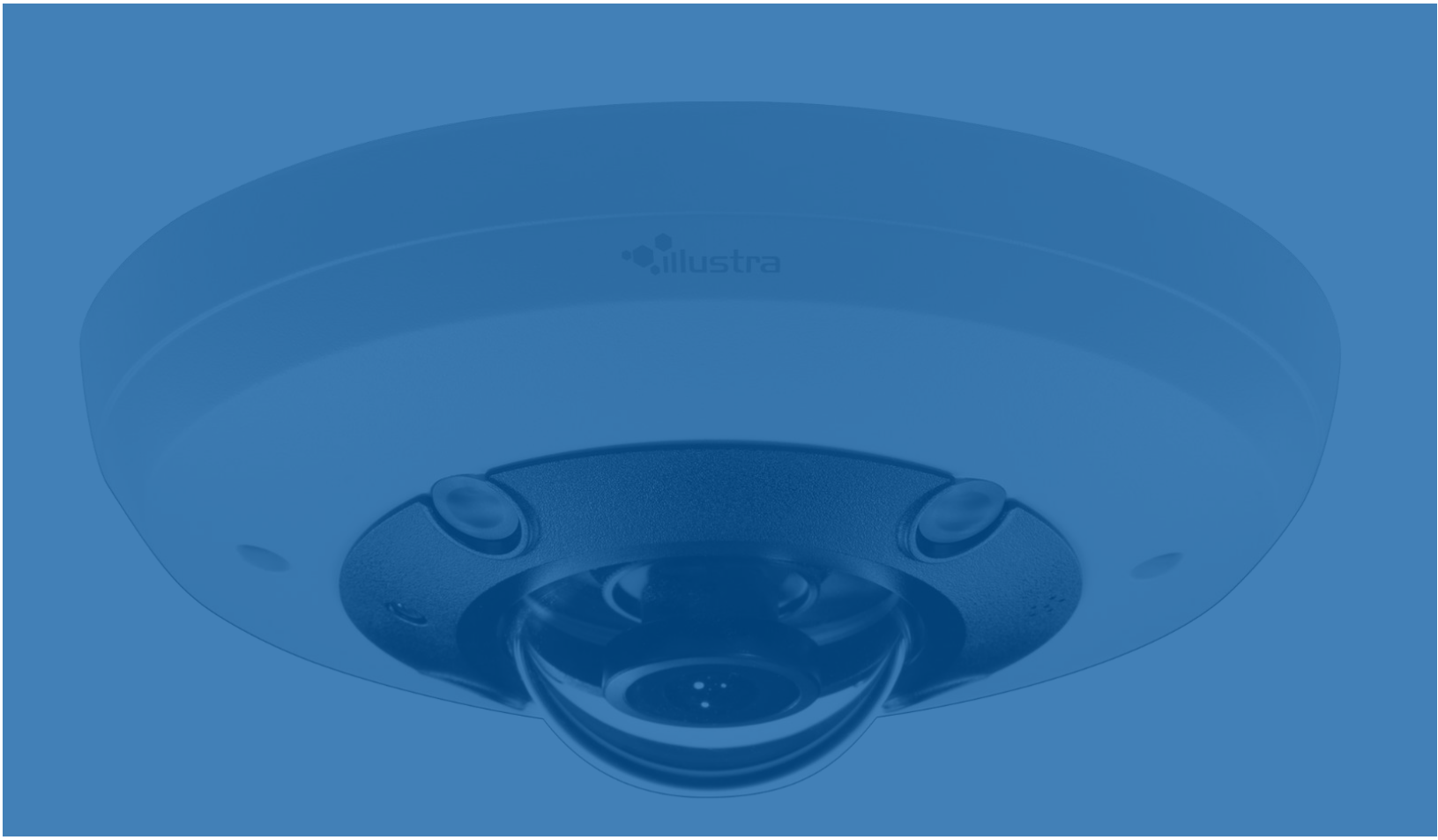
tyco security

Illustra Flex and Pro Cybersecurity Overview Whitepaper



Johnson Controls

INTRODUCTION

The Cyber Protection Product Security Program from Tyco security solutions provides peace of mind to our customers with a holistic cyber mindset beginning at initial design concept, continues through product development and is supported through deployment, including a rapid incident response to meet the comprehensive and evolving cybersecurity environments.

The Illustra Flex and Pro Cybersecurity Overview Whitepaper is intended to provide cybersecurity guidance used in planning, deployment and maintenance periods.

As cybersecurity threats have become a risk impacting all connected devices, it is important to assure that cybersecurity is considered throughout the planning, deployment and maintenance phases associated with a product's functional operation.

This guide provides hardening guidance for configuration and maintenance, including the operating system, user accounts, permissions and roles, backup and restore, redundancy, and patch management.

TABLE OF CONTENTS

ILLUSTRA FLEX AND PRO IP CAMERAS

Introduction

Illustra Flex and Illustra Pro are ranges of IP addressable video surveillance cameras that utilize Ethernet communications, commonly referred to as IP cameras. As an IP camera with an advanced feature set, Illustra IP cameras are used in many applications including retail locations for loss prevention, and schools and hospitals to protect the safety of students and patients. Illustra IP cameras are also used to assist governments in protecting high-risk environments such as ports and borders.

Illustra IP cameras are designed to integrate seamlessly with victor clients and VideoEdge NVRs. The native support in victor and VideoEdge allows the operator to access video and audio using high-performance streaming and leverage its most advanced features including motion meta-data. Also compliant with the ONVIF open communication standard, Illustra IP cameras are interoperable with a wide range of other ONVIF compliant components such as video and access control management systems.

Illustra IP cameras are part of an end-to-end security and surveillance solution that is used to keep what you value safe and enables your business to operate effectively.

OVERVIEW

Enhanced Security Mode

Enhanced Security Mode is a feature on Illustra cameras. By enabling the Enhanced Security Mode, it forces all users to change default usernames and change passwords to something with an enhanced level of complexity. Enhanced Security Mode also defaults to the minimum configuration of communication methods and discovery methods, such as allowing only HTTPS and disabling discovery methods.

Encrypted Communications

Illustra cameras only support encrypted communications using TLSv1.2 and cipher suites with a 256 bit minimum length.

Security Overview Page

Illustra cameras have a security overview page which allows for convenient viewing the status of security relevant items. The user has the ability to see what protocols are enabled, what port they are utilizing, if a firewall is enabled, if 802.1x is enabled and other relevant items.

RTSP Authentication

Illustra cameras has authentication on the Real Time Streaming Protocol (RTSP) video stream, and if requested, this authentication can be sent in a more secure manner.

IEEE 802.1X

Illustra cameras supports 802.1X as a supplicant (client device). The 802.1X support allows the camera to be authenticated prior to gaining network access.

Auditability

The camera has internal logs which may be remotely viewed. Logs may be downloaded through File Transfer Protocol (FTP) or Simple Mail Transport Protocol (SMTP). This would allow for an analyst or auditor to review the information to see if malicious activity has been committed and who committed it.

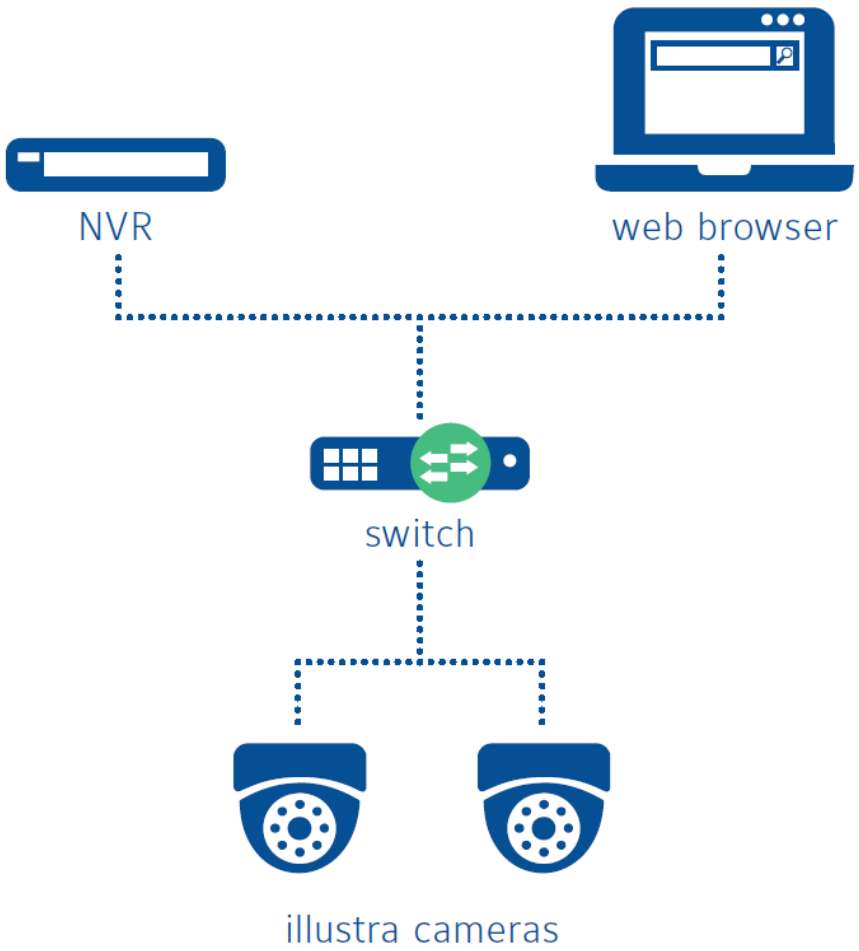
User Roles

Users may be assigned to roles to restrict their access to a subset of functions needed for their task. Admin, operator and users are different assignable roles on the camera.

Local Video Storage

If the camera is installed with an SD card, the camera will continue to record video locally in case of network loss. When the connection is restored, the recorded data is then transferred to the network video recorder reducing video loss during network outage.

Network Architecture



NVR

A Network Video Recorder (NVR) may connect to one or many Illustra cameras. Illustra cameras work with a wide range of NVRs including the Tyco security solutions VideoEdge NVRs.

Web Browser

Illustra cameras support configuration via a web browser. See compatibility list contained with the datasheets for the web browsers that are supported. https://illustracameras.com/support/downloads/

Switch

Illustra cameras are connected to a network by route of a network switch. It is recommended that the network is segmented to isolate video on a dedicated local area network for both performance and security reasons. Illustra models which support power-over-Ethernet (PoE) may be powered by a network switch that has PoE ports.

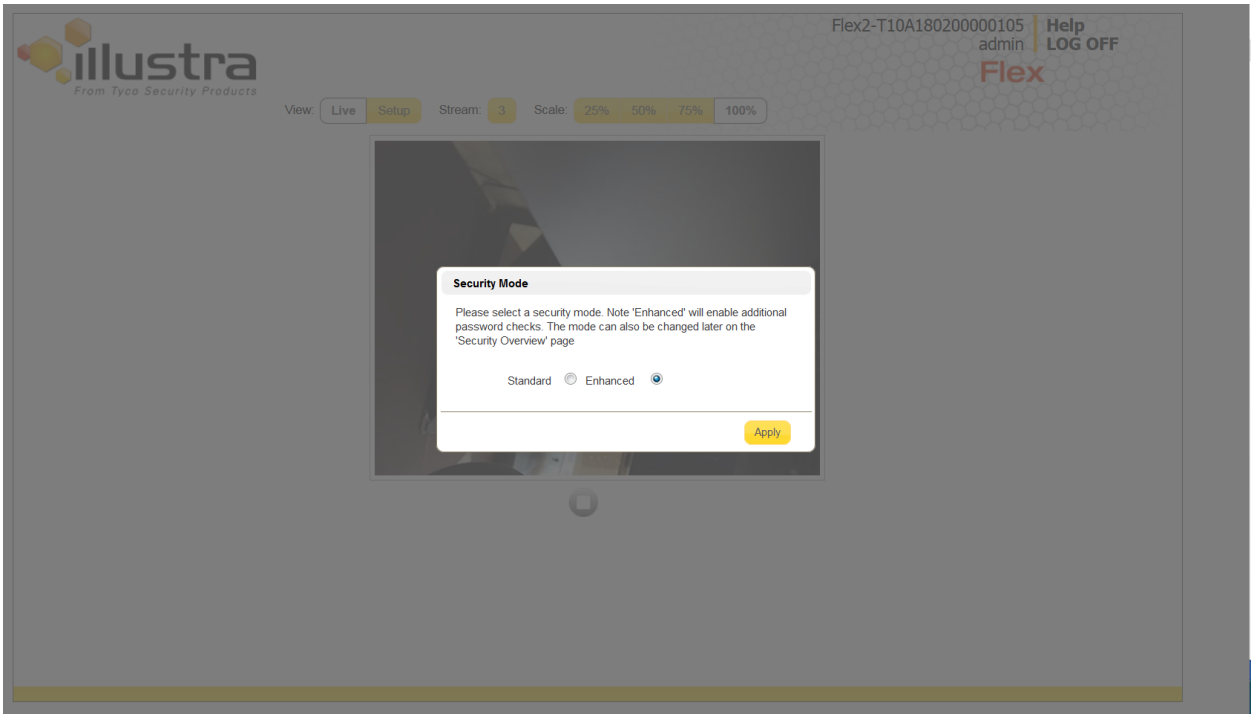
Enhanced Security Mode

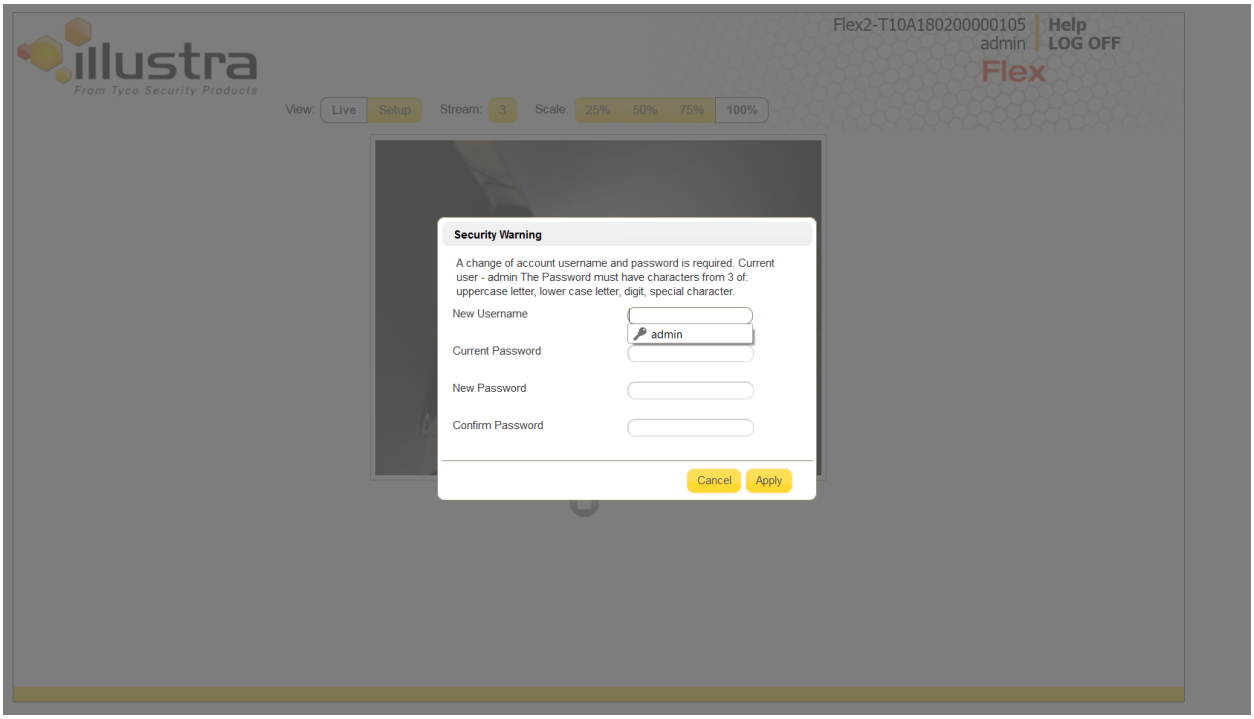
When the camera is initialized, the user has the option to choose between Standard and Enhanced Security Mode. The Enhanced Security has two main benefits:

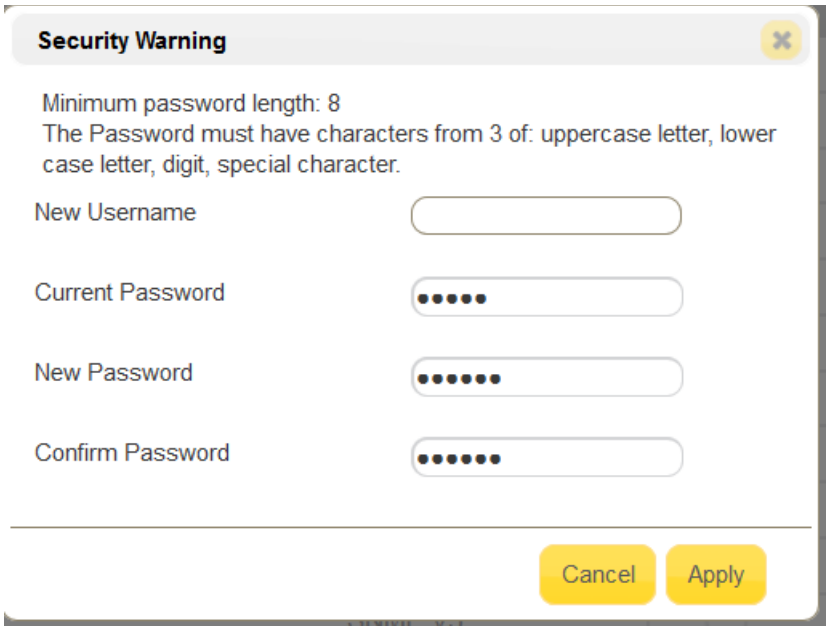
1) **Forced password complexity** - forces a change of the default credentials. The new username must be a minimum of 5 characters in length. The new password must be a minimum of 8 characters in length with characters from three of the following choices: uppercase letters, lowercase letters, numbers, and special characters.
2) **Forced Minimal Protocols Required** (least functionality) - Only the minimal required protocols (least functionality) under a normal operation are configured while Enhanced Security Mode is selected. To enabled non-required protocols, Enhanced Security Mode must be disabled.

Enhanced Security Mode shall be enabled. This setting may be changed from the Security overview page (see Security overview page).

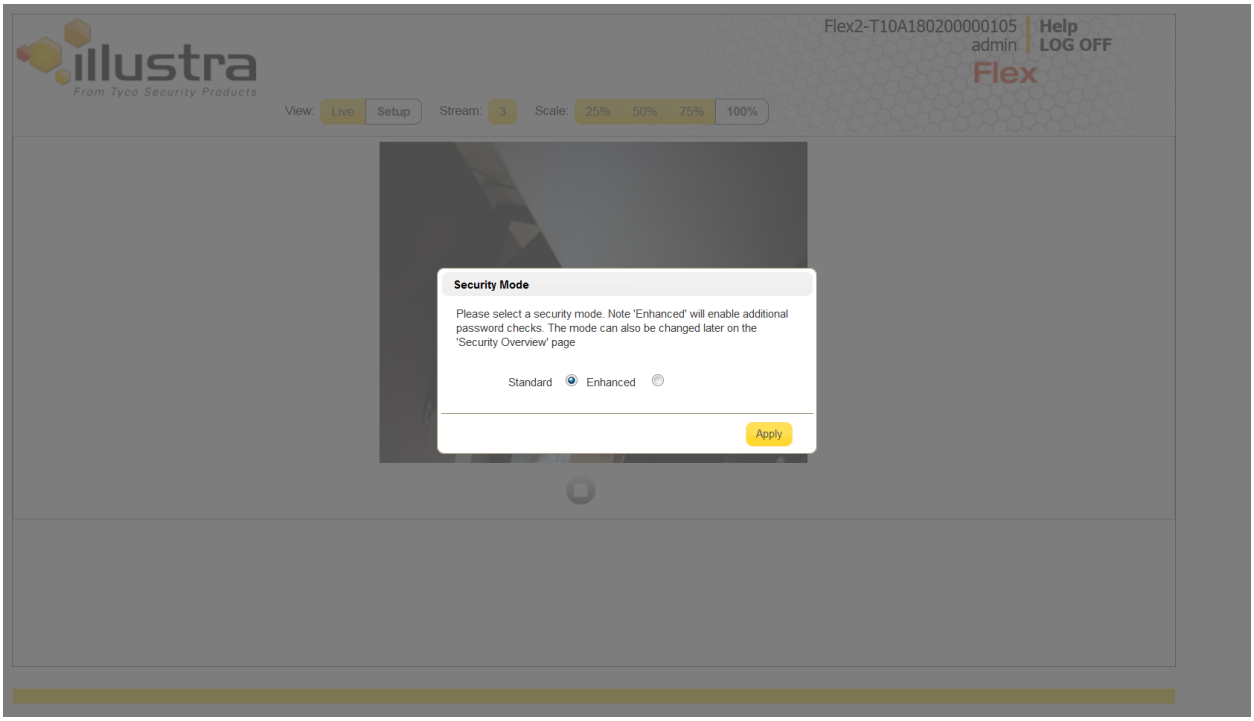
Users should not utilize default credentials as this allows malicious users to successfully guess the password and gain unauthorized access to the camera.

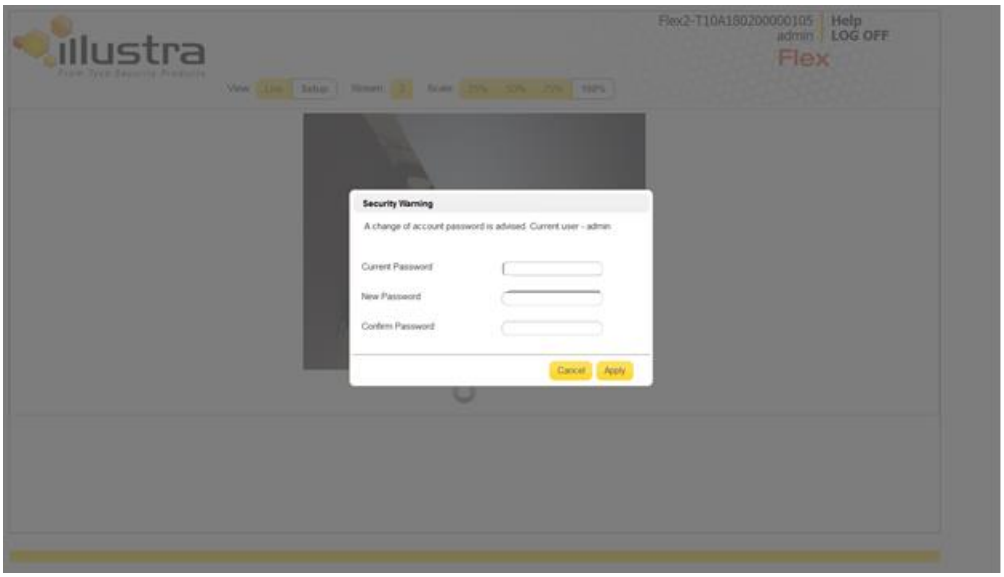






If the Standard Security Mode is selected, a security warning will recommend an update to the default password.




illustra
Flex2-T10A180200000105
admin
Help
LOG OFF
Flex
Security Warning
A change of account password is advised. Current user - admin
Current Password
New Password
Confirm Password
Cancel
Apply

Security Overview Page

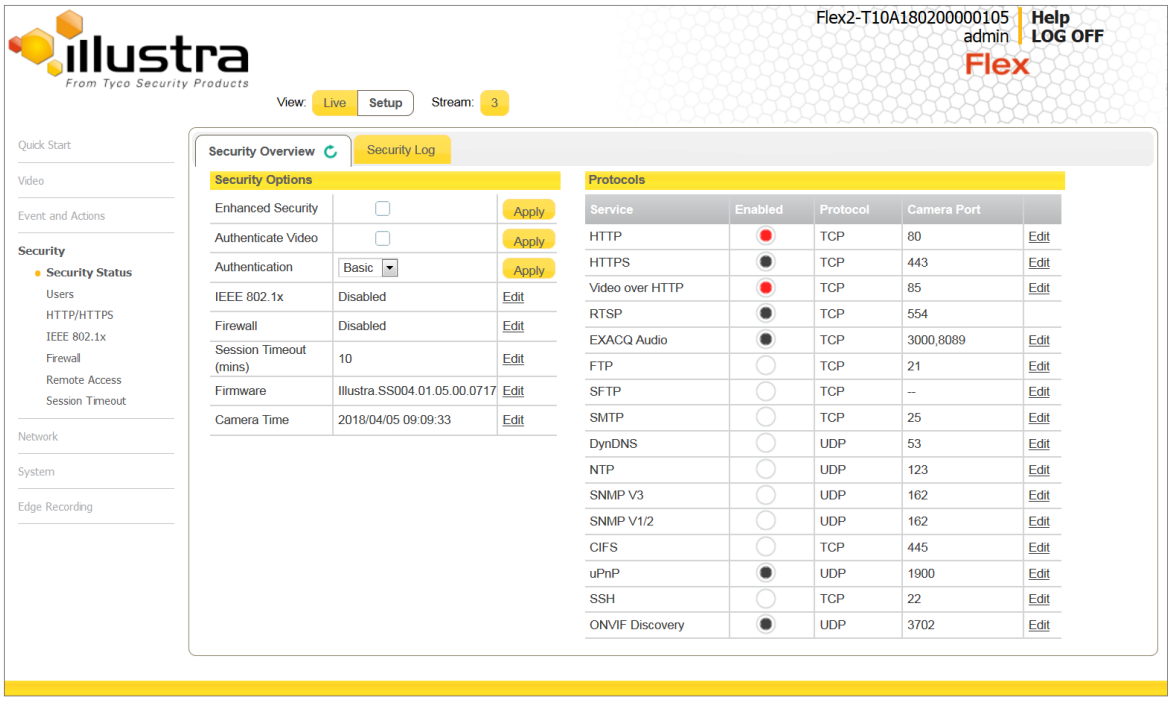
Illustra cameras contains a security overview page. The security status of the camera is provided on this page, which includes security options and protocols.

> **NOTE**: The full list is also provided in the Illustra port document located on the Cyber Protection website.

Protocols

The security overview page is a simple capture of services, protocols, and port number information. Only the minimal required protocols (least functionality) under a normal operation are configured while Enhanced Security Mode is selected. To enabled non-required protocols, Enhanced Security Mode must be disabled.

> **NOTE**: A red radio button indicates the enabled protocol is insecure and an alternative method of communication should be used.



NOTE: Services not required for normal operation or integration should not be enabled.

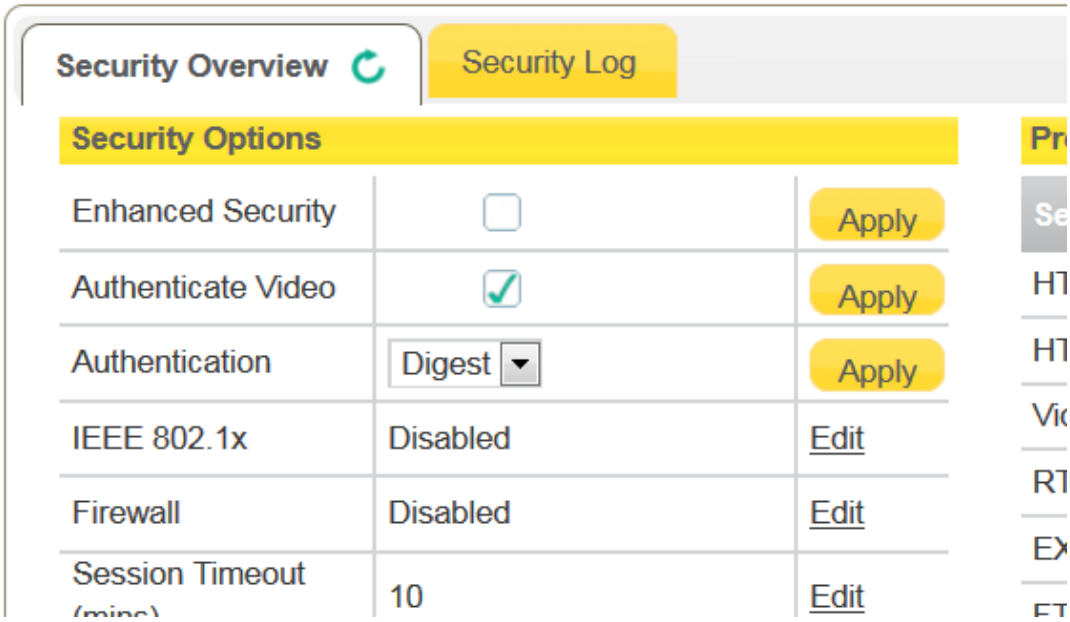
To disable or enable a protocol simply click on the Edit button, and you will be redirected to the protocol specific page where the enable/disable button is located.

Security Options

Enhanced Security – The Enhance Security mode may be enabled/disabled. (See Operational: Enhanced Security Mode for more details).

Authenticate Video - The video camera to network video recorder RTSP communications may be authenticated. To enable RTSP authentication, click the Authenticate Video checkbox on the Security Overview page, then click apply.

Authentication – The type of authentication used for RTSP communications is presented here when Authenticate Video is enabled.. To enable RTSP digest authentication, select Digest in the dropdown under authentication on the Security Overview page.



The Digest authentication means that the username and password being passed in the RTSP authentication of the video is not passed in clear text. Basic authentication does not protect the transmission of the username and password and is not recommended.

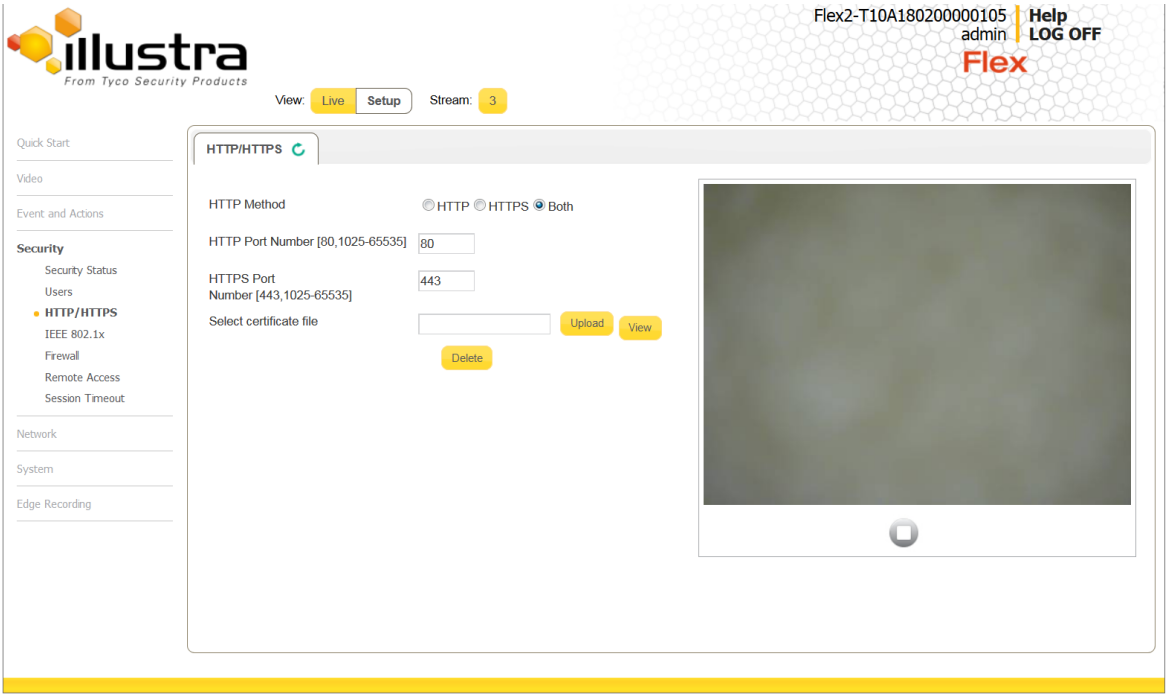
Encrypted Communications

Illustra cameras have the ability to operate as HTTPS only. It is recommended that the camera be enabled to work as HTTPS only.

HTTPS is the secure method of HTTP, which means that browser data will be encrypted.

The camera only supports TLS v1.2 with minimum of 256 bits of encryption. The full list of supported ciphers is located in the Annex.

By default, the camera is provided with a certificate signed by American Dynamics Inc. The certificate can be updated, as this self-signed certificate is not recognized by any modern web browsers.



To update the SSL certificate

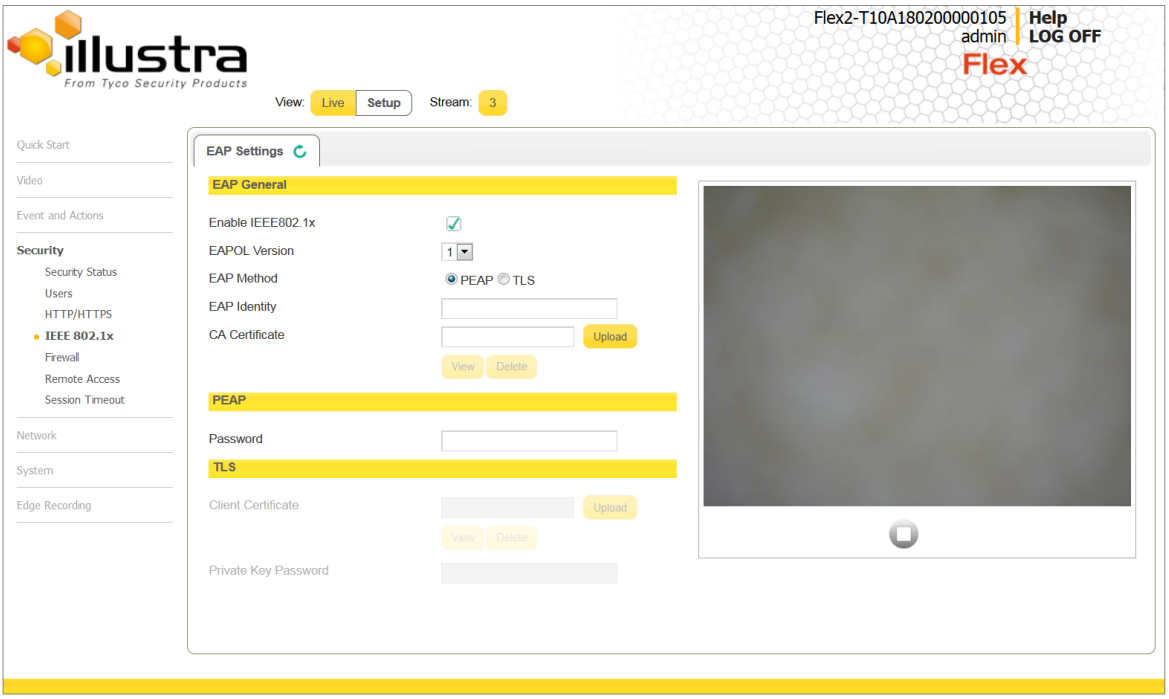
1. Select **Setup** on the Web User Interface banner to display the setup menus.
2. Select **HTTP/HTTPS** from the **Security** menu.
3. Click on the **Upload** button and navigate to the certificate location.
4. Select the file and click **Open.**

NOTE: The camera only accepts .pem format certificates.

The certificate must have the server certificate and private key combined, and the private key must NOT be password protected.

IEEE 802.1X

IEEE 802.1X is an IEEE Standard for Port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.



1. Filling Out the Form
    a. Basic Settings
        i. To enable the IEEE 802.1X, choose ON from the drop down menu.
            1. If you do not need the IEEE 802.1X security, leave in OFF configuration. The rest of the configuration is related only to IEEE 802.1X security requirements.
        ii. EAPOL version can either be a 1 or 2, choose the appropriate number.
            1. EAPOL is Extensible Authentication Protocol over LAN.
        iii. EAP Method shall stay at TLS. EAP is an authentication framework providing for the transport and usage of keying materials and parameters generated by EAP methods.
        iv. EAP Identity is a text field in which any comments related to the 802.1X security can be entered.

b. PEAP
    i. PEAP stands for password extensible authentication protocol.
    ii. If your EAP requires a password, the password should be entered in the text box.
c. EAP-TLS
    i. Browse to the CA certificate using the Windows navigation, and click Open. Once you have located the certificate, click on the certificate to be installed and press the Open button, this will upload the certificate.
        1. The CA certificate is a digital certificate from a certificate authority. The digital certificate certifies the ownership of a public key by the named subject of the certificate.

    ii. Browse to the Client certificate using the Windows navigation and click Open. Once you have located the certificate, Once you have located the certificate, click on the certificate to be installed and press the Open button, this will upload the certificate.
        1. The Client certificate is the digital certificate belongs to the client in a HTTP connection. The client certificate verifies itself to the requesting server.
    iii. PEM encoded file including certificate and private key will be displayed in the text box below.

Firewalls

ICMP Blocking

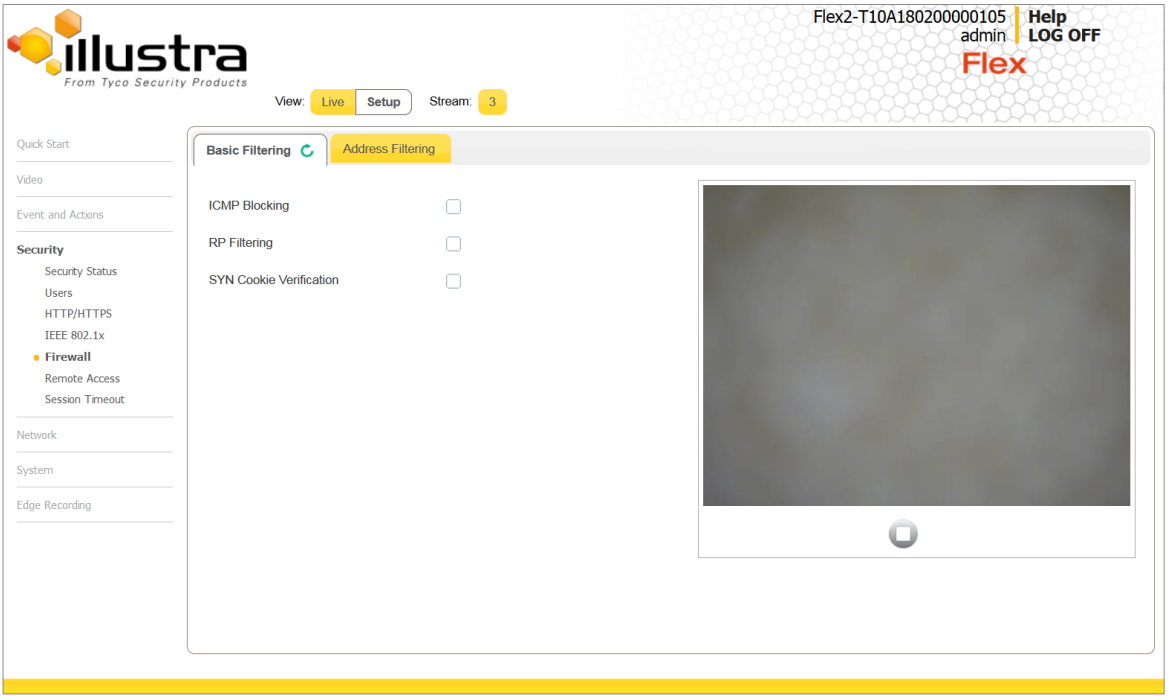
ICMP stands for internet control message protocol. By enabling ICMP blocking, you disable the ability for a host to indicate if the camera is online using methods such as a 'ping test'.

RP Filtering

RP Filtering stands for reverse path filtering. This protection will disallow packets which 'obviously' do not belong on the network from interacting with the camera. If the camera has an IP address of 10.10.10.2 and RP filtering is enabled, you would not allow packets from 192.168.1.3 to work with the camera.

SYN cookie verification

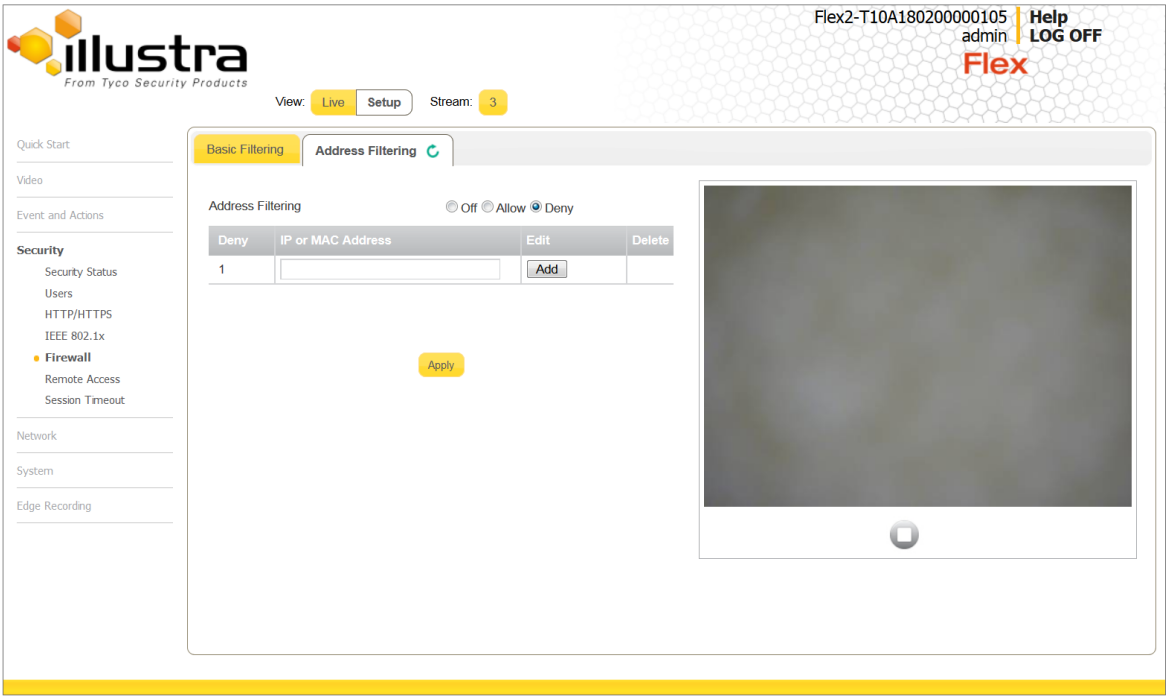
The TCP handshake sequence is SYN -> SYN-ACK -> ACK. TCP is a lower level of communication used by computer devices. SYN cookie verification confirms that the next step in a TCP handshake is correct to prevent a SYN flood attack.



Address Filtering

The camera can restrict communication to only specific IP addresses. This ability to restrict access to allowed IP addresses is known as a "whitelist." Attention must be paid in entering addresses. If the addresses are entered incorrectly, access to the camera can become completely locked out.

The "deny" option is a "blacklist". This list disallows particular IP addresses from connecting to the camera.


illustra
From Tyco Security Products
Flex2-T10A180200000105
admin
Help
LOG OFF
Flex
View:
Live
Setup
Stream:
3
Quick Start
Video
Event and Actions
Security
Security Status
Users
HTTP/HTTPS
IEEE 802.1x
Firewall
Remote Access
Session Timeout
Network
System
Edge Recording
Basic Filtering
Address Filtering
Address Filtering
Off
Allow
Deny
Deny
IP or MAC Address
Edit
Delete
1
Add
Apply

Remote Access Protocols

The camera has the ability to allow or disable remote access. When enhanced security mode is enabled, these are off by default.

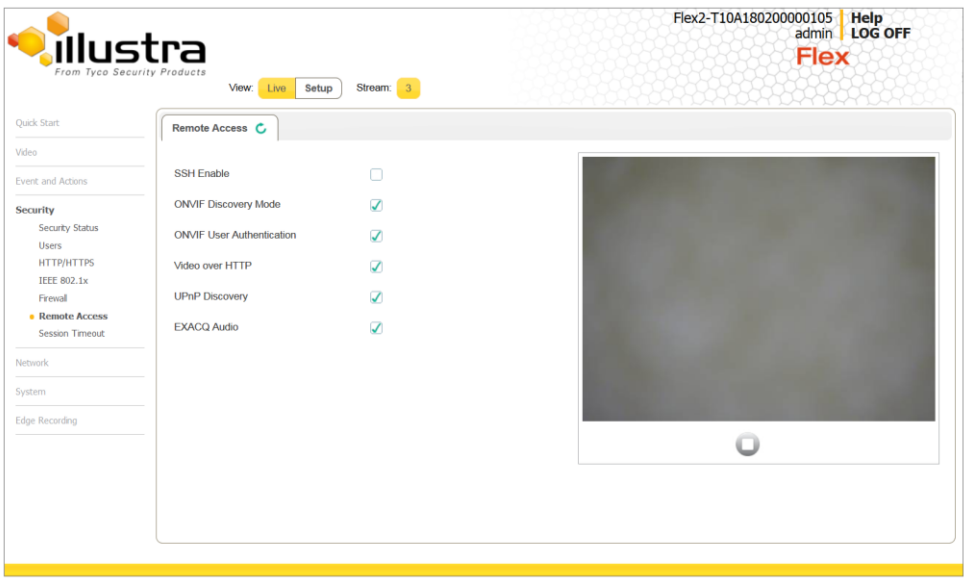
SSH: Secure Shell, this protocol is only used by Tyco technical support.

ONVIF: This is a discovery protocol for an industry standard tool. It provides information about the camera and can be used to update information without using the webpage.

Video over HTTP: Video can be transmitted over HTTP rather than RTSP.

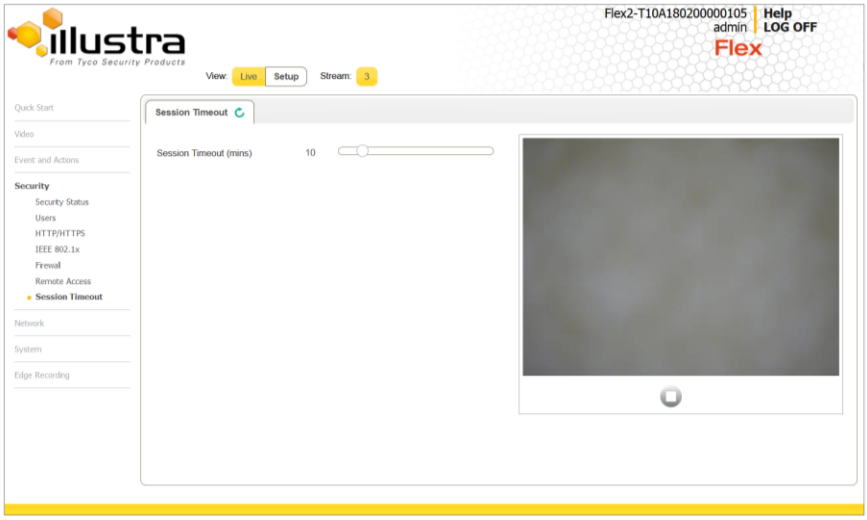
UPnP Discovery: This is a standard discovery protocol. Universal Plug and Play(UPnP) is a set of networking protocols that permits networked devices, such as personal computers, printers, Internet gateways, Wi-Fi access points and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and entertainment.

EXACQ Audio: This is used for output audio connections to Exacq recorder.



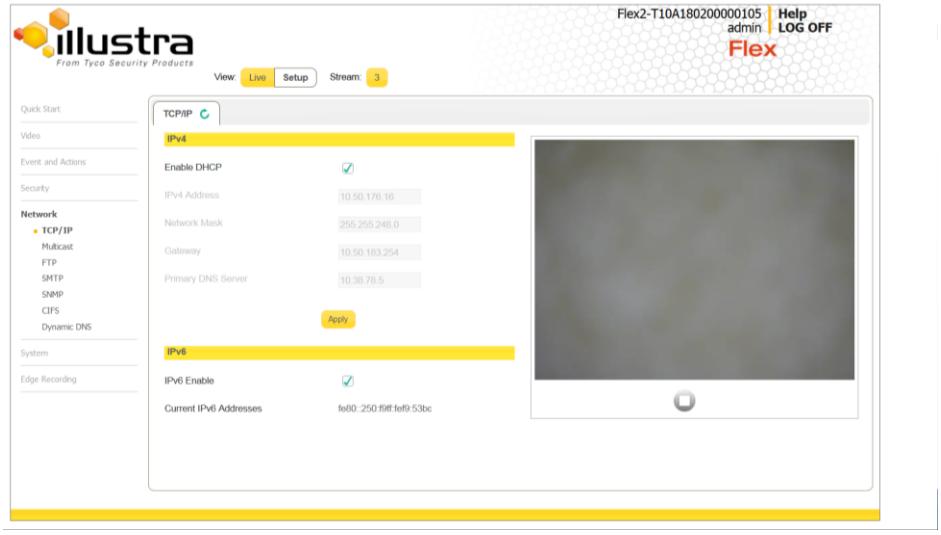
Session Timeout

The camera will log out if there is no user activity based on a configurable amount of time.



IPv6

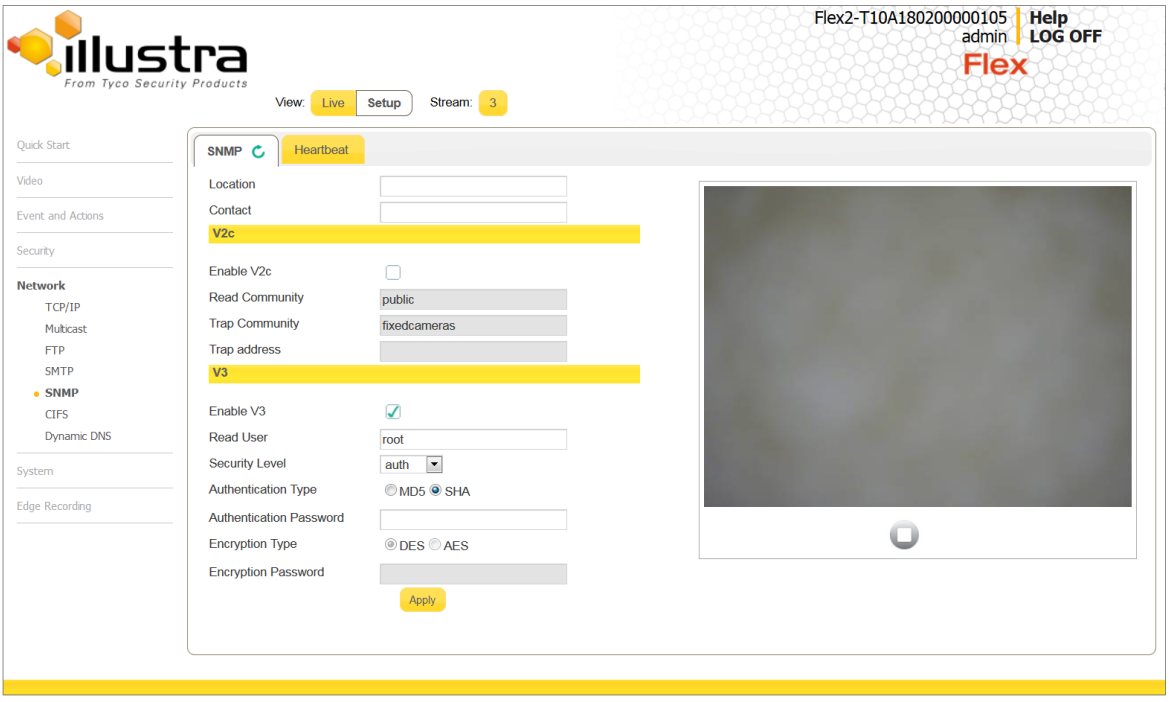
The camera supports IPv6, which is the most recent version of the internet protocol. If the network supports, the camera should be set to use IPv6. The IPv6 implementation in Illustra cameras supports the mandatory inclusion of IPsec, which increases the level of security on network traffic.



SNMP

The camera supports Simple Network Management Protocol (SNMP) version 3 and version 2c. If SNMP is preferred by network administration policies within the video camera network, it should utilize SNMP version 3 only. If SNMP is not required, it should not be enabled in the camera.

NOTE: The authentication type should be SHA and if encryption is required, AES is the recommended method. Please note that MD5 and DES are determined to be deprecated and should not be used for any secure communications.

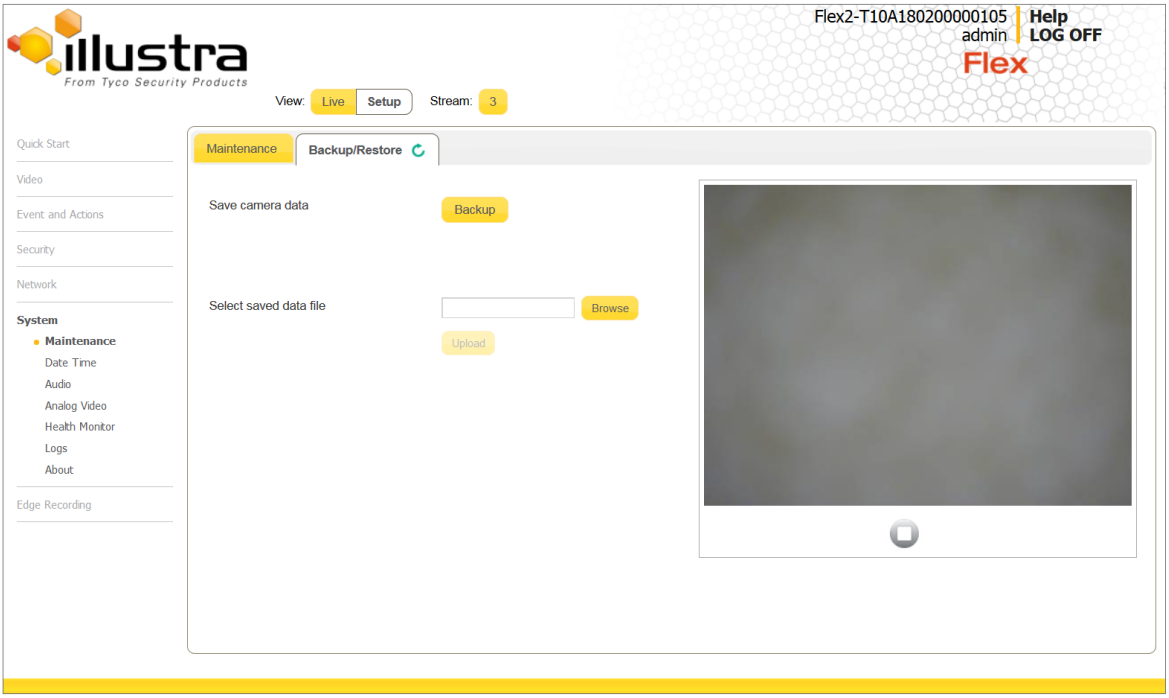


Backup and Restore

The camera should be backed up at a regular cadence. The advantage to performing regular backups and keeping them in a secure location is that if a compromise does occur, the camera can be returned quickly to its saved state.

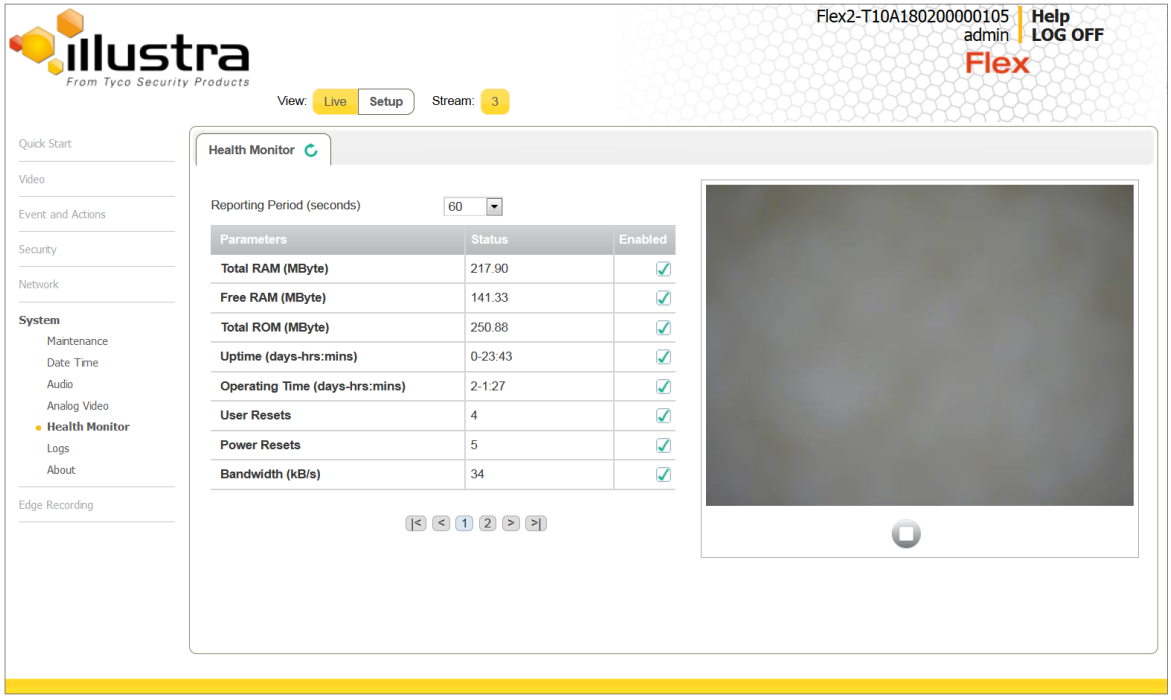
To perform a backup, navigate to the Backup page and press the Backup button. Please store the image in a safe location. Images are encrypted.

To perform a Restore, locate the file you wish to restore to and press Upload. Images are checked prior to upload, and only trusted and known good images can be restored.



Heath Monitor

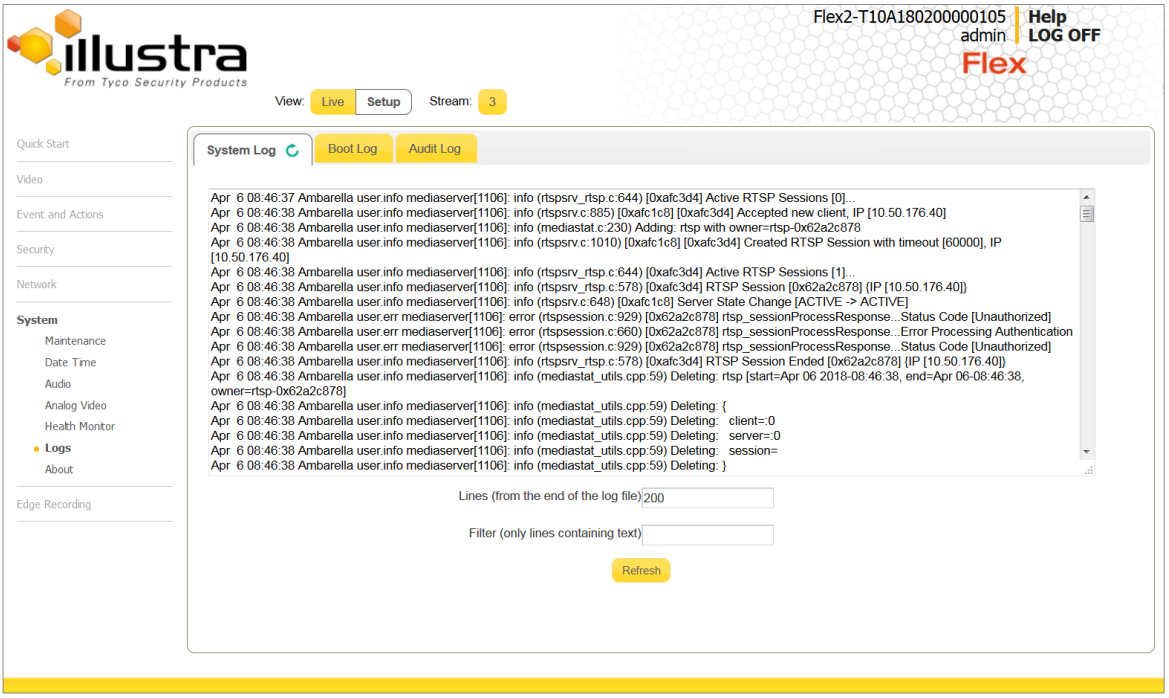
The Health Monitor is an enhancement that allows camera information such as uptime and operating time to be viewed in a single screen.



Logs

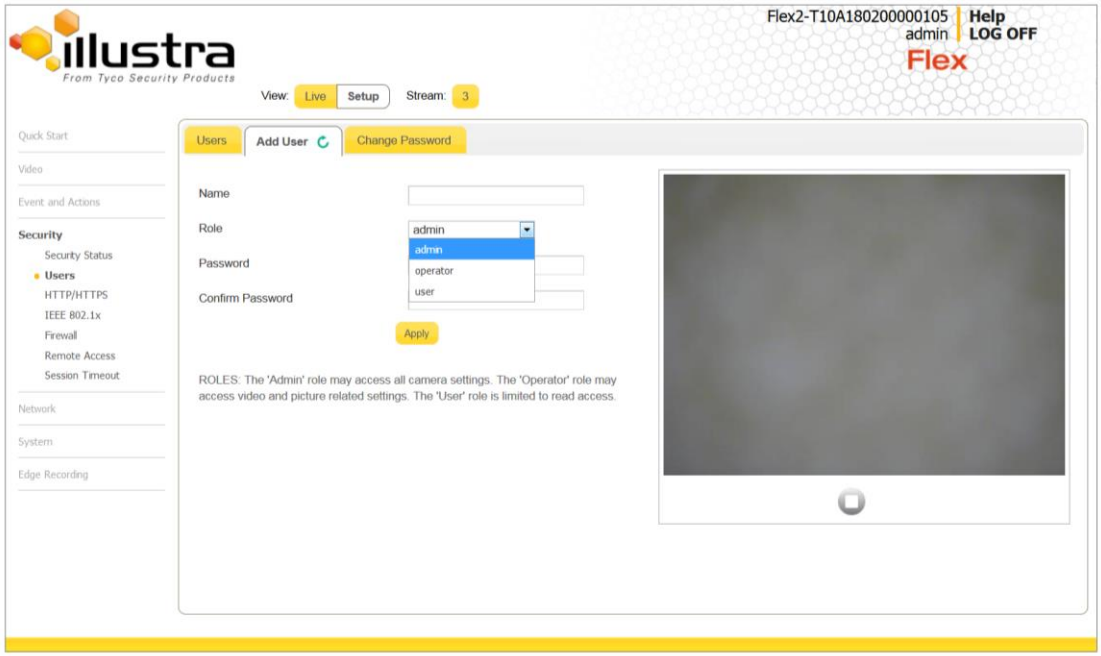
The Logs page provides system information on the camera. Items such as: users logged in, connections made, change in any security related features, new users created and passwords changed are recorded. These logs can be exported through SMTP or FTP for Security Information and Event Management (SIEM) reporting.

Review of logs allow for in-depth audit of the camera.



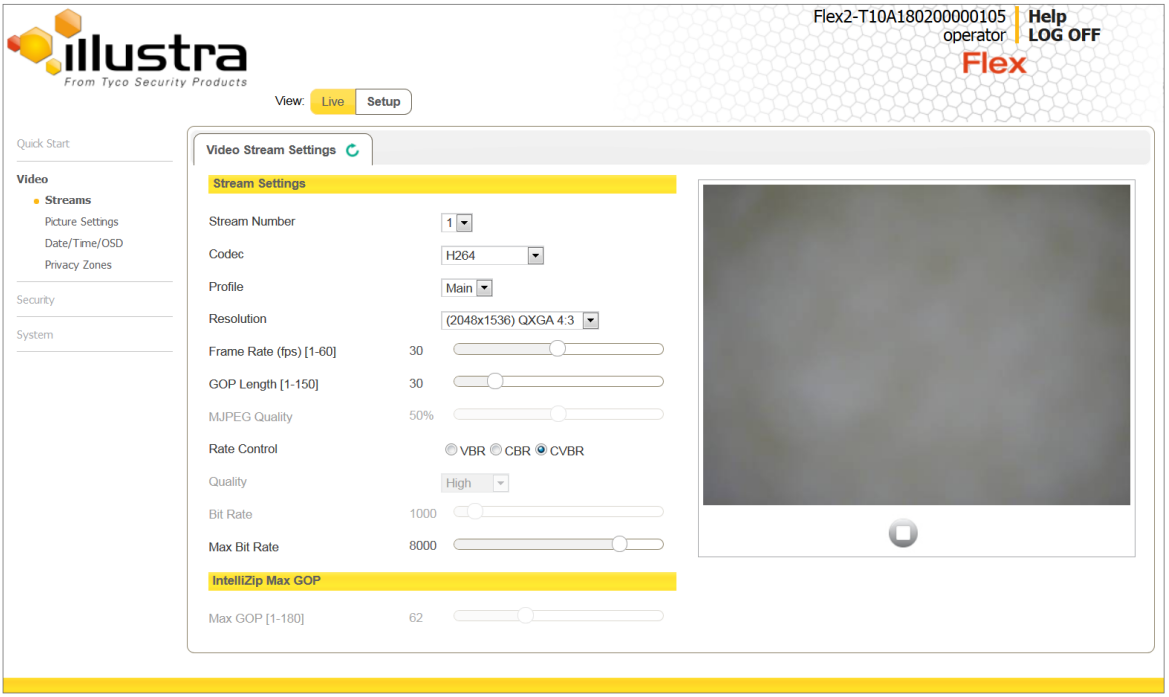
Separation of Roles

There are three levels of roles available on Illustra cameras: Admin, Operator and User.

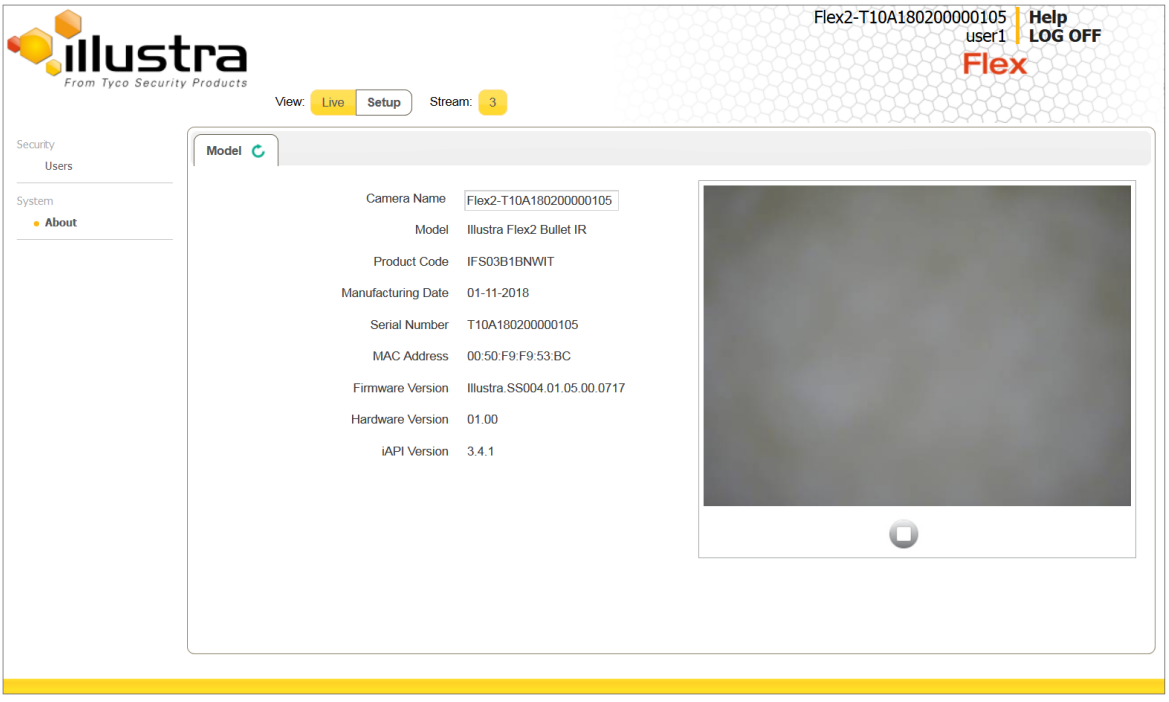


Admin – This user has full functionality of the camera, and care should be taken when assigning new admin users. The admin role has the ability to create and delete users, enable and disable protocols, and create or disable alerts.

Operator – This user only has the ability to change Video settings, picture settings and privacy zones.



User – The User only has the ability to view video.

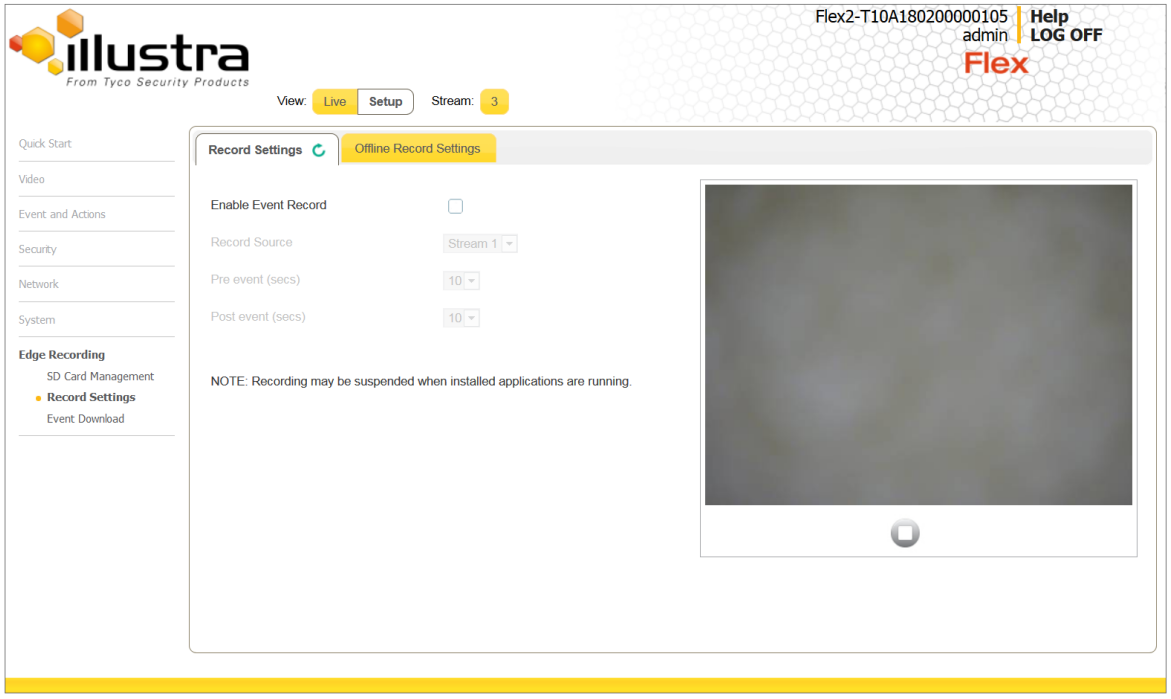


NOTE: It is important to only allow the user to perform the functions that are required for day-to-day operation.

Auditing of a user responsibility should be performed on a regular basis to prevent privilege creep.

High Camera Availability

The camera has a featured named Trickle-Store which allows for local storage of video to prevent the loss of recorded video if network video recorder connection is interrupted.



By utilizing SD card storage, if a network video recorder goes offline, the camera has the ability to record some amount of video internally.

For details on how to enable, refer to the user manual.

SUMMARY

- Enable Enhanced Security Mode
- Change all default credentials
- Perform firmware updates
- Only enable protocols required for normal operation
- Only allow HTTPS
- Keep a regular backup of the camera
- If required, utilize SNMPv3
- Configure Firewall settings
- Enable RTSP authentication with Digest
- Utilize 802.1X
- Update the SSL certificate and add it to a CA

MAINTENANCE

Vulnerability Management and Updates

The policy documented here sets forth the current internal operating guidelines and process for Illustra cameras, which may change from time to time at the sole discretion of Johnson Controls. Johnson Controls employs commercially reasonable efforts to pursue the operating guidelines and process described herein. However, other mitigating factors may prevent complete adherence to this policy, as determined by Johnson Controls at its discretion. Regardless, Johnson Controls endeavors to address issues that arise within Illustra cameras with the severity that they warrant.

Patch Policy

When CRITICAL security vulnerabilities are discovered within Illustra cameras, Johnson Controls will use commercially reasonable efforts to issue a Critical Service Pack for the current version of Illustra cameras as soon as is reasonably practicable.

When non-CRITICAL vulnerabilities are discovered within Illustra cameras, Johnson Controls will use commercially reasonable efforts to:

- Apply fixes for HIGH severity vulnerabilities in the next immediate release of Illustra cameras
- Apply fixes for LOW and MEDIUM vulnerabilities within one of the next two available releases of Illustra cameras

This policy is limited to commercial life of the product whereby Illustra cameras based on a particular hardware design or model are commercially available.

Note: Illustra cameras do not have a backport policy. Updates are only applied to latest version of the released product.

Firmware Update

Prior to installation, the camera shall be updated with the most recent firmware available on the website.

https://www.illustracameras.com

Release Schedule:

An update to Illustra cameras including new features and security fixes is released approximately every 6-8 months.

No updates to Illustra cameras will be released without undergoing extensive quality assurance testing.

Vulnerability Assessment – Illustra cameras

Vulnerabilities discovered in the proprietary software of Illustra cameras are assessed on the CVSS v3 score.

CVSS v3 Score	Assessment
≥ 9	Critical
≥ 7	High
< 7	Medium

Vulnerability Assessment – Third Party Software

Johnson Controls shall use commercially reasonable efforts to monitor third party and open source software included within Illustra cameras for disclosed vulnerabilities from the product vendors and open source communities. Vulnerabilities that are discovered and disclosed will be assessed, first on its assigned CVSS v3 score from the product vendor or the National Vulnerability Database, and then on the ability to be exploited within Illustra cameras.

CVSS v3 Score	Exploitability	Assessment
≥ 9	Exploitable	Critical
≥ 9	Not Exploitable	High
≥ 7	Exploitable	High
≥ 7	Not Exploitable	Medium
< 7	Exploitable	Medium
< 7	Not Exploitable	Low

If a patch is not available to correct the vulnerability, Johnson Controls will use commercially reasonable efforts to mitigate the vulnerability within its capabilities.

Reporting a Vulnerability

To better protect our customers and honor the trust they put in us, we are firm believers in responsible coordinated disclosure. Security Researchers, consultants and others who believe they may have found a potential security vulnerability in a Security Product can make immediate notice to our Cyber Protection Team through email to TSPCyberProtection@tycoint.com or via the Building Products Vulnerability Reporting webpage to make immediate notice to our Product Security Incident

Response Team (PSIRT).

Those working directly on behalf of a Tyco security solutions' customer should also notify their local Tyco security solutions representative. Thank you for your partnership with us in creating a smarter, safer more sustainable world

Additionally, Technical Support staff have direct access to the Cyber Protection team to help assess and resolve any issues.

PENETRATION TESTING

As part of its commitment to the Product Security Program, Illustra cameras receive regular vulnerability and penetration testing from our internal product security engineers. However, Illustra cameras are also subjected to third party penetration testing annually and at milestone releases.

Performing Penetration Testing

If you require penetration testing to be performed on Illustra cameras, the Cyber Protection Team is available to assist where possible including consultation and response directly to the testing team. For assistance, reach out to TSPCyberProtection@tycoint.com

PRODUCT SECURITY TESTING

Illustra cameras regularly undergo repeated security tests during the development process including network vulnerability scans. Web application scans are done on a regular maintenance schedule. Web applications are also tested during development to identify flaws such as cross-site injection points and missing security flags. Proprietary code is analyzed during the development cycle for items such as buffer overflow points, null dereference points and memory leaks. Third party and open source code is continuously scanned to identify released security flaws.

Table: Product Security Testing[1]

Development Cycle	
Test	**Tool**
Vulnerability scanning	Nexpose, Nessus
Web application scanning	Rapid7 AppSpider, BurpSuite professional, OWASP ZAP
Static code analysis – proprietary source code	SonarQube, HP Fortify
Static code analysis – open source code	Comparison against National Vulnerability Database (NVD), BlackDuck knowledge database

Release Cycle		
Test	**Tool / Method**	**Frequency**
Vulnerability scanning	Nexpose, Nessus	Weekly
Web application scanning	Rapid7 AppSpider, BurpSuite professional, OWASP ZAP	Monthly
Static code analysis – open source code	Comparison against National Vulnerability Database (NVD), BlackDuck knowledge database	Continuous

[1]A regular testing schedule for Illustra will apply during the actively supported period of the product's lifecycle. The frequency, tools and methods used are subject to change to accommodate the current best practices for cybersecurity, market conditions and tools available for a given period.

CERTIFICATIONS

Illustra cameras have undergone review by third party organizations resulting in the following certifications:

DHS SAFETY Act Designation – The technology of Illustra Cameras were included in a certificate of SAFETY Act Designation issued on March 19, 2018 by the United States Department of Homeland Security. This designation is described as follows:

March 19, 2018 – Johnson Controls International plc, Sensormatic Electronics, LLC, and Tyco International Management Company, provide VideoEdge, victor, and Illustra (the "Technology"). The Technology is a scalable video management system consisting of video recorder hardware and management software supporting the integration of

cameras and third-party devices, enabling management through a single interface. This Designation will expire on April 30, 2023.

ANNEX A – PORT ASSIGNMENTS FOR ILLUSTRA CAMERAS

For port assignments see Illustra Port Assignments document.

ANNEX B – ENCRYPTION CIPHERS

- The minimum supported encryption key strength in Illustra cameras is 256 bits.
- Export ciphers are disabled by default.
- RC4 cipher is disabled by default.

Supported ciphers

TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve P-256 DHE 256

TLSv1.2 256 bits ECDHE-RSA-AES256-SHA384 Curve P-256 DHE 256

TLSv1.2 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256

TLSv1.2 256 bits DHE-RSA-AES256-GCM-SHA384 DHE 1024 bits

TLSv1.2 256 bits DHE-RSA-AES256-SHA256 DHE 1024 bits

TLSv1.2 256 bits DHE-RSA-CAMELLIA256-SHA DHE 1024 bits

TLSv1.2 256 bits AES256-GCM-SHA384

TLSv1.2 256 bits AES256-SHA256

ANNEX C – EVENTS

To setup alerts, see Illustra *User Guide*.

Event Actions	Description
Output	The camera can enable an output for local event action
Record	Event to record upon fault action will be enabled
Email	Email notification of fault
FTP	FTP upload of fault notification
CIFS	Common Internet File System upload of fault notification

Analytics	Description
ROI	A region of interest is a defined area of the camera view which considered to be higher priority than areas of non-interest
Motion Detection	Motion detection enables you to define a region of interest in the camera's field of view which can be used to trigger an Event Action
Blur Detection	The camera generates an alarm and then takes the action you specified during configuration when the Blur Detection feature is enabled and the camera detects incidents that make the video image blur, such as: redirection, blocking, or defocusing