must also include all prior versions of the Software. You agree that failure to meet all of these conditions renders such transfer null and void.

d. Termination. Without prejudice to any other rights, Tyco may terminate this EULA if you fail to comply with the terms and conditions herein. In such event, you must immediately destroy all copies of the Software and all of its component parts. To the extent the Software is embedded in hardware or firmware, you will provide prompt access to Tyco or its representative to remove or lock Software features or functionality as Tyco determines.

e. Subsequent EULA. Tyco may also supersede this EULA with a subsequent EULA pursuant to providing you with any future component, release, upgrade or other modification or addition to the Software. Similarly, to the extent that the terms of this EULA conflict with any prior EULA or other agreement between you and Tyco regarding the Software, the terms of this EULA shall prevail.

f. Incorporation of "Open Source" and other Third Party Software. Portions of the Software may be subject to certain third party license agreements governing the use, copying, modification, redistribution and warranty of those portions of the Software, including what is commonly known as "open source" software. Such portions of the Software are governed solely by the terms of such other license, and no warranty is provided under this License for open source software. 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 software or receive source code for such 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 source code may be obtained free of charge by contacting your Tyco representative.

g. Trademarks. This EULA does not grant you any rights in connection with any trademarks or service marks of Tyco, its affiliates or its suppliers.

h. Rental. You may not sublicense, rent, lease or lend the Software. You may not make it available to others or post it on a server or web site or otherwise distribute it.

i. **Software Keys.** The hardware/software key, where applicable, is your proof of license to exercise the rights granted herein and must be retained by you. Lost or stolen keys will not be replaced.

j. **Demonstration and Evaluation Copies.** A demonstration or evaluation copy of the Software is covered by this EULA; provided that the licenses contained herein shall expire at the end of the demonstration or evaluation period.

k. **Registration of Software.** The Software may require registration with Tyco prior to use. If you do not register the Software, this EULA is automatically terminated and you may not use the Software.

l. **Additional Restrictions.** The Software may be subject to additional restrictions and conditions on use as specified in the documentation accompanying such Software, which additional restrictions and conditions are hereby incorporated into and made a part of this EULA.

m. **Upgrades and Updates.** To the extent Tyco makes them available, Software upgrades and updates may only be used to replace all or part of the original Software that you are licensed to use. Software upgrades and updates do not increase the number of copies licensed to you. If the Software is an upgrade of a component of a package of Software programs that you licensed as a single product, the Software may be used and transferred only as part of that single product package and may not be separated for use on more than one computer or System. Software upgrades and updates downloaded free of charge via a Tyco authorized World Wide Web or FTP site may be used to upgrade multiple Systems provided that you are licensed to use the original Software on those Systems.

n. **Tools and Utilities.** Software distributed via a Tyco-authorized World Wide Web or FTP site (or similar Tyco-authorized distribution means) as a tool or utility may be copied and installed without limitation provided that the Software is not distributed or sold and the Software is only used for the intended purpose of the tool or utility and in conjunction with Tyco products. All other terms and conditions of this EULA continue to apply.

o. **Compliance with Law.** Certain functions of the Software may require compliance by you with local, national and international laws and regulations. You are solely responsible for compliance with all applicable laws and regulations relating to your use of those functions, including but not limited to those laws and regulations pertaining to personal data protection, privacy and security, any laws relating to the collection and sharing of personal data, including video and face recognition with third parties, or any laws requiring notice to or consent of persons with respect to your use of the capabilities and functionalities of the Software.

4. **EXPORT RESTRICTIONS.** You agree that you will not export, re-export or transfer any portion of the Software, or any direct product thereof (the foregoing collectively referred to as the "Restricted Components"), to IRAN, NORTH KOREA, SYRIA, CUBA and SUDAN, including any entities or persons in those countries, either directly or indirectly ("Tyco's Position"). You also agree that you will not export, re-export or transfer the Restricted Components to any other countries except in full compliance with all applicable governmental requirements, including but not limited to applicable economic sanctions and constraints administered by the U.S. Treasury Department and applicable export control measures administered by the U.S. Department of Commerce and U.S. Department of State, any other U.S. government agencies, and measures administered by the European Union or the government agencies of any other countries. Any violation by you of the applicable laws or regulations of the U.S. or any other government, or where you breach Tyco's Position notwithstanding whether or not this is contrary to any aforementioned applicable laws or regulations, will result in automatic termination of this EULA.

5. **U.S. GOVERNMENT RESTRICTED RIGHTS.** The Software is Commercial Computer Software provided with "restricted rights" under Federal Acquisition Regulations and agency supplements to them. Any use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFAR 255.227-7013 et. seq. or 252.211-7015, or subparagraphs (a) through (d) of the Commercial

Computer Software Restricted Rights at FAR 52.227-19, as applicable, or similar clauses in the NASA FAR Supplement. Contractor/manufacturer is Sensomatic Electronics, LLC, 6 Technology Park Drive, Westford, MA 01886.

6. LIMITED WARRANTY.

a. **Warranty.** Tyco warrants that the recording medium on which the Software is recorded, hardware key, and the documentation provided with it, will be free of defects in materials and workmanship under normal use for a period of ninety (90) days from the date of delivery to the first user. Tyco further warrants that for the same period, the Software provided on the recording medium under this license will substantially perform as described in the user documentation provided with the product when used with specified hardware. THE FOREGOING EXPRESS WARRANTY REPLACES AND IS IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING BUT NOT LIMITED TO, ANY IMPLIED OR OTHER WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT OR NON-MISAPPROPRIATION OF INTELLECTUAL PROPERTY RIGHTS OF A THIRD PARTY, CUSTOM, TRADE, QUIET ENJOYMENT, ACCURACY OF INFORMATIONAL CONTENT, OR SYSTEM INTEGRATION. TYCO MAKES NO WARRANTY THAT ANY PORTION OF THE SOFTWARE WILL OPERATE ERROR-FREE, FREE OF ANY SECURITY DEFECTS OR IN AN UNINTERRUPTED MANNER. TYCO SHALL NOT BE RESPONSIBLE FOR PROBLEMS CAUSED BY CHANGES IN THE OPERATING CHARACTERISTICS OF THE DEVICE(S) UPON WHICH THE SOFTWARE IS OPERATING, OR FOR PROBLEMS IN THE INTERACTION OF THE SOFTWARE WITH NON-TYCO SOFTWARE OR HARDWARE PRODUCTS. TYCO NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON PURPORTING TO ACT ON ITS BEHALF TO MODIFY OR TO CHANGE THIS WARRANTY, NOR TO ASSUME FOR IT ANY OTHER WARRANTY OR LIABILITY CONCERNING THIS SOFTWARE. THE WARRANTY MADE BY TYCO MAY BE VOIDED BY ABUSE OR MISUSE. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS UNDER MANDATORY LAW THAT VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

b. **Exclusive Remedy.** Tyco's entire liability and your exclusive remedy under the warranty set forth in this Section 6 will be, at Tyco's option, to (i) attempt to correct Software errors with efforts Tyco believes suitable to the problem, (ii) replace at no cost the recording medium, Software or documentation with functional equivalents as applicable, or (iii) refund a pro-rated portion of the license fee paid for such Software (less depreciation based on a five-year life expectancy) and terminate this EULA, provided, in each case, that Tyco is notified in writing of all warranty problems during the applicable warranty period. Any replacement item will be warranted for the remainder of the original warranty period. No remedy is provided for failure of the Software if such failure is the result of accident, abuse, alteration or misapplication with respect to the Software or any hardware on which it is loaded. Warranty service or assistance is provided at the original point of purchase.

7. LIMITATION OF LIABILITY & EXCLUSION OF DAMAGES.

a. **LIMITATION OF LIABILITY.** IN NO EVENT WILL TYCO'S AGGREGATE LIABILITY (INCLUDING, BUT NOT LIMITED TO, LIABILITY FOR NEGLIGENCE, STRICT LIABILITY, BREACH OF CONTRACT, MISREPRESENTATION AND OTHER CONTRACT OR TORT CLAIMS) ARISING FROM OR RELATED TO THIS EULA, OR THE USE OF THE SOFTWARE, EXCEED THE GREATER OF USD\$5.00 OR THE AMOUNT OF FEES YOU PAID TO TYCO OR ITS RESELLER FOR THE SOFTWARE THAT GIVES RISE TO SUCH LIABILITY. BECAUSE AND TO THE EXTENT THAT SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSIONS OR LIMITATIONS OF LIABILITY ABOVE, THESE MAY NOT APPLY TO YOU. b. **EXCLUSION OF OTHER DAMAGES.** UNDER NO CIRCUMSTANCES SHALL TYCO OR ANY OF ITS RESELLERS OR LICENSORS BE LIABLE FOR ANY OF THE FOLLOWING: (I) THIRD PARTY CLAIMS; (II) LOSS OR DAMAGE TO ANY SYSTEMS, RECORDS OR DATA, OR LIABILITIES RELATED TO A VIOLATION OF AN INDIVIDUAL'S PRIVACY RIGHTS; OR (III) INDIRECT,

INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE, RELIANCE, OR COVER DAMAGES (INCLUDING LOST PROFITS AND LOST SAVINGS), IN EACH CASE EVEN IF TYCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOU ARE SOLELY RESPONSIBLE AND LIABLE FOR VERIFYING THE SECURITY, ACCURACY AND ADEQUACY OF ANY OUTPUT FROM THE SOFTWARE, AND FOR ANY RELIANCE THEREON. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, OR THE LIMITATION ON HOW LONG AN IMPLIED WARRANTY LASTS, SO SOME OF THE ABOVE LIMITATIONS MAY APPLY TO YOU ONLY TO THE EXTENT PERMITTED BY THOSE LAWS.

8. GENERAL. If any provision of this EULA is found to be unlawful, void, or for any reason unenforceable, then that provision shall be severed from this EULA and shall not affect the validity and enforceability of the remaining provisions. You should retain proof of the license fee paid, including model number, serial number and date of payment, and present such proof of payment when seeking service or assistance covered by the warranty set forth in this EULA. This EULA is governed by the laws of the State of New York, without regards to its conflicts of law principles. The parties hereby irrevocably agree that they submit themselves to the personal jurisdiction of the state and federal courts of New York for purposes of resolving any and all disputes arising under or related to these terms and conditions. The parties specifically exclude the application of the provisions of the United Nations Convention on Contracts for the International Sale of Goods.

9. ADDITIONAL NOTICES.

a. For Software that implements the MPEG-4 Visual Standard: PORTIONS OF THIS PRODUCT ARE LICENSED UNDER THE MPEG-4 VISUAL PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER FOR (I) ENCODING VIDEO IN COMPLIANCE WITH THE MPEG-4 VISUAL STANDARD ("MPEG-4 VIDEO") AND/OR (II) DECODING MPEG-4 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED BY MPEG LA TO PROVIDE MPEG-4 VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION INCLUDING THAT RELATING TO PROMOTIONAL, INTERNAL AND COMMERCIAL USES AND LICENSING MAY BE OBTAINED FROM MPEG LA, LLA. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpeg-la.com).

b. For Software that implements the AVC Standard: PORTIONS OF THIS PRODUCT ARE LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpeg-la.com)

e. Backup Copy. You may make a back-up copy of the Software (other than embedded software) solely for archival purposes, which copy may only be used to replace a component of the Software for which you have current valid license. Except as expressly provided in this EULA, you may not otherwise make copies of the Software, including the printed materials.

3. OTHER RIGHTS AND LIMITATIONS. Your use of the Software is subject to the following additional limitations. Failure to comply with any of these restrictions will result in automatic termination of this EULA and will make available to Tyco other legal remedies.

a. Limitations on Reverse Engineering and Derivative Works. You may not reverse engineer, decompile, or disassemble the Software, and any attempt to do so shall immediately terminate this EULA - except and only to the extent that such activity may be expressly permitted, notwithstanding

this limitation, either by applicable law or, in the case of open source software, the applicable open source license. You may not make any changes or modifications to any portion of the Software, or create any derivative works, without the written permission of an officer of Tyco (except as provided in Section 3(f) of this EULA with respect to "open source" software). You may not remove any proprietary notices, marks or labels from the Software. You shall institute reasonable measures to ensure compliance with the terms and conditions of this EULA by your personnel and agents.

b. Copyright Notices. You must maintain all copyright notices on all copies of the Software.

c. Transfer. You may only transfer your rights under this EULA (i) as part of a permanent sale or transfer of all of the devices for which the Software is licensed as applicable; (ii) if you transfer all of the Software (including all component parts, the media and printed materials, any upgrades and this EULA); (iii) if you do not retain any copies of any portion of the Software; (iv) if the recipient agrees to the terms of this EULA; and (v) if the Software is an upgrade, such transfer must also include all prior versions of the Software. You agree that failure to meet all of these conditions renders such transfer null and void.

d. Termination. Without prejudice to any other rights, Tyco may terminate this EULA if you fail to comply with the terms and conditions herein. In such event, you must immediately destroy all copies of the Software and all of its component parts. To the extent the Software is embedded in hardware or firmware, you will provide prompt access to Tyco or its representative to remove or lock Software features or functionality as Tyco determines.

e. Subsequent EULA. Tyco may also supersede this EULA with a subsequent EULA pursuant to providing you with any future component, release, upgrade or other modification or addition to the Software. Similarly, to the extent that the terms of this EULA conflict with any prior EULA or other agreement between you and Tyco regarding the Software, the terms of this EULA shall prevail.

f. Incorporation of "Open Source" and other Third Party Software. Portions of the Software may be subject to certain third party license agreements governing the use, copying, modification, redistribution and warranty of those portions of the Software, including what is commonly known as "open source" software. Such portions of the Software are governed solely by the terms of such other license, and no warranty is provided under this License for open source software. 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 software or receive source code for such 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 source code may be obtained free of charge by contacting your Tyco representative.

g. Trademarks. This EULA does not grant you any rights in connection with any trademarks or service marks of Tyco, its affiliates or its suppliers.

h. Rental. You may not sublicense, rent, lease or lend the Software. You may not make it available to others or post it on a server or web site or otherwise distribute it.

i. Software Keys. The hardware/software key, where applicable, is your proof of license to exercise the rights granted herein and must be retained by you. Lost or stolen keys will not be replaced.

j. Demonstration and Evaluation Copies. A demonstration or evaluation copy of the Software is covered by this EULA; provided that the licenses contained herein shall expire at the end of the demonstration or evaluation period.

k. Registration of Software. The Software may require registration with Tyco prior to use. If you do not register the Software, this EULA is automatically terminated and you may not use the Software.

l. Additional Restrictions. The Software may be subject to additional restrictions and conditions on use as specified in the documentation accompanying such Software, which additional restrictions and conditions are hereby incorporated into and made a part of this EULA.

m. Upgrades and Updates. To the extent Tyco makes them available, Software upgrades and updates may only be used to replace all or part of the original Software that you are licensed to use. Software upgrades and updates do not increase the number of copies licensed to you. If the Software is an upgrade of a component of a package of Software programs that you licensed as a single product, the Software may be used and transferred only as part of that single product package and may not be separated for use on more than one computer or System. Software upgrades and updates downloaded free of charge via a Tyco authorized World Wide Web or FTP site may be used to upgrade multiple Systems provided that you are licensed to use the original Software on those Systems.

n. Tools and Utilities. Software distributed via a Tyco-authorized World Wide Web or FTP site (or similar Tyco-authorized distribution means) as a tool or utility may be copied and installed without limitation provided that the Software is not distributed or sold and the Software is only used for the intended purpose of the tool or utility and in conjunction with Tyco products. All other terms and conditions of this EULA continue to apply.

o. Compliance with Law. Certain functions of the Software may require compliance by you with local, national and international laws and regulations. You are solely responsible for compliance with all applicable laws and regulations relating to your use of those functions, including but not limited to those laws and regulations pertaining to personal data protection, privacy and security, any laws relating to the collection and sharing of personal data, including video and face recognition with third parties, or any laws requiring notice to or consent of persons with respect to your use of the capabilities and functionalities of the Software.

4. EXPORT RESTRICTIONS. You agree that you will not export, re-export or transfer any portion of the Software, or any direct product thereof (the foregoing collectively referred to as the "Restricted Components"), to IRAN, NORTH KOREA, SYRIA, CUBA and SUDAN, including any entities or persons in those countries, either directly or indirectly ("Tyco's Position"). You also agree that you will not export, re-export or transfer the Restricted Components to any other countries except in full compliance with all applicable governmental requirements, including but not limited to applicable economic sanctions and constraints administered by the U.S. Treasury Department and applicable export control measures administered by the U.S. Department of Commerce and U.S. Department of State, any other U.S. government agencies, and measures administered by the European Union or the government agencies of any other countries. Any violation by you of the applicable laws or regulations of the U.S. or any other government, or where you breach Tyco's Position notwithstanding whether or not this is contrary to any aforementioned applicable laws or regulations, will result in automatic termination of this EULA.

5. U.S. GOVERNMENT RESTRICTED RIGHTS. The Software is Commercial Computer Software provided with "restricted rights" under Federal Acquisition Regulations and agency supplements to them. Any use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFAR 255.227-7013 et. seq. or 252.211-7015, or subparagraphs (a) through (d) of the Commercial Computer Software Restricted Rights at FAR 52.227-19, as applicable, or similar clauses in the NASA FAR Supplement. Contractor/manufacturer is Sensomatic Electronics, LLC, 6 Technology Park Drive, Westford, MA 01886.

6. LIMITED WARRANTY.

a. Warranty. Tyco warrants that the recording medium on which the Software is recorded, hardware key, and the documentation provided with it, will be free of defects in materials and workmanship under normal use for a period of ninety (90) days from the date of delivery to the first user. Tyco further warrants that for the same period, the Software provided on the recording medium under this

license will substantially perform as described in the user documentation provided with the product when used with specified hardware. THE FOREGOING EXPRESS WARRANTY REPLACES AND IS IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING BUT NOT LIMITED TO, ANY IMPLIED OR OTHER WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT OR NON-MISAPPROPRIATION OF INTELLECTUAL PROPERTY RIGHTS OF A THIRD PARTY, CUSTOM, TRADE, QUIET ENJOYMENT, ACCURACY OF INFORMATIONAL CONTENT, OR SYSTEM INTEGRATION. TYCO MAKES NO WARRANTY THAT ANY PORTION OF THE SOFTWARE WILL OPERATE ERROR-FREE, FREE OF ANY SECURITY DEFECTS OR IN AN UNINTERRUPTED MANNER. TYCO SHALL NOT BE RESPONSIBLE FOR PROBLEMS CAUSED BY CHANGES IN THE OPERATING CHARACTERISTICS OF THE DEVICE(S) UPON WHICH THE SOFTWARE IS OPERATING, OR FOR PROBLEMS IN THE INTERACTION OF THE SOFTWARE WITH NON-TYCO SOFTWARE OR HARDWARE PRODUCTS. TYCO NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON PURPORTING TO ACT ON ITS BEHALF TO MODIFY OR TO CHANGE THIS WARRANTY, NOR TO ASSUME FOR IT ANY OTHER WARRANTY OR LIABILITY CONCERNING THIS SOFTWARE. THE WARRANTY MADE BY TYCO MAY BE VOIDED BY ABUSE OR MISUSE. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS UNDER MANDATORY LAW THAT VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

b. Exclusive Remedy. Tyco's entire liability and your exclusive remedy under the warranty set forth in this Section 6 will be, at Tyco's option, to (i) attempt to correct Software errors with efforts Tyco believes suitable to the problem, (ii) replace at no cost the recording medium, Software or documentation with functional equivalents as applicable, or (iii) refund a pro-rated portion of the license fee paid for such Software (less depreciation based on a five-year life expectancy) and terminate this EULA, provided, in each case, that Tyco is notified in writing of all warranty problems during the applicable warranty period. Any replacement item will be warranted for the remainder of the original warranty period. No remedy is provided for failure of the Software if such failure is the result of accident, abuse, alteration or misapplication with respect to the Software or any hardware on which it is loaded. Warranty service or assistance is provided at the original point of purchase.

7. LIMITATION OF LIABILITY & EXCLUSION OF DAMAGES.

a. LIMITATION OF LIABILITY. IN NO EVENT WILL TYCO'S AGGREGATE LIABILITY (INCLUDING, BUT NOT LIMITED TO, LIABILITY FOR NEGLIGENCE, STRICT LIABILITY, BREACH OF CONTRACT, MISREPRESENTATION AND OTHER CONTRACT OR TORT CLAIMS) ARISING FROM OR RELATED TO THIS EULA, OR THE USE OF THE SOFTWARE, EXCEED THE GREATER OF USD\$5.00 OR THE AMOUNT OF FEES YOU PAID TO TYCO OR ITS RESELLER FOR THE SOFTWARE THAT GIVES RISE TO SUCH LIABILITY. BECAUSE AND TO THE EXTENT THAT SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSIONS OR LIMITATIONS OF LIABILITY ABOVE, THESE MAY NOT APPLY TO YOU. b. EXCLUSION OF OTHER DAMAGES. UNDER NO CIRCUMSTANCES SHALL TYCO OR ANY OF ITS RESELLERS OR LICENSORS BE LIABLE FOR ANY OF THE FOLLOWING: (I) THIRD PARTY CLAIMS; (II) LOSS OR DAMAGE TO ANY SYSTEMS, RECORDS OR DATA, OR LIABILITIES RELATED TO A VIOLATION OF AN INDIVIDUAL'S PRIVACY RIGHTS; OR (III) INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE, RELIANCE, OR COVER DAMAGES (INCLUDING LOST PROFITS AND LOST SAVINGS), IN EACH CASE EVEN IF TYCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOU ARE SOLELY RESPONSIBLE AND LIABLE FOR VERIFYING THE SECURITY, ACCURACY AND ADEQUACY OF ANY OUTPUT FROM THE SOFTWARE, AND FOR ANY RELIANCE THEREON. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, OR THE LIMITATION ON HOW LONG AN IMPLIED WARRANTY LASTS, SO SOME OF THE ABOVE LIMITATIONS MAY APPLY TO YOU ONLY TO THE EXTENT PERMITTED BY THOSE LAWS.

8. GENERAL. If any provision of this EULA is found to be unlawful, void, or for any reason unenforceable, then that provision shall be severed from this EULA and shall not affect the validity and enforceability of the remaining provisions. You should retain proof of the license fee paid, including model number, serial number and date of payment, and present such proof of payment when seeking service or assistance covered by the warranty set forth in this EULA. This EULA is governed by the laws of the State of New York, without regards to its conflicts of law principles. The parties hereby irrevocably agree that they submit themselves to the personal jurisdiction of the state and federal courts of New York for purposes of resolving any and all disputes arising under or related to these terms and conditions. The parties specifically exclude the application of the provisions of the United Nations Convention on Contracts for the International Sale of Goods.

9. ADDITIONAL NOTICES.

a. For Software that implements the MPEG-4 Visual Standard: PORTIONS OF THIS PRODUCT ARE LICENSED UNDER THE MPEG-4 VISUAL PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER FOR (I) ENCODING VIDEO IN COMPLIANCE WITH THE MPEG-4 VISUAL STANDARD ("MPEG-4 VIDEO") AND/OR (II) DECODING MPEG-4 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED BY MPEG LA TO PROVIDE MPEG-4 VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION INCLUDING THAT RELATING TO PROMOTIONAL, INTERNAL AND COMMERCIAL USES AND LICENSING MAY BE OBTAINED FROM MPEG LA, LLA. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpeg-la.com).

b. For Software that implements the AVC Standard: PORTIONS OF THIS PRODUCT ARE LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpeg-la.com)

e. Backup Copy. You may make a back-up copy of the Software (other than embedded software) solely for archival purposes, which copy may only be used to replace a component of the Software for which you have current valid license. Except as expressly provided in this EULA, you may not otherwise make copies of the Software, including the printed materials.

3. OTHER RIGHTS AND LIMITATIONS. Your use of the Software is subject to the following additional limitations. Failure to comply with any of these restrictions will result in automatic termination of this EULA and will make available to Tyco other legal remedies.

a. Limitations on Reverse Engineering and Derivative Works. You may not reverse engineer, decompile, or disassemble the Software, and any attempt to do so shall immediately terminate this EULA - except and only to the extent that such activity may be expressly permitted, notwithstanding this limitation, either by applicable law or, in the case of open source software, the applicable open source license. You may not make any changes or modifications to any portion of the Software, or create any derivative works, without the written permission of an officer of Tyco (except as provided in Section 3(f) of this EULA with respect to "open source" software). You may not remove any proprietary notices, marks or labels from the Software. You shall institute reasonable measures to ensure compliance with the terms and conditions of this EULA by your personnel and agents.

b. Copyright Notices. You must maintain all copyright notices on all copies of the Software.

c. Transfer. You may only transfer your rights under this EULA (i) as part of a permanent sale or transfer of all of the devices for which the Software is licensed as applicable; (ii) if you transfer all of the Software (including all component parts, the media and printed materials, any upgrades and this EULA); (iii) if you do not retain any copies of any portion of the Software; (iv) if the recipient agrees to the terms of this EULA; and (v) if the Software is an upgrade, such transfer must also include all prior versions of the Software. You agree that failure to meet all of these conditions renders such transfer null and void.

d. Termination. Without prejudice to any other rights, Tyco may terminate this EULA if you fail to comply with the terms and conditions herein. In such event, you must immediately destroy all copies of the Software and all of its component parts. To the extent the Software is embedded in hardware or firmware, you will provide prompt access to Tyco or its representative to remove or lock Software features or functionality as Tyco determines.

e. Subsequent EULA. Tyco may also supersede this EULA with a subsequent EULA pursuant to providing you with any future component, release, upgrade or other modification or addition to the Software. Similarly, to the extent that the terms of this EULA conflict with any prior EULA or other agreement between you and Tyco regarding the Software, the terms of this EULA shall prevail.

f. Incorporation of "Open Source" and other Third Party Software. Portions of the Software may be subject to certain third party license agreements governing the use, copying, modification, redistribution and warranty of those portions of the Software, including what is commonly known as "open source" software. Such portions of the Software are governed solely by the terms of such other license, and no warranty is provided under this License for open source software. 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 software or receive source code for such 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 source code may be obtained free of charge by contacting your Tyco representative.

g. Trademarks. This EULA does not grant you any rights in connection with any trademarks or service marks of Tyco, its affiliates or its suppliers.

h. Rental. You may not sublicense, rent, lease or lend the Software. You may not make it available to others or post it on a server or web site or otherwise distribute it.

i. Software Keys. The hardware/software key, where applicable, is your proof of license to exercise the rights granted herein and must be retained by you. Lost or stolen keys will not be replaced.

j. Demonstration and Evaluation Copies. A demonstration or evaluation copy of the Software is covered by this EULA; provided that the licenses contained herein shall expire at the end of the demonstration or evaluation period.

k. Registration of Software. The Software may require registration with Tyco prior to use. If you do not register the Software, this EULA is automatically terminated and you may not use the Software.

l. Additional Restrictions. The Software may be subject to additional restrictions and conditions on use as specified in the documentation accompanying such Software, which additional restrictions and conditions are hereby incorporated into and made a part of this EULA.

m. Upgrades and Updates. To the extent Tyco makes them available, Software upgrades and updates may only be used to replace all or part of the original Software that you are licensed to use. Software upgrades and updates do not increase the number of copies licensed to you. If the Software is an upgrade of a component of a package of Software programs that you licensed as a single product, the Software may be used and transferred only as part of that single product package and may not be separated for use on more than one computer or System. Software upgrades and updates downloaded free of charge via a Tyco authorized World Wide Web or FTP site may be used to

upgrade multiple Systems provided that you are licensed to use the original Software on those Systems.

n. Tools and Utilities. Software distributed via a Tyco-authorized World Wide Web or FTP site (or similar Tyco-authorized distribution means) as a tool or utility may be copied and installed without limitation provided that the Software is not distributed or sold and the Software is only used for the intended purpose of the tool or utility and in conjunction with Tyco products. All other terms and conditions of this EULA continue to apply.

4. EXPORT RESTRICTIONS. You agree that you will not export, re-export or transfer any portion of the Software, or any direct product thereof (the foregoing collectively referred to as the "Restricted Components"), to IRAN, NORTH KOREA, SYRIA, CUBA and SUDAN, including any entities or persons in those countries, either directly or indirectly ("Tyco's Position"). You also agree that you will not export, re-export or transfer the Restricted Components to any other countries except in full compliance with all applicable governmental requirements, including but not limited to applicable economic sanctions and constraints administered by the U.S. Treasury Department and applicable export control measures administered by the U.S. Department of Commerce and U.S. Department of State, any other U.S. government agencies, and measures administered by the European Union or the government agencies of any other countries. Any violation by you of the applicable laws or regulations of the U.S. or any other government, or where you breach Tyco's Position notwithstanding whether or not this is contrary to any aforementioned applicable laws or regulations, will result in automatic termination of this EULA.

5. U.S. GOVERNMENT RESTRICTED RIGHTS. The Software is Commercial Computer Software provided with "restricted rights" under Federal Acquisition Regulations and agency supplements to them. Any use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFAR 255.227-7013 et. seq. or 252.211-7015, or subparagraphs (a) through (d) of the Commercial Computer Software Restricted Rights at FAR 52.227-19, as applicable, or similar clauses in the NASA FAR Supplement. Contractor/manufacturer is Sensomatic Electronics, LLC, 6 Technology Park Drive, Westford, MA 01886.

6. LIMITED WARRANTY.

a. **Warranty.** Tyco warrants that the recording medium on which the Software is recorded, hardware key, and the documentation provided with it, will be free of defects in materials and workmanship under normal use for a period of ninety (90) days from the date of delivery to the first user. Tyco further warrants that for the same period, the Software provided on the recording medium under this license will substantially perform as described in the user documentation provided with the product when used with specified hardware. THE FOREGOING EXPRESS WARRANTY REPLACES AND IS IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING BUT NOT LIMITED TO, ANY IMPLIED OR OTHER WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT OR NON-MISAPPROPRIATION OF INTELLECTUAL PROPERTY RIGHTS OF A THIRD PARTY, CUSTOM, TRADE, QUIET ENJOYMENT, ACCURACY OF INFORMATIONAL CONTENT, OR SYSTEM INTEGRATION. TYCO MAKES NO WARRANTY THAT ANY PORTION OF THE SOFTWARE WILL OPERATE ERROR-FREE, FREE OF ANY SECURITY DEFECTS OR IN AN UNINTERRUPTED MANNER. TYCO SHALL NOT BE RESPONSIBLE FOR PROBLEMS CAUSED BY CHANGES IN THE OPERATING CHARACTERISTICS OF THE DEVICE(S) UPON WHICH THE SOFTWARE IS OPERATING, OR FOR PROBLEMS IN THE INTERACTION OF THE SOFTWARE WITH NON-TYCO SOFTWARE OR HARDWARE PRODUCTS. TYCO NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON PURPORTING TO ACT ON ITS BEHALF TO MODIFY OR TO CHANGE THIS WARRANTY, NOR TO ASSUME FOR IT ANY OTHER WARRANTY OR LIABILITY CONCERNING THIS SOFTWARE. THE WARRANTY MADE BY TYCO MAY BE VOIDED BY ABUSE OR MISUSE. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS UNDER MANDATORY LAW THAT VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

b. **Exclusive Remedy.** Tyco's entire liability and your exclusive remedy under the warranty set forth in this Section 6 will be, at Tyco's option, to (i) attempt to correct Software errors with efforts Tyco believes suitable to the problem, (ii) replace at no cost the recording medium, Software or documentation with functional equivalents as applicable, or (iii) refund a pro-rated portion of the license fee paid for such Software (less depreciation based on a five-year life expectancy) and terminate this EULA, provided, in each case, that Tyco is notified in writing of all warranty problems during the applicable warranty period. Any replacement item will be warranted for the remainder of the original warranty period. No remedy is provided for failure of the Software if such failure is the result of accident, abuse, alteration or misapplication with respect to the Software or any hardware on which it is loaded. Warranty service or assistance is provided at the original point of purchase.

7. LIMITATION OF LIABILITY & EXCLUSION OF DAMAGES.

a. **LIMITATION OF LIABILITY.** IN NO EVENT WILL TYCO'S AGGREGATE LIABILITY (INCLUDING, BUT NOT LIMITED TO, LIABILITY FOR NEGLIGENCE, STRICT LIABILITY, BREACH OF CONTRACT, MISREPRESENTATION AND OTHER CONTRACT OR TORT CLAIMS) ARISING FROM OR RELATED TO THIS EULA, OR THE USE OF THE SOFTWARE, EXCEED THE GREATER OF USD\$5.00 OR THE AMOUNT OF FEES YOU PAID TO TYCO OR ITS RESELLER FOR THE SOFTWARE THAT GIVES RISE TO SUCH LIABILITY. BECAUSE AND TO THE EXTENT THAT SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSIONS OR LIMITATIONS OF LIABILITY ABOVE, THESE MAY NOT APPLY TO YOU.

b. **EXCLUSION OF OTHER DAMAGES.** UNDER NO CIRCUMSTANCES SHALL TYCO OR ANY OF ITS RESELLERS OR LICENSORS BE LIABLE FOR ANY OF THE FOLLOWING: (I) THIRD PARTY CLAIMS; (II) LOSS OR DAMAGE TO ANY SYSTEMS, RECORDS OR DATA, OR LIABILITIES RELATED TO A VIOLATION OF AN INDIVIDUAL'S PRIVACY RIGHTS; OR (III) INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE, RELIANCE, OR COVER DAMAGES (INCLUDING LOST PROFITS AND LOST SAVINGS), IN EACH CASE EVEN IF TYCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOU ARE SOLELY

RESPONSIBLE AND LIABLE FOR VERIFYING THE SECURITY, ACCURACY AND ADEQUACY OF ANY OUTPUT FROM THE SOFTWARE, AND FOR ANY RELIANCE THEREON. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, OR THE LIMITATION ON HOW LONG AN IMPLIED WARRANTY LASTS, SO SOME OF THE ABOVE LIMITATIONS MAY APPLY TO YOU ONLY TO THE EXTENT PERMITTED BY THOSE LAWS.

8. GENERAL. If any provision of this EULA is found to be unlawful, void, or for any reason unenforceable, then that provision shall be severed from this EULA and shall not affect the validity and enforceability of the remaining provisions. You should retain proof of the license fee paid, including model number, serial number and date of payment, and present such proof of payment when seeking service or assistance covered by the warranty set forth in this EULA. This EULA is governed by the laws of the State of New York, without regards to its conflicts of law principles. The parties hereby irrevocably agree that they submit themselves to the personal jurisdiction of the state and federal courts of New York for purposes of resolving any and all disputes arising under or related to these terms and conditions. The parties specifically exclude the application of the provisions of the United Nations Convention on Contracts for the International Sale of Goods.

9. ADDITIONAL NOTICES.

a. For Software that implements the MPEG-4 Visual Standard: PORTIONS OF THIS PRODUCT ARE LICENSED UNDER THE MPEG-4 VISUAL PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER FOR (I) ENCODING VIDEO IN COMPLIANCE WITH THE MPEG-4 VISUAL STANDARD ("MPEG-4 VIDEO") AND/OR (II) DECODING MPEG-4 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED BY MPEG LA TO PROVIDE MPEG-4 VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION INCLUDING THAT RELATING TO PROMOTIONAL, INTERNAL AND COMMERCIAL USES AND LICENSING MAY BE OBTAINED FROM MPEG LA, LLA. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

b. For Software that implements the AVC Standard: PORTIONS OF THIS PRODUCT ARE LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).