tyco | Illustra

Illustra Pro Gen 2 Series

12MP Fisheye Installation and Configuration Guide

Johnson Controls

Notice

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

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

Copyright

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.

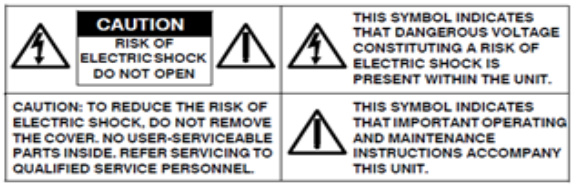
Trademarks

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

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.
- To reduce the risk of fire or electric shock, do not expose the product to rain or moisture.
- 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.
- This product is intended for professional installation, please follow local wiring regulations.
- This camera must be installed by qualified personnel and the installation should conform to all local codes.
- Do not replace batteries of the camera. Risk of explosion may occur if the battery is replaced by an incorrect type.
- To use an external power supply, please contact the camera manufacturer to confirm that the power supply complies with the LPS requirements and shares the same power specifications with the camera.
- Please use a DC 12V power adaptor and plug it to the camera and the power outlet. Alternatively, users can use an Ethernet cable and connect it to the RJ-45 connector of the camera and a Power Sourcing Equipment (PSE) switch.
- This product is intended to be supplied by a listed power adaptor or DC power source marked "L.P.S." (or "Limited Power Supply"), rated 12Vdc, 0.93A minimum or 48Vdc, 0.27A minimum (for PoE), Tma = 55 degree C minimum. If you need further assistance, please contact American Dynamics at (800) 507-6268 or (561) 912-6259 or on the Web at www.americandynamics.net.



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.

Illustra Pro Gen 2 Series 12MP Fisheye Camera

This chapter provides product features, installation procedures, and connection information regarding the Illustra Pro Gen 2 12 MP Fisheye cameras.

Product features

Lens cases require special care when handling and cleaning to avoid scratches. For information on bubble handling and cleaning, see *8200-1174-01 Bubble Clearing Procedure Application Note*.

Go to https://illustracameras.com/products.

From the Products page, select your camera product range and then select your camera model. Click **Downloads** and search for *Bubble Handling and Cleaning Procedure*.

Product overview

This chapter explains the features and installation of the Illustra Pro Gen 2 12MP Fisheye camera. Product code and description of the camera is provided in the table below.

Table 1 Product code and description of the Illustra Pro Gen 2 12MP Fisheye camera

Product Code	Model Name	Description
IPS12-F27-OI02	Illustra Pro Gen 2, 12MP Fisheye camera	Illustra Pro 12MP Fisheye, indoor/outdoor, vandal, white, TDN, w/IR, WDR

In the box

- 1 x Illustra Pro Gen2 12MP Fisheye Camera
- 1 x Security Torx L-Key
- 1 x Mounting template sticker
- 1 x Adaptor plate
- 1 x Standoff ring
- 3 x ‘4.8x24.7mm’ plastic screw anchors
- 6 x ‘M4*8H’ screws with flat spring and washer (Adaptor plate & Pendant)
- 6 x ‘8-32UNC*5/16H’ screws (Standoff ring, 4s electrical box)
- 3 x M3 Self-tapping screws (without washer)
- 3 x M3 Standard screws (without washer)
- 1 x Printed Quick Start Guide
- 1 x 2 pin terminal block
- 1 x Desiccant bag
- 1 x 12cm/5” tape
- 1 x ‘O’ ring

- 1 x Rubber cable seal

Installation tools

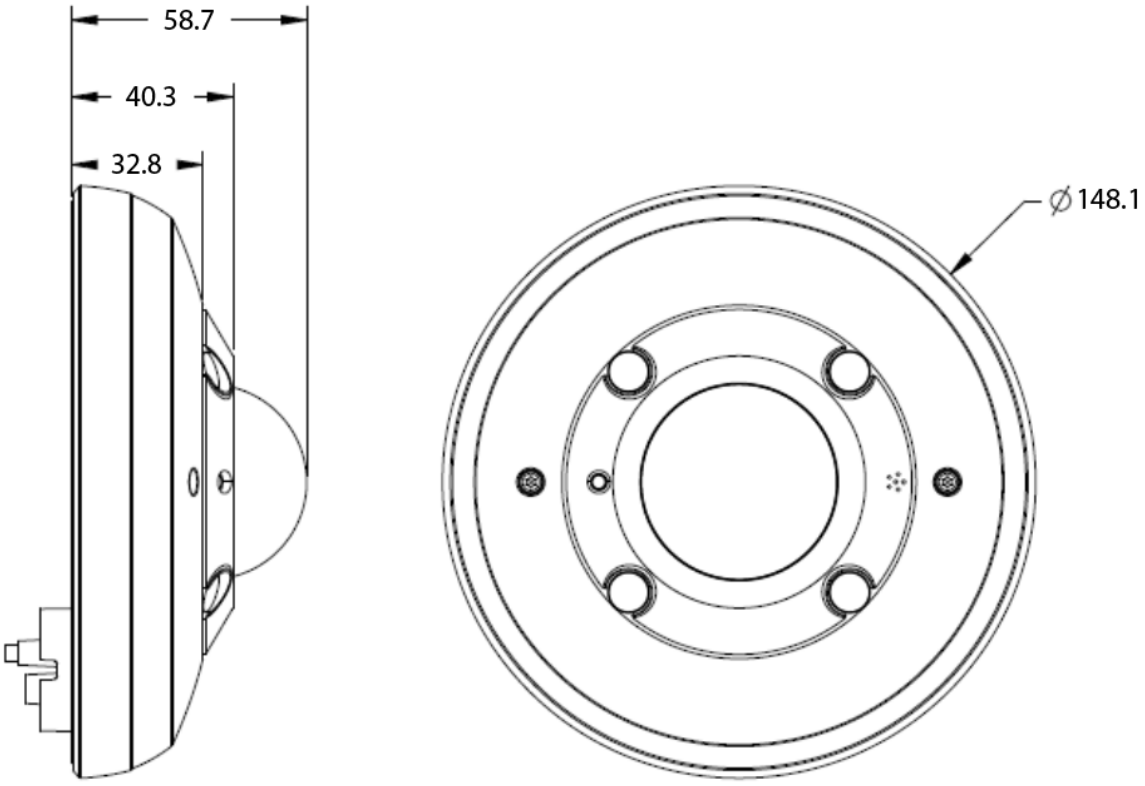
- 1 x Screw driver
- 1 x Security Torx L-Key
- 1 x Drill

Quick reference

- Default IP: 192.168.1.168 (DHCP enabled)
- Default Username / Password: admin / admin
- Power: PoE or DC 12V

Note: To provide maximum protection against condensation, replace the desiccant bag each time the top cover is removed.

Figure 1: Pro Gen2 12MP Fisheye camera



Procedure 1 Mounting the camera to a wall and powering it up

Step	Action
1	Place the mounting template sticker on the wall.

2 On the wall drill two Ø 8.01mm holes and cut out an Ø 31.5mm cabling hole as per the markings identified on the mounting template sticker.

3 Insert the two ‘4.8x24.7mm’ plastic screw anchors into the two Ø 8.01mm holes.

4 Use the Torx L-key to loosen the two screws (Figure 2) on the camera cover and remove the camera cover from the camera base.

Figure 2 Camera cover screws

5 Insert the power cable through the cable hole and hold the camera base up to the wall and connect the DC 12V cable to a DC 12V terminal or connect the RJ-45 jack to a PoE compatible network device that supplies power through the ethernet cable.

6 Align the two holes on the camera base with the two holes on the wall, insert the two M3 self-tapping screws into the two holes and securely attach the camera base to the wall.

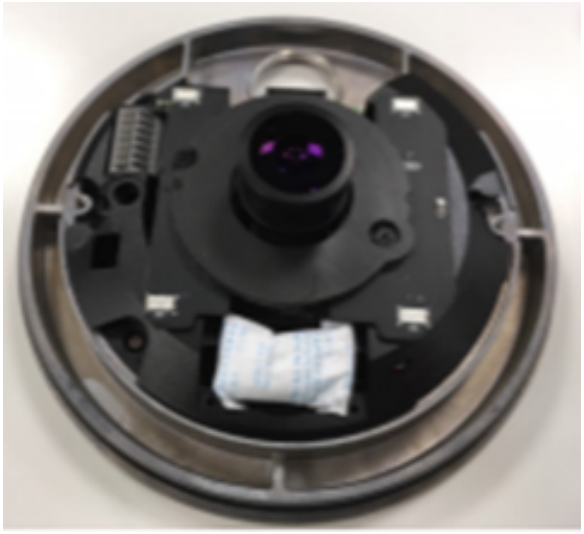
7 Remove the desiccant bag from its sealed bag and remove the protective membrane from the desiccant bag.

8 Insert the desiccant bag into the camera. See this location in Figure 3.

9 Hold the camera cover up to the camera base and align the two captive screws on the camera cover with the two threaded holes on the camera base.

10 Use the Torx L-key to secure the two camera cover screws (Figure 2) to the camera base.

Figure 3 Desiccant bag location



- End -

Procedure 2 Mounting the camera to an electrical box and powering it up

You can mount the camera to a 4s electrical box, a single gang electrical box or a dual gang electrical box.

Step	Action
1	Remove the electrical box cover.
2	Hold the standoff ring up to the electrical box and align the four holes on the standoff ring with the four holes on the electrical box.
3	Insert four 8-32UNC*5/16H' screws into the four holes and securely attach the standoff ring to the electrical box.
4	Use the Torx L-key to loosen the two screws (Figure 2) on the camera cover and remove the camera cover from the camera base.
5	Insert the power cable through the cable hole on the standoff ring and hold the camera base up to the standoff ring and connect the DC 12V cable to a DC 12V terminal or connect the RJ-45 jack to a PoE compatible network device that supplies power through the ethernet cable.
6	Align the two holes on the camera base with the two holes on the standoff ring, insert the two M3 standard screws into the two holes and securely attach the camera base to the standoff ring.
7	Remove the desiccant bag from its sealed bag and remove the protective membrane from the desiccant bag.
8	Insert the desiccant bag into the camera. See this location in Figure 3.
9	Hold the camera cover up to the camera base and align the two captive screws on the camera cover with the two threaded holes on the camera base.
10	Use the Torx L-key to secure the two camera cover screws (Figure 2) to the camera base.

- End -

Procedure 3 Mounting the camera to a tilt mount

IPFETILTMOUNT (tilt mount) accessory is applicable with the camera. See https://illustracameras.com/accessories/ for further information.

Step	Action
1	Use the Torx L-key to loosen the two screws (Figure 2) on the camera cover and remove the cover from the camera base.
2	Insert the power cable through the cable hole on the tilt mount and hold the camera base up to the tilt mount and connect the DC 12V cable to a DC 12V terminal or connect the RJ-45 jack to a PoE compatible network device that supplies power through the ethernet cable.
3	Align the two holes on the camera base with the two holes on the tilt mount, insert the two M3 standard screws into the two holes and securely attach the camera base to the tilt mount.
4	Remove the desiccant bag from its sealed bag and remove the protective membrane from the desiccant bag.
5	Insert the desiccant bag into the camera. See this location in Figure 3.
6	Hold the camera cover up to the camera base and align the two captive screws on the camera cover with the two threaded holes on the camera base.
7	Use the Torx L-key to secure the two camera cover screws (Figure 2) to the camera base.

- End -

Procedure 4 Mounting the camera to a wall mount or pendant cap

ADCiM6WALLWK (wall mount) and ADCi6DPCAPOW (pendant cap) accessories are applicable with the camera. See https://illustracameras.com/accessories/ for further information.

Step	Action
1	Hold the adaptor plate up to the accessory and align the four holes on the adaptor plate with the four holes on the accessory.
2	Insert four ‘M4*8H’ screws into the four holes and securely attach the adaptor plate to the accessory.
3	Use the Torx L-key to loosen the two screws (Figure 2) on the camera cover and remove the cover from the camera base.
4	Insert the power cable through the cable hole on the adaptor plate and hold the camera base up to the adaptor plate and connect the DC 12V cable to a DC 12V terminal or connect the RJ-45 jack to a PoE compatible network device that supplies power through the ethernet cable.
5	Align the two holes on the camera base with the two holes on the adaptor plate, insert the two M3 standard screws into the two holes and securely attach the camera base to the adaptor plate.
6	Remove the desiccant bag from its sealed bag and remove the protective membrane from the desiccant bag.
7	Insert the desiccant bag into the camera. See this location in Figure 3.
8	Hold the camera cover up to the camera base and align the two captive screws on the camera cover with the two threaded holes on the camera base.
9	Use the Torx L-key to secure the two camera cover screws (Figure 2) to the camera base.

- End -

Figure 4 Camera buttons and connections

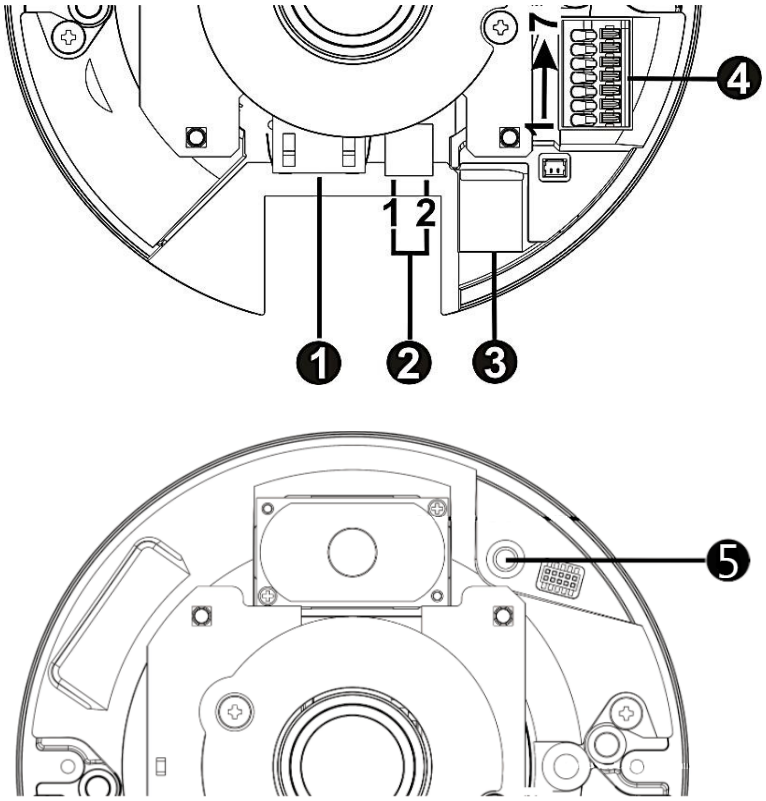


Table 1: Camera button / connection descriptions

Camera Part	Description	Comments
1	RJ-45 (PoE connection)	Network connection
2	Power (DC 12V power connection)	Power connection
3	microSD Card Slot	Insert the microSD card into the card slot to store videos and snapshots. Do not remove the microSD card when the camera is powered on.
4	Do NOT connect external power supply to the alarm I/O connector of the camera).	1 – Alarm out + 2 – Alarm out – 3 – Alarm In + 4 – Alarm In – 5 – GND 6 – Audio Out (Line Out) 7 – Audio In (Line In)
5	Factory default button	Press the button with a proper tool for at least 20 seconds to restore the system.

Procedure 5 Inserting the cable through the cable seal

Where conduit is not being used, sealing the cables that are fed through the cable seal is required. This is to protect the camera and maintain camera performance. Note: The cable seal is located on the underside of the camera body.

Step	Action
1	Locate the rubber cable seal (Figure 5) on the underside of the camera body.

Figure 5 Rubber cable seal

Note: Note: There are three tubes on the cable seal, two closed and one open.

2 Insert the power cable through the ‘open’ tube on the cable seal.

Note: Note: If additional cables are required then cut the top of the other two tubes and insert a cable into one or both tubes.

Note: Note: Ensure that there are no gaps between the cables and the tubes.

3 To add further protection to the cable then use the self-fusing tape provided and wrap it around the point where the cable enters the tube.

- End -

Network Topology

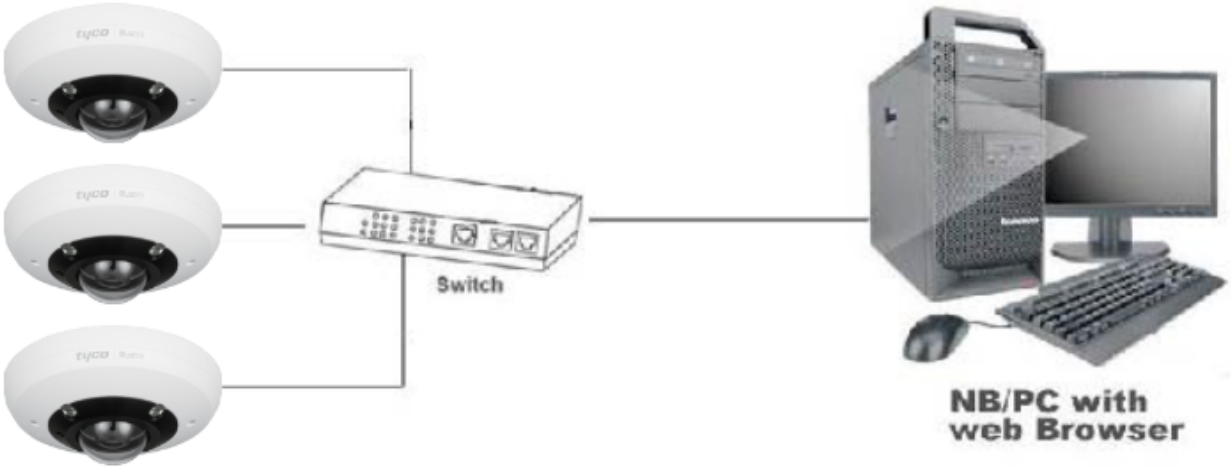
The Illustra Pro 12MP cameras deliver video images and audio in real-time using the internet and intranet. It is equipped with an Ethernet RJ-45 network interface.

The following images illustra the network topologies of the cameras.

12MP Fisheye Camera Topology

Figure 6 Camera Network Topology Type I.

Figure 7 Camera Network Topology Type II



Network Connection

Default IP Address

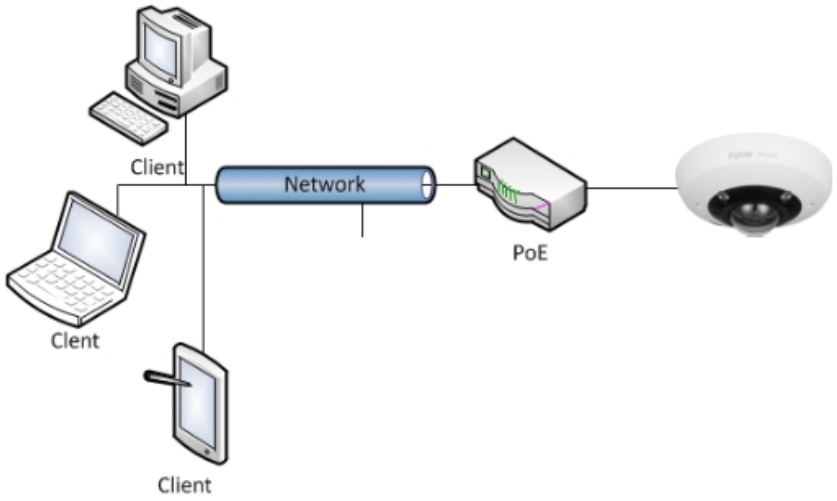
Since this is a network-based unit, an IP address must be assigned at the very first bootup. The default IP address of the unit is 192.168.1.168 and sub mask is 255.255.255.0.

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 8 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 6 Connecting from a computer

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

- End -

DHCP

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

Procedure 7 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 8 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 18 for further information regarding using the Illustra Connect tool for configuring the cameras.

Procedure 9 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 10 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 11 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 12 Enabling the correct video orientation for a wall mounted camera

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

- End -

Configuration

The following sections explain the how you can configure Illustra Pro Gen 2 cameras using the Web User Interface.

Security Mode Profiles for First Time Connection

The Illustra Pro Gen 2 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 19 for further information regarding the differences between Standard and Enhanced Security modes.

Accessing the Illustra Pro Gen 2 Camera Web User Interface

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

Procedure 13 Logging in to the Camera

Step	Action
1	Refer to Network Connection on page 14 for details on how to connect the camera to your network or computer.
2	When you select the camera, the sign in page displays.
3	Select your preferred language from the drop-down menu. The default language is English.
4	Enter the default username and password when prompted - Username: admin, Password: admin.
5	Click **Log in**. The camera Web User Interface displays. The first time that you access the camera, or after a factory reset, you are prompted to **Define a Host ID** and **Select a Security Type**. • **Define a Host ID**: The admin user must enter a 6 character code for the Host ID that includes both letters and/or numbers. This unique password can be used to access the operating system files. The HostID is not stored on the camera for security reasons and must be presented to Illustra Technical Support when remote access to the operating system is required. • **Select a Security Type**: Standard Security or Enhanced Security.
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 14 Change the Camera Web User Interface Language

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

The camera web User Interface displays in the selected language.

- End -

Live menu

When you log in to the Illustra Web User Interface, the **Live** menu appears, as seen in Figure 9 on page 21.

Figure 9 Live menu page

Displaying the Live View Page

Display the live camera view page.

Procedure 15 Display Live View Page

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

- End -

Accessing the Setup Menus from Live View

Setup menus within the Web User Interface are restricted by user account access levels. Refer to Appendix A: User Account Access on page 93 for details on the features which are available to each role.

Procedure 16 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 Live menu displays. After this, on each login the Stream page on the Video menu displays.

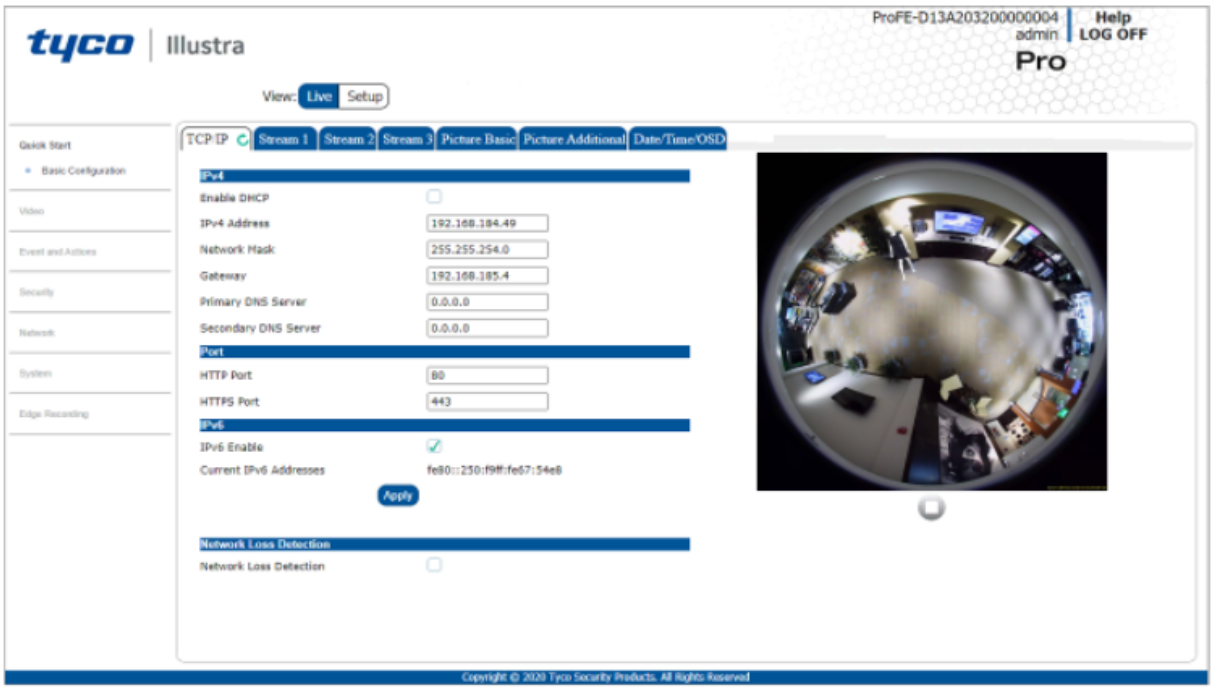
- End -

Quick Start Menu

When you select the Quick Start menu, the Basic Configuration Page displays, as shown in Figure 10 on page 23.

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 10 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 (Stream 1 / Stream 2 / Stream 3)
- 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 23 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 17 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 18 Disable DHCP

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

- End -

IPv4

Configure the IPv4 network settings for the camera.

Procedure 19 Configure the IPv4 Settings

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

- End -

IPv6

Enable or disable IPv6 on the camera.

Procedure 20 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 21 Configure the Video Stream settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select a **Stream 1, Stream 2 or Stream 3** tab in the **Basic Configuration** menu.
3	Select the desired **Image Source**.
4	Select **Stream1**, **2** or **3**,from the **Stream Number** drop-down menu.
5	Select the required **Codec** from the drop-down list: • **H264** • **H264 IntelliZip** • **H265** • **H265 IntelliZip** • **MJPEG** The default setting is 'H264'.
6	Select the required **Resolution** from the drop-down menu. The resolutions available depend on the model selected: **See the full 12MP Fisheye Streaming Combinations in Appendix C.**
7	Use the slider bar to select the **Frame Rate (fps).**

Note:FPS varies depending on other features - refer to the Appendix C for further information.

8	If MJPEG has been selected, MJPEG Quality enables. Use the slider bar to select the **MJPEG Quality**. The default setting is 75. OR
9	If MJPEG is not selected then Bitrate 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'.
10	Use the slider bar to select the **Frame Rate (fps).**

Note:FPS varies depending on other features - refer to the Appendix C for further information.

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 8192.

OR

c If CVBR has been selected, CVBR Quality and Bitrate will be enabled. Select the required CVBR Quality from the dropdown menu.

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

The default setting is 'High'.

11 Use the slider bar to select the **CVBR Bit Rate**.

12 Use the slider bar to select the **Group of Pictures (GOP)** length.

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

- End -

Picture Basic

Region of Interest (ROI)

The Camera provides an Exposure ROI which allows the user to optimize the overall brightness or darkness based on an area of interest.

Note:IR Compensation is greyed out when ROI is enabled.

Auto Shutter Mode

In this mode, the camera controls the shutter speed automatically (automatically control amount of light onto the camera sensor).

Manual Mode

In this mode, the user chooses the shutter speed.

Procedure 22 Enable or Disable exposure ROI

The default ROI is Full Field Of View (FFOV) but it can be adjusted by resizing the red rectangle (overlay).

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Picture Basic** tab in the **Basic Configuration** menu.
3	Select the **ROI Setting** drop-down menu and select ON to enable ROI Setting.
	Or

Select he **ROI Setting** drop-down menu and select OFF to disable ROI Setting.

4 When ON is selected a red box is then visible on the video pane. You can increase or reduce the size of the region of interest by clicking on and dragging the red box.

- End -

Auto Shutter Mode

The user can also adjust the Maximum Gain (i.e. auto gain adjustment) and the Maximum Exposure (auto shutter adjustment).

Procedure 23 Enable / Disable Auto Shutter Mode

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Picture Basic** tab in the **Basic Configuration** menu.
3	Select the **Auto Shutter** check box to enable Auto Shutter mode. Or Deselect the **Auto Shutter** check box to enable Auto Shutter mode.
4	Select **Apply** to save your settings.

- End -

Procedure 24 Configure Maximum Gain and shutter speed in Auto Shutter Mode

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Picture Basic** tab in the **Basic Configuration** menu.
3	Select the **Auto Shutter** check box to enable Auto Shutter mode.
4	Adjust the **Max Gain** by using the dropdown menu to select the desired minimum shutter speed.
5	Adjust t**he Min Shutter Speed** settings using the dropdown menu to select the desired value.
6	Select **Apply** to save your settings.

- End -

Procedure 25 Enable / Disable Manual Mode

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Picture Basic** tab in the **Basic Configuration** menu.
3	Select the **Manual Mode** check box to enable Auto Shutter mode. Or Deselect the **Manual** check box to enable Auto Shutter mode.
4	Select **Apply** to save your settings.

- End -

Procedure 26 Configure Manual Mode Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Picture Basic** tab in the **Basic Configuration** menu.
3	Select the **Manual Mode** check box to enable Auto Shutter mode.
4	Adjust the **Shutter Speed** by using the drop-down menu to select the desired minimum shutter speed.
5	Adjust the **Gain** settings using the drop-down menu to select the desired value.
6	Select **Apply** to save your settings.

- 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).

The 12MP Fisheye uses gamma curve adjustment for digital image rendering to enhance the dark and/or light areas – also called Digital WDR and WDR.

Procedure 27 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 in the **Basic Configuration** menu.
3	Use the required **WDR Level** from the drop-down list: • **Off** • **Low** • **Medium** • **High**
4	Select **Apply** to save your settings.

- 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 28 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** tab in 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’.
4	Select **Apply** to save your settings.

- 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 29 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** tab in the **Basic Configuration** menu.
3	Select a **Day Night Mode** setting from the drop-down menu: • **Auto High** - increases the chance of switching to BW mode as light levels drop. • **Auto Mid** - camera give a good balance of Color and BW depending on the scene. • **Auto Low**- camera will adjust between BW and Color depending on light levels. • **Forced B&W** - enable full-time black and white mode. • **Forced Color** - enable full-time color mode. • **Manual** - a slider bar displays, the user can adjust the setting to suit the environment. The default setting is 'Auto Mid'.

4 Select an **IR Light Compensation** setting from the from the drop-down list. IR Light Compensation allows the camera to adjust its IR to prevent over exposure (i.e. image being too bright) This option is Grayed Out when Exposure ROI Setting is ON (see Picture Basic Section).

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

- End -

Picture Adjustment

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

Procedure 30 Adjust the Brightness, Contrast and Saturation

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Picture Additional** tab in 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: • **Brightness** • **Sharpness** • **Contrast** • **Saturation** • **Hue** The values range from 1% to 100%. The video pane updates to display the new settings.
5	Select **Apply** to save your settings.

- End -

Procedure 31 Restore Picture Balance Defaults

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Picture Additional** tab in the **Basic Configuration** menu.
3	Select **Defaults** to restore the default settings.

- 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 32 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 in the **Basic Configuration** menu.
3	Select  to start the video stream if it is not already active. The video pane displays the current camera view.
4	Select the required **White Balance** from the drop-down menu: • **Auto:** The Auto mode is suitable for environments with light source having color temperature in the range roughly from 2700K to 7800K. • **Auto ATW:** The ATW Mode is suitable for environments with light source having color temperature in the range roughly from 2500K to 10000K. • **One Push**: The One Push mode adjust and fix the white balance is adjusted according to the scene the camera sees at the moment. This function is best for situations with minimal scene changes and continuous lighting. Important: In this mode, the value of white balance will not change as the scene or the light source varies. • **Manual:** In Manual mode the user can adjust the Red and Blue gain. The default setting is 'Auto'.
5	Select **Apply** to save your settings.

- End -

Procedure 33 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 in 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 -

Noise Reduction

The camera provides multiple Noise Reduction options for delivering optimized image quality, especially in extra low-light conditions. The 3D Noise Reduction (3DNR) feature delivers optimized

image quality, especiallly in extra low-light conditions. The Color Noise Reduction (ColorNR) feature eliminates color noise when the camera is in color mode in a dark environment.

Procedure 34 Configure 3DNR settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Picture Additional** tab in the **Basic Configuration** menu.
3	Select 3**DNR** from the Picture Additional menu.
4	Select an option from the 3**DNR** drop-down menu: • **OFF** • **3DNR High** • **3DNR Mid** • **3DNR Low**
5	Select **Apply** to save your settings.

- End -

Procedure 35 Enable/Disable 2DNR

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Picture Additional** tab in the **Basic Configuration** menu.
3	Select **2DNR** from the Picture Additional menu.
4	Select an option from the **2DNR** dropdown menu: • **ON** • **OFF**
5	Select A**pply** to save your settings.

- End -

Date / Time / OSD

Change the camera name and date and time and enable On Screen Display (OSD).

Camera Name

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

Procedure 36 Change the Camera Name

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Date / Time / OSD** in the **Basic Configuration** menu. The Date/Time/OSD tab displays.
3	Enter the name of the camera in the **Camera Friendly Name** text box.
4	Select **Apply** to save your changes.

- End -

Procedure 37 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** in the **Basic Configuration** menu.
3	Select the **Time 24-hour** check box to enable the 24-hour clock. Or Deselect the **Time 24-hour** check box to enable the 12-hour clock. The default setting is '24-hour'.
4	Select the **Date Display Format** from the drop-down menu: • **DD/MM/YYYY** • **MM/DD/YYYY** • **YYYY/MM/DD** The default setting is 'YYYY/MM/DD'.
5	Select the **Time Zone** from the drop-down menu. The default setting is '(GMT-05:00) Eastern Time (US & Canada)
6	Select the **Set Time** setting by selecting the radio buttons: • **Manually** • **via NTP** The default setting is 'Manually'.
7	If you select Manually in step 5: a Select the Date **(DD/MM/YYYY)** using the drop-down menus. b Select the Time **(HH:MM:SS)** using the drop-down menus.
8	If you select via NTP in step 5: a Enter the **NTP Server Name** in the text box.
9	Select **Apply** to save your changes.

- End -

OSD (On-Screen Display)

Within OSD you can choose whether to enable or disable the camera name and/or time in the on-screen display.

Procedure 38 Display or Hide the Camera Name/Date OSD/Camera Time OSD

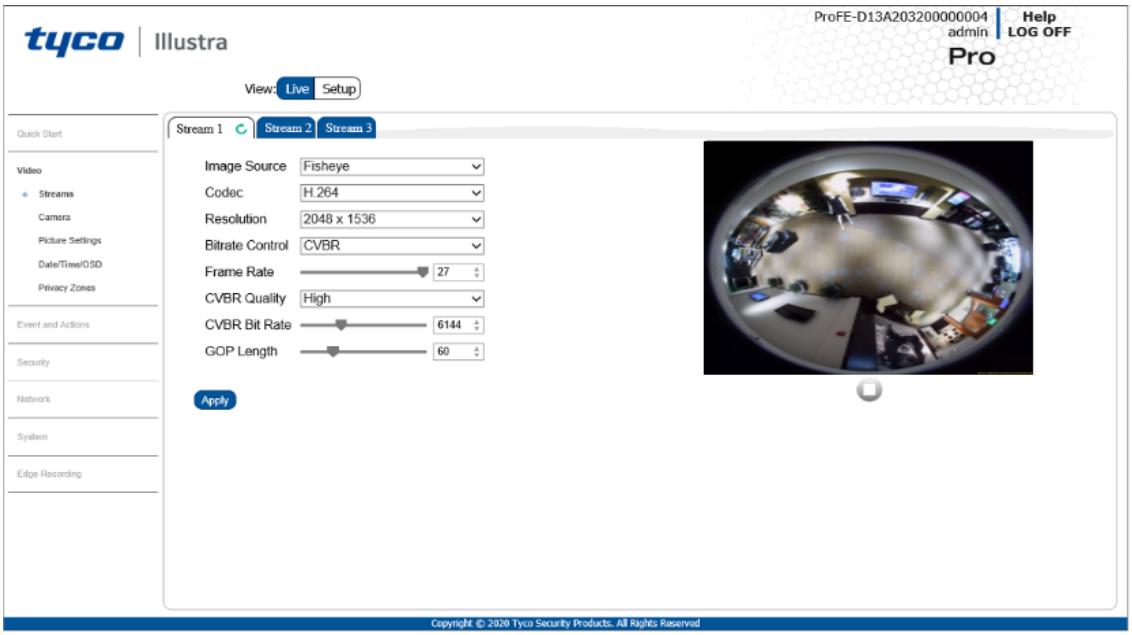
Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Date / Time / OSD** in the **Basic Configuration** menu.
3	In the **Enable OSD**, select the **Camera Na**me check box to display the camera name in the OSD. OR Deselect the **Camera Name** check box to hide the camera name in the OSD. The default setting is ‘Disabled'.
4	In the **Enable OSD**, select the **Date** check box to display the date in the OSD. OR Deselect the **Date** check box to hide the date in the OSD. The default setting is ‘Disabled’.
5	In the **Enable OSD**, select the Time check box to display the camera time in the OSD. OR Deselect the **Time** check box to hide the camera time in the OSD. The default setting is ‘Disabled’.
6	Further text may also be entered to be displayed by selecting the **Subtitle** checkbox and then entering the desired text in the text field.
7	Select **Apply** to save your changes.

- End -

Video Menu

When you select the **Video** menu, the **Streams** page displays, as seen in Figure 11 on page 36.

Figure 11 Video Menu



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

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

Streams

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

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.

Alarm Video

Edge Recording

Camera can directly record specific events directly to Micro SD card. User can chose either Stream 1, 2 or 3 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 3 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 39 Configure the Video Stream settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select a **Stream 1, Stream 2 or Stream 3** tab in the **Basic Configuration** menu.
3	Select the desired **Image Source**.
4	Select **Stream1**, **2** or **3**,from the **Stream Number** drop-down menu.
5	Select the required **Codec** from the drop-down list: • **H264** • **H264 IntelliZip** • **H265** • **H265 IntelliZip** • **MJPEG** The default setting is 'H264'.
6	Select the required **Resolution** from the drop-down menu. The resolutions available depend on the model selected: **See the full 12MP Fisheye Streaming Combinations in Appendix C.**
7	Use the slider bar to select the **Frame Rate (fps).**

Note:FPS varies depending on other features - refer to the Appendix C for further information.

8	If MJPEG has been selected, MJPEG Quality enables. Use the slider bar to select the **MJPEG Quality**. The default setting is 75. OR
9	If MJPEG is not selected then Bitrate 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'.
10	Use the slider bar to select the **Frame Rate (fps).**

Note: FPS varies depending on other features - refer to the Appendix C for further information.

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 8192.

OR

c If CVBR has been selected, CVBR Quality and Bitrate will be enabled. Select the required CVBR Quality from the dropdown menu.

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

The default setting is 'High'.

11 Use the slider bar to select the **CVBR Bit Rate**.

12 Use the slider bar to select the **Group of Pictures (GOP)** length.

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

- End -

Camera

The camera menu contains camera viewing options.

Mounting View

The camera view setting can be switched from wall mounted or ceiling mounted according to how you have mounted the camera.

Procedure 40 Enable Camera view

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Camera** from the Video menu. The Mounting tab displays.
3	Select the **Ceiling** checkbox to enable the ceiling mounted view OR

Select the **Wall** checkbox to enable the wall mounted view.

- End -

Dewarp

The dewarping feature corrects image distortions (i.e. non rectilinear appearance) caused by a fisheye lens. The user may choose to have a Fisheye stream or a stream that has already been dewarped directly from the camera.

Procedure 41 Enable Dewarping

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Camera** from the Video menu. The Mounting tab displays.
3	Select the **Edge** checkbox to enable Edge dewarping view. The camera provides a fisheye or a choice of dewarped streams, depending on the user's requirements. OR Select the **Client** checkbox to enable the Client dewarping view.
4	When **Edge** is selected in stpe 3 then you must select the **Refresh Rate** drop-menu and select and option. **Note:**The Refresh Rate is for users to adjust the speed of the virtual PTZ. The refresh speed options are 5, 10, 15 and 20. The larger the value, the faster the pan tilt movement is. Select **Save** to save the settings.

- End -

Picture Settings

Picture Basic Tab

Region of Interest (ROI)

The Camera provides an Exposure ROI which allows the user to optimize the overall brightness or darkness based on an area of interest.

Note:IR Compensation is greyed out when ROI is enabled.

Auto Shutter Mode

In this mode, the camera controls the shutter speed automatically (automatically control amount of light onto the camera sensor). The user can also adjust the Maximum Gain (i.e. auto gain adjustment) and the Maximum Exposure (auto shutter adjustment).

Manual Mode

In this mode, the user chooses the shutter speed.

Procedure 42 Enable or Disable Exposure ROI

The default ROI is Full Field Of View (FFOV) but it can be adjusted by resizing the red rectangle (overlay).

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Picture Setings** tab in the **Video** menu.
3	Select the **ROI Setting** drop-down menu and select ON to enable ROI Setting. Or Select he **ROI Setting** drop-down menu and select OFF to disable ROI Setting.
4	When ON is selected a red box is then visible on the video pane. You can increase or reduce the size of the region of interest by clicking on and dragging the red box.

- End -

Procedure 43 Enable / Disable Auto Shutter Mode

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Picture Settings** from the Video menu.
3	Select the **Picture Basic** tab.
4	Select the **Auto Shutter** check box to enable Auto Shutter mode. Or Deselect the **Auto Shutter** check box to enable Auto Shutter mode.
5	Select **Apply** to save your settings.

- End -

Procedure 44 Configure Maximum Gain and shutter speed in Auto Shutter Mode

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Picture Settings** from the Video menu.
3	Select the **Picture Basic** tab.
4	Select the **Auto Shutter** check box to enable Auto Shutter mode.
5	Adjust the **Max Gain** by using the dropdown menu to select the desired minimum shutter speed.
6	Adjust t**he Min Shutter Speed** settings using the dropdown menu to select the desired value.
7	Select **Apply** to save your settings.

- End -

Procedure 45 Enable / Disable Manual Mode

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Picture Settings** from the Video menu.
3	Select the **Picture Basic** tab.
4	Select the **Manual** check box to enable Auto Shutter mode. Or Deselect the **Manual** check box to enable Auto Shutter mode.
5	Select **Apply** to save your settings.

- End -

Procedure 46 Configure Manual Mode Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Picture Settings** from the Video menu.
3	Select the **Picture Basic** tab.
4	Select the **Manual** check box to enable Auto Shutter mode.
5	Adjust the **Shutter Speed** by using the dropdown menu to select the desired minimum shutter speed.
6	Adjust t**he Gain** settings using the dropdown menu to select the desired value.
7	Select **Apply** to save your settings.

- 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).

The 12MP Fisheye uses gamma curve adjustment for digital image rendering to enhance the dark and/or light areas – also called Digital WDR and WDR.

Procedure 47 Disable/Enable Wide Dynamic Range (WDR)

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Picture Settings** from the Video menu.
3	Select the **Picture Additional** tab.

4 Use the required **WDR Level** from the drop-down list:

- **Off**
- **Low**
- **Medium**
- **High**

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

- 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 48 Enable / Disable IR Illuminator

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Picture Settings** from the Video menu.
3	Select the **Picture Additional** tab.
4	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’.
5	Select **Apply** to save your settings.

- 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 49 Configure Day Night Mode

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Picture Settings** from the Video menu.
3	Select the **Picture Additional** tab.
4	Select a **Day Night Mode** setting from the drop-down menu: • **Auto High** - increases the chance of switching to BW mode as light levels drop. • **Auto Mid** - camera give a good balance of Color and BW depending on the scene. • **Auto Low**- camera will adjust between BW and Color depending on light levels. • **Forced B&W** - enable full-time black and white mode. • **Forced Color** - enable full-time color mode. • **Manual** - a slider bar displays, the user can adjust the setting to suit the environment. The default setting is 'Auto Mid'.
5	Select an **IR Light Compensation** setting from the from the drop-down list. IR Light Compensation allows the camera to adjust its IR to prevent over exposure (i.e. image being too bright) This option is Grayed Out when Exposure ROI Setting is ON (see Picture Basic Section).
6	Select **Apply** to save your settings.

- End -

Picture Adjustment

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

Procedure 50 Adjust the Brightness, Contrast and Saturation

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Picture Settings** from the Video menu.
3	Select the **Picture Adjustment** tab.
4	Select  to start the video stream if it is not already active. The video pane displays the current camera view.
5	Use the slider bars to adjust: • **Brightness** • **Contrast** • **Saturation** • **Sharpness** • **Hue**

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

- End -

Procedure 51 Restore Picture Balance Defaults

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Picture Settings** from the Video menu.
3	Select the **Picture Adjustment** tab.
4	Select **Defaults** to restore the default settings.

- 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 52 Configure Auto White Balance

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Picture Settings** from the Video menu.
3	Select the **Picture Adjustment** tab.
4	Select  to start the video stream if it is not already active. The video pane displays the current camera view.
5	Select the required **White Balance** from the drop-down menu: • **Auto:** The Auto mode is suitable for environments with light source having color temperature in the range roughly from 2700K to 7800K. • **Auto ATW:** The ATW Mode is suitable for environments with light source having color temperature in the range roughly from 2500K to 10000K. • **One Push**: The One Push mode adjust and fix the white balance is adjusted according to the scene the camera sees at the moment. This function is best for situations with minimal scene changes and continuous lighting. Important: In this mode, the value of white balance will not change as the scene or the light source varies. • **Manual:** In Manual mode the user can adjust the Red and Blue gain. The default setting is ‘Auto’.
6	Select **Apply** to save your settings.

- End -

Procedure 53 Manually Select White Balance

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Picture Settings** from the Video menu.
3	Select the **Picture Adjustment** tab.
4	Select  to start the video stream if it is not already active. The video pane displays the current camera view.
5	Select **Manual** from the White Balance drop-down menu. The Red and Blue slider bars display.
6	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 -

Noise Reduction

The camera provides multiple Noise Reduction options for delivering optimized image quality, especially in extra low-light conditions. The 3D Noise Reduction (3DNR) feature delivers optimized image quality, especiallly in extra low-light conditions. The Color Noise Reduction (ColorNR) feature eliminates color noise when the camera is in color mode in a dark environment.

Procedure 54 Configure 3DNR settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Picture Settings** from the Video menu.
3	Select the **Picture Adjustment** tab.
4	Select 3**DNR** from the Picture Additional menu.
5	Select an option from the 3**DNR** dropdown menu: • **OFF** • **3DNR High** • **3DNR Mid** • **3DNR Low**
6	Select **Apply** to save your settings.

- End -

Procedure 55 Enable/Disable 2DNR

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Picture Settings** from the Video menu.
3	Select the **Picture Adjustment** tab.
4	Select **2DNR** from the Picture Additional menu.
5	Select an option from the **2DNR** dropdown menu: • **ON** • **OFF**
6	Select Apply to save your settings.

- End -

Procedure 56 Configure ColorNR settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Picture Settings** from the Video menu.
3	Select the **Picture Adjustment** tab.
4	Select an option from the **ColorNR** dropdown menu: • **Off color** • **Low color** • **Mid color** • **High color**
5	Select **Apply** to save your settings.

- End -

Date / Time / OSD

Change the camera name and date and time and enable On Screen Display (OSD).

Camera Name

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

Procedure 57 Change the Camera Name

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. The Date/Time/OSD tab displays.
3	Enter the name of the camera in the **Camera Friendly Name** text box.

4 Select **Apply** to save your changes.

- End -

Procedure 58 Configuring the Date and Time

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

- End -

OSD (On-Screen Display)

Within OSD you can choose whether to enable or disable the camera name and/or time in the on-screen display.

Procedure 59 Display or Hide the Camera Name/Date OSD/Camera Time OSD

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 In the **Enable OSD**, select the **Camera Na**me 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'.

4 In the **Enable OSD**, select the **Date** check box to display the date in the OSD.

OR

Deselect the **Date** check box to hide the date in the OSD.

The default setting is ‘Disabled’.

5 In the **Enable OSD**, select the Time check box to display the camera time in the OSD.

OR

Deselect the **Time** check box to hide the camera time in the OSD.

The default setting is ‘Disabled’.

6 Further text may also be entered to be displayed by selecting the **Subtitle** checkbox and then entering the desired text in the text field.

7 Select **Apply** to save your changes.

- 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 9 rectangular privacy zones can be used on the camera.

Defining a Privacy Zone

Create a privacy zone on the camera.

Procedure 60 Define a Privacy Zone

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Privacy Zones** from the **Video** menu.
3	Select  to start the video stream if it is not already active. The video pane displays the current camera view.
4	Click on the edit pencil button. Click and drag on the camera picture to define an area for the privacy zone.
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.

8 Select **Add** to save the current privacy zone.

- End -

Enabling or Disabling a Privacy Zone

Select a privacy zone to hide or display on the camera. The PTZ camera does not support Enabling or Disabling a Privacy Zone, zones should be deleted and redrawn when necessary.

Procedure 61 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 62 Delete a Privacy Zone

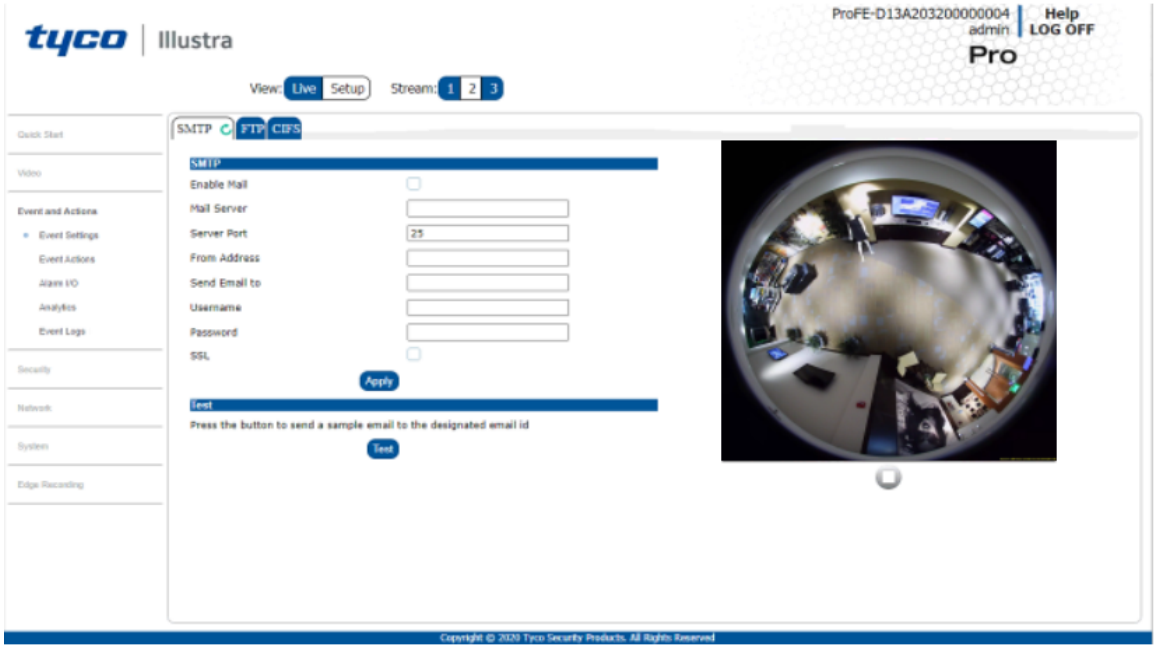
Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Privacy Zones** from the **Video** menu. The Privacy zones tab displays.
3	Select the corresponding **Delete** check box to mark the privacy zone for deletion.
4	Select **Delete** to delete the selected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

- End -

Events and Actions Menu

When you select the Events and Actions menu the Event Settings page displays, as seen in Figure 12 on page 50.

Figure 12 Events and Actions Menu



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

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

Event Settings

Configure the SMTP, FTP, and CIFS 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.

Note:SMTP settings must be configured to enable email alerts when using analytics.

Procedure 63 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	Check the **Enable Mail** check box to enable SMPT. Text boxes on the tab become available for entry. **Note:**When in Enhanced Security mode, enabling SMTP requires the admin account password.
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 from email to send email alerts to in the **Send Email** text box.
9	Select the **Username** text box and enter a username.
10	Select the **Password** text box and enter a password.
11	Check the **SSL** check box to enable SSL.
12	Select **Apply** to save the settings.

- End -

Test SMTP Settings

Test the SMTP settings that have been configured correctly.

Procedure 64 Test the 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 **Test**. A sample text file will be sent to the specified SMTP destination to confirm that SMTP settings are correct.

- End -

FTP

Configure the FTP settings for the FTP server. This is required to send video files from triggered analytic alerts. FTP must be configured to enable FTP video alerts when using analytics.

Note:FTP settings can also be configured in the **Network** menu.

Procedure 65 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 Deselect the **Enable FTP** check box to disable FTP. The default setting is 'Enabled'. **Note:**When in Enhanced Security mode, enabling FTP requires the admin account password.
5	If required, select the **Secure FTP** checkbox. The default setting is 'Disabled'.
6	Enter the IP address of the FTP Server in the **FTP Server** text box.
7	Enter the FTP port in the **FTP Port** text box. The default setting is 21.
8	Enter the FTP username in the **Username** text box.
9	Enter the FTP password in the **Password** text box.
10	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>'
11	Select the **Passive Mode** check box to enable Passive mode
12	Select **Apply** to save the settings.

- End -

Test FTP Settings

Test the FTP settings that have been configured correctly.

Procedure 66 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 will be 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 via the Common Internet File System protocol. This supplements existing distribution methods such as FTP, SFTP and email.

Procedure 67 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 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.
5	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>'
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.
9	Select **Apply** to save the settings.

- End -

Test CIFS Settings

Test the CIFS settings that have been configured correctly.

Procedure 68 Test the CIFS 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 **Test**. A sample text file will be sent to the specified CIFS destination to confirm that CIFS settings are correct.

- 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 69 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 **Record** check box to enable the Record Settings.
5	Select the **Email** check box to send an e-mail to the email address configured in the Configure SMTP Settings procedure.
6	Select the **FTP** check box to send a video file to the FTP details configured in the Configure FTP Server Settings procedure.
7	Select the **CIFS** check box to send a video file to the SFTP details configured in the Configure CIFS Server Settings procedure.
8	Select the **Output** check box to send out an output.

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 **Apply** to save your settings.

- End -

Editing a Event Action

Modify the details of an existing event action.

Procedure 70 Edit an Event Action

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Event Actions** from the Events and Actions menu.
3	Select an entry on the event actions list, you can edit the following: • **Name** • **Record** - Enable/Disable • **Email** - Enable/Disable • **FTP** - Enable/Disable • **CIFS** - Enable/Disable
4	Select **Apply** to save your settings.

- 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 71 Configure an Alarm

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

- End -

Procedure 72 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 73 Enable/Disable Alarm Output

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

2 Select **Alarm I/O** from the **Event and Actions** menu.

3 Select the **Output** check box to enable alarm output.

OR

Clear the **Output** check box to disable alarm output.

- End -

Procedure 74 Clearing Alarm Output

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Alarm I/O** from the **Event and Actions** menu.
3	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.

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 75 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 **Motion Detection** tab.
4	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.
5	Select the zone for detection in the **Motion zone** drop-down list.
6	Select the **Enable motion zone** check box to enable the zone for motion detection.
7	Select **Edit** in the **Region configuration** field.
8	Use the drawing tools on the Motion Detection Configuration Pane to draw the region of interest on the pane. Multiple selections can be made.
9	Select the sensitivity from the **Sensitivity** drop-down menu: • **Highest** • **High** • **Medium** • **Low** • **Lowest** The default setting is 'High'.
10	Adjust the size (% FOV) by entering a value between 1-100.
11	Adjust the hysteresis (measured in seconds) by entering a value between 0-3600.
12	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.

13 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 76 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 -

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 77 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 78 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 Log tab 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 -

Security

When you select the **Security** menu, the **Security Status** page appears, as seen in Figure 13 on page 61.

Figure 13 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

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 19.

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

Procedure 79 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 **Enhanced Security** check box to enable enhanced security. A prompt appears asking you for your current password and the new password for the Enchanced Security feature. Your password must adhere to the minimum requriments for an Enhanced Security password as seen below. OR Clear the **Enhanced Security** check box to disable enhanced security. Enhanced Security is disabled by default. The Security Warning dialog appears.
5	Enter the current password in the **Current Password** text box.

6	Enter the new password in the **New Password** text box.
	The password for enhanced security must meet the following requirements:
	• Be a minimum of eight characters long
	• Have at least one character from one of the following character groups:
	  • Upper-case letters
	  • Lower-case letters
	  • Numeric characters
	  • Special characters

7	Re-enter the new password in the **Confirm Password** text box.
8	Click **Apply**. **Note:**Any changes to the Security Mode are logged in the Security Log.

- End -

Procedure 80 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, and SNMP V3.

Procedure 81 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 82 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 83 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 93 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 84 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 85 Add a User

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Users** from the **Security** menu.
3	Select the **Add User** tab.
4	Enter a User Name in the **Name** text box. The username must start with a letter and can be followed by any alphanumeric values (a-z, A-Z, 0-9) and the following special characters, underscore(_), dash(-), or dot(.)
5	Select a **Role**: • admin • operator • user Refer to Appendix A: User Account Access for details on the features which are available to each role.

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

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

- End -

Changing the User Accounts Password

Change the password of an existing user account.

Procedure 86 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 87 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 88 Specify HTTP Method

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

- End -

Procedure 89 Add a HTTPS Certificate

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **HTTP/HTTPS** from the **Security** menu.
3	Click on the **Upload** button and navigate to the certificate location.
4	Select the file and select **Open**. **Note:**The camera only accepts .pem format certificates. The certificate must have the server certificate and private key combined and the private key must not be password protected. After the certificate has been uploaded the camera must be rebooted to take affect.

- End -

Delete a HTTPS Certificate

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

Procedure 90 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 91 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

A firewall may be enabled to perform address filtering to allow or deny specific IP and MAC addresses.

Procedure 92 Enable/Disable Firewall

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 93 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 94 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

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 95 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 96 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 -

UPnP Discovery

Enable or disable UPnP Discovery on the camera.

Procedure 97 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 -

Session Timeout

Session timeout specifies the number of minutes that a web session can remain idle before it is automatically terminated.

Procedure 98 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.

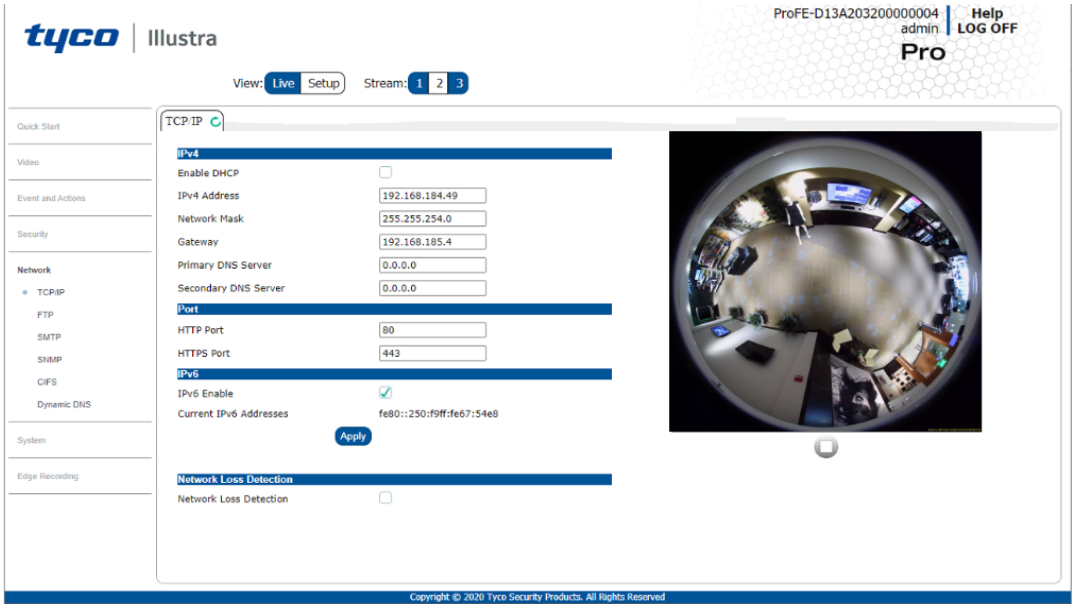
3 Use the slider bar to select the **Session Timeout (mins)**. The default setting is 15 minutes.

- End -

Network Menu

When you select the **Network** menu, the **TCP/IP** page displays, as seen in Figure 14 on page 73.

Figure 14 Network Menu



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

- TCP/IP
- FTP
- SMTP
- SNMP
- CIFS
- Dynamic DNS

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 73 for more information.

Procedure 99 Configure the IPv4 Settings

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

- End -

IPv6

Enable IPv6 on the camera.

Procedure 100 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 -

Network Loss Detection

Enable the camera to detect when there is a network loss from the Network menu.

Procedure 101 Enable / Disable Network Loss Detection

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 Network Loss Detection** check box to enable Network Loss Detection on the camera. OR Deselect the **Enable Network Loss Detection** check box to disable Network Loss Detection on the camera. The default setting is 'Enabled''.

- End -

FTP

Configure the FTP settings for the FTP server. This is required to send video files from triggered analytic alerts. FTP must be configured to enable FTP video alerts when using analytics.

Note:FTP settings can also be configured in the **Network** menu.

Procedure 102 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 FTP** check box to enable FTP. OR Deselect the **EnableFTP** 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>'

10 Select the **Passive Mode** check box to enable Passive mode

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

- End -

Test FTP Settings

Test the FTP settings that have been configured correctly.

Procedure 103 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 **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 104 Configure SMTP Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **SMPT** from the **Network** menu.
3	Check the **Enable Mail** check box to enable SMPT. Text boxes on the tab become available for entry. **Note:**When in Enhanced Security mode, enabling SMTP requires the admin account password.
4	Enter the IP Address of the mail server in the **Mail Server** text box.
5	Enter the server port in the **Server Port** text box. The default setting is ‘25’.
6	Enter the from email address in the **From Address** text box.
7	Enter the from email to send email alerts to in the **Send Email** text box.
8	Select the **Username** text box and enter a username.
9	Select the **Password** text box and enter a password.

10 Check the **SSL** check box to enable SSL.

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

- End -

Test SMTP Settings

Test the SMTP settings that have been configured correctly.

Procedure 105 Test the 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.
3	Select **Test**. A sample text file will be sent to the specified SMTP destination to confirm that SMTP settings are correct.

- 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 106 Configure SNMP Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **SNMP** from the **Network** menu.
3	Enter a location reference in the **Location** text box.
4	Enter an SNMP managing contact reference in the **Contact** text box.
5	If using **V2**: a Select the **Enable V2** checkbox. b Enter the authorized ID for reading SNMP data in the **Read Community** text box. c Enter the **Trap Community**. d Enter the **Trap Address**. e Select **Apply**. OR If using **V3**: a Select the **Enable V3** checkbox. b Enter the **Read User**.

c Select the **Authentication Type** using the radio buttons.

d Enter the Authentication Password

e Select the **EncryptionType** using the radio buttons.

f Enter the **Encryption** Password

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

- 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 107 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.
8	Select **Apply** to save the settings.

- End -

Test CIFS Settings

Test the CIFS settings that have been configured correctly.

Procedure 108 Test the CIFS 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 **Test**.

A sample text file will be sent to the specified CIFS destination to confirm that CIFS settings are correct.

- End -

Dynamic DNS

Dynamic DNS is supported for updating, in real time a changing IP address on the Internet to provide a persistent domain name for a resource that may change location on the network. RFC 2136 Dynamic Updates in the Domain Name System. In this situation the camera talks only to the DHCP server and the DHCP server is responsible for updating the DNS server. The camera sends its hostname to the DHCP server when requesting a new lease and the DHCP server updates the DNS records accordingly. This is suitable for an intranet style configuration where there is an internal DHCP and DNS service and the user wants only to access their camera within their own network.

By default, when making a DHCP request the camera transmits its hostname as part of the DHCP request. This option is not user configurable. The 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 109 Configure Dynamic DNS

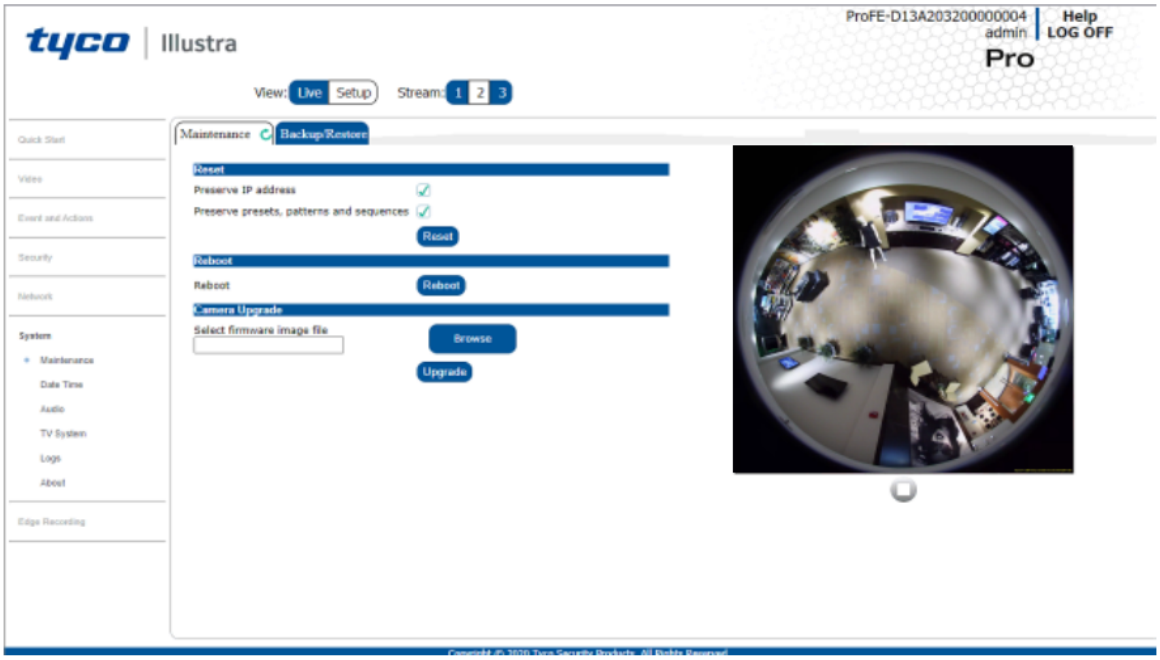
Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Dynamic DNS** from the **Network** menu.
3	Select the **Service Enable** check box to enable Dynamic DNS. OR Deselect **Service Enable** check box to disable Dynamic DNS. The default setting is ‘Disabled’.
4	If Service Enable has been enabled: a Enter the Camera Alias in the text box. b Select a Service Provider from the drop-down list: • **Dyndns.org (Dynamic)** • **Dynds.org (Custom)** • **No-IP** • **Change IP** c Enter a **Username** in the text box. d Enter a **Password** in the text box.
5	Select **Apply** to save the settings.

- End -

System

When you open the **System** menu, the **Maintenance** page appears, as seen in Figure 15 on page 80.

Figure 15 System Menu



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

- Maintenance
- Date Time
- Audio
- TV System
- 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 110 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 the **Preserve presets, patterns and sequences** check box to retain the current presets and sequences during the camera reset. OR Deselect the **Preserve presets, patterns and sequences** check box to remove existing presets and sequences. The default setting is 'Disabled'.
5	Select **Reset** You will be prompted to confirm the camera reset. • Select **OK** to confirm. The Web User Interface will display a "Camera Resetting" page with a progress bar showing the reboot progress. • When the camera is restarted it will take 2 - 3 minutes until it is online and ready to be accessed and controlled. OR Select **Cancel**. 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 111 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**.

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 112 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 113 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 114 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 115 Configuring the Date and Time

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Date Time** from the **System** menu.
3	Select the **Time 24-hour** check box to enable the 24-hour clock. Or Deselect the **Time 24-hour** check box to enable the 12-hour clock. The default setting is '24-hour'.
4	Select the **Date Display Format** from the drop-down menu: • **DD/MM/YYYY** • **MM/DD/YYYY** • **YYYY/MM/DD** The default setting is 'YYYY/MM/DD'.

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

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

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

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

The default setting is 'Manually'.

7 If you select Manually in step 5:

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

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

8 If you select via NTP in step 5:

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

9 Select **Apply** to save your changes.

- 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 116 Configure Audio Input

Step	Action

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

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

3 Select the **Input 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'.

4 Select one of the following values for Audio Codec:

- **G711A**
- **G711u**
- **G726**
- **AAC**
- **PCM**

5 Use the slider bar to select the **Input Volume**.

Values range from 1 to 100.

The default setting is 72.

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

- End -

Procedure 117 Configuring Audio Output

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Audio** from the Camera Configuration menu.
3	Select the **Audio Out** tab.
4	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'.
5	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.
6	Select **Apply** to save your changes.

- End -

TV System

You can choose between having the TV System operate through NTSC or PAL format depending on which format suits your location best. NTSC is used predominantly in America and Asia. PAL is used in most of Europe.

Note: Changes to TV System will affect both IP and Analogue stream if supported.

Procedure 118 Enable TV System

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **TV System** from the System menu.
3	Select the TV System you would like to use from the dropdown menu: • **NTSC** • **PAL**
4	Select **Apply** to save your settings.

- 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 119 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 120 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 121 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 122 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

Procedure 123 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 124 Edit Camera Name

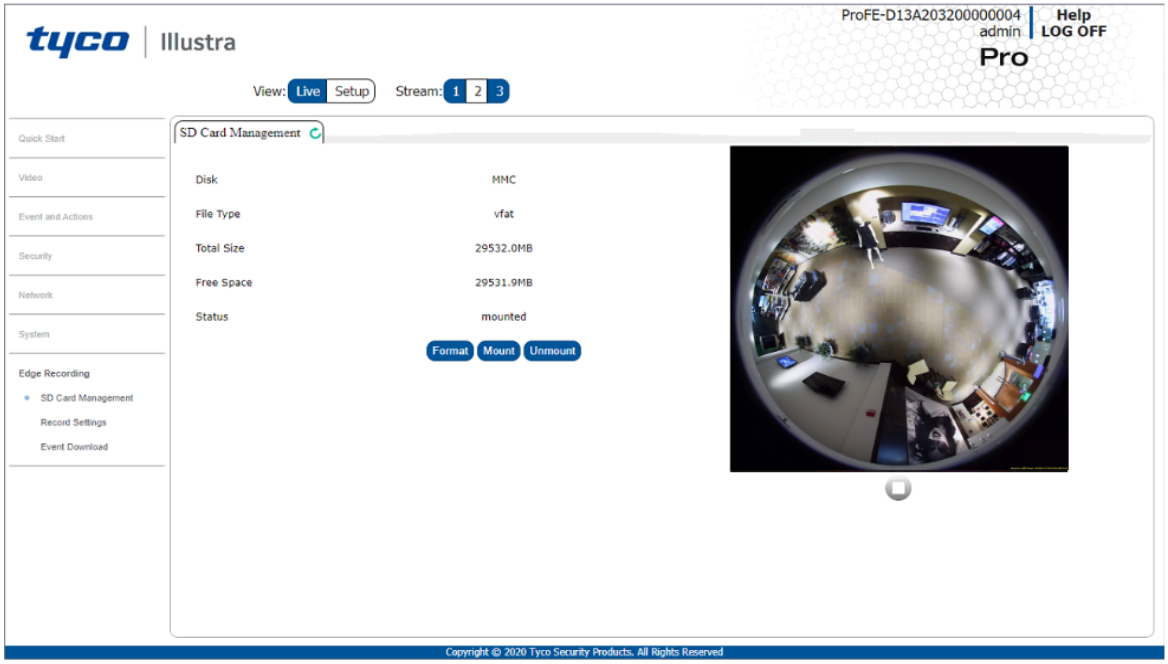
Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **About** from the **System** menu. The model tab displays.
3	Edit the name in the **Camera Name** textbox.

- End -

Edge Recording

When you select the **Edge Recording** menu, the **Micro SD Card Management** page appears, as seen in Figure 16 on page 89.

Figure 16 Edge Recording Menu



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

- SD Card Management
- Record Settings
- Event Download

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 125 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 126 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 127 Remove the Micro SD Card by powering down the Camera

Step	Action
1	Turn off the camera by disconnecting the power supply.
2	Remove the Micro SD card from the camera.

Note: AVI clips are not available on the camera until the Micro SD card has been inserted and the camera rebooted.

3 Reconnect the power supply and power up the camera.

- End -

Procedure 128 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 -

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 129 Configure Record Settings

Step	Action
1	Select **Setup** on the Web User Interface Banner to display the setup menus.
2	Select **Record Settings** from the **Edge Recording** menu.
3	Select **Enable Record** to allow the camera to create a playable video clip. OR Deselect **Enable Record** to disable the feature.
4	If **Enable Record** has been enabled: a Select the required video stream from the Video drop-down menu. Refer to Procedure 54 Configure the Video Stream Settings. b Select the Pre Event (secs) in seconds from the drop-down menu. Values range from 0 to 10. The default setting is 5 seconds. c Select the Post Event (secs) in seconds from the drop-down menu. Values range from 0 to 10. The default setting is 5 seconds.

5 Select **Apply** to save.

- End -

Event Download

If an event action has record mode enabled, when triggered, the associated video is logged in the event download table where it can later be downloaded from an Micro SD Card using the specified upload protocol.

Note: An event action must have record mode enabled to be logged and downloaded. This is configured in **Event Actions** under the **Events and Actions** menu.

Appendix A: User Account Access

Camera Menu	Sub Menu	Tab	Admin	Operator	User
Live View	Live View		X	X	X
Quick Start	Basic Configuration	TCP/IP	X		
		Video Stream Settings	X	X	
		Picture Basic	X	X	
		Picture Additional	X	X	
		Date / Time / OSD	X	X	
Video	Streams	Video Stream Settings	X	X	
	Picture Settings	Picture Basic	X	X	
		Picture Additional	X	X	
		Lens Calibration	X		
		Lens selection	X		
	Date/Time/OSD	Date Time	X	X	
		OSD	X	X	
	Privacy Zones	Privacy Zones	X	X	
Events and Actions	Event Settings	SMTP	X		
		FTP	X		
		CIFS	X		
	Event Actions	Event Actions	X		
	Alarm I/O	Alarm I/O	X		
	Analytics	ROI	X		
		Motion Detection	X		
		Blur Detection	X		
	Event Logs	Event Log	X		
		Fault Log	X		
Security	Security Status	Security Overview	X		
		Security Log	X		

Camera Menu	Sub Menu	Tab	Admin	Operator	User
	Users	User	X	X	
		Add User	X	X	
		Change Password	X	X	X
	HTTP/HTTPS	HTTP/HTTPS	X		
	IEEE 802.1x	EAP Settings	X		
	Firewall	Basic Filtering	X		
		Address Filtering	X		
	Remote Access	Remote Access	X		
	Session Timeout	Session Timeout	X		
Network	TCP/IP	TCP/IP	X		
	Multicast	Multicast	X		
	FTP	FTP	X		
	SMTP	SMTP	X		
	SNMP	SNMP	X		
	CIFS	CIFS	X		
	Dynamic DNS	Dynamic DNS	X		
System	Maintenance	Maintenance	X		
		Backup / Restore	X		
	Date Time	Date Time	X		
	Audio	Audio	X		
		Audio Clips	X	X	
	Analog Video	Analog Video	X	X	
	Health Monitor	Health Monitor	X		
		PTZ Summary	X		
	Logs	System Log	X		
		Boot Log	X		
		Audit Log	X		
	About	Model	X	X	X
Edge Recording	SD Card Management	SD Card Management	X		
	Record Settings	Record Settings	X		
		Offline Record	X		

Camera Menu	Sub Menu	Tab	Admin	Operator	User
		Settings			
	Event Download	Event Download	X		

Appendix B: 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 130 Viewing RTSP Stream through Media Player

Step	Action

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

1 Select **Media** then **Open Network Stream**.

2 Enter the IP address of the camera stream in the **Network URL** text box in the following format to view Stream 1 and 2:

- **Stream 1:** rtsp://cameraip:554/videoStreamId=1
- **Stream 2:** rtsp://cameraip:554/audioStreamId=1

For example: rtsp://192.168.1.168:554/videoStreamId=1

OR

rtsp://192.168.1.168:554/videoStreamId=1&audioStreamId=1

3 Select **Play**.The live video stream displays.

- End -

Appendix C: Stream Tables

Pro Gen 2 - 12MP Streaming Combinations

Table 17 Client dewarp stream table

		Resolution	Max FPS
		Client Dewarp	
Stream 1	H.265 H.264 H.265 Intellizip H.264 Intellizip	(2992x2992) (2048x2048) (1408x1408) (1072x1072) (960x960)	30 30 30 30 30
	MJPEG	1408x1408 1072x1072 960x960	30 30 30
Stream 2	H.265 H.264 H.265 Intellizip H.264 Intellizip	(1072x1072) (960x960) (720x720) (640x640) (480x480) (384x384)	30 30 30 30 30 30
	MJPEG	(1072x1072) (960x960) (720x720) (640x640) (480x480) (384x384)	30 30 30 30 30 30
Stream 3	MJPEG	(720x720) (640x640) (480x480) (384x384)	30 30 30 30

Table 18 Edge dewarp stream table with a Fisheye view on Stream 1

			Image Source Max FPS			
Stream 1			**Fisheye**	**Fisheye**	**Fisheye**	**Fisheye**
	Stream 2		Fisheye	Active Image	Panorama	QUAD CEILING Triple WALL
		Stream 3	Active Image	Active Image	Active Image	Active Image
2976x2976	960x960	480x360	15	15	N/A	15
2976x2976	960x720	480x360	15	15	15	15
2976x2976	960x544	480x360	15	15	15	15
2048x2048	2048x2048	480x360	27	27	N/A	25
2048x2048	2048x1536	480x360	27	27	27	27
2048x2048	1920x1080	480x360	27	30	27 - Ceiling 30 - Wall	
2048x2048	1600x1200	480x360	27	30		30 - Ceiling 27 - Wall
2048x2048	1408x1408	480x360	27	30	N/A	
2048x2048	960x960	480x360	27	30		
2048x2048	960x720	480x360	27	30	30 - Ceiling 27 - Wall	30
2048x2048	960x544	480x360	27	30		
2048x1536	2048x2048	480x360	27	27	N/A	25
2048x1536	2048x1536	480x360	27	27	27	27
2048x1536	1920x1080	480x360	27	30	27 - Ceiling 30 - Wall	
2048x1536	1600x1200	480x360	27	30		30 - Ceiling 27 - Wall
2048x1536	1408x1408	480x360	27	30	N/A	
2048x1536	960x960	480x360	27	30		
2048x1536	960x720	480x360	27	30	27 - Ceiling 30 - Wall	30
2048x1536	960x544	480x360	27	30		
1920x1080	2048x2048	480x360	27	27	N/A	25
1920x1080	2048x1536	480x360	27	27	27	27
1920x1080	1920x1080	480x360	27	30	27 - Ceiling 30 - Wall	30
1920x1080	1600x1200	480x360	27	30		
1920x1080	1408x1408	480x360	27	30	N/A	
1920x1080	960x960	480x360	27	30		
1920x1080	960x720	480x360	27	30	27 - Ceiling 30 - Wall	
1920x1080	960x544	480x360	27	30		

Table 19 Edge dewarp stream table with an Active Image on Stream 1

			Image Source Max FPS			
Stream 1			Active Image	Active Image	Active Image	Active Image
	Stream 2		Fisheye	Active Image	Panorama	QUAD CEILING Triple WALL
		Stream 3	Active Image	Active Image	Active Image	Active Image
2976x2976	960x960	480x360	15 - Ceiling N/A - Wall	15 - Ceiling N/A - Wall	N/A	15 - Ceiling N/A - Wall
2976x2976	960x720	480x360	15 - Ceiling N/A - Wall	15 - Ceiling N/A - Wall	15 - Ceiling N/A - Wall	15 - Ceiling N/A - Wall
2976x2976	960x544	480x360	15 - Ceiling N/A - Wall	15 - Ceiling N/A - Wall	15 - Ceiling N/A - Wall	15 - Ceiling N/A - Wall
2048x2048	2048x2048	480x360	27	27	N/A	25
2048x2048	2048x1536	480x360	27	27	27	27
2048x2048	1920x1080	480x360	27	30	27 - Ceiling 30 - Wall	
2048x2048	1600x1200	480x360	27	30		30 - Ceiling 27 - Wall
2048x2048	1408x1408	480x360	27	30	N/A	
2048x2048	960x960	480x360	27	30		
2048x2048	960x720	480x360	27	30	30 - Ceiling 27 - Wall	30
2048x2048	960x544	480x360	27	30		
2048x1536	2048x2048	480x360	27	27	N/A	27
2048x1536	2048x1536	480x360	27	27	27 - Ceiling 30 - Wall	
2048x1536	1920x1080	480x360	27	30		30
2048x1536	1600x1200	480x360	27	30		
2048x1536	1408x1408	480x360	27	30	N/A	
2048x1536	960x960	480x360	27	30		
2048x1536	960x720	480x360	27	30	27 - Ceiling 30 - Wall	
2048x1536	960x544	480x360	27	30		
1920x1080	2048x2048	480x360	30	27	N/A	27
1920x1080	2048x1536	480x360	30	27	30	30

			Image Source Max FPS			
Stream 1			Active Image	Active Image	Active Image	Active Image
1920x1080	1920x1080	480x360	30	30	30	30
1920x1080	1600x1200	480x360	30	30		
1920x1080	1408x1408	480x360	30	30	N/A	
1920x1080	960x960	480x360	30	30		
1920x1080	960x720	480x360	30	30	30	
1920x1080	960x544	480x360	30	30		

Table 20 Edge dewarp stream table with Panorama View on Stream 1

			Image Source Max FPS			
Stream 1			Panorama	Panorama	Panorama	Panorama
	Stream 2		Fisheye	Active Image	Panorama	QUAD CEILING Triple WALL
		Stream 3	Active Image	Active Image	Active Image	Active Image
2976x2976	960x960	480x360	N/A	N/A	N/A	N/A
2976x2976	960x720	480x360	N/A	N/A	N/A	N/A
2976x2976	960x544	480x360	N/A	N/A	N/A	N/A
2048x2048	2048x2048	480x360	N/A	N/A	N/A	N/A
2048x2048	2048x1536	480x360	N/A	N/A	N/A	N/A
2048x2048	1920x1080	480x360	N/A	N/A	N/A	N/A
2048x2048	1600x1200	480x360	N/A	N/A	N/A	N/A
2048x2048	1408x1408	480x360	N/A	N/A	N/A	N/A
2048x2048	960x960	480x360	N/A	N/A	N/A	N/A
2048x2048	960x720	480x360	N/A	N/A	N/A	N/A
2048x2048	960x544	480x360	N/A	N/A	N/A	N/A
2048x1536	2048x2048	480x360	27	27	N/A	27 - Ceiling 27 - Wall
2048x1536	2048x1536	480x360	27	27 - Ceiling 27 - Wall	25 - Ceiling 30 - Wall	27
2048x1536	1920x1080	480x360	27	30	27 - Ceiling 27 - Wall	27 - Ceiling 27 - Wall
2048x1536	1600x1200	480x360	27		25 - Ceiling 30 - Wall	30
2048x1536	1408x1408	480x360	27		N/A	
2048x1536	960x960	480x360	27			
2048x1536	960x720	480x360	27		25- Ceiling 30 - Wall	
2048x1536	960x544	480x360	27		27 - Ceiling 30 - Wall	
1920x1080	2048x2048	480x360	27 Ceiling 30- Wall	27 Ceiling 30- Wall	N/A	27
1920x1080	2048x1536	480x360	27 Ceiling 30- Wall		27 - Ceiling 30 - Wall	27 - Ceiling 30 - Wall

			Image Source Max FPS			
Stream 1			**Panorama**	**Panorama**	**Panorama**	**Panorama**
1920x1080	1920x1080	480x360	27 Ceiling 30- Wall	30	27 - Ceiling 30 - Wall	30
1920x1080	1600x1200	480x360	27 Ceiling 30- Wall	30		
1920x1080	1408x1408	480x360	27 Ceiling 30- Wall	30	N/A	
1920x1080	960x960	480x360	27 Ceiling 30- Wall	30		
1920x1080	960x720	480x360	27 Ceiling 30- Wall	30	27 - Ceiling 30 - Wall	
1920x1080	960x544	480x360	27 Ceiling 30- Wall	30		

Table 21 Edge dewarp stream table with Quad View Ceiling / Triple View Wall on Stream 1

			Image Source Max FPS			
Stream 1			QUAD CEILING Triple WALL	QUAD CEILING Triple WALL	QUAD CEILING Triple WALL	QUAD CEILING Triple WALL
	Stream 2		Fisheye	Active Image	Panorama	Active Image
		Stream 3	Active Image	Active Image	Active Image	Active Image
2976x2976	960x960	480x360	15	15	N/A	15
2976x2976	960x720	480x360	15	15	15	15
2976x2976	960x544	480x360	15	15	15	15
2048x2048	2048x2048	480x360	25	25	N/A	25
2048x2048	2048x1536	480x360	25	27	25 - Ceiling 27 - Wall	27
2048x2048	1920x1080	480x360	25	27	27	
2048x2048	1600x1200	480x360	25	30	25 - Ceiling 27 - Wall	
2048x2048	1408x1408	480x360	25	30	N/A	
2048x2048	960x960	480x360	25	30		30 - Ceiling 27 - Wall
2048x2048	960x720	480x360	25	30	25 - Ceiling 27 - Wall	
2048x2048	960x544	480x360	25	30	27	30
2048x1536	2048x2048	480x360	27	27	N/A	27
2048x1536	2048x1536	480x360	27		27	
2048x1536	1920x1080	480x360	27	30	27 - Ceiling 30 - Wall	30 - Ceiling 27 - Wall
2048x1536	1600x1200	480x360	27	30		
2048x1536	1408x1408	480x360	27	30	N/A	
2048x1536	960x960	480x360	27	30		30
2048x1536	960x720	480x360	27	30	27 - Ceiling 30 - Wall	
2048x1536	960x544	480x360	27	30		
1920x1080	2048x2048	480x360	27	27	N/A	27
1920x1080	2048x1536	480x360	27	30	27 - Ceiling 30 - Wall	27 - Ceiling 30 - Wall

			Image Source Max FPS			
Stream 1			**QUAD CEILING Triple WALL**	**QUAD CEILING Triple WALL**	**QUAD CEILING Triple WALL**	**QUAD CEILING Triple WALL**
1920x1080	1920x1080	480x360	30	30	30	30
1920x1080	1600x1200	480x360	30	30	27 - Ceiling 30 - Wall	
1920x1080	1408x1408	480x360	30	30	N/A	
1920x1080	960x960	480x360	30	30		
1920x1080	960x720	480x360	30	30	30	
1920x1080	960x544	480x360	30	30		

Appendix D:Technical Specifications

The table below lists technical specifications of the Pro Gen 2 12MP Fisheye camera.

Operational		
Video Compression	H265, H264+, H265+	
Max Frame Rate	30fps @ 12MP, 27fps @ 1080p	
Resolution & Aspect Ratio	Edge Dewarp (2688x1512) 16:9 (1920x1080) 1080p 16:9 (1664x936) 16:9 (1280x720) 720p 16:9 (1024x576) PAL 16:9 (960x544) 16:9 (640x360) nHD 16:9 (480x360) 480 4:3 (384x288) 4:3 (384x216) 16:9	Client Dewarp (2992x2992) 1:1 (2048x2048) 1:1 (1408x1408) 1:1 (1072x1072) 1:1 (960x960) 1:1 (720x720) 1:1 (640x640) 1:1 (480x480) 1:1 (384x384) 1:1
Video Streams	Client: Triple Edge: Depends on Image sources selection	
Imager	Progress Scan RGB CMOS 1/1.7”	
Lens Type	Glass Aspherical	
Focal Length	1.65 mm	
Field of View	180°	
Aperture	F2.8	
Minimum Illumination Color B/W	0.6 Lux @ 1/15s 0.2 Lux @ 1/4s 0.003 Lux @ 1/4s	
IR Illumination	Yes	
IR Distance	15m	
Wide Dynamic Range	DIgital WDR	
Day/Night	Mechanical ICR	
ONVIF-Compliant	Profile S, G, Q	
Motion Detection	Yes	
Privacy Zones	5	
Alarm Input/Output	1/1	

Audio	1/1
Simultaneous Users	3
Supported Languages	Arabic, Czech, Chinese (Simplified), Chinese (Traditional), Danish, Dutch, English (US), French, German, Italian, Japanese, Korean, Polish, Portuguese (Brazilian), Russian, Spanish, Turkish
Network	
Ethernet Interface	10/100/1Gbps Ethernet, RJ-45
Supported Protocols	IPv4/v6, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, ICMP, FTP, SMTP, DHCP, CIFS, PPPoE, UPnP, IGMP, SNMP, QoS, ONVIF, ARP
Configuration Management	
Web Browsers	IE10 or higher
Security	Enhanced Security Mode (forces complex passwords, HTTPS and disables discovery); TLS 1.2 (256 bit cipher minimum); Security Overview Page (status and configuration); RTSP Authentication; IEEE 802.1X Client; Remote Accessible Audit logs; Role-Based Access Control
Onboard Storage	
Card Support	microSDXC 64GB
Pre-Alarm Recording	10 sec
Recording Format	AVI
Recording Trigger	Video Motion, Alarm Input, Network Failure Detection
Electrical	
Power Input	DC 12V, Power over Ethernet (PoE) IEEE 802.3af/802.3at Type 1 Class 3
Power Draw	7.1W PoE, 8.1W DC12V
Physical	
Dimensions (RxH)	Ø5.8 x 2.2 in (Ø148x 55 mm)
Weight	0.73 lb (330 g)
Housing Color	RAL 9003 - Signal White
Operating Temperature	-22°F - 122°F (-30°C - 50°C)
Humidity	Up to 95% RH Non-Condensing
Vandal Resist-	IK10

ant	
Outdoor Rating	IP66
Regulatory	
Safety	UL 62368-1; CAN/CSA-C22.2 No. 62368-1; EN 62368-1; IEC 62368-1
Emissions	FCC Part 15 Class A; CE EN55032 Class A; AS/NZS CISPR 32 Class A; ICES-003 Class A
Immunity	EN50130-4
Environment	RoHS; WEEE

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 Sensormatic 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 LCICENSING MAY BE OBTAINED FROM MPEG LA, LLA. SEE 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

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 Sensormatic 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 LCICENSING MAY BE OBTAINED FROM MPEG LA, LLA. SEE 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

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 Sensormatic 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 MEPG-4 VISUAL STANTARD (“MPEG-4 VIDEO”) AND/OR (II) DECODING MEPG-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 MEPG LA TO PROVIDE MPEG-4 VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHE RUSE. ADDITOINAL INFORMATION INCLUDING THAT RELATING TO PROMOTIONAL, INTERNAL AND COMMERCIAL USES AND LCICENSING MAY BE OBTAINED FROM MPEG LA, LLA. SEE 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.