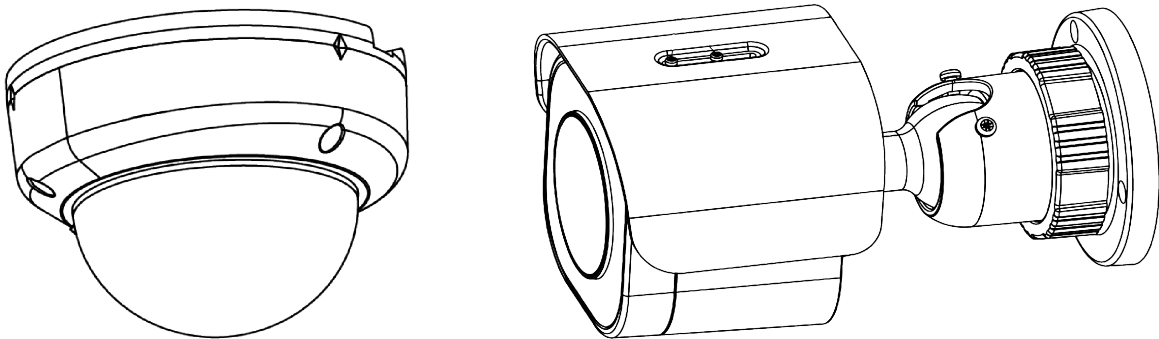


Illustra

Illustra Essentials Gen 4 Series Installation and Configuration Guide



Notice

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

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

Copyright

This product includes advanced facial detection technology developed by INTELLIVISION.

Under copyright laws, the contents of this manual may not be copied, photocopied, reproduced, translated or reduced to any electronic medium or machine-readable form, in whole or in part, without prior written consent of Tyco Security Products.

© 2023 Tyco Security Products. All rights reserved.

Tyco Security Products

6600 Congress Avenue

Boca Raton, FL 33487 U.S.A.

Customer Service

Thank you for using Illustra products. We support our products through an extensive worldwide network of dealers. The dealer through whom you originally purchased this product is your point of contact if you need service or support. Our dealers are empowered to provide the very best in customer service and support. Dealers in North America should contact Illustra at (800) 507-6268 (dial Option 1) or (800) 392-2873 (dial Option 2). For other regions, please visit www.illustracameras.com.

Tyco Illustra Cameras

Tyco Illustra is a leading video surveillance specialist. Our domestic & commercial options give high-performance with affordability. Browse our products.

Camera Firmware Upgrade

The camera can be upgraded via the web GUI using firmware provided by Illustra which can be found on www.illustracameras.com. The firmware can also be upgraded using the Illustra Connect tool (windows based) or Illustra Tools (mobile app) or victor/VideoEdge, which also provides bulk firmware upgrade capability. Please refer to the respective application documents for further information.

Trademarks

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

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

Table of Contents

| | |
|---|-----------|
| Overview | 5 |
| Illustra Essentials Gen 4 Dome cameras | 6 |
| Product overview | 6 |
| Installation | 6 |
| Illustra Essentials Gen 4 Bullet cameras | 13 |
| Product overview | 13 |
| Installation | 13 |
| Network Topology | 20 |
| Network Connection | 22 |
| Default IP Address | 22 |
| DHCP | 23 |
| Managing cameras with the Illustra Connect tool | 24 |
| Configuration | 27 |
| Live menu | 30 |
| Quick Start Menu | 32 |
| Basic Configuration | 32 |
| Video Menu | 49 |
| Streams | 49 |
| Picture Settings | 54 |
| Privacy Zones | 63 |
| Events and Actions Menu | 66 |
| Event Settings | 66 |
| Event Actions | 70 |
| Analytics | 71 |
| Event Logs | 74 |
| Security | 76 |
| Security Status | 76 |
| Security Status | 78 |
| Users | 78 |

| | |
|--|------------|
| HTTP/HTTPS | 80 |
| IEEE 802.1x | 82 |
| Firewall | 82 |
| Remote Access | 84 |
| Session Timeout | 86 |
| Network Menu | 87 |
| TCP/IP | 87 |
| FTP | 88 |
| SMTP | 90 |
| SNMP | 91 |
| Heartbeat | 93 |
| Dynamic DNS | 93 |
| System | 95 |
| Maintenance | 95 |
| Date / Time | 99 |
| Health Monitor | 100 |
| Logs | 100 |
| About | 101 |
| Edge Recording | 103 |
| Micro SD Card Management | 103 |
| Record Settings | 105 |
| Event Download | 106 |
| Appendix A: User Account Access | 107 |
| Appendix B: Using Media Player to View RTSP Streaming | 109 |
| Appendix C: Stream Tables | 110 |
| Appendix D: Camera Defaults | 112 |
| Appendix E: Technical Specifications | 120 |
| END USER LICENSE AGREEMENT (EULA) | 128 |

Overview

This Illustra Essentials Gen 4 Installation and Configuration Guide is a user manual which provides physical properties, installation, and configuration information of the cameras in Table 1 on Page 5.

Table 1 Product codes

| Product Code | Model Name | Description |
|----------------|--|--|
| IES02-D10-OI04 | Illustra Essentials Gen 4, 2MP Fixed Dome camera | Illustra Essentials Gen 4, 2MP Dome, 2.8mm, Outdoor, vandal, clear, white, TDN w/IR |
| IES02-D12-OI04 | Illustra Essentials Gen 4, 2MP Varifocal Dome camera | Illustra Essentials Gen 4, 2MP Dome, 2.7-13.5mm, Outdoor, vandal, clear, white, TDN w/IR |
| IES02-B10-BI04 | Illustra Essentials Gen 4, 2MP Fixed Bullet camera | Illustra Essentials Gen 4, 2MP Bullet, 2.8mm, Outdoor, vandal, white, TDN w/IR |
| IES02-B12-BI04 | Illustra Essentials Gen 4, 2MP Varifocal Bullet camera | Illustra Essentials Gen 4, 2MP Bullet, 2.7-13.5mm, Outdoor, vandal, white, TDN w/IR |

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

- For the Illustra Essentials Gen 4 Dome cameras, refer to Illustra Essentials Gen 4 Dome cameras on page 6.
- For the Illustra Essentials Gen 4 Bullet cameras, refer to Illustra Essentials Gen 4 Bullet cameras on page 13.

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 27 for procedural information pertaining to camera configuration.

Illustra Essentials Gen 4 Dome cameras

This chapter provides product features, installation procedures, and connection information regarding the Illustra Essentials Gen 4 Dome cameras.

Product overview

This chapter explains the installation of the Illustra Essentials Gen 4 2MP Dome cameras. Product codes and description of the cameras are provided in Table 2 on page 6.

Table 2 Product code and description of the Essential Gen 4 2MP Dome cameras

| Product Code | Model Name | Description |
|----------------|--|--|
| IES02-D10-OI04 | Illustra Essentials Gen 4, 2MP Fixed Dome camera | Illustra Essentials Gen 4, 2MP Dome, 2.8mm, Outdoor, vandal, clear, white, TDN w/IR |
| IES02-D12-OI04 | Illustra Essentials Gen 4, 2MP Varifocal Dome camera | Illustra Essentials Gen 4, 2MP Dome, 2.7-13.5mm, Outdoor, vandal, clear, white, TDN w/IR |

Installation

In the box

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

- 1 x Essentials Indoor / Outdoor Dome camera
- 1 x Printed Quick Guide
- 1 x Desiccant
- 1 x Torx Wrench
- 3 x Plastic Anchors
- 3 x Tapping Screws
- 1 x Mounting Guide Pattern

Contact your dealer if any item is missing.

Installation tools

The following tools assist with installation:

- Drill
- Screw Drivers
- Wire cutters

Quick reference

- Default IP: 192.168.1.168 (DHCP enabled)
- Default Username: admin
- Default Password: admin
- Power: 12Vdc / PoE (IEEE 802.3af Class 3)

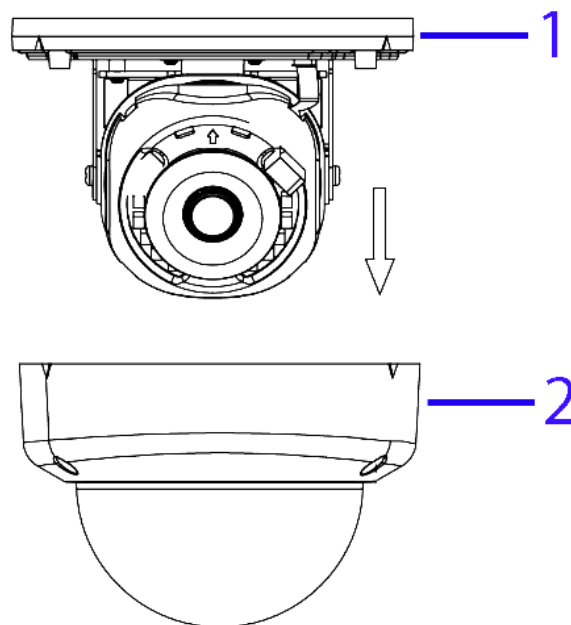
Checking appearance

When first unboxing, check whether if there is any visible damage to the appearance of the unit and its accessories. The protective materials used for the packaging should be able to protect the unit from most types of accidents during transportation. Remove the protective part of the unit when every item is checked in accordance with the list in Installation tools on page 7.

Procedure 1 Disassembling the camera.

| Step | Action |
|------|---|
| 1 | Use the Torx wrench to loosen the three screws on the camera top cover (1) (Figure 3) and gently remove the cover (2) (Figure 3). |

Figure 3 Removing the camera top cover



- End -

Internal Interface pictorial index

Figure 4 Internal interface pictorial index

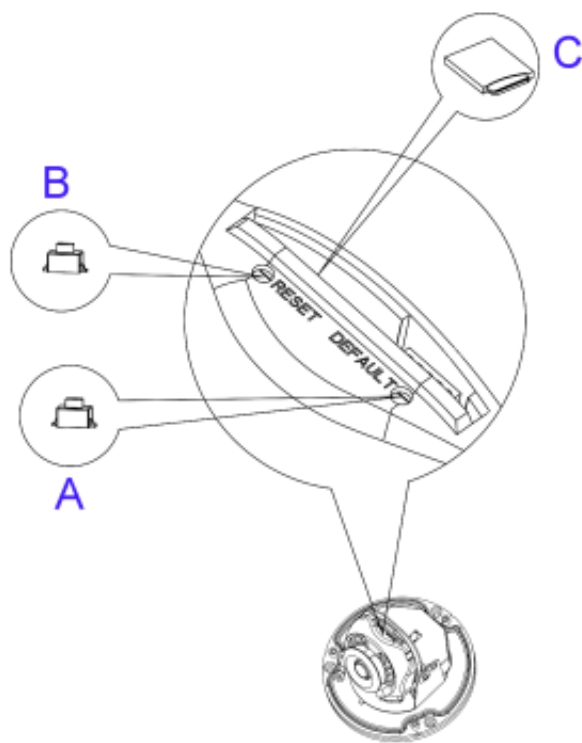


Table 5 Internal interface pictorial index descriptions

| | Name | Description |
|---|--------------------|--|
| A | Reboot Button | Press and release to reboot the camera. |
| B | Reset Button | Press the button for 5 seconds to reset the camera. |
| C | Micro SD card slot | Insert a micro SD card into the slot for video recording and file storage. |

Procedure 2 Mounting the camera

| Step | Action |
|------|--|
| 1 | Place the mounting template on the wall / ceiling and drill three Ø4.5mm holes. |
| 2 | Insert the three plastic anchors into the three holes. |
| 3 | Determine how the camera pigtail cable should be routed: <ul style="list-style-type: none"> • Through the cable entry on top of the camera (Figure 6) |

Note: If required then drill a cable hole on the wall as identified on the mounting template.

OR

- Through the cable side entry slot (Figure 7)

Note: You do not need to drill a cable hole on the wall as identified on the mounting template when using the cable side entry slot.

- 4 Route the camera pigtail cable as per one of the options in step 3 and place the camera onto the wall / ceiling and align the holes on the camera with the three holes on the wall / ceiling.

Figure 6 Cable hole on top of the camera body

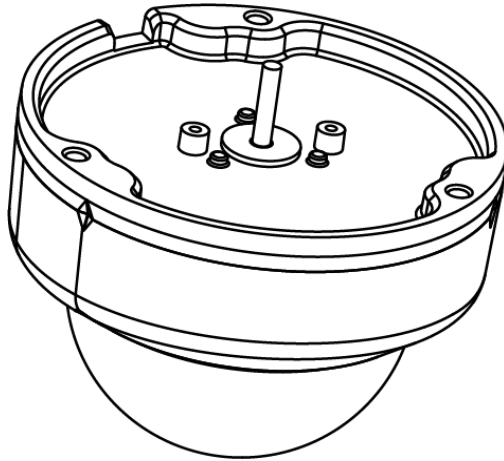
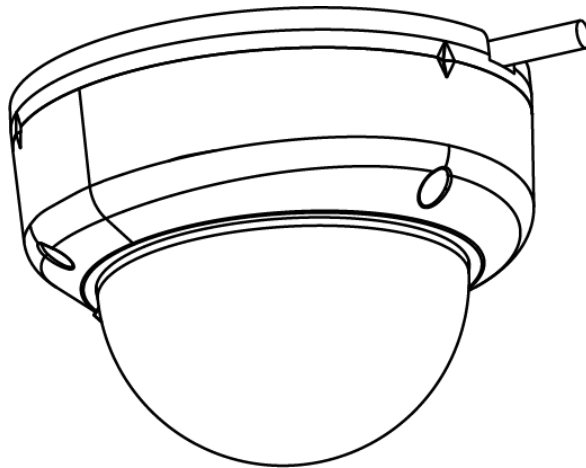
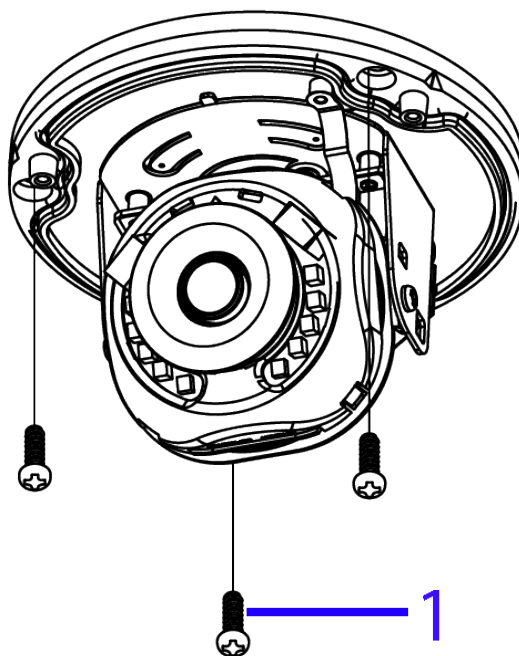


Figure 7 Cable side entry slot



- 5 Insert the three tapping screws (1) (Figure 8) into the three holes on the camera body and using the screw driver securely attach the camera to the wall / ceiling.

Figure 8 Inserting the three tapping screws into the camera body

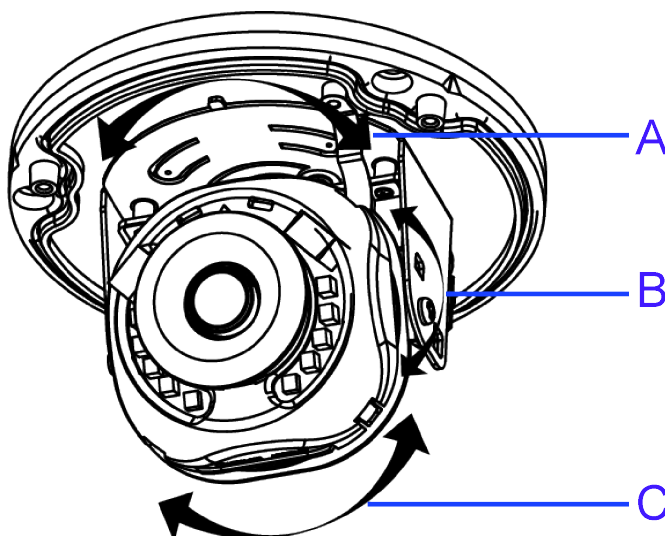


- End -

Procedure 3 Adjusting the camera position

The camera has three axes to adjust the field of view for different Applications (Figure 9). While screening live view on your monitor, adjust the axes as per the information below.

Figure 9 Adjusting the camera position



- **Pan Adjustment** (A – Figure 9) Rotate the lens base until satisfied with the field of view. Please DO NOT rotate over the default limit of $>355^{\circ}$.
- **Tilt Adjustment** (B – Figure 9) Tilt the camera lens within the certain range (70°) to your desired field of view.

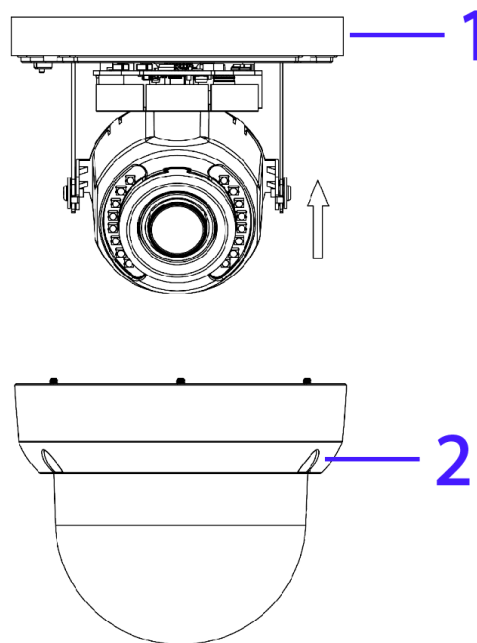
- **Horizontal Rotation** (C – Figure 9) Rotate the 3D assembly in the lens, DO NOT turn the assembly more than the limit ($\pm 355^\circ$) as this may result in the internal cables becoming twisted, disconnected, or broken.

- End -

Procedure 4 Assembling the camera

| Step | Action |
|------|---|
| 1 | Place the camera top cover (2) (Figure 10) onto the camera body (1) (Figure 10). |
| 2 | Use the Torx wrench to securely attach the three Torx screws located on the camera top cover (2) (Figure 10). |

Figure 10 Attaching the camera top cover



- End -

Procedure 5 Powering up the camera

- 12Vdc: Connect the 12Vdc cable to the DC 12V terminal.
- OR
- PoE: Connect the RJ-45 jack to a PoE compatible network device that supplies power through the Ethernet cable.

- 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 Essentials Gen 4 Bullet cameras

This chapter provides product features, installation procedures, and connection information regarding the Illustra Essentials Gen 4 Bullet cameras.

Product overview

This chapter explains the installation of the Illustra Essentials Gen 4 2MP Bullet cameras. Product codes and description of the cameras are provided in Table 11 on page 13.

Table 11 Product code and description of the Essentials Gen 4 Bullet cameras

| Product Code | Model Name | Description |
|----------------|--|---|
| IES02-B10-BI04 | Illustra Essentials Gen 4, 2MP Fixed Bullet camera | Illustra Essentials Gen 4, 2MP Bullet, 2.8mm, Outdoor, vandal, white, TDN w/IR |
| IES02-B12-BI04 | Illustra Essentials Gen 4, 2MP Varifocal Bullet camera | Illustra Essentials Gen 4, 2MP Bullet, 2.7-13.5mm, Outdoor, vandal, white, TDN w/IR |

Installation

In the box

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

- 1 x Essentials Outdoor IR Bullet camera
- 1 x Printed Quick Start Guide
- 1 x Torx wrench
- 3 x Plastic anchors
- 3 x Tapping screws
- 1 x Mounting template
- 1 x T6 Wrench 130mm X 30mm (Varifocal Camera)

Contact your dealer if any item is missing.

Installation tools

The following tools assist with installation:

- 1 x Drill
- 1 x Screwdrivers
- 1 x Wire cutters

Quick reference

- Default IP: 192.168.1.168 (DHCP enabled)
- Default Username: admin
- Default Password: admin
- Power: PoE (IEEE 802.3af Class 3)

Figure 12 Camera parts and connections

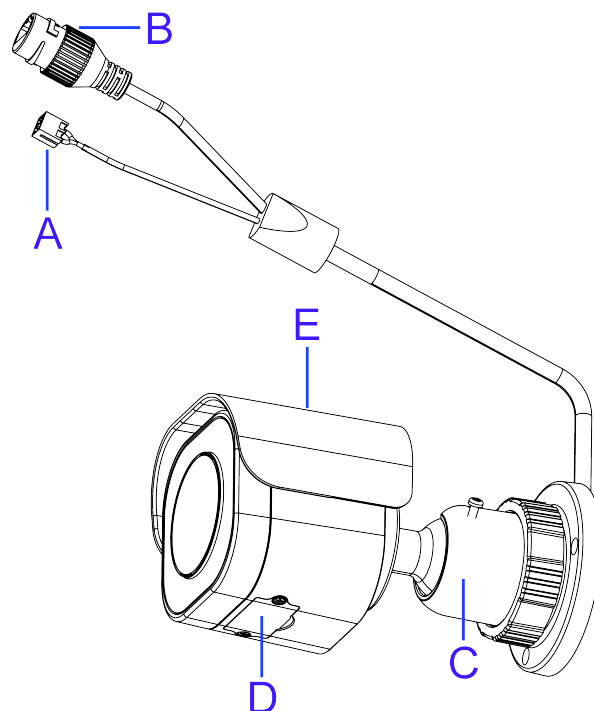


Table 13 Camera parts and connections descriptions

| | Name | Description |
|---|---------------------------|--|
| A | DC 12V Port | For powering on the camera through the DC12V power source. |
| B | RJ-45 Ethernet / PoE Port | Connect an Ethernet cable terminated with RJ-45 connector to the PoE RJ-45 port for both power supply and network connectivity purposes simultaneously. |
| C | Mounting Bracket | To mount the camera onto different environments, the mounting bracket is designed with three axes for flexible adjustment. |
| D | Internal Interface Cover | Use a screwdriver to loosen the 2 screws and open the cover to access the internal interfaces including the "RESET" and "DEFAULT" button, "Micro SD Card Slot", and LED's. |
| E | Protection Shield Hood | For minimizing the effects of rain and sunlight on image quality. |

Figure 14 Camera internal interface and descriptions

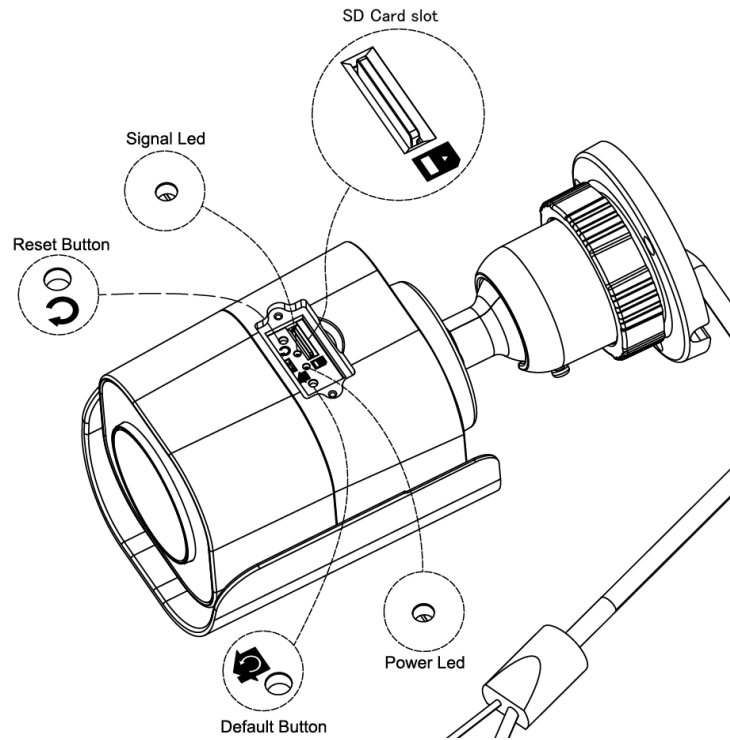


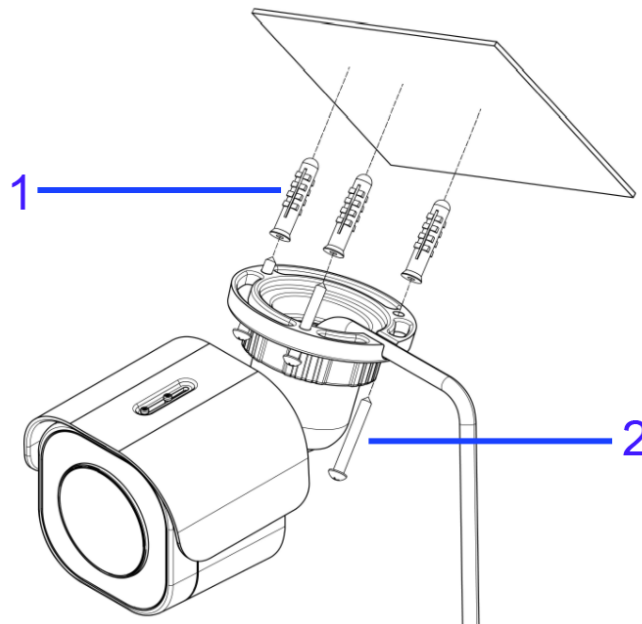
Table 15 Camera internal interface descriptions

| Name | Description |
|--------------------|--|
| Reset Button | Press and release to reboot the camera |
| Signal LED (RED) | Indicates network data is being transmitted. |
| Micro SD card slot | Insert a micro SD card into the slot for recording and file storage. |
| Power LED (GREEN) | Indicates camera is powered on. |
| Default Button | Press the button for 5 seconds to restore the camera to factory defaults |

Procedure 6 Mounting the camera

| Step | Action |
|------|--|
| 1 | Place the mounting template on the mounting surface and drill three 6mm (0.25") holes. |
| 2 | Insert the three plastic anchors (1) (Figure 16) into the three holes. |
| 3 | Place the camera on the mounting surface and align the three holes on the camera with the three holes on the mounting surface. |
| 4 | Insert the three tapping screws (2) (Figure 16) into the three holes on the camera body and using the screw driver securely attach the camera to the wall / ceiling. |

Figure 16 Plastic anchors and camera screws



- End -

Wiring the camera

You can run the cable through the mounting bracket or you can run the cable through the cable side entry on the mounting bracket.

| Step | Action |
|------|--|
| 1 | When mounting the camera, pass the cable through the mounting bracket and then through the: <ul style="list-style-type: none">• hole on the mounting surface (1) (Figure 17). OR <ul style="list-style-type: none">• the cable side entry on the mounting bracket (1) (Figure 18). |

Figure 17 Mounting surface cable hole

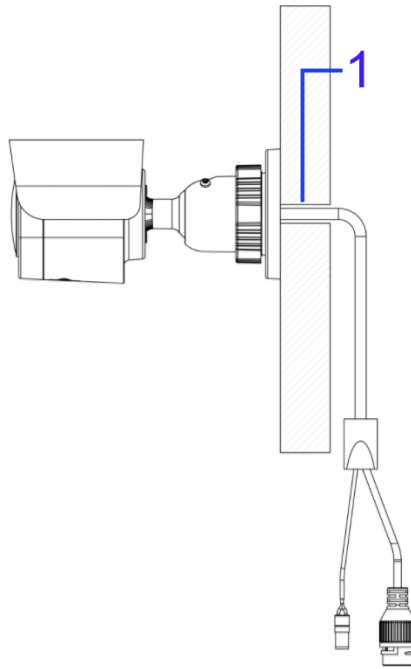
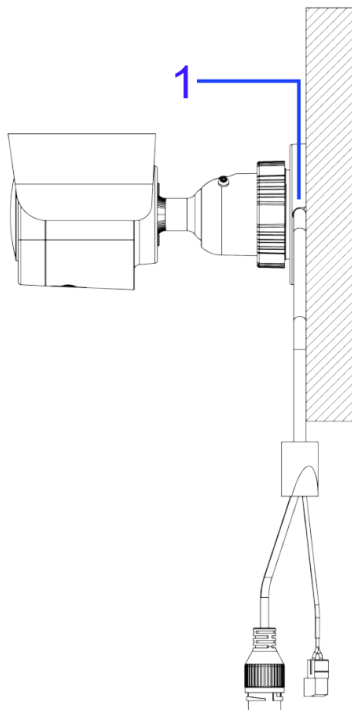


Figure 18 Camera cable side entry slot



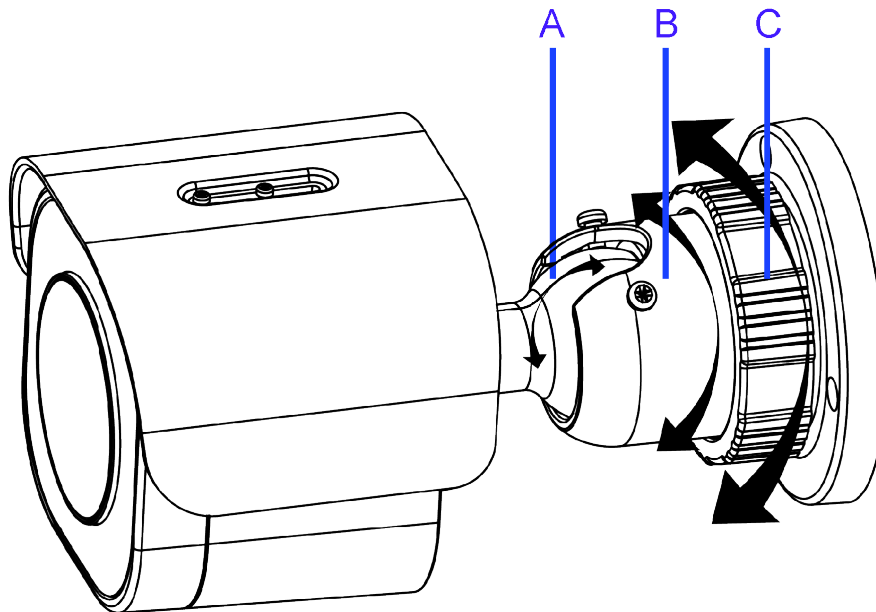
- 2 Connect an Ethernet cable terminated with the RJ-45 connector to the PoE port and ensure that the other end of the Ethernet cable is connected with a PoE compatible network device.
- 3 If necessary, connect the DC 12V power source to the DC 12V port.

- End -

Adjusting the camera position

The camera has three axes to adjust the field of view for different Applications (Figure 19). While screening live view on your monitor, adjust the axes as per the information below.

Figure 19 Adjusting the camera position



- **Tilt Adjustment** (A - Figure 19) Tilt this joint to adjust the camera vertically. The Tilt range is $0^{\circ} - 90^{\circ}$.
- **Pan Adjustment** (B - Figure 19) Rotate this joint to adjust the camera horizontally. DO NOT rotate over the default limit of $\pm 360^{\circ}$.
- **Locking Ring** (C - Figure 19) Rotating the C ring counter-clockwise, the Pan & Tilt joints loosen and you can adjust for different angles. Rotating the C ring clockwise fastens the pan & tilt joints altogether.

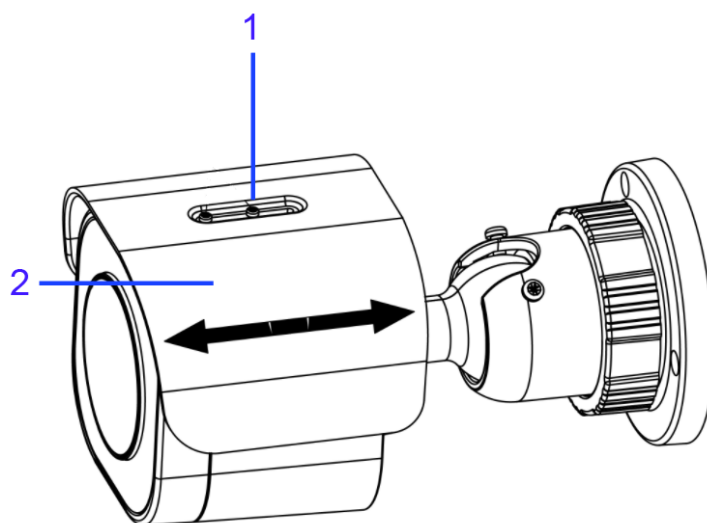
- End -

Adjusting the protection shield hood

The protection shield hood protects the camera from both sunlight and rain.

| Step | Action |
|------|--|
| 1 | Use the L-Key (1) (Figure 20) to loosen the two screws located on the protection shield hood. |
| 2 | Slide the protection shield (2) (Figure 20) forward or backward until the correct position is found. |

Figure 20 Adjusting the protection shield hood



- 3 Use the L-Key and secure the two screws located on the protection shield hood.

Note: Be careful not to excessively adjust the hood or you may damage the camera housing.

- End -

Network Topology

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

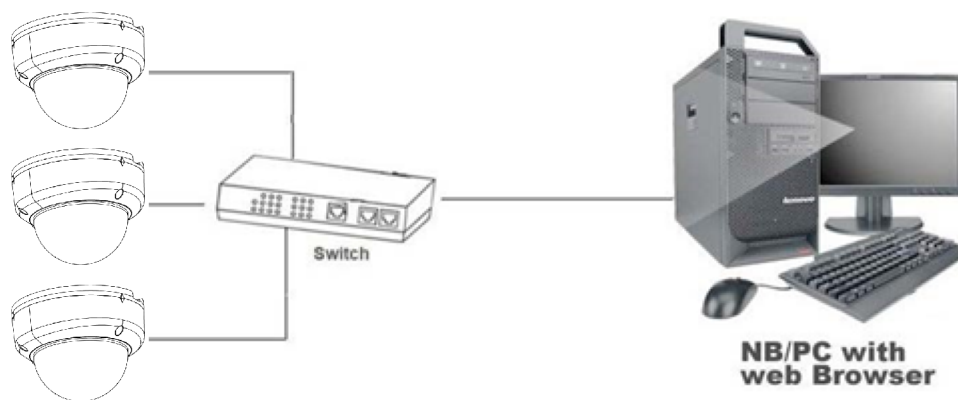
The following images illustrate the network topologies of the Dome and Bullet cameras.

Essentials Gen 4 Dome Camera Topology

Figure 21 Dome Cameras Network Topology Type I.



Figure 22 Dome Cameras Network Topology Type II

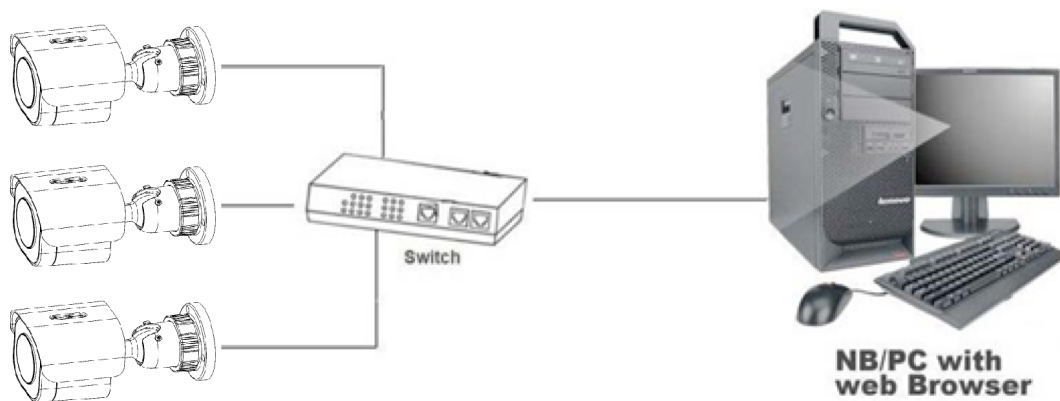


Essentials Gen 4 Bullet Camera Topology

Figure 23 Bullet Cameras Network Topology Type I.



Figure 24 Bullet Cameras Network Topology Type II



Network Connection

Default IP Address

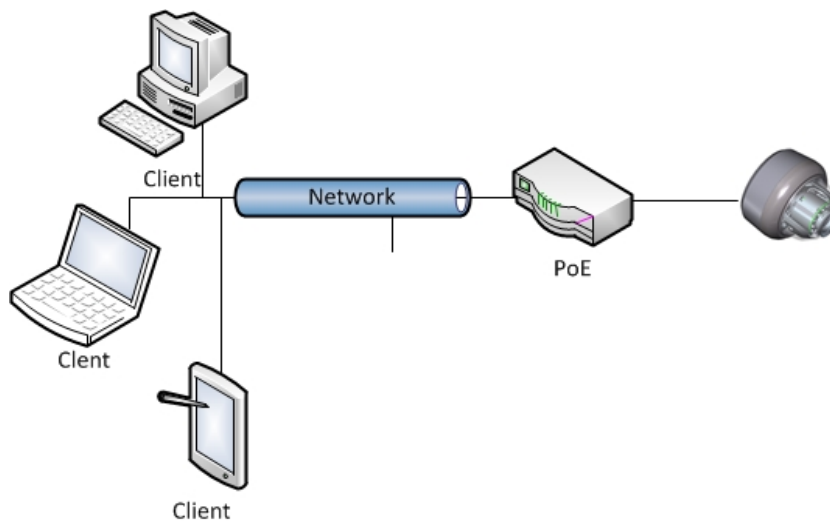
Since this is a network-based unit, an IP address must be assigned at the very first bootup. The default IP address of the unit is 192.168.1.168 and sub mask is 255.255.255.0.

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

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

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

Figure 25 Network connection diagram



Default camera settings

The following table describes the default camera settings.

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

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

Procedure 7 Connecting from a computer

| Step | Action |
|---------|--|
| 1 | Ensure the camera and your computer are in the same subnet. |
| 2 | Check whether if the network is available between the unit and the computer by pinging the default IP address. <ol style="list-style-type: none"> Start a command prompt. Type "Ping 192.168.1.168". If the message "Reply from..." appears, it means the connection is available. |
| 3 | Start Internet Explorer and enter IP address: 192.168.1.168. A login window appears. In the window, enter the default user name: admin and password: admin to log in. |
| - End - | |

DHCP

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

Procedure 8 Enable DHCP

| Step | Action |
|---|---|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select the TCP/IP tab in the Basic Configuration menu. |
| 3 | Select the Enable DHCP check box to enable DHCP and disable manual settings. |
| 4 | Select Apply to save the settings. |
| The camera searches for a DHCP server. If one is found it connects to that server. If no connection is made to a DHCP server within two minutes, the camera goes to the default IP address 192.168.1.168, but continues to search for a DHCP address. | |
| Note: If you assign the camera a Static IP address prior to DHCP being enabled, the camera first reboots for approximately 30 seconds and then remains accessible at its Static IP until it connects to a DHCP server. | |
| - End - | |

Procedure 9 Disable DHCP

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

- a Enter the IPv4 Address in the **IPv4 Address** text box in the form xxx.xxx.xxx.xxx. The default setting is '192.168.1.168'
 - b Enter the Network Mask in the **Network Mask** text box xxx.xxx.xxx.xxx. The default setting is '255.255.255.0'
 - c Enter the Gateway IP address in **Gateway** text box xxx.xxx.xxx.xxx.
 - d Enter the Primary DNS Server in the **Primary DNS Server** text box xxx.xxx.xxx.xxx.
- 5 Select **Apply** to save the settings.

- End -

Managing cameras with the Illustra Connect tool

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

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

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

Refer to Configuration on page 27 for further information regarding using the Illustra Connect tool for configuring the cameras.

Procedure 10 Connecting to the camera using Illustra Connect

Note:

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

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

- End -

Procedure 11 Connecting to the camera using the static IP address

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

Note:

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

- End -

Procedure 12 Logging on to the camera web user interface

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

Note: The first time that you access the camera or after a factory reset the following two pop up windows are visible: A pop up window that requests the user to **Define a Host ID** and a pop up window that requests the user to select a **Security Type**. Please refer to the Define a Host ID section in Procedure 14 for further information on this.

5 The Live view page is visible. This displays the current view of the camera.

Note: When Standard security is selected and at first login the user is prompted to change the default password.

Note: When Enhanced security is selected and at first login the user is prompted to change the default username and password.

- End -

Procedure 13 Enabling the correct video orientation for a wall mounted camera

| Step | Action |
|------|--|
| 1 | Log on to the camera web user interface. |
| 2 | Select Setup on the camera web user interface banner to display the setup menus. |
| 3 | Select the Picture Basic tab from the Basic Configuration menu. |
| 4 | Select the required Orientation setting: <ul style="list-style-type: none"> • Mirror • Flip |
| 5 | The video pane updates to display the new settings. |

- End -

Configuration

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

Security Mode Profiles for First Time Connection

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

When the camera is in Enhanced Security mode, you require a complex eight character Administrator password to make changes to these protocols.

Refer to Summary of Security Modes on page 28 for further information regarding the differences between Standard and Enhanced Security modes.

Accessing the Illustra Essentials Gen 4 Series Camera Web User Interface

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

Procedure 14 Logging in to the Camera

| Step | Action |
|------|---|
| 1 | Refer to Network Connection on page 22 for details on how to connect the camera to your network or computer. |
| 2 | When you select the camera, the sign in page displays. |
| 3 | Select your preferred language from the drop-down menu. The default language is English. |
| 4 | Enter the default username and password when prompted - Username: admin, Password: admin. |
| 5 | Click Log in . The camera Web User Interface displays. The first time that you access the camera, or after a factory reset, you are prompted to Define a Host ID and Select a Security Type . <ul style="list-style-type: none">• Define a Host ID: The admin user must enter a 6 character code for the Host ID that includes both letters and/or numbers. This unique password can be used to access the operating system files. The HostID is not stored on the camera for security reasons and must be presented to Illustra Technical Support when remote access to the operating system is required.• Select a Security Type: Standard Security or Enhanced Security. |
| 6 | If you select the Standard Security option, password change is mandatory. |

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

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

Note: The password must meet the following requirements:

Be a minimum of eight characters long.

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

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

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

- End -

Summary of Security Modes

Standard Security:

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

Enhanced Security:

- Unsecure Protocols are disabled by default until enabled by a user.
- When you select enhanced security you must change the default 'admin' username and password.
- Discovery protocols are disabled by default until enabled by a user.
- Changes in the protocols are only be available to a user with administrative privileges and require that user to reenter their password.
- Authentication method is set to Digest by default.
- HTTPS protocol is enabled by default.
- Passwords for all accounts will meet the following password complexity requirements:
 - Minimum characters: 8
 - The password cannot contain the username
 - 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

Changing the Camera Web User Interface Language

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

Procedure 15 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 | <p>Select your preferred language from the drop-down menu:</p> <ul style="list-style-type: none">• English• Arabic• Czech• Danish• German• Spanish• French• Hungarian• Italian• Japanese• Korean• Dutch• Polish• Portuguese• Swedish• Turkish• Chinese Simplified• Chinese Traditional• Russian• Hindi <p>The default language is English.</p> |
| 3 | Enter the Username. |
| 4 | Enter the Password. |
| 5 | Select Log in. |
| The camera web User Interface displays in the selected language. | |
| <hr/> - End - <hr/> | |

Live menu

When you log in to the Illustra Web User Interface, the **Live** menu appears, as seen in Figure 26 on page 30.

Figure 26 Live menu page



Displaying the Live View Page

Display the live camera view page.

Procedure 16 Display Live View Page

| Step | Action |
|----------------------------|---|
| 1 | Select Live in the Web User Interface banner. The Live view page displays. |
| 2 | Select a video stream from Stream to view. |
| 3 | Select a percentage from Scale to change the display size of the video pane: <ul style="list-style-type: none">• 25%• 50%• 75%• 100% The default setting is 100%. |
| <hr/> - End - <hr/> | |

Accessing the Setup Menus from Live View

Setup menus within the Web User Interface are restricted by user account access levels. Refer to Appendix A: User Account Access on page 107 for details on the features which are available to each role.

Procedure 17 Access Setup Menus from Live View

| Step | Action |
|--|--|
| 1 | On the Live menu, click the Setup tab. |
| Note: When an admin user logs in for the first time the Live menu displays. After this, on each login the Stream page on the Video menu displays. | |
| - End - | |

Quick Start Menu

When you select the Quick Start menu, the Basic Configuration Page displays, as shown in Figure 27 on page 32.

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

Figure 27 Basic Configuration Menu

The screenshot displays the Tyco Illustra web interface. At the top left is the Tyco logo. To its right is the word 'Illustra'. In the top right corner, the text 'Essentials4-T92350117' and 'admin' are shown, along with a 'Help LOG OFF' link and the word 'Essentials' in red. Below the Tyco logo is a 'View: Live Setup' button. On the left side, there is a 'Quick Start' menu with 'Basic Configuration' selected. Below this are links for 'Video', 'Event and Actions', 'Security', 'Network', 'System', and 'Edge Recording'. The main content area has tabs for 'TCP/IP', 'Video Stream Settings', 'Picture Basic', 'Picture Additional', 'Date Time', and 'OSD'. The 'TCP/IP' tab is active, showing 'IPv4' and 'IPv6' sections. The 'IPv4' section includes fields for 'Enable DHCP' (unchecked), 'IPv4 Address' (192.168.184.170), 'Network Mask' (255.255.254.0), 'Gateway' (192.168.185.4), and 'Primary DNS Server' (0.0.0.0), with an 'Apply' button below. The 'IPv6' section includes 'IPv6 Enable' (checked) and 'Current IPv6 Addresses' (fe80::566d:52ff:fe00:5b89). A large video player window is on the right.

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 32 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: <ol style="list-style-type: none"> Enter the IPv4 Address in the IPv4 Address text box in the form xxx.xxx.xxx.xxx. The default setting is '192.168.1.168' Enter the Network Mask in the Network Mask text box xxx.xxx.xxx.xxx. The default setting is '255.255.255.0' Enter the Gateway IP address in Gateway text box xxx.xxx.xxx.xxx. Enter the Primary DNS Server in the Primary DNS Server text box xxx.xxx.xxx.xxx. |
| 5 | Select Apply to save the settings. |

- End -

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: <ul style="list-style-type: none">a Enter the IPv4 Address in the IPv4 Address text box in the form xxx.xxx.xxx.xxx. The default setting is '192.168.1.168'b Enter the Network Mask in the Network Mask text box xxx.xxx.xxx.xxx. The default setting is '255.255.255.0'c Enter the Gateway IP address in Gateway text box xxx.xxx.xxx.xxx.d Enter the Primary DNS Server in the Primary DNS Server text box xxx.xxx.xxx.xxx. |
| 5 | Select Apply to save the settings. |

- End -

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 two 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 Video Streams Settings 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: <ul style="list-style-type: none"> • H264 • H265 • H264 IntelliZip • H265 IntelliZip • MJPEG <p>The default setting is 'H264'.</p> |
| Note: When you select H264 you can set the Profile. If you do not select either of these options then continue at step 6 below. | |
| 5 | Select the required Profile from the drop-down list: <ul style="list-style-type: none"> • Main • High <p>The default setting is 'Main'.</p> |
| 6 | Select the required Resolution from the drop-down menu. The resolutions available depend on the type of camera sensor (megapixel). |

Table 28 2MP Camera Stream Set A (all resolution, codes and frame rate combinations of Stream 1, 2 and 3 are valid)

| | | Normal Mode | | | |
|----------|---|-------------|--------------|----------|------|
| | | Resolution | Description | Max FPS | |
| | | | | TWDR Off | TWDR |
| Stream 1 | h.264, h.265, h.264 IntelliZip h.265 IntelliZip MJPEG | 1920 x 1080 | (1080p) 16:9 | 30 | 30 |
| | | 1600 x 900 | (HD+) 16:9 | 30 | 30 |
| | | 1280 x 720 | (720p) 16:9 | 30 | 30 |
| | | 1024 x 576 | (PAL+) 16:9 | 30 | 30 |
| | | 960 x 540 | 16:9 | 30 | 30 |
| | | 800 x 480 | 16:9 | 30 | 30 |
| | | 640 x 360 | (mHD) 16:9 | 30 | 30 |
| | | 480 x 270 | 16:9 | 30 | 30 |
| | | 320 x 180 | 16:9 | 30 | 30 |
| Stream 2 | h.264, h.265, h.264 IntelliZip h.265 IntelliZip MJPEG | 1920 x 1080 | (1080p) 16:9 | 30 | 30 |
| | | 1600 x 900 | (HD+) 16:9 | 30 | 30 |
| | | 1280 x 720 | (720p) 16:9 | 30 | 30 |
| | | 1024 x 576 | (PAL+) 16:9 | 30 | 30 |
| | | 960 x 540 | 16:9 | 30 | 30 |
| | | 800 x 480 | 16:9 | 30 | 30 |
| | | 640 x 360 | (mHD) 16:9 | 30 | 30 |
| | | 480 x 270 | 16:9 | 30 | 30 |
| | | 320 x 180 | 16:9 | 30 | 30 |
| Stream 3 | h.264, h.265, h.264 IntelliZip h.265 IntelliZip MJPEG | 1280 x 720 | (720p) 16:9 | 30 | 30 |
| | | 1024 x 576 | (PAL+) 16:9 | 30 | 30 |
| | | 960 x 540 | 16:9 | 30 | 30 |
| | | 800 x 480 | 16:9 | 30 | 30 |
| | | 640 x 360 | (mHD) 16:9 | 30 | 30 |
| | | 480 x 270 | 16:9 | 30 | 30 |
| | | 320 x 180 | 16:9 | 30 | 30 |
| | | | | | |

Note: A maximum of three concurrent streams are supported by the camera. This includes shared streams.

| | | Corridor Mode | | | |
|----------|--|---------------|--------------|----------|------|
| | | Resolution | Description | Max FPS | |
| | | | | TWDR Off | TWDR |
| Stream 1 | h.264, h.265, h.264 IntelliZip h.265 IntelliZip | 1920 x 1080 | (1080p) 16:9 | 30 | 30 |
| | | 1600 x 900 | (HD+) 16:9 | 30 | 30 |
| | | 1280 x 720 | (720p) 16:9 | 30 | 30 |
| | | 1024 x 576 | (PAL+) 16:9 | 30 | 30 |
| | | 960 x 540 | 16:9 | 30 | 30 |
| | | 800 x 480 | 16:9 | 30 | 30 |
| | | 640 x 360 | (mHD) 16:9 | 30 | 30 |
| | | 480 x 270 | 16:9 | 30 | 30 |
| Stream 2 | h.264, h.265, h.264 IntelliZip h.265 IntelliZip | 1920 x 1080 | (1080p) 16:9 | 30 | 30 |
| | | 1600 x 900 | (HD+) 16:9 | 30 | 30 |
| | | 1280 x 720 | (720p) 16:9 | 30 | 30 |
| | | 1024 x 576 | (PAL+) 16:9 | 30 | 30 |
| | | 960 x 540 | 16:9 | 30 | 30 |
| | | 800 x 480 | 16:9 | 30 | 30 |
| | | 640 x 360 | (mHD) 16:9 | 30 | 30 |
| | | 480 x 270 | 16:9 | 30 | 30 |
| Stream 3 | h.264, h.265, h.264 IntelliZip h.265 IntelliZip | 1280 x 720 | (720p) 16:9 | 30 | 30 |
| | | 1024 x 576 | (PAL+) 16:9 | 30 | 30 |
| | | 960 x 540 | 16:9 | 30 | 30 |
| | | 800 x 480 | 16:9 | 30 | 30 |
| | | 640 x 360 | (mHD) 16:9 | 30 | 30 |
| | | 480 x 270 | 16:9 | 30 | 30 |
| | | | | | |

Note:A maximum of three concurrent streams are supported by the camera. This includes shared streams.

Note:MJPEG is not a supported codec for any stream when corridor mode is enabled.

Note:Resolution 320x180 is not supported with Corridor mode. If any stream is set to 320x180, it will be updated to 480x270 when corridor mode is applied.

Note:GUI stream is dynamic depending on current stream settings. Refer to the release notes for further information.

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

The settings for the 2MP cameras are:

- **Stream 1** - 1 - 30 fps, default 30 fps.
- **Stream 2** - 1 - 30 fps, default is 30 fps.

- **Stream 3** - 1 - 30 fps, default is 30 fps.

Note:FPS varies depending on other features - refer to the Essentials Gen 4 Release Notes for further information.

- 8 If H264 or H265 has been selected in step 4 then you can adjust the **GOP Length [1-60]**. Use the slider bar to select the **GOP Length [1-60]**.
The default setting is 30.

Note:If H264 IntelliZip or H265 IntelliZip has been selected in step 4 then you can adjust the IntelliZip Max GOP Length [1-180]. Use the slider bar to select the IntelliZip Max GOP Length [1-180]. The default setting is 62.

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

The default setting is 50.

OR

- 10 If H264 or H265 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 4000.

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 -

Picture Basic

Adjust Picture Rotation, 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: <ul style="list-style-type: none"> • Mirror • Flip <p>Mirror and Flip settings are selected by default. The video pane updates to display the new settings.</p> <p>Note:When wall mounting the camera you should select Flip and Mirror to correct the lens orientation.</p> |

- 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: <ul style="list-style-type: none"> • None • -90° • +90° <p>Note:Resolution 320x180 is not supported with Corridor mode. If any stream is set to 320x180, it will be updated to 480x270 when corridor mode is applied.</p> |

- 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 29 Lens features supported for the Outdoor Dome

| | Varifocal Dome | Varifocal Bullet |
|------------------|----------------|------------------|
| Motorized Focus | X | X |
| Motorized Zoom | X | X |
| Lens Calibration | X | X |
| Auto One Touch | X | X |

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 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.


Note: The user can create a ROI focus point for the camera to use during the one touch procedure - use the pencil icon and highlight the desired ROI.

- End -

Exposure


Configure the exposure settings for the camera.

Procedure 27 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: <ul style="list-style-type: none"> • Auto • Manual • Shutter Priority |
| 5 | Select the Exposure Method from the drop-down menu: <ul style="list-style-type: none"> • Full Picture Weighted • Upper • Lower • Center Weighted • Spot • Left • Right <p>The default setting is center weighted.</p> |
| 6 | Select the Min Exposure (sec) from the drop-down menu. The default setting is 1/10000s. |
| 7 | Select the Max Exposure (sec) from the drop-down menu. The default setting is 1/7.5s. |
| 8 | Select the Exposure Offset (F-stops) 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 (db) from the drop-down menu. The default setting is 45db. |
| 11 | Select Exposure (sec) from the drop down. |
| 12 | The Default is 1/30. |
| 13 | Select Manual Gain from the drop down. |
| 14 | The Default is 0db. |
| 15 | Select the Frequency radio button for either 50Hz or 60Hz . The default setting is 60Hz. |
| 16 | Select or clear the check box for Flickerless Mode . This feature is not selected by default. <ul style="list-style-type: none"> • 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 28 Restore Exposure Defaults

| Step | Action |
|------|---|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select the Picture Settings tab from the Basic Configuration menu. |
| 3 | Select  to start the video stream if it is not already active. |
| 4 | Select Exposure Defaults to restore the default settings. |

- End -

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.

Digital Wide Dynamic

Digital wide dynamic range, enhancing detail in darker areas.

Procedure 29 Disable/Enable Wide Dynamic Range (WDR)

| Step | Action |
|------|---|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select the Picture Additional tab from the Basic Configuration menu. |
| 3 | Select the required WDR from the drop-down list: <ul style="list-style-type: none">• True WDR: Two shutter wide dynamic range, to compensate for bright and dark areas in the scene.• Digital WDR: Digital wide dynamic range, enhancing detail in darker areas. The default setting is Off. |
| 4 | When you select DigitalWDR in step 3 then you can select the WDR level. |
| 5 | Select the WDR level from the drop-down menu. |

- 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 30 Enable / Disable IR Illuminator

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

Day Night Mode

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

Procedure 31 Configure Day Night Mode

| Step | Action |
|------|---|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select the Picture Additional from the Basic Configuration menu. |
| 3 | Select a Day Night Mode setting from the drop-down menu: <ul style="list-style-type: none"> • 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. |

- **Forced Color** - enable full-time color mode.
- **Forced B&W** - enable full-time black and white mode.


The default setting is 'Auto Mid'.

- End -

Picture Adjustment

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

Procedure 32 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: <ul style="list-style-type: none"> • Brightness • Contrast • Saturation • Hue • Sharpness <p>The values range from 1% to 100%. The video pane updates to display the new settings.</p> |

- End -

Procedure 33 Restore Picture Balance Defaults

| Step | Action |
|------|---|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select the Picture Settings tab from the Basic Configuration menu. |
| 3 | Select Defaults to restore the default settings. The default values are: <ul style="list-style-type: none"> • 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 34 Configure Auto White Balance

| Step | Action |
|---------|--|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select the Picture Additional tab from the Basic Configuration menu. |
| 3 | Select  to start the video stream if it is not already active. The video pane displays the current camera view. |
| 4 | Select the required White Balance from the drop-down menu: <ul style="list-style-type: none"> • Auto Normal Suitable for a normal range of lighting conditions • Manual: Adjustable red and blue balance • Auto Wide: Suitable for a wider than normal range of lighting conditions |
| - End - | |

Procedure 35 Manually Select White Balance

| Step | Action |
|---------|--|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select the Picture Additional tab from the Basic Configuration menu. |
| 3 | Select  to start the video stream if it is not already active. The video pane displays the current camera view. |
| 4 | Select Manual from the White Balance drop-down menu. The Red and Blue slider bars display. |
| 5 | Use the slider bars to adjust the Red and Blue balance. The live video pane updates to display the new settings. The red and blue values range from 1% to 100%. If you change the configuration to Manual , the slider bar reads the real-time setting of the FOV. |
| - End - | |

Date / Time

Change the camera name and set the date and time.

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 36 Change the Camera Name

| Step | Action |
|---------|---|
| 1 | Select Setup on the Web User Interface banner. |
| 2 | Select the Date/Time 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 37 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 Basic Configuration menu. |
| 3 | Select the Time 24-hour check box to enable the 24-hour clock. Or Deselect the Time 24-hour check box to enable the 12-hour clock. The default setting is '24-hour'. |
| 4 | Select the Date Display Format from the drop-down menu: <ul style="list-style-type: none">• DD/MM/YYYY• MM/DD/YYYY• YYYY/MM/DD The default setting is 'DD/MM/YYYY'. |
| 5 | Select the Time Zone from the drop-down menu. The default setting is (GMT) GMT+0. |
| 6 | Select the Set Time setting by selecting the radio buttons: <ul style="list-style-type: none">• Manually• via NTP The default setting is 'Manually'. |
| 7 | If you select Manually in step 5: <ul style="list-style-type: none">a Select the Date (DD/MM/YYYY) using the drop-down menus.b Select the Time (HH:MM:SS) using the drop-down menus. |
| 8 | If you select via NTP in step 5: |

- 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 38 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'. |
| 4 | In the Camera Name section, select the Location drop-down menu to select where the camera name is displayed on screen. |

- End -

Procedure 39 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'. |
| 4 | In the Date Time section, select the Format drop-down menu to select if the date or time or both should be visible on screen. The default setting is 'Time'. |

- End -

Procedure 40 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:

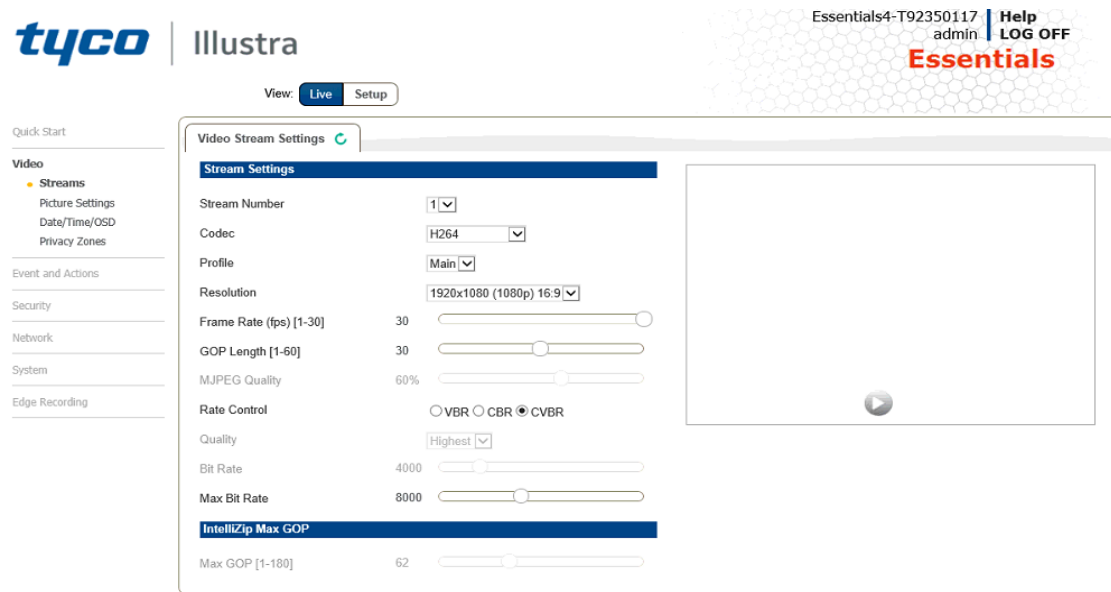
- 0 - 24 characters
- Cannot begin or end with:
 - . (dot)
 - - (hyphen)
 - _ (underscore)
 - \ (backslash)
 - " (quotes)

- End -

Video Menu

When you select the **Video** menu, the **Streams** page displays, as seen in Figure 30 on page 49.

Figure 30 Video Menu



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

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

Streams

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

Alarm Video

Edge Recording

Camera can directly record specific events (MD) 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, all 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 three 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 41 Configure the Video Stream settings

| Step | Action |
|---|--|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select the Video Streams Settings tab in the Basic Configuration menu. |
| 3 | Select either Stream1, 2 or 3 from the Stream Number drop-down menu. |
| 4 | Select the required Codec from the drop-down list: <ul style="list-style-type: none"> • H264 • H265 • H264 IntelliZip • H265 IntelliZip • MJPEG <p>The default setting is 'H264'.</p> |
| Note: When you select H264 or H264 IntelliZip you can set the Profile. If you do not select either of these options then continue at step 6 below. | |
| 5 | Select the required Profile from the drop-down list: <ul style="list-style-type: none"> • Main • High <p>The default setting is 'Main'.</p> |
| 6 | Select the required Resolution from the drop-down menu. The resolutions available depend on the type of camera sensor (megapixel). |

Table 31 2MP Camera Stream Set A (all resolution, codes and frame rate combinations of Stream 1 and 2 are valid)

| | | Normal Mode | | | |
|----------|---|-------------|--------------|----------|------|
| | | Resolution | Description | Max FPS | |
| | | | | TWDR Off | TWDR |
| Stream 1 | h.264, h.265, h.264 IntelliZip h.265 IntelliZip MJPEG | 1920 x 1080 | (1080p) 16:9 | 30 | 30 |
| | | 1600 x 900 | (HD+) 16:9 | 30 | 30 |
| | | 1280 x 720 | (720p) 16:9 | 30 | 30 |
| | | 1024 x 576 | (PAL+) 16:9 | 30 | 30 |
| | | 960 x 540 | 16:9 | 30 | 30 |
| | | 800 x 480 | 16:9 | 30 | 30 |
| | | 640 x 360 | (mHD) 16:9 | 30 | 30 |
| | | 480 x 270 | 16:9 | 30 | 30 |
| Stream 2 | h.264, h.265, h.264 IntelliZip h.265 IntelliZip MJPEG | 320 x 180 | 16:9 | 30 | 30 |
| | | 1920 x 1080 | (1080p) 16:9 | 30 | 30 |
| | | 1600 x 900 | (HD+) 16:9 | 30 | 30 |
| | | 1280 x 720 | (720p) 16:9 | 30 | 30 |
| | | 1024 x 576 | (PAL+) 16:9 | 30 | 30 |
| | | 960 x 540 | 16:9 | 30 | 30 |
| | | 800 x 480 | 16:9 | 30 | 30 |
| | | 640 x 360 | (mHD) 16:9 | 30 | 30 |
| Stream 3 | h.264, h.265, h.264 IntelliZip h.265 IntelliZip MJPEG | 480 x 270 | 16:9 | 30 | 30 |
| | | 320 x 180 | 16:9 | 30 | 30 |
| | | 1280 x 720 | (720p) 16:9 | 30 | 30 |
| | | 1024 x 576 | (PAL+) 16:9 | 30 | 30 |
| | | 960 x 540 | 16:9 | 30 | 30 |
| | | 800 x 480 | 16:9 | 30 | 30 |
| | | 640 x 360 | (mHD) 16:9 | 30 | 30 |
| | | 480 x 270 | 16:9 | 30 | 30 |

Note:A maximum of three concurrent streams are supported by the camera. This includes shared streams.

| | | Corridor Mode | | | |
|----------|--|---------------|--------------|----------|------|
| | | Resolution | Description | Max FPS | |
| | | | | TWDR Off | TWDR |
| Stream 1 | h.264, h.265, h.264 IntelliZip h.265 IntelliZip | 1920 x 1080 | (1080p) 16:9 | 30 | 30 |
| | | 1600 x 900 | (HD+) 16:9 | 30 | 30 |
| | | 1280 x 720 | (720p) 16:9 | 30 | 30 |
| | | 1024 x 576 | (PAL+) 16:9 | 30 | 30 |
| | | 960 x 540 | 16:9 | 30 | 30 |
| | | 800 x 480 | 16:9 | 30 | 30 |
| | | 640 x 360 | (mHD) 16:9 | 30 | 30 |
| | | 480 x 270 | 16:9 | 30 | 30 |
| Stream 2 | h.264, h.265, h.264 IntelliZip h.265 IntelliZip | 1920 x 1080 | (1080p) 16:9 | 30 | 30 |
| | | 1600 x 900 | (HD+) 16:9 | 30 | 30 |
| | | 1280 x 720 | (720p) 16:9 | 30 | 30 |
| | | 1024 x 576 | (PAL+) 16:9 | 30 | 30 |
| | | 960 x 540 | 16:9 | 30 | 30 |
| | | 800 x 480 | 16:9 | 30 | 30 |
| | | 640 x 360 | (mHD) 16:9 | 30 | 30 |
| | | 480 x 270 | 16:9 | 30 | 30 |
| Stream 3 | h.264, h.265, h.264 IntelliZip h.265 IntelliZip | 1280 x 720 | (720p) 16:9 | 30 | 30 |
| | | 1024 x 576 | (PAL+) 16:9 | 30 | 30 |
| | | 960 x 540 | 16:9 | 30 | 30 |
| | | 800 x 480 | 16:9 | 30 | 30 |
| | | 640 x 360 | (mHD) 16:9 | 30 | 30 |
| | | 480 x 270 | 16:9 | 30 | 30 |
| | | | | | |

Note:A maximum of three concurrent streams are supported by the camera. This includes shared streams.

Note:MJPEG is not a supported codec for any stream when corridor mode is enabled.

Note:Resolution 320x180 is not supported with Corridor mode. If any stream is set to 320x180, it will be updated to 480x270 when corridor mode is applied.

Note:GUI stream is dynamic depending on current stream settings. Refer to the release notes for further information.

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

The settings for the 2MP cameras are:

- **Stream 1** - 1 - 30 fps, default 30 fps.
- **Stream 2** - 1 - 30 fps, default is 30 fps.

- **Stream 3** - 1 - 30 fps, default is 30 fps.

Note:FPS varies depending on other features - refer to the Essentials Gen 4 Release Notes for further information.

- 8 If H264 or H265 has been selected in step 4 then you can adjust the **GOP Length [1-60]**. Use the slider bar to select the **GOP Length [1-60]**.
The default setting is 30.

Note:If H264 IntelliZip or H265 IntelliZip has been selected in step 4 then you can adjust the IntelliZip Max GOP Length [1-180]. Use the slider bar to select the IntelliZip Max GOP Length [1-180]. The default setting is 62.

- 9 If MJPEG has been selected, MJPEG Quality is enabled. Use the slider bar to select the **MJPEG Quality**.
The default setting is 50.
OR
- 10 If H264, H265, H264 IntelliZip or H265 IntelliZip 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 4000.
- 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 42 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.

Lens Calibration

Use the lens calibration process to recover focus and zoom.

Procedure 43 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: <ul style="list-style-type: none"> • Mirror • Flip <p>Mirror and Flip settings are not selected by default. The video pane updates to display the new settings.</p> <p>Note:When wall mounting the camera you should select Flip to correct the lens orientation.</p> |
| - 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 32 Lens features supported for the Outdoor Dome and Bullet cameras

| | Varifocal Dome | Varifocal Bullet |
|------------------|----------------|------------------|
| Motorized Focus | X | X |
| Motorized Zoom | X | X |
| Lens Calibration | X | X |
| Auto One Touch | X | X |

Procedure 44 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 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 45 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 | 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. |
| Note: The user can create a ROI focus point for the camera to use during the one touch procedure - use the pencil icon and highlight the desired ROI. | |
| - End - | |

Exposure

Configure the exposure settings for the camera.


Procedure 46 Configure Exposure Settings

| Step | Action |
|------|--|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select the Picture Settings tab from the Basic Configuration menu. |
| 3 | Select  to start the video stream if it is not already active. |
| 4 | Select the Exposure Mode from the drop-down menu: <ul style="list-style-type: none"> • Auto • Manual • Shutter Priority |
| 5 | Select the Exposure Method from the drop-down menu: <ul style="list-style-type: none"> • Full Picture Weighted • Upper • Lower • Center Weighted • Spot • Left • Right <p>The default setting is center weighted.</p> |
| 6 | Select the Min Exposure (sec) from the drop-down menu. The default setting is 1/10000s. |
| 7 | Select the Max Exposure (sec) from the drop-down menu. The default setting is 1/7.5s. |
| 8 | Select the Exposure Offset (F-stops) 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 (db) from the drop-down menu. The default setting is 45db. |
| 11 | Select Exposure (sec) from the drop down. |
| 12 | The Default is 1/30. |
| 13 | Select Manual Gain from the drop down. |
| 14 | The Default is 0db. |
| 15 | Select the Frequency radio button for either 50Hz or 60Hz . The default setting is 60Hz. |
| 16 | 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 47 Restore Exposure Defaults

| Step | Action |
|------|---|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select the Picture Settings tab from the Basic Configuration menu. |
| 3 | Select  to start the video stream if it is not already active. |
| 4 | Select Exposure Defaults to restore the default settings. |

- End -

Picture Additional

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

Wide Dynamic Range

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

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

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

Digital Wide Dynamic

Digital wide dynamic range, enhancing detail in darker areas.

Procedure 48 Disable/Enable Wide Dynamic Range (WDR)

| Step | Action |
|------|---|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select the Picture Additional tab from the Basic Configuration menu. |
| 3 | Select the required WDR from the drop-down list: <ul style="list-style-type: none"> • True WDR: Two shutter wide dynamic range, to compensate for bright and dark areas in the scene. • Digital WDR: Digital wide dynamic range, enhancing detail in darker areas. <p>The default setting is Off.</p> |
| 4 | When you select DigitalWDR in step 3 then you can select the WDR level. |

- 5 Select the WDR level from the drop-down menu.

- 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 49 Enable / Disable IR Illuminator

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

- End -

Day Night Mode

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

Procedure 50 Configure Day Night Mode

| Step | Action |
|------|---|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select the Picture Additional from the Basic Configuration menu. |
| 3 | Select a Day Night Mode setting from the drop-down menu: <ul style="list-style-type: none"> • 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.
- **Forced Color** - enable full-time color mode.
- **Forced B&W** - enable full-time black and white mode.


The default setting is 'Auto Mid'.

- End -

Picture Adjustment

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

Procedure 51 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: <ul style="list-style-type: none"> • Brightness • Contrast • Saturation • Hue • Sharpness <p>The values range from 1% to 100%. The video pane updates to display the new settings.</p> |

- End -

Procedure 52 Restore Picture Balance Defaults

| Step | Action |
|------|---|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select the Picture Settings tab from the Basic Configuration menu. |
| 3 | Select Defaults to restore the default settings. The default values are: <ul style="list-style-type: none"> • 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 53 Configure Auto White Balance

| Step | Action |
|---------|--|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select the Picture Additional tab from the Basic Configuration menu. |
| 3 | Select  to start the video stream if it is not already active. The video pane displays the current camera view. |
| 4 | Select the required White Balance from the drop-down menu: <ul style="list-style-type: none"> • Auto Normal Suitable for a normal range of lighting conditions • Manual: Adjustable red and blue balance • Auto Wide: Suitable for a wider than normal range of lighting conditions |
| - End - | |

Procedure 54 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.

Procedure 55 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

Change the camera name and set the date and time.

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 56 Change the Camera Name

| Step | Action |
|---------|---|
| 1 | Select Setup on the Web User Interface banner. |
| 2 | Select the Date/Time 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 57 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 Basic Configuration menu. |
| 3 | Select the Time 24-hour check box to enable the 24-hour clock. Or Deselect the Time 24-hour check box to enable the 12-hour clock. The default setting is '24-hour'. |
| 4 | Select the Date Display Format from the drop-down menu: <ul style="list-style-type: none">• DD/MM/YYYY |

- **MM/DD/YYYY**

- **YYYY/MM/DD**

The default setting is 'DD/MM/YYYY'.

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

The default setting is (GMT) GMT+0.

- 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 58 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'. |
| 4 | In the Camera Name section, select the Location drop-down menu to select where the camera name is displayed on screen. |

- End -

Procedure 59 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'.

- 4 In the **Date Time** section, select the **Format** drop-down menu to select if the date or time or both should be visible on screen.
The default setting is 'Time'.

- End -

Procedure 60 Display or Hide the User Defined OSD

| Step | Action |
|------|---|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select the OSD tab in the Basic Configuration menu. |
| 3 | In the User Defined section, select the Enable check box to display the camera name in the OSD. OR In the User Defined section, clear the Enable check box to hide the camera name in the OSD. The default setting is 'Disabled'. |
| 4 | Select a Location from the drop-down menu. |
| 5 | Enter a name in the Name field. The OSD User Defined fields must comply with the following validation criteria: <ul style="list-style-type: none">• 0 - 24 characters• Cannot begin or end with:<ul style="list-style-type: none">• . (dot)• - (hyphen)• _ (underscore)• \ (backslash)• " (quotes) |

- End -

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.

Enabling or Disabling a Privacy Zone

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


Procedure 61 Enable/Disable a Privacy Zone

| Step | Action |
|---|---|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select Privacy Zones from the Video menu. The Privacy Zones tab displays. |
| 3 | Select  to start the video stream if it is not already active. The video pane displays the current camera view. |
| 4 | Select the Enabled check box to enable the privacy zone feature. OR Clear the Enabled check box to disable the privacy zone feature. |
| Note: Disabling zones will not delete configured zones, it hides them from Live video. | |
| - End - | |

Defining a Privacy Zone

Create a privacy zone on the camera.

Procedure 62 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 | Enable Privacy zones as per procedure 59. |
| 5 | Select the desired colour for the Zone overlay. |
| 6 | Click on the edit pencil button. Click and drag on the camera picture to define an area for the privacy zone. |
| 7 | Release the mouse button. The selected privacy area will turn yellow. |
| 8 | Select Add to save the current privacy zone. |
| 9 | To reselect an alternative area for the privacy zone select Cancel and repeat from step 4. |
| - End - | |

Deleting a Privacy Zone

Delete a privacy zone from the camera.

Procedure 63 Delete a Privacy Zone

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

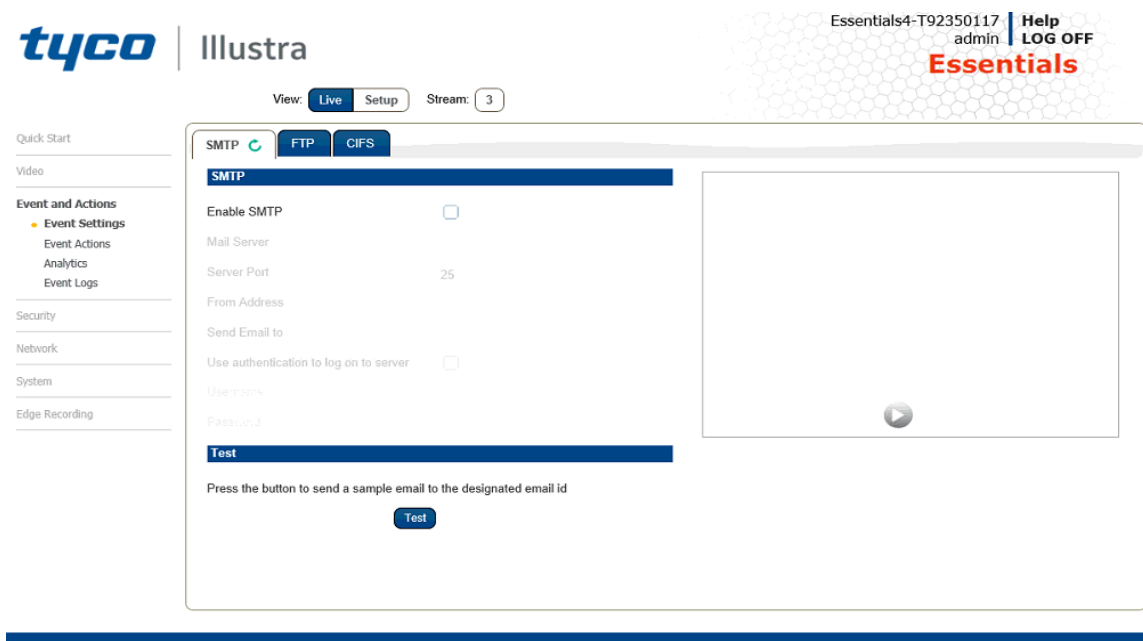
- 2 Select **Privacy Zones** from the **Video** menu.
The Privacy zones tab displays.
- 3 Select  for the privacy zone that you want to delete.
- 4 Select **Delete** to delete the selected privacy zones.
- 5 You are prompted to confirm the deletion.
- 6 Select **OK** to confirm the deletion.
OR
Select **Cancel**.

- End -

Events and Actions Menu

When you select the Events and Actions menu the Event Settings page displays, as seen in Figure 33 on page 66.

Figure 33 Events and Actions Menu



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

- Event Settings
- Event Actions
- Analytics
- Events Logs

Event Settings

Configure the SMTP, CIFS and FTP 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 64 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: <ol style="list-style-type: none"> Enter the username for the SMTP account in the Username text box. Enter the password for the SMTP account in the Password text box. |
| - End - | |

Procedure 65 Test the SMTP Settings

| Step | Action |
|---------|---|
| 11 | Select Setup on the Web User Interface banner to display the setup menus. |
| 12 | Select Event Settings from the Events and Actions menu. |
| 13 | Select the SMTP tab. |
| 14 | Select Test . A sample text file is sent to the specified SMTP destination to confirm that SMTP settings are correct. |
| - End - | |

FTP

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

Procedure 66 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'. |
| Note: When in Enhanced Security mode, enabling FTP requires the admin account password. | |
| 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. |
| 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 SMTP Settings on page 67 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 67 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 FTP settings that have been configured in Procedure 72 Configure FTP Server Settings.

Procedure 68 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 via the Common Internet File System protocol. This supplements existing distribution methods such as FTP, SFTP and email.

Procedure 69 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 in the Password text box. |
| - End - | |

Event Actions

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

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

- Record a clip to 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 server. The video file contains pre and post alarm video buffer.

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.

Creating an Event Action

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

Procedure 70 Create an Event Action

| Step | Action |
|------|--|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select Event Actions from the Events and Actions menu. |
| 3 | Select an entry on the event actions list and enter an event action name in the Name text box. |
| 4 | Select the Record check box to enable the Record Settings. |
| 5 | Select the Email check box to send an e-mail to the email address configured in the Configure SMTP Settings procedure. |
| 6 | Select the FTP check box to send a video file to the FTP details configured in the Configure FTP Server Settings procedure. |

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 has been selected.
 3. The selected pre and post event duration buffer is included in any video clips sent through FTP.
-

- End -

Editing an Event Action

Modify the details of an existing event action.

Procedure 71 Edit an Event Action

| Step | Action |
|---------|--|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select Event Actions from the Events and Actions menu. |
| 3 | Select an entry on the event actions list, you can edit the following: <ul style="list-style-type: none"> • Name • Record - Enable/Disable • Email - Enable/Disable • FTP - Enable/Disable • CIFS - Enable/Disable |
| - End - | |

Analytics

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

Region of Interest (ROI)

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


Procedure 72 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 73 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.

Procedure 74 Create a Motion Detection Alert

| Step | Action |
|------|---|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select Analytics from the Events and Actions menu. |
| 3 | Select the Motion Detection tab. |
| 4 | Select the Enable motion detection check box to enable Motion Detection on the camera. |

OR

Clear the **Enable motion detection** check box to disable Motion Detection on the camera.

- 5 Select the zone for detection in the **Motion zone** drop-down list.
- 6 Select the **Enable motion zone** check box to enable the zone for motion detection.
- 7 Select **Edit** in the **Region configuration** field.

Note: The user can configure three separate rules each with a different region, sensitivity and fault actions.

- 8 Use the drawing tools on the Motion Detection Configuration Pane to draw the region of interest on the pane. Multiple selections can be made.
- 9 Select the sensitivity from the **Sensitivity** drop-down menu:
 - **High**
 - **Medium**
 - **Low**
- 10 Select the fault action from the **Action** drop-down menu.
This fault action activates when motion is detected in the selected region of interest.
- 11 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 75 Enable or Disable a Motion Detection Alert

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

- End -

Blur Detection

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

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

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

Procedure 76 Enable Blur 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. |
| 3 | Select the Blur Detection tab. The Blur Detection Configuration pane displays. |
| 4 | Select the Enable Blur Detection checkbox to enable blur detection on the camera. |
| 5 | Select Apply to save. |
| - End - | |

Event Logs

Event Log

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

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

Procedure 77 Display Event Log

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

Procedure 78 Delete Current Events

- 1 Select **Setup** on the Web User Interface banner to display the setup menus.
- 2 Select **Event Logs** from the **Event and Actions** menu. The Event Logtab displays.
- 3 Select the corresponding **Delete** check box to mark the motion detection alert for deletion.
OR
Clear the corresponding **Delete** check box to keep the motion detection alert.

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

- 4 Select **Delete** to delete the selected motion detection alerts.
You are prompted to confirm the deletion.
- 5 Select **OK** to confirm the deletion.
OR
Select **Cancel**.

- End -

Security

When you select the **Security** menu, the **Security Status** page appears, as seen in Figure 34 on page 76.

Figure 34 Security menu

The screenshot displays the Tyco Illustra web interface. At the top, the Tyco logo and 'Illustra' brand name are visible. The top right corner shows the user 'Essentials4-T92350117 admin' with a 'Help' and 'LOG OFF' link. Below the header, there's a 'View: Live Setup' toggle. The left sidebar contains a 'Security' menu with sub-items: Security Status, Users, HTTP/HTTPS, IEEE 802.1x, Firewall, Remote Access, and Session Timeout. The main content area is titled 'Security Overview' and features two tables. The 'Security Options' table includes settings for Enhanced Security, Authenticate Video, Authentication, IEEE 802.1x, Firewall, Session Timeout, Firmware, and Camera Time. The 'Protocols' table lists various services like HTTP, HTTPS, RTSP, FTP, SFTP, SMTP, DynDNS, NTP, SNMP V3, SNMP V1/2, uPhP, SSH, and ONVIF Discovery, along with their status (Enabled/Disabled) and camera ports.

| Security Options | | |
|------------------------|-------------------------------------|-----------------------|
| Enhanced Security | <input type="checkbox"/> | Apply |
| Authenticate Video | <input checked="" type="checkbox"/> | Apply |
| Authentication | Basic <input type="text"/> | Apply |
| IEEE 802.1x | Disabled | Edit |
| Firewall | Disabled | Edit |
| Session Timeout (mins) | 15 | Edit |
| Firmware | Illustra.Ess4.00.01.03.2780 | Edit |
| Camera Time | 13/01/2020 10:39:11 | Edit |

| Protocols | | | | |
|-----------------|----------------------------------|----------|-------------|----------------------|
| Service | Enabled | Protocol | Camera Port | |
| HTTP | <input checked="" type="radio"/> | TCP | 80 | Edit |
| HTTPS | <input checked="" type="radio"/> | TCP | 443 | Edit |
| RTSP | <input checked="" type="radio"/> | TCP | 554 | Edit |
| FTP | <input type="radio"/> | TCP | 21 | Edit |
| SFTP | <input type="radio"/> | TCP | -- | Edit |
| SMTP | <input type="radio"/> | TCP | 25 | Edit |
| DynDNS | <input type="radio"/> | UDP | 53 | Edit |
| NTP | <input type="radio"/> | UDP | 123 | Edit |
| SNMP V3 | <input type="radio"/> | UDP | 162 | Edit |
| SNMP V1/2 | <input type="radio"/> | UDP | 162 | Edit |
| uPhP | <input checked="" type="radio"/> | UDP | 1900 | Edit |
| SSH | <input type="radio"/> | TCP | 22 | Edit |
| ONVIF Discovery | <input checked="" type="radio"/> | UDP | 3702 | Edit |

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

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

Security Status

This section explains how to configure security features for the camera and modify the communication protocols that are used.

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 28.

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

Procedure 79 Enable Enhanced Security

| Step | Action |
|------|---|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select Security Status from the Security menu. |
| 3 | Select the Security Overview tab. |
| 4 | Check the Enable Enhanced Security check box and then the Apply button 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 Username in the New Username text box. |
| 7 | Enter the new password in the New Password text box. The password for enhanced security must meet the following requirements: <ul style="list-style-type: none"> • Be a minimum of eight characters long • Have at least one character from each of the following character groups: <ul style="list-style-type: none"> Upper-case letters Lower-case letters Numeric characters Special characters |
| 8 | Re-enter the new password in the Confirm Password text box. |
| 9 | Click Apply . |

- End -

Procedure 80 Disable Enhanced Security Mode

| Step | Action |
|---------|--|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select Security Status from the Security menu. |
| 3 | Select the Security Overview tab. |
| | Note: When in Enhanced Security mode, changing the security mode requires the admin account password. |
| 4 | Click Apply . |
| - End - | |

Security Status

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

Security Overview

Procedure 81 Enable/Disable Communication Protocols

| Step | Action |
|------|---|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select Security Status from the Security menu. |
| 3 | Select the Security Overview tab. |
| 4 | Select the Edit button to configure the Protocol . |
| | Note: When in Enhanced Security, enabling/disabling individual protocols requires the admin account password. |

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 107 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 is required to be changed on first log in.

View Current User Accounts

View a list of the current user accounts assigned to the camera.

Procedure 82 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 83 Add a User

| Step | Action |
|------|---|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select Users from the Security menu. |
| 3 | Select the Add User tab. |
| 4 | Enter a User Name in the Name text box. The username must start with a letter and can be followed by any alphanumeric values (a-z, A-Z, 0-9) and the following special characters, underscore(_), dash(-), or dot(.) |
| 5 | Select a Role : <ul style="list-style-type: none"> • admin • operator • user Refer to Appendix A: User Account Access for details on the features which are available to each role. |
| 6 | Enter a password in the Password text box. The password for Standard Security must start with an alphanumeric character and is case sensitive, it can contain alphanumeric characters with a length of between 5 and 32 characters. The password for enhanced security must meet the following requirements: <ul style="list-style-type: none"> • Be a minimum of eight characters long. • The password cannot contain the username. • Have at least one character from each of the following character groups: <ul style="list-style-type: none"> • Upper-case letters - ABCDEFGHIJKLMNOPQRSTUVWXYZ • Lower-case letters - abcdefghijklmnopqrstuvwxyz • Numeric characters - 0123456789 • 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 84 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 85 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 86 Specify HTTP Method

| Step | Action |
|---------|--|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select HTTP/HTTPS from the Security menu. |
| 3 | Select the HTTP Method using the radio buttons <ul style="list-style-type: none"> • HTTP • HTTPS • Both |
| - End - | |

Procedure 87 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 . |
| <p>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.</p> <p>After the certificate has been uploaded the camera must be rebooted to take affect.</p> | |
| - 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 88 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 89 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 . |
| <hr/> - End - <hr/> | |

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

Procedure 90 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'. |
| - End - | |

Address Filtering

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

Procedure 91 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. <div style="border: 1px solid black; padding: 5px;">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.</div> b Select Add . |
| 6 | Select Apply to save the settings. |

- End -

Editing an Address Filter

Edit an existing address filter.

Procedure 92 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 93 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 94 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 95 Enable/Disable ONVIF Discovery Mode

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

- End -

ONVIF User Authentication

To utilize ONVIF User Authentication, there must be at least one admin level user in the ONVIF service.

Note:When in Enhanced Security mode, editing ONVIF User Authentication requires the admin account password.

Procedure 96 Enable/Disable ONVIF User Authentication

| Step | Action |
|------|--|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select Remote Access from the Security menu. |

The Remote Access tab displays.

- 3 Select the **ONVIF User Authentication** check box to enable ONVIF User Authentication.
OR
Deselect **ONVIF User Authentication** check box to disable ONVIF User Authentication.
The default setting is 'Enabled'.

- End -

UPnP Discovery

Enable or disable UPnP Discovery on the camera.

Procedure 97 Enable/Disable UPnP Discovery

| Step | Action |
|------|--|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select Remote Access from the Security menu. The Remote Access tab displays. |
| 3 | Select the UPnP Discovery check box to enable UPnP Discovery. OR Deselect UPnP Discovery check box to disable UPnP Discovery. The default setting is 'Enabled'. |

- End -

Session Timeout

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

Procedure 98 Set a Session Timeout time

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

- End -

Network Menu

When you select the **Network** menu, the **TCP/IP** page displays, as seen in Figure 35 on page 87.

Figure 35 Network Menu

The screenshot displays the Tyco Illustra web interface. The top navigation bar includes the Tyco logo, the word 'Illustra', and user information: 'Essentials4-T92350117 admin' with 'Help' and 'LOG OFF' links. Below this is a 'View: Live Setup Stream: 3' section. The left sidebar contains a 'Network' menu with sub-items: TCP/IP (selected), FTP, SMTP, SNMP, CIFS, and Dynamic DNS. The main content area is titled 'TCP/IP' and features two sections: 'IPv4' and 'IPv6'. The 'IPv4' section includes fields for 'Enable DHCP' (unchecked), 'IPv4 Address' (192.168.184.170), 'Network Mask' (255.255.254.0), 'Gateway' (192.168.185.4), and 'Primary DNS Server' (0.0.0.0), with an 'Apply' button. The 'IPv6' section shows 'IPv6 Enable' (checked) and 'Current IPv6 Addresses' (fe80::56d:52ff:fe00:5b89).

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

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

TCP/IP

Configure the IPv4 and IPv6 settings on the camera.

IPv4

Configure the IPv4 settings for the camera.

Note: When you perform a factory reset or reboot the unit searches for the last known IP address. If this is not available it reverts to the default IP address of 192.168.1.168. This could result duplicate IP addresses. Refer to Network Menu on page 87 for more information.

Procedure 99 Configure the IPv4 Settings

| Step | Action |
|---------|---|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select TCP/IP from the Network menu. |
| 3 | Select the Enable DHCP check box to enable DHCP and disable manual settings. OR Deselect Enable DHCP to disable DHCP and allow manual settings to be entered. The default setting is 'Disabled'. |
| 4 | If Enable DHCP has been disabled: <ol style="list-style-type: none"> Enter the IPv4 Address in the IPv4 Address text box in the form xxx.xxx.xxx.xxx. The default setting is '192.168.1.168' Enter the Network Mask in the Network Mask text box xxx.xxx.xxx.xxx. The default setting is '255.255.255.0' Enter the Gateway IP address in Gateway text box xxx.xxx.xxx.xxx. Enter the Primary DNS Server in the Primary DNS Server text box xxx.xxx.xxx.xxx. |
| 5 | Select Apply to save the settings. |
| - End - | |

IPv6

Enable IPv6 on the camera.

Procedure 100 Enable/Disable IPv6

| Step | Action |
|---------|---|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select TCP/IP from the Network menu. |
| 3 | Select the IPv6 Enable check box to enable IPv6 on the camera. OR Deselect the IPv6 Enable check box to disable IPv6 on the camera. The default setting is 'Enabled'. If IPv6 is enabled the Link Local and DHCP address displays beside 'Current IPv6 Addresses' if available. |
| - End - | |

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 101 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 102 Configure the FTP Transfer Rate

| 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 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 103 Test the FTP Settings

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

- End -

SMTP

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

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

Procedure 104 Configure SMTP Settings

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

- a Enter the username for the SMTP account in the **Username** text box.
 - b Enter the password for the SMTP account in the **Password** text box.
- 10 Select **Apply** to save the settings.

- End -

Procedure 105 Test the SMTP Settings

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

- End -

SNMP

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

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

Procedure 106 Configure SNMP Settings

| Step | Action |
|------|--|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select SNMP from the Network menu. |
| 3 | Enter a location reference in the Location text box. |
| 4 | Enter an SNMP managing contact reference in the Contact text box. |
| 5 | If using V2 : <ul style="list-style-type: none"> a Select the Enable V2 checkbox. b Enter the authorized ID for reading SNMP data in the Read Community text box. c Enter the Trap Community. d Enter the Trap Address. e Select Apply. |
| | OR |
| | If using V3 : <ul style="list-style-type: none"> a Select the Enable V3 checkbox. b Enter the Read User. c Select the Security Level from the drop down menu: <ul style="list-style-type: none"> - noauth: No authentication / no encryption. |

- **auth**: Authentication / no encryption. A user password is required. It is symmetrically encrypted using either MD5 or SHA.
- **priv**: Authentication / encryption. A user password is required as is symmetrically encrypted using either MD5 or SHA. A data encryption password is required as is symmetrically encrypted using either DES or AES.

- d Select the **Authentication Type** using the radio buttons.
- e Enter the Authentication Password
- f Select the **EncryptionType** using the radio buttons.
- g Enter the **Encryption** Password
- h Select **Apply**.

- End -

CIFS

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

Procedure 107 Configure CIFS Server Settings

| Step | Action |
|---------|--|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select CIFS from the Network menu. |
| 3 | Select the Enable check box to enable CIFS. OR Deselect the Enable check box to disable CIFS. The default setting is 'Disabled'. |
| | Note: When in Enhanced Security mode, enabling CIFS requires the admin account password. |
| 4 | Enter the network path in the Network Path text box. Note: When entering the network path the following format should be used '//<IP Address>/<folder name>' |
| 5 | Enter the domain name in the Domain Name in the text box. |
| 6 | Enter the username in the Username text box. |
| 7 | Enter the password h in the Password text box. |
| - End - | |

Heartbeat

Procedure 108 Enable/Disable Heartbeat

| Step | Action |
|---------|---|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select SNMP from the Network menu. |
| 3 | Select the Heartbeat tab. |
| 4 | Select the Enable Heartbeat check box to enable Heartbeat. OR Deselect the Enable Heartbeat check box to disable Heartbeat. The default setting is 'Disabled'. |
| - End - | |

Procedure 109 Enable select Heartbeat intervals

| Step | Action |
|---------|--|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select SNMP from the Network menu. |
| 3 | Select the Heartbeat tab. |
| 4 | Select the Enable Heartbeat check box to enable Heartbeat. |
| 5 | Use the slider bar to select the Heartbeat Interval (secs) . |
| 6 | The default setting is '60' seconds. The seconds range from 5 to 500. |
| - End - | |

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.

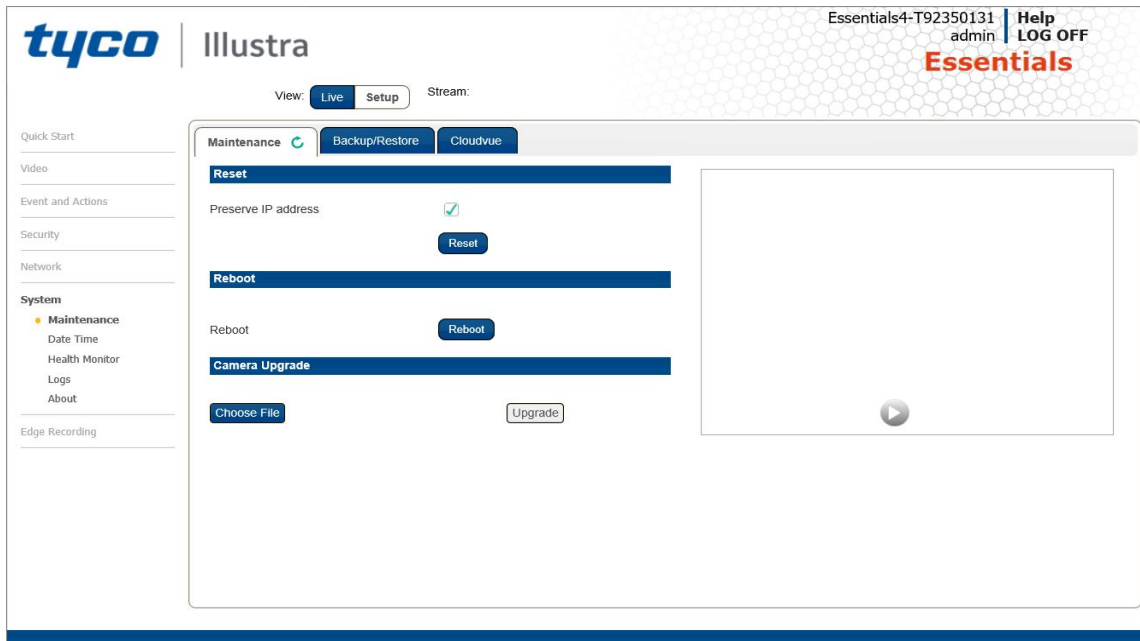
Procedure 110 Configure Dynamic DNS

| Step | Action |
|---------|--|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select Dynamic DNS from the Network menu. |
| 3 | Select the Service Enable check box to enable Dynamic DNS. OR Deselect Service Enable check box to disable Dynamic DNS. The default setting is 'Disabled'. |
| 4 | If Service Enable has been enabled: <ol style="list-style-type: none"> Enter the Camera Alias in the text box. Select a Service Provider from the drop-down list: <ul style="list-style-type: none"> • dyndns.org • easydns.com • no-ip.com • zerigo.com • dynsip.org • tzo.com Enter a Username in the text box. Enter a Password in the text box. Enter Service Data in the text box. |
| 5 | Select Apply to save the settings. |
| - End - | |

System

When you open the **System** menu, the **Maintenance** page appears, as seen in Figure 36 on page 95.

Figure 36 System Menu



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

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

Maintenance

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

Reset

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

Note: Network settings can be retained if required.

Procedure 111 Resetting the Camera

| Step | Action |
|------|--|
| 1 | Select Setup on the Web User Interface banner to display the setup menus. |
| 2 | Select Maintenance from the System menu. |
| 3 | Select the Preserve IP address check box to retain the current network settings during the camera reset. OR Deselect the Preserve IP address check box to restore the default networking settings. The default setting is 'Enabled'. |
| 4 | Select Reset . You will be prompted to confirm the camera reset. <ul style="list-style-type: none"> • Select OK to confirm. The Web User Interface will display a "Camera Resetting" page with a progress bar showing the reboot progress. • When the camera is restarted it will take 2 - 3 minutes until it is online and ready to be accessed and controlled. OR Select Cancel . |
| 5 | The Log in page displays. |

- End -

Reboot

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

Procedure 112 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 113 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 Choose File . 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 Upgrade . 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. |
| <hr/> - End - <hr/> | |

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 114 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 . |
| <hr/> - End - <hr/> | |

Procedure 115 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 Choose File . 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 - | |

CloudVue

The Cloudvue feature implements Illustra Cameras to Cloudvue (C2C) from Cloudvue 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 116 Enabling Cloudvue integration

Note: If a Cloudvue server is not setup when enabling the Cloudvue 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 Cloudvue tab. |
| 4 | Select Apply . |
| 5 | Enter an administrator password to validate the request. <ul style="list-style-type: none"> If the camera detects an Internet connection, it continues with the Cloudvue integration request. If an Internet connection is not detected an error displays and the request is rejected. |
| <p>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 Cloudvue mode and is only accessible using HTTPS. The password changes to a string of characters determined by the Cloudvue.</p> | |
| 6 | Refer to Cloudvue documentation and follow the procedure to add a camera to regain access. |

- End -

Procedure 117 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: <ul style="list-style-type: none">a Factory Reset: Resets the camera and boots the camera in Illustra mode.b Cloudvue Reset: Resets the camera and boots the camera in Cloudvue 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 118 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 Basic Configuration menu. |
| 3 | Select the Time 24-hour check box to enable the 24-hour clock. Or Deselect the Time 24-hour check box to enable the 12-hour clock. The default setting is '24-hour'. |
| 4 | Select the Date Display Format from the drop-down menu: <ul style="list-style-type: none">• DD/MM/YYYY• MM/DD/YYYY• YYYY/MM/DD The default setting is 'DD/MM/YYYY'. |
| 5 | Select the Time Zone from the drop-down menu. The default setting is (GMT) GMT+0. |
| 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 -

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 119 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 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 120 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 121 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 - | |

About

The About menu provides the following camera information:

- Camera Name
- Model
- Product Code
- Manufacturing Date
- Serial Number
- MAC Address
- Firmware Version
- Hardware Version
- iAPI Version

Procedure 122 Display Model Information

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

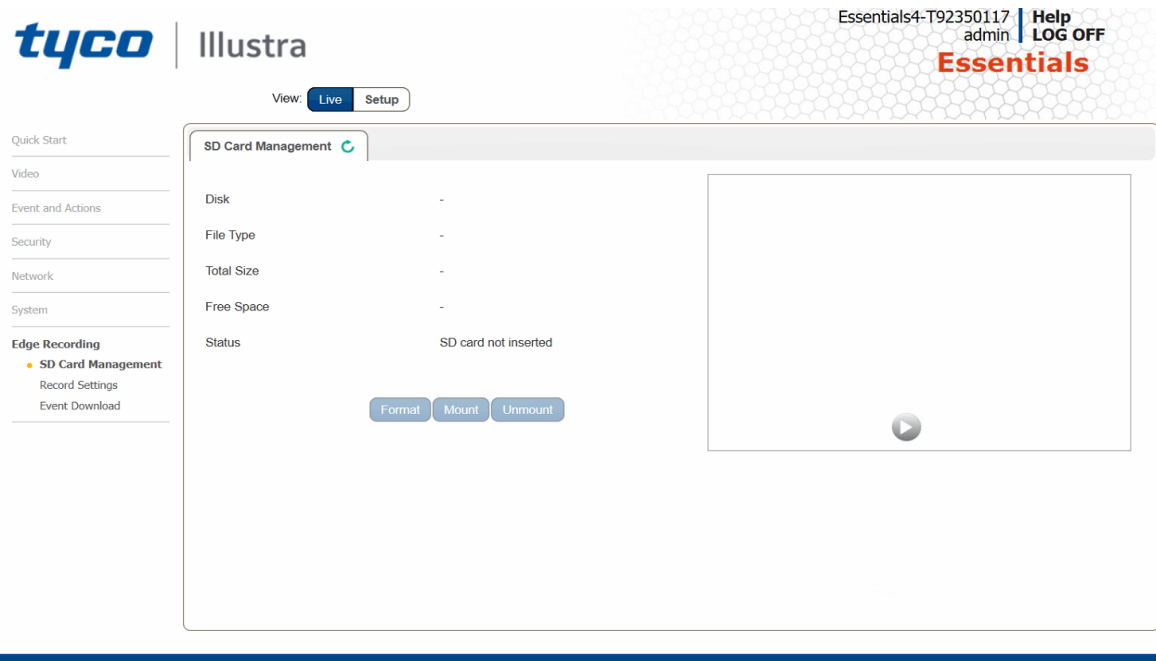
Procedure 123 Edit Camera Name

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

Edge Recording

When you select the **Edge Recording** menu, the **Micro SD Card Management** page appears, as seen in Figure 37 on page 103.

Figure 37 Edge Recording Menu



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 and screen shot are saved to the SD card.
- SMTP notifications can be sent.
- FTP uploads of video can be sent.

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 124 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 125 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 126 Remove the Micro SD Card by powering down the Camera

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

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

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

- End -

Procedure 127 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. MP4 clips are not available on the camera until the Micro SD card has been inserted and mounted. |

- End -

Record Settings

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

Procedure 128 Configure Record Settings

| Step | Action |
|------|---|
| 1 | Select Setup on the Web User Interface Banner to display the setup menus. |
| 2 | Select Record Settings from the Edge Recording menu. |
| 3 | Select Enable Record to allow the camera to create a playable video clip. OR Deselect Enable Record to disable the feature. |
| 4 | If Enable Record has been enabled: <ol style="list-style-type: none">a Select the required video stream from the Video drop-down menu. Refer to Procedure 5-1 Configure the Video Stream Settings.b Select the Post 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.d 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 129 Configure Offline Recording Settings

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

Event Download

If an event action has record mode enabled, when triggered, the associated video is logged in the event download table where it can later be downloaded from 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 | | |
| | | 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 | | |
| | | OSD | X | X | |
| | Privacy Zones | Privacy Zones | X | X | |
| Events and Actions | Event Settings | SMTP | X | | |
| | | FTP | X | | |
| | Event Actions | Event Actions | X | | |
| | Analytics | ROI | X | | |
| | | Motion Detection | X | | |
| | | Blur Detection | X | | |
| | Event Logs | Event Log | X | | |
| Security | Security Status | Security Overview | X | | |
| | Users | User | X | | |
| | | Add User | X | | |
| | | Change Password | X | X | X |
| | HTTP/HTTPS | HTTP/HTTPS | X | | |
| | IEEE 802.1x | EAP Settings | X | | |

| Camera Menu | Sub Menu | Tab | Admin | Operator | User |
|-----------------------|--------------------|--------------------|-------|----------|------|
| | Firewall | Basic Filtering | X | | |
| | | Address Filtering | X | | |
| | Remote Access | Remote Access | X | | |
| | Session Timeout | Session Timeout | X | | |
| Network | TCP/IP | TCP/IP | X | | |
| | FTP | FTP | X | | |
| | SMTP | SMTP | X | | |
| | SNMP | SNMP | X | | |
| | Dynamic DNS | Dynamic DNS | X | | |
| System | Maintenance | Maintenance | X | | |
| | | Backup / Restore | X | | |
| | Date Time | Date Time | X | | |
| | Health Monitor | Health Monitor | X | | |
| | Logs | System Log | X | | |
| | About | Model | X | X | X |
| Edge Recording | SD Card Management | SD Card Management | X | | |
| | Record Settings | Record Settings | X | | |
| | Event Download | Event Download | X | | |

Appendix B: Using Media Player to View RTSP Streaming

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

Procedure 130 Viewing RTSP Stream through Media Player

| Step | Action |
|---|--|
| You can use Media Player to view live video 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, 2 and 3: <ul style="list-style-type: none">• Stream 1: rtsp://cameraip:554/videoStreamId=1• Stream 2: rtsp://cameraip:554/videoStreamId=2• Stream 3: rtsp://cameraip:554/videoStreamId=3 For example: rtsp://192.168.1.168:554/videoStreamId=1 |
| 3 | Select Play . The live video stream displays. |
| <hr/> - End - <hr/> | |

Appendix C: Stream Tables

Essentials Gen 4 - 2MP, Streaming Combinations

Table 38 on page 110 provide information for the stream resolutions and supported FPS of the Essentials Gen 4 2MP cameras herein.

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

| | | Normal Mode | | | |
|----------|---|-------------|--------------|----------|------|
| | | Resolution | Description | Max FPS | |
| | | | | TWDR Off | TWDR |
| Stream 1 | h.264, h.265, h.264 IntelliZip h.265 IntelliZip MJPEG | 1920 x 1080 | (1080p) 16:9 | 30 | 30 |
| | | 1600 x 900 | (HD+) 16:9 | 30 | 30 |
| | | 1280 x 720 | (720p) 16:9 | 30 | 30 |
| | | 1024 x 576 | (PAL+) 16:9 | 30 | 30 |
| | | 960 x 540 | 16:9 | 30 | 30 |
| | | 800 x 480 | 16:9 | 30 | 30 |
| | | 640 x 360 | (mHD) 16:9 | 30 | 30 |
| | | 480 x 270 | 16:9 | 30 | 30 |
| | | 320 x 180 | 16:9 | 30 | 30 |
| Stream 2 | h.264, h.265, h.264 IntelliZip h.265 IntelliZip MJPEG | 1920 x 1080 | (1080p) 16:9 | 30 | 30 |
| | | 1600 x 900 | (HD+) 16:9 | 30 | 30 |
| | | 1280 x 720 | (720p) 16:9 | 30 | 30 |
| | | 1024 x 576 | (PAL+) 16:9 | 30 | 30 |
| | | 960 x 540 | 16:9 | 30 | 30 |
| | | 800 x 480 | 16:9 | 30 | 30 |
| | | 640 x 360 | (mHD) 16:9 | 30 | 30 |
| | | 480 x 270 | 16:9 | 30 | 30 |
| | | 320 x 180 | 16:9 | 30 | 30 |
| Stream 3 | h.264, h.265, h.264 IntelliZip h.265 IntelliZip MJPEG | 1280 x 720 | (720p) 16:9 | 30 | 30 |
| | | 1024 x 576 | (PAL+) 16:9 | 30 | 30 |
| | | 960 x 540 | 16:9 | 30 | 30 |
| | | 800 x 480 | 16:9 | 30 | 30 |
| | | 640 x 360 | (mHD) 16:9 | 30 | 30 |
| | | 480 x 270 | 16:9 | 30 | 30 |
| | | 320 x 180 | 16:9 | 30 | 30 |

Note: A maximum of three concurrent streams are supported by the camera. This includes shared streams.

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

| | | Corridor Mode | | | |
|----------|--|---------------|--------------|----------|------|
| | | Resolution | Description | Max FPS | |
| | | | | TWDR Off | TWDR |
| Stream 1 | h.264, h.265, h.264 IntelliZip h.265 IntelliZip | 1920 x 1080 | (1080p) 16:9 | 30 | 30 |
| | | 1600 x 900 | (HD+) 16:9 | 30 | 30 |
| | | 1280 x 720 | (720p) 16:9 | 30 | 30 |
| | | 1024 x 576 | (PAL+) 16:9 | 30 | 30 |
| | | 960 x 540 | 16:9 | 30 | 30 |
| | | 800 x 480 | 16:9 | 30 | 30 |
| | | 640 x 360 | (mHD) 16:9 | 30 | 30 |
| | | 480 x 270 | 16:9 | 30 | 30 |
| Stream 2 | h.264, h.265, h.264 IntelliZip h.265 IntelliZip | 1920 x 1080 | (1080p) 16:9 | 30 | 30 |
| | | 1600 x 900 | (HD+) 16:9 | 30 | 30 |
| | | 1280 x 720 | (720p) 16:9 | 30 | 30 |
| | | 1024 x 576 | (PAL+) 16:9 | 30 | 30 |
| | | 960 x 540 | 16:9 | 30 | 30 |
| | | 800 x 480 | 16:9 | 30 | 30 |
| | | 640 x 360 | (mHD) 16:9 | 30 | 30 |
| | | 480 x 270 | 16:9 | 30 | 30 |
| Stream 3 | h.264, h.265, h.264 IntelliZip h.265 IntelliZip | 1280 x 720 | (720p) 16:9 | 30 | 30 |
| | | 1024 x 576 | (PAL+) 16:9 | 30 | 30 |
| | | 960 x 540 | 16:9 | 30 | 30 |
| | | 800 x 480 | 16:9 | 30 | 30 |
| | | 640 x 360 | (mHD) 16:9 | 30 | 30 |
| | | 480 x 270 | 16:9 | 30 | 30 |

Note:A maximum of three concurrent streams are supported by the camera. This includes shared streams.

Note:MJPEG is not a supported codec for any stream when corridor mode is enabled.

Note:Resolution 320x180 is not supported with Corridor mode. If any stream is set to 320x180, it will be updated to 480x270 when corridor mode is applied.

Note:GUI stream is dynamic depending on current stream settings. Refer to the release notes for further information.

Appendix D: Camera Defaults

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

Table 40 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 | H264 | |
| | Profile | Main | Main | Main | |
| | 2MP Resolution | 1920x1080 | 1920x1080 | 640x360 | |
| | 2MP Frame Rate (fps) | 30 | 30 | 30 | |
| | 2MP GOP Length [1-150] | 30 | 30 | 30 | |
| | MJPEG Quality | N/A | N/A | N/A | |
| | Rate Control | CVBR | CVBR | CVBR | |
| | VBR Quality | N/A | N/A | N/A | |
| | CVBR Max Bit Rate 2MP | 8000 | 8000 | 8000 | |
| | CBR Bit Rate 2MP | 3000 | 3000 | 3000 | |
| Picture Basic | | | | | |

| Tab | Item | Default | | | |
|--------------------|---------------------------|------------------------------|--|--|--|
| | 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) | 45dB | | | |
| | 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 Wide | | | |
| | Red | Scene dependent | | | |
| | Blue | Scene dependent | | | |
| Date/Time/OSD | | | | | |
| | Camera Friendly Name | Essential4 - SERIALNUMBER | | | |

| Tab | Item | Default | | | |
|---------------|--|--------------|--|--|--|
| | Camera Time | Unspecified | | | |
| | Time 24-hour | ON | | | |
| | Date Display Format | YYYY/MM/DD | | | |
| | Time Zone | (GMT) GMT +0 | | | |
| | 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 | | | |
| | FTP Server | Unspecified | | | |
| | FTP Port | 21 | | | |
| | Username | Unspecified | | | |
| | Password | Unspecified | | | |

| Tab | Item | Default | | | |
|------------------|--------------------------|-------------|--|--|--|
| | 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 | | | |
| Event Actions | | | | | |
| | Fault action 1 | Unspecified | | | |
| | Fault action 2 | Unspecified | | | |
| | Fault action 3 | Unspecified | | | |
| | Fault action 4 | Unspecified | | | |
| | Fault action 5 | Unspecified | | | |
| ROI | | | | | |
| | Table | Unspecified | | | |
| | Action | Unspecified | | | |
| Motion Detection | | | | | |
| | Enable Motion Detection | OFF | | | |
| | Sensitivity | HIGH | | | |
| | Action | Unspecified | | | |
| Blur Detection | | | | | |
| | Enable Blur Detection | OFF | | | |

| Tab | Item | Default | | | |
|-----------------|-------------------------|-------------|--|--|--|
| Event Log | | Unspecified | | | |
| Security | | | | | |
| | Security Status | Standard | | | |
| | Enhanced Security | Disabled | | | |
| | Authenticate Video | Enabled | | | |
| | Authentication | Basic | | | |
| Users | | | | | |
| | Logon Name | Admin | | | |
| | Role | Admin | | | |
| Add User | | | | | |
| | Name | Unspecified | | | |
| | Role | Unspecified | | | |
| | Password | Unspecified | | | |
| | Confirm Password | Unspecified | | | |
| Change Password | | | | | |
| | Name | Unspecified | | | |
| | Current Password | Unspecified | | | |
| | New Password | Unspecified | | | |
| | Confirm New Password | Unspecified | | | |
| HTTP/HTTPS | | | | | |
| | HTTP Method | BOTH | | | |
| | Select Certificate File | Unspecified | | | |
| EAP Settings | | | | | |
| | Enable IEEE802.1x | OFF | | | |
| | EAPOL Version | 1 | | | |

| Tab | Item | Default | | | |
|-------------------|---------------------------|-------------|--|--|--|
| | EAP Method | PEAP | | | |
| | EAP Identity | Unspecified | | | |
| | CA Certificate | Unspecified | | | |
| | Password | Unspecified | | | |
| | Client Certificate | Unspecified | | | |
| | Private Key Password | Unspecified | | | |
| Basic Filtering | | | | | |
| | ICMP Blocking | OFF | | | |
| | Rp Filtering | OFF | | | |
| | SYN Cookie Verification | OFF | | | |
| Address Filtering | | | | | |
| | Filtering | OFF | | | |
| | IP or MAC Address | Unspecified | | | |
| Remote Access | | | | | |
| | SSH Enable | OFF | | | |
| | ONVIF Discovery Mode | ON | | | |
| | ONVIF User Authentication | ON | | | |
| | UPnP Discovery | ON | | | |
| Session Timeout | | | | | |
| | Session Timeout (mins) | 15 | | | |
| Dynamic DNS | | | | | |
| | Service Enable | OFF | | | |
| | Camera Alias | Unspecified | | | |
| | Service Provider | dyndns.org | | | |

| Tab | Item | Default | | | |
|----------------|--------------------------------------|-----------------------|--|--|--|
| | Username | Unspecified | | | |
| | Password | Unspecified | | | |
| | Service Data | Unspecified | | | |
| Maintenance | | | | | |
| | Preserve IP Address | ON | | | |
| | Select Firmware Image File | Unspecified | | | |
| 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 | | | |
| Health Monitor | | | | | |
| | Reporting Period (seconds) | 60 | | | |
| | Health Monitor Table | Unspecified | | | |
| System Log | | | | | |
| | Lines (From The End Of The Log File) | Unspecified | | | |
| | Filter (Only Lines Containing Text) | Unspecified | | | |
| Model | | | | | |
| | Camera Name | Factory configuration | | | |
| | Model | Factory configuration | | | |

| Tab | Item | Default | | | |
|--------------------|-----------------------|-----------------------|--|--|--|
| | 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 | | | |
| | Post Event (secs) | 10 | | | |
| Event Download | | | | | |
| | File Name Table | Unspecified | | | |

Appendix E: Technical Specifications

The table below lists technical specifications of the Illustra Essentials Gen 4 2MP Dome cameras.

| General Features | | |
|-------------------------|---------------------------------|---------------------------------|
| Model Type | 2MP Fixed Dome camera | 2MP VF Dome camera |
| Model No. | IES02-D10-OI04 | IES02-D12-OI04 |
| Camera Body Color | RAL 9003 - Signal White | RAL 9003 - Signal White |
| Vandal Resistant Rating | IK10 | IK10 |
| Mechanical Features | | |
| Dimensions | Ø110 x 82 mm(Ø4.33in x 3.29in) | Ø124 x 113mm(Ø4.88in x 4.45in) |
| Weight | 0.53kg (1.16 lb.) | 0.65kg (1.43 lb.) |
| Pan Rotation Angle | 355° | 355° |
| Tilt Angle | 70° | 70° |
| Z-axis Rotation | 355° | 355° |
| Housing Material | Aluminum Alloy (ADC 12) | Aluminum Alloy (ADC 12) |
| Bubble | PC (S3000UR) | PC (S3000UR) |
| Other Housing Material | PC (141R) Silicon (TSE2183U) | PC (141R) Silicon (TSE2183U) |
| Video Processor | | |
| ROM/Flash Size | 256 Mbytes | 256 Mbytes |
| RAM Size | 512 Mbytes | 512 Mbytes |
| RTC Hold Up Time | 24 hours | 24 hours |
| Image Sensor | | |
| Format | 1/2.8" CMOS | 1/2.8" CMOS |
| Capture Method | Rolling | Rolling |
| Scan Method | Progressive | Progressive |
| Lens | | |
| Design Type | 2 glasses, 3 plastics | 6 groups, 9 elements |

| | | |
|-----------------------------|---|---|
| Aperture Range | f 1.8 | f 1.4 – 2.8 |
| Focal Length Range | f 2.8mm | f 2.7-13.5mm |
| Focal Means | Fixed | Motorized |
| Focal Type | Fixed | Varifocal |
| Focus Type | Fixed | Motorized |
| Auto Focus | N/A | One-Touch / Manual |
| IR Correction | Optical corrected | Optical corrected |
| Day/Night | True D/N with ICR | True D/N with ICR |
| Horizontal Angle of View | 112° | 105° (Wide); 30° (Tele) |
| Vertical Angle of View | 60° | 75° (Wide); 22° (Tele) |
| Format | 1 / 2.7" | 1 / 2.7" |
| Illuminator | | |
| Wavelength | 850 nm | 850 nm |
| IR Distance | 25m range IR | 30m range IR |
| Smart IR | Yes | Yes |
| Adaptive IR | N/A | N/A |
| Power Supply | | |
| Power Requirement | Power over Ethernet (PoE) IEEE 802.3af Type 1 Class 3 DC 12V | Power over Ethernet (PoE) IEEE 802.3af Type 1 Class 3 DC 12V |
| Current Draw Amps | PoE = 0.15A DC 12V = 0.6A | PoE = 0.2A DC 12V = 0.82A |
| Wattage | PoE = 7.2W DC 12V = 7.3W | PoE = 9.7W DC 12V = 9.9W |
| Line Frequency Range | N/A | N/A |
| 12V DC range | -10% +10% | -10% +10% |
| Video Codecs | | |
| Frame Rate Range | 1 to 30 fps | 1 to 30 fps |
| Maximum Resolution and Rate | 1920 x 1080 @ 30 fps | 1920 x 1080 @ 30 fps |

| Video Imaging | | |
|-----------------------------|--|--|
| Dynamic Range Method | Digital WDR, True WDR | Digital WDR, True WDR |
| I/O Interfaces | | |
| Micro SD Card | Micro SD & SDXC slot up to 256GB; Class 10 or higher; Card not included | Micro SD & SDXC slot up to 256GB; Class 10 or higher; Card not included |
| Alarm Inputs | N/A | N/A |
| Auxiliary Outputs | N/A | N/A |
| Video Output | N/A | N/A |
| IP Connector | RJ-45 | RJ-45 |
| LED Indicators | Power (Red), Network communication (Green) | Power (Red), Network communication (Green) |
| Reset Buttons | Reboot Return to defaults | Reboot Return to defaults |
| Environmental | | |
| Operating Temperature Range | -30° to +55°C (-22° to +131°F) | -30° to +55°C (-22° to +131°F) |
| Start-up Temperature Range | -20° to +55°C (-4° to +131°F) | -20° to +55°C (-4° to +131°F) |
| Water/Dust Intrusion | IP67 | IP67 |
| Client Interfaces | | |
| Browsers supported | IE 9 or above, Firefox, Safari, Chrome | IE 9 or above, Firefox, Safari, Chrome |
| Networking | | |
| Languages supported | English (default), Arabic, Czech, Danish, German, Spanish, French, Hungarian, Italian, Korean, Japanese, Netherlands, Polish, Portuguese, Swedish, Turkish, Chinese Traditional, Chinese Simplified, Russian, Hindi. | English (default), Arabic, Czech, Danish, German, Spanish, French, Hungarian, Italian, Korean, Japanese, Netherlands, Polish, Portuguese, Swedish, Turkish, Chinese Traditional, Chinese Simplified, Russian, Hindi. |
| Ethernet | 10/100 Base-T | 10/100 Base-T |
| Supported Protocols | TCP/IP, IPv4, IPv6, TCP, UDP, HTTP, FTP, DHCP, WS-Discovery, DNS, DDNS, RTP, TLS, Unicast, NTP, SMTP, WSSecurity, IEEE 802.1x, PEAP, SSH, CIFS, HTTPS, SSL, SOAP, WSAddressing, SNMP, UPnP, RTSP, LLDP | TCP/IP, IPv4, IPv6, TCP, UDP, HTTP, FTP, DHCP, WS-Discovery, DNS, DDNS, RTP, TLS, Unicast, NTP, SMTP, WSSecurity, IEEE 802.1x, PEAP, SSH, CIFS, HTTPS, SSL, SOAP, WSAddressing, SNMP, UPnP, RTSP, LLDP |
| Base Protocol | TCP/IP - RFC4614 | TCP/IP - RFC4614 |

| | | |
|-------------------------------|--|--|
| Internet Layer Addressing | IPv4 - RFC791 IPv6 - RFC2460 | IPv4 - RFC791 IPv6 - RFC2460 |
| Transport Layer | TCP - RFC973 UDP - RFC768 | TCP - RFC973 UDP - RFC768 |
| Data Transmission | HTTP/HTTPS - RFC2616 FTP - RFC959 | HTTP/HTTPS - RFC2616 FTP - RFC959 |
| Network Address Configuration | DHCP - RFC2131 Zeroconf - RFC3927 Static IP address LLDP | DHCP - RFC2131 Zeroconf - RFC3927 Static IP address LLDP |
| Time Synchronization | NTP - RFC1305 IETF NTP Working Group i minute poll rate | NTP - RFC1305 IETF NTP Working Group i minute poll rate |
| E-mail | SMTP - RFC5321 Authenticated SMTP - RFC4954 | SMTP - RFC5321 Authenticated SMTP - RFC4954 |
| Authentication and Security | IEEE.802.1x - TLS/PEAP HTTPS (HTTP over TLS) - RFC2818 WS-Security Multi-level password protection IP address filtering HTTPS encryption User access log | IEEE.802.1x - TLS/PEAP HTTPS (HTTP over TLS) - RFC2818 WS-Security Multi-level password protection IP address filtering HTTPS encryption User access log |
| Streaming | RTP - RFC3550 RTSP - RFC2326 Unicast Streaming | RTP - RFC3550 RTSP - RFC2326 Unicast Streaming |
| Firmware Upgrade | Browser/illustra Connect/ONVIF | Browser/illustra Connect/ONVIF |

The table below lists technical specifications of the Illustra Essentials Gen 4 2MP Bullet cameras.

| General Features | | |
|-------------------------|---|---|
| Model Type | 2MP Fixed Bullet camera | 2MP VF Bullet camera |
| Model No. | IES02-B10-BI04 | IES02-B12-BI04 |
| Camera Body Color | RAL 9003 - Signal White | RAL 9003 - Signal White |
| Vandal Resistant Rating | Front: IK07 Body: IK08 | Front: IK07 Body: IK08 |
| Mechanical Features | | |
| Dimensions | 77x84x147mm(3.03in x 3.3in x 5.78in) | 77x84x176mm(3.03in x 3.3in x 6.92in) |
| Weight | 0.49kg (1.08 lb) | 0.58kg (1.28lb) |
| Pan Rotation Angle | 360° | 360° |
| Tilt Angle | 90° | 90° |
| Z-axis Rotation | N/A | N/A |
| Housing Material | PC (L-1250Z) | PC (L-1250Z) |
| Bracket Material | PC (L-1250Z) | PC (L-1250Z) |
| Other Housing Material | PC (S-3000UR) (L-1225Z) Silicon (TSE2183U) (KE-951U) | PC (S-3000UR) (L-1225Z) Silicon (TSE2183U) (KE-951U) |
| Video Processor | | |
| ROM/Flash Size | 256 Mbytes | 256 Mbytes |
| RAM Size | 512 Mbytes | 512 Mbytes |
| RTC Hold Up Time | 24 hours | 24 hours |
| Image Sensor | | |
| Format | 1/2.8" CMOS | 1/2.8" CMOS |
| Capture Method | Rolling | Rolling |
| Scan Method | Progressive | Progressive |
| Lens | | |
| Design Type | 2 glasses, 3 plastics | 6 groups, 9 elements |
| Mount | 14mm | 14mm |
| Aperture Range | F 1.8 | F 1.4 – 2.8 |
| Focal Length Range | F 2.8mm | F 2.7-13.5mm |

| | | |
|-----------------------------|---|---|
| Focal Means | Fixed | Motorized |
| Focal Type | Fixed | Varifocal |
| Focus Type | Fixed | Motorized |
| Auto Focus | N/A | One-Touch / Manual |
| IR Correction | Optical corrected | Optical corrected |
| Day/Night | True D/N with ICR | True D/N with ICR |
| Horizontal Angle of View | 112° | 105° (Wide); 30° (Tele) |
| Vertical Angle of View | 60° | 75° (Wide); 22° (Tele) |
| Format | 1 / 2.7 | 1 / 2.7 |
| Illuminator | | |
| Wavelength | 850 nm | 850 nm |
| IR Distance | 30m range IR | 30m range IR |
| Smart IR | Yes | Yes |
| Adaptive IR | N/A | N/A |
| Power Supply | | |
| Power Requirement | Power over Ethernet (PoE) IEEE 802.3af Type 1 Class 3 DC 12V | Power over Ethernet (PoE) IEEE 802.3af Type 1 Class 3 DC 12V |
| Current Draw Amps | PoE = 0.17A DC 12V = 0.69A | PoE = 0.2A DC 12V = 0.82A |
| Wattage | PoE = 8.2W DC 12V = 8.3A | PoE = 9.7W DC 12V = 9.9A |
| Line Frequency Range | N/A | N/A |
| 12V DC range | -10% + 10% | -10% + 10% |
| Video Codecs | | |
| Frame Rate Range | 1 to 30 fps | 1 to 30 fps |
| Maximum Resolution and Rate | 1920 x 1080 @ 30 fps | 1920 x 1080 @ 30 fps |
| Video Imaging | | |
| Dynamic Range Method | Digital WDR, True WDR | Digital WDR, True WDR |
| I/O Interfaces | | |
| Micro SD Card | Micro SD & SDXC slot up to 256GB; | Micro SD & SDXC slot up to 256GB; Class 10 or |

| | | |
|-----------------------------|--|--|
| | Class 10 or higher; Card not included | higher; Card not included |
| Alarm Inputs | N/A | N/A |
| Auxiliary Outputs | N/A | N/A |
| Video Output | N/A | N/A |
| IP Connector | RJ-45 | RJ-45 |
| LED Indicators | Network, Green LED, Orange LED | Network, Green LED, Orange LED |
| Reset Buttons | Reboot Return to defaults | Reboot Return to defaults |
| Environmental | | |
| Operating Temperature Range | -30° to +55°C (-22° to +131°F) | -30° to +55°C (-22° to +131°F) |
| Start-up Temperature Range | -20° to +55°C (-4° to +131°F) | -20° to +55°C (-4° to +131°F) |
| Water/Dust Intrusion | IP67 | IP67 |
| Client Interfaces | | |
| Browsers supported | IE 9 or above, Firefox, Safari, Chrome | IE 9 or above, Firefox, Safari, Chrome |
| Networking | | |
| Languages supported | English (default), Arabic, Czech, Danish, German, Spanish, French, Hungarian, Italian, Korean, Japanese, Netherlands, Polish, Portuguese, Swedish, Turkish, Chinese Traditional, Chinese Simplified, Russian, Hindi. | English (default), Arabic, Czech, Danish, German, Spanish, French, Hungarian, Italian, Korean, Japanese, Netherlands, Polish, Portuguese, Swedish, Turkish, Chinese Traditional, Chinese Simplified, Russian, Hindi. |
| Ethernet | 10/100 Base-T | 10/100 Base-T |
| Supported Protocols | TCP/IP, IPv4, IPv6, TCP, UDP, HTTP, FTP, DHCP, WS-Discovery, DNS, DDNS, RTP, TLS, Unicast, NTP, SMTP, WSSecurity, IEEE 802.1x, PEAP, SSH, HTTPS, SSL, SOAP, WSAddressing, SNMP, UPnP, RTSP, LLDP | TCP/IP, IPv4, IPv6, TCP, UDP, HTTP, FTP, DHCP, WS-Discovery, DNS, DDNS, RTP, TLS, Unicast, NTP, SMTP, WSSecurity, IEEE 802.1x, PEAP, SSH, HTTPS, SSL, SOAP, WSAddressing, SNMP, UPnP, RTSP, LLDP |
| Base Protocol | TCP/IP - RFC4614 | TCP/IP - RFC4614 |
| Internet Layer Addressing | IPv4 - RFC791 IPv6 - RFC2460 | IPv4 - RFC791 IPv6 - RFC2460 |
| Transport Layer | TCP - RFC973 UDP - RFC768 | TCP - RFC973 UDP - RFC768 |
| Data Transmission | HTTP/HTTPS - RFC2616 FTP - RFC959 | HTTP/HTTPS - RFC2616 FTP - RFC959 |

| | | |
|-------------------------------|--|--|
| Network Address Configuration | DHCP - RFC2131 Zeroconf - RFC3927 Static IP address LLDP | DHCP - RFC2131 Zeroconf - RFC3927 Static IP address LLDP |
| Time Synchronization | NTP - RFC1305 IETF NTP Working Group i minute poll rate | NTP - RFC1305 IETF NTP Working Group i minute poll rate |
| E-mail | SMTP - RFC5321 Authenticated SMTP - RFC4954 | SMTP - RFC5321 Authenticated SMTP - RFC4954 |
| Authentication and Security | IEEE.802.1x - TLS/PEAP HTTPS (HTTP over TLS) - RFC2818 WS-Security Multi-level password protection IP address filtering HTTPS encryption User access log | IEEE.802.1x - TLS/PEAP HTTPS (HTTP over TLS) - RFC2818 WS-Security Multi-level password protection IP address filtering HTTPS encryption User access log |
| Streaming | RTP - RFC3550 RTSP - RFC2326 Unicast Streaming | RTP - RFC3550 RTSP - RFC2326 Unicast Streaming |
| Firmware Upgrade | Browser/illustra Connect/ONVIF | Browser/illustra Connect/ONVIF |

END USER LICENSE AGREEMENT (EULA)

IMPORTANT NOTICE: This End User License Agreement (“Agreement”) is a binding legal contract between you (“you”) and Johnson Controls International plc. (including its Affiliates such as Johnson Controls, Inc.) with a corporate address at 507 E. Michigan St., Milwaukee, WI (“JCI”, “we”, or “us”). By downloading, installing, accessing or using the accompanying software (the “Software”) you will be bound by the terms of this Agreement. If you do not agree to the terms of this Agreement, JCI is not willing to grant you any right to use or access the Software. In such event, you may not download, install, access, use or copy the Software. If this agreement is being agreed to by a company or other legal entity, then the person agreeing to this agreement on behalf of that company or entity represents and warrants that he or she is authorized and lawfully able to bind that company or entity to this agreement. You should print and retain a copy of this agreement for your records. Unless a separate agreement is provided, other JCI application software distributed by this Software will also be subject to the terms of this agreement.

PLEASE READ THE FOLLOWING TERMS AND CONDITIONS CAREFULLY BEFORE DOWNLOADING, INSTALLING, ACCESSING OR USING THE SOFTWARE.

Agreement Structure. This Agreement includes Part 1 – General Terms and Part 2 – Country Specific Terms, as applicable. The terms of Part 2 may replace or modify those of Part 1. In the event of a conflict between the terms of any or all of Part 1 and Part 2, the terms of Part 2 shall prevail over Part 1.

PART 1 – General Terms

1. Grant of License. During the term of this Agreement, JCI grants you and your individual employees a revocable, non-transferable, non-sublicensable, nonexclusive license to use the object code version of the Software and any Documentation for your internal use only, subject to all Scope Restrictions. The order document under which you have licensed the Software may contain additional terms limiting the scope your license, including, but not limited to, a specified number of users or specific systems, licensed facilities, geographic areas, etc. (collectively, “Scope Restrictions”). In the event the Software is furnished for use in connection with a particular JCI system or hardware product, it may only be used in conjunction with that JCI system or hardware product. If the Software is furnished embedded in a JCI system or hardware product, the Software may not be extracted or used separately from that system or product. “Documentation” means JCI then current generally available documentation for use and operation of the Software. Documentation is deemed included in the definition of Software. The term “Software” will be deemed to include any updates, bug fixes, and versions (collectively, “Enhancements”) that JCI may, in its discretion, make available to you. You are responsible for ensuring your employees comply with all relevant terms of this Agreement and any failure to comply will constitute a breach by you. The Software is licensed, not sold. Except for the limited license granted above, JCI and its licensors retain all right, title and interest in the Software, all copies thereof, and all proprietary rights in the Software, including copyrights, patents, trademarks and trade secret rights.

2. Restrictions. Your use of the Software must be in accordance with the Documentation. You will be solely responsible for ensuring your use of the Software is in compliance with all applicable foreign, federal, state and local laws, rules and regulations. You may not (i) copy or distribute the Software except to the extent that copying is necessary to use the Software for purposes set forth herein; provided you may make a single copy of the Software for backup and archival purposes; (ii) modify or create derivative works of the Software; (iii) decompile, disassemble, reverse engineer, or otherwise attempt to derive the trade secrets embodied in the Software, except and only to the extent that such activity may be expressly permitted, notwithstanding this limitation or another limitation contained in this agreement, either by applicable law or, in the case of open source software, the

applicable open source license; (iv) use the Software for purposes of developing a competing product or service; (v) remove any copyright, trademark, proprietary rights, disclaimer, or warning notice included on or embedded in any part of the Documentation and Software; (v) assign, sublicense, rent, timeshare, loan, lease or otherwise transfer the Software, or directly or indirectly permit any third party to use or copy the Software. Under no circumstances will JCI be liable or responsible for any use, or any results obtained by the use, of the services in conjunction with any services, software, or hardware that are not provided by JCI. All such use will be at your sole risk and liability.

3. Third Party Software. To the extent any software licensed from third parties, including open source software, (collectively, "Third Party Software") is provided with or incorporated into the Software, you will comply with the terms and conditions of the applicable third party licenses associated with the Third Party Software, in addition to the terms and restrictions contained in this Agreement. All relevant licenses for the Third Party Software are provided at www.johnsoncontrols.com/buildings/legal/digital. By using the Software you are also agreeing to be bound to the terms of such third party licenses. If provided for in the applicable third party license, you may have a right to reverse engineer such open source software or receive open source code for such open source software for use and distribution in any program that you create, so long as you in turn agree to be bound to the terms of the applicable third party license, and your programs are distributed under the terms of that license. If applicable, a copy of such open source code may be obtained free of charge by contacting your Johnson Controls representative. JCI MAKES NO WARRANTY OF ANY KIND, WHETHER EXPRESS OR IMPLIED, WITH REGARD TO ANY THIRD PARTY SOFTWARE. ALL THIRD PARTY SOFTWARE IS PROVIDED "AS-IS," WITHOUT WARRANTIES OF ANY KIND. IN NO EVENT WILL JCI BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY DIRECT, INDIRECT, PUNITIVE, EXEMPLARY, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE THIRD PARTY SOFTWARE, EVEN IF JCI HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSSES.

4. Metering Devices. The Software may contain technology based metering devices and passive restraints to regulate usage. For example, the Software may contain a license file limiting use to the licensed number of concurrent users or named users or may temporarily restrict usage until license and other fees have been paid in full. You acknowledge that such restraints and metering devices are a reasonable method to ensure compliance with the license and have been factored into the license and other fees and the Agreement as a whole. You agree that You will not circumvent, override, or otherwise bypass such metering devices and restraints that regulate the use of the Software.

5. Term and Termination. Unless provided otherwise in an accompanying order document, this Agreement will commence on the earlier of the date you first download, install, access or use the Software (the "Effective Date") and continue in effect for the term specified in the order document or, if no term is specified, until it is terminated (the "Term") as provided in this Section. Either party may terminate this Agreement on written notice to the other party if the other party is in material breach of its obligations hereunder and fails to cure the breach within thirty (30) days of such written notice. In addition, either party may, in its sole discretion, elect to terminate this Agreement on written notice to the other party upon the bankruptcy or insolvency of the other party or upon the bankruptcy or insolvency of the other party upon the commencement of any voluntary or involuntary winding up, or upon the filing of any petition seeking the winding up of the other party. In the event of any claim of infringement relating to the Software, JCI may terminate this Agreement on written notice to you and, as your sole and exclusive remedy, refund the license fees paid, if any, hereunder (less depreciation calculated on a three (3)-year straight-line basis commencing on the date of initial delivery to you). Sections 9 and 10 shall remain unaffected. Upon any termination or expiration of this Agreement, the license granted in Section 1 will automatically terminate and you will have no further right to possess or use the Software. On JCI's request, you will provide JCI with a signed written statement confirming that the Software has been permanently removed from your systems.

6. Fees; Taxes. You will pay the fees, if any, associated with the Software. All amounts due hereunder shall be paid within thirty (30) days of the date of the invoice. Payments not made within such time period shall be subject to late charges equal to the lesser of (i) one and one-half percent (1.5%) per month of the overdue amount or (ii) the maximum amount permitted under applicable law. If the license granted to You is a term or subscription license: then, unless set forth in your applicable ordering document, any renewal of such license shall be at then-current JCI list price and any such license shall automatically terminate upon nonpayment of amounts due hereunder. All taxes, duties, fees and other governmental charges of any kind (including sales and use taxes, but excluding taxes based on the gross revenues or net income of JCI) that are imposed by or under the authority of any government or any political subdivision thereof on the fees for the Software shall be borne solely by you, unless you can evidence tax exemption and shall not be considered a part of a deduction from or an offset against such fees. If you lose tax exempt status, you will pay any taxes due as part of any renewal or payment. You will promptly notify JCI if your tax status changes. You will pay all court costs, fees, expenses and reasonable attorneys' fees incurred by JCI in collecting delinquent fees.

7. Limited Warranty; Disclaimer. JCI warrants that (i) for a period of thirty (30) days from delivery initial delivery to you (the "Warranty Period"), the Software will operate in substantial conformity with its Documentation; and (ii) it shall use screening software to scan the Software prior to delivery for viruses, Trojan horses, and other malicious code. If, during the Warranty Period, you notify JCI of any non-compliance with the foregoing warranties, JCI will, in its discretion: (a) use commercially reasonable efforts to provide the programming services necessary to correct any verifiable non-compliance with the foregoing warranties; or (b) replace any non-conforming Software; or if neither of foregoing options is reasonably available to JCI, (c) terminate this Agreement in whole or in part, and refund to You the fees, if any, paid for the non-conforming Software (less depreciation calculated on a three (3)-year straight-line basis commencing on the date of initial delivery to you). JCI shall not be liable for failures caused by third party hardware and software (including your own systems), misuse of the Software, or your negligence or willful misconduct. EXCEPT AS PROVIDED IN THIS SECTION, THE SOFTWARE IS PROVIDED ON AN "AS AVAILABLE," "AS IS" BASIS. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JCI AND ITS AFFILIATES, AND THEIR RESPECTIVE SUPPLIERS AND VENDORS DISCLAIM ALL OTHER WARRANTIES WITH RESPECT TO THE SOFTWARE, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, TITLE, MERCHANTABILITY, QUIET ENJOYMENT, QUALITY OF INFORMATION, AND FITNESS FOR A PARTICULAR PURPOSE. JCI AND ITS AFFILIATES AND THEIR RESPECTIVE SUPPLIERS AND VENDORS DO NOT WARRANT THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS, OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE SOFTWARE WILL BE CORRECTED. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY JCI OR ANY OF ITS PERSONNEL OR AGENTS SHALL CREATE ANY ADDITIONAL JCI WARRANTIES OR IN ANY WAY INCREASE THE SCOPE OF JCI'S OBLIGATIONS HEREUNDER.

8. Indemnities. JCI will indemnify, defend, and hold you harmless from any claim, demand, action, proceeding, judgment, or liability arising out of a claim by a third-party that your use of the Software in conformance with the terms of this Agreement infringes a United States patent, copyright, or trade secret of that third party. The foregoing indemnification obligation of JCI is contingent upon you promptly notifying JCI in writing of such claim, permitting JCI sole authority to control the defense or settlement of such claim, and providing JCI reasonable assistance in connection therewith. If a claim of infringement under this Section occurs, or if JCI determines a claim is likely to occur, JCI will have the right, in its sole discretion, to either: (i) procure for you the right or license to continue to use the Software free of the infringement claim; or (ii) modify the Software to make it non-infringing, without loss of material functionality. If either of these remedies is not reasonably available to JCI, JCI may, in its sole discretion, immediately terminate this Agreement and return the license fees paid by you for the Software, prorated on a three (3)-year straight-line basis commencing on the date of initial delivery to you. Notwithstanding the foregoing, JCI shall have no obligation with respect to any claim

of infringement that is based upon or arises out of (the “Excluded Claims”): (i) the use or combination of the Software with any third party hardware, software, products, data or other materials, including your own systems and data; (ii) modification or alteration of the Software by anyone other than JCI; (iii) your use of the Software in excess of the rights granted in this Agreement; or (iv) any Third Party Software. The provisions of this Section state the sole and exclusive obligations and liability of JCI and its JCIs and suppliers for any claim of intellectual property infringement arising out of or relating to the Software and/or this Agreement and are in lieu of any implied warranties of non-infringement, all of which are expressly disclaimed. Section 9 shall remain unaffected. You will, subject to your culpability, indemnify, defend, and hold JCI harmless from any claim, demand, action, proceeding, judgment, or liability from a third-party claim arising out of an Excluded Claim. JCI must promptly notify you in writing of any such claim, permit you sole authority to control the defense or settlement of the claim, and provide you reasonable assistance in connection therewith.

9. Limitation of Liability. TO THE MAXIMUM EXTENT PERMITTED BY LAW, IN NO EVENT SHALL JCI AND ITS AFFILIATES AND THEIR RESPECTIVE SUPPLIERS AND VENDORS BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE, OR INDIRECT DAMAGES, WHICH SHALL INCLUDE, WITHOUT LIMITATION, DAMAGES FOR PERSONAL INJURY, LOST PROFITS, LOST DATA AND BUSINESS INTERRUPTION, ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE, EVEN IF THEY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ANY CASE, THE ENTIRE AGGREGATE LIABILITY OF JCI AND ITS AFFILIATES AND THEIR RESPECTIVE SUPPLIERS AND VENDORS UNDER THIS AGREEMENT FOR ALL DAMAGES, LOSSES, AND CAUSES OF ACTION (WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE) SHALL BE LIMITED TO FEES PAID BY YOU FOR THE SOFTWARE, IF ANY, DURING THE THREE (3) MONTHS IMMEDIATELY PRECEDING THE FIRST EVENT GIVING RISE TO LIABILITY.

10. Confidentiality. You acknowledge that the ideas, methods, techniques, and expressions thereof contained in the Software (collectively, “JCI Confidential Information”) constitute confidential and proprietary information of JCI, the unauthorized use or disclosure of which would be damaging to JCI. You agree to hold the Software and JCI Confidential Information in strictest confidence, disclosing information only to permitted individual employees who are required to have access in order to perform under this Agreement and to use such information only for the purposes authorized by this Agreement. You are responsible for and agree to take all reasonable precautions, by instruction, agreement or otherwise, to ensure that your employees who are required to have access to such information in order to perform under this Agreement, are informed that the Software and JCI Confidential Information are confidential proprietary information belonging to JCI and to ensure that they make no unauthorized use or disclosure of such information. You may disclose JCI Confidential Information if you are required to do so pursuant to a governmental agency, a court of law or to any other competent authority so long as you provide JCI with written notice of such request prior to such disclosure and cooperate with JCI to obtain a protective order. Prior to disposing of any media reflecting or on which is stored or placed any Software, you will ensure any Software contained on the media has been securely erased or otherwise destroyed. You recognize and agree a remedy at law for damages will not be adequate to fully compensate JCI for the breach of Sections 1, 2, or 10. Therefore, JCI will be entitled to temporary injunctive relief against you without the necessity of proving actual damages and without posting bond or other security. Injunctive relief will in no way limit any other remedies JCI may have as a result of breach by You of the foregoing Sections or any other provision of this Agreement.

11. Data Collection and Use. You acknowledge and agree that the Software and/or hardware used in connection with the Software may collect data resulting from or otherwise relating to your use of the Software and/or hardware (“Data”) for purposes of providing you with service/product recommendations, benchmarking, energy monitoring, and maintenance and support. JCI shall be the exclusive owner of all Data. JCI shall have the right to de-identify your Data so that it does not identify you directly or by inference (the “De-Identified Data”). JCI shall have the right and ability to

use the De-Identified Data for its business purposes, including improvement of the Software, research, product development, product improvement and provision of products and services to JCI's other customers (collectively, "JCI's Business Purposes". In the event JCI does not own or is unable to own the De-Identified Data as a result of applicable law, or contractual commitments or obligations, you grant JCI a non-exclusive, perpetual, irrevocable, fully-paid-up, royalty free license to use, copy, distribute, and otherwise exploit statistical and other data derived from your use of the De-Identified Data for JCI's Business Purposes.

12. Feedback. You may provide suggestions, comments, or other feedback (collectively, "Feedback") to JCI with respect to its products and services, including the Software. Feedback is voluntary and JCI is not required to hold it in confidence. JCI may use Feedback for any purpose without obligation of any kind. To the extent a license is required under your intellectual property rights to make use of the Feedback, you grant JCI an irrevocable, non-exclusive, perpetual, worldwide, royalty-free license to use the Feedback in connection with JCI's business, including enhancement of the Software, and the provision of products and services to JCI's customers.

13. Governing Law and Jurisdiction.

13.1 Governing Law. This Agreement is governed by and construed in accordance with the laws of the State of Wisconsin, as applied to agreements entered into and wholly performed within Wisconsin between Wisconsin residents. In the event the foregoing sentence is determined by a court of competent jurisdiction to not be enforceable or applicable to an action or proceeding brought by either party relating to or under this Agreement, the parties agree to the application of the laws of the country in which you entered into this Agreement to govern, interpret, and enforce all of your and JCI's respective rights, duties, and obligations arising from, or relating in any manner to, the subject matter of this Agreement, without regard to conflict of law principles. The United Nations Convention on Contracts for the International Sale of Goods does not apply to any such action or proceeding.

13.2 Jurisdiction. Any action or proceeding brought by either party hereto shall be brought only in a state or federal court of competent jurisdiction located in Milwaukee, Wisconsin and the parties submit to the in personam jurisdiction of such courts for purposes of any action or proceeding. In the event the foregoing sentence is determined by a court of competent jurisdiction to not be enforceable or applicable to an action or proceeding brought by either party relating to or under this Agreement, the parties agree all rights, duties, and obligations of the parties are subject to the courts of the country in which You entered into this Agreement.

14. General. This Agreement constitutes the entire understanding and agreement between the parties with respect to the transactions contemplated in this Agreement and supersedes all prior or contemporaneous oral or written communications with respect to the subject matter of this Agreement, all of which are merged in this Agreement. This Agreement shall not be modified, amended or in any way altered except by an instrument in writing signed by authorized representatives of both parties. In the event that any provision of this Agreement is found invalid or unenforceable pursuant to judicial decree, the remainder of this Agreement shall remain valid and enforceable according to its terms. Any failure by JCI to strictly enforce any provision of this Agreement will not operate as a waiver of that provision or any subsequent breach of that provision. The following provisions shall survive any termination or expiration of this Agreement: Sections 2 (Restrictions), 4 (Term and Termination), 6 (Fees and Taxes) (to the extent of any fees accrued prior to the date of termination), 9 (Limitation of Liability), 10 (Confidentiality), 11 (Feedback), 13 (Governing Law), 14 (General), and 16 (U.S. Government Rights). JCI may assign any of its rights or obligations hereunder as it deems appropriate. **IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT IN THE EVENT ANY REMEDY HEREUNDER IS DETERMINED TO HAVE FAILED OF ITS ESSENTIAL PURPOSE, ALL LIMITATIONS OF LIABILITY AND EXCLUSIONS OF DAMAGES SET FORTH HEREIN SHALL REMAIN IN EFFECT.**

15. Export/Import. The Software is licensed for use in the specific country authorized by JCI. You may not export or import the Software to another country without JCI's written permission and

payment of any applicable country specific surcharges. You agree to comply fully with all relevant and applicable export and import laws and regulations of the United States and foreign nations in which the Software will be used ("Export/Import Laws") to ensure that neither the Software nor any direct product thereof are (a) exported or imported, directly or indirectly, in violation of any Export/Import Laws; or (b) are intended to be used for any purposes prohibited by the Export/Import Laws. Without limiting the foregoing, you will not export or re-export or import the Software: (a) to any country to which the United States or European Union has embargoed or restricted the export of goods or services or to any national of any such country, wherever located, who intends to transmit or transport the Software back to such country; (b) to any user who you know or have reason to know will utilize the Software in the design, development or production of nuclear, chemical or biological weapons; or (c) to any user who has been prohibited from participating in export transactions by any federal or national agency of the U.S. government or European Union. You will defend, indemnify, and hold harmless JCI and its affiliates and their respective licensors and suppliers from and against any and all damages, fines, penalties, assessments, liabilities, costs and expenses (including attorneys' fees and expenses) arising out of any your breach of this Section.

16. U.S. Government Rights. The Software is a "commercial item" as that term is defined at 48 CFR 2.101 (October 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 CFR 12.212 (September 1995), and is provided to the U.S. Government only as a commercial end item. Consistent with 48 CFR 12.212 and 48 CFR 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire the Software with only those rights set forth herein.

17. Electronic Acceptance. This Agreement may be accepted in electronic form (e.g., by an electronic or other means of demonstrating assent) and your acceptance will be deemed binding between the parties. Neither party may contest the validity or enforceability of this Agreement, including under any applicable statute of frauds, because it was accepted or signed in electronic form. Electronically maintained records when produced in hard copy form shall constitute business records and shall have the same validity as any other generally recognized business records.

PART 2 - Country Specific Terms

For licenses granted in the countries specified below, the following terms replace or modify the referenced terms in Part 1 and Part 3. All terms in Part 1 and Part 3 that are not changed by these amendments remain unchanged and in effect. This Part 2 is organized as follows:

13.1 Governing Law The phrase "the laws of the country in which You entered into this Agreement" in Section 13.1 (Governing Law) is replaced by the following language as it applies to the countries identified below:

Americas

Canada: the laws in the Province of Ontario;

Mexico: the federal laws of the Republic of Mexico;

United States, Anguilla, Antigua/Barbuda, Aruba, British Virgin Islands, Cayman Islands, Dominica, Grenada, Guyana, Saint Kitts and Nevis, Saint Lucia, Saint Maarten, and Saint Vincent and the Grenadines: the laws of the State of Wisconsin, United States;

Venezuela: the laws of the Bolivarian Republic of Venezuela;

Asia Pacific

Cambodia and Laos: the laws of the State of Wisconsin, United States;

Australia: the laws of the State or Territory in which the transaction is performed;

Hong Kong SAR and Macau SAR: the laws of Hong Kong Special Administrative Region ("SAR");

Taiwan: the laws of Taiwan;

Europe, Middle East, and Africa

Albania, Armenia, Azerbaijan, Belarus, Bosnia-Herzegovina, Bulgaria, Croatia, Former Yugoslav Republic of Macedonia, Georgia, Hungary, Kazakhstan, Kyrgyzstan, Moldova, Montenegro, Poland, Romania, Russia, Serbia, Slovakia, Tajikistan, Turkmenistan, Ukraine, and Uzbekistan: the laws of Austria;

Algeria, Andorra, Benin, Burkina Faso, Cameroon, Cape Verde, Central African Republic, Chad, Comoros, Congo Republic, Djibouti, Democratic Republic of Congo, Equatorial Guinea, French Guiana, French Polynesia, Gabon, Gambia, Guinea, Guinea-Bissau, Ivory Coast, Lebanon, Madagascar, Mali, Mauritania, Mauritius,

Mayotte, Morocco, New Caledonia, Niger, Reunion, Senegal, Seychelles, Togo, Tunisia, Vanuatu, and Wallis and Futuna: the laws of France;

Estonia, Latvia, and Lithuania: the laws of Finland;

Angola, Bahrain, Botswana, Burundi, Egypt, Eritrea, Ethiopia, Ghana, Jordan, Kenya, Kuwait, Liberia, Malawi, Malta, Mozambique, Nigeria, Oman, Pakistan, Qatar, Rwanda, Sao Tome and Principe, Saudi Arabia, Sierra Leone, Somalia, Tanzania, Uganda, United Arab Emirates, the United Kingdom, West Bank/Gaza, Yemen, Zambia, and Zimbabwe: the laws of England and Wales; and South Africa, Namibia, Lesotho, and Swaziland: the laws of the Republic of South Africa.

13.2 Jurisdiction The following provisions replace Section 13.2 (Jurisdiction) as it applies for those countries identified below: All rights, duties, and obligations are subject to the courts of the country in which You entered into this Agreement except that in the countries identified below all claims or proceedings arising out of or related to this Agreement, including summary proceedings, will be brought before and subject to the exclusive jurisdiction of the following courts of competent jurisdiction:

Americas

Argentina: the Ordinary Commercial Court of the city of Buenos Aires;

Brazil: the court of Rio de Janeiro, RJ;

Chile: the Civil Courts of Justice of Santiago;

Ecuador: the civil judges of Quito for executory or summary proceedings (as applicable);

Mexico: the courts located in Mexico City, Federal District;

Peru: the judges and tribunals of the judicial district of Lima, Cercado;

Uruguay: the courts of the city of Montevideo;

Venezuela: the courts of the metropolitan area of the city of Caracas;

Europe, Middle East, and Africa

Austria: the court of law in Vienna, Austria (Inner-City);

Algeria, Andorra, Benin, Burkina Faso, Cameroon, Cape Verde, Central African Republic, Chad, Comoros, Congo Republic, Djibouti, Democratic Republic of Congo, Equatorial Guinea, France, French Guiana, French Polynesia, Gabon, Gambia, Guinea, Guinea-Bissau, Ivory Coast, Lebanon, Madagascar, Mali, Mauritania, Mauritius, Mayotte, Monaco, Morocco, New Caledonia, Niger, Reunion, Senegal, Seychelles, Togo, Tunisia, Vanuatu, and Wallis and Futuna: the Commercial Court of Paris;

Angola, Bahrain, Botswana, Burundi, Egypt, Eritrea, Ethiopia, Ghana, Jordan, Kenya, Kuwait, Liberia, Malawi, Malta, Mozambique, Nigeria, Oman, Pakistan, Qatar, Rwanda, Sao Tome and Principe, Saudi Arabia, Sierra Leone, Somalia, Tanzania, Uganda, United Arab Emirates, the United Kingdom, West Bank/Gaza, Yemen, Zambia, and Zimbabwe: the courts of England and Wales;

South Africa, Namibia, Lesotho, and Swaziland: the High Court in Johannesburg;

Greece: the competent court of Athens;

Israel: the courts of Tel Aviv-Jaffa;

Italy: the courts of Milan;

Portugal: the courts of Lisbon;

Spain: the courts of Madrid; and

Turkey: the Istanbul Central Courts and Execution Directorates of Istanbul, the Republic of Turkey

13.3 Arbitration The following paragraph is added as a new Subsection 13.3 (Arbitration) as it applies for those countries identified below. The provisions of this Subsection 13.3 prevail over those of Subsection 13.2 (Jurisdiction) to the extent permitted by the applicable governing law and rules of procedure:

Asia Pacific

A. In Cambodia, India, Laos, Philippines, and Vietnam:

Disputes arising out of or in connection with this Agreement will be finally settled by arbitration which will be held in Singapore in accordance with the Arbitration Rules of Singapore International Arbitration Center ("SIAC Rules") then in effect. The arbitration award will be final and binding for the parties without appeal and will be in writing and set forth the findings of fact and the conclusions of law.

The number of arbitrators will be three, with each side to the dispute being entitled to appoint one arbitrator. The two arbitrators appointed by the parties will appoint a third arbitrator who will act as chairman of the proceedings. Vacancies in the post of chairman will be filled by the president of the SIAC. Other vacancies will be filled by the respective nominating party. Proceedings will continue from the stage they were at when the vacancy occurred.

If one of the parties refuses or otherwise fails to appoint an arbitrator within 30 days of the date the other party appoints its, the first appointed arbitrator will be the sole arbitrator, provided that the arbitrator was validly and properly appointed.

All proceedings will be conducted, including all documents presented in such proceedings, in the English language. The English language version of this Agreement prevails over any other language version.

B. In the People's Republic of China:

In case no settlement can be reached, the disputes will be submitted to China International Economic and Trade Arbitration Commission for arbitration according to the then effective rules of the said Arbitration Commission. The arbitration will take place in Beijing and be conducted in Chinese. The arbitration award will be final and binding on both parties. During the course of arbitration, this agreement will continue to be performed except for the part which the parties are disputing and which is undergoing arbitration.

C. In Indonesia:

Each party will allow the other reasonable opportunity to comply before it claims that the other has not met its obligations under this Agreement. The parties will attempt in good faith to resolve all

disputes, disagreements, or claims between the parties relating to this Agreement. Unless otherwise required by applicable law without the possibility of contractual waiver or limitation, i) neither party will bring a legal action, regardless of form, arising out of or related to this Agreement or any transaction under it more than two years after the cause of action arose; and ii) after such time limit, any legal action arising out of this Agreement or any transaction under it and all respective rights related to any such action lapse.

Disputes arising out of or in connection with this Agreement shall be finally settled by arbitration that shall be held in Jakarta, Indonesia in accordance with the rules of Board of the Indonesian National Board of Arbitration (Badan Arbitrase Nasional Indonesia or "BANI") then in effect. The arbitration award shall be final and binding for the parties without appeal and shall be in writing and set forth the findings of fact and the conclusions of law.

The number of arbitrators shall be three, with each side to the dispute being entitled to appoint one arbitrator. The two arbitrators appointed by the parties shall appoint a third arbitrator who shall act as chairman of the proceedings. Vacancies in the post of chairman shall be filled by the chairman of the BANI. Other vacancies shall be filled by the respective nominating party. Proceedings shall continue from the stage they were at when the vacancy occurred.

If one of the parties refuses or otherwise fails to appoint an arbitrator within 30 days of the date the other party appoints its, the first appointed arbitrator shall be the sole arbitrator, provided that the arbitrator was validly and properly appointed.

All proceedings shall be conducted, including all documents presented in such proceedings, in the English and/or Indonesian language.

Europe, Middle East, And Africa

D. In Albania, Armenia, Azerbaijan, Belarus, Bosnia-Herzegovina, Bulgaria, Croatia, Former Yugoslav Republic of Macedonia, Georgia, Hungary, Kazakhstan, Kyrgyzstan, Moldova, Montenegro, Poland, Romania, Russia, Serbia, Slovakia, Tajikistan, Turkmenistan, Ukraine, and Uzbekistan:

All disputes arising out of this Agreement or related to its violation, termination or nullity will be finally settled under the Rules of Arbitration and Conciliation of the International Arbitral Center of the Federal Economic Chamber in Vienna (Vienna Rules) by three arbitrators appointed in accordance with these rules. The arbitration will be held in Vienna, Austria, and the official language of the proceedings will be English. The decision of the arbitrators will be final and binding upon both parties. Therefore, pursuant to paragraph 598 (2) of the Austrian Code of Civil Procedure, the parties expressly waive the application of paragraph 595 (1) figure 7 of the Code. JCI may, however, institute proceedings in a competent court in the country of installation.

E. In Estonia, Latvia, and Lithuania: All disputes arising in connection with this Agreement will be finally settled in arbitration that will be held in Helsinki, Finland in accordance with the arbitration laws of Finland then in effect. Each party will appoint one arbitrator. The arbitrators will then jointly appoint the chairman. If arbitrators cannot agree on the chairman, then the Central Chamber of Commerce in Helsinki will appoint the chairman.

Additional Country Specific Amendments

Canada

The following is added as a new Section 18:

For purposes of this Section 18, "Personal Data" refers to information relating to an identified or identifiable individual made available by one of the parties, its personnel or any other individual to the other in connection with this Agreement. The following provisions apply in the event that one party makes Personal Data available to the other:

a. General

- i. Each party is responsible for complying with any obligations applying to it under applicable Canadian data privacy laws and regulations ("Laws").
- ii. Neither party will request Personal Data beyond what is necessary to fulfill the purpose(s) for which it is requested. The purpose(s) for requesting Personal Data must be reasonable. Each party will agree in advance as to the type of Personal Data that is required to be made available.

b. Security Safeguards

- i. Each party acknowledges that it is solely responsible for determining and communicating to the other the appropriate technological, physical and organizational security measures required to protect Personal Data.
- ii. Each party will ensure that Personal Data is protected in accordance with the security safeguards communicated and agreed to by the other.
- iii. Each party will ensure that any third party to whom Personal Data is transferred is bound by the applicable terms of this section.
- iv. Additional or different services required to comply with the Laws will be deemed a request for new services.

c. Use

Each party agrees that Personal Data will only be used, accessed, managed, transferred, disclosed to third parties or otherwise processed to fulfill the purpose(s) for which it was made available.

d. Access Requests

- i. Each party agrees to reasonably cooperate with the other in connection with requests to access or amend Personal Data.
- ii. Each party agrees to reimburse the other for any reasonable charges incurred in providing each other assistance.
- iii. Each party agrees to amend Personal Data only upon receiving instructions to do so from the other party or its personnel.

e. Retention

Each party will promptly return to the other or destroy all Personal Data that is no longer necessary to fulfill the purpose(s) for which it was made available, unless otherwise instructed by the other or its personnel or required by law.

f. Public Bodies Who Are Subject to Public Sector Privacy Legislation

If you are a public body subject to public sector privacy legislation, this Section 18 applies only to Personal Data made available to you in connection with this Agreement, and the obligations in this section apply only to ** you **, except that: 1) section (b)(i) applies only to JCI; 2) sections (a)(i) and (d)(i) apply to both parties; and 3) section (d)(ii) and the last sentence in (a)(ii) do not apply.

Peru

9. Limitation of Liability

The following is added to the end of this Section 9 (Limitation of Liability):

Except as expressly required by law without the possibility of contractual waiver, you and JCI intend that the limitation of liability in this Section 9 (Limitation of Liability) applies to damages caused by all types of claims and causes of action. If any limitation on or exclusion from liability in this section is held by a court of competent jurisdiction to be unenforceable with respect to a particular claim or

cause of action, the parties intend that it nonetheless apply to the maximum extent permitted by applicable law to all other claims and causes of action. Additionally, in accordance with Article 1328 of the Peruvian Civil Code, the limitations and exclusions specified in this section will not apply to damages caused by JCI's willful misconduct ("dolo") or gross negligence ("culpa inexcusable").

United States of America

6. Fees; Taxes

The following is added to the end of Section 6 (Fees; Taxes)

For Software delivered electronically in the United States for which you claim a state sales and use tax exemption, you agree not to receive any tangible personal property (e.g., media and publications) associated with the electronic program. You agree to be responsible for any sales and use tax liabilities that may arise as a result of your subsequent redistribution of the Software after delivery by JCI.

14. General

The following is added to the end of Section 14 (General):

Each party waives any right to a jury trial in any proceeding arising out of or related to this Agreement.

Australia

6. Fees; Taxes

The following is added to the end of Section 6 (Fees; Taxes)

Notwithstanding the foregoing, if any government or authority imposes a duty, tax (other than income tax), levy, or fee, on this Agreement or on the Software itself, that is not otherwise provided for in the amount payable, you agree to pay it when JCI invoices you. If the rate of GST changes, you may adjust the charge or other amount payable to take into account that change from the date the change becomes effective.

7. Limited Warranty; Disclaimer

The following is added to the first paragraph of Section 7 (Limited Warranty; Disclaimer): Although JCI disclaims certain warranties, you may have certain rights under the Competition and Consumer Act 2010 or other legislation and are only limited to the extent permitted by the applicable legislation. If JCI is in breach of a condition or warranty implied by the Competition and Consumer Act 2010, JCI's liability is limited to the repair or replacement of the goods, or the supply of equivalent goods. Where that condition or warranty relates to right to sell, quiet possession or clear title, or the goods are of a kind ordinarily obtained for personal, domestic or household use or consumption, then none of the limitations in this paragraph apply.

Hong Kong Sar, Macau Sar, and Taiwan

For licenses obtained in Taiwan and the special administrative regions, phrases throughout this Agreement containing the word "country" (for example, "the country in which you entered into this Agreement") are replaced with the following:

- a. In **Hong Kong SAR**: "Hong Kong SAR"
- b. In **Macau SAR**: "Macau SAR" except in the Governing Law clause (Section 11.1)
- c. In **Taiwan**: "Taiwan."

India

14. General

The following is added to the end of Section 14 (General):

If no suit or other legal action is brought, within three years after the cause of action arose, in respect of any claim that either party may have against the other, the rights of the concerned party in respect of such claim will be forfeited and the other party will stand released from its obligations in respect of such claim.

Indonesia

5. Term and Termination

The following is added to the end of Section 5 (Term and Termination):

Both parties waive the provision of article 1266 of the Indonesian Civil Code, to the extent the article provision requires such court decree for the termination of an agreement creating mutual obligations.

Japan

14. General

The following is added to the end of Section 14 (General):

Any doubts concerning this Agreement will be initially resolved between us in good faith and in accordance with the principle of mutual trust.

Malaysia

7. Limited Warranty; Disclaimer

The word "SPECIAL" in Section 7 is deleted.

New Zealand

7. Limited Warranty; Disclaimer

The following is added to the first paragraph of Section 7 (Limited Warranty; Disclaimer): Although JCI disclaims certain warranties, you may have certain rights under the Consumer Guarantees Act 1993 or other legislation which cannot be excluded or limited. The Consumer Guarantees Act 1993 will not apply in respect of any goods which JCI provides, if you require the goods for the purposes of a business as defined in that Act.

9. Limitation of Liability

The following is added to Section 9 (Limitation of Liability):

Where the Software is not obtained for the purposes of a business as defined in the Consumer Guarantees Act 1993, the limitations in this Section are subject to the limitations in that Act.

People's Republic of China

6. Fees; Taxes

The following is added to the end of Section 6 (Fees; Taxes)

All banking charges incurred in the People's Republic of China will be borne by you and those incurred outside the People's Republic of China will be borne by JCI.

9. Limitation of Liability

The following is added to the end of Section 9 (Limitation of Liability)

nothing in these Terms shall exclude any liability of JCI: (i) for the death of or injury to any person; (ii) for damage to property caused by wilful misconduct and/or gross negligence of JCI; (iii) for fraud or

fraudulent misrepresentation; or (iv) for any matter which it would be illegal for JCI to exclude or limit or attempt to exclude or limit its liability under PRC law.

Philippines

9. Limitation of Liability

The following replaces the first sentence of Section 9 (Limitation of Liability):

TO THE MAXIMUM EXTENT PERMITTED BY LAW, IN NO EVENT SHALL JCI AND AFFILIATES AND THEIR RESPECTIVE ITS SUPPLIERS AND VENDORS BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY SPECIAL, (INCLUDING NOMINAL AND EXEMPLARY DAMAGES), INCIDENTAL, CONSEQUENTIAL, PUNITIVE, INDIRECT DAMAGES, MORAL, INCIDENTAL, OR INDIRECT DAMAGES OR FOR ANY ECONOMIC CONSEQUENTIAL DAMAGES WHICH SHALL INCLUDE, WITHOUT LIMITATION, DAMAGES FOR PERSONAL INJURY, LOST PROFITS, LOST DATA AND BUSINESS INTERRUPTION, ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE, EVEN IF THEY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Singapore

11. Data Collection and Use.

The following is added to the end of Section 11 (Data Collection and Use):

You have the right to request access to your personal information in the possession or under the control of JCI, and to request for corrections to be made on any errors in your personal information. Where possible, JCI will validate personal information provided using generally accepted practices and guidelines, for example, validating such personal information against pre-existing data held by JCI, or request to see supporting documentation before the personal information may be updated.

JCI will retain personal information we process on behalf of our customers for as long as needed to provide services to our customers. JCI may further retain and use this personal information as necessary to comply with our legal obligations, resolve disputes, maintain accurate accounting, financial and other operational records and enforce our agreements. You consent and authorize JCI to collect, use and retain information relating to your use of the Software and/or hardware in the manner set out above.

14. General

The following is added to the end of Section 14 (General):

Subject to the rights provided to JCI's suppliers and vendors provided in Section 9 (Limitation of Liability), a person who is not a party to this Agreement will have no right under the Contracts (Right of Third Parties) Act (Cap. 53B) to enforce any of its terms.

Taiwan

9. Limitation of Liability

The following is added to the end of Section 9 (Limitation of Liability):

To the extent required by applicable law, the words "AND THEIR RESPECTIVE SUPPLIERS AND VENDORS" are deleted.

European Union Member States

7. Limited Warranty; Disclaimer

The following is added to Section 7 (Limited Warranty; Disclaimer):

In the European Union ("EU"), consumers have legal rights under applicable national legislation governing the sale of consumer goods. Such rights are not affected by the provisions set out in this Section 7 (Limited Warranty; Disclaimer).

EU Member States And The Following Identified Countries

Iceland, Liechtenstein, Norway, Switzerland, Turkey, and any other European country that has enacted local data privacy or protection legislation similar to the EU model.

14. General

The following is added to the end of Section 14 (General): In the European Union ("EU"), consumers have legal rights under applicable national legislation governing the sale of consumer goods. Nothing in this Agreement shall in anyway whatsoever be intended to affect or in any way limit such rights, which remain in full force and effect.

A. Definitions – For the purposes of this Section 14 (General), the following additional definitions apply:

(1) **Business Contact Information** – business-related contact information disclosed by you to JCI, including names, job titles, business addresses, telephone numbers and email addresses of your employees and contractors. For Austria, Italy and Switzerland, Business Contact Information also includes information about you and your contractors as legal entities (for example, your revenue data and other transactional information).

(2) **Business Contact Personnel** – Your employees and contractors to whom the Business Contact Information related

(3) **Data Protection Authority** – The authority established by the Data Protection and Electronic Communications Legislation in the applicable country or, for non-EU countries, the authority responsible for supervising the protection of personal data in that country, or (for any of the foregoing) any duly appointed successor entity thereto.

(4) **Data Protection & Electronic Communications Legislation** – (i) the applicable local legislation and regulations in force implementing EU Directive 95/46/EC (on the protection of individuals with regard to the processing of personal data and on the free movement of such data) and of EU Directive 2002/58/EC (concerning the processing of personal data and the protection of privacy in the electronic communications sector), as amended or replaced from time to time (such as the General Data Protection Regulation, when and as applicable); or (ii) for non-EU countries, the legislation and/or regulations passed in the applicable country relating to the protection of personal data and the regulation of electronic communications involving personal data, including (for any of the foregoing) any statutory replacement or modification thereof.

JCI Group – Johnson Controls International, Plc, including Johnson Controls, Inc., its subsidiaries, and their respective Business Partners and subcontractors.

B. You authorize JCI:

(1) to process and use Business Contact Information within JCI Group in support of you and your business including the provision of support services, and for the purpose of furthering the business relationship between you and JCI Group, including, without limitation, contacting Business Contact Personnel (by email or otherwise) and marketing JCI Group products and services (the "Specified Purpose"); and

(2) to disclose Business Contact Information to other members of JCI Group in pursuit of the Specified Purpose only.

C. JCI agrees that all Business Contact Information will be processed in accordance with the Data Protection & Electronic Communications Legislation and will be used only for the Specified Purpose.

(1) To the extent required by the Data Protection & Electronic Communications Legislation, you represent that (a) you have obtained (or will obtain) any consents from (and has issued (or will issue) any notices to) the Business Contact Personnel as are necessary in order to enable JCI Group to process and use the Business Contact Information for the Specified Purpose.

(2) You authorize JCI to transfer Business Contact Information outside the European Economic Area, provided that the transfer is made on contractual terms approved by the Data Protection Authority or the transfer is otherwise permitted under the Data Protection & Electronic Communications Legislation.

Austria

9. Limitation of Liability

The following is added to the beginning of Section 9 (Limitation of Liability):

THE FOLLOWING LIMITATIONS AND EXCLUSIONS OF JCI'S LIABILITY DO NOT APPLY FOR DAMAGES CAUSED BY GROSS NEGLIGENCE OR WILLFUL MISCONDUCT. CIRCUMSTANCES MAY ARISE WHERE, BECAUSE OF A DEFAULT BY JCI IN THE PERFORMANCE OF ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHER LIABILITY, YOU ARE ENTITLED TO RECOVER DAMAGES FROM JCI.

The following is added to the end of Section 9 (Limitation of Liability):

THE LIMITATIONS AND EXCLUSIONS OF JCI'S LIABILITY DO NOT APPLY FOR DAMAGES CAUSED BY GROSS NEGLIGENCE OR WILLFUL MISCONDUCT.

The following words are deleted from Section 9 (Limitation of Liability): "(WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE)"

The following replaces the first sentence (second sentence after the above amendment) of Section 9 (Limitation of Liability):

"TO THE MAXIMUM EXTENT PERMITTED BY LAW, IN NO EVENT SHALL JCI AND AFFILIATES AND THEIR RESPECTIVE ITS SUPPLIERS AND VENDORS BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INDIRECT DAMAGES OR CONSEQUENTIAL DAMAGES, WHICH SHALL INCLUDE, WITHOUT LIMITATION, DAMAGES FOR PERSONAL INJURY, LOST PROFITS, LOST DATA AND BUSINESS INTERRUPTION, ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE, EVEN IF THEY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES."

Belgium, France and Luxembourg

9. Limitation of Liability

The following replaces the Section 9 (Limitation of Liability) in its entirety:

"EXCEPT AS OTHERWISE PROVIDED BY MANDATORY LAW, JCI'S ENTIRE LIABILITY FOR ALL CLAIMS IN THE AGGREGATE FOR ANY DAMAGES AND LOSSES THAT MAY ARISE AS A CONSEQUENCE OF THE FULFILLMENT OF ITS OBLIGATIONS UNDER OR IN CONNECTION WITH THIS AGREEMENT OR DUE TO ANY OTHER CAUSE RELATED TO THIS AGREEMENT IS LIMITED TO THE COMPENSATION OF ONLY THOSE DAMAGES AND LOSSES PROVED AND ACTUALLY ARISING AS AN IMMEDIATE AND DIRECT CONSEQUENCE OF THE NON-FULFILLMENT OF SUCH OBLIGATIONS (IF JCI IS AT FAULT) OR OF SUCH CAUSE, FOR A MAXIMUM OF EUR 500,000 (FIVE HUNDRED THOUSAND EURO). THE ABOVE LIMITATION WILL NOT APPLY TO DAMAGES FOR BODILY INJURIES (INCLUDING DEATH) AND DAMAGES TO REAL PROPERTY AND TANGIBLE PERSONAL PROPERTY FOR WHICH JCI IS LEGALLY LIABLE. UNDER NO CIRCUMSTANCES IS JCI OR ANY OF ITS SUPPLIERS OR VENDORS LIABLE FOR ANY OF THE FOLLOWING, EVEN IF INFORMED OF THEIR POSSIBILITY:

1) LOSS OF, OR DAMAGE TO, DATA; 2) INCIDENTAL, EXEMPLARY OR INDIRECT DAMAGES, OR FOR ANY ECONOMIC CONSEQUENTIAL DAMAGES; AND / OR 3) LOST PROFITS, BUSINESS, REVENUE, GOODWILL, OR ANTICIPATED SAVINGS, EVEN IF THEY ARISE AS AN IMMEDIATE CONSEQUENCE OF THE EVENT THAT GENERATED THE DAMAGES.

THE LIMITATION AND EXCLUSION OF LIABILITY HEREIN AGREED APPLIES NOT ONLY TO THE ACTIVITIES PERFORMED BY JCI BUT ALSO TO THE ACTIVITIES PERFORMED BY ITS SUPPLIERS AND VENDORS, AND REPRESENTS THE MAXIMUM AMOUNT FOR WHICH JCI AS WELL AS ITS SUPPLIERS AND VENDORS ARE COLLECTIVELY RESPONSIBLE.

France

6. Fee; Taxes

The following replaces the Section 6 (Fee; Taxes) in its entirety:

You will pay the fees, if any, associated with the Software. All amounts due hereunder shall be paid within thirty (30) days of the date of the invoice. Pursuant to article L. 441-6 of the French Commercial Code, late payment penalties as well as a fixed compensation for recovery costs of the amount of 40 Euros (forty Euros) are due in the event that the amounts due are paid after the due date, and this without the necessity of a reminder without prejudice to damages and other expenses that JCI has the right to claim. The late penalties due to, under the mentioned legislation, will be claimed by JCI at the rate equal to the interest rate applied by the European Central Bank to its most recent refinancing operation plus 10 percentage points.

All taxes, duties, fees and other governmental charges of any kind (including sales and use taxes, but excluding taxes based on the gross revenues or net income of JCI) that are imposed by or under the authority of any government or any political subdivision thereof on the fees for the Software shall be borne solely by you, unless you can evidence tax exemption and shall not be considered a part of a deduction from or an offset against such fees. If you lose tax exempt status, you will pay any taxes due as part of any renewal or payment.

You will promptly notify JCI if your tax status changes. You will pay all court costs, fees, expenses and reasonable attorneys' fees incurred by JCI in collecting delinquent fees.

11. Data Collection and Use

The following replaces the Section 11 (Data Collection and Use) in its entirety:

A. Definitions – For the purposes of this Section 11 (Data Collection and Use), the following additional definitions apply:

(1) **Data** – Data resulting from or otherwise relating to your use of the Software and/or hardware used in connection with the Software.

(2) **Data Protection Authority** – The authority established by the Data Protection and Electronic Communications Legislation in the applicable country or, for non-EU countries, the authority responsible for supervising the protection of personal data in that country, or (for any of the foregoing) any duly appointed successor entity thereto.

(3) **Data Protection & Electronic Communications Legislation** – (i) the applicable local legislation and regulations in force implementing the requirements of EU Directive 95/46/EC (on the protection of individuals with regard to the processing of personal data and on the free movement of such data) and of EU Directive 2002/58/EC (concerning the processing of personal data and the protection of privacy in the electronic communications sector), as amended or replaced from time to time; or (ii) for non-EU countries, the legislation and/or regulations passed in the applicable country relating to the protection of personal data and the regulation of electronic communications involving personal data, including (for any of the foregoing) any statutory replacement or modification thereof.

JCI Group – Johnson Controls International, Plc., including Johnson Controls, Inc., its subsidiaries, and their respective Business Partners and subcontractors.

B. You authorize JCI:

(1) to process and use your Data within JCI Group for purposes of providing you with service/product recommendations, benchmarking, energy monitoring, and maintenance and support (the "Specified Purpose");

(2) to disclose your Data to other members of JCI Group in pursuit of the Specified Purpose only;

(3) to de-identify your Data so that it does not identify you directly or by inference (the "De-Identified Data");

(4) to use the De-Identified Data for its business purposes, including improvement of the Software, research, product development, product improvement and provision of products and services to JCI's other customers (collectively, "JCI's Business Purposes");

(5) to use, copy, distribute, and otherwise exploit statistical and other data derived from your use of the De-Identified Data for JCI's Business Purposes.

C. JCI agrees that all Data will be processed in accordance with the Data Protection & Electronic Communications Legislation and will be used only for the Specified Purpose.

D. You authorize JCI to transfer Data outside the European Economic Area, provided that the transfer is made on contractual terms approved by the Data Protection Authority or the transfer is otherwise permitted under the Data Protection & Electronic Communications Legislation.

E. According to the Data Protection Act of January 6th, 1978, you have at any time, a right of access to and rectification of all of your personal data. If you wish to exercise this right and gain access to your personal data, please write to us via <https://www.johnsoncontrols.com/contact-us>. You may also oppose, for legitimate reasons, the processing of your personal data."

Italy

4. Metering devices

The following is added to Section 4 (Metering devices): The metering devices and passive restraints mentioned in this Section are those specified in the accompanying order document.

5. Term and termination

The following paragraph is deleted in its entirety from Section 5:

"In addition, either party may, in its sole discretion, elect to terminate this Agreement on written notice to the other party upon the bankruptcy or insolvency of the other party or upon the commencement of any voluntary or involuntary winding up, or upon the filing of any petition seeking the winding up of the other party."

The following wording is added to Section 5 (Term and termination): Without prejudice to the above, if no term is specified, either party shall have the right to terminate the Agreement at any time by giving the other Party a six months prior written notice.

11 Data Collection and Use

The following replaces the Section 11 (Data Collection and Use) in its entirety:

You acknowledge and agree the Software and/or hardware used in connection with the Software may collect data resulting from or otherwise relating to your use of the Software and/or hardware ("Data") for purposes of providing you with service/product recommendations, benchmarking, energy monitoring, and maintenance and support. JCI shall have the right and ability to use the De-Identified Data for its business purposes, including improvement of the Software, research, product

development, product improvement and provision of products and services to JCI's other customers (collectively, "JCI's Business Purposes"). JCI shall have the right to use the Data provided that: (i) the Data have been De-Identified by JCI, so that JCI does not identify You directly or by inference; the Data, as De-Identified, will be used in compliance with the applicable local legislation and regulations in force.

9. Limitation of Liability

The following replaces the Section 9 (Limitation of Liability) in its entirety:

"TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, JCI'S ENTIRE LIABILITY FOR ALL CLAIMS IN THE AGGREGATE FOR ANY DAMAGES AND LOSSES THAT MAY ARISE IN CONNECTION WITH THE FULFILLMENT OF ITS OBLIGATIONS UNDER OR IN CONNECTION WITH THIS AGREEMENT OR DUE TO ANY OTHER CAUSE RELATED TO THIS AGREEMENT IS LIMITED TO THE COMPENSATION OF ONLY THOSE DAMAGES AND LOSSES PROVED AND ACTUALLY ARISING AS AN IMMEDIATE AND DIRECT CONSEQUENCE OF THE NON-FULFILLMENT OF SUCH OBLIGATIONS (IF JCI IS AT FAULT) OR OF SUCH CAUSE, FOR A MAXIMUM OF EUR 500,000 (FIVE HUNDRED THOUSAND EURO). THE ABOVE LIMITATION WILL NOT APPLY TO DAMAGES FOR BODILY INJURIES (INCLUDING DEATH) AND DAMAGES TO REAL PROPERTY AND TANGIBLE PERSONAL PROPERTY FOR WHICH JCI IS LEGALLY LIABLE. SAVE IN CASE OF GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, UNDER NO CIRCUMSTANCES JCI OR ANY OF ITS SUPPLIERS OR VENDORS LIABLE FOR ANY OF THE FOLLOWING, EVEN IF INFORMED OF THEIR POSSIBILITY:

1) LOSS OF, OR DAMAGE TO, DATA; 2) INCIDENTAL, EXEMPLARY OR INDIRECT DAMAGES, OR FOR ANY ECONOMIC CONSEQUENTIAL DAMAGES; AND / OR 3) LOST PROFITS, BUSINESS, REVENUE, GOODWILL, OR ANTICIPATED SAVINGS, EVEN IF THEY ARISE AS AN IMMEDIATE CONSEQUENCE OF THE EVENT THAT GENERATED THE DAMAGES.

THE LIMITATION AND EXCLUSION OF LIABILITY HEREIN AGREED APPLIES NOT ONLY TO THE ACTIVITIES PERFORMED BY JCI BUT ALSO TO THE ACTIVITIES PERFORMED BY ITS SUPPLIERS AND VENDORS, AND REPRESENTS THE MAXIMUM AMOUNT FOR WHICH JCI AS WELL AS ITS SUPPLIERS AND VENDORS ARE COLLECTIVELY RESPONSIBLE.

Germany

9. Limitation of Liability

The following replaces the Section 9 (Limitation of Liability) in its entirety:

1. JCI WILL BE LIABLE WITHOUT LIMIT FOR 1) LOSS OR DAMAGE CAUSED BY A BREACH OF AN EXPRESS GUARANTEE; 2) DAMAGES OR LOSSES RESULTING IN BODILY INJURY (INCLUDING DEATH); 3) DAMAGES CAUSED INTENTIONALLY OR BY GROSS NEGLIGENCE; AND 4) claims pursuant to the German Product Liability Act (Produkthaftungsgesetz, ProdHaftG)..

2. IN THE EVENT OF LOSS, DAMAGE AND FRUSTRATED EXPENDITURES CAUSED BY SLIGHT NEGLIGENCE OR IN BREACH OF ESSENTIAL CONTRACTUAL OBLIGATIONS (I.E. an obligation which must be fulfilled to enable a due performance of the AGREEMENT and on whose fulfilment YOU generally rely and may rely ON), JCI WILL BE LIABLE, REGARDLESS OF THE BASIS ON WHICH YOU ARE ENTITLED TO CLAIM DAMAGES FROM JCI (INCLUDING FUNDAMENTAL BREACH, NEGLIGENCE, MISREPRESENTATION, OR OTHER CONTRACT OR TORT CLAIM), PER CLAIM ONLY UP TO 500,000 EURO FOR THE PROGRAM THAT CAUSED THE LOSS OR DAMAGE. A NUMBER OF DEFAULTS WHICH TOGETHER RESULT IN, OR CONTRIBUTE TO, SUBSTANTIALLY THE SAME LOSS OR DAMAGE WILL BE TREATED AS ONE DEFAULT.

3. IN THE EVENT OF LOSS, DAMAGE AND FRUSTRATED EXPENDITURES CAUSED BY SLIGHT NEGLIGENCE, JCI WILL NOT BE LIABLE FOR INDIRECT OR CONSEQUENTIAL DAMAGES, EVEN IF JCI WAS INFORMED ABOUT THE POSSIBILITY OF SUCH LOSS OR DAMAGE. THIS LIMITATION SHALL NOT APPLY WHERE THE LOSS, DAMAGE AND FRUSTRATED EXPENDITURES WAS CAUSED BY A SLIGHT NEGLIGENT BREACH OF ESSENTIAL CONTRACTUAL OBLIGATIONS.

4. IN CASE OF DELAY ON JCI'S PART: 1) JCI WILL PAY TO YOU AN AMOUNT NOT EXCEEDING THE LOSS OR DAMAGE CAUSED BY JCI'S DELAY AND 2) JCI WILL BE LIABLE ONLY IN RESPECT OF THE RESULTING DAMAGES THAT YOU SUFFER, SUBJECT TO THE PROVISIONS OF ITEMS A AND B ABOVE.

14. General

The following is added to the end of Section 14 (General):

Any claims resulting from this Agreement are subject to a limitation period of three years, except as stated in Section 7 (Limited Warranty; Disclaimer) of this Agreement.

Ireland

7. Limited Warranty; Disclaimer

The following is added to Section 7 (Limited Warranty; Disclaimer):

Except as expressly provided in these terms and conditions, or Section 12 of the Sale of Goods Act 1893 as amended by the Sale of Goods and Supply of Services Act, 1980 (the "1980 Act"), all conditions or warranties (express or implied, statutory or otherwise) are hereby excluded including, without limitation, any warranties implied by the Sale of Goods Act 1893 as amended by the 1980 Act (including, for the avoidance of doubt, Section 39 of the 1980 Act).

United Kingdom

Agreement Structure

The following sentence is added:

Nothing in this paragraph shall be interpreted or construed as excluding or limiting the liability of any person for fraud or fraudulent misrepresentation.

2. Restrictions

The following is added at the end of point (iii):

(if it is necessary for You to decompile the Software, to obtain the information necessary to create an independent program which can be operated with the Software, You will inform JCI that this is the case and will allow JCI a reasonable opportunity to provide such information to You so that it is no longer necessary for You to carry out that decompilation)

9. Limitation of Liability

The following replaces the Section 9 (Limitation of Liability) in its entirety:

FOR THE PURPOSES OF THIS SECTION, A "DEFAULT" MEANS ANY ACT, STATEMENT, OMISSION OR NEGLIGENCE ON THE PART OF JCI IN CONNECTION WITH, OR IN RELATION TO, THE SUBJECT MATTER OF AN AGREEMENT IN RESPECT OF WHICH JCI IS LEGALLY LIABLE TO YOU, WHETHER IN CONTRACT OR IN TORT. A NUMBER OF DEFAULTS WHICH TOGETHER RESULT IN, OR CONTRIBUTE TO, SUBSTANTIALLY THE SAME LOSS OR DAMAGE WILL BE TREATED AS ONE DEFAULT. TO THE MAXIMUM EXTENT PERMITTED BY LAW, IN NO EVENT SHALL JCI AND AFFILIATES AND THEIR RESPECTIVE ITS SUPPLIERS AND VENDORS BE LIABLE TO YOU OR ANY THIRD PARTY

FOR ANY SPECIAL, CONSEQUENTIAL, OR INDIRECT DAMAGES; OR WASTED MANAGEMENT TIME OR LOST PROFITS, BUSINESS, REVENUE, GOODWILL, OR ANTICIPATED SAVINGS, WHICH SHALL INCLUDE, WITHOUT LIMITATION, DAMAGES FOR LOST PROFITS, LOST DATA AND BUSINESS INTERRUPTION, ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE, EVEN IF THEY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.. CIRCUMSTANCES MAY ARISE WHERE, BECAUSE OF A DEFAULT BY JCI IN THE PERFORMANCE OF ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHER LIABILITY, YOU ARE ENTITLED TO RECOVER DAMAGES FROM JCI. REGARDLESS OF THE BASIS ON WHICH YOU ARE ENTITLED TO CLAIM DAMAGES FROM JCI AND EXCEPT AS EXPRESSLY REQUIRED BY LAW WITHOUT THE POSSIBILITY OF CONTRACTUAL WAIVER, JCI'S ENTIRE LIABILITY FOR ANY ONE DEFAULT WILL NOT EXCEED THE AMOUNT OF ANY DIRECT DAMAGES, TO THE EXTENT ACTUALLY SUFFERED BY YOU AS AN IMMEDIATE AND DIRECT CONSEQUENCE OF THE DEFAULT, UP TO 500,000 EURO (OR THE EQUIVALENT IN THEN-PREVAILING LOCAL CURRENCY) FOR THE PROGRAM THAT IS THE SUBJECT OF THE CLAIM.

NOTWITHSTANDING THE ABOVE, NOTHING IN THIS AGREEMENT WILL OPERATE TO EXCLUDE OR RESTRICT A PARTY'S LIABILITY (IF ANY) TO THE OTHER: (i) FOR DEATH OR PERSONAL INJURY; (ii) FOR FRAUD OR FRAUDULENT MISREPRESENTATION; (iii) FOR BREACH OF ITS OBLIGATIONS ARISING UNDER SECTION 12 SALE OF GOODS ACT 1979; (iii) FOR BREACH OF ITS OBLIGATIONS ARISING UNDER SECTION 2 SUPPLY OF GOODS AND SERVICES ACT 1982; (iv) FOR BREACH OF ITS OBLIGATIONS ARISING UNDER SECTION 8 SUPPLY OF GOODS (IMPLIED TERMS) ACT 1973; OR (v) FOR ANY MATTER FOR WHICH IT IS NOT PERMITTED BY LAW TO EXCLUDE OR LIMIT, OR TO ATTEMPT TO EXCLUDE OR LIMIT, ITS LIABILITY.

Additional Country Specific Amendments

Spain

7. Limited Warranty; Disclaimer

Section 7 (limited warranty; disclaimer) is replaced with the following:

JCI warrants that (i) for a period of thirty (30) days from delivery initial delivery to you (the "Warranty Period"), the Software will operate in substantial conformity with its Documentation; and (ii) it shall use screening software to scan the Software prior to delivery for viruses, Trojan horses, and other malicious code. If, during the Warranty Period, you notify JCI of any non-compliance with the foregoing warranties, JCI will, in its discretion: (a) use commercially reasonable efforts to provide the programming services necessary to correct any verifiable non-compliance with the foregoing warranties; or (b) replace any non-conforming Software; or if neither of foregoing options is reasonably available to JCI, (c) terminate this Agreement in whole or in part, and refund to You the fees, if any, paid for the non-conforming Software (less depreciation calculated on a three (3)-year straight-line basis commencing on the date of initial delivery to you. JCI shall not be liable for failures caused by third party hardware and software (including your own systems), misuse of the Software, or your negligence or willful misconduct. EXCEPT AS PROVIDED IN THIS SECTION, THE SOFTWARE IS PROVIDED ON AN "AS AVAILABLE," "AS IS" BASIS. THIS WITHOUT PREJUDICE THAT JCI WILL BE LIABLE FOR ANY HIDDEN FAULTS OF THE PRODUCTS PROVIDED, AS WELL AS ANY DAMAGES ARISED AS A RESULT OF PROVIDING A PRODUCT THAT DO NOT CONFORM WITH JCI'S DESCRIPTION, AND/OR THAT IT IS USELESS FOR THE PURPOSES OF THIS AGREEMENT. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JCI AND ITS AFFILIATES, AND THEIR RESPECTIVE SUPPLIERS AND VENDORS DISCLAIM ALL OTHER WARRANTIES WITH RESPECT TO THE SOFTWARE, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, TITLE, MERCHANTABILITY, QUIET ENJOYMENT, QUALITY OF INFORMATION, AND FITNESS FOR A PARTICULAR PURPOSE. JCI AND AFFILIATES AND THEIR RESPECTIVE

ITS SUPPLIERS AND VENDORS DO NOT WARRANT THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS, OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE SOFTWARE WILL BE CORRECTED. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY JCI OR ANY OF ITS PERSONNEL OR AGENTS SHALL CREATE ANY ADDITIONAL JCI WARRANTIES OR IN ANY WAY INCREASE THE SCOPE OF JCI'S OBLIGATIONS HEREUNDER.

9. Limitation of liability

The following is added to the end of this section 9 (limitation of liability):

NOTHING IN THIS AGREEMENT SHALL EXCLUDE OR LIMIT EITHER PARTY'S LIABILITY FOR: (I) DEATH OR PERSONAL INJURY CAUSED BY NEGLIGENCE; (II) FRAUD OR DECEIT; (III) WILLFULLY COSTS DAMAGES OR (IV) ANY OTHER LIABILITY THAT CANNOT BE EXCLUDED BY APPLICABLE LAW.

11. Data Collection and Use

Section 11 (data collection and use) is modified in the following terms:

You acknowledge and agree that the Software and/or hardware used in connection with the Software may collect data resulting from or otherwise relating to your use of the Software and/or hardware ("Data"). You hereby agree that your Data will be incorporated into a data file controlled by JCI, for the purposes of providing you with service/product recommendations, benchmarking, energy monitoring, maintenance and support, as well as for any purposes related to the execution of this agreement. You may exercise your rights of access, rectification, cancellation and opposition by writing to JCI corporate address stated above, or by contacting us at <https://www.johnsoncontrols.com/contact-us>, accompanying the request with a copy of an official identifying document. JCI shall be the exclusive owner of all Data. JCI shall have the right to de-identify your Data so that it does not identify you directly or by inference (the "De-Identified Data"). JCI shall have the right and ability to use the De-Identified Data for its business purposes, including improvement of the Software, research, product development, product improvement and provision of products and services to JCI's other customers (collectively, "JCI's Business Purposes").

© 2023 Johnson Controls. All rights reserved.

JOHNSON CONTROLS, TYCO and ILLUSTRATE are trademarks and/or registered trademarks.

Unauthorized use is strictly prohibited.