tyco | Illustra

Release Notes

Illustra Flex Gen 3 Cameras

Product Code	Model Name	Firmware
IFS03-D21-OI03	Illustra Flex3 3MP Outdoor Dome	SS008.03.03.00.0002
IFS08-D22-OI03	Illustra Flex3 8MP Outdoor Dome	SS009.03.03.00.0002
IFS03-D21-AT03	Illustra Flex3 3MP Indoor Dome	SS008.03.03.00.0002
IFS08-D22-AT03	Illustra Flex3 8MP Indoor Dome	SS009.03.03.00.0002
IFS03-B21-OI03	Illustra Flex3 3MP Bullet	SS008.03.03.00.0002
IFS08-B22-OI03	Illustra Flex3 8MP Bullet	SS009.03.03.00.0002
IFS03-C10-OI03	Illustra Flex3 3MP Outdoor Compact	SS008.03.03.00.0002
IFS08-C10-OI03	Illustra Flex3 8MP Outdoor Compact	SS009.03.03.00.0002

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

June 2022

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

8200-1937-05 D

Johnson Controls

Table of Contents

What's in This Release

What's New

Firmware Illustra.SS008.03.03.00.0002 / SS009.03.03.00.0002

Adds the following new features:

- Traffic Control
- Quality of service
- Secure streaming (HTTPS)

ONVIF enhancements
DHCP enhancements
Security enhancements
Bandwidth enhancements

Previous Release

Firmware Illustra.SS008.03.02.00.0001 / SS009.03.02.00.0001

- Application support (including ExacqVision Edge app) added to 4K models
- Cloudvue updates
- Bug fixes

Firmware Illustra.SS008.03.01.00.0002 (3MP models only) / SS009.03.01.00.0002 (4K models only)

- Video Intelligence and Face Detection support added to 4K models only
- Video over HTTPS support (which will allow integrations for Secure Streaming with VideoEdge 5.7 onwards). **Note: a camera factory reset is required to fully apply the above updates (IP setting only can be retained).**
- Encrypted SD Card Storage feature
- Option to by-pass security on initial security prompt
- iAPI3 for Metadata transport changes to HTTPS with Enhanced Security selection
- Bug fixes

Firmware Illustra.SS008.03.00.00.0302 / SS009.03.00.00.0302

1. Adds the following new Flex Gen 3 camera models to the line.

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

Features

Key Features

- High resolution, 2 to 8 megapixel images, Multiple IP streams of H.264, H.264IntelliZip, H.265, H.265IntelliZip and MJPEG video
- 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
- ONVIF 2.4 profile S compliant
- Power over Ethernet (PoE) or AC powered (model specific)
- Motion Detection and Blur Detection support on camera
- Wide Dynamic Range, TWDR and TWDR3x (model specific)
- Auto & Manual White Balance Modes
- Manual Focus and Zoom Control (model specific)
- One touch Focus (model specific)
- Eventing with RTP meta-data streaming
- Support for up to five Regions of Interest
- Support for up to nine Privacy Zones
- Enhanced Security
- Support for FTP, SNMP, SMTP, CIFS, 8021.x and Firewall filtering
- SD card event buffering (requires micro-SD or SD-HC card)
- Offline recording to SD card
- SD card event download
- TrickleStor integration with VENVR
- Outstanding color reproduction
- No dependencies on 3rd Party Utilities for Camera Setup (No QuickTime and Java requirements)
- Expanded Browser Support: IE, Chrome, Firefox, Safari
- UPnP Discovery
- Easy to install
- Sleek and compact design
- Cloudvue Integration for fixed cameras
- Video Intelligence and Face Detection support (4K models only)

Firmware Upgrade

You can upgrade the Illustra Flex Camera 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 Internet Explorer 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

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, it is best practice to select the Change Password check box to immediately change the default password to one unique to your surveillance system.

6. Optional - If you select the Enhanced Security option, you are required and instructed to create a complex password.

See below for further information on Security configuration.

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.

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. Passwords complexity is set to require minimum of any 5 characters (admin cannot be used).
4. Authentication Method is set to basic by default.

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 HTTPS
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 (case sensitive) 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 camera 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.
- Disables all ONVIF capabilities.
- Disables UPnP Discovery protocol.
- Disables Exacq Audio Ports.

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.

DIO (alarm in & alarm out) and Edge Analytics with Enhanced security

From Firmware SS004.01.02 onwards if a user requires DIO (alarm in/out) or Analytics with VideoEdge VENVR Edge analytics or ExacqVision Server, while the camera is in Enhanced Security Mode the user shall be required 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.

This allows for VENVR Edge support or Motion and DIO alarms integration on the ExacqVision Server when the camera is on Enhanced Security mode.

RTSP Authentication

We now require video stream authentication – if upgrading to 1.01 from previous version the authentication won't be applied, however If the camera gets factory defaulted or was received with FW 1.01 then RTSP authentication will be enabled.

We don't recommend disabling RTSP authentication, but if required it can be managed via Security Tab in camera GUI.

Multicast

Multicast feature is included on FW 1.2 onwards. 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" or HTTP only when integrating with this feature.

Analytics

	Motion Detection Events	Motion Detection Metadata	Video Intelligence Metadata	Video Intelligence Events	Face Detection Metadata	Face Detection Events	Blur Detection Events	Tamper Detection Events
Illustra Flex 3MP Mini-Dome, Bullet, Compact	Yes	Yes	N/A	N/A	N/A	N/A	Yes	Yes
Illustra Flex 8MP Mini-Dome, Bullet, Compact	Yes	Yes	Yes*	Yes	Yes**	Yes	Yes	Yes

* Requires Licence Purchase
** Requires Free License Request

Video Intelligence

- The camera supports the configuration of Video Intelligence Alerts. You can define Video Intelligence settings that can be used to set up Analytics Rules.
- You can add up to three Analytics Rules by default on the camera web user interface. An alarm is generated each time an event is triggered.
- You can add up to twenty Analytics Rules and access continuous metadata if you purchase a license for *Video Intelligence - Full Suite*. See *www.illustracameras.com* for more information.
- Illustra Connect must be used to generate the xml required to purchase a license. Once purchased, the license can be uploaded to the camera using Illustra Connect or on the camera web user interface licensing page.
- On a hardware Factory Default, this license will be removed from the camera and will need to be re-added. On a software factory default, users can choose whether to retain the license. (Illustra Connect soft reset will automatically retain the license).
- For detailed information about configuring each rule, refer to the user manual.
- Video Intelligence alarms are compatible with VENVR 5.2.
- It is recommended to configure Video Intelligence 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**.

Stream Tables

Flex Gen 3 - 3MP camera stream tables

		Normal Mode				
				Max FPS		
Stream Resolution	**Codecs**	**Resolution**	**Description**	**TWDR Off**	**TWDR 2x**	**TWDR 3x**
Stream 1	H.264 H.265 H264 IntelliZip H265 IntelliZip MJPEG	2048 x 1536 1920 x 1080 1664 x 936 1280 x 720	4:3 (1080p) 16:9 (HD+) 16:9 (720P) 16:9	30 60 60 60	30 30 30 30	20 20 20 20
Stream 2	H.264 H.265 H264 IntelliZip H265 IntelliZip MJPEG	1280 x 720 1024 x 576 640 x 480 640 x 360 480 x 360 384 x 288	(720p) 16:9 (PAL+) 16:9 4:3 (mHD) 16:9 4:3 4:3	30*1 30*1 30*1 30*1 30*1 30*1	30 30 30 30 30 30	20 20 20 20 20 20
Stream 3	MJPEG	640 x 360 480 x 360 384 x 288	(mHD) 16:9 4:3 4:3	15 15 15	15 15 15	15 15 15

Note:*1 Streams 2 and 3 are restricted to 15 FPS when Stream 1 is greater than 30 FPS.
Note:*2 Streams 1 and 2 are restricted to 30 FPS when TrueWDR 2x is enabled.
Note:*3 Streams 1 and 2 are restricted to 20 FPS when TrueWDR 3x is enabled.
Note:*4 The maximum frame rate of any stream is 30 FPS when corridor mode is enabled.
Note:*5 The maximum frame rate of any stream is 30 FPS when corridor mode is enabled.
Note: A maximum of 5 concurrent streams are supported by each camera, this includes shared streams.

		Corridor Mode				
				Max FPS		
Stream Resolution	**Codecs**	**Resolution**	**Description**	**TWDR Off**	**TWDR 2x**	**TWDR 3x**
Stream 1	H.264 H.265 H264 IntelliZip H265 IntelliZip MJPEG	2048 x 1536 1920 x 1080 1664 x 936 1280 x 720	4:3 (1080p) 16:9 (HD+) 16:9 (720P) 16:9	30 30 30 30	30 30 30 30	20 20 20 20
Stream 2	H.264 H.265 H264 IntelliZip H265 IntelliZip MJPEG	1280 x 720 1024 x 576 640 x 480 640 x 360 480 x 360 384 x 288	(720p) 16:9 (PAL+) 16:9 4:3 (mHD) 16:9 4:3 4:3	30*1 30*1 30*1 30*1 30*1 30*1	30 30 30 30 30 30	20 20 20 20 20 20
Stream 3	MJPEG	640 x 360 480 x 360 384 x 288	(mHD) 16:9 4:3 4:3	15 15 15	15 15 15	15 15 15

Note:*1 Streams 2 and 3 are restricted to 15 FPS when Stream 1 is greater than 30 FPS.
Note:*2 Streams 1 and 2 are restricted to 30 FPS when TrueWDR 2x is enabled.
Note:*3 Streams 1 and 2 are restricted to 20 FPS when TrueWDR 3x is enabled.
Note:*4 The maximum frame rate of any stream is 30 FPS when corridor mode is enabled.
Note:*5 The maximum frame rate of any stream is 30 FPS when corridor mode is enabled.
Note: A maximum of 5 concurrent streams are supported by each camera, this includes shared streams.

Flex Gen 3 - 8MP camera stream tables

		Normal Mode				
		Resolution	Description	Max FPS		
Stream Resolution	Codecs			TWDR Off	TWDR 2x	TWDR 3x
Stream 1	H.264 H.265 H264 IntelliZip H265 IntelliZip MJPEG	3840 x 2160 3264 x 1840 2688 x 1520 1920 x 1080 1664 x 936 1280 x 720	(4K) 16:9 16:9 16:9 (1080p) 16:9 (HD+) 16:9 (720P) 16:9	30 30 30 60 60 60	25 25 25 25 25 25	15 15 15 15 15 15
Stream 2	H.264 H.265 H264 IntelliZip H265 IntelliZip 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 (mHD) 16:9 16:9	30*1 30*1 30*1 30*1 30*1 30*1	25 25 25 25 25 25	15 15 15 15 15 15
Stream 3	MJPEG	640 x 360 480 x 272	(mHD) 16:9 4:3	30*1 30*1	25 25	15 15

Note:*1 Stream 2 is restricted to 15 FPS when Stream 1 is greater than 30 FPS or when Stream 1 resolution is greater than 1920x1080.
Note:*2 Stream 3 is restricted to 10 FPS when Stream 1 is greater than 30 FPS or when Stream 1 resolution is greater than 1920x1080.
Note:*3 All streams are restricted to 25 FPS when TrueWDR 2x is enabled.
Note:*4 All streams are restricted to 15 FPS when TrueWDR 3x is enabled.
Note:*5 The maximum frame rate of any stream is 30 FPS when corridor mode is enabled.
Note: A maximum of 5 concurrent streams are supported by each camera, this includes shared streams.

		Corridor Mode				
		Resolution	Description	Max FPS		
Stream Resolution	Codecs			TWDR Off	TWDR 2x	TWDR 3x
Stream 1	H.264 H.265 H264 IntelliZip H265 IntelliZip MJPEG	3840 x 2160 3264 x 1840 2688 x 1520 1920 x 1080 1664 x 936 1280 x 720	(4K) 16:9 16:9 16:9 (1080p) 16:9 (HD+) 16:9 (720P) 16:9	30 30 30 30 30 30	25 25 25 25 25 25	15 15 15 15 15 15
Stream 2	H.264 H.265 H264 IntelliZip H265 IntelliZip 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 (mHD) 16:9 16:9	30*1 30*1 30*1 30*1 30*1 30*1	25 25 25 25 25 25	15 15 15 15 15 15
Stream 3	MJPEG	640 x 360 480 x 272	(mHD) 16:9 4:3	30*1 30*1	25 25	15 15

Note:*1 Stream 2 is restricted to 15 FPS when Stream 1 is greater than 30 FPS or when Stream 1 resolution is greater than 1920x1080.
Note:*2 Stream 3 is restricted to 10 FPS when Stream 1 is greater than 30 FPS or when Stream 1 resolution is greater than 1920x1080.
Note:*3 All streams are restricted to 25 FPS when TrueWDR 2x is enabled.
Note:*4 All streams are restricted to 15 FPS when TrueWDR 3x is enabled.
Note:*5 The maximum frame rate of any stream is 30 FPS when corridor mode is enabled.
Note: A maximum of 5 concurrent streams are supported by each camera, this includes shared streams.

Known Limitations and Issues

Setup

Description	Suggested Work-Around
Applicable to all Flex cameras: If the camera date/time has been set manually, camera date/time may not be accurate if camera has been without power for more than 24 hours	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 clock has reset to 1970, once the date/time page is accessed the camera will automatically sync to the machine used in the active GUI session.
Applicable to all Flex cameras: 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
Applicable to all Flex cameras: 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
Firmware upgrade is not successful: 406 firmware decryption error.	Re-apply upgrade.
Applicable to all Flex cameras: The camera can occasionally lose its personality details after a reset.	Reset the camera.

Video

Description	Suggested Work-Around
Applicable to all Flex cameras: Privacy Zones can sometimes move position and resize slightly when stream resolutions are changed.	It is advised to set up your stream configurations prior to setting up Privacy Zones.
Applicable to all Flex cameras: Video playing through camera GUI may not be live - browser cache issue	Refresh page or clear cache.
Applicable to all Flex cameras: 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.
Applicable to all Flex cameras: 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
Applicable to all Flex cameras: Under certain lights (Mercury and Sodium outdoor lighting) the user may observe that the picture does not have the correct colors.	The user can change the White Balance setting from the default 'Auto WB Normal' to 'Auto WB Wide'.

Picture Settings

Description	Suggested Work-Around
Applicable to all Flex cameras: 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.
Applicable to all Flex cameras: 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.
Applicable to all Flex cameras: Noise banding in TWDR with high Exposure Offset.	Will be addressed in a future release.
Applicable to all Flex cameras: Exposure Offset setting of -2 may lockup in extreme conditions.	The issue is specific to -2 and specific light conditions, we recommend to use the other available option in Exposure offset.
Applicable to all Flex cameras: 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.
Applicable to all Flex cameras: Stream 1 will automatically reconfigure stream 2 to 15 FPS if stream 1 is updated to 31 FPS or above.	GUI will provide a warning of this change but changes via IAPI or ONVIF will change stream 2 without warning
Applicable to all Flex cameras: When TWDR is enabled, stream configuration restrictions apply	Ensure that stream is configured correctly before enabling TWDR. See stream tables for supported configurations.
Applicable to all Flex cameras: Exposure method position does not change when Mirror or Flip orientation is applied.	Re-configure Exposure Method after Mirror or Flip orientation is applied.
Applicable to all Flex cameras: The sharpness value increases by 1 when set to a value within the range of 26-49.	N/A
Applicable to all Flex cameras: 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.

Edge Recording & SD Card

Description	Suggested Work-Around
Applicable to all Flex cameras: 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.
Applicable to all Flex cameras: 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.
Applicable to all Flex cameras: Changing stream configurations when a clip is being recorded may cause the camera to reboot.	It is advised to setup your stream configurations prior to enabling Clip Record. Otherwise, please stop recording before changing stream configurations.
Applicable to all Flex cameras: 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.
Applicable to all Flex cameras: 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.
It is recommended that Stream 2 is used as the recorded stream if edge analytics are running on a camera with Stream 1 that is greater than 3mp at 30fps	

Security

Description	Suggested Work-Around
Applicable to all Flex cameras: 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 displayed 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.
Applicable to all Flex cameras: 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.
Applicable to all Flex cameras: Under Admin Login – when managing other users accounts – current password is meant for the admin user password and not for the account being managed	
Applicable to all Flex cameras: 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
Applicable to all Flex cameras: Login page may not fully load when the user logs in using the HTTPS method through the Chrome browser.	Refresh the browser.
Applicable to all Flex cameras: TrickleStor Integration with VideoEdge does not work under HTTPS mode.	Use “both” or HTTP only setting on camera
Applicable to all Flex cameras: 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
Applicable to all Flex cameras: 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

Description	Suggested Work-Around
Camera GUI can lockup occasionally when using HTTPS.	If using HTTPS stop the video on the GUI to prevent lock-up.
Applicable to all models: 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.
Applicable to all Flex cameras: Firewall address filtering settings on backup and restore fail to recover.	To prevent camera isolation, the 'OFF' option under address filtering is selected after a camera restore, as opposed to the 'Deny' option being restored. All information within the 'Deny' table remains saved after the restore, and can then be selected and altered as desired.
Applicable to all Flex cameras: 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.
Applicable to all Flex cameras: 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.
Applicable to all Flex cameras: Camera cannot be accessed using UPnP when set to https mode.	Ensure camera is set to HTTP when using UPnP
Applicable to all Flex cameras: Sometimes Firewall settings are lost during an upgrade.	Re-configure the firewall settings after up-grading the camera.

Networking

Description	Suggested Work-Around
Applicable to all Flex cameras: 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.
Applicable to all Flex cameras: 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
Email alerts are not sent when Email and Snapshot are set to the same Fault Action	Do not configure Email and Snapshot to the same Fault Action.

Analytics

Description	Suggested Work-Around
Applicable to all Flex cameras: ROI should not be used on H264+ and H265+ as it may interfere with codec compression.	If ROI is required then another codec option should be selected.
Applicable to all Flex cameras: 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
Applicable to all Flex cameras: User may be unable to set motion detection fault action after a camera reset.	Reset the camera again
Applicable to all Flex cameras: Motion Fault Action may reset to blank after a firmware upgrade.	Re-select motion fault action.
Email alerts are not sent when Email and Snapshot are set to the same Fault Action	Do not configure Email and Snapshot to the same Fault Action.
Continuous Metadata license and Face detection 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 (ScheduledAlarm) event details are incorrect/missing in event log	N/A
Periodic event config change requires reboot to apply	N/A
Periodic Events currently only works with Snapshot and FTP	N/A
It is recommended that Stream 2 is used as the recorded stream if edge analytics are running on a camera with Stream 1 that is greater than 3mp at 30fps	

IAPI3

Description	Suggested Work-Around
Applicable to all Flex cameras: 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.
Applicable to all Flex cameras: GUI, ONVIF 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
Only applicable to non PTZ Flex cameras: On ONVIF Device Manager (ODM) Tool the camera may display PTZ Settings.	These cameras do not support PTZ as they are fixed lens units.
Applicable to all Flex cameras: Camera does not stream when added to Exacq using the onvif protocol.	Add camera to Exacq as Illustra3

Audio

Description	Suggested Work-Around
Applicable to all Flex cameras: 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.

Server Integration Limitations

Description	Suggested Work-Around
DIO and Motion events not available on Milestone Server with ONVIF integration	Camera limitation. ONVIF events are not supported.
DIO - Alarm out clears with a camera reboot	No workaround
Applicable to all Flex cameras: Genetec Recorders do not support all the resolutions the camera supports. For example, 1664x936 and 3264x1840 is not available on Genetec Recorders.	N/A - This is a limitation of the recorder.
Applicable to all Flex cameras - ONVIF Integration - Profile S Integration does not support Codec: H264 Intellizip, H265, H265 Intellizip.	If those codecs are required then an iAPI3 integration is necessary
VENVR Edge support or Motion 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.

Contact Information

If you have any questions regarding these release notes, please contact Tyco Security Products Technical Services at:

Toll Free: 800-507-6268, Option 2 **International:** 561-912-6259, Option 2 **Alternative Number:** 800-392-2873

Fax: 450-444-2029 **Hours:** 08:00 – 20:00 EST

Email: adtechservices@tycoint.com **Website:** www.illustracameras.com

In Europe, Middle East and Africa, contact Technical Support at:

Toll Free: 00 800 CALLTYCO or 00 800 2255 8926 **Direct**: +31 475 352 722

Hours: 8am – 6pm CET **Email:** video-support@jci.com

Website: www.tycosecurityproduct.com **Website:** www.tycosecurityproducts.com

Local Direct dial numbers:

UK	+44 (0) 330 7771 300	**Bahrain**	(0) 800 041 27
France	0800 90 79 72	**Greece**	00800 31 229 453
Spain	900 99 31 61	**Russia**	810 800 20 521 031
Germany	0800 1806 757	**Turkey**	00800 31 923 007
Italy	+39 02 3051 0112 or +39 02 8998 1845	**United Arab Emirates**	(0) 800 0310 7123
Belgium	0800 76 452	**Israel**	+972 (0) 77 220 1350
Ireland	180 094 3570	**Nordic Countries**	+45 4494 9001
S. Africa	(0) 10 100 3292	**Qatar**	(00) 800 100 841
Oman	(00) 800 743 64	**Lebanon**	01 426 801 first, then dial 855 234 3677
Egypt	(0) 800 000 9697	**KSA**	+966 (0) 800 850 0830

In Latin America and Caribbean, contact Technical Support at:

Southern Latin America
Contact: Cristian Bustamante Meza
Cell: +56 933769309
Email:
cristian.enrique.bustamantemeza@jci.com

Brazil
Contact: Robson Santos
Phone: +55 11 3833 6792
Cell: +55 11 99106 8125
Email: robson.2.santos@jci.com

Caribbean & Central America
Contact: Virginia Baez Medina
Phone: +1 787 474 9824
Cell: +1 787 619 6527
Email: virgina.baez@jci.com

Northern Latin America
Contact: Jaime Trujillo
Phone: +1 305 330 6447
Cell: +57-317 863 0661
Email: jaime.trujillo@jci.com

Mexico
Contact: Luis Saavedra Sol
Phone: +52 1 (55) 7960 0398
Email: luis.saavedra@jci.com

In Asia Pacific, contact Technical Support at:

Toll Free: 00 800 CALLTYCO or 00 800 2255 8926 **China Direct:** +86 21 6163 8644

China Hotline: 400 671 1528 **India Direct:** +91 80 4199 0994

Australia Toll Free: 1 800 580 946 **New Zealand & Pacific Direct:** +64 9942 4004

Hours: 9am – 6pm Monday to Friday, China local time **Email:** video-support@jci.com

Hours: 9am – 7pm Monday to Friday, India local time **Hours:** 8am – 6pm Monday to Friday, Australia local time