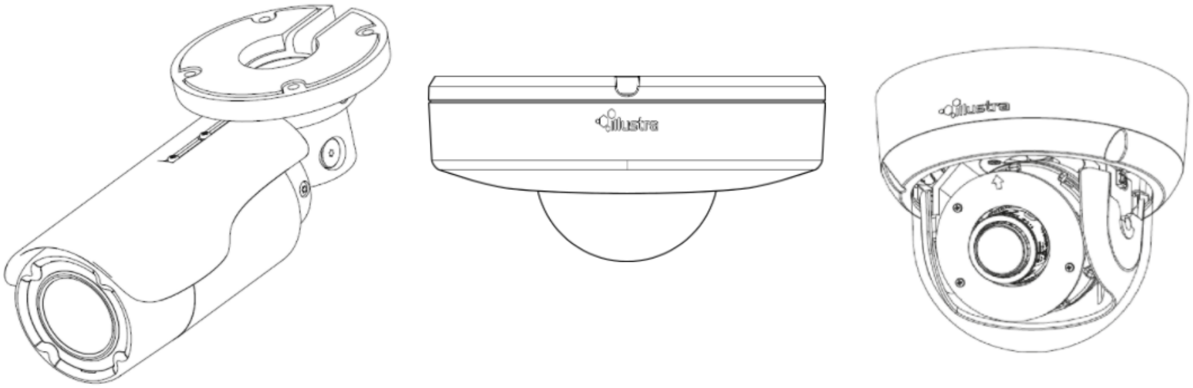
tyco | Illustra

Illustra Flex Gen 3 Series

Installation and Configuration Guide



Johnson Controls

Notice

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

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

Copyright

Tyco Security Products

6600 Congress Avenue

Boca Raton, FL 33487 U.S.A.

Customer Service

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

Trademarks

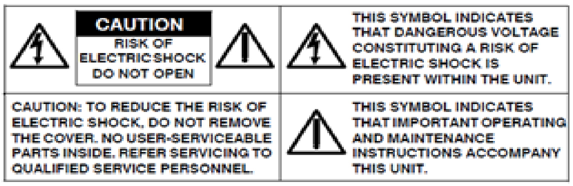
The trademarks, logos, and service marks displayed on this document are registered in the United States [or other countries]. Any misuse of the trademarks is strictly prohibited and Tyco Security Products will aggressively enforce its intellectual property rights to the fullest extent of the law, including 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

- These units operate at AC 24V/ PoE .
- The Compact Dome camera is powered by PoE (IEEE 802.3at Class 1).
- Installation and service should be performed only by qualified and experienced technicians and comply with all local codes and rules to maintain your warranty.
- The Compact Dome, Bullet, Mini-Dome cameras are not intended to be directly connected to an external network and the video coax connections should only be connected intra-building.
- To avoid damaging the Bullet and Mini-Dome cameras, never connect more than one type of power supply (PoE IEEE802.3 Ethernet Class 0) at the same time. If using any type of PoE, these cameras must be connecting only to PoE networks without routing to heterogeneous devices.
- 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.
- To meet EU EMC immunity requirements for security equipment the mains power for equipment powering the unit should be backed up by an uninterruptible power supply.
- 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.
- The power supply shall be approved for ITE NEC Class 2 or LPS with a rating of 24VAC, 550mA minimum and 50 degrees Celsius. The Compact Mini Dome 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:
        - Indoor Minidome: -20˚C to 50˚C (-4˚F to 122˚F)
        - Outdoor Minidome: -50˚C to 50˚C (-58˚F to 122˚F)
        - Bullet: -40˚C to 50˚C (-40˚F to 122˚F)
        - 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 Flex Installation and Configuration Guide is a user manual which provides physical properties, installation, and configuration information of the cameras in Table 1 on Page 8.

Table 1 Product codes

Product Code	Model Name	Description
IFS03-D21-OI03	Illustra Flex3 3MP Outdoor Dome	Illustra Flex Gen 3, 3MP Dome, 3.2-10mm, outdoor, clear bubble, white, TDN w/IR, Multi-Exposure WDR
IFS03-D21-AT03	Illustra Flex3 3MP Indoor Dome	Illustra Flex Gen 3, 3MP Dome, 3.2-10mm, indoor, clear bubble, white, TDN, Multi-Exposure WDR
IFS08-D22-AT03	Illustra Flex3 3MP Indoor Dome	Illustra Flex Gen 3, 8MP Dome, 4.17-9.48mm, indoor, clear bubble, white, TDN, Multi-Exposure WDR
IFS03-B21-OI03	Illustra Flex3 3MP Bullet	Illustra Flex Gen 3, 3MP Bullet, 3.2-10mm, indoor, clear bubble, white, TDN w/IR, Multi-Exposure WDR
IFS03-C10-OI03	Illustra Flex3 3MP outdoor Compact	Illustra Flex Gen 3, 3MP Compact, outdoor, white, TDN w/IR, Multi-Exposure WDR
IFS08-B22-OI03	Illustra Flex3 4K Bullet	Illustra Flex Gen 3, 8MP Bullet, 4.17-9.48mm, indoor, clear bubble, white, TDN w/IR, Multi-Exposure WDR
IFS08-C10-OI03	Illustra Flex3 4K outdoor Compact	Illustra Flex Gen 3, 8MP Compact, outdoor, white, TDN w/IR, Multi-Exposure WDR
IFS08-D22-OI03	Illustra Flex3 4K Outdoor Dome	Illustra Flex Gen 3, 8MP Compact, 4.17-9.48mm, outdoor, clear bubble, white, TDN w/IR, Multi-Exposure WDR

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

- For the Illustra Flex Gen 3 3MP and 8MP Dome cameras, refer to Illustra Flex Gen 3 3MP Indoor Dome Cameras on page 19.
- For the Illustra Flex Gen 3 3MP and 8MP Bullet camera, refer to Illustra Flex Gen 3 3MP and 8MP Indoor Bullet Cameras on page 14.
- For the Illustra Flex Gen 3 3MP and 8MP Outdoor Compact Mini Dome camera, refer to Illustra Flex Gen 3 3MP and 8MP Outdoor Compact Dome Camera on page 9.

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 37 for procedural information pertaining to camera configuration.

Illustra Flex Gen 3 3MP and 8MP Outdoor Compact Dome Camera

This chapter provides product features, installation procedures, and connection information regarding the Illustra Flex Gen 3 3MP and 8MP Outdoor Compact Dome camera.

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 Ilustra Flex Gen 3 - 3MP and 8MP Outdoor Compact Dome camera. Product code and description of the camera is provided in Table 2 on page 9.

Table 2 Product code and description of the Compact Mini Dome camera

Product Code	Description
IFS03-C10-OI03	Illustra Flex Gen 3, 3MP Compact, outdoor, white, TDN w/IR, Multi-Exposure WDR
IFS08-C10-OI03	Illustra Flex Gen 3, 8MP Compact, outdoor, white, TDN w/IR, Multi-Exposure WDR

In the box

- 1 x Compact Dome camera
- 1 x Mounting template sticker
- 1 x Mounting plate
- 3 x 40x6mm plastic screw anchors
- 3 x 50x4mm tapping screws
- 3 x 10x4mm mounting plate screws
- 1 x Printed Quick Start Guide
- 1 x Waterproof RJ45 cable accessory
- 1 x Torx driver

Installation tools

- 1 x Screw driver
- 1 x Torx driver
- 1 x Drill

Quick reference

- Default IP: 192.168.1.168 (DHCP enabled)
- Default Username: admin
- Default Password: admin
- Power: PoE 802.3af

Figure 3 Camera Parts

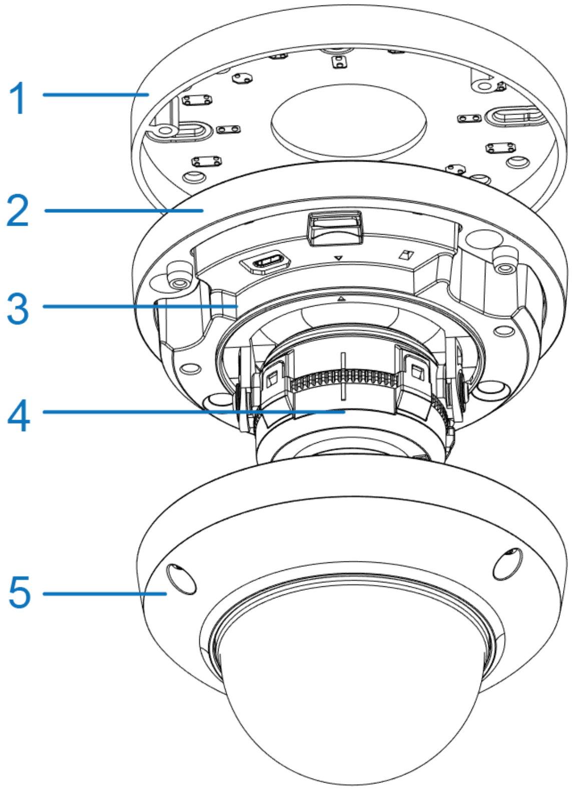


Table 4 Camera part descriptions

Camera	Part Description
1	Mounting Plate
2	Camera Base
3	Camera body
4	Camera lens
5	Dome cover

Procedure 1 Mounting and powering up the camera

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

2 On the mounting surface drill three Ø 6mm holes and cut out an Ø 22mm cabling hole as per the markings identified on the mounting template sticker.

3 Securely place the three screw anchors into the three Ø 6mm holes.

4 Unscrew the three screws on the camera dome (5) (Figure 3) to remove the dome cover from the camera base.

5 Place the PoE cable:

a through the cable side entry slot on the camera base (2) (Figure 3).

OR

a through the cable hole on the mounting plate (1) (Figure 3).

6 Place the camera base (2) (Figure 3) on to the camera mounting plate (1) (Figure 3) and ensure that the three holes on the camera base align with the three holes on the mounting plate.

Note: Note: If the PoE cable is placed through the cable hole on the mounting plate then insert the PoE cable through the Ø 22mm hole on the mounting surface.

7 Hold the mounting plate and camera base up to the mounting template and align the three holes on the mounting plate and camera base with the three holes on the mounting template.

8 Insert the three screws onto the three holes on the camera base and securely attach the mounting plate and camera base to the surface.

9 Cover the camera body with the dome cover (5) (Figure 3) and securely attach the dome to the camera with the three screws.

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

- End -

Figure 5 Camera buttons and connections

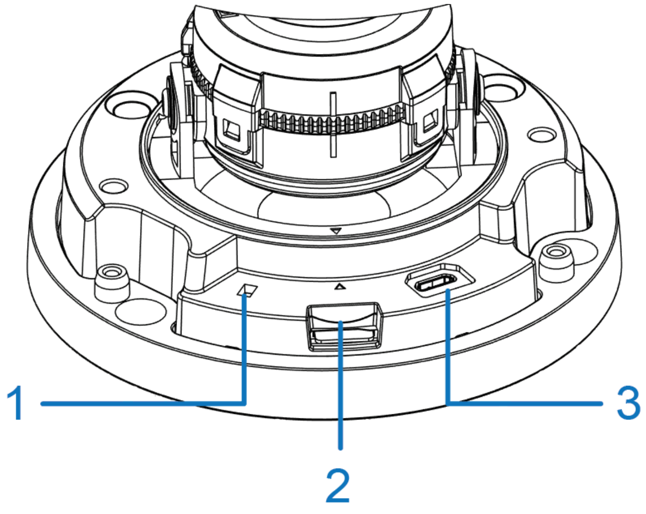
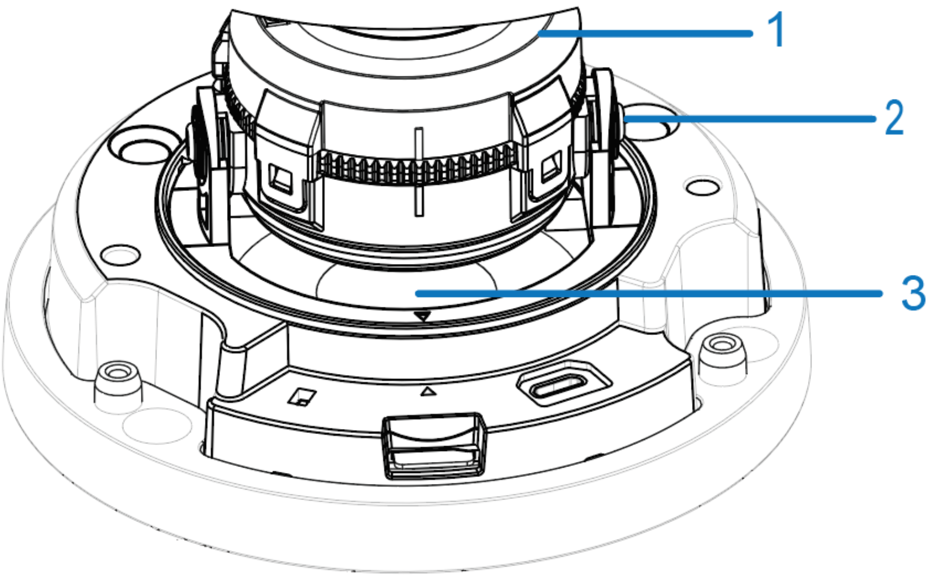


Table 6 Camera buttons and connections descriptions

Camera button / connections	Description
1	Reset button • Hold for 5 seconds for soft reset • Hold for 20 seconds for hard reset
2	Micro SD card
3	USB cable connection

Figure 7 Adjusting the camera position



1 **Rotate:** The rotate range of the 3-axis gimbal is 0° to a minimum of 355°

2 **Tilt:** The tilt range of the 3-axis gimbal is 0° to 67°.

3 **Pan:** The pan range of the 3 axis gimbal is 0° to 355°.

Table 8 Mounting plate symbols and descriptions

Symbol	Name	Description
A	Single Gang Box	Attach the plate to a North American single gang electrical box
B	Octagon Box	Attach the plate to a North American octagon electrical box
C	Double Gang Box	Attach the plate to a North American double gang electrical box
D	4S Junction Box	Attach the plate to a North American 4 inch square electrical box

Warnings

- This product is intended for professional installation, please follow local wiring regulations.
- To meet EU security immunity requirements this product should be used with an Uninterruptable Power Supply to feed the mains input of any power adaptor.

- The product should be powered by a limited power supply (LPS) sized according to the product rating label.
- The LAN symbol on the unit means this is not intended for connection to a
- public network or a LAN from a different building.
- Do not install where children are likely to have access.
- For outdoor use the camera should be mounted at least 3m above ground level.

Illustra Flex Gen 3 3MP and 8MP Indoor Bullet Cameras

Product features

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

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

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

Product overview

This chapter explains the features and installation of the Illustra Flex Gen 3 Indoor Bullet cameras. Product code and description of the camera is provided in the table below.

Table 9 Product code and description of the Illustra Flex Bullet cameras

Product Code	Model Name	Description
IFS03-B21-OI03	Illustra Flex3 3MP Bullet	Illustra Flex Gen 3, 3MP Bullet, 3.2-10mm, indoor, clear bubble, white, TDN w/IR, Multi-Exposure WDR
IFS08-B22-OI03	Illustra Flex3 4K Bullet	IIllustra Flex Gen 3, 8MP Bullet, 4.17-9.48mm, indoor, clear bubble, white, TDN w/IR, Multi-Exposure WDR

In the box

- 1 x Bullet camera
- 1 x Mounting template sticker
- 1 x Mounting plate
- 4 x 50x4mm tapping screws
- 4 x 40x6mm plastic screw anchors
- 1 x Cap installer
- 1 x Cable bush
- 1 x Printed Quick Start Guide
- 1 x Torx driver

Installation tools

- 1 x Philips Screw Driver
- 1 x ‘L' type wrench
- 1 x Drill

Figure 10 Camera parts

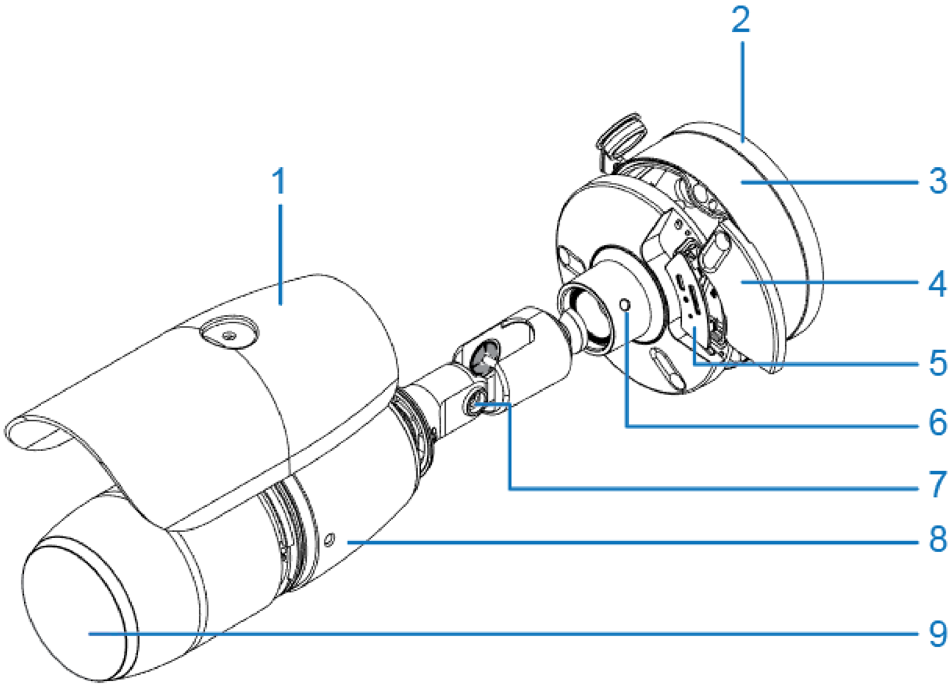


Table 11 Camera part descriptions

Camera part	Description
1	Sun shield cover
2	Mounting plate
3	Camera base
4	Camera buttons cover
5	Camera Buttons
6	Tilt Adjustment body
7	Pan Adjustment body
8	Camera body
9	Camera lens

Quick reference

- Default IP: 192.168.1.168 (DHCP enabled)
- Default Username / Password: admin
- Power: AC24V / PoE 802.3af

Procedure 2 Mounting and powering up the camera

Step Action

1 Place the mounting template sticker on the surface that you want to attach the camera.

2 On the surface drill four Ø 5mm holes and cut out two Ø 23mm cable holes as per the markings identified on the mounting template sticker.

3 Securely place the four screw anchors into the four Ø 5mm holes.

4 Hold the mounting plate (2) (Figure 10) up to the surface and align the holes on the mounting plate with the Ø 5mm holes and securely attach the mounting plate to the surface with the four screws.

5 Unscrew the three screws on the camera base (3) (Figure 10) to remove the camera from the camera base.

Note: To fully disconnect the camera from the camera base you must disconnect the safety wire from the 'arrow' in the camera base.

6 Insert the PoE cable or AC24V cable through one of the cable holes on the camera base.

Note: Ensure that the rubber plugs on the cable is correctly inserted into the cable hole on the camera base.

7 You must run the cable through the cable side entry hole on the camera base or through the hole on the mounting surface before you attach the camera base to the mounting plate.

- If you decided to use the cable hole on the mounting surface then place the cable through the hole and securely attach the camera base to the mounting plate with the three screws.
- If you decided to use the cable side entry slot on the camera base then unscrew the mounting plate and remove the screw holding the cable side entry cover in place. Then insert the cable through the cable side entry slot and securely attach the mounting plate to the surface.

8 Hold the camera up to the mounting plate and securely connect the safety wire in the camera to the 'arrow' in the camera base.

9 Connect the PoE cable to the PoE slot on the camera or the AC24V cable to the AC24 connection on the camera.

10 Securely attach the camera body (8) (Figure 10) to the camera base with the three screws.

11 Connect the 24Vac cable to the AC 24V terminal or connect the RJ-45 jack to a PoE compatible network device that supplies power through the Ethernet cable.

- End -

Figure 12 Camera buttons and connections

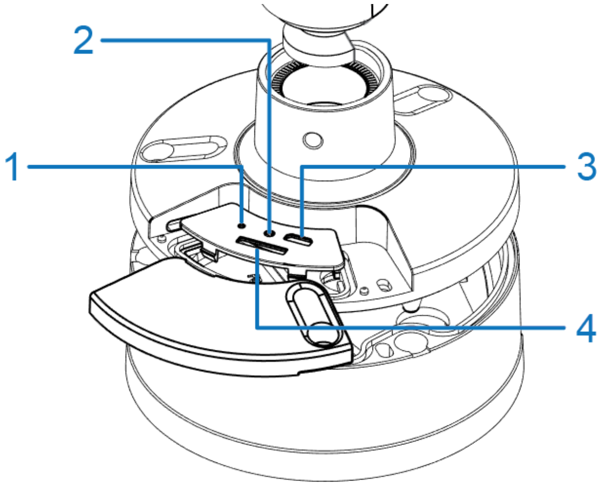


Figure 13 Camera buttons and connections

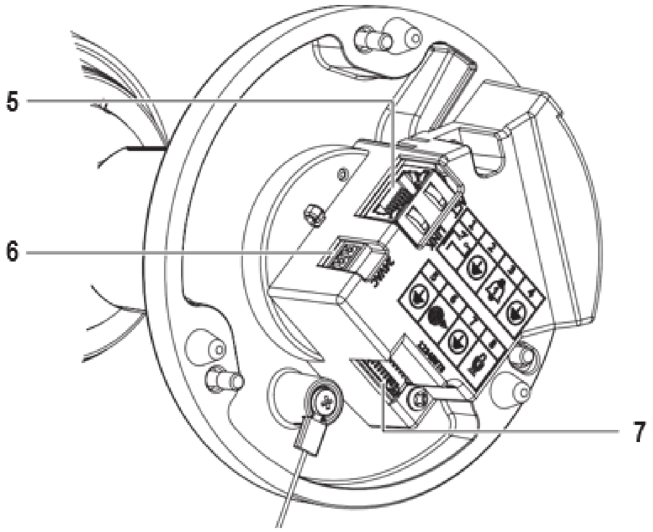


Table 14 Camera buttons and connections descriptions

Camera button / connection	Description
1	Focus button • Hold for 3 seconds to run one touch focus
2	Factory reset • Hold for 5 seconds for soft reset • Hold for 20 seconds for hard reset
3	USB cable connection
4	Micro SD card slot

5	PoE cable slot
6	AC cable connection
7	Audio / Alarm cable connection

Procedure 3 Adjusting the camera position

Step **Action**

1 Use the ‘L’ type wrench to:

a Unlock the screw (6) (Figure 10) and tilt the camera body.

b Unlock and screw (7) (Figure 10) and rotate the camera body.

Note: You must securely attach both screws to ensure that the camera holds the modified position.

- End -

Procedure 4 Adjusting the sun shield

Step **Action**

1 Loosen the thumb-screw on the sun-shield cover (1) (Figure 10) to move the sun shield cover forward and backward over the camera body.

Note: You must securely lock the sun shield thumb-screw to ensure that the covers holds the modified position.

- End -

Warnings

- This product is intended for professional installation, please follow local wiring regulations.
- To meet EU security immunity requirements this product should be used with an Uninterruptable Power Supply to feed the mains input of any power adaptor.
- The product should be powered by a limited power supply (LPS) sized according to the product rating label.
- The LAN symbol on the unit means this is not intended for connection to a
- public network or a LAN from a different building.
- Do not install where children are likely to have access.
- For outdoor use the camera should be mounted at least 3m above ground level.

Illustra Flex Gen 3 3MP Indoor Dome Cameras

This chapter provides product features, installation procedures, and connection information regarding the Illustra Flex Series Indoor Dome cameras.

Product features

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

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

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

Product overview

This chapter explains the features and installation of the Illustra Flex Gen 3 Indoor Dome cameras. Product code and description of the camera is provided in the table below.

Table 15 Product code and description of the Illustra Flex Indoor Dome cameras

Product Code	Model Name	Description
IFS03-D21-AT03	Illustra Flex3 3MP Indoor Dome	Illustra Flex Gen 3, 3MP Dome, 3.2-10mm, indoor, clear bubble, white, TDN, Multi-Exposure WDR
IFS08-D22-AT03	Illustra Flex3 3MP Indoor Dome	Illustra Flex Gen 3, 8MP Dome, 4.17-9.48mm, indoor, clear bubble, white, TDN, Multi-Exposure WDR

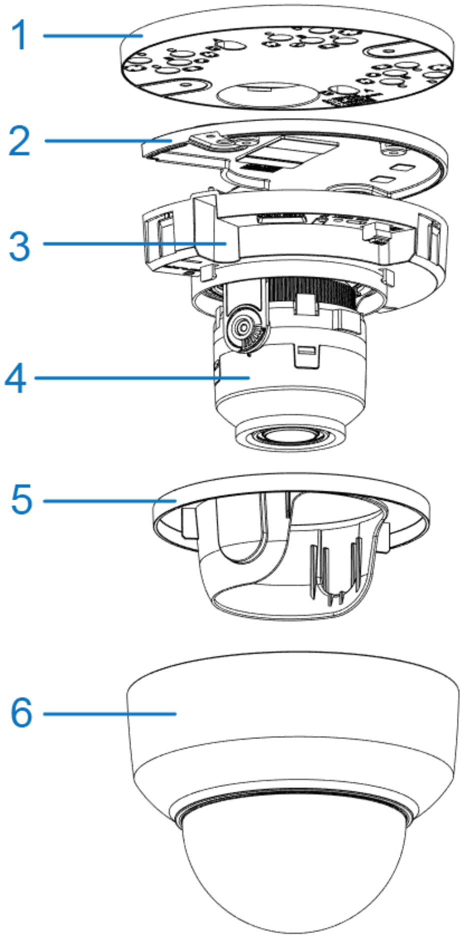
In the box

- 1 x Indoor dome camera
- 1 x Mounting template sticker
- 1 x Mounting plate
- 2 x 50x4mm tapping screws
- 2 x 40x6mm plastic screw anchors
- 2 x 10x4mm mounting plate screws
- 1 x Printed Quick Start Guide

Installation tools

- 1 x Drill
- 1 x Screw Driver

Figure 16 Camera parts



Quick reference

- Default IP: 192.168.1.168 (DHCP enabled)
- Default Username / Password: admin
- Power: AC24V / PoE 802.3af

Table 17 Camera part descriptions

Camera Part	Description
1	Mounting plate
2	Camera base
3	Camera body
4	Camera lens
5	Camera lens cover
6	Dome cover

Procedure 5 Mounting and powering up the camera

Step **Action**

1 Place the mounting template sticker on the surface that you want to attach the camera.

2 On the surface drill two Ø 6mm holes and cut out a cable hole as per the markings identified on the mounting template sticker.

3 Securely place the two screw anchors into the two Ø 6mm holes.

4 Hold the camera dome with one hand and rotate the camera base to unlock it and remove it from the dome.

Note: The camera dome includes a ‘lock’ and ‘unlock’ symbol to assist with step 4.

5 Gently pull up and remove the camera lens cover (5) (Figure 16) to easily access the cable connections and buttons.

6 Connect the PoE cable to the PoE slot on the camera or the AC24V cable to the AC24 connection on the camera.

7 Before you secure the mounting plate (1) (Figure 16) to the camera base (2) (Figure 16) you must place the cable through the cable hole on the camera mounting plate.

8 Place the mounting plate onto the camera base so that the three semicircular swellings on the mounting plate fit correctly into the three screw holes on the camera base.

9 Place the cable through the cable hole on the mounting surface.

10 Hold the mounting plate with camera base up to the mounting template and align two screw holes on the camera base with the two screw holes on the mounting surface.

11 Insert the two screws into the two holes on the camera base and securely attach the mounting plate and camera base to the surface.

12 Insert the camera lens cover (5) (Figure 16) on to the camera lens.

13 Hold the camera dome (6) (Figure 16) up to the camera base and rotate the camera dome to securely lock it to the camera base.

Note: The camera dome includes a ‘lock’ and ‘unlock’ symbol to assist with step 13.

14 Connect the AC 24V cable to an AC 24V terminal or connect the RJ-45 jack to a PoE compatible network device that supplies power through the Ethernet cable.

- End -

Figure 18 Camera buttons and connections

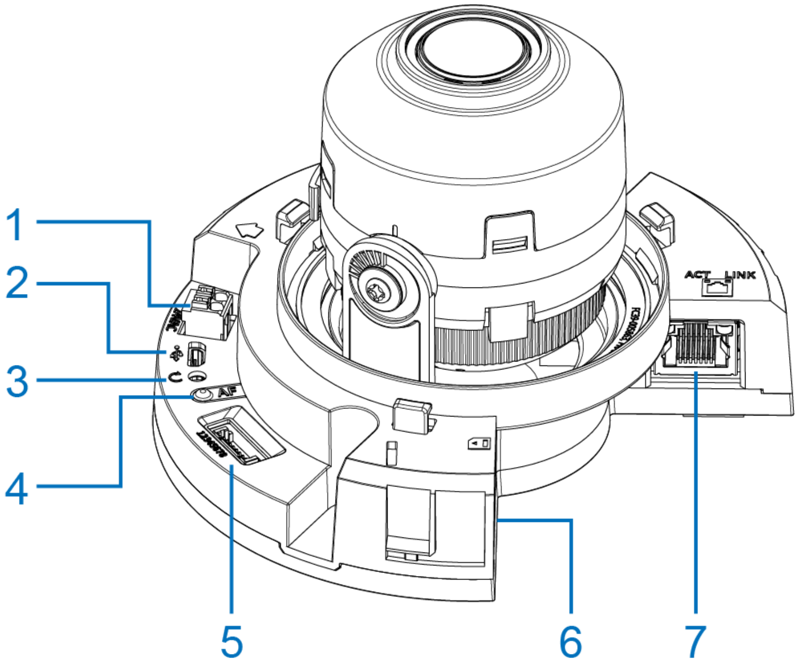
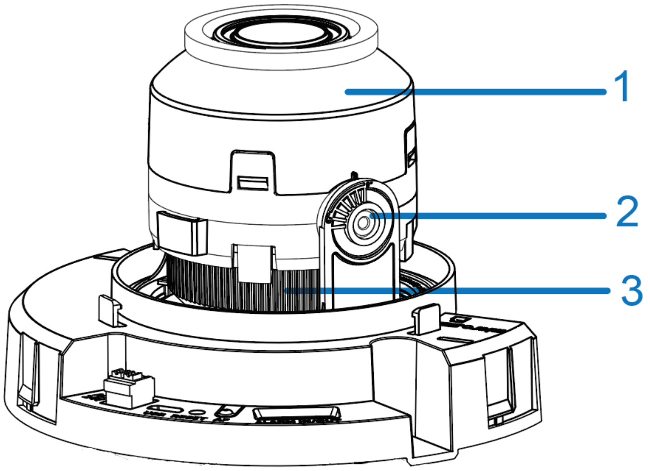


Table 19 Camera buttons and connections descriptions

Camera buttons / connections	Description
1	AC cable connection
2	USB cable connection
3	Factory reset • Hold for 5 seconds for soft reset • Hold for 20 seconds for hard reset
4	Focus button • Hold for 3 seconds to run one touch focus
5	Audio / Alarm cable connection
6	Micro SD card insert
7	PoE cable slot

Figure 20 Adjusting the camera position



1 **Rotate:** The rotate range of the 3-axis gimbal is 0° to a minimum of 355°

2 **Tilt:** The tilt range of the 3-axis gimbal is 0° to 67°.

3 **Pan:** The pan range of the 3 axis gimbal is 0° to 355°.

Table 21 Mounting plate symbols and descriptions

Symbol	Name	Description
A	Single Gang Box	Attach the plate to a North American single gang electrical box.
B	Octagon Box	Attach the plate to a North American octagon electrical box
C	Double Gang Box	Attach the plate to a North American double gang electrical box.
D	4S Junction Box	Attach the plate to a North American 4 inch square electrical box.

Procedure 6 Removing or attaching the dome cover

To remove the dome:

- Hold the camera dome (6) (Figure 16) with one hand and rotate the camera base (2) (Figure 1) to unlock it and remove it from the dome.

Note: The camera dome includes a ‘lock’ and ‘unlock’ symbol to assist with the above step.

To install the dome:

- Hold the camera dome (6) (Figure16) up to the camera base (2) (Figure 16) and rotate the camera dome to securely lock it to the camera base.

Note: The camera dome includes a ‘lock’ and ‘unlock’ symbol to assist with the above step.

- End -

Warnings

- This product is intended for professional installation, please follow local wiring regulations.
- To meet EU security immunity requirements this product should be used with an Uninterruptable Power Supply to feed the mains input of any power adaptor.
- The product should be powered by a limited power supply (LPS) sized according to the product rating label.
- The LAN symbol on the unit means this is not intended for connection to a
- public network or a LAN from a different building.
- Do not install where children are likely to have access.

Illustra Flex Gen 3 3MP and 8MP Outdoor Dome Cameras

This chapter provides product features, installation procedures, and connection information regarding the Illustra Flex Series Outdoor Dome cameras.

Product features

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

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

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

Product overview

This chapter explains the features and installation of the Illustra Flex Gen 3 Outdoor Dome cameras. Product code and description of the camera is provided in the table below.

Table 22 Product code and description of the Illustra Flex Outdoor Dome cameras

Product Code	Model Name	Description
IFS03-D21-OI03	Illustra Flex3 3MP Outdoor Dome	Illustra Flex Gen 3, 3MP Dome, 3.2-10mm, outdoor, clear bubble, white, TDN w/IR, Multi-Exposure WDR
IFS08-D22-OI03	Illustra Flex3 4K Outdoor Dome	Illustra Flex Gen 3, 8MP Compact, 4.17-9.48mm, outdoor, clear bubble, white, TDN w/IR, Multi-Exposure WDR

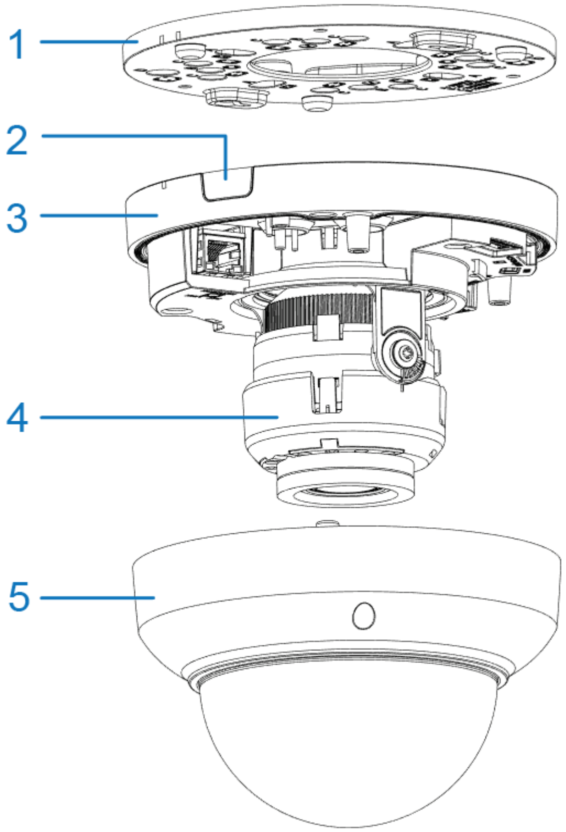
In the bo

- 1 x Dome camera
- 1 x Mounting template sticker
- 1 x Mounting plate
- 3 x 10x4mm mounting plate screws
- 3 x 40x6mm plastic screws anchors
- 3 x 50x4mm tapping screws
- 1 x Cap Installer
- 1 x Cable Bush
- 1 x Printed Quick Start Guide
- 1 x Torx driver
- 1 x Safety wire
- 2 x 8x3mm screw

Installation tools

- 1 x Screw Driver
- 1 x Torx driver
- 1 x Drill

Figure 23 Camera parts



Quick reference

- Default IP: 192.168.1.168 (DHCP enabled)
- Default Username / Password: admin
- Power: AC24V / PoE 802.3af

Table 24 Camera part descriptions

Camera Part	Description
1	Mounting plate
2	Camera side entry
3	Camera base
4	Camera lens
5	Dome cover

Procedure 7 Mounting and powering up the camera

Step Action

1 Place the mounting template sticker on the surface that you want to attach the camera.

2 On the surface drill three Ø 6mm holes, cut out a larger Ø 60mm cabling hole and triangle as per the markings identified on the mounting template sticker.

3 Securely place the three screw anchors into the three Ø 6mm holes.

4 Unscrew the three screws on the camera dome (5) (Figure 23) to remove the dome from the camera base (3) (Figure 23).

5 Insert the PoE cable or AC24V cable through the hole on the camera base.

Note: Ensure that the rubber plugs on the cable is correctly inserted into the cable hole on the camera base.

6 Connect the PoE cable to the PoE slot on the camera.

OR

Connect the AC24V cable to the AC24 connection on the camera.

7 Before you lock the mounting plate (1) (Figure 23) to the camera base you must place the cable through the cable side entry slot on the camera base (2) (Figure 23) or through the cable hole in the camera mounting plate.

- When using the cable side entry slot you must first remove the cable side entry screw that holds the cable side entry cover in place.
- If the cable is placed through the hole on the camera mounting plate then insert the cable through the hole on the mounting surface.

8 Place the camera base onto the mounting plate and rotate the camera base to lock it to the mounting plate.

Note: The mounting plate includes a ‘lock’ and ‘unlock’ symbol to assist with step 7.

9 Hold the mounting plate with camera base up to the mounting template and align the three holes on the mounting template with the three holes on the camera base.

10 Insert the three screws into the three holes on the camera base and securely attach the mounting plate and camera base to the surface.

11 Cover the camera with the dome cover and securely attach the dome to the camera with the three screws.

12 Connect the AC24V cable to the AC 24V terminal or connect the RJ-45 jack to a PoE compatible network device that supplies power through the Ethernet cable.

- End -

Figure 25 Camera buttons and connections

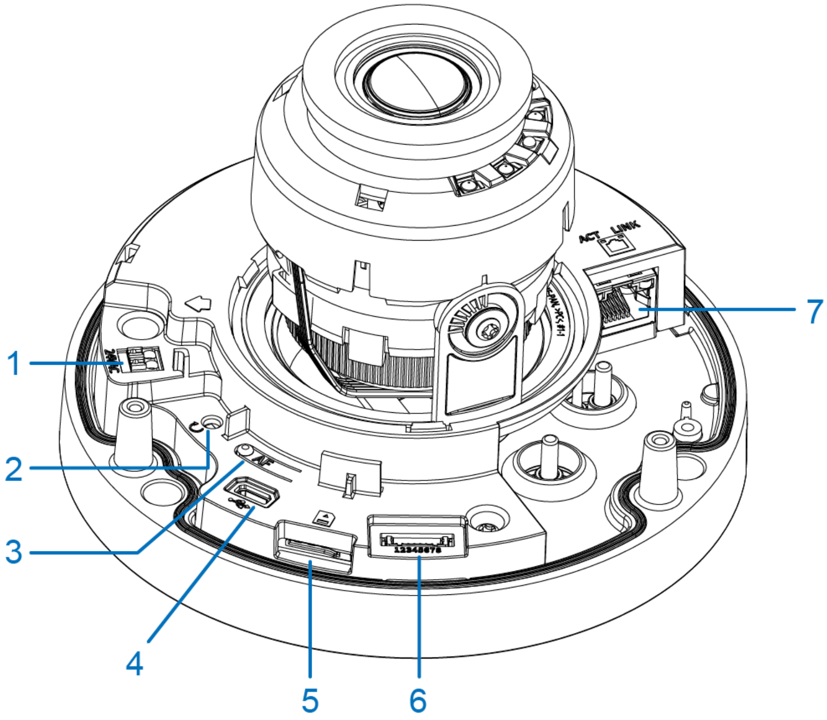
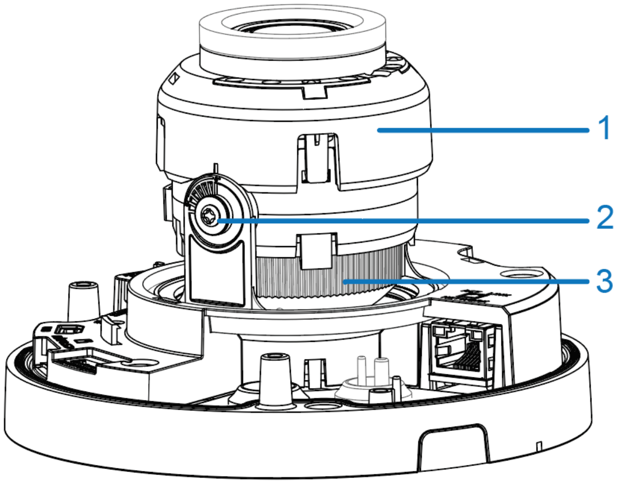


Table 26 Camera buttons and connections descriptions

Camera buttons / connections	Description
1	AC cable connection
2	Factory reset • Hold for 5 seconds for soft reset • Hold for 20 seconds for hard reset
3	Focus button • Hold for 3 seconds to run one touch focus
4	USB cable connection
5	Micro SD card slot
6	Audio / Alarm cable connection
7	PoE cable slot

Figure 27 Adjusting the camera position



1 **Rotate:** The rotate range of the 3-axis gimbal is 0° to a minimum of 355°.

2 **Tilt:** The tilt range of the 3-axis gimbal is 0° to 67°.

3 **Pan:** The pan range of the 3 axis gimbal is 0° to 355°.

Table 28 Mounting plate symbols and descriptions

Symbol	Name	Description
A	Single Gang Box	Attach the plate to a North American single gang electrical box.
B	Octagon Box	Attach the plate to a North American octagon electrical box
C	Double Gang Box	Attach the plate to a North American double gang electrical box.
D	4S Junction Box	Attach the plate to a North American 4 inch square electrical box.

Warnings

- This product is intended for professional installation, please follow local wiring regulations.
- To meet EU security immunity requirements this product should be used with an Uninterruptable Power Supply to feed the mains input of any power adaptor.
- The product should be powered by a limited power supply (LPS) sized according to the product rating label.
- The LAN symbol on the unit means this is not intended for connection to a
- public network or a LAN from a different building.
- Do not install where children are likely to have access.
- For outdoor use the camera should be mounted at least 3m above ground level.

Network Topology

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

The following images illustra the network topologies of the cameras.

Indoor and Outdoor Dome Camera Topology

Figure 29 Dome Cameras Network Topology Type I.

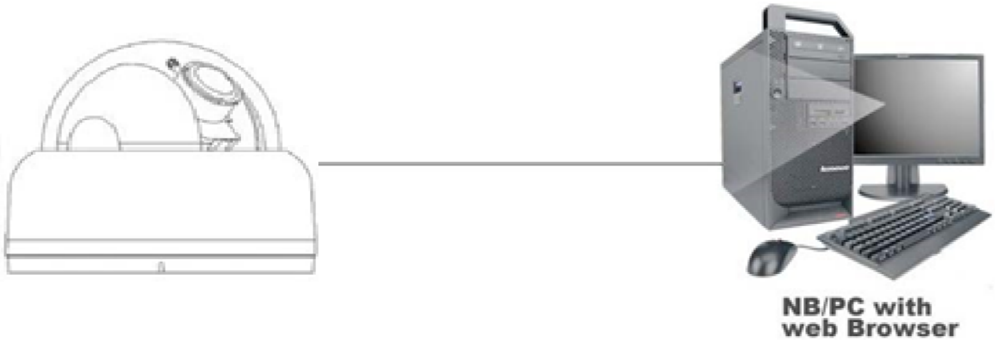
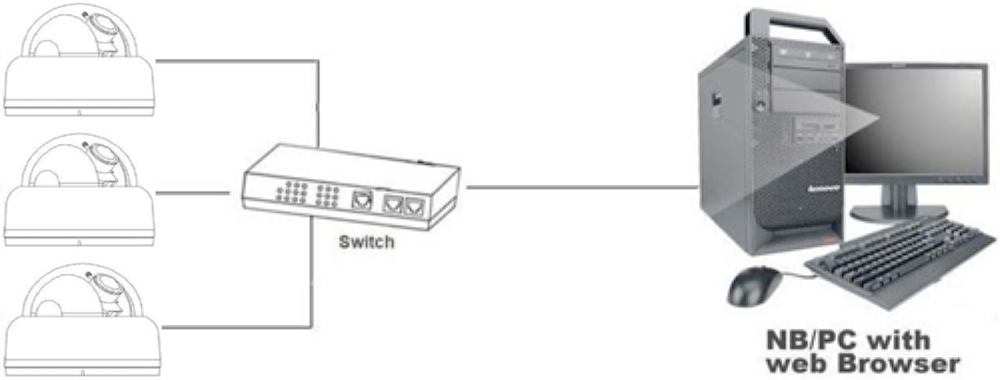


Figure 30 Dome Cameras Network Topology Type II



Bullet Camera Topology

Figure 31 Illustra Flex Bullet Camera Network Topology Type I

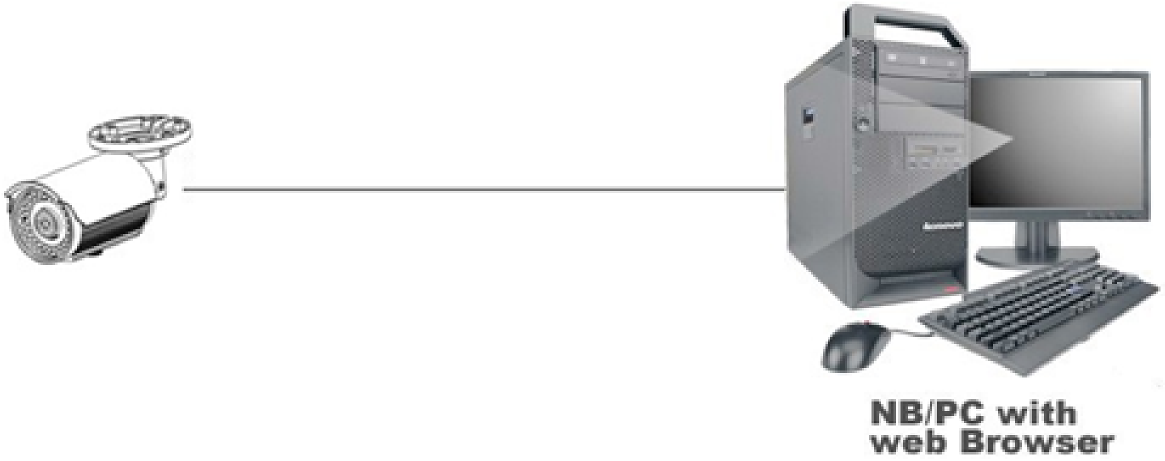
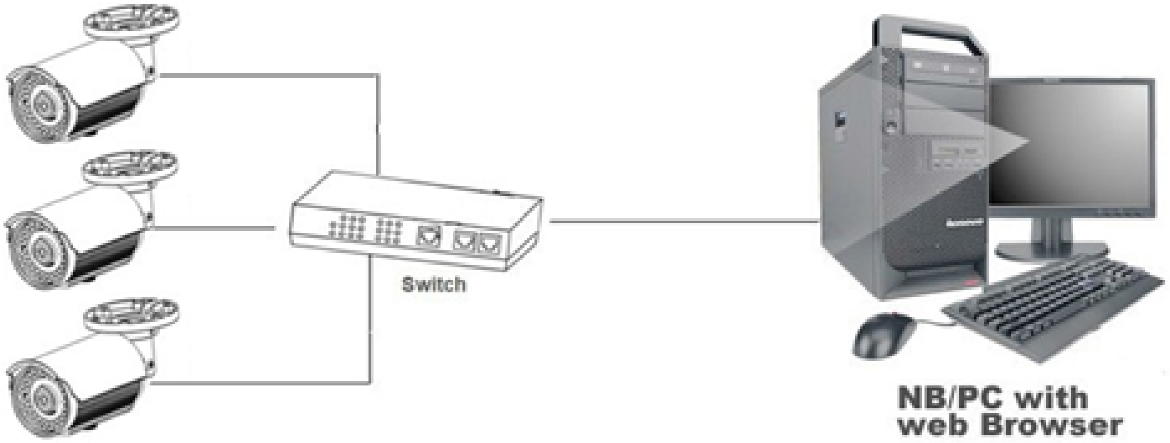


Figure 32 Illustra Flex Bullet Camera Network Topology Type II



Compact Mini Dome Camera 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 33 Compact Mini Dome Cameras Network Topology Type I

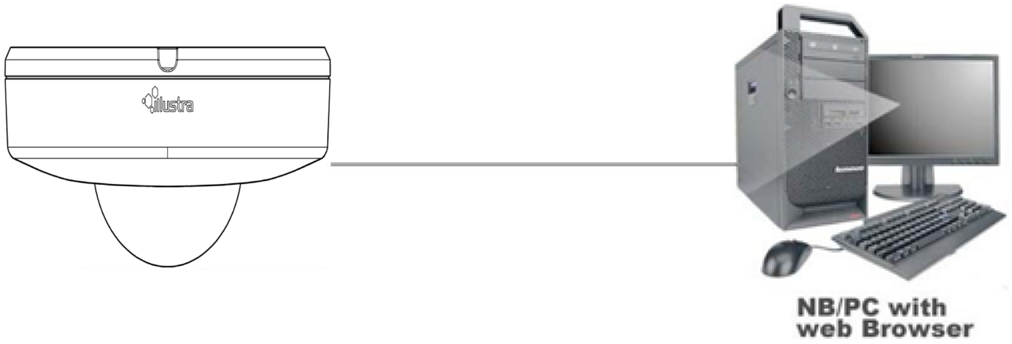
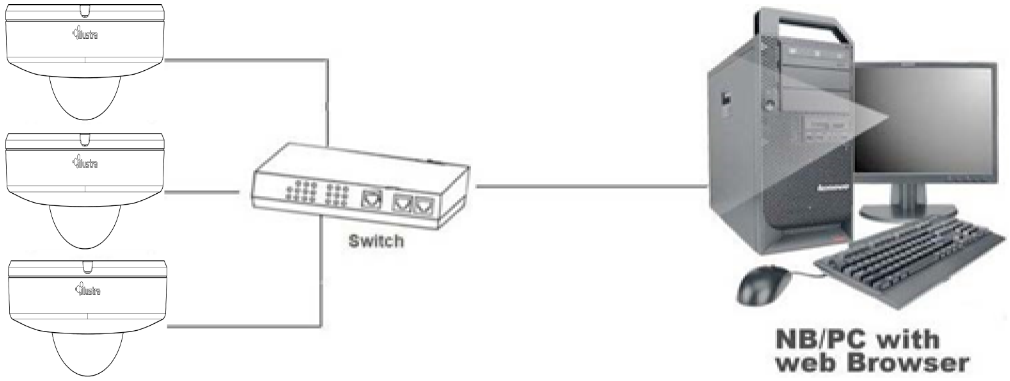


Figure 34 Compact Mini Dome Cameras Network Topology Type II



Network Connection

Default IP Address

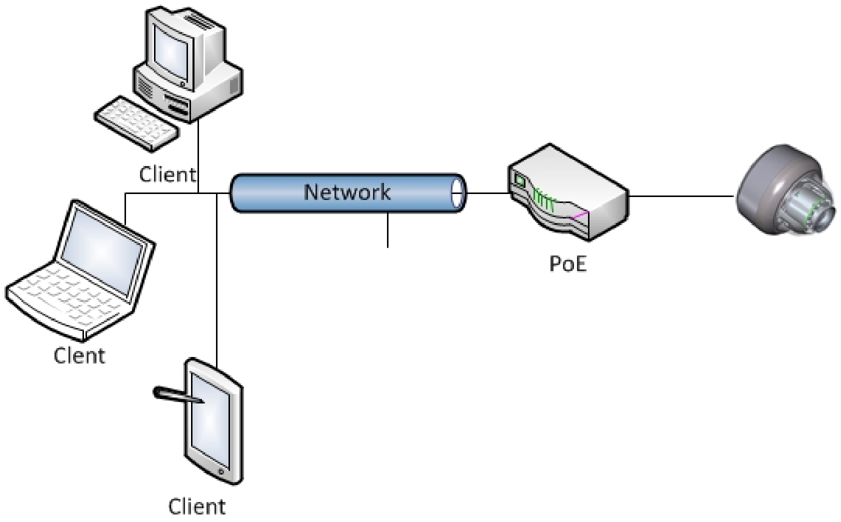
Since this is a network-based unit, an IP address must be assigned at the very first bootup. The default IP address of the unit is 192.168.1.168 and sub mask is 255.255.255.0.

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 35 Network connection diagram



Default camera settings

The following table describes the default camera settings.

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

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

Procedure 8 Connecting from a computer

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

- End -

DHCP

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

Procedure 9 Enable DHCP

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

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

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

- End -

Procedure 10 Disable DHCP

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

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

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

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

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

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

- End -

Managing cameras with the Illustra Connect tool

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

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

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

Refer to Configuration on page 37 for further information regarding using the Illustra Connect tool for configuring the cameras.

Procedure 11 Connecting to the camera using Illustra Connect

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

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

- End -

Procedure 12 Connecting to the camera using the static IP address

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

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

- End -

Procedure 13 Logging on to the camera web user interface

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

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

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 14 Enabling the correct video orientation for a wall mounted camera

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

- End -

Configuration

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

Security Mode Profiles for First Time Connection

The Illustra Flex 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 38 for further information regarding the differences between Standard and Enhanced Security modes.

Accessing the Illustra Flex 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 33 for details on how to connect the camera to your network or computer.
2	When you select the camera, the sign in page displays.
3	Select your preferred language from the drop-down menu. The default language is English.
4	Enter the default username and password when prompted - Username: admin, Password: admin.
5	Click **Log in**. The camera Web User Interface displays. The first time that you access the camera, or after a factory reset, you are prompted to **Define a Host ID** and **Select a Security Type**. • **Define a Host ID**: The admin user must enter a 6 character code for the Host ID that includes both letters and/or numbers. This unique password can be used to access the operating system files. The HostID is not stored on the camera for security reasons and must be presented to Illustra Technical Support when remote access to the operating system is required. • **Select a Security Type**: Standard Security or Enhanced Security.
6	If you select the Standard Security option, password change is mandatory.

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

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

Note: The password must meet the following requirements:
Be a minimum of eight characters long.

Have at least one character from each of the following character groups:
• Upper-case letters - ABCDEFGHIJKLMNOPQRSTUVWXYZ
• Lower-case letters - abcdefghijklmnopqrstuvwxyz
• Numeric characters - 0123456789
• Special characters - @ % + \ / ‘ ! # $ ^ ? : , ( ) { } [ ] ~ - _ `

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

- End -

Summary of Security Modes

Standard Security:

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

Enhanced Security:

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

Changing the Camera Web User Interface Language

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

Procedure 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.

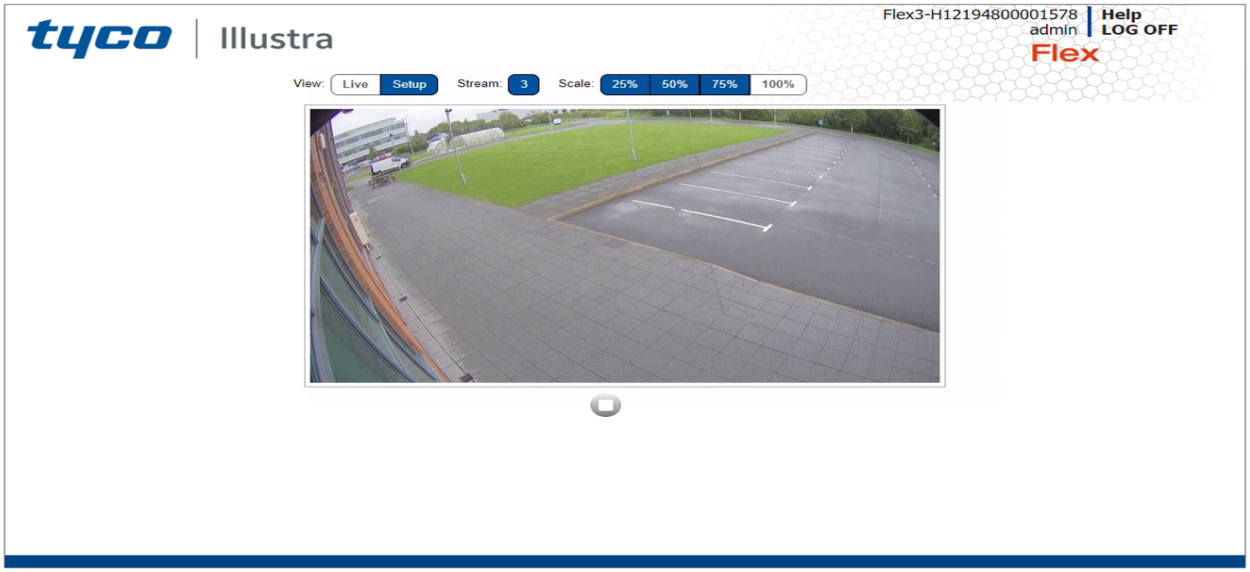
The camera web User Interface displays in the selected language.

- End -

Live menu

When you log in to the Illustra Web User Interface, the **Live** menu appears, as seen in Figure 36 on page 40.

Figure 36 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%.

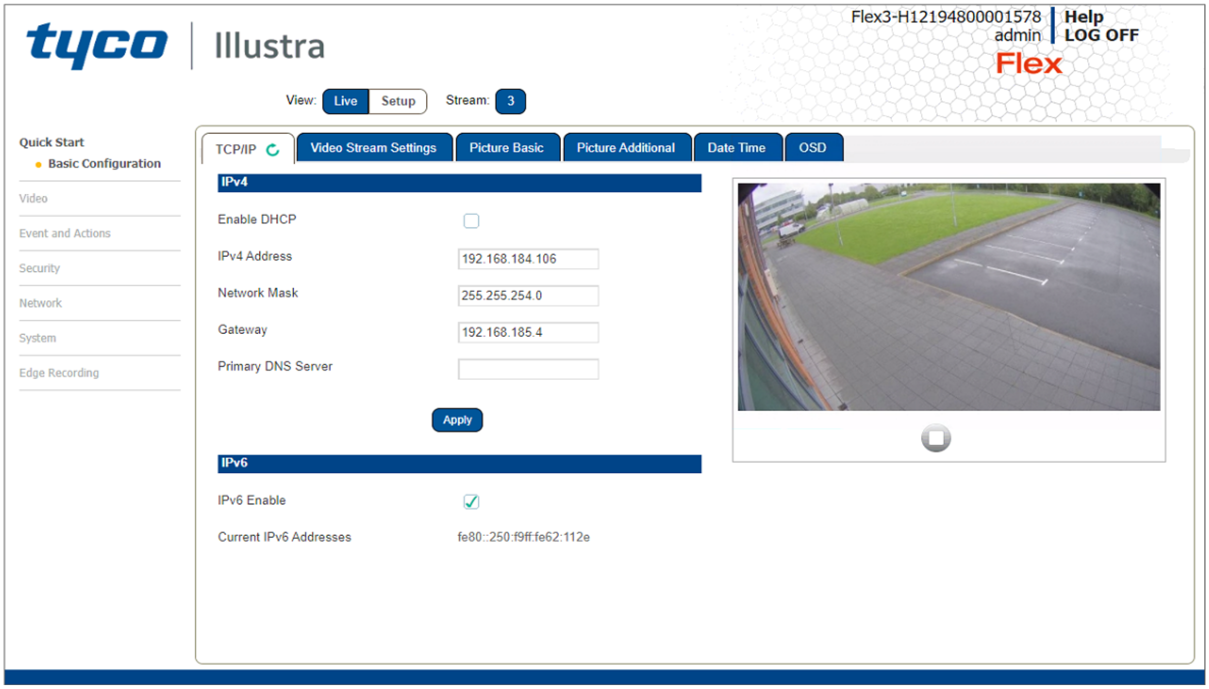
- End -

Quick Start Menu

When you select the Quick Start menu, the Basic Configuration Page displays, as shown in Figure 37 on page 41.

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

Figure 37 Basic Configuration Menu



Enable DHCP □

IPv4 Address 192.168.184.106

Network Mask 255.255.254.0

Gateway 192.168.185.4

Primary DNS Server

IPv6 Enable ☑

Current IPv6 Addresses fe80::250:f9ff:fe62:112e

Basic Configuration

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

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

TCP/IP

Configure the IPv4 and IPv6 network settings on the camera.

Note: When you perform a factory reset or reboot the unit searches for the last known IP address. If this is not available it reverts to the default IP address of 192.168.1.168. This could result in duplicate IP addresses. Refer to Quick Start Menu on page 41 for more information.

DHCP

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

Procedure 18 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 19 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 20 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 21 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 22 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 continue 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 Image Source selected. **Note:**See Appendix C for all streaming combinations.

Table 38 3MP Camera Stream Set (all resolution, codes and frame rate combinations of Stream 1, 2 and 3 are valid)

		Normal Mode				
		Resolution	Description	Max FPS		
				TWDR Off	TWDR 2x	TWDR 3x
Stream 1	H.264 H.265 H.264 IntelliZip H.265 IntelliZip MJPEG	2048x1536 1920x1080 1664x936 1280x720	4:3 (1080p) 16:9 (HD+) 16:9 (720p) 16:9	30 60 60 60	30 30 30 30	20 20 20 20
Stream 2	H.264 H.265 H.264 IntelliZip H.265 IntelliZip MJPEG	1280x720 1024x576 640x480 640x360 480x360 384x288	(720p) 16:9 (PAL+) 16:9 4:3 (mHD) 16:9 4:3 4:3	30*1 30*1 30*1 30*1 30*1 30*1	30 30 30 30 30 30	20 20 20 20 20 20
Stream 3	MJPEG	640x360 480x360 384x288	(mHD) 16:9 4:3 4:3	15 15 15	15 15 15	15 15 15

Note:*1 Streams 2 and 3 are restricted to 15 FPS when Stream 1 is greater than 30 FPS.

Note:*2 Streams 1 and 2 are restricted to 30 FPS when TrueWDR 2x is enabled.

Note:*3 Streams 1 and 2 are restricted to 20 FPS when TrueWDR 3x is enabled.

Note:*4 The maximum frame rate of any stream is 30 FPS when corridor mode is enabled.

Note:*5 The maximum frame rate of any stream is 30 FPS when corridor mode is enabled.

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

Table 39 3MP Camera Stream Set (all resolution, codes and frame rate combinations of Stream 1, 2 and 3 are valid)

		Corridor Mode				
		Resolution	Description	Max FPS		
				TWDR Off	TWDR 2x	TWDR 3x
Stream 1	H.264 H.265 H.264 IntelliZip H.265 IntelliZip MJPEG	2048x1536	4:3	30	30	20
		1920x1080	(1080p) 16:9	30	30	20
		1664x936	(HD+) 16:9	30	30	20
		1280x720	(720p) 16:9	30	30	20
Stream 2	H.264 H.265 H.264 IntelliZip H.265 IntelliZip MJPEG	1280x720	(720p) 16:9	30*1	30	20
		1024x576	(PAL+) 16:9	30*1	30	20
		640x480	4:3	30*1	30	20
		640x360	(mHD) 16:9	30*1	30	20
		480x360	4:3	30*1	30	20
		384x288	4:3	30*1	30	20
Stream 3	MJPEG	640x360	(mHD) 16:9	15	15	15
		480x360	4:3	15	15	15
		384x288	4:3	15	15	15

Note:*1 Streams 2 and 3 are restricted to 15 FPS when Stream 1 is greater than 30 FPS.

Note:*2 Streams 1 and 2 are restricted to 30 FPS when TrueWDR 2x is enabled.

Note:*3 Streams 1 and 2 are restricted to 20 FPS when TrueWDR 3x is enabled.

Note:*4 The maximum frame rate of any stream is 30 FPS when corridor mode is enabled.

Note:*5 The maximum frame rate of any stream is 30 FPS when corridor mode is enabled.

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

Table 40 8MP Camera Stream Set (all resolution, codes and frame rate combinations of Stream 1, 2 and 3 are valid)

		Normal Mode				
		Resolution	Description	Max FPS		
				TWDR Off	TWDR 2x	TWDR 3x
Stream 1	H.264 H.265 H.264 IntelliZip H.265 IntelliZip MJPEG	3840x2160	(4K) 16:9	30	25	15
		3264x1840	16:9	30	25	15
		2688x1520	16:9	30	25	15
		1920x1080	(1080p) 16:9	60	25	15
		1664x936	(HD+) 16:9	60	25	15
		1280x720	(720p) 16:9	60	25	15
Stream 2	H.264 H.265 H.264 IntelliZip H.265 IntelliZip MJPEG	1280x720	(720p) 16:9	30*1	25	15
		1024x576	(PAL+) 16:9	30*1	25	15
		960x544	(qHD) 16:9	30*1	25	15
		816x464	16:9	30*1	25	15
		640x360	(mHD) 16:9	30*1	25	15
		480x272	16:9	30*1	25	15
Stream 3	MJPEG	640x360	(mHD) 16:9	30 *1	25	15
		480x272	4:3	30 *1	25	15

Note:*1 Stream 2 is restricted to 15 FPS when Stream 1 is greater than 30 FPS or when Stream 1 resolution is greater than 1920x1080.

Note:*2 Stream 3 is restricted to 10 FPS when Stream 1 is greater than 30 FPS or when Stream 1 resolution is greater than 1920x1080.

Note:*3 All streams are restricted to 25 FPS when TrueWDR 2x is enabled.

Note:*4 All streams are restricted to 15 FPS when TrueWDR 3x is enabled.

Note:*5 The maximum frame rate of any stream is 30 FPS when corridor mode is enabled.

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

Table 41 8MP Camera Stream Set (all resolution, codes and frame rate combinations of Stream 1, 2 and 3 are valid)

		Corridor Mode				
		Resolution	Description	Max FPS		
				TWDR Off	TWDR 2x	TWDR 3x
Stream 1	H.264 H.265 H.264 IntelliZip H.265 IntelliZip MJPEG	3840x2160	(4K) 16:9	30	25	15
		3264x1840	16:9	30	25	15
		2688x1520	16:9	30	25	15
		1920x1080	(1080p) 16:9	30	25	15
		1664x936	(HD+) 16:9	30	25	15
		1280x720	(720p) 16:9	30	25	15
Stream 2	H.264 H.265 H.264 IntelliZip H.265 IntelliZip MJPEG	1280x720	(720p) 16:9	30*1	25	15
		1024x576	(PAL+) 16:9	30*1	25	15
		960x544	(qHD) 16:9	30*1	25	15
		816x464	16:9	30*1	25	15
		640x360	(mHD) 16:9	30*1	25	15
		480x272	16:9	30*1	25	15
Stream 3	MJPEG	640x360	(mHD) 16:9	30 *1	25	15
		480x272	4:3	30 *1	25	15

Note:*1 Stream 2 is restricted to 15 FPS when Stream 1 is greater than 30 FPS or when Stream 1 resolution is greater than 1920x1080.

Note:*2 Stream 3 is restricted to 10 FPS when Stream 1 is greater than 30 FPS or when Stream 1 resolution is greater than 1920x1080.

Note:*3 All streams are restricted to 25 FPS when TrueWDR 2x is enabled.

Note:*4 All streams are restricted to 15 FPS when TrueWDR 3x is enabled.

Note:*5 The maximum frame rate of any stream is 30 FPS when corridor mode is enabled.

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

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

The settings for the 3MP cameras are:

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

The settings for 8MP cameras are:

- **Stream 1 -** 1 - 15 fps, or 1-60 fps depending on the resolution. Default is 15 fps. 60 fps is only available on Stream 1 with resolution 1920x1080 or lower.
- **Stream 2 -** 1 - 15 fps, or 1-30 fps depending on the resolution. The default is 15 fps. This stream is limited to 15 fps if stream1 is 60 fps.
- **Stream 3** 7 - 15 fps. The default is 15 fps.

Note:FPS varies depending on other features - refer to the Flex Gen 3 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, Corridor mode, Focus / Zoom and Exposure displayed in the video pane.

Picture Rotation

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

Procedure 23 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 -

Corridor Mode

Provides a better perspective when viewing a long corridor.

Procedure 24 Configure Corridor Mode 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 Play button to start the video stream if it is not already active.

4 Select the required Corridor Mode setting:

- None
- -90°
- +90°

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

- End -

Focus / Zoom

You can configure the focus and zoom using the Web User Interface. You can use the plus and minus arrows to fine tune the image. The Zoom slider bar is used to manually zoom in and out to manually configure to picture. The table below describes the features supported by each camera.

Table 42 Lens features supported for the Indoor and Outdoor Dome, and Bullet cameras

	Indoor Dome	Outdoor Dome	Bullet
Mechanical Focus			
Motorized Focus	X	X	X
Mechanical Zoom			
Motorized Zoom	X	X	X
Lens Calibration	X	X	X
Lens Selection			
Auto One Touch	X	X	X
Configurable Continuous Auto-Focus			

Note: None of the options in Table 99 apply to the Compact Mini Dome.

Procedure 25 Adjust Camera Focus / Zoom

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

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

- End -

Procedure 26 Adjust Camera Focus using OneTouch Autofocus

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

4 In the **Focus/Zoom** section, click the **One Touch** button.The camera refocuses to the zoom level selected for the image.

The video pane updates to display the new settings.

- End -

Picture Basic

Configure the Auto Focus, Exposure, and Wide Dynamic Range (WDR) settings on the camera.

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

Setting Exposure

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

Automatic Gain Control (AGC)

AGC amplifies the video signal in scenes when there is not enough light to produce full video levels. The maximum level of AGC is controlled by the Max Gain control. It is adjustable from 0dB (off) to 37dB. As gain is increased, the sensor noise is also amplified, which can result in more noticeable noise in the image.

Open Shutter

This is a technique that is used for really low light performance applications. It allows the shutter speed to be slowed down further than normal to allow the sensor to collect more light. The maximum level of Open Shutter is controlled by the Shutter Speed control. It is adjustable from 1/30 down to ½ second. The slower the Shutter Speed, the higher the chance for image blur which may affect moving object identification. It is only in effect during low-light situations where an image would not be obtainable otherwise and does not affect the camera performance in normal orbright light situations.

Max Gain

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

Procedure 27 Configure Exposure Settings

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 to ▶ start the video stream if it is not already active.
4	Select a **AGC/Shutter Setting** from the drop-down menu. • **AGC off** - produces the cleanest image with the least noise but the worst low-light performance. • **AGC on** - good low-light performance with the chance for some noise. • **openshutter** - best for low-light performance. However, there is a chance for some noise and some image blur. The default setting is ‘open shutter’.

Note: If you require “Real Time”video, open shutter must be turned off to ensure that the resulting video quality is acceptable for prosecution purposes.

5 If open shutter has been selected in Step 4, Max Exposure will be enabled. Select **Max Exposure (sec)** from the drop-down menu:

- **1/2**
- **1/4**
- **1/8**
- **1/15**
- **1/30**

6 If AGC on or open shutter has been selected in Step 4, Max Gain Exposure will be enabled. Use the slider bar to select the **Max Gain (dB):**

The settings are 0-37.

The video pane will update to display the new settings.

- End -

Exposure

Configure the exposure settings for the camera.

Procedure 28 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:

- **P-Iris**
- **Manual**
- **Shutter Priority**
- **Iris 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 (sec)** from the drop-down menu.
The default setting is 1/8s.

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

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

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

Note: The Iris Level differs depending on the camera.

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

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

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

- End -

Procedure 29 Restore Exposure Defaults

Step Action

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

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

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

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

- End -

Setting Auto Focus

Enable or disable auto focus. When auto-focus is on the camera focuses on the moving object.

Procedure 30 Enable/Disable Auto Focus

Step Action

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

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

3 Select the **Auto Focus** check box to enable auto focus. OR

Deselect the **Auto Focus** check box to disable auto focus.

The default setting is 'Enabled'.

- End -

Picture Additional

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

Wide Dynamic Range

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

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

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

Procedure 31 Disable/Enable Wide Dynamic Range (WDR)

Step Action

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

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

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

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

Note: TrueWDR3x does not apply to 8MP models.

The default setting is OFF.

4 Select the **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.

IR Illuminator

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

Procedure 32 Enable / Disable IR Illuminator

This feature is not supported on the Indoor Dome camera. Refer to product codes for feature support.

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

- End -

Day Night Mode

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

Procedure 33 Configure Day Night Mode

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

- End -

Picture Adjustment

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

Procedure 34 Adjust the 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 1% to 100%. The video pane updates to display the new settings.

- End -

Procedure 35 Restore Picture Balance Defaults

Step **Action**

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

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

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

The default values are:

- **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 36 Configure Auto White Balance

Step Action

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

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

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

The video pane displays the current camera view.

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

- **Auto 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 37 Manually Select White Balance

Step Action

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

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

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

The video pane displays the current camera view.

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

The Red and Blue slider bars display.

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

The live video pane updates to display the new settings.

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

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

- End -

Lens Calibration

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

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

This feature applies only to the Illustra Flex 3MP Indoor Dome, Outdoor Dome, and Bullet cameras.

Procedure 38 Run a Lens Calibration

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

- End -

Date / Time / OSD

Change the camera name, date and time and enable 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 39 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 40 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 41 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 42 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 43 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 44 Display or Hide the User Defined OSD

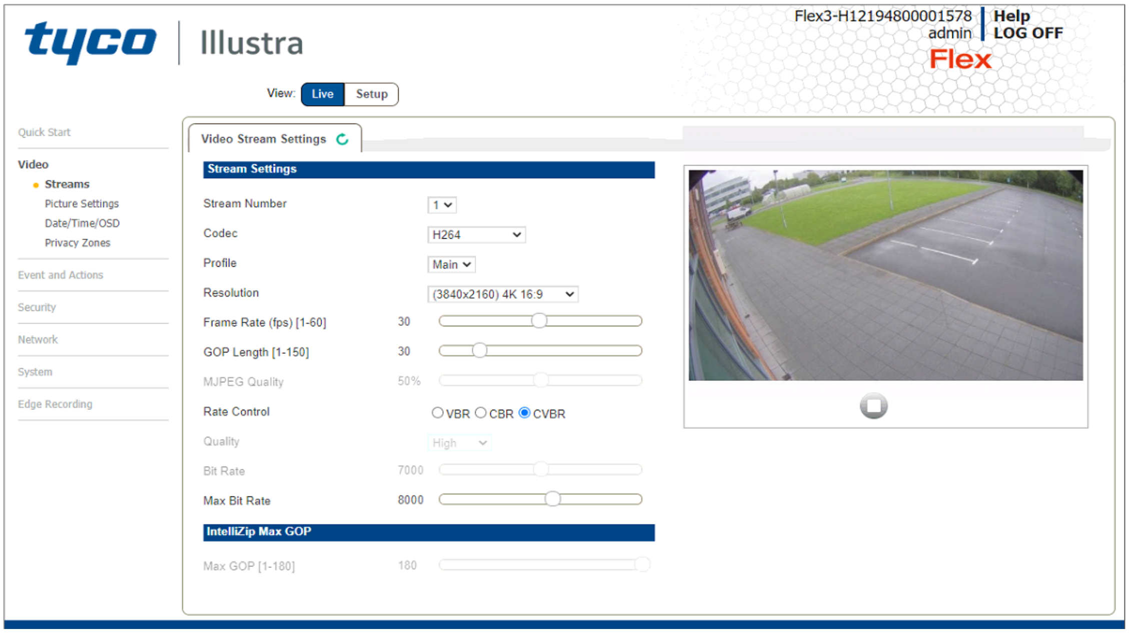
Step	Action
1	Select Setup on the Web User Interface banner to display the setup menus.
2	Select the **OSD** tab in the **Basic Configuration** menu.
3	In the **User Defined** section, select the **Enable** check box to display the camera name in the OSD. OR In the **User Defined** section, clear the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

- End -

Video Menu

When you select the **Video** menu, the **Streams** page displays, as seen in Figure 43 on page 62.

Figure 43 Video Menu



Stream Settings

Stream Number		1
Codec		H264
Profile		Main
Resolution		(3840x2160) 4K 16:9
Frame Rate (fps) [1-60]	30	
GOP Length [1-150]	30	
MJPEG Quality	50%	
Rate Control		○ VBR ○ CBR ● CVBR
Quality		High
Bit Rate	7000	
Max Bit Rate	8000	

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 Micro SD card. User can chose either Stream 1, 2 or 3 to be recorded. When setting up motion detection on the camera, both streams can be used. Alarm Video is configured in the Edge Recording > Record Settings menu.

Integration with other Illustra API Clients

You can configure the 3 video streams through the Web User Interface, as detailed here, or through the Illustra API interface. Changes made to the streams through either method are applied and the video displays according to the configuration.

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

Configuring the Video Stream

Adjust the settings for each video stream.

Procedure 45 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.

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

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

The default setting is ‘Main’.

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

Note: See Appendix C for all streaming combinations.

Table 44 3MP Camera Stream Set (all resolution, codes and frame rate combinations of Stream 1, 2 and 3 are valid)

		Normal Mode				
		Resolution	Description	Max FPS		
				TWDR Off	TWDR 2x	TWDR 3x
Stream 1	H.264 H.265 H.264 IntelliZip H.265 IntelliZip MJPEG	2048x1536 1920x1080 1664x936 1280x720	4:3 (1080p) 16:9 (HD+) 16:9 (720p) 16:9	30 60 60 60	30 30 30 30	20 20 20 20
Stream 2	H.264 H.265 H.264 IntelliZip H.265 IntelliZip MJPEG	1280x720 1024x576 640x480 640x360 480x360 384x288	(720p) 16:9 (PAL+) 16:9 4:3 (mHD) 16:9 4:3 4:3	30*1 30*1 30*1 30*1 30*1 30*1	30 30 30 30 30 30	20 20 20 20 20 20
Stream 3	MJPEG	640x360 480x360 384x288	(mHD) 16:9 4:3 4:3	15 15 15	15 15 15	15 15 15

Note:*1 Streams 2 and 3 are restricted to 15 FPS when Stream 1 is greater than 30 FPS.

Note:*2 Streams 1 and 2 are restricted to 30 FPS when TrueWDR 2x is enabled.

Note:*3 Streams 1 and 2 are restricted to 20 FPS when TrueWDR 3x is enabled.

Note:*4 The maximum frame rate of any stream is 30 FPS when corridor mode is enabled.

Note:*5 The maximum frame rate of any stream is 30 FPS when corridor mode is enabled.

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

Table 45 3MP Camera Stream Set (all resolution, codes and frame rate combinations of Stream 1, 2 and 3 are valid)

		Corridor Mode				
		Resolution	Description	Max FPS		
				TWDR Off	TWDR 2x	TWDR 3x
Stream 1	H.264 H.265 H.264 IntelliZip H.265 IntelliZip MJPEG	2048x1536 1920x1080 1664x936 1280x720	4:3 (1080p) 16:9 (HD+) 16:9 (720p) 16:9	30 30 30 30	30 30 30 30	20 20 20 20
Stream 2	H.264 H.265 H.264 IntelliZip H.265 IntelliZip MJPEG	1280x720 1024x576 640x480 640x360 480x360 384x288	(720p) 16:9 (PAL+) 16:9 4:3 (mHD) 16:9 4:3 4:3	30*1 30*1 30*1 30*1 30*1 30*1	30 30 30 30 30 30	20 20 20 20 20 20
Stream 3	MJPEG	640x360 480x360 384x288	(mHD) 16:9 4:3 4:3	15 15 15	15 15 15	15 15 15

Note:*1 Streams 2 and 3 are restricted to 15 FPS when Stream 1 is greater than 30 FPS.

Note:*2 Streams 1 and 2 are restricted to 30 FPS when TrueWDR 2x is enabled.

Note:*3 Streams 1 and 2 are restricted to 20 FPS when TrueWDR 3x is enabled.

Note:*4 The maximum frame rate of any stream is 30 FPS when corridor mode is enabled.

Note:*5 The maximum frame rate of any stream is 30 FPS when corridor mode is enabled.

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

Table 46 8MP Camera Stream Set (all resolution, codes and frame rate combinations of Stream 1, 2 and 3 are valid)

		Normal Mode				
		Resolution	Description	Max FPS		
				TWDR Off	TWDR 2x	TWDR 3x
Stream 1	H.264 H.265 H.264 IntelliZip H.265 IntelliZip MJPEG	3840x2160	(4K) 16:9	30	25	15
		3264x1840	16:9	30	25	15
		2688x1520	16:9	30	25	15
		1920x1080	(1080p) 16:9	60	25	15
		1664x936	(HD+) 16:9	60	25	15
		1280x720	(720p) 16:9	60	25	15
Stream 2	H.264 H.265 H.264 IntelliZip H.265 IntelliZip MJPEG	1280x720	(720p) 16:9	30*1	25	15
		1024x576	(PAL+) 16:9	30*1	25	15
		960x544	(qHD) 16:9	30*1	25	15
		816x464	16:9	30*1	25	15
		640x360	(mHD) 16:9	30*1	25	15
		480x272	16:9	30*1	25	15
Stream 3	MJPEG	640x360	(mHD) 16:9	30 *1	25	15
		480x272	4:3	30 *1	25	15

Note:*1 Stream 2 is restricted to 15 FPS when Stream 1 is greater than 30 FPS or when Stream 1 resolution is greater than 1920x1080.

Note:*2 Stream 3 is restricted to 10 FPS when Stream 1 is greater than 30 FPS or when Stream 1 resolution is greater than 1920x1080.

Note:*3 All streams are restricted to 25 FPS when TrueWDR 2x is enabled.

Note:*4 All streams are restricted to 15 FPS when TrueWDR 3x is enabled.

Note:*5 The maximum frame rate of any stream is 30 FPS when corridor mode is enabled.

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

Table 47 8MP Camera Stream Set (all resolution, codes and frame rate combinations of Stream 1, 2 and 3 are valid)

		Corridor Mode				
		Resolution	Description	Max FPS		
				TWDR Off	TWDR 2x	TWDR 3x
Stream 1	H.264 H.265 H.264 IntelliZip H.265 IntelliZip MJPEG	3840x2160	(4K) 16:9	30	25	15
		3264x1840	16:9	30	25	15
		2688x1520	16:9	30	25	15
		1920x1080	(1080p) 16:9	30	25	15
		1664x936	(HD+) 16:9	30	25	15
		1280x720	(720p) 16:9	30	25	15
Stream 2	H.264 H.265 H.264 IntelliZip H.265 IntelliZip MJPEG	1280x720	(720p) 16:9	30*1	25	15
		1024x576	(PAL+) 16:9	30*1	25	15
		960x544	(qHD) 16:9	30*1	25	15
		816x464	16:9	30*1	25	15
		640x360	(mHD) 16:9	30*1	25	15
		480x272	16:9	30*1	25	15
Stream 3	MJPEG	640x360	(mHD) 16:9	30 *1	25	15
		480x272	4:3	30 *1	25	15

Note:*1 Stream 2 is restricted to 15 FPS when Stream 1 is greater than 30 FPS or when Stream 1 resolution is greater than 1920x1080.

Note:*2 Stream 3 is restricted to 10 FPS when Stream 1 is greater than 30 FPS or when Stream 1 resolution is greater than 1920x1080.

Note:*3 All streams are restricted to 25 FPS when TrueWDR 2x is enabled.

Note:*4 All streams are restricted to 15 FPS when TrueWDR 3x is enabled.

Note:*5 The maximum frame rate of any stream is 30 FPS when corridor mode is enabled.

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

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

The settings for 3MP cameras are:

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

The settings for 8MP cameras are:

- **Stream 1 -** 1 - 15 fps, or 1-60 fps depending on the resolution. Default is 15 fps. 60 fps is only available on Stream 1 with resolution 1920x1080 or lower.
- **Stream 2 -** 1 - 15 fps, or 1-30 fps depending on the resolution. The default is 15 fps. This stream is limited to 15 fps if stream1 is 60 fps.
- **Stream 3** 7 - 15 fps. The default is 15 fps.

Note:FPS varies depending on other features - refer to the Flex Gen 3 Release Notes for further information.

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

The default setting is 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 46 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, Focus / Zoom, Exposure and White Balance settings.

Picture Rotation

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

Procedure 47 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 -

Focus/Zoom

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

Table 48 Lens features supported for the Indoor and Outdoor Dome, and Bullet cameras

	Indoor Dome	Outdoor Dome	Bullet
Mechanical Focus			
Motorized Focus	X	X	X
Mechanical Zoom			
Motorized Zoom	X	X	X
Lens Calibration	X	X	X
Lens Selection			
Auto One Touch	X	X	X
Configurable Continuous Auto-Focus			

Procedure 48 Adjust Camera Focus / Zoom

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 ▶ to start the video stream if it is not already active.
4	Use the plus and minus arrows to manually configure the focus and the slider bar to adjust zoom settings until the image in clear. The video pane updates to display the new settings.

- End -

Procedure 49 Adjust Camera Focus using OneTouch Autofocus

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 ▶ to start the video stream if it is not already active.
4	Select the **One Touch** button. The camera refocuses to the zoom level selected for the image. The video pane updates to display the new settings.

Exposure

Configure the exposure settings for the camera.

Procedure 50 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:

- **P-Iris**
- **Manual**
- **Shutter Priority**
- **Iris 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 **Iris Level** from the drop-down menu.
The default setting is 1.

Note: The Iris Level differs depending on the camera.

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

12 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 51 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 **Video** 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, Flicker Control and Picture Adjustments including Brightness, Contrast, White Balance, Saturation and Sharpness displayed in the video pane.

Wide Dynamic Range

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

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

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

Procedure 52 Disable/Enable Wide Dynamic Range (WDR)

Step **Action**

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

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

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

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

Note: TrueWDR3x does not apply to the 8MP models.

The default setting is OFF.

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.

IR Illuminator

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

Procedure 53 Enable / Disable IR Illuminator

The Indoor Dome camera does not support this feature. Refer to product codes for feature support.

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Picture Additional** from the **Basic Configuration** menu.
3	Select the **Enable IR Illuminator** check box to enable IR Illuminator. OR Clear the **Enable IR Illuminator** check box to disable **IR Illuminator**. The default setting is ‘Disabled’.

- End -

Day Night Mode

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

Procedure 54 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 55 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 1% to 100%. The video pane updates to display the new settings.

- End -

Procedure 56 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 57 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 58 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 -

Lens Calibration

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

You can run a lens calibration from the **Lens Calibration** tab.

This feature applies only to the Illustra Flex 3MP Indoor Dome, Outdoor Dome, and Bullet cameras.

Procedure 59 Run a Lens Calibration

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

- 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 60 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 61 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 62 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 63 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 64 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 65 Display or Hide the User Defined OSD

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

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

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

OR

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

The default setting is ‘Disabled’.

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

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

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

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

- End -

Privacy Zones

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

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

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

Defining a Privacy Zone

Create a privacy zone on the camera.

Procedure 66 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 67 Enable/Disable a Privacy Zone

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Privacy Zones** from the **Video** menu. The **Privacy Zones** tab displays.
3	Select ▶ to start the video stream if it is not already active. The video pane displays the current camera view.
4	Select the corresponding **Enabled** check box to enable the privacy zone. OR Clear the corresponding **Enabled** check box to disable the privacy zone.

- End -

Deleting a Privacy Zone

Delete a privacy zone from the camera.

Procedure 68 Delete a Privacy Zone

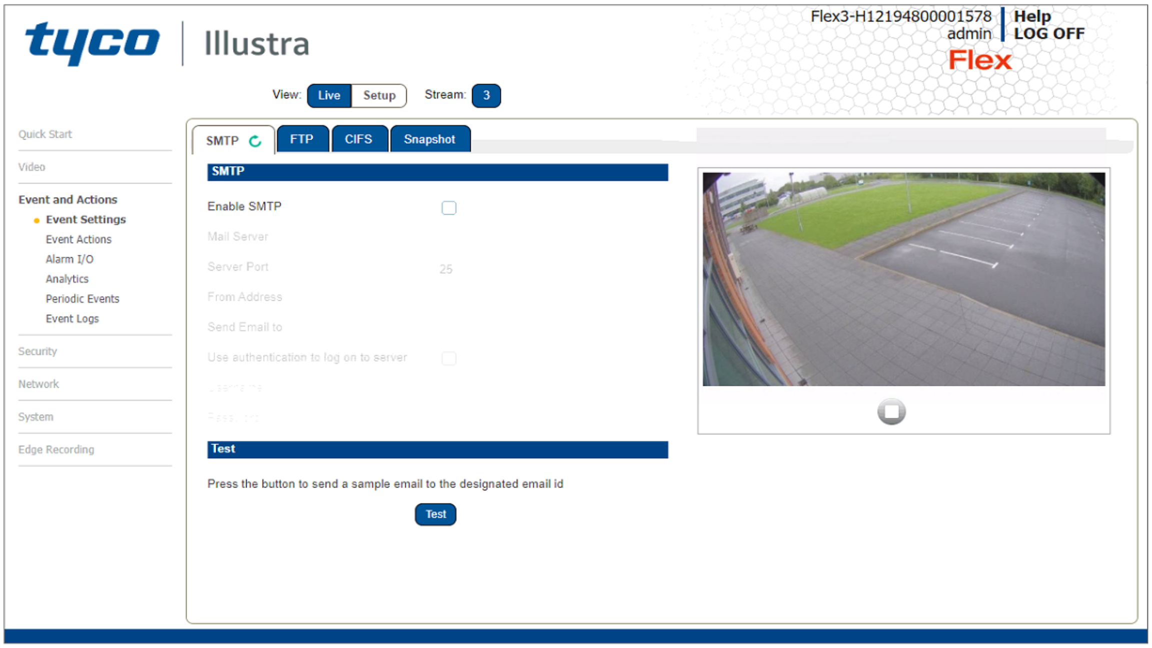
Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Privacy Zones** from the **Video** menu. The Privacy zones tab displays.
3	Select the corresponding **Delete** check box to mark the privacy zone for deletion.
4	Select **Delete** to delete the selected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

- End -

Events and Actions Menu

When you select the Events and Actions menu the Event Settings page displays, as seen in Figure 49 on page 81.

Figure 49 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

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
- Alarms I / O
- Analytics
- Periodic Events
- Events Logs

Event Settings

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

SMTP

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

Procedure 69 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 SMTP** check box to enable SMTP. Fields on the tab become available for entry of information. OR Clear the **Enable SMTP** check box to disable SMTP. The default setting is 'Disabled'. **Note:**When in Enhanced Security mode, enabling SMTP requires the admin account password.
5	Enter the IP Address of the mail server in the **Mail Server** text box.
6	Enter the server port in the **Server Port** text box. The default setting is ‘25’.
7	Enter the from email address in the **From Address** text box.
8	Enter the email address to send email alerts to in the **Send Email to** text box.
9	Select the **Use authentication to log on to server** check box to allow authentication details to be entered. OR Clear the **Use authentication to log on to server** to disable authentication. The default setting is ‘Disabled’.
10	If ‘Use authentication to log on to server’ check box has been selected: a Enter the username for the SMTP account in the **Username** text box. b Enter the password for the SMTP account in the **Password** text box.

- End -

FTP

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

Procedure 70 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 84 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 71 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 72 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 73 Configure CIFS Server Settings

Step Action

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

2 Select **Event Settings** from the **Events and Actions** menu.

3 Select the **CIFS** tab.

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

OR

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

The default setting is ‘Enabled’.

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

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

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

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

- End -

Snapshot

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

Procedure 74 Enable a snapshot

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

- End -

Event Actions

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

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

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

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

Creating an Event Action

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

Procedure 75 Create an Event Action

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Event Actions** from the **Events and Actions** menu.
3	Select an entry on the event actions list and enter an event action name in the **Name** text box.
4	Select the **Output** check box to enable an alarm output.
5	Select the **Record** check box to enable the Record Settings.

6 Select the **Email** check box to send an e-mail to the email address configured in the Configure SMTP Settings procedure.

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

8 Select the **CIFS** check box to send a video file to the SFTP details configured in the Configure CIFS Server Settings procedure.

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

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

Note: Audio Playback is not applicable to the Compact Mini Dome.

- End -

Editing a Event Action

Modify the details of an existing event action.

Procedure 76 Edit an Event Action

Step **Action**

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

2 Select **Event Actions** from the Events and Actions menu.

3 Select an entry on the event actions list, you can edit the following:

- **Name**
- **Output** - Enable/Disable
- **Record** - Enable/Disable
- **Email** - Enable/Disable
- **FTP** - Enable/Disable
- **CIFS** - Enable/Disable
- **Audio Playback** - select the required audio clip

- End -

Alarm I / O

Note: This section does not apply to the Compact Mini Dome.

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

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

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

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

Alarm Actions

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

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

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

Procedure 77 Configure an Alarm

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

- End -

Procedure 78 Enable/Disable an Alarm

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

2 Select the **Enabled** check box to enable the corresponding alarm.

OR

Clear the **Enabled** check box to disable the corresponding alarm.

- End -

Enable or Disable Alarm Output

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

Procedure 79 Enable/Disable Alarm Output

Step	Action
1	Select **Alarm I/O** from the **Event and Actions** menu.
2	Select the **Output** check box to enable alarm output. OR Clear the **Output** check box to disable alarm output.

- End -

Procedure 80 Clearing Alarm Output

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

- End -

Analytics

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

Region of Interest (ROI)

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

Procedure 81 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 82 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.

Note:

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

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

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

Procedure 83 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 84 Enable or Disable a Motion Detection Alert

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

- End -

Video Intelligence

Note: This section only applies to the 4K models.

Video Intelligence Camera Alarms

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

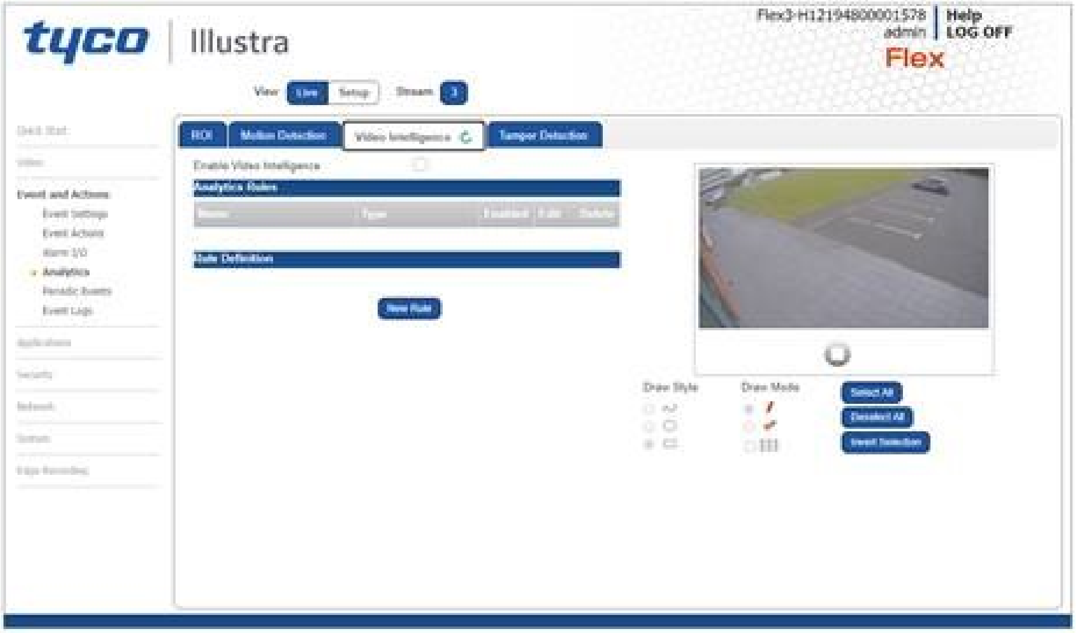
Each camera can have any number of independent Video Intelligence rules. In each rule you can define the areas in the cameras view that you want to monitor. You can name each alarm rule. It is best to use descriptive names like ‘Back Door’ or ‘Conference Room’, as these names make it easier to identify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

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

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

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

Figure 50 Video Intelligence Tab



Video Intelligence Best Practices

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

- An object exhibiting movement or a change in the scene background must be large enough to be detected, i.e. it must be around 1/25 of the image size.
- The color of the object (in grayscale) should be approximately 10-15% different than the background.
- The frame rate of the video should be high enough to capture the object in one or more captured frames.
- Video Intelligence events create entries in the victor Application Server database. It is important to ensure that the Video Intelligence parameters are accurate to avoid generating false log entries.
- Exclude the Time Stamp region from the region of interest, because the time stamp changes constantly and could register as movement.
- Try not to point cameras into sunlight, because high brightness will prevent detection of movement of bright objects such as a person with a white shirt.
- Avoid areas with persistent motion, such as trees, blinking lights, or spinning signs, by using an appropriate region of interest.
- Choose your Video Intelligence alarms selectively. You do not want to create alarms that will trigger a high number of alerts, making the important alerts more difficult to identify.
- Situate cameras to provide the best possible views of the areas of interest, objects and people. It is best to ensure camera views separate objects from people, ensure objects and people take up a larger portion of the camera view, and keep the entire region of interest within the camera’s view.

- Use staff to help identify regions of interest to monitor based on their observations, for example, of missing merchandise or missing fixtures. Video Intelligence alarms can therefore be configured to monitor areas of potential activity.
- Use searches frequently and watch activity leading up to an alarm being triggered. This may give an indication of suspicious activity and other areas to monitor.
- Tune your alarms regularly to ensure the alarms reflect changes to the environment, for example, objects being rearranged or replaced. Monitoring these changes and re-tuning your alarms will ensure maximum effectiveness of the Video Intelligence alarms and searches.
- Use the new information that Video Intelligence provides to learn and adapt. Use it to implement changes that will improve surveillance and reduce losses, for example, eliminate blind spots, make staff aware of suspicious behavior, or re-design the environment and alarms

Creating a Video Intelligence Camera Alarm

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

Procedure 85 Enable/Disable Video Intelligence

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Analytics** from the **Events and Actions** menu.
3	Select the **Video Intelligence** tab.
4	Select the **Enable Video Intelligence** check box to enable Video Intelligence on the camera. OR Deselect the **Enable Video Intelligence** check box to disable Video Intelligence on the camera.
5	Select **Save** to save your changes.

- End -

Procedure 86 Creating a Video Intelligence alert

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Analytics** from the **Events and Actions** menu.
3	Select the **Enable Video Intelligence** check box to enable Video Intelligence on the camera.
4	Use the drawing tools beneath the live video feed to create a Region of Interest
5	Type a **Rule Name** for your rule definition in the field provided.
6	Select a fault action from the **Action** drop-down menu. This fault action is activated when the parameters of the analytics rule are met.
7	Select a rule type from the **Rule Type** drop-down menu:

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

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

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

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

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

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

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

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

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

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

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

9 To apply a color filter over the Region of Interest, select one of the seven **Color Filter** check boxes.

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

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

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

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

Object Detection

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

Abandoned / Removed

a Overlap (%) - The amount of background change that must be in the region of interest before an alarm is triggered. Use a higher setting to avoid finding nearby changes or changes that are not completely in the region of interest.

b Minimum Skip (secs) - This is the period of time after an alert, during which no further alerts are generated. A setting of 0 seconds triggers all alerts.

c Fast Trigger - Enable Fast trigger to reduce the time required to assess if an object is abandoned or removed. As a result, alerts trigger more quickly, but the number of false alarms also increases.

d Wipeout Amount Changed (%) - The percentage of the region of interest that must change before an alarm is triggered. Adjust to look for either a larger or smaller change in the region.

e Wipeout Within (secs) - Time frame within which the change must occur in order to trigger the alarm. A setting of 0 seconds represents instantaneous change.

Direction

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

b Direction - This is the general direction the object must move in to trigger an alarm. You can choose North, South, East or West.

c Traversal Time- This is the maximum amount of time which an object can take to traverse most of the region before the alarm is triggered. This is to exclude objects that move too slow.

Linger

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

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

Dwell

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

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

Queue Analysis

a Select Area - Additional tools display when using queue analysis to highlight zones of interest; Short, Medium and Long. Use these to define the zones of interest that must be occupied to form a short medium and long queue, all 3 zones must be defined, regardless of the queue length. Each selection is highlighted via a different color (Short = green, Medium = yellow and Long = purple).

b Overlap (%) - The amount of detected object that must be in the region of interest to be identified as a person in a queue.

c Queue Length - The required minimum length for an alarm to be generated. The following options are available:

- **Empty**; this will generate an alarm when no objects are present in the designated regions of interest.
- **Not Empty**; this will generate an alarm when an object(s) is present in the designated regions of interest.
- **Short**; this will generate an alarm when objects are present in the short designated region of interest and meet the overlap requirements.
- **Medium**; this will generate an alarm when objects are present in both the short and medium designated regions of interest and meet the overlap requirements.
- **Long**; this will generate an alarm when objects are present in the short, medium and long designated regions of interest and meet the overlap requirements.

Perimeter

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

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

Crowd Formation

a Overlap (%) - The amount of detected object that must be in the region of interest to be considered for determining the crowd size.

b Minimum Crowd Size - The minimum number of people that must be present to generate an alarm. This can be between 2-50 people.

Exit

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

Enter

a Overlap (%) - The amount of detected object that must be in the region of interest when it first appears in the camera view. The object must leave the region of interest by the same amount before an alarm is triggered. For best results select a higher overlap setting.

- End -

Procedure 87 Enable/Disable an Analytics Rule

Step Action

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

2 Select **Analytics** from the **Events and Actions** menu.

3 Select the **Video Intelligence** tab.

4 From the **Analytics Rules** table, select the check box of the target Analytics Rule to enable the analytics rule

OR

Deselect the check box of the target Analytics Rule to disable the analytics rule.

- End -

Procedure 88 Edit an Analytics Rule

Step Action

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

2 Select **Analytics** from the **Events and Actions** menu.

3 Select the **Video Intelligence** tab.

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

5 Edit the settings in the Rule Definition until you are happy with your changes.

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

- End -

Procedure 89 Delete an Analytics Rule

Step Action

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

2 Select **Analytics** from the **Events and Actions** menu.

3 Select the **Video Intelligence** tab.

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

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

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

- End -

Face Detection

Note: This section only applies to the 4K models.

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

Procedure 90 Enable / Disable Face Detection

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

- End -

Tamper Detection

A Tamper Detection event can be created when the screen is blocked or camera position is changed.

Blur Detection

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

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

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

Periodic Events

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

Procedure 91 Configure a Periodic Event

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Periodic Events** from the **Events and Actions** menu. The **Periodic Events** tab displays.
3	Enter the name of the periodic event in the **Name** text box.
4	Select the **Enabled** check box to enable the Periodic Event. OR Clear the **Enabled** check box to disable the Periodic Event.
5	Select the **Periodic Time (min)** drop-down menu to select a value for the periodic time.
6	Select the **Action** drop-down menu to select a fault action.

- End -

Event Logs

Event Log

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

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

Procedure 92 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 93 Delete Current Events

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

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

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

OR

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

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

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

You are prompted to confirm the deletion.

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

OR

Select **Cancel**.

- End -

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 94 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 95 Delete Current Faults

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

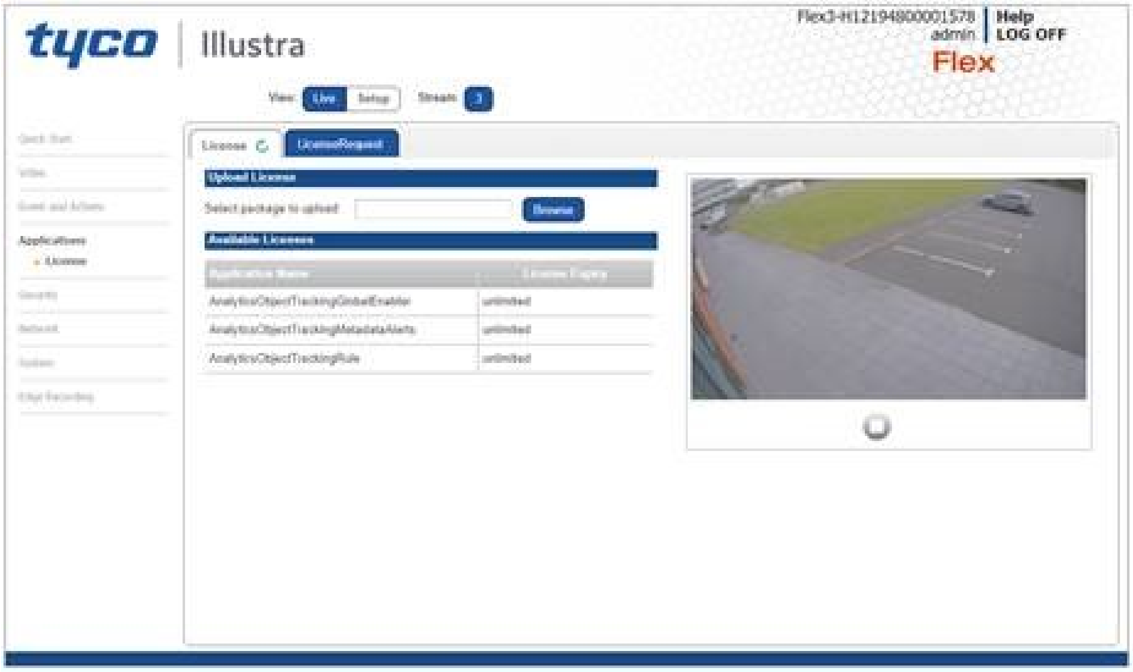
- End -

Applications

When you select the Applications menu the License page displays, as seen in on page 102.

Note: This section is only applicable to the 4K models.

Figure 51 Applications Menu



Application Name	License Expiry
AnalyticsObjectTrackingGlobalEnabler	unlimited
AnalyticsObjectTrackingMetadataAlerts	unlimited
AnalyticsObjectTrackingRule	unlimited

License

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

Procedure 96 Upload an License

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

- End -

Available Licenses

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

Procedure 97 Start, Stop or Remove a License

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Applications** menu. The License tab displays.
3	Select the corresponding **License** checkbox to Start, Stop or Remove.
4	Select one of the following options: a **Start** to start the License running. b **Stop** to stop the License running. c **Remove** to remove the License.

- End -

Procedure 98 Request a License File XML

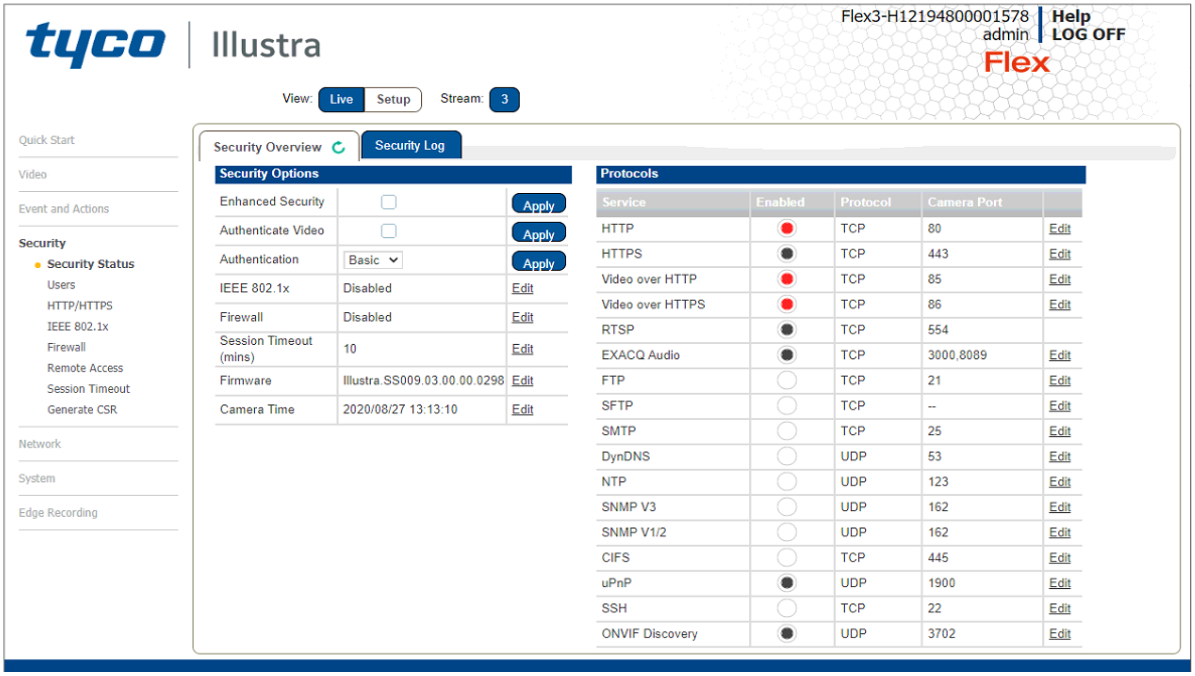
Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **License** from the **Applications** menu.
3	Select the **LicenseRequest** tab.
4	Select **Download**. The following file is automatically downloaded LicReq-camera_serial_number.xml.

- End -

Security

When you select the **Security** menu, the **Security Status** page appears, as seen in Figure 52 on page 104.

Figure 52 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.SS009.03.00.00.0298	Edit
Camera Time	2020/08/27 13:13:10	Edit

Protocols

Service	Enabled	Protocol	Camera Port	
HTTP	●	TCP	80	Edit
HTTPS	●	TCP	443	Edit
Video over HTTP	●	TCP	85	Edit
Video over HTTPS	●	TCP	86	Edit
RTSP	●	TCP	554	
EXACQ Audio	●	TCP	3000,8089	Edit
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
- Generate SCR

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 38.

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

Procedure 99 Enable Enhanced Security

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

- End -

Procedure 100 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 101 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 102 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 103 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 147 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 104 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 105 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 106 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 107 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 108 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 109 Add a HTTPS Certificate

Step   Action

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

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

3 Click on the **Upload** button and navigate to the certificate location.

4 Select the file and select **Open**.

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

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

- End -

Delete a HTTPS Certificate

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

Procedure 110 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 111 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 112 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 113 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 114 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 115 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 116 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 117 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 118 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 119 Enable/Disable Video over HTTP

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

The default setting is ‘Enabled’.

- End -

Video over HTTPS

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

Procedure 120 Enable/Disable Video over HTTPS

Step Action

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

2 Select **Remote Access** from the **Security** menu.

The Remote Access tab displays.

3 Select the **Video over HTTPS** check box to enable Video over HTTPS.

OR

Deselect **Video over HTTPS** check box to disable Video over HTTPS.

The default setting is ‘Enabled’.

- End -

UPnP Discovery

Enable or disable UPnP Discovery on the camera.

Procedure 121 Enable/Disable UPnP Discovery

Step Action

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

2 Select **Remote Access** from the **Security** menu.

The Remote Access tab displays.

3 Select the **UPnP Discovery** check box to enable UPnP Discovery.

OR

Deselect **UPnP Discovery**check box to disable UPnP Discovery.

The default setting is ‘Enabled’.

- End -

ExacqVision Server Audio

Enable or disable audio ports used for ExacqVision bidirectional audio integration.

Procedure 122 Enable/Disable EXACQ Audio

Step Action

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

2 Select **Remote Access** from the **Security** menu.

The Remote Access tab displays.

3 Select the **EXACQ Audio** check box to enable EXACQ Audio.

OR

Deselect **EXACQ Audio** check box to disable EXACQ Audio.

The default setting is ‘Enabled’.

- End -

Session Timeout

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

Procedure 123 Set a Session Timeout time

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Session Timeout** from the **Security** menu. The Session Timeout tab displays.
3	Use the slider bar to select the **Session Timeout (mins)**. The default setting is 15 minutes.

- End -

Generate CSR

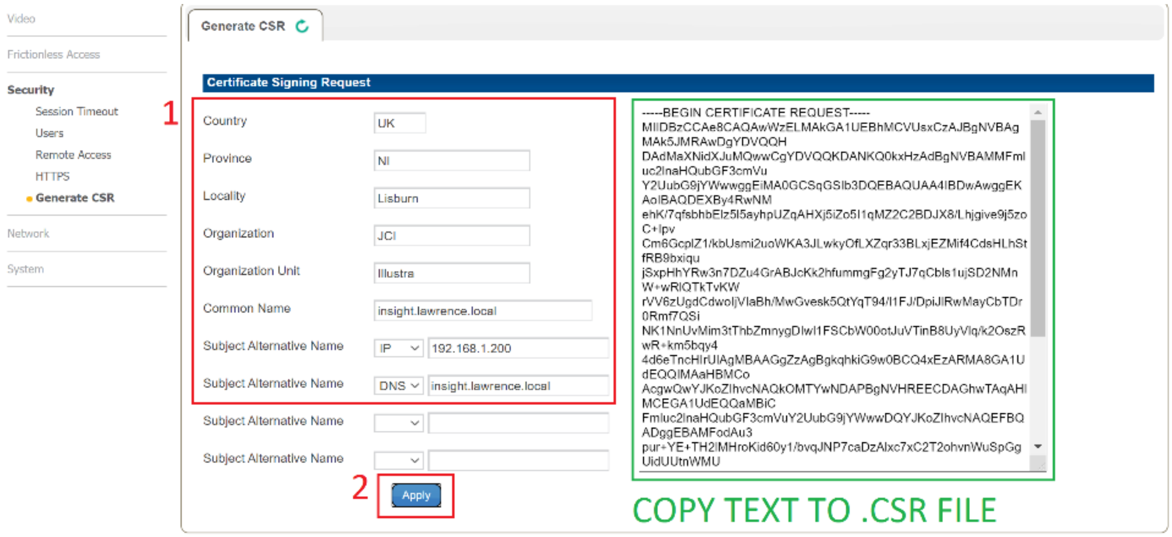
When accessing a camera web GUI via HTTPS, the browser shows an insecure / not secure browser warning. This warning is due to the camera having a ‘self-signed certificate’; which offers communication encryption but cannot be used for authentication. Introduction of the Certificate Signing Request (CSR) feature, which allows the user to generate a certificate signing request that can be used by a certificate authority to create an SSL certificate specifically for the individual camera.

Note:SSL certificates can only be used for a single device.

Procedure 124 Generate a .csr file

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

Figure 53 .CSR file tab



Certificate Signing Request

Country	UK	
Province	NI	
Locality	Lisburn	
Organization	JCI	
Organization Unit	Illustra	
Common Name	insight.lawrence.local	
Subject Alternative Name	IP	192.168.1.200
Subject Alternative Name	DNS	insight.lawrence.local
Subject Alternative Name		
Subject Alternative Name		

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDBzCCAe8CAQAwWzELMAkGA1UEBhMCVUsxCzAJBgNVBAg
MAk5JMRAwDgYDVQQH
DAdMaXNidXJuMQwwCgYDVQQKDANKQ0kxHzAdBgNVBAMMFml
uc2lnaHQubGF3cmVu
Y2UubG9jYWwwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQDEXBy4RwNM
ehK/7qfsbhbElz5l5ayhpUZqAHXj5iZo5l1qMZ2C2BDJX8/Lhjgive9j5zo
C+Ipv
Cm6GcplZ1/kbUsmi2uoWKA3JLwkyOfLXZqr33BLxjEZMif4CdsHLhSt
fRB9bxiqu
jSxpHhYRw3n7DZu4GrABJcKk2hfummgFg2yTJ7qCbls1ujSD2NMn
W+wRIQTkTvKW
rVV6zUgdCdwoljVlaBh/MwGvesk5QtYqT94/I1FJ/DpiJlRwMayCbTDr
0Rmf7QSi
NK1NnUvMim3tThbZmnygDlwl1FSCbW00otJuVTinB8UyVlq/k2OszR
wR+km5bqy4
4d6eTncHIrUIAgMBAAGgZzAgBgkqhkiG9w0BCQ4xEzARMA8GA1U
dEQQIMAaHBMCo
AcgwQwYJKoZIhvcNAQkOMTYwNDAPBgNVHREECDAGhwTAqAHI
MCEGA1UdEQQaMBiC
Fmluc2lnaHQubGF3cmVuY2UubG9jYWwwDQYJKoZIhvcNAQEFBQ
ADggEBAMFodAu3
pur+YE+TH2IMHroKid60y1/bvqJNP7caDzAlxc7xC2T2ohvnWuSpGg
UidUUtnWMU
```

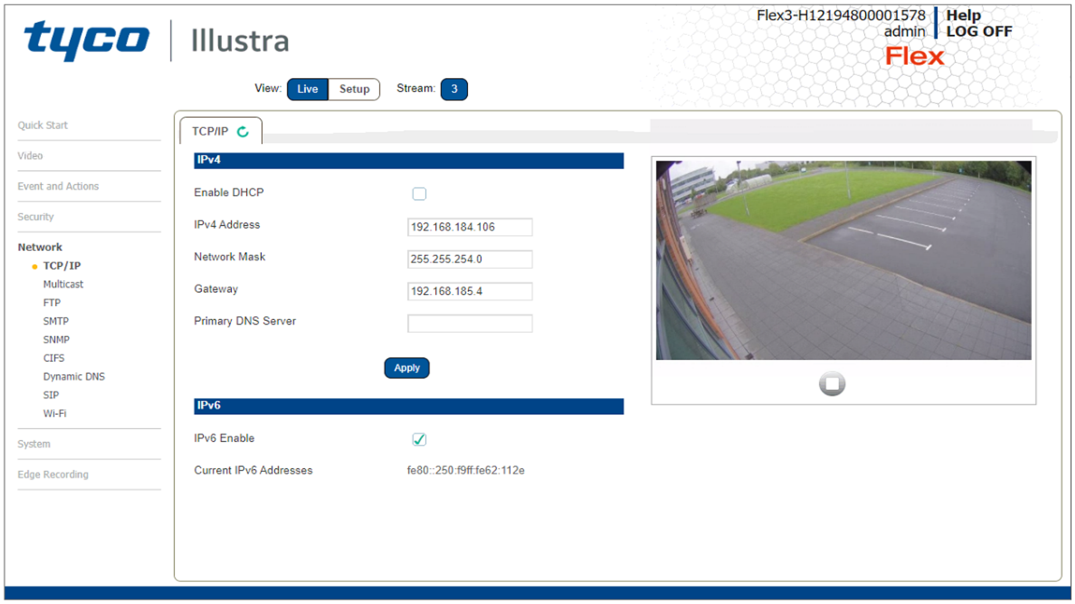
4 Copy the text shown in Green above & paste into a text file with .csr file extension.

- End -

Network Menu

When you select the **Network** menu, the **TCP/IP** page displays, as seen in Figure 54 on page 119.

Figure 54 Network Menu



IPv4

Enable DHCP □

IPv4 Address 192.168.184.106

Network Mask 255.255.254.0

Gateway 192.168.185.4

Primary DNS Server

IPv6

IPv6 Enable ☑

Current IPv6 Addresses fe80::250:f9ff:fe62:112e

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

- TCP/IP
- FTP
- SMTP
- SNMP
- CIFS
- Dynamic DNS
- SIP
- Wi-fi

TCP/IP

Configure the IPv4 and IPv6 settings on the camera.

IPv4

Configure the IPv4 settings for the camera.

Note: When you perform a factory reset or reboot the unit searches for the last known IP address. If this is not available it reverts to the default IP address of 192.168.1.168. This could result duplicate IP addresses. Refer to Network Menu on page 119 for more information.

Procedure 125 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 126 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 127 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 128 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 129 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 130 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 131 Configure SMTP Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **SMTP** from the **Network** menu. The **SMTP** tab displays.
3	Check the **Enable SMTP** check box to enable SMTP. Text boxes on the tab become available for entry. **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 132 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 133 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 134 Configure Dynamic DNS

Step Action

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

2 Select **Dynamic DNS** from the **Network** menu.

3 Select the **Service Enable** check box to enable Dynamic DNS.

OR

Deselect **Service Enable** check box to disable Dynamic DNS.

The default setting is 'Disabled'.

4 If Service Enable has been enabled:

a Enter the Camera Alias in the text box.

b Select a Service Provider from the drop-down list:

- **dyndns.org**
- **easydns.com**
- **no-ip.com**
- **zerigo.com**
- **dynsip.org**
- **tzo.com**

c Enter a **Username** in the text box.

d Enter a **Password** in the text box.

e Enter **Service Data** in the text box.

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

- End -

SIP

The Session Initiation Protocol (SIP) feature enables the camera to be configured as a SIP User Agent that can register with a SIP server to make and receive audio calls to another SIP device, for example, a SIP IP phone or softphone. The camera can operate as a SIP phone if it is equipped with an external microphone and speaker. The camera can also be configured to monitor the audio from a SIP call and make this available as an RTSP/RTP stream.

Note: Only the the SIP incoming audio is recorded in the RTSP stream.

Procedure 135 Enable/Disable SIP

Step Action

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

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

3 Check the **Enabled** check box to enable SIP

OR

Clear the **Enabled** check box to disable SIP.

The default setting is 'Disabled'.

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

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

- End -

Procedure 136 Configure the SIP Server Settings

Step Action

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

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

3 Check the **Enabled** check box to enable SIP.

4 Enter the IP address of the SIP Server in the **Domain** text box.

5 Enter the SIP account username in the **Username** text box.

6 Enter the SIP account password in the **Password** text box.

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

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

8 From the **Audio Output** dropdown menu, select an audio output:

- **Speaker -** the SIP call audio is output to the external speaker.
- **Network Stream -** the SIP call audio can be streamed using an RTSP Audio Stream.

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

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

- End -

Procedure 137 Place a SIP call

Step Action

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

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

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

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

5 Click **Hang up** to end the call.

Note: The Status Log, located below the Dial and Hang up buttons, reports the status of SIP connection and active calls.

- End -

Wi-Fi

The Wi-Fi option allows wireless configuration of the camera at the point of install in conjunction with the Illustra Tools app (Illustra Wi-Fi dongle required).

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

Procedure 138 Enable wireless configuration of the camera

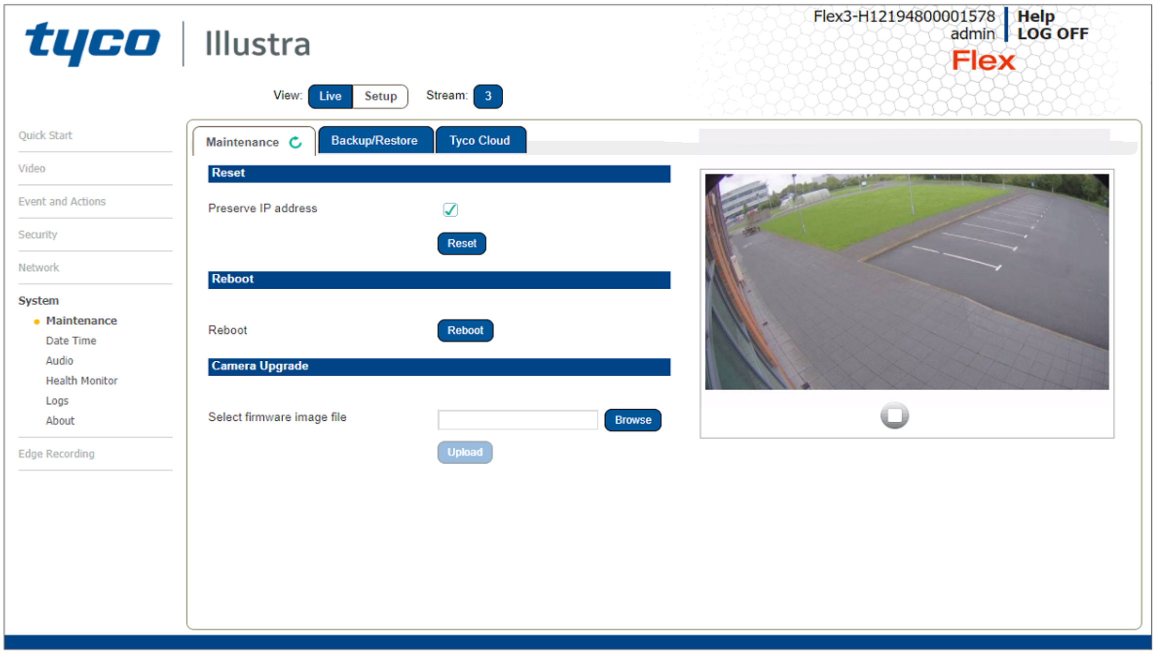
Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Wi-Fi** from the **Network** menu.
3	Check the **Enable USB** check box to enable WIFI configuration. **Note:**The Illustra Tools app can now connect to the camera using the IP address 10.181.182.1 or by scanning the QR code shown or on the product packaging. **Note:**USB will be enabled for 1 hour after the camera is powered from a factory reset. After 1hr, Wi-Fi will be disabled and will require a factory reset to re-enable. Illustra Wi-Fi dongle must inserted in camera for Wi-Fi access.

- End -

System

When you open the **System** menu, the **Maintenance** page appears, as seen in Figure 55 on page 129.

Figure 55 System Menu



Preserve IP address ☑

Reboot

Select firmware image file

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

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

Maintenance

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

Reset

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

Note: Network settings, presets, patterns and sequences can be retained if required.

Procedure 139 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 140 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 141 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 142 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 143 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 -

Tyco Cloud

The Tyco Cloud feature implements Illustra Cameras to Cloud (C2C) from Tyco Cloud 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 144 Enabling Tyco Cloud integration

Note: If a Tyco Cloud server is not setup when enabling the Tyco Cloud 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 **Tyco Cloud** tab.
4	Select **Apply**.
5	Enter an administrator password to validate the request. • If the camera detects an Internet connection, it continues with the Tyco Cloud 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 Tyco Cloud mode and is only accessible using HTTPS.
The password changes to a string of characters determined by the Tyco cloud.

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

- End -

Procedure 145 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 **Tyco Cloud Reset**: Resets the camera and boots the camera in Tyco Cloud mode.
4	If you do not have the credentials to perform a reset, you can perform a factory reset on the hardware itself by using the hardware reset button as detailed in the Product Overview of each camera.

- End -

Date / Time

Set the date and time on the camera.

Note:

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

Procedure 146 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 -

Audio

Note: This section does not apply to the Compact Mini Dome.

You can configure the audio input, output, upload audio and stored audio clips, as well as configure Audio Video Synchronization on this tab.

Procedure 147 Configure Audio Input

Step Action

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

2 Select the **Input Enable** check box to enable the audio input settings.

Or

Clear the **Input Enable** check box to disable audio input settings.

The default setting is ‘Disabled’.

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

Values range from 1 to 100.

The default setting is 72.

- End -

Procedure 148 Configuring Audio Output

Step Action

1 Select **Audio** from the Camera Configuration menu.

2 Select the **Output Enable** check box to enable the audio output settings.

Or

Deselect the **Output Enable** check box to disable audio input settings.

The default setting is ‘Disabled’.

3 If Output Enable has been enabled, use the slider bar to select the Output Volume.

Values range from 1 to 100.

The default setting is 50.

- End -

Configuring Stored Audio

When connected to an appropriate device, the unit is capable of playing back stored audio when an alarm has been triggered. A maximum of five audio files can be uploaded to the unit.

Note: Audio clips can only be used if a micro SD Card has been installed. Refer to the relevant Quick Reference Guide for information on installing the micro SD Card.

When uploading an audio file it must meet the following requirements:

- The filename cannot contain spaces.
- It must be a ‘wav’ file with a ‘.wav’ extension.
- A single channel mono file with a bit depth of 16kHz.
- The sample rate must be 8kHz.
- The duration must be no longer than 20 seconds.

Procedure 149 Play Stored Audio

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

- End -

Procedure 150 Upload an Audio File

Step	Action
1	Select **Audio** from the **System** menu.
2	Select the **Audio Clips** tab.
3	Select **Browse**. The Choose file dialog displays.
4	Navigate to the location where the audio file has been saved. Select the audio file then select the **Open** button. When uploading an audio file it must meet the following requirements: • The filename cannot contain spaces. • It must be a ‘wav’ file with a ‘.wav’ extension. • A single channel mono file with a bit depth of 16kHz. • The sample rate must be 8kHz. • The duration must be no longer than 20 seconds.
5	Select **Upload**.
6	You will be prompted to confirm that you would like to upload the audio file. Select **OK** to confirm the upload.

Or

Select **Cancel**.

- End -

Procedure 151 Delete a Stored Audio file

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

- End -

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 152 Configure Health Monitor Settings

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select the **Health Monitor** from the **System** menu.
3	Select the **Recording Period** from the drop-down menu.
4	Select the corresponding check box to enable health monitoring on a parameter. OR Clear the corresponding check box to disable health monitoring on a parameter. The default setting for all parameters is Enabled.

- End -

Logs

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

System Log

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

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

Procedure 153 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 154 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 155 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 156 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 157 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 158 Edit Camera Name

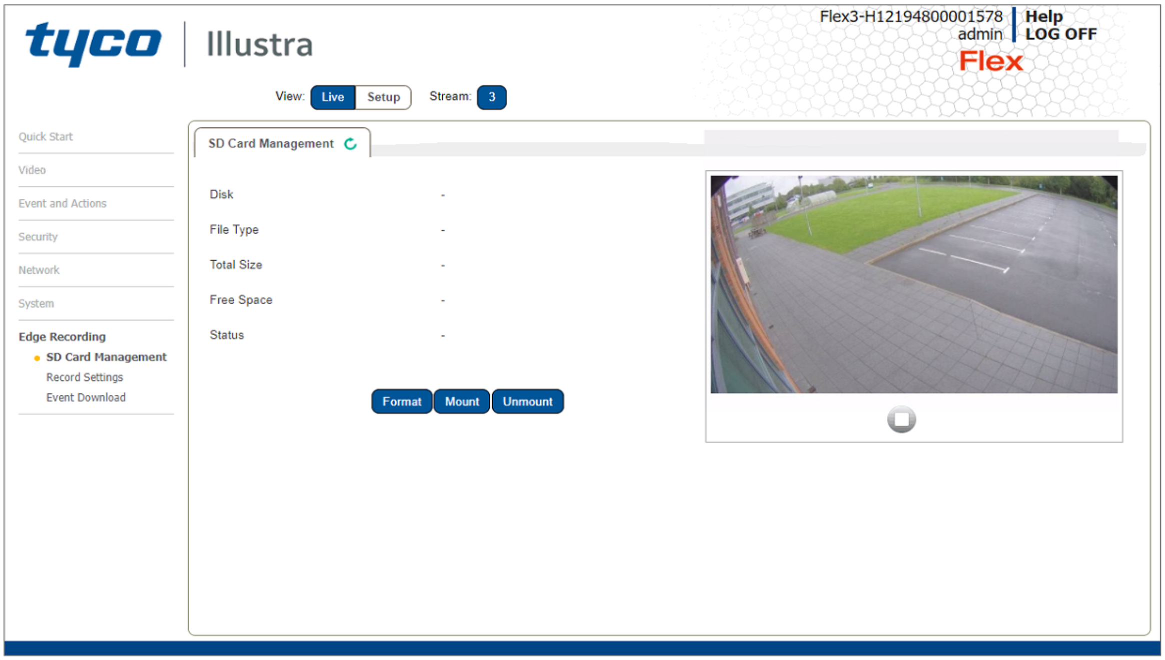
Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **About** from the **System** menu. The model tab displays.
3	Edit the name in the **Camera Name** textbox.

- End -

Edge Recording

When you select the **Edge Recording** menu, the **Micro SD Card Management** page appears, as seen in Figure 56 on page 140.

Figure 56 Edge Recording Menu



Disk -

File Type -

Total Size -

Free Space -

Status -

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

- Micro SD Card Management
- Record Settings
- Event Download

Micro SD Card Management

Edge recording provides the ability to save recorded video to a Micro SD Card. Video can be configured to be recorded based on an event. Without a Micro SD Card current faults notifications displayed on camera if an alarm is triggered. Using a Micro SD Card enables the following:

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

Inserting the Micro SD Card

When inserting a Micro SD Card it is essential that the camera is rebooted. The Micro SD Card should be mounted and unmounted through the Web User Interface. If you receive a 'Device is Busy' model you should wait and try again in a few minutes. If this does not work then it may be necessary to disable Motion Detection, FTP or any other process which may be using the Micro SD Card.

Note: Refer to the Quick Reference Guide supplied with the product for details on how to remove the housing assembly and gain access to the camera.

Procedure 159 Insert the Micro SD Card by powering down the Camera

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

- End -

Procedure 160 Mount the Micro SD Card through the Web User Interface to reboot the Camera

Step	Action
1	Insert the Micro SD card into the camera.
2	Select **Setup** on the Web User Interface banner to display the setup menus.
3	Select **SD Card Management** menu from the **Edge Recording** menu.
4	Select **Mount**.

- End -

Removing the Micro SD Card

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

- Remove the Micro SD Card by powering down the camera - Use this procedure if you do not have access to the Web User Interface and are unable to unmount the Micro SD card before removal.
- Unmount the Micro SD Card for Removal - Use this procedure when you are unable to access the power supply to the camera.

Note: Refer to the Quick Reference Guide supplied with the product for details on how to remove the housing assembly and gain access to the camera.

Procedure 161 Remove the Micro SD Card by powering down the Camera

1 Turn off the camera by disconnecting the power supply.

2 Remove the Micro SD card from the camera.

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

3 Reconnect the power supply and power up the camera.

- End -

Procedure 162 Unmount the Micro SD Card for Removal

Step	Action
1	Select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **SD Card Management** menu from the **Edge Recording** menu.
3	Select **Unmount**. You are prompted to confirm the unmounting.
4	Select **OK** to confirm. OR
5	Select **Cancel**. Remove the Micro SD card from the camera. AVI clips are not available on the camera until the Micro SD card has been inserted and mounted.

- End -

Encrypted SD card storage

Introduction of the Encrypted SD Card storage feature which offers encryption for the entire contents of their SD card. When SD card Encryption is enabled the contents of the SD Card will only be accessible through the Camera Web GUI, unless a Custom Password has been set which allows password protected access to the SD card when mounted elsewhere. Currently this mounting is only supported on Linux systems.

NOTE: The user can disable Encrypted SD Card storage to revert to being able to access the SD card via Windows based systems, without a Password.

Disabling SD card encryption is not recommended.

Procedure 163 Encrypting the contents on the SD card with firmware Illustra.SS008 / Illustra.SS009.03.01.00.003xx or later

Step	Action
1	Insert the SD card into camera.
2	Log in to the camera Web GUI and select **Setup** on the Web User Interface banner to display the setup menus.
3	Select **SD Card Management** from the Edge Recording menu. **Note:**The SD card will show as unmounted with encryption enabled. **Note:**Encryption is always enabled by default after the camera has been reset. The user may disable encryption mode but any change to the encryption status requires the SD card to be formatted.
4	Format the SD card by selecting **Format** and select **Mount** to mount the encrypted SD card.

Note: The SD card will fail to mount until it has been formatted. The user now has the option to encrypt SD card with a custom password.

The Custom Password is only required when the SD card is accessed independently from the camera. It will not affect SD card functionality while it is being used by the camera.

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

6 Select ‘Encrypt SD card with custom password’.

7 Enter the custom password into both password fields and select **Save.**

Note: Once the Custom Password has been set, it can be edited or cleared at any time in the SD Card Management tab under the Edge Recording menu.

The Custom Password will remain set after a firmware upgrade. The Custom Password will be cleared after a reset.

The SD Card Encryption can be disabled at any time by unticking ‘Encrypt entire contents of SD card’. However any changes to the encryption status requires the SD card to be formatted.

- End -

Procedure 164 Encrypting the contents on the SD card after upgrading from a firmware pre Illustra.SS008 / Illustra.SS009.03.01.00.003xx

Step Action

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

2 Select **Maintenance** from the System.

3 Click on the **Browse** button and navigate to the latest firmware.

4 Select the file and select **Open**.

5 Select **Upload**.

Wait for the Firmware Upgrade process to complete.

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

If the SD card was inserted pre-upgrade, or is inserted after the camera firmware has been upgraded, the SD card will show as mounted and encryption options will be disabled until the camera has been reset.

Note: Encryption will remain disabled by default after upgrading from firmware pre - Illustra.SS008 / Illustra.SS009.03.01.00.003xx until the user manually enables it, or resets the camera, after which it is enabled by default.

To enable Encryption:

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

b Select ‘Encrypt entire contents of SD card.

Note: Changing the encryption option requires the SD card to be formatted, all previously recorded data will be lost.

c The user now has the option to encrypt SD card with a custom password.

Note: The Custom Password is only required when the SD card is accessed independently from the camera. It will not affect SD card functionality while it is being used by the camera.

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

e Select ‘Encrypt SD card with Custom Password’

f Enter the custom password into both password fields.

Note: Once the Custom Password has been set, it can be edited or cleared at any time in the SD Card Management tab under the Edge Recording menu.

SD Card Encryption can be disabled at any time by unticking ‘Encrypt entire contents of SD card’. However any changes to the encryption status will require the SD card to be formatted.

- End -

Procedure 165 Resetting a camera running firmware Illustra.SS008 / Illustra.SS009.03.01.00.003xx or later

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

Step	Action
1	Log in to camera Web GUI and select **Setup** on the Web User Interface banner to display the setup menus.
2	Select **Maintenance** from the System menu.
3	Select **Reset** and **OK**.
4	Wait for the Reset process to complete.
5	Log in to the camera Web GUI and run through the initial setup.
6	Select **SD Card Management** from the Edge Recording menu.

- If SD card Encryption was enabled before reset and the same HostID is used after reset, the SD card will show as mounted and Encryption will be enabled.
- If SD card Encryption was enabled before reset and a different HostID is used, the SD card will show as unmounted and Encryption will be enabled. SD card will need to be formatted before it can be mounted by the camera.
- If SD card Encryption was disabled before reset, the SD card will show as unmounted and Encryption will be enabled. SD card will need to be formatted before it can be mounted by the camera.

- End -

Record Settings

Select which video stream to use for alarm video and configure pre and post event durations for the playable video clip. The camera can record video generated from MD, face detection and DIO events.

Procedure 166 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 the Configure the Video Stream Settings procedure. b Select the Pre Event (secs) in seconds from the drop-down menu. Values range from 0 to 10. The default setting is 5 seconds. c Select the Post Event (secs) in seconds from the drop-down menu. Values range from 0 to 10. The default setting is 5 seconds.
5	Select **Apply** to save.

- End -

Offline Record Settings

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

Procedure 167 Configure Offline Recording Settings

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

6 In the **Post event (secs)** field, enter a time in seconds of the amount of time you wants recorded after the offline event.

- End -

Event Download

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

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

Appendix A: 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	
		Lens Calibration	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		
		Snapshot	X		
	Event Actions	Event Actions	X		
	Alarm I/O	Alarm I/O	X		
	Analytics	ROI	X		
		Motion Detection	X		
		Blur Detection	X		
	Event Logs	Event Log	X		
		Fault Log	X		
Security	Security Status	Security Overview	X		

Camera Menu	Sub Menu	Tab	Admin	Operator	User
		Security Log	X		
	Users	User	X	X	
		Add User	X	X	
		Change Password	X	X	X
	HTTP/HTTPS	HTTP/HTTPS	X		
	IEEE 802.1x	EAP Settings	X		
	Firewall	Basic Filtering	X		
		Address Filtering	X		
	Remote Access	Remote Access	X		
	Session Timeout	Session Timeout	X		
Network	TCP/IP	TCP/IP	X		
	Multicast	Multicast	X		
	FTP	FTP	X		
	SMTP	SMTP	X		
	SNMP	SNMP	X		
	CIFS	CIFS	X		
	Dynamic DNS	Dynamic DNS	X		
	SIP	SIP	X		
System	Maintenance	Maintenance	X		
		Backup / Restore	X		
	Date Time	Date Time	X		
	Audio	Audio	X		
		Audio Clips	X	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	X		

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

Appendix B: Using Media Player to View RTSP Streaming

Note: This appendix is provided for user instruction only. Tyco Security Products does not support or is not responsible for any error caused during the use of third party software used for RTSP playback.

Procedure 168 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=2
- **Stream 3:** rtsp://cameraip:554/audioStreamId=3

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

OR

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

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

- End -

Appendix C: Stream Tables

Flex Gen 3 - 3MP and Flex 8MP Streaming Combinations

Table 57 on page 151 provides information for the stream resolutions and supported FPS of the Flex 3MP cameras herein.

on page 151 provides information for the stream resolutions and supported FPS of the Flex 8MP cameras.

Table 57 3MP Camera Stream Set (all resolution, codes and frame rate combinations of Stream 1, 2 and 3 are valid)

		Normal Mode				
		Resolution	Description	Max FPS		
				TWDR Off	TWDR 2x	TWDR 3x
Stream 1	H.264 H.265 H.264 IntelliZip H.265 IntelliZip MJPEG	2048x1536	4:3	30	30	20
		1920x1080	(1080p) 16:9	60	30	20
		1664x936	(HD+) 16:9	60	30	20
		1280x720	(720p) 16:9	60	30	20
Stream 2	H.264 H.265 H.264 IntelliZip H.265 IntelliZip MJPEG	1280x720	(720p) 16:9	30*1	30	20
		1024x576	(PAL+) 16:9	30*1	30	20
		640x480	4:3	30*1	30	20
		640x360	(mHD) 16:9	30*1	30	20
		480x360	4:3	30*1	30	20
		384x288	4:3	30*1	30	20
Stream 3	MJPEG	640x360	(mHD) 16:9	15	15	15
		480x360	4:3	15	15	15
		384x288	4:3	15	15	15

Note:*1 Streams 2 and 3 are restricted to 15 FPS when Stream 1 is greater than 30 FPS.

Note:*2 Streams 1 and 2 are restricted to 30 FPS when TrueWDR 2x is enabled.

Note:*3 Streams 1 and 2 are restricted to 20 FPS when TrueWDR 3x is enabled.

Note:*4 The maximum frame rate of any stream is 30 FPS when corridor mode is enabled.

Note:*5 The maximum frame rate of any stream is 30 FPS when corridor mode is enabled.

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

Table 58 3MP Camera Stream Set (all resolution, codes and frame rate combinations of Stream 1, 2 and 3 are valid)

		Corridor Mode				
		Resolution	Description	Max FPS		
				TWDR Off	TWDR 2x	TWDR 3x
Stream 1	H.264 H.265 H.264 IntelliZip H.265 IntelliZip MJPEG	2048x1536 1920x1080 1664x936 1280x720	4:3 (1080p) 16:9 (HD+) 16:9 (720p) 16:9	30 30 30 30	30 30 30 30	20 20 20 20
Stream 2	H.264 H.265 H.264 IntelliZip H.265 IntelliZip MJPEG	1280x720 1024x576 640x480 640x360 480x360 384x288	(720p) 16:9 (PAL+) 16:9 4:3 (mHD) 16:9 4:3 4:3	30*1 30*1 30*1 30*1 30*1 30*1	30 30 30 30 30 30	20 20 20 20 20 20
Stream 3	MJPEG	640x360 480x360 384x288	(mHD) 16:9 4:3 4:3	15 15 15	15 15 15	15 15 15

Note:*1 Streams 2 and 3 are restricted to 15 FPS when Stream 1 is greater than 30 FPS.

Note:*2 Streams 1 and 2 are restricted to 30 FPS when TrueWDR 2x is enabled.

Note:*3 Streams 1 and 2 are restricted to 20 FPS when TrueWDR 3x is enabled.

Note:*4 The maximum frame rate of any stream is 30 FPS when corridor mode is enabled.

Note:*5 The maximum frame rate of any stream is 30 FPS when corridor mode is enabled.

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

Table 59 8MP Camera Stream Set (all resolution, codes and frame rate combinations of Stream 1, 2 and 3 are valid)

		Normal Mode				
		Resolution	Description	Max FPS		
				TWDR Off	TWDR 2x	TWDR 3x
Stream 1	H.264 H.265 H.264 IntelliZip H.265 IntelliZip MJPEG	3840x2160	(4K) 16:9	30	25	15
		3264x1840	16:9	30	25	15
		2688x1520	16:9	30	25	15
		1920x1080	(1080p) 16:9	60	25	15
		1664x936	(HD+) 16:9	60	25	15
		1280x720	(720p) 16:9	60	25	15
Stream 2	H.264 H.265 H.264 IntelliZip H.265 IntelliZip MJPEG	1280x720	(720p) 16:9	30*1	25	15
		1024x576	(PAL+) 16:9	30*1	25	15
		960x544	(qHD) 16:9	30*1	25	15
		816x464	16:9	30*1	25	15
		640x360	(mHD) 16:9	30*1	25	15
		480x272	16:9	30*1	25	15
Stream 3	MJPEG	640x360	(mHD) 16:9	30 *1	25	15
		480x272	4:3	30 *1	25	15

Note:*1 Stream 2 is restricted to 15 FPS when Stream 1 is greater than 30 FPS or when Stream 1 resolution is greater than 1920x1080.

Note:*2 Stream 3 is restricted to 10 FPS when Stream 1 is greater than 30 FPS or when Stream 1 resolution is greater than 1920x1080.

Note:*3 All streams are restricted to 25 FPS when TrueWDR 2x is enabled.

Note:*4 All streams are restricted to 15 FPS when TrueWDR 3x is enabled.

Note:*5 The maximum frame rate of any stream is 30 FPS when corridor mode is enabled.

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

Table 60 8MP Camera Stream Set (all resolution, codes and frame rate combinations of Stream 1, 2 and 3 are valid)

		Corridor Mode				
		Resolution	Description	Max FPS		
				TWDR Off	TWDR 2x	TWDR 3x
Stream 1	H.264 H.265 H.264 IntelliZip H.265 IntelliZip MJPEG	3840x2160	(4K) 16:9	30	25	15
		3264x1840	16:9	30	25	15
		2688x1520	16:9	30	25	15
		1920x1080	(1080p) 16:9	30	25	15
		1664x936	(HD+) 16:9	30	25	15
		1280x720	(720p) 16:9	30	25	15
Stream 2	H.264 H.265 H.264 IntelliZip H.265 IntelliZip MJPEG	1280x720	(720p) 16:9	30*1	25	15
		1024x576	(PAL+) 16:9	30*1	25	15
		960x544	(qHD) 16:9	30*1	25	15
		816x464	16:9	30*1	25	15
		640x360	(mHD) 16:9	30*1	25	15
		480x272	16:9	30*1	25	15
Stream 3	MJPEG	640x360	(mHD) 16:9	30 *1	25	15
		480x272	4:3	30 *1	25	15

Note:*1 Stream 2 is restricted to 15 FPS when Stream 1 is greater than 30 FPS or when Stream 1 resolution is greater than 1920x1080.

Note:*2 Stream 3 is restricted to 10 FPS when Stream 1 is greater than 30 FPS or when Stream 1 resolution is greater than 1920x1080.

Note:*3 All streams are restricted to 25 FPS when TrueWDR 2x is enabled.

Note:*4 All streams are restricted to 15 FPS when TrueWDR 3x is enabled.

Note:*5 The maximum frame rate of any stream is 30 FPS when corridor mode is enabled.

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

Appendix D: Camera Defaults

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

Table 61 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	Main	Main
	3MP Resolution	2048x1536	1280x720	640x360
	3MP Frame Rate (fps)	30	30	15
	3MP GOP Length [1-150]	30	30	N/A
	4K Resolution	3840x2160	1280x720	640x360
	4K Frame Rate (fps)	15	15	15
	4K GOP Length [1-150]	15	15	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

Tab	Item	Default		
Picture Basic				
	Mirror	OFF		
	Flip	OFF		
	Focus	Unspecified		
	Zoom	Unspecified		
	Exposure Method	Center Weighted		
	Exposure Offset (F-stops)	0		
	Min Exposure (sec)	1/10000		
	Max Exposure (sec)	1/8		
	Max Gain (dB)	51dB		
	Iris Level	1		
	Frequency	60Hz		
	Flickerless	OFF		
Picture Additional				
	Enable WDR	OFF		
	Enable IR Illuminator	ON		
	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				

Tab	Item	Default		
	Camera Friendly Name	Flex3-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		
	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		

Tab	Item	Default		
	FTP Port	21		
	Username	Unspecified		
	Password	Unspecified		
	Upload Path	Unspecified		
	Limit Transfer Rate	ON		
	Max Transfer Rate (Kbps)	50		
CIFS				
	Enable	ON		
	Network Path	Unspecified		
	Domain Name	Unspecified		
	Username	Unspecified		
	Password	Unspecified		
SIP				
	Enabled	Off		
	Domain	Empty or unspecified		
	Username	Empty or unspecified		
	Password	Empty or unspecified		
	Audio Source	Mic		
	Audio Output	Speaker		
	Extension	Empty or unspecified		
	Status	Bare SIP process not running!		
Event Actions				
	Fault action 1	Unspecified		
	Fault action 2	Unspecified		
	Fault action 3	Unspecified		
	Fault action 4	Unspecified		

Tab	Item	Default		
	Fault action 5	Unspecified		
Alarm I/O				
	Alarm input 1/2	Unspecified		
	Alarm out 1/2	Not Active		
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		
Home				
	Home Position Type	None		
Security				
	Security Status	Standard		
	Enhanced Security	Disabled		
	Authenticate Video	Disabled		
	Authentication	Basic		
Users				

Tab	Item	Default		
	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 Certificate 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		
Basic Filtering				
	ICMP Blocking	OFF		

Tab	Item	Default		
	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		
	Select Firmware Image File	Unspecified		

Tab	Item	Default		
Date Time				
	Camera Time			
	Time 24-hour	ON		
	Date Display Format	YYYY/MM/DD		
	Time Zone	Unspecified		
	Set Time	Unspecified		
	NTP Server Name	Unspecified		
Backup/Restore				
	Select Saved Data File	Unspecified		
Audio				
	Enable Audio	OFF		
	Input Enable	OFF		
	Input Volume	72		
	Output Enable	OFF		
	Output Volume	50		
Audio Clips				
	Audio Clips Table	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		

Tab	Item	Default		
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		
	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		

Tab	Item	Default		
	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		

Appendix E:Technical Specifications

The table below lists technical specifications of the Flex 3MP Indoor / Outdoor Dome camera and the Flex 8MP Outdoor Dome cameras.

	IFS08-D22-OI03 **Flex Gen3 - 8MP Outdoor Dome**	**IFS03-D21-OI03 / IFS03-D21-AT03 / IFS08-D22-AT03** **Flex Gen3 - 3MP Indoor / Outdoor Dome**
Video		
Imaging Device	1/1.8” 8.42MP CMOS	1/2.8" 3.21MP CMOS
Effective Pixels	3840(H) x 2160(V)	2065(H) x 1553(V)
Video Out	N/A	N/A
Lens		
Focal Length (Zoom Ratio)	3.6 - 11mm	YTOT 3.2 ~ 10mm (F1.4)
Max. Aperture Ratio	F/1.9	F1.6
Angular Field of View	100x60	100 x 70
Focus Control	Simple focus, (software controls: one-touch AF and manual control)	Simple focus, (software controls: one-touch AF and manual control)
Lens Type	Motorized varifocal	Motorized varifocal, P-Iris
Pan / Tilt / Rotate Range		
Pan / Tilt / Rotate Range	0˚~350˚ / 0˚~67˚ / 0˚~355˚	0˚~350˚ / 0˚~67˚ / 0˚~355˚
Operational		
IR Viewable Length	40m (Adaptive & Smart IR)	40m (Adaptive & Smart IR)
Camera Title	Illustra Flex3 8MP Dome Out	Illustra Flex3 3MP Dome Out
Day & Night	True Day/Night	Auto(ICR)
Backlight Compensation	Exposure Weighting: Top, Bottom, Left, Right, Full, Centre, Spot	Exposure Weighting: Top, Bottom, Left, Right, Full, Centre, Spot
Wide Dynamic Range	120dB	120dB
Digital Noise Reduction	2D&3DNR	2D&3DNR
Digital Image	No	No

Stabilization		
Motion Detection	3ea, polygonal zones	3ea, polygonal zones
Privacy Masking	9ea, rectangular zones	9ea, rectangular zones
Gain Control	Automatic & Manual (3dB increments)	Automatic & Manual (3dB increments)
White Balance	Automatic Wide, Automatic Normal, Manual	Automatic Wide, Automatic Normal, Manual
Lens Distortion Correction	Support	Support
Electronic Shutter Speed	Minimum 1/4s, Maximum 1/10,000s	Minimum 1/4s, Maximum 1/10,000s
Video Rotation	Mirror & Flip	Mirror & Flip
Alarm I/O	Input 1ea (digit) / Output 1ea	Input 1ea (digit) / Output 1ea
Alarm Triggers	Motion detection, Tampering Detection, Alarm input, Defocus detection, Network failure	Motion detection, Tampering Detection, Alarm input, Defocus detection, Network failure
Alarm Events	"Notification via e-mail SD/SDHC/SDXC at event triggers Alarm output"	"Notification via e-mail SD/SDHC/SDXC at event triggers Alarm output"
Audio In	Line in (via optional accessory cable)	Line in (Terminal block)
Audio Out	Line out (via optional accessory cable)	Line out (Terminal block)
Video Transmission Distance	100m Ethernet	100m Ethernet
Video Intelligence Analytics		
Standard	Motion Detection with metadata, Network failure	Motion Detection with metadata, Tampering, Defocus detection, Network failure
Advanced	Linger, Exit, Direction, Abandoned/Removed Objects, Dwell, Enter, Object Detection, Perimeter, Queue, Crowd	Linger, Exit, Direction, Abandoned/Removed objects, Queue, Dwell, Enter, Object detection, Perimeter
Face Detection	Yes	n/a
Tamper Detection	Scene Change	n/a
Blur Detection	Yes	n/a
Network		
Ethernet	10/100/1000 BaseT, RJ-45, Auto-Negotiation	RJ-45(10/100BASE-T)
Video Compression	MJPEG, H.264, H.264 IntelliZip, H.265 and H.265IntelliZip	MJPEG, H.264, H.264 IntelliZip, H.265 and H.265IntelliZip

Resolution	3840x2160 / 3264x1840 / 2688x1520 / 2560 x 1440 / 1920x1080 / 1664x936 / 1280x720 / 1024x576 / 960x544 / 816x464 / 640x360 / 480x272	2048x1536/ 1920x1080/ 1600x900/ 1280x960/ 1280x720/ 1024x768/ 800x600/ 640x480/ 640x360/ 480x360/ 384x288
Max. Framerate	8MP @ 30fps / 2MP @ 60fps	"H.265/H.264: Max. 3M@30fps, 2M@60fps MJPEG: Max. 20fps"
Smart Codec	IntelliZip	IntelliZip
Bitrate Control	H.264/H.265: CBR or VBR or CVBR	H.264/H.265: CBR or VBR or CVBR
Streaming	Multiple streaming (Up to 3 profiles)	Multiple streaming (Up to 3 profiles)
Audio Compression	G.711 alaw and ulaw selectable G.711 8KHz	"G.711 alaw and ulaw selectable G.711 8KHz"
Protocol	TCP/IP, IPv4, IPv6, TCP, UDP, HTTP, FTP, DHCP, WS-Discovery, DNS, DDNS, RTP, RTCP, RTSP, TLS, Unicast, Multicast, NTP, ICMP, IGMP, SMTP, WS-Security, IEEE 802.1x, PEAP, EAP-TLS, EAPoL, SSH, HTTPS, SOAP, WSAddressing, CIFS, SNMP, UPNP, RTSP, LLDP	TCP/IP, IPv4, IPv6, TCP, UDP, HTTP, FTP, DHCP, WS-Discovery, DNS, DDNS, RTP, RTCP, RTSP, TLS, Unicast, Multicast, NTP, ICMP, IGMP, SMTP, WS-Security, IEEE 802.1x, PEAP, EAP-TLS, EAPoL, SSH, HTTPS, SOAP, WSAddressing, CIFS, SNMP, UPNP, RTSP, LLDP
Security	TLS - RFC5246 v1.2, HTTPS (HTTP over TLS) - RFC2818, WS-Security, Certificate Management, Multi-Level Password Protection, IP Address/ Filtering, HTTPS Encryption, One-Click Security Hardening, User Access Log, Validate Complex Credentials, Disabling Unused Protocols, IEEE / 802.1x Including: PEAP, EAP-TLS, EAPoL	TLS - RFC5246 v1.2, HTTPS (HTTP over TLS) - RFC2818, WS-Security, Certificate Management, Multi-Level Password Protection, IP Address/ Filtering, HTTPS Encryption, One-Click Security Hardening, User Access Log, Validate Complex Credentials, Disabling Unused Protocols, IEEE / 802.1x Including: PEAP, EAP-TLS, EAPoL
Edge Storage	micro SDXC up to 512GB	Micro SD/SDHC/SDXC 1slot 256GB
Application Programming Interface	IAPI, ONVIF	IAPI, ONVIF
Memory	512MB RAM, 512MB Flash	512MB RAM, 512MB Flash
Environmental		
Operating Temperature / Humidity	-40C to +60C* / Less than 90% RH. Up to 5 concurrent hours at 60C.	"-40°C ~ +50°C / Less than 90% RH Up to 4 concurrent hours at up to 60°C"
Storage Temperature / Humidity	-20°C ~ +60°C / Less than 90% RH	-20°C ~ +60°C / Less than 90% RH
Certification	IP66/ IP67, IK10	IP66/ IP67, IK10
Electrical		
Input Voltage	24 VAC (-20% ~ +30%, 47 ~ 63 Hz) , PoE 802.3af (802.3at Type 1)	24 VAC (-20% ~ +30%, 47 ~ 63 Hz) , PoE 802.3af (802.3at Type 1)

Mechanical		
Color / Material	White / Aluminum	White / Aluminum
RAL Code	RAL9003	RAL9003
Product dimensions / weight	145 x 106	145 x 106
Regulatory		
Safety	EN60950-1; UL60950-1; IEC 60950-1; CSA 22.2 No. 60950	EN60950-1; UL60950-1; IEC 60950-1; CSA 22.2 No. 60950
Emissions	FCC Part 15 Class A; EN55032 Class A; AS/NZS CISPR 32 Class A; ICES-003/NMB-003 Class A	FCC Part 15 Class A; EN55032 Class A; AS/NZS CISPR 32 Class A; ICES-003/NMB-003 Class A
Immunity	EN55024; EN50130-3	EN55024; EN50130-3
Environment	RoHS; WEEE	RoHS; WEEE

The table below lists technical specifications of the Flex 3MP Indoor Bullet camera and the Flex 8MP Indoor Bullet camera.

	IFS03-B21-OI03 **Flex Gen3 - 3MP Indoor Bullet**	**IFS08-B22-OI03** **Flex Gen3 - 8MP Indoor Bullet**
Video		
Imaging Device	1/2.8" 3.21MP CMOS	1/1.8” 8.42MP CMOS
Effective Pixels	2065(H) x 1553(V)	3840(H) x 2160(V)
Video Out	N/A	N/A
Lens		
Focal Length (Zoom Ratio)	YTOT 3.2 ~ 10mm (F1.4)	Y3.6 - 11mm
Max. Aperture Ratio	F/1.6	F1.9
Angular Field of View	100 x 70	100 x 60
Focus Control	Simple focus, (software controls: one-touch AF and manual control)	Simple focus, (software controls: one-touch AF and manual control)
Lens Type	Motorized varifocal, P-Iris	Motorized varifocal
Pan / Tilt / Rotate Range		
Pan / Tilt / Rotate Range	0˚~350˚ / 0˚~67˚ / 0˚~355˚	0˚~350˚ / 0˚~67˚ / 0˚~355˚
Operational		
IR Viewable Length	40m (Adaptive & Smart IR)	40m (Adaptive & Smart IR)
Camera Title	Illustra Flex3 3MP Bullet	Illustra Flex3 8MP Bullet
Day & Night	Auto(ICR)	True Day/Night
Backlight Compensation	Exposure Weighting: Top, Bottom, Left, Right, Full, Centre, Spot	Exposure Weighting: Top, Bottom, Left, Right, Full, Centre, Spot
Wide Dynamic Range	120dB	120dB
Digital Noise Reduction	2D&3DNR	2D&3DNR
Digital Image Stabilization	No	No
Motion Detection	3ea, polygonal zones	3ea, polygonal zones
Privacy Mask-	9ea, rectangular zones	9ea, rectangular zones

ing		
Gain Control	Automatic & Manual (3dB increments)	Automatic & Manual (3dB increments)
White Balance	Automatic Wide, Automatic Normal, Manual	Automatic Wide, Automatic Normal, Manual
Lens Distortion Correction	Support	Support
Electronic Shutter Speed	Minimum 1/4s, Maximum 1/10,000s	Minimum 1/4s, Maximum 1/10,000s
Video Rotation	Mirror & Flip	Mirror & Flip
Alarm I/O	Input 1ea (digit) / Output 1ea	Input 1ea (digit) / Output 1ea
Alarm Triggers	Motion detection, Tampering Detection, Alarm input, Defocus detection, Network failure	Motion detection, Tampering Detection, Alarm input, Defocus detection, Network failure
Alarm Events	"Notification via e-mail SD/SDHC/SDXC at event triggers Alarm output"	"Notification via e-mail SD/SDHC/SDXC at event triggers Alarm output"
Audio In	Line in (Terminal Block)	Line in (via optional accessory cable)
Audio Out	Line out (Terminal Block)	Line out (via optional accessory cable)
Video Transmission Distance	100m Ethernet	100m Ethernet
Video Intelligence Analytics		
Standard	Motion Detection with metadata, Tampering, Defocus detection, Network failure	Motion Detection with metadata, Network failure
Advanced	Linger, Exit, Direction, Abandoned/Removed objects, Queue, Dwell, Enter, Object detection, Perimeter	Linger, Exit, Direction, Abandoned/Removed Objects, Dwell, Enter, Object Detection, Perimeter, Queue, Crowd
Face Detection	n/a	Yes
Tamper Detection	n/a	Scene Change
Blur Detection	n/a	Yes
Network		
Ethernet	RJ-45(10/100BASE-T)	10/100/1000 BaseT, RJ-45, Auto-Negotiation
Video Compression	MJPEG, H.264, H.264 IntelliZip, H.265 and H.265IntelliZip	MJPEG, H.264, H.264 IntelliZip, H.265 and H.265IntelliZip
Resolution	2048x1536/ 1920x1080/ 1600x900/ 1280x960/ 1280x720/ 1024x768/ 800x600/ 640x480/ 640x360/ 480x360/ 384x288	3840x2160 / 3264x1840 / 2688x1520 / 2560 x 1440 / 1920x1080 / 1664x936 / 1280x720 / 1024x576 / 960x544 / 816x464 / 640x360 / 480x272
Max. Framerate	"H.265/H.264: Max. 3M@30fps, 2M@60fps	8MP @ 30fps / 2MP @ 60fps

	MJPEG: Max. 20fps"	
Smart Codec	IntelliZip	IntelliZip
Bitrate Control	H.264/H.265: CBR or VBR or CVBR	H.264/H.265: CBR or VBR or CVBR
Streaming	Multiple streaming (Up to 3 profiles)	Multiple streaming (Up to 3 profiles)
Audio Compression	G.711 alaw and ulaw selectable G.711 8KHz	"G.711 alaw and ulaw selectable G.711 8KHz"
Protocol	TCP/IP, IPv4, IPv6, TCP, UDP, HTTP, FTP, DHCP, WS-Discovery, DNS, DDNS, RTP, RTCP, RTSP, TLS, Unicast, Multicast, NTP, ICMP, IGMP, SMTP, WS-Security, IEEE 802.1x, PEAP, EAP-TLS, EAPoL, SSH, HTTPS, SOAP, WSAddressing, CIFS, SNMP, UPNP, RTSP, LLDP	TCP/IP, IPv4, IPv6, TCP, UDP, HTTP, FTP, DHCP, WS-Discovery, DNS, DDNS, RTP, RTCP, RTSP, TLS, Unicast, Multicast, NTP, ICMP, IGMP, SMTP, WS-Security, IEEE 802.1x, PEAP, EAP-TLS, EAPoL, SSH, HTTPS, SOAP, WSAddressing, CIFS, SNMP, UPNP, RTSP, LLDP
Security	TLS - RFC5246 v1.2, HTTPS (HTTP over TLS) - RFC2818, WS-Security, Certificate Management, Multi-Level Password Protection, IP Address/ Filtering, HTTPS Encryption, One-Click Security Hardening, User Access Log, Validate Complex Credentials, Disabling Unused Protocols, IEEE / 802.1x Including: PEAP, EAP-TLS, EAPoL	TLS - RFC5246 v1.2, HTTPS (HTTP over TLS) - RFC2818, WS-Security, Certificate Management, Multi-Level Password Protection, IP Address/ Filtering, HTTPS Encryption, One-Click Security Hardening, User Access Log, Validate Complex Credentials, Disabling Unused Protocols, IEEE / 802.1x Including: PEAP, EAP-TLS, EAPoL
Edge Storage	Micro SD/SDHC/SDXC 1slot 256GB	micro SDXC up to 512GB
Application Programming Interface	IAPI, ONVIF	IAPI, ONVIF
Memory	I512MB RAM, 512MB Flash	512MB RAM, 512MB Flash
	Environmental	
Operating Temperature / Humidity	"-40°C ~ +50°C / Less than 90% RH Up to 4 concurrent hours at up to 60°C"	-40C to +60C* / Less than 90% RH. Up to 5 concurrent hours at 60C.
Storage Temperature / Humidity	--20°C ~ +60°C / Less than 90% RH	-20°C ~ +60°C / Less than 90% RH
Certification	IP66/ IP67, IK10	IP66/ IP67, IK10
	Electrical	
Input Voltage	24 VAC (-20% ~ +30%, 47 ~ 63 Hz) , PoE 802.3af (802.3at Type 1)	24 VAC (-20% ~ +30%, 47 ~ 63 Hz) , PoE 802.3af (802.3at Type 1)
	Mechanical	
Color / Material	White / Aluminum	White / Aluminum
RAL Code	RAL9003	RAL9003

Product dimensions / weight	Body: 188 x 91 Bracket: 164 x 120	Body: 188 x 91 Bracket: 164 x 120
Regulatory		
Safety	EN60950-1; UL60950-1; IEC 60950-1; CSA 22.2 No. 60950	EN60950-1; UL60950-1; IEC 60950-1; CSA 22.2 No. 60950
Emissions	FCC Part 15 Class A; EN55032 Class A; AS/NZS CISPR 32 Class A; ICES-003/NMB-003 Class A	FCC Part 15 Class A; EN55032 Class A; AS/NZS CISPR 32 Class A; ICES-003/NMB-003 Class A
Immunity	EN55024; EN50130-3	EN55024; EN50130-3
Environment	RoHS; WEEE	RoHS; WEEE

The table below lists technical specifications of the Flex 3MP Outdoor Compact Dome camera and the Flex 8MP Outdoor Compact Dome cameras.

	IFS03-C10-OI03 **Flex Gen3 - 3MP Outdoor Compact Dome**	**IFS08-C10-OI03** **Flex Gen3 - 8MP Outdoor Compact Dome**
Video		
Imaging Device	'1/2.8" 3.21MP CMOS (4:3)	'1/1.8" 8.3MP CMOS (16:9)
Effective Pixels	2065(H) x 1553(V)	3840(H) x 2160(V)
Min. Illumination	Color: min 0.05 lux (1/30sec, 30IRE) BW: 0.005Lux	Color: min 0.27 lux (1/30sec, 30IRE) BW: 0.027Lux
Video Out	Micro USB (for easy installation,Wi-Fi dongle)	Micro USB (for easy installation,Wi-Fi dongle)
Lens		
Focal Length (Zoom Ratio)	2.8mm fixed focal	4.27mm fixed focal
Max. Aperture Ratio	F2.0	F1.6
Angular Field of View	H:100.13˚ V:73.79˚ D:128˚	H: 107.97°/ V: 58.02°/ D: 126.87°
Focus Control	Fixed (peak focus at 5m)	Fixed (peak focus at 5m)
Lens Type	None	None
Pan / Tilt / Rotate Range		
Pan / Tilt / Rotate Range	0˚~350˚ / 0˚~67˚/ 0˚~355˚	0˚~350˚ / 0˚~67˚ / 0˚~355˚
Operational		
IR Viewable Length	15M (including smart IR control)	15M (including smart IR control)
Exposure Mode	Manual/ Shutter Priority	Manual/ Shutter Priority
Electronic Shutter Speed	Minimum / Maximum / Manual/ Flickerless (1/4~1/10,000sec)	Minimum / Maximum / Manual/ Flickerless (1/4~1/10,000sec)
Picture Adjustment	Brightness/ Contrast/ Saturation/ Hue/ Sharpness (0~100%, default 50%)	Brightness/ Contrast/ Saturation/ Hue/ Sharpness (0~100%, default 50%)
Day & Night	Auto Low/ Auto Mid(Default)/ Auto High/ Manual/ Forced Color/ Force B&W	Auto Low/ Auto Mid(Default)/ Auto High/ Manual/ Forced Color/ Force B&W
Wide Dynamic Range	Off (Default)/ On/ WDR/ TrueWDR/ TrueWDR3x	Off (Default)/ On/ WDR/ TrueWDR/ TrueWDR3x
Digital Noise Reduction	2D&3DNR	2D&3DNR

Motion Detection	3ea, polygonal zones	3ea, polygonal zones
Privacy Masking	9ea, rectangular zones	9ea, rectangular zones
White Balance	Auto Normal (Default) /Manual/ Auto Wide	Auto Normal (Default) /Manual/ Auto Wide
Alarm I/O	n/a	n/a
Alarm Triggers	Motion detection, Tampering Detection, Alarm input, Defocus detection, Network failure	Motion detection, Tampering Detection, Alarm input, Defocus detection, Network failure
Alarm Events	"Notification via e-mail SD/SDHC/SDXC at event triggers Alarm output"	"Notification via e-mail SD/SDHC/SDXC at event triggers Alarm output"
Audio In	n/a	n/a
Audio Out	n/a	n/a
Video Intelligence Analytics		
Analytics	Tampering,Defocus(HTW) / Motion Detection	Tampering,Defocus(HTW) / Motion Detection
Network		
Ethernet	RJ-45(10/100BASE-T)	RJ-45(10/100BASE-T)
Video Compression	MJPEG, H.264, H.264 IntelliZip, H.265 and H.265IntelliZip	MJPEG, H.264, H.264 IntelliZip, H.265 and H.265IntelliZip
Resolution	2048x1536/ 1920x1440/ 1920x1080/ 1600x1200/ 1600x900/ 1280x960/ 1280x720/ 1024x768/ 1024x576/ 960x540/ 800x450/ 640x480/ 640x360/ 480x360/ 480x270/ 384x288/ 320x180/ 160x90	2048x1536/ 1920x1440/ 1920x1080/ 1600x1200/ 1600x900/ 1280x960/ 1280x720/ 1024x768/ 1024x576/ 960x540/ 800x450/ 640x480/ 640x360/ 480x360/ 480x270/ 384x288/ 320x180/ 160x90
Max. Framerate	H.265/H.264: Max. 30fps MJPEG: Max. 20fps	H.265/H.264: Max. 30fps MJPEG: Max. 20fps
Smart Codec	IntelliZip	IntelliZip
Bitrate Control	H.264/H.265: CBR or VBR or CVBR	H.264/H.265: CBR or VBR or CVBR
Streaming	Multiple streaming (Up to 3 profiles)	Multiple streaming (Up to 3 profiles)
Audio Compression	G.711 alaw and ulaw selectable G.711 8KHz	G.711 alaw and ulaw selectable G.711 8KHz
Protocol	TCP/IP, IPv4, IPv6, TCP, UDP, HTTP, FTP, DHCP, WS-Discovery, DNS, DDNS, RTP, RTCP, RTSP, TLS, Unicast, Multicast, NTP, ICMP, IGMP, SMTP, WS-Security, IEEE 802.1x, PEAP, EAP-TLS, EAPoL, SSH, HTTPS, SOAP, WSAddressing, CIFS, SNMP, UPNP, RTSP, LLDP	TCP/IP, IPv4, IPv6, TCP, UDP, HTTP, FTP, DHCP, WS-Discovery, DNS, DDNS, RTP, RTCP, RTSP, TLS, Unicast, Multicast, NTP, ICMP, IGMP, SMTP, WS-Security, IEEE 802.1x, PEAP, EAP-TLS, EAPoL, SSH, HTTPS, SOAP, WSAddressing, CIFS, SNMP, UPNP, RTSP, LLDP

Security	TLS - RFC5246 v1.2, HTTPS (HTTP over TLS) - RFC2818, WS-Security, Certificate Management, Multi-Level Password Protection, IP Address/ Filtering, HTTPS Encryption, One-Click Security Hardening, User Access Log, Validate Complex Credentials, Disabling Unused Protocols, IEEE / 802.1x Including: PEAP, EAP-TLS, EAPoL	TLS - RFC5246 v1.2, HTTPS (HTTP over TLS) - RFC2818, WS-Security, Certificate Management, Multi-Level Password Protection, IP Address/ Filtering, HTTPS Encryption, One-Click Security Hardening, User Access Log, Validate Complex Credentials, Disabling Unused Protocols, IEEE / 802.1x Including: PEAP, EAP-TLS, EAPoL
Edge Storage	Micro SD/SDHC/SDXC 1slot 256GB	micro SDXC up to 512GB
Application Programming Interface	IAPI-3	IAPI, ONVIF
Memory	1GB RAM, 512MB Flash (lockable NAND)	1GB RAM, 512MB Flash (lockable NAND)
Environmental		
Operating Temperature / Humidity	-40°C ~ +50°C (-4°F ~ +122°F)	-40°C ~ +50°C (-4°F ~ +122°F)
Cold start	-40°C	-40°C
Storage Temperature / Humidity	-40°C ~ +55°C	-40°C ~ +55°C
Electrical		
Input Voltage	2PoE 802.3af (802.3at Type 1)	2PoE 802.3af (802.3at Type 1)
Power Consumption	'PoE: Max 8.1W	'PoE: Max 10.1W
RTC Consumption	7 days	7 days
Mechanical		
Color / Material	White / Aluminum	White / Aluminum
RAL Code	RAL9003	RAL9003
Product dimensions / weight	Φ112 x 72 mm	Φ112 x 72 mm
Regulatory		
Safety	UL60950-1; CAN/CSA-C22.2 No. 60950-1, BIS IS13252 Part 1:2010,	UL60950-1; CAN/CSA-C22.2 No. 60950-1, BIS IS13252 Part 1:2010,
Emissions	FCC Part 15 Class A; EN55032 Class A; AS/NZS CISPR 32 Class A; ICES-003/NMB-003 Class A	FCC Part 15 Class A; EN55032 Class A; AS/NZS CISPR 32 Class A; ICES-003/NMB-003 Class A
Immunity	EN50130-4	EN50130-4

Environment	RoHS; WEEE, REACH	RoHS; WEEE, REACH
Physical and Environment	IP66/67, IK10	IP66/67, IK10

End User License Agreement (EULA)

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

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

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

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

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

c. Remotely Stored Components. The Software may also include a software code component for operating one or more devices remotely. You may install and/or use one copy of such component of the Software on a remote storage device on an internal network with all of the devices and may operate such component with each device over the internal network solely in the manner set forth in any accompanying documentation or, in the absence of such, solely in the manner contemplated by the nature of the Software; provided however, you must still acquire the required number of licenses for each of the devices with which such component is to be operated. d. Embedded Software/Firmware. The Software may also include a software code component that is resident in a device as provided by Tyco for operating that device. You may use such component of the Software solely in connection with the use of that device, but may not retrieve, copy or otherwise transfer that software component to any other media or device without Tyco's express prior written authorization.

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

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

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

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

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

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

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

f. Incorporation of "Open Source" and other Third Party Software. Portions of the Software may be subject to certain third party license agreements governing the use, copying, modification, redistribution and warranty of those portions of the Software, including what is commonly known as "open source" software. Such portions of the Software are governed solely by the terms of such other license, and no warranty is provided under this License for open source software. By using the Software you are also agreeing to be bound to the terms of such third party licenses. If provided for in the applicable third party license, you may have a right to reverse engineer such software or receive source code for such software for use and distribution in any program that you create, so long as you in turn agree to be bound to the terms of the applicable third party license, and your programs are distributed under the terms of that license. If applicable, a copy of such source code may be obtained free of charge by contacting your Tyco representative.

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

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

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

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

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

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

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

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

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

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

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

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

6. LIMITED WARRANTY.

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

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

7. LIMITATION OF LIABILITY & EXCLUSION OF DAMAGES.

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

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

9. ADDITIONAL NOTICES.

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

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

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

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

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

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

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

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

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

f. Incorporation of "Open Source" and other Third Party Software. Portions of the Software may be subject to certain third party license agreements governing the use, copying, modification, redistribution and warranty of those portions of the Software, including what is commonly known as "open source" software. Such portions of the Software are governed solely by the terms of such other license, and no warranty is provided under this License for open source software. By using the Software you are also agreeing to be bound to the terms of such third party licenses. If provided for in the applicable third party license, you may have a right to reverse engineer such software or receive source code for such software for use and distribution in any program that you create, so long as you in turn agree to be bound to the terms of the applicable third party license, and your programs are distributed under the terms of that license. If applicable, a copy of such source code may be obtained free of charge by contacting your Tyco representative.

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

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

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

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

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

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

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

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

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.