

Release Notes

Illustra Pro Gen 2 12MP Fisheye Camera

Product Code	Model Name	Firmware
IPS12-F27-OI02	Illustra Pro Gen 2, 12MP Fisheye camera	Illustra.SS015.01.00.00.0011

Product Data

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

February 2021

Note

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

8200-1984-03 A0

JOHNSON CONTROLS, TYCO and ILLUSTRRA are trademarks and/or registered trademarks.
Unauthorized use is strictly prohibited
© 2021 Johnson Controls. All rights reserved.

Table of Contents

What's in This Release	3
What's New	3
Features	4
Firmware Upgrade	5
Upgrade Camera Firmware through the Web GUI	5
<i>Procedure: Upgrade Camera Firmware through the Web GUI</i>	5
Upgrade Camera Firmware through Illustra Connect	5
Known Limitations and Issues	9
Contact Information	12

What's in This Release

What's New

Firmware Illustra.SS015.01.00.00.0011

1. Introduces the following new Illustra Pro Gen 2 camera model to the line.

Product Code	Model Name	Description
IPS12-F27-OI02	Illustra Pro Gen 2, 12MP Fisheye camera	Illustra Pro 12MP Fisheye, indoor/outdoor, vandal, white, TDN, w/IR, WDR

Key Features

- High resolution, up to 12 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)
- Motion Detection support on camera
- Wide Dynamic Range
- Auto & Manual White Balance Modes
- Line-in Audio support
- 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 card)
- SD card event download
- 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

Firmware Upgrade

You can upgrade the 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 a supported web 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 **Upgrade**. 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 Pro Gen 2 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 **Select a Security Type**.

Select a Security Type: Standard Security or Enhanced Security. If you are keeping Standard Security, a password change is enforced. 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 Pro Gen 2 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 **Select a Security Type**.
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.

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.
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.

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.

Known Limitations and Issues

Description	Suggested Work-Around
When in WDR mode and OSD is enabled, flicker can occur in stream 2 and stream 3 when stream 2 and 3 are not using the same fps.	If OSD is required in WDR mode, match stream 2 and Stream 3 fps to remove all flicker.
The camera only supports edge metadata alert events. For more information, refer to the edge analytics support table.	N/A
During the configuration of analytics, or when enabling or modifying motion detection rules, video streams are affected. When the change is applied, it may cause video streams to restart causing a small loss of video. Video functionality is restored within seconds.	N/A
Each backup configuration file is specific to the camera and firmware version. Therefore, if a camera is upgraded, the old backup file becomes obsolete and the camera needs to be updated with a new copy. For example, a backup file created on a camera running on 1.0 firmware cannot be installed on a camera running 2.0.	N/A
The camera supports DHCP IP allocation for IPv4 addresses but does not support IPv6 IP ranges. IPv6 is only supported through linking local addresses.	N/A.
On the Illustra Pro Fisheye camera, the configuration of privacy zones is only supported with a Fisheye image source.	Configure privacy zones on a Fisheye image prior to changing to a new image source.
On the Illustra Pro Fisheye camera, motion detection only runs on the camera when Fisheye is selected as the active image source.	Select a Fisheye image as the camera image source, if using motion detection.
On the Illustra Pro Fisheye camera, the configuration of privacy zones is only available when Fisheye is selected as the active image source. After the privacy zones have been configured on the Fisheye, privacy zones on the other image sources are available.	During the configuration of privacy zones, select a Fisheye image as the camera image source. You can then revert back to your desired image source.
When enabling video recording - S.D. recording, FTP, CIFS, and SMTP, if analytics are already configured and enabled, events are not recorded.	Enable analytics prior to configuring an event action. If analytics weren't enabled prior to configuring an event action, disable and re-enable analytics to start recording events.
After a period of inactivity, an open web interface session can be slow to respond to a navigation request. Normal response is restored within a few seconds.	Avoid leaving the browser idle for long periods.

Description	Suggested Work-Around
The camera can save a backup configuration file for # future restorations. However, this feature is not supported when using the ONVIF integration.	Camera backup can be performed through the camera web interface.
The camera web interface can be configured to several languages. When the camera web user interface is configured to Arabic, some screen resolutions may display text that is too small to read.	If the Arabic text is difficult to read, use the browser window zoom utility to increase the text size.
If using the ONVIF device manager to upgrade the units, the tool needs to be provided with camera authentication, in order for the upgrade to complete successfully.	Use the Illustra connect tool to upgrade the camera. This tool does not have the limitation and can also provide batch upgrades on units that are running the same firmware.
During the upgrade an error message can appear. The message is: Failed to read enough bytes on the stream. The upgrade completes successfully, regardless of the error message.	
Camera events are cleared when the firmware is upgraded. This only affects logs. Recorded video on SD cards is not cleared when the firmware is upgraded.	N/A.
When integrating the Illustra Pro Fisheye camera with a third party recorder, this can result in incorrect stream configuration and unstable cameras if the camera mount setting and image sources are changed while the camera is connected to the recorder.	Configure the camera mount setting and image source before adding the camera to the recorder.
DDN username field does not allow for special character	Targeted for future implementation
Some sections of the initial login are not fully localized and shown in English.	Targeted for future implementation
The date and time on the camera web browser interface offsets incorrectly during DST time changes. All other times displayed on the web browser interface and the time registered internally maintain the current time. This relates to OSD time, event time, metadata event time, logs, and recorded clips time.	Resolved.
Changing camera dewarp/mount setting sometimes takes 2 attempts	N/A
Active image/quad digital ptz is very sensitive	N/A
When streaming video through Victor client at maximum resolution and FPS (2992x2992, 30fps) the FPS may not be steady and may fluctuate.	If steady 30 FPS is desired, please lower resolution to achieve this

Pro Gen 2 12MP Fisheye Release Notes

Description	Suggested Work-Around
Audio – mic in audio is not supported, only line-in audio is supported.	N/A
IR Compensation is greyed out when ROI is enabled.	N/A
IR Range is approx. 4m when IR compensation is ON. IR range is close to 15 m when IR compensation is OFF.	N/A
Edge dewarp does not support Zoom	N/A
Dynamic range limited to tone mapping (i.e. digital Wide Dynamic Range (dWDR))	N/A
For VideoEdge integration - if using Edge Dewarping ensure that Stream 1 and 2 are using the same Image Source to avoid incorrect integration - camera will only support dual stream configuration to the server.	Ensure Stream 1 and 2 are using the same Image Source when using Edge Dewarping.

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

Information furnished by Tyco Security Products is believed to be accurate and reliable. However, no responsibility is assumed by Tyco Security Products for its use, nor any infringements of other rights of third parties which may result from its use. No license is granted by implications or otherwise under any patent rights of Tyco Security Products.
