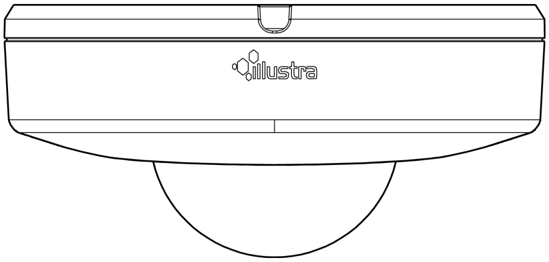
From Tyco Security Products

Illustra Pro Series

Installation and Configuration Guide



Notice

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

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

Copyright

Tyco Security Products

6600 Congress Avenue

Boca Raton, FL 33487 U.S.A.

Customer Service

Thank you for using American Dynamics products. We support our products through an extensive worldwide network of dealers. The dealer through whom you originally purchased this product is your point of contact if you need service or support. Our dealers are empowered to provide the very best in customer service and support. Dealers should contact American Dynamics at (800) 507-6268 or (561) 912-6259 or on the web at www.americandynamics.net.

Trademarks

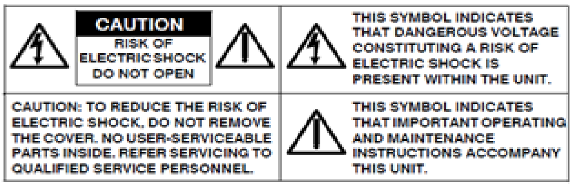
The trademarks, logos, and service marks displayed on this document are registered in the United States [or other countries]. Any misuse of the trademarks is strictly prohibited and Tyco Security Products will aggressively enforce its intellectual property rights to the fullest extent of the law, including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

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

Table of Contents

Warning

- This unit operates at PoE+.
- 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 avoid damage to the unit, never connect more than one type of power supply (PoE IEEE802.3 Ethernet Class 0) at the same time. If using PoE, this camera is to be connecting only to PoE networks without routing to heterogeneous devices.
- The camera is not intended to be directly connected to an external network and the video coax connections should only be connected intra-building.
- 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.
- Avoid aligning the lens to very bright objects (for example, light fixtures) for long periods of time.
- ITE is to be connected only to PoE networks without routing to the outside plant.
- The power supply shall be approved for ITE NEC Class 2 or LPS, 550mA minimum and 50 degrees Celsius.
- Video Out connection should be intra-building only.
- Avoid operating or storing the unit in the following locations:
    - Extremely humid, dusty, or hot/cold environments. Recommended operating temperature is:
        - Compact Mini Dome: -40˚C to 50˚C (-40˚F to 122˚F)
    - Power over Ethernet (PoE) does not support heater.
    - Near sources of powerful radio or TV transmitters.
    - Near fluorescent lamps or objects with reflections.
    - Under unstable or flickering light sources.



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

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

Overview

This Illustra Pro Installation and Configuration Guide is a user manual which provides physical properties, installation, and configuration information of the cameras in Table 1 on Page 6.

Table 1 Product codes

Product Code	Description
IPS02CFOCWST	Illustra Pro 2MP Compact Dome, 2.8mm, vandal, clear, white, SDN, TWDR
IPS03CFOCWST	Illustra Pro 3MP Compact Dome, 2.8mm, vandal, clear, white, SDN, TWDR

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

- For the Illustra Pro 2MP and 3MP Compact Mini Dome cameras, refer to Illustra Pro 2MP and 3MP Compact Cameras on page 7.

The second portion of this guide contains information regarding the Illustra User Web Interface and the web configuration of the aforementioned cameras. Refer to Configuration on page 23 for procedural information pertaining to camera configuration.

Illustra Pro 2MP and 3MP Compact Cameras

This chapter provides product features, installation procedures, and connection information regarding the Illustra Pro 2MP and 3MP Compact 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 llustra Pro 2MP and 3MP Compact cameras. Product code and description of the camera is provided in Table 2 on page 7.

Table 2 Product code and description of the Compact camera

Product Code	Description
IPS02CFOCWST	Illustra Pro 2MP Compact Dome, 2.8mm, vandal, clear, white, SDN, TWDR
IPS03CFOCWST	Illustra Pro 3MP Compact Dome, 2.8mm, vandal, clear, white, SDN, TWDR

Figure 3 Physical dimensions of the Compact cameras (mm)

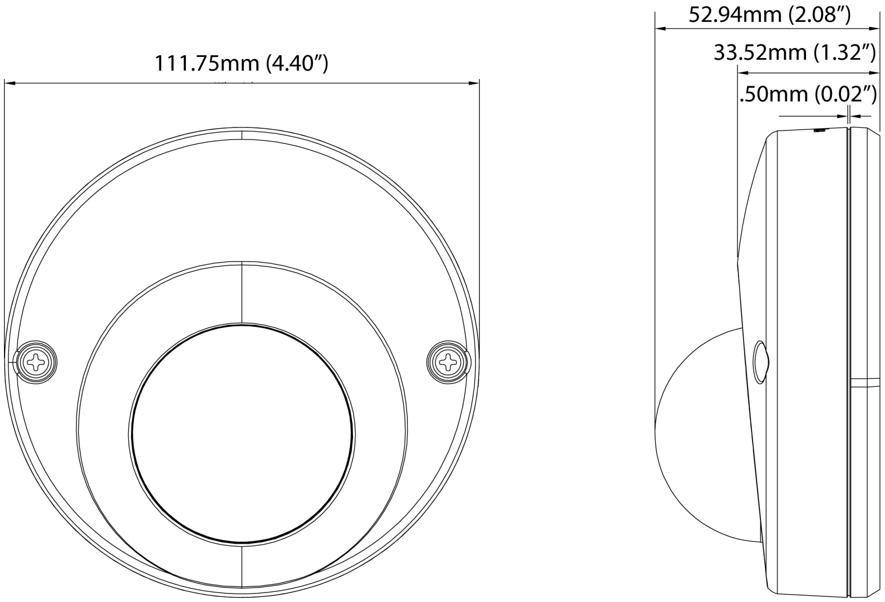


Figure 4 Physical dimensions of the Compact cameras (mm)

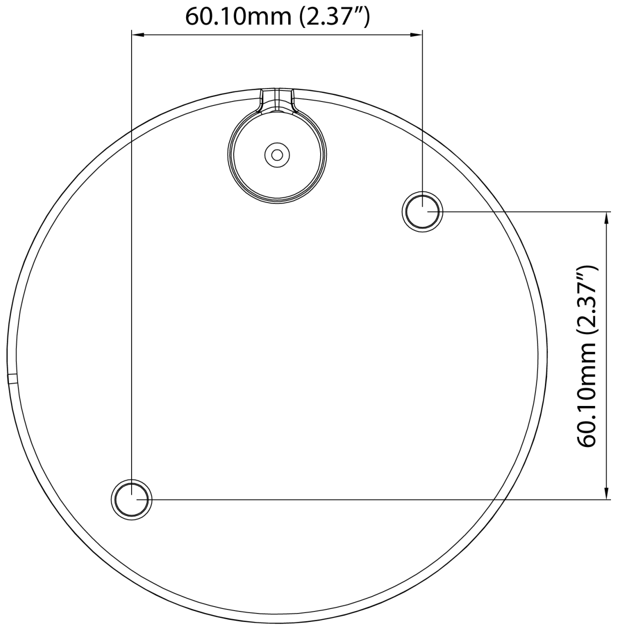


Figure 5 Pictorial index of the Compact cameras

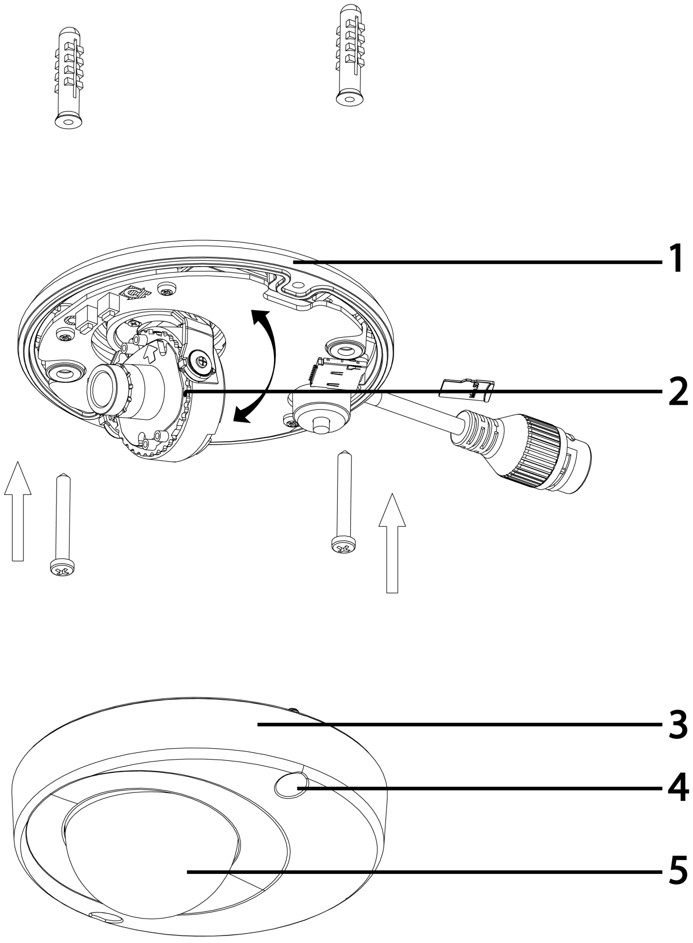


Table 6 Pictorial index descriptions

Index number	Description
1	Camera base
2	Lens Unit
3	Camera top case
4	Screw casing (Loosen the screws to take off the top cover)
5	Dome cover

Figure 7 Interior view and buttons of the unit

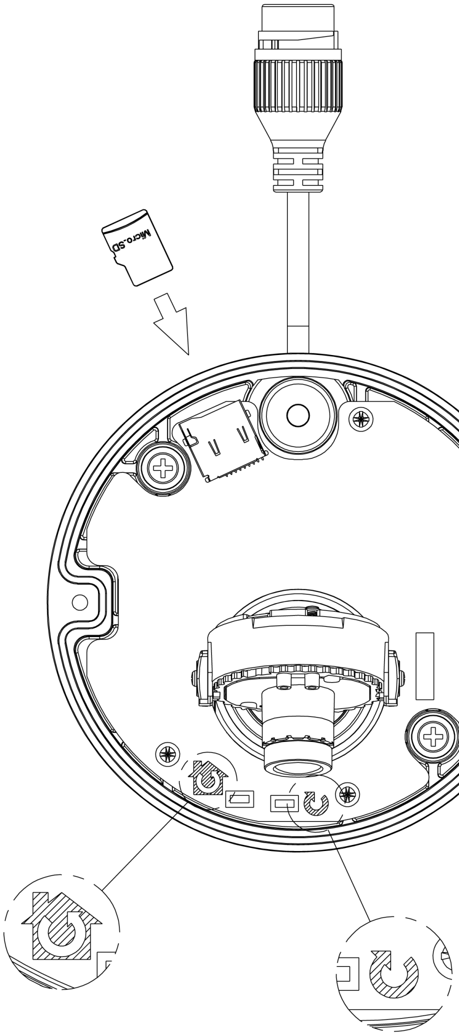


Table 8 Interior button descriptions

Interior button	Description
⌂	Resets to factory default by pressing and holding the button for five seconds.
↻	Reboots the unit.

Note: The connector cable of the Compact camera should be contained in a conduit suitable for outdoor use.

Note: Connectors and field wiring terminals for external Class 2 circuits provided with marking indicating minimum Class of wiring to be used. Class 2 shall be marked adjacent to the field wiring terminals.

Installation

In the box

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

- 2 Plastic Anchors and screws 35mm
- 1 T20 Security Torx Wrench
- 1 Installation template sticker
- 1 printed Quick Start Guide
- 1 printed Regulatory document
- 1 Desiccant bag

Contact your dealer if any item is missing.

Installation tools

The following tools assist with installation:

- a drill
- screwdrivers
- wire cutters

Checking appearance

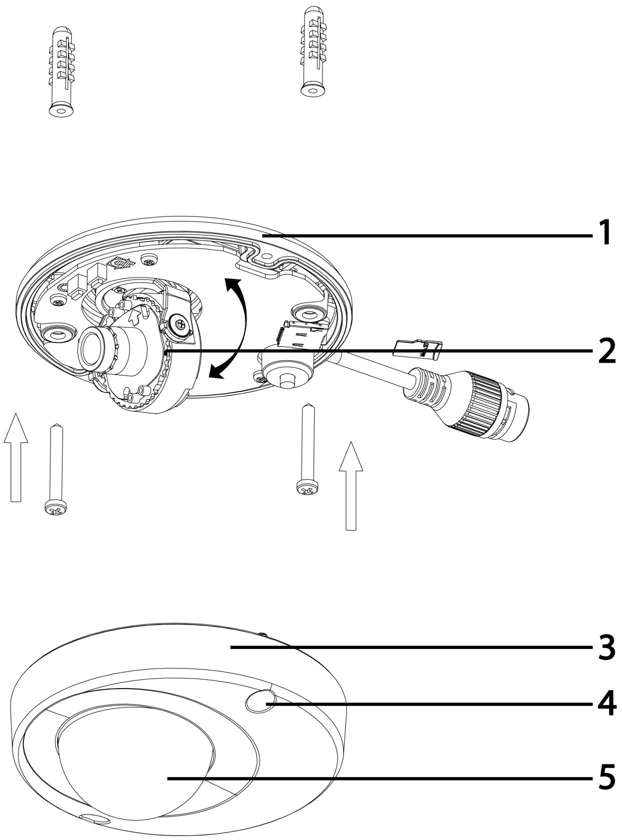
When first unboxing, check whether if there is any visible damage to the appearance of the unit and its accessories. The protective materials used for the packaging should be able to protect the unit from most types of accidents during transportation. Remove the protective part of the unit when every item is checked in accordance with the list in In the box on page 10.

Procedure 1 Disassembling the Camera

Step	Action
1	Remove the bungs from the camera base and remove the screws from the top of the camera with a safety screwdriver (4).
2	Gently remove the top cover (3).
3	Set the top cover aside.

Note: Unscrew the top cover safety wire to fully remove the top cover.

Figure 9 Disassembling the Compact camera



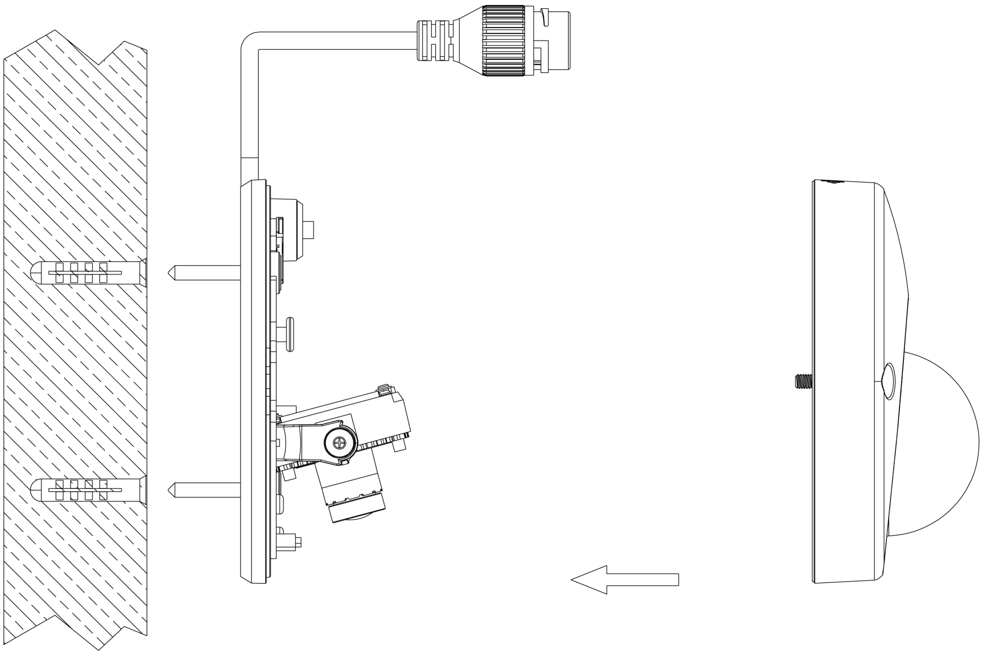
- End -

Procedure 2 Mounting the camera

Step	Action
1	Use the mounting template to mark holes that correspond to the camera base on the mounting surface.
2	Drill holes.
3	Fasten the anchors to the mounting surface with screws.
4	Secure the unit bottom case to the wall or ceiling with tapping screws.
5	Adjust the viewing angle.

6 Ensure that the top cover safety wire is connected and securely fit the top cover.

Figure 10 Mounting the camera



WARNING	Depending on the material of your mounting surface, you may require different screws and anchors than those as supplied. To prevent the unit from falling off, ensure that it is secured to a firm place (ceiling slab or channel) with the safety wire (supplied) strong enough to sustain the total weight of the unit. Pay also attention to the finishing at the end of the wire. Never turn the lens more than 360°, which should disconnect or break internal cables.

CAUTION	Ensure that the Safety wire is connected with one end to the ceiling and the other to the safety-cord screw of the unit.

- End -

Procedure 3 Adjusting the Position

The unit has three axes for positioning, refer to Figure 11 on page 13. While monitoring, adjust the position as below.

Step	Action
1	Pan Adjustment (A) For Wall Mount and Tilted Ceilings: a Rotate the lens base (maximum 140°) until you are satisfied with the field of view.
2	Horizontal Rotation (B): a Rotate 3D assembly in the base. Do not turn assembly more than 354° as this assembly may cause the internal cables to twist and disconnect or break.
3	Tilt Adjustment (C): a Tilt the lens base (maximum 125° from the frontal mounting surface) until you are satisfied with the field of view.

CAUTION	Limitation of three axis positions of lens centroid: • Pan range: 140° • Tilt range: 15° to 125° from frontal mounting surface • Rotate (z-axis): 354°

Figure 11 Adjusting the position of the camera

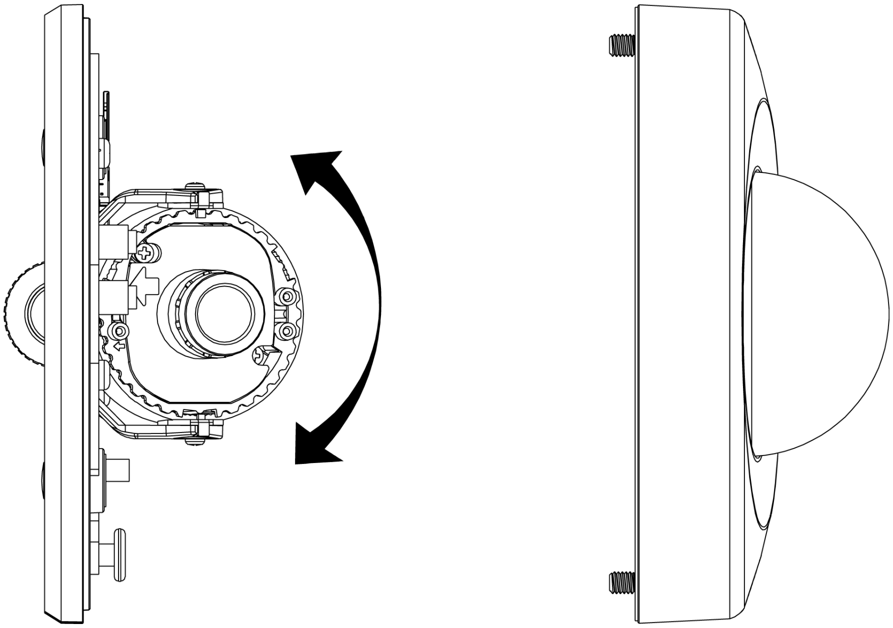
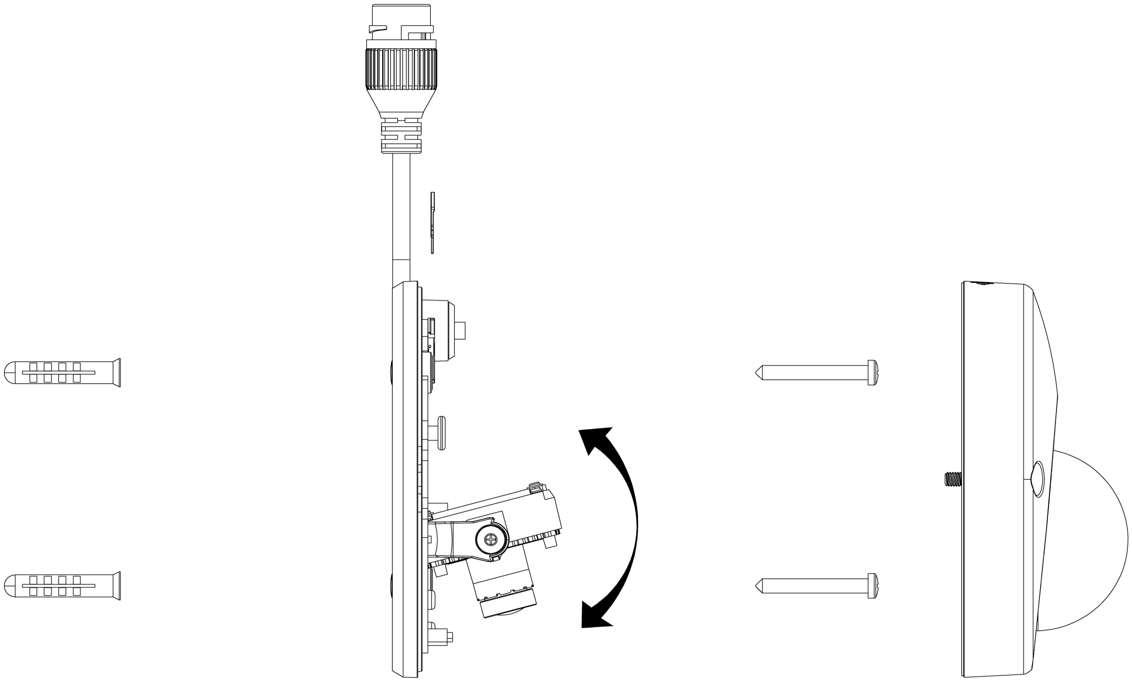


Figure 12 Adjusting the position of the camera



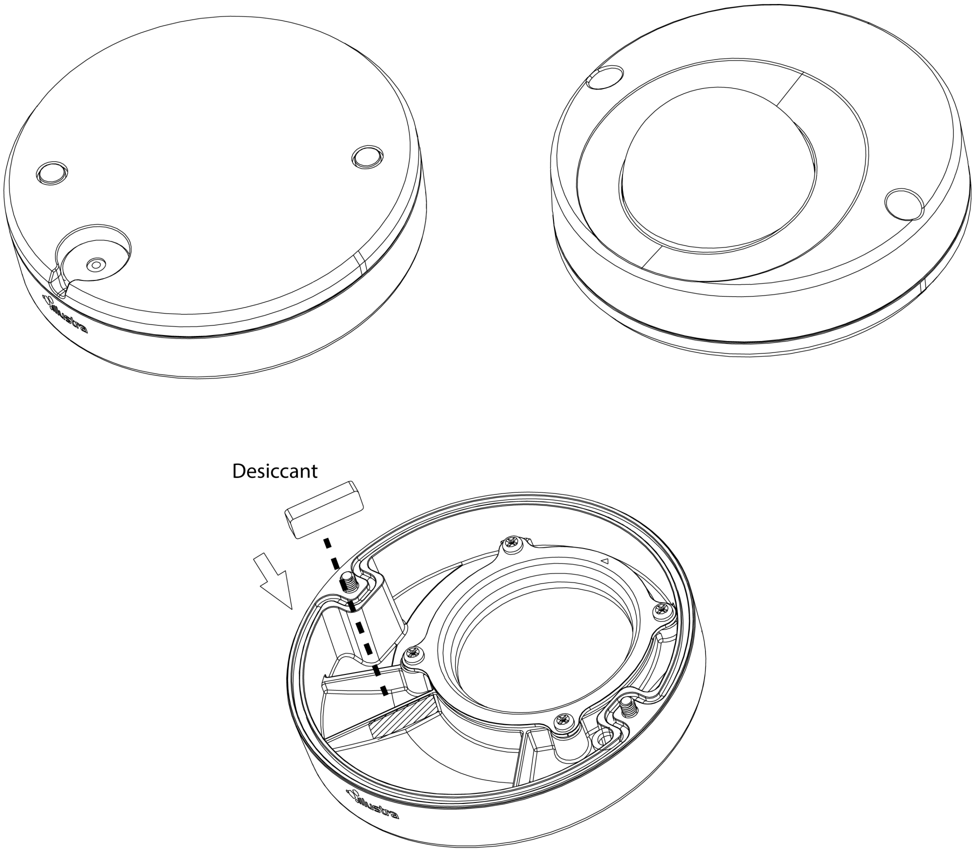
NOTE	For Compact camera series: The zoom level and focus are manually set in the factory.

- End -

Procedure 4 Installing the desiccant

Step	Action
1	Remove the papers from the back of the desiccant.
2	Attach to the interior side of the camera cover as seen in the image below.

Figure 13 Location for desiccant application



- End -

Procedure 5 Locking the Camera

Step	Action
1	Use a soft, lint-free cloth to wipe the dome cover and remove fingerprints.
2	Ensure that the top cover safety wire is connected and attach the inner liner and top cover.

- End -

Procedure 6 Powering up the camera

Connect the power cable to the power plugs as followings:

- PoE: Connect the RJ-45 jack to a PoE compatible network device that supplies power through the Ethernet cable.

Note: The PoE connection should be provided by a UL Listed product and the connections shall be made in accordance with Article 800 of the NEC or local regulations.

- End -

System requirements

The table below lists the minimum requirement to implement and operate the following Illustra Pro camera: Compact Mini Dome.

Table 14 System Requirements

System	
Browser	Microsoft Internet Explorer 9 or above, Firefox, Safari, Chrome
Unit	
Power Supply	PoE
Networking	
Wired	10/100BASE-T Ethernet (RJ-45 connector) **NOTE**: A switch is required for surveillance on multiple units.
Compact Mini Dome System hardware	
CPU	Intel Pentium 4 2.4GHz or equivalent
RAM	1 GB or above
Display	NVIDIA GeForce 6 Series or ATI Mobility Radeon 9500

NOTE	All the installation and operations should comply with your local electricity safety rules.

CAUTION	To avoid damage to the unit, never connect more than one type of power supply (PoE IEEE802.3 Ethernet Class 2) at the same time. If using PoE, this camera is to be connecting only to PoE networks without routing to heterogeneous devices.

Network Topology

The Compact Mini Dome camera delivers video images in real-time using the Internet and Intranet. It is equipped with an Ethernet RJ-45 network interface.

The following images illustrate the network topologies of the cameras.

Figure 15 Compact Mini Dome Cameras Network Topology Type I

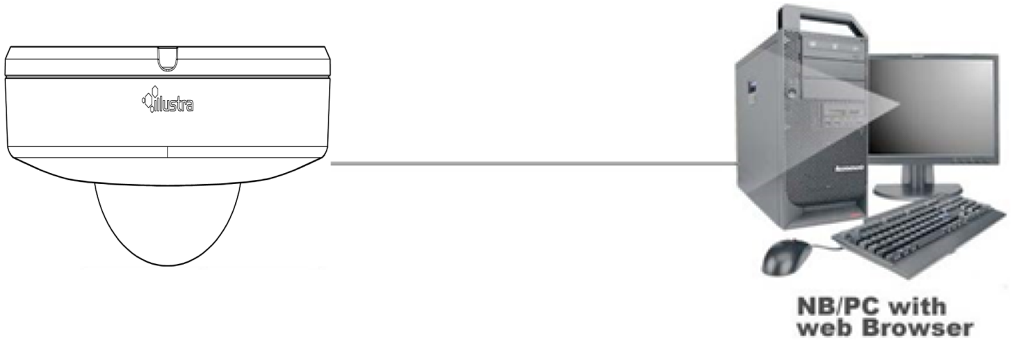
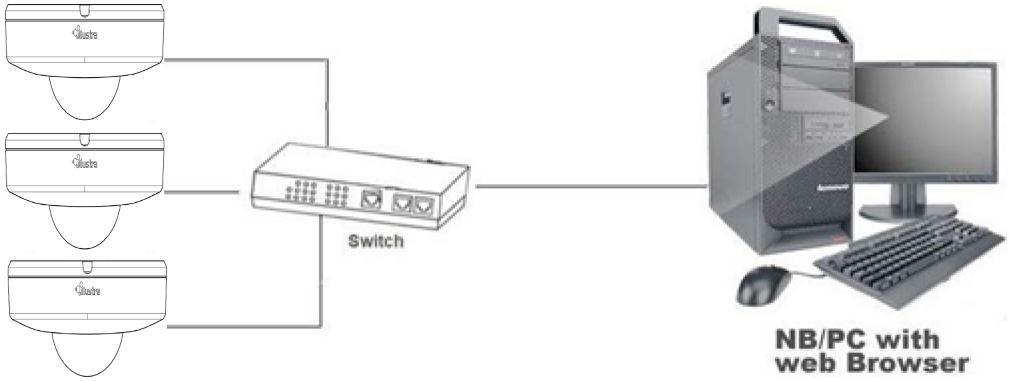


Figure 16 Compact Mini Dome Cameras Network Topology Type II



Network Connection

Default IP Address

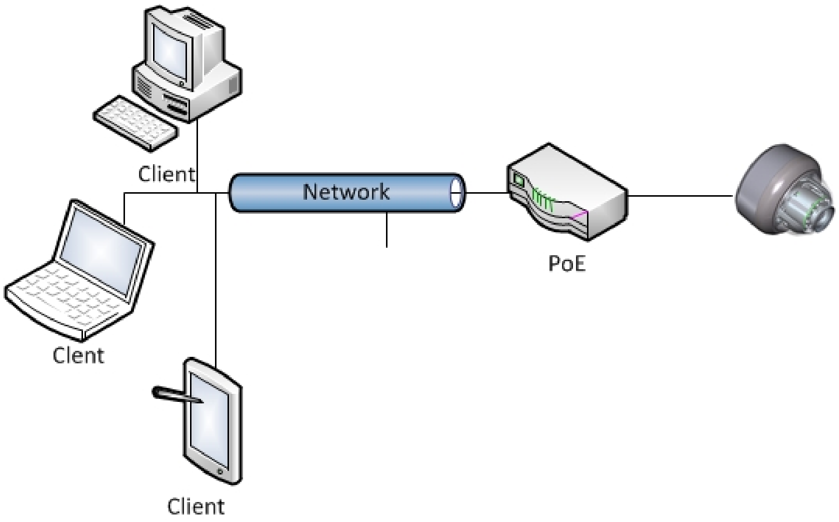
Since this is a network-based unit, an IP address must be assigned at the very first bootup. The default IP address of the unit is 192.168.1.168 and sub mask is 255.255.255.0.

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

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

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

Figure 17 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 7 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 8 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 9 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 23 for further information regarding using the Illustra Connect tool for configuring the cameras.

Procedure 10 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 11 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 12 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.

Step	Action
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 13 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 -

Procedure 14 Selecting Corridor Mode

This provides a better perspective when viewing a long corridor.

Step	Action
1	Select **Setup** on the GUI banner to display the setup menus.
2	Select the **Picture Basic** tab from the **Basic Configuration** menu.
3	Select **Play** to start the video stream if it is not already active.
4	Select the required **Corridor Mode** setting: • None • -90° • +90°
5	The video pane updates to display the new settings.

- End -

Configuration

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

Security Mode Profiles for First Time Connection

The Illustra Pro 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 24 for further information regarding the differences between Standard and Enhanced Security modes.

Accessing the Illustra Pro Series Camera Web User Interface

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

Procedure 15 Logging in to the Camera

Step	Action
1	Refer to Network Connection on page 18 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.If you are keeping Standard Security, it is best practice to use the Change Password check box to immediately change the default password to one unique to your surveillance system.
6	Optional - If you select the Enhanced Security option, you are required and instructed to create a complex password.

Note: The password 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

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:

- Changes to communication protocols are available to all users with appropriate privileges.
- Passwords complexity is set to require minimum of any 5 characters.
- 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.
- Passwords for all accounts will meet the following password complexity requirements:
  - Minimum characters: 8
  - The password must have at least one character from a minimum of three of the following character groups:

    a Upper case letters

    b Lower case letters

    c Numeric characters

    d Special characters

    e Changing protocols require an administrator to re-enter their password
- Authentication method is set to Digest by default.

Changing the Camera Web User Interface Language

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

Procedure 16 Change the Camera Web User Interface Language

Step	Action
1	Open the camera sign in page. If you are already logged in to the Web User Interface, select Log Off to display the sign in page.
2	Select your preferred language from the drop-down menu:

- English
- Arabic
- Czech
- Danish
- German
- Spanish
- French
- Hungarian
- Italian
- Japanese
- Korean
- Dutch
- Polish
- Portuguese
- Swedish
- Turkish
- Chinese Simplified
- Chinese Traditional
- Russian

The default language is English.

3 Enter the Username.

4 Enter the Password.

5 Select Log in.

The camera web User Interface displays in the selected language.

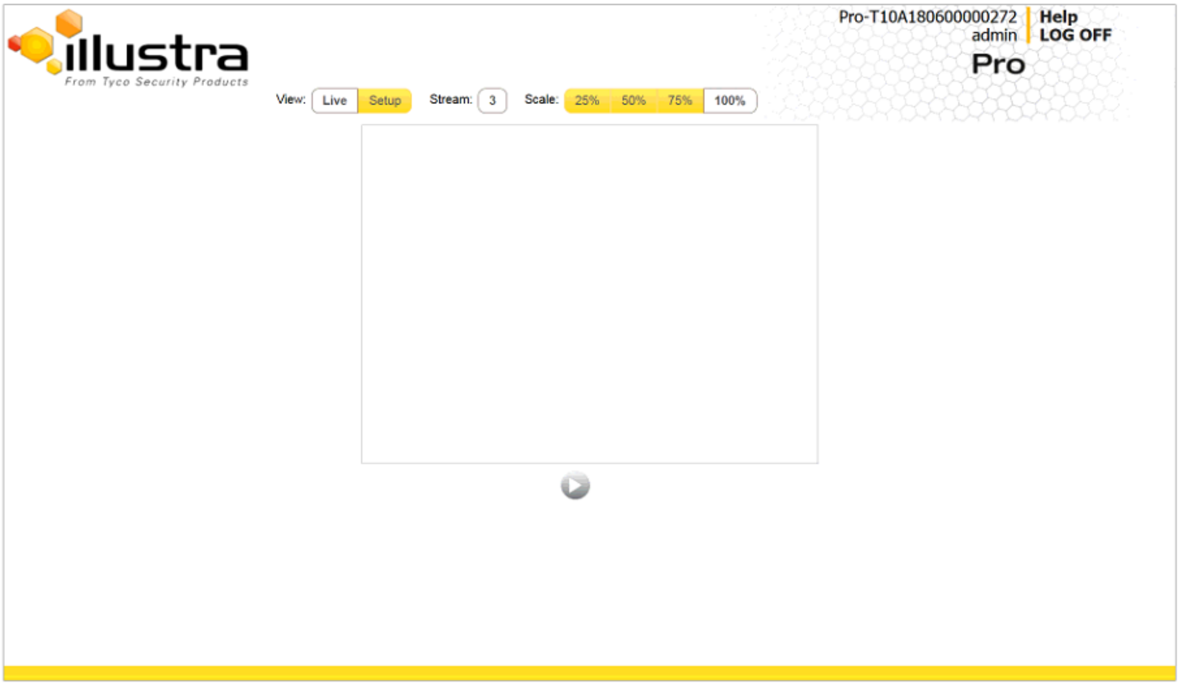
- End -

Live menu

When you log in to the Illustra Web User Interface, the **Live** menu appears, as seen in Figure 18 on page 26.

When an admin user logs in for the first time the **Live** menu page displays, but after this each time you log in the **Stream** page on the **Video** menu displays.

Figure 18 Live menu page



Displaying the Live View Page

Display the live camera view page.

Procedure 17 Display Live View Page

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

- End -

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 98 for details on the features which are available to each role.

Procedure 18 Access Setup Menus from Live View

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

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

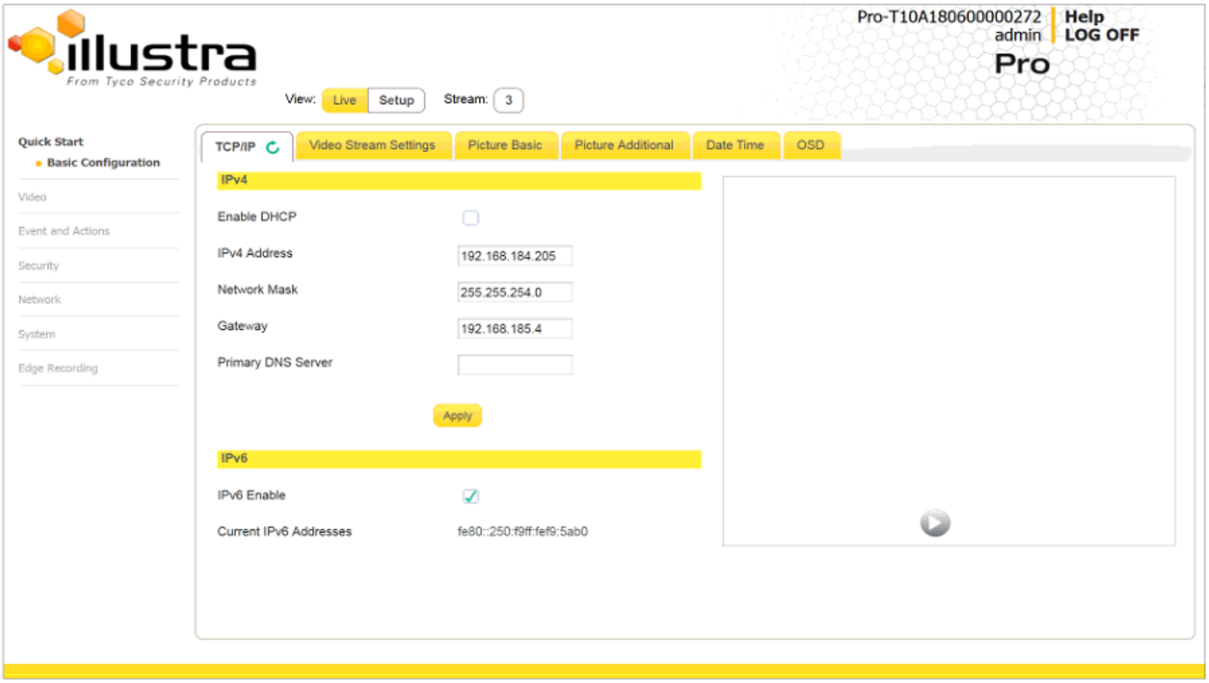
- End -

Quick Start Menu

When you select the Quick Start menu, the Basic Configuration Page displays, as shown in Figure 19 on page 28.

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 19 Basic Configuration Menu



IPv4

Enable DHCP □

IPv4 Address 192.168.184.205

Network Mask 255.255.254.0

Gateway 192.168.185.4

Primary DNS Server

IPv6

IPv6 Enable ☑

Current IPv6 Addresses fe80::250:f9ff:fef9:5ab0

Basic Configuration

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

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

TCP/IP

Configure the IPv4 and IPv6 network settings on the camera.

Note: When you perform a factory reset or reboot the unit searches for the last known IP address. If this is not available it reverts to the default IP address of 192.168.1.168. This could result duplicate IP addresses. Refer to Quick Start Menu on page 28 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 19 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 20 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 21 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 22 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 23 Configure the Video Stream settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Streams** tab in the **Basic Configuration** menu.
3	Select either **Stream 1**, **2** or **3** from the **Stream Number** drop-down menu.
4	Select the required **Codec** from the drop-down list:

- **H264**
- **H264 IntelliZip**
- **H265**
- **H265 IntelliZip**
- **MJPEG**

The default setting is ‘H264’.

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

5 Select the required **Profile** from the drop-down list:

- **Main**
- **High**

The default setting is ‘Main’.

6 Select the required **Resolution** from the drop-down menu.
The resolutions available depend on the Image Source selected:

Pro Compact Mini Dome Camera resolutions		
Stream 1	**Stream 2**	**Stream 3**
(2048x1536) QXGA 4:3	(1280x720) 720p 16:9	(640x360) nHD 16:9
(1920x1080) 1080p 16:9	(1024x576) PAL+ 16:9	(480x360) 480 4:3
(1664x936) 16:9	(640x360) nHD 16:9	(384x288) 4:3
(1280x720) 720p 16:9	(480x360) 480 4:3	
	(384x288) 4:3	

Note:2048x1536 is only applicable to model 3MP IPS03CFOCWST.

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

The settings for all cameras are:

- **Stream 1 -** 1 - 60 ips, default 30. 60FPS is only available on Stream 1 with resolution 1920x1080 or lower.

- **Stream 2 -** 1 - 30 ips, default 15 ips. This stream is limited to 15 if Stream 1 is 60 ips.
- **Stream 3** - 7 - 15 ips. The default is 15.

Note:FPS varies depending on other features - refer to the Pro Gen 2 Release Notes for further information.

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

The default setting is 50.

OR

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

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

The default setting is ‘CVBR’.

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

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

OR

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

OR

c If you select CVBR, Max Bit Rate is enabled. Use the slider bar to select the **Max Bit Rate**. The default setting is 8000.

Picture Basic

Adjust Picture Rotation and Exposure displayed in the video pane.

Picture Rotation

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

Procedure 24 Configure Orientation Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Picture Basic** tab from the **Basic Configuration** menu.
3	Select the required **Orientation** setting:

- **Mirror**
- **Flip**

Mirror and Flip settings are not selected by default. The video pane updates to display the new settings.

Note: When wall mounting the camera you should select Flip and Mirror to correct the lens orientation.

- End -

Procedure 25 Selecting Corridor Mode

This provides a better perspective when viewing a long corridor.

Step Action

1 Select **Setup** on the GUI banner to display the setup menus.

2 Select the **Picture Basic** tab from the **Basic Configuration** menu.

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

4 Select the required **Corridor Mode** setting:

- None
- -90°
- +90°

5 The video pane updates to display the new settings.

- End -

Exposure

Configure the exposure settings for the camera.

Procedure 26 Configure Exposure Settings

Step Action

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

2 Select the **Picture Settings** tab from the **Basic Configuration** menu.

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

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

- **Auto**
- **Manual**
- **Shutter Priority**

Note: Settings available depend on the Exposure Mode configuration you choose.

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

- **Full Picture Weighted**

- **Upper**
- **Lower**
- **Center Weighted**
- **Spot**
- **Left**
- **Right**

The default setting is center weighted.

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

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

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

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

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

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

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

- End -

Procedure 27 Restore Exposure Defaults

Step Action

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

2 Select the **Picture Settings** tab from the **Basic Configuration** menu.

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

4 Select **Exposure Defaults** to restore the default settings.

- End -

Picture Additional

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

Wide Dynamic Range

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

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

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

Procedure 28 Disable/Enable Wide Dynamic Range (WDR)

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Picture Additional** tab from the **Basic Configuration** menu.
3	Select the required WDR from the drop-down list: • **WDR:** Digital wide dynamic range, enhancing detail in darker areas • **True WDR**: Two shutter wide dynamic range, to compensate for bright and dark areas in the scene. • **True WDR3x:** Three shutter wide dynamic range, to compensate for bright and dark areas in the scene. The default setting is OFF.
4	Select the **WDR level** from the drop-down list: • **Off** • **Low** • **Medium** • **High**

- End -

Day Night Mode

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.

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** from the **Basic Configuration** menu.

3 Select a **Day Night Mode** setting from the drop-down menu:

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

The default setting is 'Auto Mid'.

- End -

Picture Adjustment

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

Procedure 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 from the **Basic Configuration** menu.

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

The video pane will display the current camera view.

4 Use the slider bars to adjust:

- **Brightness**
- **Contrast**
- **Saturation**
- **Sharpness**
- **Hue**

The values range from 0% to 100%. The video pane updates to display the new 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 Settings** tab from the **Basic Configuration** menu.

3 Select **Defaults** to restore the default settings.

The default values are:

- **Brightness:** 50%
- **Contrast:** 50%
- **Saturation:** 50%
- **Sharpness:** 50%
- **Hue:** 50%

- End -

White Balance

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

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

Procedure 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 from the **Basic Configuration** menu.

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

The video pane displays the current camera view.

4 Select the required **White Balance** from the drop-down menu:

- **Auto Wide:** Suitable for a wider than normal range of lighting conditions
- **Auto Normal:** Suitable for a normal range of lighting conditions
- **Manual:** Adjustable red and blue balance

The default setting is ‘Auto Normal’.

- 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 from the **Basic Configuration** menu.

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

The video pane displays the current camera view.

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

The Red and Blue slider bars display.

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

The live video pane updates to display the new settings.

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

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

- End -

Date / Time / OSD

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

Camera Name

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

Procedure 34 Changing the on screen camera text size

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

2 Select the **OSD** tab in the **Basic Configuration** menu.

3 In the **Text Size** section, select **Normal** to display the text in a normal size.

OR

In the **Text Size** section, select **Large** to display the text in a larger size.

The default setting is ‘Normal’.

- End -

Procedure 35 Change the Camera Name

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

- End -

Date / Time

Set the date and time on the camera.

Procedure 36 Configuring the Date and Time

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

3 Select the **Time 24-hour** check box to enable the 24-hour clock.

Or

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

The default setting is ‘24-hour’.

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

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

The default setting is ‘YYYY/MM/DD’.

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

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

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

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

The default setting is ‘Manually’.

7 If you select Manually in step 5:

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

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

8 If you select via NTP in step 5:

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

- End -

On-Screen Display (OSD)

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

Procedure 37 Display or Hide the Camera Name OSD

Step Action

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

2 Select the **OSD** tab in the **Basic Configuration** menu.

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

OR

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

The default setting is ‘Disabled’.

- End -

Procedure 38 Display or Hide the Camera Time OSD

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

- End -

Procedure 39 Display or Hide the User Defined OSD

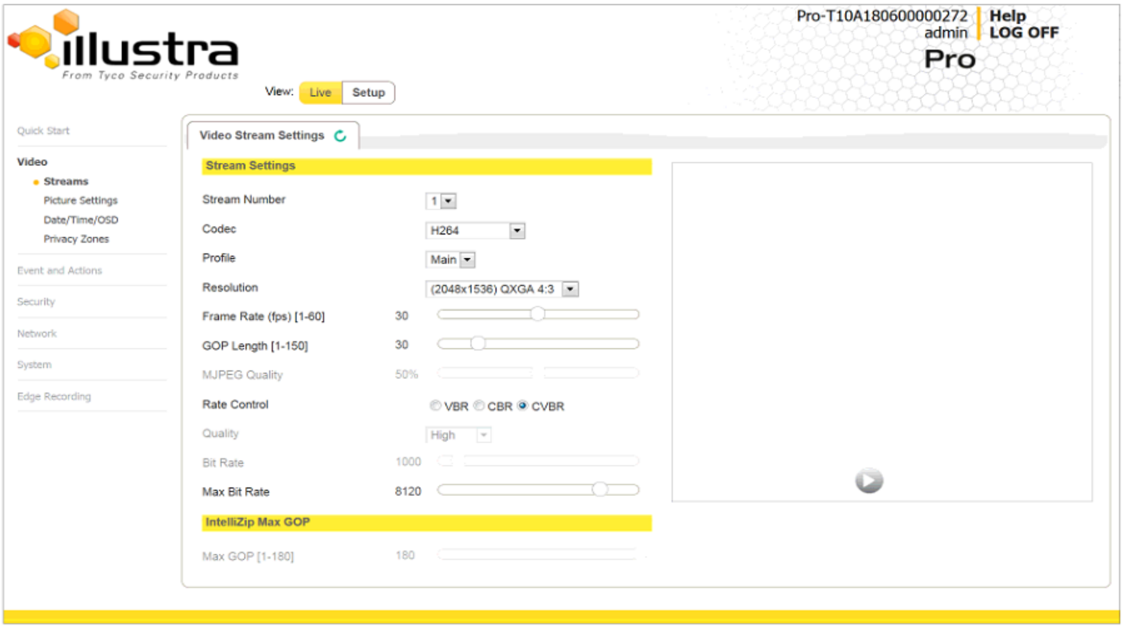
1	Select Setup on the Web User Interface banner to display the setup menus.
2	Select the **OSD** tab in the **Basic Configuration** menu.
3	In the **User Defined** section, select the **Enable** check box to display the camera name in the OSD. OR In the **User Defined** section, clear the **Enable** check box to hide the camera name in the OSD. The default setting is ‘Disabled’.
4	Select a **Location** from the drop-down menu.
5	Enter a name in the **Name** field. The OSD User Defined fields must comply with the following validation criteria: • 0 - 24 characters • Cannot begin or end with: • . (dot) • - (hyphen) • _ (underscore) • \ (backslash) • " (quotes)

- End -

Video Menu

When you select the **Video** menu, the **Streams** page displays, as seen in Figure 20 on page 41.

Figure 20 Video Menu



Stream Settings

Stream Number		1
Codec		H264
Profile		Main
Resolution		(2048x1536) QXGA 4:3
Frame Rate (fps) [1-60]	30	
GOP Length [1-150]	30	
MJPEG Quality	50%	
Rate Control		○ VBR ○ CBR ● CVBR
Quality		High
Bit Rate	1000	
Max Bit Rate	8120	

IntelliZip Max GOP

Max GOP [1-180]	180	

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

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

Streams

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

Note: The Web User Interface uses Stream 3.

Alarm Video

Edge Recording

Camera can directly record specific events (MD, DIO and Face detection) directly to 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 40 Configure the Video Stream settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Streams** tab in the **Video** menu.
3	Select **Stream1** , **2** or **3**,from the **Stream Number** drop-down menu.
4	Select the required **Codec** from the drop-down list: • **H264** • **H264 IntelliZip** • **H265** • **H265 IntelliZip** • **MJPEG** The default setting is ‘H264’.

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

Step	Action
5	Select the required **Profile** from the drop-down list: • **Main** • **High** The default setting is ‘Main’.
6	Select the required **Resolution** from the drop-down menu. The resolutions available depend on the model selected:

Compact Mini Dome camera resolutions		
Stream 1	**Stream 2**	**Stream 3**
(2048x1536) QXGA 4:3	(1280x720) 720p 16:9	(640x360) nHD 16:9
(1920x1080) 1080p 16:9	(1024x576) PAL+ 16:9	(480x360) 480 4:3
(1664x936) 16:9	(640x360) nHD 16:9	(384x288) 4:3
(1280x720) 720p 16:9	(480x360) 480 4:3	
	(384x288) 4:3	

Note:2048x1536 is only applicable to model 3MP IPS03CFOCWST.

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

The settings for all cameras are:

- **Stream 1 -** 1 - 60 ips, default 30. 60FPS is only available on Stream 1 with resolution 1920x1080 or lower.
- **Stream 2 -** 1 - 30 ips, default 15 ips. This stream is limited to 15 if Stream 1 is 60 ips.
- **Stream 3** - 7 - 15 ips. The default is 15.

8 If MJPEG has been selected, MJPEG Quality enables. Use the slider bar to select the **MJPEG Quality**.

The default setting is 50.

OR

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

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

The default setting is ‘CVBR’.

a If VBR has been selected, VBR Quality is enabled. Select the required **VBR Quality** from the drop-down menu. The default setting is ‘High’.

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

OR

b If CBR has been selected, CBR Bit Rate will be enabled. Use the slider bar to select the **CBR Bit Rate**. The default setting is 1000.

OR

c If you select CVBR, Max Bit Rate is enabled. Use the slider bar to select the **Max Bit Rate**. The default setting is 8000.

- End -

Procedure 41 Configuring IntelliZip Max GOP

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

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Streams** tab in the **Video** menu.

3	Use the slider bar to select the **Max GOP** range. Range available is 1-180.

- End -

Picture Settings

Picture Basic

Adjust the Picture Rotation, Exposure and White Balance settings.

Picture Rotation

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

Procedure 42 Configure Orientation Settings

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

- End -

Procedure 43 Selecting Corridor Mode

This provides a better perspective when viewing a long corridor.

Step	Action
1	Select **Setup** on the GUI banner to display the setup menus.
2	Select the **Picture Basic** tab from the **Basic Configuration** menu.
3	Select **Play** to start the video stream if it is not already active.
4	Select the required **Corridor Mode** setting: • None • -90° • +90°
5	The video pane updates to display the new settings.

- End -

Exposure

Configure the exposure settings for the camera.

Procedure 44 Configure Exposure Settings

Step Action

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

2 Select the **Picture Settings** tab from the **Basic Configuration** menu.

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

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

- **Auto**
- **Manual**
- **Shutter Priority**

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

- **Full Picture Weighted**
- **Upper**
- **Lower**
- **Center Weighted**
- **Spot**
- **Left**
- **Right**

The default setting is Center Weighted.

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

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

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

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

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

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

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

- End -

Procedure 45 Restore Exposure Defaults

Step Action

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

2 Select the **Picture Settings** tab from the **Basic Configuration** menu.

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

4 Select **Exposure Defaults** to restore the default settings.

- End -

Picture Additional

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

Wide Dynamic Range

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

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

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

Procedure 46 Disable/Enable Wide Dynamic Range (WDR)

Step Action

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

2 Select the **Picture Additional** tab from the **Picture Settings** menu.

3 Select the required WDR from the drop-down list:

- **WDR**: Digital wide dynamic range, enhancing detail in darker areas
- **True WDR**: Two shutter wide dynamic range, to compensate for bright and dark areas in the scene.
- **True WDR3x**: Three shutter wide dynamic range, to compensate for bright and dark areas in the scene.

The default setting is OFF.

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

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

- 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.

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 47 Configure Day Night Mode

Step Action

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

2 Select the **Picture Additional** from the **Basic Configuration** menu.

3 Select a **Day Night Mode** setting from the drop-down menu:

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

The default setting is 'Auto Mid'.

Picture Adjustment

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

Procedure 48 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 from the **Basic Configuration** menu.

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

The video pane displays the current camera view.

4 Use the slider bars to adjust:

- **Brightness**
- **Contrast**
- **Saturation**
- **Sharpness**
- **Hue**

The values range from 0% to 100%. The video pane updates to display the new settings.

- End -

Procedure 49 Restore Picture Balance Defaults

Step **Action**

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

2 Select the **Picture Settings** tab from the **Basic Configuration** menu.

3 Select **Defaults** to restore the default settings.

The default values are:

- **Brightness:** 50%
- **Contrast:** 50%
- **Saturation:** 50%
- **Sharpness:** 50%
- **Hue:** 50%

- End -

White Balance

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

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

Procedure 50 Configure Auto White Balance

Step **Action**

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

2 Select the **Picture Additional** tab from the **Basic Configuration** menu.

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

The video pane displays the current camera view.

4 Select the required **White Balance** from the drop-down menu:

- **Auto Wide:** Suitable for a wider than normal range of lighting conditions
- **Auto Normal:** Suitable for a normal range of lighting conditions
- **Manual:** Adjustable red and blue balance

The default setting is ‘AutoNormal’.

- End -

Procedure 51 Manually Select White Balance

Step Action

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

2 Select the **Picture Additional** tab from the **Basic Configuration** menu.

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

The video pane displays the current camera view.

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

The Red and Blue slider bars display.

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

The live video pane updates to display the new settings.

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

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

- End -

Date / Time / OSD

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

Camera Name

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

Procedure 52 Changing the on screen camera text size

Step Action

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

2 Select the **OSD** tab in the **Basic Configuration** menu.

3 In the **Text Size** section, select **Normal** to display the text in a normal size.

OR

In the **Text Size** section, select **Large** to display the text in a larger size.

The default setting is ‘Normal’.

- End -

Procedure 53 Change the Camera Name

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

- End -

Date / Time

Set the date and time on the camera.

Procedure 54 Configuring the Date and Time

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

- End -

On-Screen Display (OSD)

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

Procedure 55 Display or Hide the Camera Name

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

- End -

Procedure 56 Display or Hide the Camera Time

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

- End -

Procedure 57 Display or Hide the User Defined OSD

Step	Action
1	Select Setup on the Web User Interface banner to display the setup menus.
2	Select the **OSD** tab in the **Basic Configuration** menu.
3	In the **User Defined** section, select the **Enable** check box to display the camera name in the OSD. OR In the **User Defined** section, clear the **Enable** check box to hide the camera name in the OSD. The default setting is ‘Disabled’.
4	Select a **Location** from the drop-down menu.
5	Enter a name in the **Name** field. The OSD User Defined fields must comply with the following validation criteria: • 0 - 24 characters • Cannot begin or end with: • . (dot)

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

- End -

Privacy Zones

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

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

Up to 8 rectangular privacy zones can be used on the camera.

Defining a Privacy Zone

Create a privacy zone on the camera.

Procedure 58 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.

- End -

Enabling or Disabling a Privacy Zone

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

Procedure 59 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.

4 The video pane displays the current camera view.

5 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 60 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.

Note: More than one privacy zone can be deleted at a time. You can also use the **Select All** check box.

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

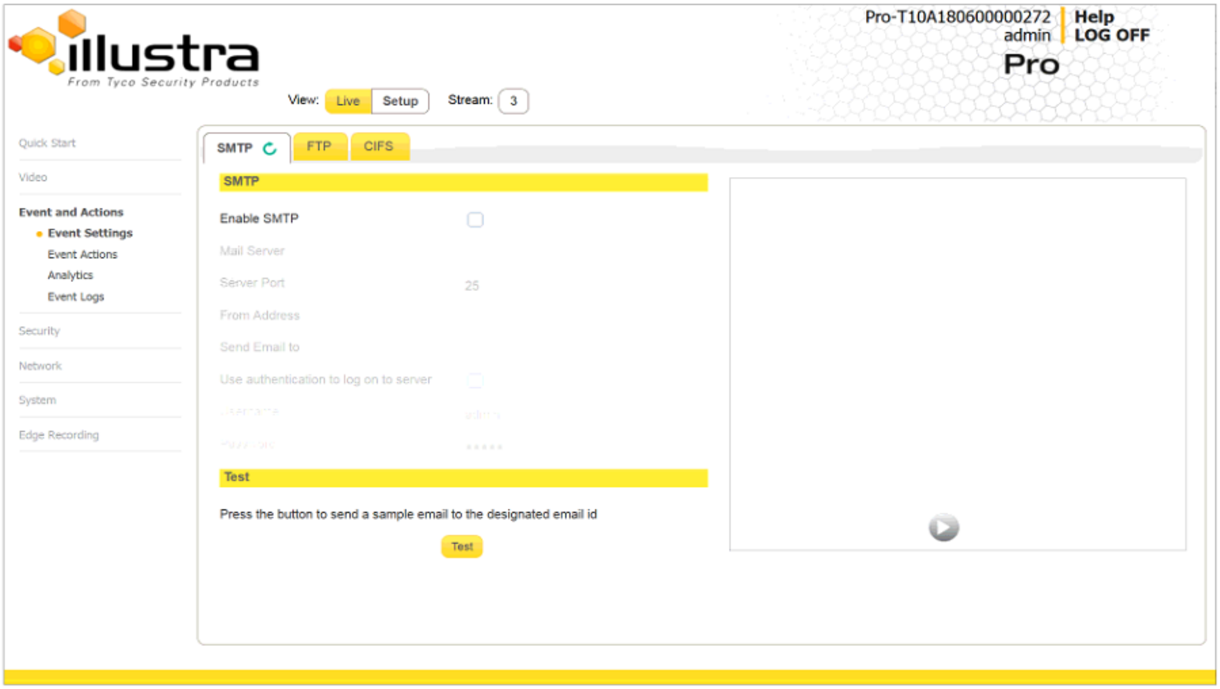
Select **Cancel**.

- End -

Events and Actions Menu

When you select the Events and Actions menu the Event Settings page displays, as seen in Figure 21 on page 54.

Figure 21 Events and Actions Menu



SMTP

Enable SMTP □

Mail Server

Server Port 25

From Address

Send Email to

Use authentication to log on to server □

Username admin

Password *****

Test

Press the button to send a sample email to the designated email id

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

- Event Settings
- Event Actions
- 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 61 Configure SMTP Settings

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

- End -

FTP

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

Note: You can configure FTP settings through the **Network** menu.

Procedure 62 Configure FTP Server Settings

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

3 Select the **FTP** tab.

4 Select the **Enable FTP** check box to enable FTP.

OR

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

The default setting is ‘Enabled’.

5 If required, select the **Secure FTP** checkbox.

The default setting is ‘Disabled’.

Note: When in Enhanced Security mode, enabling FTP requires the admin account password.

6 Enter the IP address of the FTP Server in the **FTP Server** text box.

7 Enter the FTP username in the **Username** text box.

8 Enter the FTP password in the **Password** text box.

9 Enter the FTP upload path in the **Upload Path** text box.

Note:

Refer Test the FTP Settings on page 57 to confirm that the FTP settings are working as expected.

- End -

File Transfer Rate

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

Procedure 63 Configure the FTP Transfer Rate

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

- End -

Test FTP Settings

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

Procedure 64 Test the FTP Settings

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

- End -

CIFS

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

Procedure 65 Configure CIFS Server Settings

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

- End -

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 microSD 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 microSD Card. If MJPEG is not being recorded on microSD 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.

A microSD Card must be inserted to send an SMTP email, video files and images from triggered analytic alerts.

Creating an Event Action

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

Procedure 66 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.

Note:
1. If you select Record, the AVI clip is saved to the microSD 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 microSD 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.

- End -

Editing a Event Action

Modify the details of an existing event action.

Procedure 67 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

- End -

Analytics

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

Region of Interest (ROI)

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

Procedure 68 Configure a Region of Interest

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Analytics** from the **Events and Actions** menu.
	The **ROI** tab displays.
3	Use the drawing tools to draw the region of interest overlay on the video stream.
4	Enter the name of the region of interest in the **Name** text box.
5	Select the **Enabled** check box to enable the region of interest.
	OR
	Clear the **Enabled** check box to disable the region of interest.
6	Click **Add**. The region of interest is configured.

- End -

Procedure 69 Delete a Region of Interest

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

- End -

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.

Procedure 70 Create a Motion Detection Alert

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Analytics** from the **Events and Actions** menu.
3	Select the **Enable motion detection** check box to enable Motion Detection on the camera. OR Clear the **Enable motion detection** check box to disable Motion Detection on the camera.
4	Select the zone for detection in the **Motion zone** drop-down list.
5	Select the **Enable motion zone** check box to enable the zone for motion detection.
6	Select **Edit** in the **Region configuration** field.
7	Use the drawing tools on the Motion Detection Configuration Pane to draw the region of interest on the pane. Multiple selections can be made.
8	Select the sensitivity from the **Sensitivity** drop-down menu: • **Highest** • **High** • **Medium** • **Low** • **Lowest**
9	Select the fault action from the **Action** drop-down menu.

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

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

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

- End -

Enable or Disable a Motion Detection Alert

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

Procedure 71 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 -

Blur Detection

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

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

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

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 72 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 73 Delete Current Events

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

2 Select **Event Logs** from the **Event and Actions** menu. The Event Logtab displays.

3 Select the corresponding **Delete** check box to mark the motion detection alert for deletion.

OR

Clear the corresponding **Delete** check box to keep the motion detection alert.

Note: You can select the **Select All** check box to mark all motion detection alerts displayed in the list for deletion.

4 Select **Delete** to delete the selected motion detection alerts.

You are prompted to confirm the deletion.

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

OR

Select **Cancel**.

- End -

Fault Log

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

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

System Faults

The following system faults may be raised:

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

Environmental Monitor (ENVM) Component

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

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

Procedure 74 Display Current Faults

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

- End -

Procedure 75 Delete Current Faults

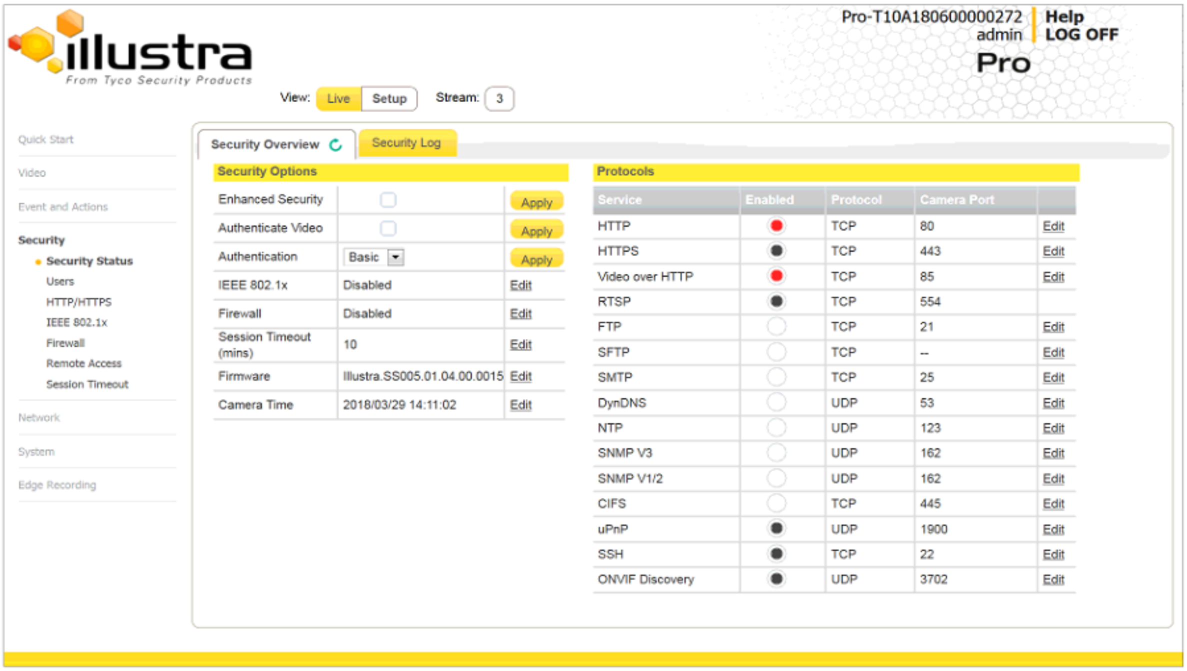
Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Event Logs** from the **Events and Actions** menu.
3	Select the **Fault Log** tab.
4	Select the corresponding **Delete** check box to mark the fault for deletion. OR Clear the corresponding **Delete**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

- End -

Security

When you select the **Security** menu, the **Security Status** page appears, as seen in Figure 22 on page 65.

Figure 22 Security menu



Security Options

Enhanced Security	□	Apply
Authenticate Video	□	Apply
Authentication	Basic ▾	Apply
IEEE 802.1x	Disabled	Edit
Firewall	Disabled	Edit
Session Timeout (mins)	10	Edit
Firmware	Illustra.SS005.01.04.00.0015	Edit
Camera Time	2018/03/29 14:11:02	Edit

Protocols

Service	Enabled	Protocol	Camera Port	
HTTP	●	TCP	80	Edit
HTTPS	●	TCP	443	Edit
Video over HTTP	●	TCP	85	Edit
RTSP	●	TCP	554	
FTP	○	TCP	21	Edit
SFTP	○	TCP	--	Edit
SMTP	○	TCP	25	Edit
DynDNS	○	UDP	53	Edit
NTP	○	UDP	123	Edit
SNMP V3	○	UDP	162	Edit
SNMP V1/2	○	UDP	162	Edit
CIFS	○	TCP	445	Edit
uPnP	●	UDP	1900	Edit
SSH	●	TCP	22	Edit
ONVIF Discovery	●	UDP	3702	Edit

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 24.

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

Procedure 76 Enable Enhanced Security

Step Action

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

2 Select **Security Status** from the **Security** menu.

3 Select the **Security Overview** tab.

4 Check the **Enable Enhanced Security** check box to enable enhanced security.

A prompt appears asking you for your current password and the new password for the Enchanced Security feature. Your password must adhere to the minimum requriments for an Enhanced Security password as seen below.

OR

Clear the **Enable Enhanced Security** check box to disable enhanced security.

Enhanced Security is disabled by default.

The Security Warning dialog appears.

5 Enter the current password in the **Current Password** text box.

6 Enter the new password in the **New Password** text box.

The password for enhanced security must meet the following requirements:

- Be a minimum of eight characters long
- Have at least one character from at least three 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 77 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.

Step	Action
4	Click **Apply**.

Note: Any changes to the Security mode are logged in the Security Log.

- End -

Security Status

This section summarizes the communication protocols that are used and their status. The following communication protocols can be enabled: HTTP, FTP, CIFS, Dyn DNS, SMTP, HTTPS, SNMP V1/2, SNMP V3, uPNP, and SFTP.

Security Overview

Procedure 78 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 79 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 80 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 98 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 81 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 82 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 83 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 84 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 85 Specify HTTP Method

Step Action

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

2 Select **HTTP/HTTPS** from the **Security** menu.

3 Select the **HTTP Method** using the radio buttons

- **HTTP**
- **HTTPS**
- **Both**

- End -

Procedure 86 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	Select **Browse** to navigate to the certificate location. The Choose file dialog displays.
4	Navigate to the location where the HTTPS certificate has been saved. Select the file and select **Open**. **Note:**The certificate needs to match the camera 'host name'.
5	Select **Upload**. You will be prompted to confirm that you would like to upload the HTTPS certificate.
6	Select **OK** to confirm the upload. OR Select **Cancel**.

- 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 87 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 88 Configure IEEE 802.1x Security

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

- End -

Firewall

Configure the Basic Filtering and Address Filtering for the firewall.

Basic Filtering

Enable or disable basic filtering for the camera this includes:

- ICMP (Internet Control Message Protocol) Blocking
- RP (Reverse Path) Filtering
- SYN Cookie Verification.

Procedure 89 Enable/Disable Basic Filtering

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Firewall** from the **Security** menu. The **Basic Filtering** tab displays.
3	Select the **ICMP Blocking** check box to enable ICMP blocking. OR Clear the **ICMP Blocking** check box to disable ICMP blocking. The default setting is 'Disabled'.
4	Select the **RP Filtering** check box to enable the RP filtering. OR Deselect the **RP Filtering** check box to disable. The default setting is 'Disabled'.
5	Select **SYN Cookie Certification** check box to enable SYN cookie certification. OR Deselect the **SYN Cookie Certification** check box to disable. The default setting is 'Disabled'.

- End -

Address Filtering

Configure the IP or MAC addresses which are denied access to the camera.

Procedure 90 Enable/Disable and configure Address Filtering

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Firewall** from the **Security** menu.
3	Select the **Address Filtering** tab.
4	Select **Off** to disable address filtering completely. OR Select **Allow** to allow address filtering for specified addresses OR Select **Deny** to deny address filtering for specific addresses. The default setting is 'Off'.
5	If address filtering has been set to **Allow** or **Deny**: a Enter an IP or MAC Address to allow / deny in the **IP or MAC Address** text box in the following format xxx.xxx.xxx.xxx.

Note:CIDR (Classless Inter-Domain Routing) is supported when using address filtering. If using a CIDR address use the following format xxx.xxx.xxx.xxx/xx.

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

- End -

Editing an Address Filter

Edit an existing address filter.

Procedure 91 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 92 Delete an Address Filter

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

- End -

Remote Access

SSH Enable

Enables Secure Shell access into the camera, if remote access is permitted by the camera network. This will also enable Tyco Security Products Level 3 Technical Support to diagnose any problems on the camera.

Note: It is recommended to keep SSH Enable disabled. This function should only be enabled this when it is requested by Tyco Security Products Level 3 Technical Support.

Procedure 93 Configure SSH

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Remote Access** from the **Security** menu.
	The **Remote Access** tab displays.
3	Select the **SSH Enable** check box to enable SSH.
	OR
	Deselect **SSH Enable** check box to disable SSH.
	The default setting is ‘Disabled’.

- End -

ONVIF

The Web User Interface allows ONVIF functionality to be managed at a high level. ONVIF Discovery Mode and User Authentication can be enabled or disabled.

- ONVIF Discovery Mode allows enabling or disabling discovery of the camera via ONVIF.
- ONVIF User Authentication allows the camera to accept ONVIF commands from all users or only authenticated users. Enabling User Authentication ensures the camera will only execute commands from authenticated users.

The separation of Discovery Mode and User Authentication allows the camera to be set up in a configuration that suits requirements for the network and users. The preferred discovery method for the camera is Illustra Connect, and this utilizes ONVIF discovery. It is therefore recommended that ONVIF Discovery Mode is always enabled.

ONVIF Discovery Mode

Enable or disable ONVIF discovery on the camera.

Procedure 94 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 95 Enable/Disable ONVIF User Authentication

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Remote Access** from the **Security** menu.
	The Remote Access tab displays.
3	Select the **ONVIF User Authentication** check box to enable ONVIF User Authentication.
	OR
	Deselect **ONVIF User Authentication** check box to disable ONVIF User Authentication.
	The default setting is ‘Enabled’.

- End -

Video over HTTP

Enable or disable video or steam metadata over HTTP on the camera.

Procedure 96 Enable/Disable Video over HTTP

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Remote Access** from the **Security** menu.
	The Remote Access tab displays.
3	Select the **Video over HTTP** check box to enable Video over HTTP.
	OR
	Deselect **Video over HTTP**check box to disable Video over HTTP.
	The default setting is ‘Enabled’.

- End -

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.

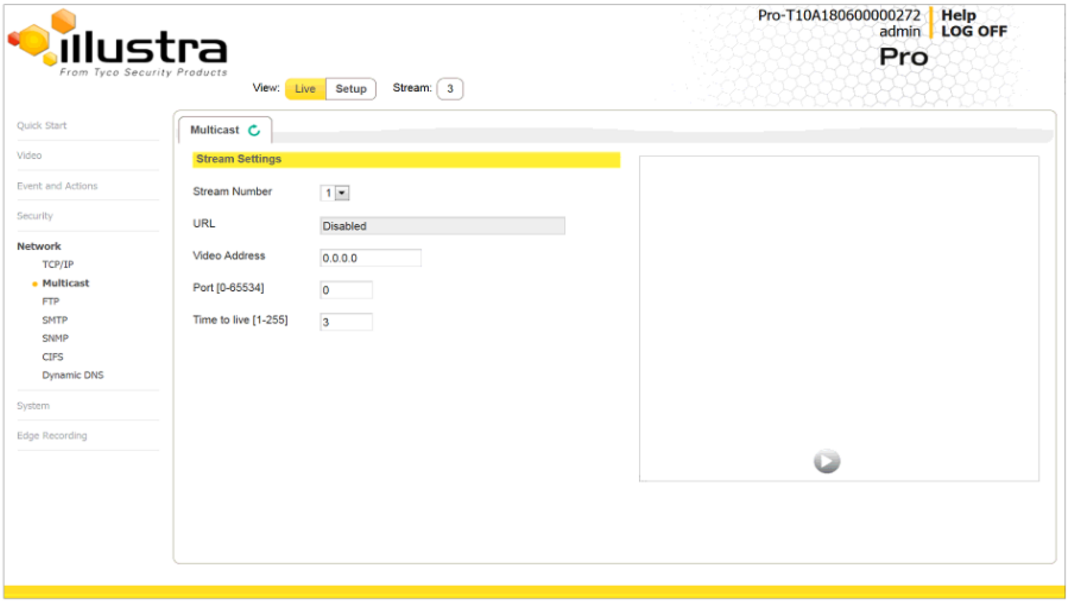
3 Use the slider bar to select the **Session Timeout (mins)**. The default setting is 15 minutes.

- End -

Network Menu

When you select the **Network** menu, the **TCP/IP** page displays, as seen in Figure 23 on page 78.

Figure 23 Network Menu



Stream Number 1

URL Disabled

Video Address 0.0.0.0

Port [0-65534] 0

Time to live [1-255] 3

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

- TCP/IP
- FTP
- SMTP
- SNTP
- 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 78 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 -

Multicast

Multicast streaming is a one-to-many relationship between a camera and the clients receiving the stream. With a multicast stream, the server streams to a multicast IP address on the network, and clients receive the stream by subscribing to the IP address.

Procedure 101 Configure Multicast Streaming

Step	Action
1	Select **Network** on the Web User Interface to display the Network menu options and click the **Multicast** tab.
2	Select the **Stream Number** from the drop-down list you want to configure.
3	In the **Video Address** field, enter a valid IP address for the Multicast broadcasting. The valid range for the IP address is:

```
224.xxx.xxx.xxx

232.xxx.xxx.xxx

234.xxx.xxx.xxx

239.xxx.xxx.xxx
```

Multicast stream addresses must be unique to the stream and cameras.

Step	Action
4	In the **Port** field, enter a port for the Multicast broadcasting. The Multicast stream port must be unique to stream cameras. The approved port range is: 0-65535.
5	In the **Time to live** field, enter a value.

Example of correct Mutlicast configuration:

```
Stream.1.Multicast.IPAddress=224.16.18.2

Stream.1.Multicast.Port=1032

Stream.2.Multicast.IPAddress=224.16.18.2

Stream.2.Multicast.Port=1030

Stream.3.Multicast.IPAddress=0.0.0.0

Stream.3.Multicast.Port=0
```

FTP

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

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

Procedure 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** check box to enable FTP. OR

Deselect the **Enable** check box to disable FTP.

The default setting is ‘Enabled’.

Note: When in Enhanced Security mode, enabling FTP requires the admin account password.

4	If required, select the **Secure FTP** checkbox. The default setting is ‘Disabled’.
5	Enter the IP address of the FTP Server in the **FTP Server** text box.
6	Enter the FTP port in the **FTP Port** text box. The default setting is 21.
7	Enter the FTP username in the **Username** text box.
8	Enter the FTP password in the **Password** text box.
9	Enter the FTP upload path in the **Upload Path** text box.

Note: When entering the upload path the following format should be used '//<name of ftp directory>/<folder>'

- End -

File Transfer Rate

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

Procedure 103 Configure the FTP Transfer Rate

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Event Settings** from the **Events and Actions** menu.
3	Select the **FTP** tab.
4	Select the **Limit Transfer Rate** check box to limit the FTP transfer rate. OR Clear the **Limit Transfer Rate** check box to disable limited FTP transfer. The default setting is ‘Enabled’.
5	Enter the Max Transfer Rate in the **Max Transfer Rate** (Kbps) textbox. The default setting is 50.

- End -

Test FTP Settings

Test the FTP settings that have been configured correctly.

Procedure 104 Test the FTP Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **FTP** from the **Network** menu.
3	Select the **FTP** tab.
4	Select **Test**. A sample text file will be sent to the specified FTP destination to confirm that FTP settings are correct.

- End -

SMTP

Configure the SMTP settings to allow e-mail alerts to be sent from the camera when an analytic alert is triggered.

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

Procedure 105 Configure SMTP Settings

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

- End -

SNMP

The camera introduces support for the Simple Network Management Protocol making it easier to manage on an IP network.

The SNMP support includes support for V2 and V3. Using V2 means no authentication is required to access the data and results are unencrypted. V3 offers enhanced encryption and authentication security features.

Procedure 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 **Security Level** from the drop down menu: **- noauth:** No authentication / no encryption. - **auth:** Authentication / no encryption. A user password is required. It is symmetrically encrypted using either MD5 or SHA. - **priv**: Authentication / encryption. A user password is required as is symmetrically encrypted using either MD5 or SHA. A data encryption password is required as is symmetrically encrypted using either DES or AES. d Select the **Authentication Type** using the radio buttons. e Enter the Authentication Password f Select the **EncryptionType** using the radio buttons. g Enter the **Encryption** Password h Select **Apply**.

- End -

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.

- 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 108 Configure Dynamic DNS

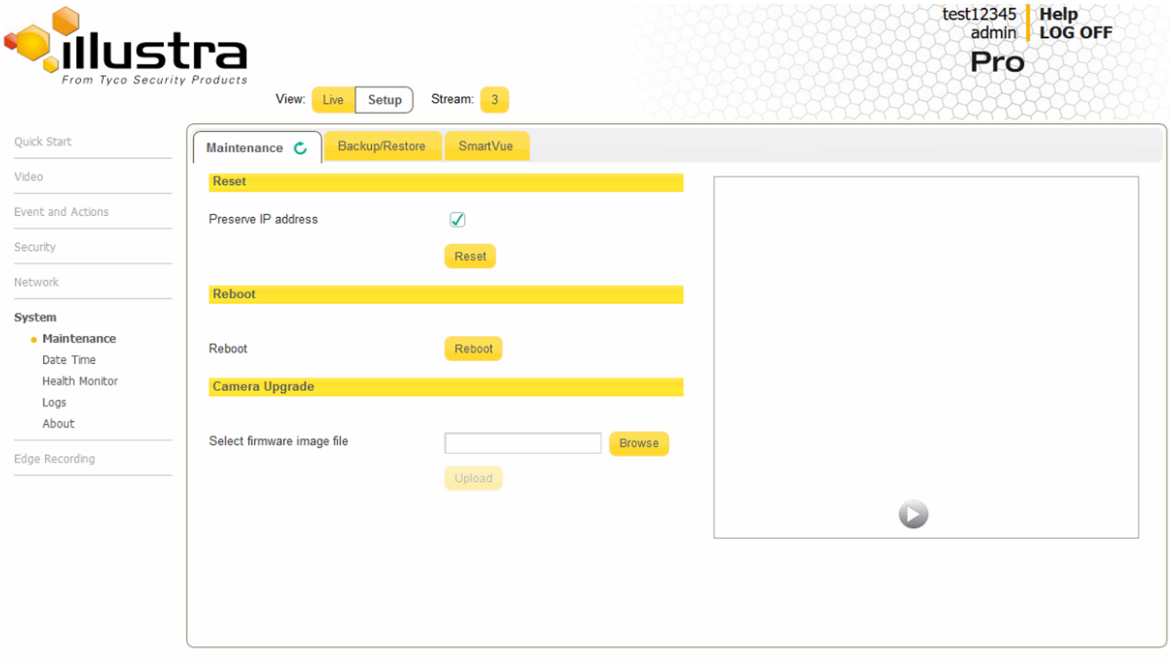
Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Dynamic DNS** from the **Network** menu.
3	Select the **Service Enable** check box to enable Dynamic DNS. OR Deselect **Service Enable** check box to disable Dynamic DNS. The default setting is ‘Disabled’.
4	If Service Enable has been enabled: a Enter the Camera Alias in the text box. b Select a Service Provider from the drop-down list: • **dyndns.org** • **easydns.com** • **no-ip.com** • **zerigo.com** • **dynsip.org** • **tzo.com** c Enter a **Username** in the text box. d Enter a **Password** in the text box. e Enter **Service Data** in the text box.
5	Select **Apply** to save the settings.

- End -

System

When you open the **System** menu, the **Maintenance** page appears, as seen in Figure 24 on page 86.

Figure 24 System Menu



Preserve IP address ☑

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

- Maintenance
- Date Time
- Health Monitor
- Logs
- About

Maintenance

The Maintenance menu allows you to restore the camera settings to factory default, reboot the camera and apply a firmware upgrade.

Reset

To perform a physical reset of the camera, refer to the chapter regarding your camera model in this guide.

Note: Network settings can be retained if required.

Procedure 109 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 **Reboot**

You will be prompted to confirm the camera reset.

- Select **OK** to confirm. The Web User Interface will display a “Camera Resetting” page with a progress bar showing the reboot progress.
- When the camera is restarted it will take 2 - 3 minutes until it is online and ready to be accessed and controlled.

  OR

  Select **Cancel**.

5 The Log in page displays.

- End -

Reboot

To perform a physical reset of the camera, refer to the chapter regarding your camera model in this guide.

Procedure 110 Reboot the Camera

Step **Action**

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

2 Select **Maintenance** from the **System** menu.

3 Select **Reboot**.

You will be prompted to confirm the camera reboot.

4 Select **OK** to confirm.

The Web User Interface will display a “Camera Rebooting” page with a progress bar showing the reboot progress.

When the camera is restarted it will take 2 - 3 minutes until it is online and ready to be accessed and controlled.

OR

Select **Cancel**.

5 The Log in page displays.

- End -

Camera Firmware Upgrade

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

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

⚠ Caution

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

Procedure 111 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 112 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 113 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 -

SmartVue

The SmartVue feature implements Illustra Cameras to Cloud (C2C) from SmartVue to provide a secure, scalable, cloud-based storage solution. Before you enable this feature, you need to install the mobile application. You can download the app from either the iOS App Store or the Google Play Store and then you can complete the registration using the app.

Procedure 114 Enabling SmartVue integration

Note: If a SmartVue server is not setup when enabling the SmartVue feature then the camera may become inaccessible.

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 **SmartVue** tab.
4	Select **Apply**.
5	Enter an administrator password to validate the request. • If the camera detects an Internet connection, it continues with the SmartVue integration request. If an Internet connection is not detected an error displays and the request is rejected.

Note: If an Internet connection is detected, a factory reset begins. This clears all previous user defined configurations including user management settings.
The camera boots in SmartVue mode and is only accessible using HTTPS.
The password changes to a string of characters determined by the SmartVue cloud.

Step	Action
6	Refer to SmartVue documentation and follow the procedure to add a camera to regain access.

- End -

Procedure 115 Resetting the camera to normal operation

Note: There are two procedures for resetting the camera, please select one.

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Maintenance** from the **System** menu.
3	Select the **Maintenance** tab. This page displays two types of factory reset: a **Factory Reset**: Resets the camera and boots the camera in Illustra mode. b **SmartVue Reset**: Resets the camera and boots the camera in SmartVue mode.
4	If you do not have the credentials to perform a reset, you can perform a factory reset on the hardware itself by using the hardware reset button as detailed in Table 8 on Page 10.

- 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 116 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:

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

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

8 If you select via NTP in step 5:

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

- End -

Health Monitor

The Health Monitor function provides visibility on the health status of popular device parameters. Each parameter can be enabled or disabled. The refresh frequency of the health monitor can be determined by selecting a duration from the Reporting Period drop-down menu.

Procedure 117 Configure Health Monitor Settings

Step Action

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

2 Select the **Health Monitor** from the **System** menu.

3 Select the **Recording Period** from the drop-down menu.

4 Select the corresponding checkbox to enable health monitoring on a parameter.

OR

Clear the corresponding checkbox to disable health monitoring on a parameter.

The default setting for all parameters is Enabled.

- End -

Logs

Information is provided on system and boot logs created by the camera.

System Log

The system log gives the most recent messages from the unix /var/log/messages file. Information will include the following:

- Messages about system behavior such as process startup/shutdown.
- Warnings about recoverable problems that processes encounter.
- Error messages where processes encounter problems they cannot fix; note that this does not mean that the process will not continue to work, only that it encountered an issue it could do nothing about.

Procedure 118 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 119 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 120 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 121 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 122 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 123 Edit Camera Name

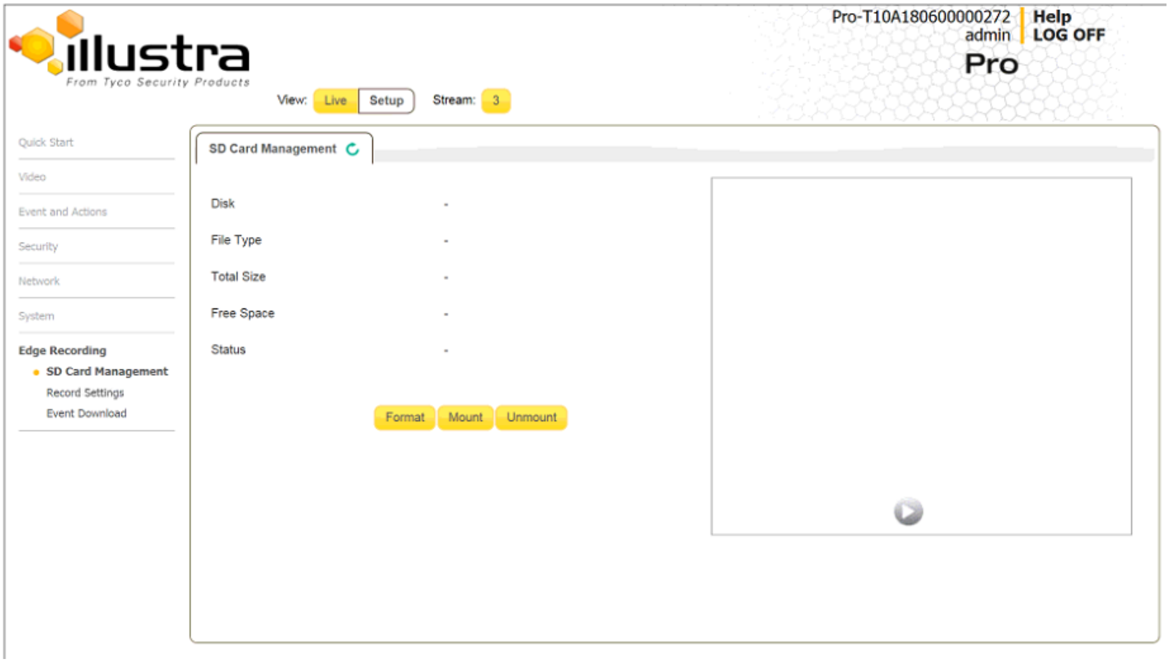
Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **About** from the **System** menu. The model tab displays.
3	Edit the name in the **Camera Name** textbox.

- End -

Edge Recording

When you select the **Edge Recording** menu, the **SD Card Management** page appears, as seen in Figure 25 on page 94.

Figure 25 Edge Recording Menu



Disk -
File Type -
Total Size -
Free Space -
Status -

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 SD Card. Video can be configured to be recorded based on an event. Without an SD Card current faults notifications displayed on camera if an alarm is triggered. Using an SD Card enables the following:

- Current faults notifications displayed on camera if an alarm is triggered.
- Video and screen shot are saved to the SD card.
- SMTP notifications can be sent.
- FTP and CIFS uploads of video can be sent.

Inserting the SD Card

When inserting an SD Card it is essential that the camera is rebooted. The 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 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 124 Insert the SD Card by powering down the Camera

Step	Action
1	Turn off the camera by disconnecting the power supply.
2	Insert the SD card into the camera.
3	Reconnect the power supply and power up the camera.

- End -

Procedure 125 Mount the SD Card through the Web User Interface to reboot the Camera

Step	Action
1	Insert the MicroSD 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 MicroSD Card

If at any stage you need to remove the MicroSD card from the camera one of the following two procedures should be used:

- Remove the 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 MicroSD card before removal.
- Unmount the 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 126 Remove the MicroSD Card by powering down the Camera

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

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

3 Reconnect the power supply and power up the camera.

- End -

Procedure 127 Unmount the MicroSD 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 SD card from the camera. AVI clips are not available on the camera until the 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 128 Configure Record Settings

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

5 Select **Apply** to save.

- End -

Offline Record Settings

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

Procedure 129 Configure Offline Recording Settings

Step	Action
1	Select **Setup** on the Web User Interface Banner to display the setup menus.
2	Select **Record Settings** from the **Edge Recording** menu.
3	Select the **Offline Record Settings** tab.
4	In the **Video Edge IP Address** field, enter the IP address of the Video Edge recorder the camera is connected to.
5	In the **Pre event (secs)** field, enter a time in seconds of the amount of time you want recorded before the offline event.
6	In the **Post event (secs)** field, enter a time in seconds of the amount of time you wants recorded after the offline event.

- End -

Event Download

If an event action has record mode enabled, when triggered, the associated video is logged in the event download table where it can later be downloaded from an 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	X	X	
		OSD	X	X	
Video	Streams	Video Stream Settings	X	X	
	Picture Settings	Picture Basic	X	X	
		Picture Additional	X	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		
	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		
	Users	User	X	X	
		Add User	X	X	
		Change Password	X	X	X

Camera Menu	Sub Menu	Tab	Admin	Operator	User
	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		
	FTP	FTP	X		
	SMTP	SMTP	X		
	SNTP	SNTP	X		
	CIFS	CIFS	X		
	Dynamic DNS	Dynamic DNS	X		
System	Maintenance	Maintenance	X		
		Backup / Restore	X		
	Date Time	Date Time	X		
	Health Monitor	Health Monitor	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 Settings	X		
	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 Resolutions

Pro 2MP and 3MP Compact Mini Dome Streaming Combinations

	Normal Mode			
	Codec: H264 (w/IntelliZip), H265 (w/IntelliZip), MJPEG			
	Resolution	Max FPS with TWDR Off	Max FPS with TWDR 2x	Max FPS with TWDR 3x
Stream 1 **Note:**2048x1536 is only supported on the 3MP model	2048 x 1536 / QXGA / 4:3	30	30	20
	1920 x 1080 / 1080p / 16:9	60	30	20
	1664 x 936 / 16:9	60	30	20
	1280 x 720p / 16:9	60	30	20
Stream 2	1280 x 720 / 720p / 16:9	30 *1	30	20
	1024 x 576 / PAL+ / 16:9	30 *1	30	20
	640 x 360 / nHD / 16:9	30 *1	30	20
	480 x 360 / 480p / 4:3	30 *1	30	20
	384 x 288 / 4:3	30 *1	30	20
Stream 3	640 x 360 /nHD / 16:9	15 *2	15 *2	15 *2
	480 x 360 / 480p / 4:3	15 *2	15 *2	15 *2
	384 x 288 / 4:3	15 *2	15 *2	15 *2

	Corridor Mode			
	Codec: H264 (w/IntelliZip), H265 (w/IntelliZip), MJPEG			
	Resolution	Max FPS with TWDR Off	Max FPS with TWDR 2x	Max FPS with TWDR 3x
Stream 1 **Note:**1536x2048 is only supported on the 3MP mode	1536 x 2048 / QXGA / 3:4	30	30	20
	1088 x 1920 / 1080p / 9:16	30	30	20
	944 x 1664 / 9:16	30	30	20
	720 x 1280 / 720p / 9:16	30	30	20
Stream 2	720 x 1280 / 720p / 9:16	30	15	15
	576 x 1024 / PAL+ / 9:16	30	15	15
	368 x 640 / nHD / 9:16	30	15	15
	368 x 480 / 480p / 3:4	30	15	15
	288 x 384 / 3:4	30	15	15
Stream 3	368 x 640 / nHD / 9:16	15 *2	15 *2	15 *2
	368 x 480 / 480 / 3:4	15 *2	15 *2	15 *2
	288 x 384 / 3:4	15 *2	15 *2	15 *2

Note:*1 - Stream 2 is restricted to 15 FPS when Stream 1 is greater than 30 FPS.

Note:*2 - Stream 3 is restricted to MJPEG only.

Note:*3 - Only 3MP models can support 1546x2048 (QXGA) 3:4 or 1536x2048 (QXGA) 3:4, and is not available in MJPEG.

Note: Maximum of 5 concurrent streams are supported by each camera, this includes shared streams.(Example: Stream 1 can be shared twice along with a running Stream 2 and Stream 3, or Stream 1 can be shared four times if Stream 2 and Stream 3 are not running.

Appendix D: Camera Defaults

The below table details the defaults for the Illustra Connect Web User Interface.

Table 26 Camera Defaults

Tab	Item	Default		
TCP/IP				
	Enable DHCP	ON		
	IPv4 Address	192.168.1.168		
	Network Mask	255.255.255.0		
	Gateway	Unspecified		
	Primary DNS	Unspecified		
	IPv6 Enable	ON		
	Current IPv6 Address	Unspecified		
Video Stream Settings				
	Stream Number	1	2	3
	Codec	H264	H264	MJPEG
	Profile	Main		
	Resolution	2048x1536	1280x720	480x360
	Frame Rate (fps) [1-30]	30	15	15
	GOP Length [1-150]	30	30	N/A
	MJPEG Quality	N/A	N/A	N/A
	Rate Control	CVBR	CVBR	N/A
	VBR Quality	N/A	N/A	N/A
	CBR/CVBR Bit Rate	8000	8000	N/A
Picture Basic				
	Mirror	OFF		
	Flip	OFF		

Tab	Item	Default		
	Corridor Mode	OFF		
	Exposure Method	Center Weighted		
	Exposure Offset (F-stops)	0		
	Min Exposure (sec)	1/10000		
	Max Exposure (sec)	1/8		
	Max Gain (dB)	51dB		
	Frequency	60Hz		
	Flickerless	OFF		
Picture Additional				
	Enable WDR	OFF		
	Day Night Mode	Auto Mid		
	Brightness	50%		
	Contrast	50%		
	Saturation	50%		
	Sharpness	50%		
	White Balance Mode	Auto Normal		
	Red	50%		
	Blue	50%		
Date/Time/OSD				
	Camera Friendly Name	Pro-SERIALNUMBER		
	Camera Time	Unspecified		
	Time 24-hour	ON		
	Date Display Format	YYYY/MM/DD		
	Time Zone	(GMT-05:00) Eastern Time (US and Canada)		
	Set Time	Manually		

Tab	Item	Default		
	Date(DD/MM/YY)	Unspecified		
	Time(HH:MM:SS)	Unspecified		
	Text size	Normal		
	OSD Name	OFF		
	OSD Time	OFF		
	OSD User defined	Unspecified		
Privacy Zones				
	Name	Unspecified		
SMTP				
	Mail Server	Unspecified		
	Server Port	25		
	From Address	Unspecified		
	Send Email To	Unspecified		
	Use authentication to log on to server	OFF		
FTP				
	Enable FTP	ON		
	Secure FTP	OFF		
	FTP Server	Unspecified		
	FTP Port	21		
	Username	Unspecified		
	Password	Unspecified		
	Upload Path	Unspecified		
	Limit Transfer Rate	ON		
	Max Transfer Rate (Kbps)	50		
CIFS				
	Enable	ON		

Tab	Item	Default		
	Network Path	Unspecified		
	Domain Name	Unspecified		
	Username	Unspecified		
	Password	Unspecified		
Event Actions				
	Fault action 1	Unspecified		
	Fault action 2	Unspecified		
	Fault action 3	Unspecified		
	Fault action 4	Unspecified		
	Fault action 5	Unspecified		
ROI				
	Table	Unspecified		
	Enable Face Detection	OFF		
	Highlight Faces	OFF		
	Enhance Faces	OFF		
	Face Orientation	UP		
	Action	Unspecified		
Motion Detection				
	Enable Motion Detection	OFF		
	Sensitivity	HIGH		
	Action	Unspecified		
Blur Detection				
	Enable Blur Detection	OFF		
Event Log		Unspecified		
Fault Log		Unspecified		
Security				

Tab	Item	Default		
	Security Status	Standard		
Users				
	Logon Name	Admin		
	Role	Admin		
Add User				
	Name	Unspecified		
	Role	Unspecified		
	Password	Unspecified		
	Confirm Password	Unspecified		
Change Password				
	Name	Unspecified		
	Current Password	Unspecified		
	New Password	Unspecified		
	Confirm New Password	Unspecified		
HTTP/HTTPS				
	HTTP Method	BOTH		
	Select Cirtificate File	Unspecified		
EAP Settings				
	Enable IEEE802.1x	OFF		
	EAPOL Version	1		
	EAP Method	PEAP		
	EAP Identity	Unspecified		
	CA Certificate	Unspecified		
	Password	Unspecified		
	Client Certificate	Unspecified		
	Private Key Password	Unspecified		

Tab	Item	Default		
Basic Filtering				
	ICMP Blocking	OFF		
	Rp Filtering	OFF		
	SYN Cookie Verification	OFF		
Address Filtering				
	Filtering	OFF		
	IP or MAC Address	Unspecified		
Remote Access				
	SSH Enable	OFF		
	ONVIF Discovery Mode	ON		
	ONVIF User Authentication	ON		
	Video Over HTTP	ON		
	UPnP Discovery	ON		
	ExacqVision Server Audio	ON		
Session Timeout				
	Session Timeout(mins)	15		
Dynamic DNS				
	Service Enable	OFF		
	Camera Alias	Unspecified		
	Service Provider	dyndns.org		
	Username	Unspecified		
	Password	Unspecified		
	Service Data	Unspecified		
Maintenance				
	Preserve IP Address	ON		
	Preserve Applications	ON		

Tab	Item	Default		
	Select Firmware Image File	Unspecified		
Backup/Restore				
	Select Saved Data File	Unspecified		
Health Monitor				
	Reporting Period (seconds)	20		
	Health Monitor Table	Unspecified		
System Log				
	Lines (From The End Of The Log File)	Unspecified		
	Filter (Only Lines Containing Text)	Unspecified		
Boot Log				
	Lines (From The End Of The Log File)	Unspecified		
	Filter (Only Lines Containing Text)	Unspecified		
Audit Log				
	Search By	Unspecified		
	Filter Text 1	TEXT		
	Filter Text 2	Unspecified		
	Start Date (DD/MM)	Unspecified		
	End Date (DD/MM)	Unspecified		
Model				
	Camera Name	Factory configuration		
	Model	Factory configuration		
	Product Code	Factory configuration		
	Manufacturing Date	Factory configuration		
	Serial Number	Factory configuration		
	MAC Address	Factory configuration		

Tab	Item	Default		
	Firmware Version	Factory configuration		
	Hardware Version	Factory configuration		
SD Card Management				
	Disk	Unspecified		
	File Type	Unspecified		
	Total Size	Unspecified		
	Free Space	Unspecified		
	Status	Unspecified		
Record Settings				
	Enable Even Recording	OFF		
	Record Source	Stream 1		
	Pre Event (secs)	10		
	Post Event (secs)	10		
Offline Record Setting				
	Video Edge IP address	Unspecified		
	Pre event (sec)	10		
	Post event (sec)	10		
Event Download				
	File Name Table	Unspecified		

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.

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.