ILLUSTRA IQ

Release Notes

Illustra Flex Gen 4 Dual sensor Dome Series Cameras

Product code	Model Name	Firmware
FS10-M10-OIA4	llustra Flex4 10MP Dual sensor	Illustra.SS022.06.03.01.0010
IFS10-M10-OTA4	llustra Flex4 10MP Dual sensor	Illustra.SS022.06.03.01.0010
IFS16-M10-OIA4	llustra Flex4 16MP Dual sensor	Illustra.SS022.06.03.01.0010

Product Data
Visit the IP Cameras section of our web site, www.illustracameras.com, to download datasheets and other documentation in PDF format.

November 2023

Note
In case of discrepancy, the information in this document supersedes the information in any document referenced herein.

A163821KC9_A

Johnson Controls

Table of Contents

What's in This Release

What's New

Firmware Illustra.SS022.06.03.01.0010
Introduces the new Flex Gen4 Dual sensor Dome camera models:

Product Code	Model Name	Description
IFS10-M10-OIA4	Illustra Flex4 10MP Dual sensor	Illustra Flex 10MP Dual Sensor, indoor/outdoor, clear bubble, white, TDN w/IR, TWDR
IFS10-M10-OTA4	Illustra Flex4 10MP Dual sensor	Illustra Flex 10MP Dual Sensor, indoor/outdoor, clear bubble, white, TDN, TWDR
IFS16-M10-OIA4	Illustra Flex4 16MP Dual sensor	Illustra Flex 16MP Dual Sensor, indoor/outdoor, clear bubble, white, TDN w/IR, TWDR

Features

- Two cameras, one IP address
- Up to 2 SD Cards can be installed (one per sensor)
- High resolution, 10 to 16 megapixels Dual sensor (2 x 5MP/8MP cameras), Multiple IP streams of H.264, H.264IntelliZip, H.265, H.265IntelliZip and MJPEG video
- Power over Ethernet (PoE) or AC powered
- Dual power failover maximizes camera uptime
- Support for up to five Regions of Interest per sensor
- AI Object classification, Motion Detection and Blur Detection support on camera
- Edge Eventing with RTP meta-data streaming
- Outstanding color reproduction
- Ultra-low light capabilities to maintain color image quality without
- Auto & Manual White Balance Modes
- Smart WDR, TWDR
- Manual Focus and Zoom Control with One touch Focus
- Profile settings allow the mini dome to adapt to scenarios such as retail, gaming, and more
- Support for up to ten Privacy Zones per sensor
- Support for FTP, SNMP, SMTP, CIFS, 8021.x and Firewall filtering
- Offline recording to SD card
- SD card event download
- SD card event buffering (requires micro-SD or SD-HC card)
- Encrypted SD card feature
- Expanded Browser Support: Edge, Chrome, Firefox, Safari
- No dependencies on 3rd Party Utilities for Camera Setup (No QuickTime and Java requirements)
- UPnP Discovery
- Cloudvue Integration
- SIP call support
- TrickleStor integration with VENVR, Exacq
- Enhanced Security spec compliant 2.4
- Enhanced Security Feature Provides: One-Click Security Hardening, User Access Log, Validates Complex Credentials, Disables Unused Protocols
- Crypto Authentication Device for key management and Encryption functionality
- Secure boot, which ensures the camera will not boot if software has tampered with in any way
- Integration with VideoEdge NVR, VideoEdge Hybrid, victor Unified Client, ExacqVision recorders and Clients
- Integration with Illustra Connect v 3.2 and above
- Illustra API v3.4.4
- Network Quality of Service control
- Network Traffic control

Firmware Upgrade

The Illustra Flex Camera can be upgraded through the camera web GUI or by using Illustra Connect.

Upgrade Camera Firmware through the Web GUI

NOTE: All camera settings are maintained after you upgrade the camera firmware. It is recommended to clear your browser cache after a firmware upgrade.

Procedure: Upgrade Camera Firmware through the Web GUI

1. Using a supported internet browser connect to the camera via the IP Address and login to the Web GUI.
2. Select **Setup** from the web banner to access the setup menus.
3. Select **Maintenance** from the **System** menu and identify the **Camera Upgrade** section.
4. Select **Browse**. The Choose file dialog displays.
5. Navigate to the location where the firmware file has been saved. Select the firmware file then select the **Open** button.
6. Select **Upload**. The file transfer begins, and a progress bar displays.

Upgrade Camera Firmware through Illustra Connect

NOTE: All camera settings are maintained after you upgrade the camera firmware.

Procedure: Update Camera Firmware through Illustra Connect

1. Install and launch the Illustra Connect software utility.
2. From the displayed list of cameras; right-click on the camera requiring the software upgrade.
3. Select **Upgrade Firmware**. The Firmware Upload window will display.
4. Select **Choose File** and browse to the firmware upgrade file.
5. Select **Upgrade** to start the upgrade.

Features

Accessing the Illustra Flex Series Camera Web User Interface for the first time

1. Select a supported browser and navigate to the camera IP address.
2. When you select the camera, the sign in page is displayed.
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 is displayed. The first time that you access the camera, or after a factory reset, you are prompted to **Define a Host ID** and **Select a Security Type**.
   Define a Host ID: The admin user must enter a 6-character code for the Host ID that includes both letters and/or numbers. This unique password is used to access the operating system files. The HostID is not stored on the camera for security reasons and must be presented to Illustra Technical Support when remote access to the operating system is required.
   Select a Security Type: Standard Security or Enhanced Security. If you are keeping Standard Security, default admin password change is **enforced**.
6. Optional - If you select the Enhanced Security option, you are required and instructed to change the username and create a complex password.

See below for further information on Security configuration.

Enhanced Security

The Enhanced Security feature intends to advance the security of the Illustra cameras by enforcing security best practices and adding features to allow the installer and end-users to customize the camera's security to meet their controls.

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**.

- The **End User License Agreement** displays. Select the **Accept** button to continue.
- **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.

Security Modes Summary

Standard Security

1. Default admin password change is enforced.
2. Changes to communication protocols is available to all users with appropriate privileges.
3. Password's complexity is set to require minimum of any 5 characters (admin cannot be used).
4. Authentication Method is set to basic by default.

Enhanced Security

1. Unsecure Protocols are disabled by default until enabled by a user.
2. Discovery Protocols are disabled by default until enabled by a user.
3. Changes in the protocols will only be available to a user with administrative privileges and require that user to re-enter their password.
4. Default admin username & password change is enforced.
5. Usernames for all accounts must meet the Username Password Complexity Requirements, which are detailed below.
6. Passwords for all accounts must meet the Password Complexity Requirements, which are detailed below.
7. AUTHENTICATION OF VIDEO STREAM, INCLUDING DISABLING VIDEO OVER HTTP.
8. Authentication Method is set to HTTPS Digest by default (HTTP disabled).

Note: When applying Enhanced security all these changes will be done automatically, but if changing from Enhanced to Standard the settings will not be changed automatically – to reset to standard profile user will need to do changes manually or factory reset camera and select standard Security when prompted.

Username and Password Complexity Requirements

Username Complexity for Enhanced Security Mode:

a. Minimum characters: 5

Password Complexity for Enhanced Security Mode:

a. Minimum characters: 8
b. Have least one character from each of the following character groups:
   i. upper case letters ABCDEFGHIJKLMNOPQRSTUVWXYZ
   ii. lower case letters abcdefghijklmnopqrstuvwxyz
   iii. numeric characters 0123456789
   iv. Special characters @ % + \ / ‘ ! # $ ^ ? : , ( ) { } [ ] ~ - _ `
c. The password cannot contain the username.

Default admin/admin & Automatic prompt for username and password change at first login

The admin/admin user is hardcoded until security mode is selected on first login.

For Standard Security

Password change is mandatory after first login.

New Password should be a minimum of five characters long.

New Password cannot be admin.

For Enhanced Security

When selected, a pop up is visible requiring you to change your username and password.

• **A username & password change is mandatory** – Note: If the user sets a new username and password – admin/admin is automatically replaced.

• Certain criteria apply to both the username and password (See Username and Password complexity).

NOTE:

When Enhanced Security is enabled the user is prompted to change the username and password from the default admin/admin. If not, all rules are applied then the change request is denied and credentials remain as admin/admin. Failure to comply by rules, intermittently may result in cam- era log in being unavailable for a few minutes to allow camera to restore default functionality.

How to restore admin/admin:

1. Restore factory default camera.

Changes in Enhanced security profile

When changing security to ‘enhanced’, the camera performs the following changes:

- Admin/admin password automatically replaced by new Enhanced username/password.
- Change from basic to Digest HTTPS authentication.
- Enables RTSP authentication and disables Video over HTTP.
- Disables all ONVIF discovery capabilities.
- Disables UPnP Discovery protocol.
- Disables Exacq Audio Ports.
- Sets Secure connection for Metadata streaming

Note: When applying Enhanced security all these changes will be done automatically, but if changing from Enhanced to Standard the settings will not be changed automatically – to reset to standard profile user will need to do changes manually or factory reset camera and select standard Security when prompted.

The Lens Calibration Advisory pop-up is now visible:

Note: Before you perform a lens calibration, ensure that all packaging, including the bubble packaging is removed.

a. Select **No (Skip)** to skip a lens calibration.
OR
a. Select **Yes (Start Calibration)** to begin the lens calibration.

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

DHCP

- On initial camera start up, and after a hardware factory reset, DHCP is enabled by default and it remains enabled until the camera receives either a DHCP address or is assigned a Static IP address.
- If no connection is made to a DHCP server within two minutes, the camera will go to default IP address 192.168.1.168, but will continue to search for a DHCP address.
- If the camera is assigned a Static IP address prior to DHCP being enabled, the camera first reboots for approximately 2 minutes, and then remains accessible at its Static IP until a connection is made to a DHCP server.

UPnP feature

UPnP (Universal Plug and Play) broadcasts information about the camera to other devices on the network. The UPnP uses the Windows Network apps to discover the devices in the network that you are connected to.
The information broadcasts about the camera are:

- Device Name: <Product Code>-<Serial Number>
- Manufacturer and manufacturer URL
- Model (product code) and model URL (same as manufacturer URL)
- Device webpage (camera homepage)
- Serial number
- MAC address
- Unique Identifier: uuid<unique id for that camera type>-<serial number
- IP address

Note: The information broadcast on Windows XP is slightly different from the above.

Unsupported Key UPnP Functions: Video streaming, Audio streaming.

Analytics

	Motion Detection Events	Motion Detection Metadata	AI Object Classification Alerts	AI Object Classification Metadata	Tamper and Blur Detection Events
Illustra Flex4 10MP Dual sensor	Yes	Yes	Yes	Yes	Yes
Illustra Flex4 10MP Dual sensor	Yes	Yes	Yes	Yes	Yes
Illustra Flex4 16MP Dual sensor	Yes	Yes	Yes	Yes	Yes

AI Object Classification

- The camera supports the configuration of AI Object Classification. You can define the AI Object Classification settings that can be used to set-up Analytic Rules
- You can add up to 10 Analytic Rules by default on the camera web user interface. An alarm is generated each time an event is triggered
- For detailed information about configuring each rule, please refer to the user manual
- It is recommended to configure AI Object Classification rules on the camera before adding the camera to a VENVR
- After enabling Video Intelligence on a camera that is already on a VENVR, it is necessary to restart the NVR services in order for the new configuration to be recognized by the NVR. To restart the NVR services, select Advanced, then select Shutdown, and then select Restart NVR Services.

Multicast

Multicast streaming is a one-to-many relationship between a camera and the clients receiving the stream. With a multicast stream, the server streams to a multicast IP address on the network, and clients receive the stream by subscribing to the IP address.
User can configure the Multicast via camera GUI or iAPI, on VideoEdge Camera configuration. The feature was released specifically to integrate with VideoEdge 5.1 Failover.

VENVR TrickleStor Integration / Offline Record Settings

When you configure the Offline Record Settings feature and once it detects a loss of connection with the recorder, it sends the video stream to the SD card within the unit. This satisfies the loss of video and continues recording.
Once the recorder is back online the camera initiates sending recorded video from the SD card to the recorder. The maximum time recording during the outage depends on the SD card and the recorded stream you selected. If the SD reaches full capacity, it deletes video from earliest recording to latest recording. This feature integrates with the VE NVR 5.0 and above. At present this feature is limited to only support Codec: H264 and H264+ Intellizip.
Note: TrickleStor integration is not supported under HTTPS connection, please use “both” and HTTP only when integrating with this feature.

Enhanced security & DIO (alarm in & alarm out) and Edge Analytics Alarm & Metadata Stream

Camera Firmware will automatically set Stream Metadata Transport to Secure HTTPS streaming when Enhanced Security is selected.

Some recent Integration can support this configuration and will provide a full secure connection including the metadata streams, other integration, while camera is in Enhanced Security Mode still require the user to manually enable “Video over HTTP” in GUI: Setup/ Security/Remote Access or Manage the Video over HTTP setting Via GUI Setup/Security Status page. Information should be available on Integration’s documentation.

Picture Profiles

Profile settings allow the mini dome to adapt to scenarios such as retail, gaming, and more with a simple drop down selection. Picture profiles are described below:

Picture Profile behaviour:

- Demo Mode VBR Highest is the default out of the box (or after a factory reset)
- Exposure default buttons will Default Exposure profile to Auto (it will not apply any bitrate changes)
- Demo mode will only revert to VBR Highest on a Factory reset.
- Demo mode to other values will change the bitrate to CVBR Max Bitrate 8000
- Other to Demo will not change the bitrate under any circumstance
- Other to Other will not change the bitrate under any circumstance

Demo

- Bitrate controller VBR
- Quality highest
- Set max exposure and min exposure allowed
- Set max gain value allowed
- Auto exposure selects shutter speed (between min and max exposure values) and gain (between 0db and max gain selection) to adjust exposure if light level or scene changes
- Use case: Out of the box configuration for optimal video and image quality

Auto

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 8000
- Set max gain allowed
- Set max exposure allowed
- Set min exposure allowed
- Auto Exposure selects shutter speed (between min and max exposure values), gain (between 0db and max gain selection) and iris position to adjust exposure if light level or scene changes
- Use case: General use

Shutter Priority

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 8000
- Set any shutter speed
- Set max gain value allowed
- Auto Exposure selects gain (between 0db and max gain selection) and iris position to adjust exposure if light level or scene changes
- Use case: Typically for use in scenes with motion, e.g., overlooking traffic. Caution: The illumination required for this configuration would need to be quite consistent.

Iris-Priority

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 8000
- Set any iris position
- Set Max exposure and Min exposure allowed
- Set max gain value allowed
- Auto Exposure selects shutter speed (between min and max exposure values) and gain (between 0db and max gain selection) to adjust exposure if light level or scene changes
- Use case: To select a required depth of focus. Selecting a high iris value will give a larger depth of focus so that objects close to and far from the camera can be in focus at the same time.

Caution: With a high iris value the camera is not able to produce a bright image in very low light levels

Gaming

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 8000
- Set Stream 1 Framerate to 30 (if lower than)
- Set max gain value allowed
- Set min exposure allowed
- Set max exposure no slower than 1/30s (NTSC/60Hz) or 1/25s (PAL/50Hz)
- Use case: Casinos or other situations where Frame Rate must be no slower than 30fps (NTSC/60Hz) or 25fps (PAL/50Hz)

Indoor

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 8000
- Set max gain allowed
- Set max exposure allowed
- Set min exposure allowed
- Auto Exposure selects shutter speed (between min and max exposure values), gain (between 0db and max gain selection) and iris position to adjust exposure if light level or scene changes
- Use case: Office environment where light levels can change quickly

Outdoor

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 8000
- Set max gain allowed
- Set max exposure allowed
- Set min exposure allowed
- Auto Exposure selects shutter speed (between min and max exposure values), gain (between 0db and max gain selection) and iris position to adjust exposure if light level or scene changes
- Iris operation tailored to give larger depth of focus if conditions are bright enough
- Use case: Outdoor operation with or without IR illumination enabled

License Plate Recognition (LPR) low, mid and high

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 8000Set max gain value allowed
- Set min exposure allowed
- Low vs mid vs high, set slower or faster max exposure values
- Auto exposure selects iris position, shutter speed and gain to adjust exposure if light level or scene changes
- Use case: License Plate Recognition such as parking garages or other moving vehicle scenario where a fast shutter speed must be maintained to give sharper images, while the vehicle or object is moving, to help License Plate Recognition software.

Manual

- Set camera Bitrate controller to CVBR
- Set Max Bitrate to 8000
- Set any shutter speed, gain value and iris position
- Fixed exposure
- Does not auto adjust if light level or scene changes
- Use case: Fixed conditions where illumination and scene will not change. If the lighting or scene changes the apparent brightness of the image will change.

Stream Tables – 10MP Normal Mode

		Normal Mode				
		Resolution	Description	Max FPS		
				TWDR Off	TWDR 2x	TWDR 3x
Stream 1	H.264, H.265, H.264+ H.265+ MJPEG	2560 x 1920 2560 x 1440*1 1920 x 1080 1664 x 936 1280 x 720	4:3 16:9 (1080p) 16:9 (HD+) 16:9 (720p) 16:9	30 30 60 60 60	25 25 25 25 25	15 15 15 15 15
Stream 2	H.264, H.265, H.264+ H.265+ MJPEG	1280 x 720 1024 x 576 800 x 600 816 x 464 640 x 480 640 x 360 480 x 272	(720p) 16:9 (PAL+) 16:9 (SVGA) 4:3 16:9 (VGA) 4:3 (nHD) 16:9 16:9	30 30 30 30 30 30 30	25 25 25 25 25 25 25	15 15 15 15 15 15 15
Stream 3	MJPEG	800x448	16:9	7	7	7

Note: *1 The default resolution of stream 1 will be 2560x1440.
Note: A maximum of 5 concurrent streams are supported by each camera, this includes shared streams.
Note: Enabling TWDR will restrict the frame rate of Stream 1 and Stream 2 to 25 FPS for any resolution.

Stream Tables – 10MP Corridor Mode

		Corridor Mode				
		Resolution	Description	Max FPS		
				TWDR Off	TWDR 2x	TWDR 3x
Stream 1	H.264, H.265, H.264+ H.265+ MJPEG	2560 x 1920 2560 x 1440*1 1920 x 1080 1664 x 936 1280 x 720	4:3 16:9 (1080p) 16:9 (HD+) 16:9 (720p) 16:9	30 30 30 30 30	25 25 25 25 25	15 15 15 15 15
Stream 2	H.264, H.265, H.264+ H.265+ MJPEG	1280 x 720 1024 x 576 800 x 600 816 x 464 640 x 480 640 x 360 480 x 272	(720p) 16:9 (PAL+) 16:9 (SVGA) 4:3 16:9 (VGA) 4:3 (nHD) 16:9 16:9	30 30 30 30 30 30 30	25 25 25 25 25 25 25	15 15 15 15 15 15 15
Stream 3	MJPEG	800x448	16:9	7	7	7

Note: *1 The default resolution of stream 1 will be 2560x1440.
Note: A maximum of 5 concurrent streams are supported by each camera, this includes shared streams.
Note: Enabling TWDR will restrict the frame rate of Stream 1 and Stream 2 to 25 FPS for any resolution.

Stream Tables – 16MP Normal Mode

		Normal Mode				
		Resolution	Description	Max FPS		
				TWDR Off	TWDR 2x	TWDR 3x
Stream 1	H.264, H.265, H.264+ H.265+	3840 x 2160 3264 x 1840 2688 x 1520	(4K) 16:9 16:9 16:9	15 15 15	15 15 15	15 15 15
	H.264, H.265, H.264+ H.265+ MJPEG	1920 x 1080 1664 x 936 1280 x 720	(1080p) 16:9 (HD+) 16:9 (720p) 16:9	60 60 60	25 25 25	15 15 15
Stream 2	H.264, H.265, H.264+ H.265+ MJPEG	1280 x 720 1024 x 576 960 x 544 816 x 464 640 x 360 480 x 272	(720p) 16:9 (PAL+) 16:9 (qHD) 16:9 16:9 (nHD) 16:9 16:9	30*1 30*1 30*1 30*1 30*1 30*1	25*1 25*1 25*1 25*1 25*1 25*1	15 15 15 15 15 15
Stream 3	MJPEG	800x448	16:9	7	7	7

Note: *1 Stream 2 is restricted to 15 FPS when Stream 1 resolution is greater than 1920x1080.
Note: Enabling TWDR will restrict the frame rate of Stream 1 and Stream 2 to 25 FPS for any resolution.
Note: A maximum of 5 concurrent streams are supported by each camera, this includes shared streams.

Stream Tables – 16MP Corridor Mode

		Corridor Mode				
		Resolution	Description	Max FPS		
				TWDR Off	TWDR 2x	TWDR 3x
Stream 1	H.264, H.265, H.264+ H.265+	3840 x 2160 3264 x 1840 2688 x 1520	(4K) 16:9 16:9 16:9	15 15 15	15 15 15	15 15 15
	H.264, H.265, H.264+ H.265+ MJPEG	1920 x 1080 1664 x 936 1280 x 720	(1080p) 16:9 (HD+) 16:9 (720p) 16:9	30 30 30	25 25 25	15 15 15
Stream 2	H.264, H.265, H.264+ H.265+ MJPEG	1280 x 720 1024 x 576 960 x 544 816 x 464 640 x 360 480 x 272	(720p) 16:9 (PAL+) 16:9 (qHD) 16:9 16:9 (nHD) 16:9 16:9	30*1 30*1 30*1 30*1 30*1 30*1	25*1 25*1 25*1 25*1 25*1 25*1	15 15 15 15 15 15
Stream 3	MJPEG	800x448	16:9	7	7	7

Note: *1 Stream 2 is restricted to 15 FPS when Stream 1 resolution is greater than 1920x1080.
Note: Enabling TWDR will restrict the frame rate of Stream 1 and Stream 2 to 25 FPS for any resolution.
Note: A maximum of 5 concurrent streams are supported by each camera, this includes shared streams.

Known Limitations and Issues

Set Up

Description	Suggested Work-Around
If camera date/time has been set manually, camera date/time may not be accurate if the camera has been without power for more than 24 hours	At first power up, and following every factory reset, when the camera is accessed for the first time it automatically sync's with the workstation to get new Date and Time settings. Following this the camera should be setup with a NTP server to ensure the time is always accurate. NTP will guarantee clock sync as soon as camera is operational. If NTP is not available user should review date and time setting manually after the camera is plugged in. If the camera remains disconnected for an extended period the clock battery will probably discharge and cause the clock reset to 1970, once the date/time page is accessed the camera will automatically sync to the machine used in the active GUI session.
Depending on how and when audio is enabled it can cause the camera to fail to record any video to SD card. Incorrect workflow: • Configure motion and apply to a fault action • enable recording and select stream to record to • enable audio • enable audio input	Correct workflow: • Configure motion and apply to a fault action • enable audio • enable audio input • enable record to SD and select stream to record to
At first boot or after a factory reset the camera will sync time zone, date and time with PC used on First Login. However, the camera may select a generic time zone which will not have DST time changes associated to it or, during Daylight saving time, the time zone may be offset if using a workstation on UTC time zone (windows)	Please check the time zone is assigned correctly at initial boot or after a factory default
If Chrome Browser cache is cleared while the user has an active GUI session open, a credential pop up appears and repeatedly refreshes which does not allow user to input credentials.	Close and reopen Chrome browser or tab
The camera can occasionally lose its personality details after a reset.	Reset the camera.

Description	Suggested Work-Around
Continuous Metadata License doesn't get removed on a factory reset	N/A
Events and Actions>Analytics>Video Intelligence> Unable to change draw style once Perimeter has been selected as rule type	Select draw style before selecting rule type
Periodic (Scheduled Alarm) event details are incorrect/missing in event log	N/A
Periodic Events currently only works with Snapshot	N/A
Blur will not trigger if the lens is covered suddenly with, say, polythene.	N/A
Privacy Zones should be added before the camera is added to an NVR – when adding Privacy Zones, Stream 3's resolution must be a 16:9 aspect ratio (refer to the camera GUI dropdown / manual for resolution options).	N/A
No JPEG attachment on emails sent from the camera when recording is disabled or Snapshot is enabled.	Enable recording to SD card
Event logs and recordings timestamps are all in UTC regardless of camera time zone	N/A
502 Bad Gateway intermittently after an upgrade	Refresh browser after upgrade
Record Event Action can be enabled when Event Recording is disabled – there is no pop up to inform user that Event recording is not enabled.	Ensure Event Recording is enabled prior to enabling Record Event Action
Motion mask doesn't move when flip/mirror is enabled	Create motion mask after enabling mirror/flip
Privacy zone will move position when stream resolution is changed	Ensure camera resolutions are set to required values before creating Privacy Zones
Privacy Zones will move with the image when the camera is moved	Ensure camera is set to optimal position before creating Privacy Zones
Snapshot and record event actions can be enabled when features are disabled	Check that the feature is enabled before selecting it as an event action
SD card management page may appear blank after formatting large SD cards	Refresh page
CIFS – 'Test' may take 2 attempts for success	N/A
Reboot may take over 5 minutes to complete if DHCP is enabled and there is no active DHCP router	N/A

Networking

Description	Suggested Work-Around
CIFS sometimes shows 'Operation Failed' dialog despite all setup on the camera being correct.	If this occurs, please ensure there is sufficient free space on your machine. Also clear out your temporary folders.
When disabling UPnP, note that the camera will still be accessible on some machines as discovery results may have been cached.	UPnP will be fully disabled when Enhanced Security is enabled, cached results will also be blocked
Camera cannot be accessed using UPnP when set to https mode.	Ensure camera is set to HTTP when using UPnP
When camera switches to DCHP and a server is not found the camera will revert back to last configured IP but removes the gateway from the network settings	Enter gateway if required
The camera will support SIP calling as described below. SIP (audio output Speakers) Camera connected to Server/No audio stream to server - SIP call connect. SIP (audio output Speakers) Camera connected to Server/ audio stream to server - SIP calls will be automatically rejected once answered SIP (audio output Network stream) Camera connected to Server/ audio stream to server - SIP call connect -once SIP is enabled on camera this will take over audio stream to server, recorder will not record microphone audio but only incoming SIP calls	N/A

Picture Settings

Description	Suggested Work-Around
The Frequency setting in Exposure can limit FPS to 50FPS if the frame rate is set to 60 and 25 FPS if the frame rate is set to 30 when the frequency is set to 50Hz.	If FPS needs to be set above 50FPS, Frequency should be set to 60Hz.
Changing Exposure settings on the camera can sometimes affect frame rate, lowering it well below what is set on the camera.	If frame rate is a priority, it is advised that Maximum Exposure is set to at least '1/60' to reach 60FPS or to '1/30' to reach 30FPS.
The sharpness value increases by 1 when set to a value within the range of 26-49.	N/A
Picture settings page can become slow/unresponsive	Factory reset required to fix
Setting Exposure Profile to Manual and then changing WDR settings can cause Picture settings page to become unresponsive	WDR settings should not be used when exposure in Manual Profile. Factory reset required to fix
When starting/changing a stream all three video streams will restart their exposure settings meaning the image darkens slightly before brightening up again. This will last just a few seconds.	N/A

Description	Suggested Work-Around
Exposure profiles have the following behaviour 1. Demo Mode VBR Highest is the default out of the box (or after a factory reset) 2. Exposure default buttons will Default Exposure profile to Auto (it will not apply any bitrate changes) 3. Demo mode will only revert back to VBR Highest on a Factory reset 4. Demo mode to other values will change the bitrate to CVBR Max Bitrate 8000 5. Other to Demo will not change the bitrate under any circumstance 6. Other to Other will not change the bitrate under any circumstance 7. When Exposure profiles sets new bitrate values, they will not automatically restart active stream to update to the new settings. Manual restart is required.	

Video

Description	Suggested Work-Around
Sometimes Video playing through camera GUI may not be live – it will show as a looping few seconds clip. This is due to a browser cache issue	Refresh page or clear cache.
Privacy Zones can sometimes move position and resize slightly when stream resolutions are changed.	It is advised to setup your stream configurations prior to setting up Privacy Zones.
If streaming to VLC and the camera undergoes a considerable time change either through factory defaulting of the unit, or manual/NTP change, the VLC video goes grey. This is a VLC application Bug – the issue does not occur on other applications or server integrations.	Restart the VLC stream or configure times prior to starting a VLC stream.
H265 Framerate is being reported incorrectly in logs.	Divide the reported framerate by 3 to get the actual framerate of the video. (This is only applicable to FW before 1.5.0).
Setting the framerate to 1FPS when the stream is using the H265 IntelliZip codec may cause issues with bitrate.	Raise the framerate and reboot the camera.
4K. The camera shall support 30PFS on stream 1, there are however video combinations that will just fall short of 30 (29fps) When Stream 2 is at full stream capabilities MJPEG 15fps	Adjust stream 2 to slightly lower resolution then max supported in order to allow stream 1 to reach full 30 FPS
Video streaming to external players may show some stutter at default 1/8	Increasing max exposure to 1/30 or higher provides a smoother video playback
Using Gaming mode with IntelliZip is not a supported combination - Gaming mode and IntelliZip are pretty much opposite of each other and the codec bandwidth saving feature will prevail over gaming mode maintaining FPS.	IntelliZip shall not be associated to Gaming mode exposure profile

Audio

Description	Suggested Work-Around
Unable to clearly hear audio input stream when audio volume level is at default setting of 74%	Depending on the audio source (microphone, direct line) setting the volume too high can introduce noise. Test the audio source at different levels to find a higher quality volume setting.

DIO

Description	Suggested Work-Around
DIO - Alarm out clears with a camera reboot	No workaround

Analytics

Description	Suggested Work-Around
ROI only working on H264, the GUI will always show this feature, but user should set the correct codec to support this feature.	ROI is only applicable to H264 stream
Motion Fault Action may reset to blank after a firmware upgrade.	Re-select motion fault action.
Motion detection region drawing Grid does not do what it is supposed to do	The Motion detection grid option is only a visual aid, it will not allow for cell selection
GUI event log - cannot delete single event	Camera evet log will not allow delete single event logs user can only delete all events
All AI OC Events appear as Object Tracking in the Event Download page	Due the extent of AI OC rules the clips recording for AI OC analytics will use the generic Object Tracking clip title
If a licence is invalid the licence page will just refresh with no error message. The analytics support table will show no changes	N/A
If using FTP to transfer alert video, when FTP transfer is enabled with Limit Transfer Rate set it may cause a pause in alerts being generated while transfer is taking place, causing Events to burst with a delay of up to 400 seconds	Unselecting Limit transfer rate will prevent these burst
Highlight faces in Face Detections is not supported on RTSP Streams and is only visible on the Web GUI	None. Hardware Limitation

Edge recording & SD card

Description	Suggested Work-Around
Formatting or unmounting a SD Card is sometimes met with a 'Device is Busy' modal.	This usually means the camera is currently recording a clip to the SD Card. It is advised to wait for a period of time when no clips are being recorded or turn off recording on the Camera.
When DST time change are applied to the region, Events and clip names will not apply the 1h offset as they are managed and generated using UTC time	No Workaround
Clip Record (TrickleStor Integration) is not supported when the Stream's codec is set to MJPEG.	Ensure your record stream's codec is either H264/H265 or H264/H265 IntelliZip to allow for the Clip Record feature to work.
Changing Video Settings when a clip is recording may produce a corrupt MP4 due to the interruption	Setup your stream settings before you enable recording.
Occasionally it can happen that if a camera is recording to SD card at the exact time it loses power, this can generate a corrupt file. When the SD card culling comes to deleting this file, it will fail putting the SD card in read only mode. System logs will be generated to notify SD card status	Copy required clips off the SD card before formatting to restore full writing ability.
Clip Recording: Clips can sometimes be longer or shorter than the expected duration due to the gap between IFrames. This issue will be more prominent in Intellizip codecs.	N/A - This is a side effect of the stream settings.
Edge recording - When changing Stream setting on a stream which is also used for SD card recording, the recording will need re-enabled as the camera will give preference to the live stream	Re enable Record to allow for new streams to be picked up by event record stream.
The camera GUI Edge Recording /Event download page will only allow for (the newest) 1000 Clips to be listed. Camera SD card may contain more especially on bigger SD.	To retrieve these users will need to directly access SD card.
Occasionally SD Card Unmount then Mount may cause camera to have DSP Crash	Camera will bank swap and reboot to recover

Security

Description	Suggested Work-Around
When Enhanced Security is enabled the user is prompted to change the username and pass- word from the default admin/admin. If not, all rules are applied then the change request is denied and credentials remain as admin/admin. Failure to comply by rules, intermittently may result in camera log in being unavailable for a few minutes to allow camera to restore default functionality.	Ensure that all username and password rules are followed.
When the user logs out and selects the back arrow on the browser, they are brought back into the GUI without being required to log in. Live video is dis- played but if the user attempts to navigate to another page within the GUI an authentication pop up is visible. Logging in through this pop up causes issues with time and date.	When the user manually logs off and then back in there are no issues.
Under Admin Login – when managing other users accounts – current password is meant for the admin user password and not for the account being managed	
In Security status - Changing the value of Authentication will cause a service restart which will result in GUI being inaccessible for about 10 seconds	Wait 10 seconds for service to restart and GUI working again
Security → Firewall → Address Filtering → Deny option selected. When restoring a camera backup which has the 'Deny' option selected, the Address Filtering tab will have 'Off' selected instead, after the restore is complete. When selecting the 'Deny' option, all IP/MAC addresses that were previously entered remain saved and will be displayed within the table when the 'Deny' option is re-selected.	Re-select the 'Deny' option for Address Filtering - All previously entered details, prior to the creation of the backup, will have been saved and will be displayed as expected.
Changing the enabled status of a feature in Basic Firewall can take up to 5 seconds to save. If the page is refreshed before the status change can be fully implemented, the incorrect status may be displayed on the GUI.	When enabling or disabling Basic Firewall features, wait for 5 seconds after changing the value.
Sometimes Firewall settings are lost during an upgrade.	Re-configure the firewall settings after up- grading the camera.
Login page may not fully load when the user logs in using the HTTPS method through the Chrome browser.	Refresh the browser.
When selecting Enhanced Security - the admin user will be required to conform to new username & password rules- the new rules will not be applied to already created user profiles - all new profiles will require to apply to these rules	If required change user and operator passwords manually
Camera GUI can lockup Occasionally when using HTTPS.	If using HTTPS stop the video on the GUI to prevent lock-up.
Backup/Restore: When the restoration changes the HTTP/HTTPS policy the camera may not be restored correctly.	Set the correct HTTP/HTTPS policy before restoring the file or reboot the camera after the restore.
Session timeout: Camera may log the user out of the GUI when in the Analytics events section when session timeout expires despite pressing buttons on the pages	The camera Event Log page does not account for activity on it and user may be logged out as part of the timeout setting

IAPI3

Description	Suggested Work-Around
When configuring Event Actions via GUI – the iAPI3 configuration may not reflect the correct configuration for these settings.	Will be addressed in a future release.
GUI, and IAPI3 stream configuration combination may not always reflect the camera limitation	The camera will automatically adjust to its limitation (check the stream table for details).

ONVIF

Description	Suggested Work-Around
ONVIF functionality is not currently supported for Flex Gen4 Dual sensor cameras. Only ONVIF Discovery is supported.	N/A

Server Integration Limitations

Description	Suggested Work-Around
VideoEdge Integration: VENVR & Enhanced Security: Edge support Motion VI and DIO alarms integration on VideoEdge VENVR and ExacqVision Server is not supported when Enhanced Security mode is selected on the camera.	Enable video over HTTP on the camera (Setup > Security > Remote Access) when Enhanced Security mode is enabled to allow Metadata to be sent out from the camera.
VideoEdge Integration: If a Video Intelligence licence is added to a camera while configured on NVR, in order for the Server to see the NEW Video Intelligence continues metadata, it will require the camera to be removed and added back to NVR for VI metadata to show support on Edge analytics.	
VideoEdge Integration: TrickleStor Integration with VideoEdge does not work under HTTPS mode in VideoEdge 5.2 or lower.	If using 5.2 or lower Use “both” or HTTP only setting on camera. Alternatively upgrade to 5.3 or above for full HTTPS integration
Genetec iAP3 Integration: To add iAPI3 camera to Genetec using iAPI3 the camera will need set to Digest (Security/Authentication tab) and Video over HTTP enabled (Security /Remote access tab) on the camera.	

Contact Information

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.