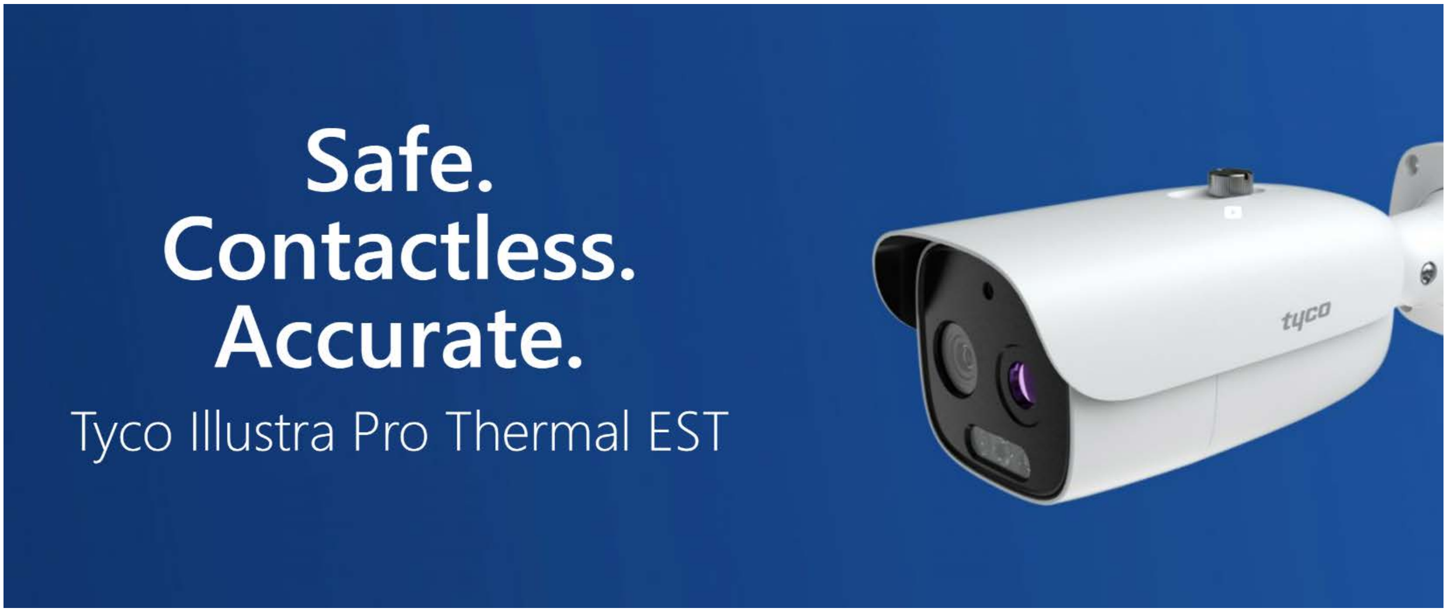
tyco | Illustra

Illustra Pro Thermal EST Hardening guide



GPS0005-CE-20200619-EN
Rev A

Johnson Controls

Contents

Introduction 5

Legal disclaimer 6

1 Planning 7

1.1.0 Illustra overview 7

1.1.1 Deployment architecture 7

1.1.2 Supporting components 8

1.1.2.1 NVR 8

1.1.2.2 Web Browser 8

1.1.2.3 Switch 8

1.2.0 Security feature set 8

1.2.1 User accounts 8

1.2.2 User password policy 8

1.2.3 User authentication 9

1.2.4 User authorization 9

1.2.5 Digital certificate management 9

1.2.6 Encryption/hash algorithms 9

1.2.7 Logs 9

1.2.8 Alarms and alerts 9

1.2.9 Availability assurance 9

1.2.10 Software updates 9

1.2.11 Encryption ciphers 9

1.2.12 Timely response to events 10

1.2.13 Resource availability 10

1.3.0 Intended environment 10

1.3.1 Internet connectivity 10

1.3.2 Integration with IT networks 10

1.3.3 Integration with external systems 10

1.4.0 Patch policy 10

1.5.0 Hardening methodology 11

1.6.0 Communication paths table 11

1.7.0 Bandwidth requirements table or calculator 12

1.8.0 Network planning 12

1.9.0 Hardware and software requirements 12

2 Deployment 12

2.1.0 Deployment overview 12

2.1.1 Getting started 13
2.1.2 Physical installation considerations 13
2.1.3 Default security behaviour 13
2.1.4 Resetting factory defaults 13
2.1.5 Knowledge level 13
2.2.0 Hardening 13
2.2.1 Hardening checklist 13
2.2.2 Administration 13
2.2.2.1 Security 14
2.2.2.2 Network 14
2.2.2.3 Maintenance 14
2.2.3 User management overview 14
2.2.4 User management best practices 14
2.2.4.1 No shared accounts 14
2.2.4.2 Least privilege 15
2.2.4.3 Separation of duties 15
2.2.4.4 Strong passwords 15
2.2.4.5 Password policy 15
2.2.5 User management 15
2.2.5.1 OS level accounts 15
2.2.5.2 Local application user accounts 16
2.2.5.3 Password policy configuration 16
2.2.5.4 Change default password 16
2.2.5.5 Assign roles 16
2.3.0 Communication hardening 16
2.3.1 Least functionality 16
2.3.2 Encrypted communications 16
2.3.3 Communication port configuration 16
2.3.3.1 Firewall/router configuration 16
2.3.3.2 Network isolation 16
2.3.4 Communication certificate support 17
2.3.5 802.1X. Configuration 17
2.4.0 Configuring security monitoring features 17
2.4.1 Logs 17
2.5.0 Availability hardening 17
2.6.0 Privacy considerations 18

3 Maintain 19

3.1.0 Cybersecurity maintenance checklist 19

3.1.1 Backup configuration data 20

3.1.2 Test backup data 20

3.1.3 Disable accounts on termination of employment 20

3.1.4 Remove inactive user accounts 20

3.1.5 Update user account roles and permissions 21

3.1.6 Disable unused features, ports and services 21

3.1.7 Check for and prioritize advisories 21

3.1.8 Plan and execute advisory recommendations 21

3.1.9 Check and prioritize patches and updates 21

3.1.10 Plan and execute software patches and updates 21

3.1.10.1 Update process 21

3.1.11 Review organizational policy updates 22

3.1.12 Review updates to regulations 22

3.1.13 Update as-built documentation 22

3.1.14 Conduct security audits 22

3.1.15 Update password policies 22

3.1.16 Update as-build documentation 22

3.1.17 Update standard operating procedures 22

3.1.18 Monitor for cyber attacks 23

3.2.0 Patch policy 23

3.3.0 Release schedule 23

3.4.0 Recovery and factory reset 23

3.5.0 Illustra testing process 23

3.5.1 Vulnerability assessment 24

3.5.2 Vulnerability assessment – third party components 24

3.6.0 Illustra vulnerability reporting 24

Introduction

Our solution provides peace of mind to our customers with a holistic cyber mind set 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 Hardening Guide intends 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 ensure that cybersecurity is considered throughout the planning, deployment and maintenance phases associated with a solution’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.

Legal disclaimer

The cybersecurity practices described in this guide are recommended practices to facilitate the secure installation and configuration of the products described herein. However, Johnson Controls cannot guaranty that the implementation of the cybersecurity practices or recommendations described in this guide will ensure the security of the relevant product or system, or prevent, or alter the potential impact of, any unauthorised access or damage caused by a cybersecurity incident. This guide is provided “as is”, and Johnson Controls makes no representation or warranty, express or implied, as to the efficacy of the cybersecurity practices or recommendations described in this guide. Johnson Controls disclaims all liability for any damages that may occur as a result of, or despite, reliance on this guide or compliance with any cybersecurity practices or recommendations set forth herein.

1 Planning

Use this section to plan for deployment functions including:

- How to assure compliance with the cybersecurity criteria that governs the target environment.
- How to design the deployment architecture.
- Reference for settings made during deployment.

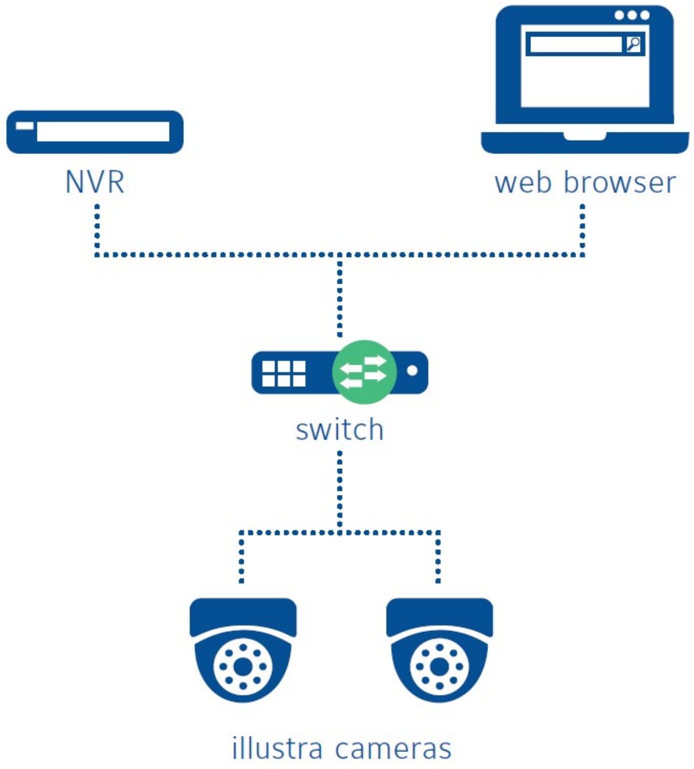
1.1.0 Illustra overview

Illustra cameras are Internet Protocol (IP) video surveillance devices that use Ethernet communications. Use Illustra IP cameras in retail locations for loss prevention, schools and hospitals to protect the safety of students and patients, and to assist governments to protect high-risk environments such ports and borders.

Illustra IP cameras integrate seamlessly with victor clients and VideoEdge NVRs. The native support in victor and VideoEdge means you can access video and audio using high-performance streaming and leverage its most advanced features including motion meta-data.

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

1.1.1 Deployment architecture



Product offerings and specifications are subject to change without notice.

1.1.2 Supporting components

Johnson Controls designed Illustra cameras to be a core component in a video surveillance system. Our cameras seamlessly integrate with Johnson Controls components but also work with third party components and systems.

1.1.2.1 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 Johnson Controls NVRs; VideoEdge and ExacqVision.

1.1.2.2 Web Browser

You can configure an Illustra camera through a web browser. See compatibly list contained with the datasheet for the supported web browsers. You can find this on the Illustra website, or on the camera web GUI. The camera's web GUI is called Illustra Connect. To download Illustra Connect navigate to the following link: https://illustracameras.com/software-downloads/

1.1.2.3 Switch

A network switch connects Illustra cameras to a network. It is best practice to segment the network to isolate video on a dedicated local area network (LAN) for both performance and security reasons. You can use a networking switch that has PoE ports to power Illustra models that support Power-Over-Ethernet (PoE).

1.2.0 Security feature set

- User accounts including roles
- User account management
- Password strength enforcement
- IP address whitelist or blacklist
- MAC address whitelist or blacklist
- Encryption
- Network protocol configuration
- Logging

1.2.1 User accounts

Illustra supports user accounts with varying levels of privilege. Each account is given a user type for separation of duties dependent upon the functionality required to perform necessary tasks. For more information on the benefits and best practices to observe see section 2.2.4.

1.2.2 User password policy

Illustra enforces strong passwords by default. Passwords must be 9 – 13 characters long and contain the following:

- Upper case letters
- Lower case letters
- Numbers
- Special characters.

After initial commissioning you may lower the required password strength, however it is advised that the strong password requirement is unchanged.

1.2.3 User authentication

User authentication requires a user name and password combination across all functions, by default, this includes video streaming. For unrestricted video streaming you may enable an anonymous log on session, which requires no user name or password, on the settings page.

1.2.4 User authorization

To control the level of user authorization, use the principle of separation of duties (see section 1.2.1) and divide accounts into user types. There are three levels of role, Admin, Advanced User, and User. See section 2.2.3.

1.2.5 Digital certificate management

The camera comes with a certificate signed by Tyco Security Products. You can update this certificate. Web browsers highlight self-signed certificates as insecure because they are inadequate for authentication. The certificates are valid for encryption purposes.

1.2.6 Encryption/hash algorithms

TLS v1.2 is supported with a minimum of 256 bits of encryption. The full list of supported ciphers is listed in Section 1.2.11.

1.2.7 Logs

Use the Logs page to access camera logs. The following logs are enabled by default: users logged in, connections made, change in any security related features, new users created, and passwords changed are recorded. Logs may also display events a user creates that use advanced features, for example, motion detection.

1.2.8 Alarms and alerts

You may implement alarms and alerts that correspond to user defined parameters. You can view alarms and alerts in the logs if the camera is paired with a compatible system.

1.2.9 Availability assurance

You can back up the camera configuration to a text file. To restore camera configuration, upload a valid configuration text file.

1.2.10 Software updates

To manually update the camera complete the following steps:

1. Open **Illustra Connect**.
2. Click on **Maintenance**.
3. Click on **Update**.

1.2.11 Encryption ciphers

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

Supported Ciphers

- TLSv1.2 256 bits ECDHE-RSA-AES265-GCM-SHA384, Curve P-256, DHE 256
- TLSv1.2 256 bits ECDHE-RSA-AES265-SHA384, Curve P-256, DHE 256
- TLSv1.2 256 bits ECDHE-RSA-AES265-SHA, Curve P-256, DHE 256

- TLSv1.2 256 bits DHE-RSA-AES265-GCM-SHA384, DHE 1024
- TLSv1.2 256 bits DHE-RSA-AES265-SHA256, DHE 1024
- TLSv1.2 256 bits DHE-RSA-CAMELLIA256-SHA, DHE 1024
- TLSv1.2 256 bits AES265-GCM-SHA384
- TLSv1.2 256 bits AES265-SHA384

1.2.12 Timely response to events

If integrated with a system that supports it alerts and events may be displayed immediately to operators of those systems. Email alert functionality and alarm output is also available.

1.2.13 Resource availability

Camera settings may be exported using the Backup and Restore page on Illustra Connect. Settings may also be restored on the page with a user supplied file that had been previously exported.

Video may be recorded on user supplied SD card as a response to events such as analytics triggers and alarm input. Additionally, if the camera is integrated with an NVR, video may be recorded by that device.

1.3.0 Intended environment

You can install Illustra cameras in a range of environments; including internal and externally to a building. It is important that a qualified installer provides and defines physical mounting and network infrastructure.

1.3.1 Internet connectivity

Illustra cameras do not need Internet connectivity to function, but need access to a local area network in order to avail of the full feature set.

1.3.2 Integration with IT networks

You may integrate Illustra cameras into standard IT deployments, but it is best practice to deploy Illustra systems and any supporting components to a dedicated and isolated network.

1.3.3 Integration with external systems

Integration with external systems is optional.

1.4.0 Patch policy

The policy documented here sets forth the current internal operating guidelines and process in regards to Illustra, 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 endeavours to address issues that arise within Illustra with the severity that they warrant.

When CRITICAL security vulnerabilities are discovered within Illustra cameras, Johnson Controls uses commercially reasonable efforts to issue a critical service pack for the current version of Illustra cameras as soon as is reasonable practical.

When non-CRITCIAL 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 the latest version of the released product.

1.5.0 Hardening methodology

Illustra has many onboard security safeguards, including many secure-by-default settings. However Johnson Controls recommends that the device is hardened according to the guidance outlined in section 2 Deployment. Generally a defence-in-depth strategy employing standard IT hardening methods and compensating controls as needed to complement the base security features of each component.

1.6.0 Communication paths table

Protocol	Function	Default State	Required	Configurable	Type	Default Port	Configurable Port Range
DNS	Automatic IP address configuration	Enabled	No	No	UDP or TCP	53	N/A
DDNS	Dynamic IP address mapping to hostname	Disabled	No	Yes	UDP or TCP	Dependent upon provider	N/A
TELNET	Reserved for Tyco technical support	Disabled	No	No	TCP	28	N/A
RTSP	Video streaming	Enabled	Yes	Yes	TCP or UDP	554	1 – 65535
UPnP	Automatic IP discovery and setup	Enabled	Yes	Yes	TCP or UDP	1900	N/A
SMTP	Sending of security events	Disabled	No	Yes	TCP	25	10 – 65535
FTP	Sending of events and event triggered video captures	Disabled	No	Yes	TCP	20	0 – 65535
HTTP	Communication to the Web GUI	Enabled	Yes	Yes	TCP	80	1 – 65535
HTTPS	Secure communication to the Web GUI	Disabled	No	Yes	TCP	443	1 – 65535
Data Port (Proprietary)	Upload AI events such as facial image to a third Party VMS	Disabled	No	Yes	TCP	9008	1 – 65535
Persistent connection (Proprietary)	For viewing audio/video stream on the web GUI (plugin version)	Disabled	No	Yes	TCP	8080	1 – 65535

1.7.0 Bandwidth requirements table or calculator

Bandwidth requirements depend on the video settings applied to the camera and on the number of cameras installed.

A bandwidth calculator is available at the following:
https://tycosecurityproducts.com/calculators/ipconfig/index.html

1.8.0 Network planning

A qualified provider must install and design the network infrastructure tailored to the specific needs of the customer.

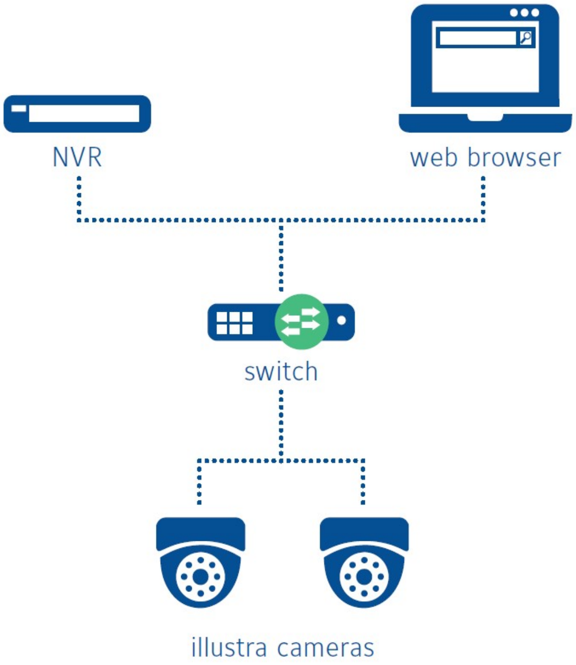
1.9.0 Hardware and software requirements

For basic operation the user must have access to a web browser, a list of supported browsers may be found at the Illustra website, www.illustracameras.com. The hardware requirements for any one browser are vendor specific.

2 Deployment

Use this section to initiate secure deployment for new installations, harden Illustra and complete additional steps after commissioning required before turning over to runtime operations.

2.1.0 Deployment overview



2.1.1 Getting started

Before you install Illustra, consider the guidance outlined in the following sections.

2.1.2 Physical installation considerations

Install the software using the instructions provided in the installation guide.

Note: The physical access to the device and physical installation of the device can impact the cybersecurity.

2.1.3 Default security behaviour

On initial start-up a standard login page appears. Use the login page to access the camera using the default credentials.

At this point the operator must change the default password. Password restrictions ensure password strength. Only Strong passwords are accepted.

2.1.4 Resetting factory defaults

If the camera was previously used as part of another installation or test environment it must be reset to factory defaults before redeployment. To reset the camera complete the following steps:

1. Open **Illustra Connect**.
2. Click **Maintenance**.
3. Click **Backup and Restore**.

There is also a hardware reset button. See Section 3.4.0 for further details.

2.1.5 Knowledge level

The operator must have Illustra administration and networking technologies experience.

2.2.0 Hardening

While the camera has several secure-by-default safeguards. To meet the security requirements of the target environment, harden the Illustra camera.

2.2.1 Hardening checklist

To harden this product, complete the following tasks:

- Perform firmware updates
- Only enable protocols required for normal operation
- Keep a regular backup of the camera
- Configure Firewall settings
- Use 802.1X
- Update the SSL certificate and add it to the CA
- Follow best practise for user accounts, see Section 2.2.3

2.2.2 Administration

To administer settings complete the following steps:

1. Open **Illustra Connect**.
2. Log on as an administrator.

There are three main areas, Security, Network, and Maintenance.

2.2.2.1 Security

To create user accounts, complete the following steps:

1. Open **Illustra Connect**.
2. Click **Security**.
3. Click **User**.
4. To view users logged on to the camera click **Online User**.

Use block and allow lists to blacklist or whitelist IP or MAC addresses.

Click Security Management to set the password strength and expiration. For non-administrative users this is set to **Medium** with a password expiration of **Never**. Increase the password strength for non-administrative users to **Strong**.

2.2.2.2 Network

To change network settings complete the following steps:

- Click **Network**.
- To change general IP settings click **TCP/IP**.
- To view the range of network protocols click **More…**.

2.2.2.3 Maintenance

Use the Maintenance to configure backup and restore functionality, apply upgrades, and to view and download logs.

2.2.3 User management overview

Create unique user accounts for each operator of the camera. A role-based access control (RBAC) feature set controls operator functions. With RBAC, a user is assigned a role in which they acquire the permissions associated with that role.

There are three user roles, admin, advanced user, and user.

- Admin – This user has access to the full functionality of the camera only use admin roles when absolutely necessary. The admin role has the ability to create and delete users, change any camera or picture setting, and create or disable alerts.
- Advanced user – This user can change non-security based configuration. For example, video and picture settings.
- User – The user only has the ability to view video.

To ensure you follow security best practices configure individual user accounts properly. Best practices for account management are described in the next section.

2.2.4 User management best practices

To improve the security for Illustra follow best practices for managing user accounts, their credentials and authorizations (permissions).

2.2.4.1 No shared accounts

Do not use shared accounts. Each user or system entitled to access the camera must have individual login credentials. Adding separate accounts for each user ensures the principle of least privilege and separation of duties but also allows for finer granularity in logging and when paired with good System Information and Event Monitoring practices system administrators can detect potential issues.

2.2.4.2 Least privilege

Least privilege is when only the minimum necessary rights are assigned to a subject that requests access to a resource and should be in effect for the shortest duration necessary (remember to relinquish privileges). Granting permissions to a user beyond the scope of the necessary rights of an action means the user may obtain or change information in unwanted ways. Careful delegation of access rights can limit attackers from damaging a system. For example a user who needs to view a camera stream and change picture settings should not have administrative privileges, with which they can add or modify other user accounts. Following this practice reduces the potential for attacks, malfeasance, or accidental system damage.

2.2.4.3 Separation of duties

This is similar to but distinct from least privilege. Separation of duties involves creating accounts for specified purposes. For example, accounts with administrative access must not be used for common day-to-day tasks such as viewing video streams. Instead separate accounts should be used for these different tasks. This helps prevent attacks that take advantage of ongoing connections and allow event monitoring to more easily detect suspicious administrative actions.

2.2.4.4 Strong passwords

By default the camera enforces a strong password policy for administrative users and medium for non-administrative users. It is recommended that the strongest level is enforced. Strong passwords help to prevent attacks by making a password difficult to guess and to deny easy access to would-be attackers.

2.2.4.5 Password policy

While Illustra cameras include safeguards to prevent the use of weak passwords, it is recommended that an organizational password policy is defined and followed to educate operators on the benefits of a strong password and avoid common mistakes that can weaken security.

2.2.5 User management

You must have administrative privileges to manage users. To manage users complete the following steps:

1. Open **Illustra Connect**.
2. Click **User**.
3. Click **Security**.

You can now create or modify existing users and designate roles.

Use unique accounts during all phases of operation for Illustra. Installers, technicians, auditors and other deployment phase users should never share common user accounts to ensure a non-reputable audit trail of their actions.

2.2.5.1 OS level accounts

Only Johnson Controls Technical Support use OS level accounts.

2.2.5.2 Local application user accounts

A user with admin privileges manages local application user accounts.

2.2.5.3 Password policy configuration

Modify required password strength for non-administrative users on the Security Management page.

2.2.5.4 Change default password

The user is asked to change the default password once they log on to Illustra Connect.

2.2.5.5 Assign roles

Roles limit the actions a user can take. See Section 2.2.3. You can assign roles when you create a user.

2.3.0 Communication hardening

Communication hardening limits an attacker’s ability to gain access to Illustra. Attackers look for weaknesses in communication protocols, and unencrypted/unauthenticated communications. Implement the following techniques to harden the communication interfaces and the transmission of data.

2.3.1 Least functionality

Least functionality is a security measure designed to limit functions only to those that the target application and communication sessions require at a given time. When you apply least functionality when you configure components you reduce the attack surface and minimize the risk of a cybersecurity breach.

2.3.2 Encrypted communications

Encrypted communications help to stop attacks by preventing simple connection eavesdropping. See section 2.3.4 for instructions on how to enable this feature.

2.3.3 Communication port configuration

To configure communication ports, complete the following steps:

1. Open **Illustra Connect**.
2. Click the relevant tab.
3. Click **More…**.

By default the minimum number of ports for essential functionality are open. To maximize security it is advised not to enable additional ports unless necessary, and to enable encryption wherever possible.

2.3.3.1 Firewall/router configuration

To increase security use a firewall or router, dependent upon vendor, to restrict communications to known addresses. Alternatively, use address whitelisting/blacklisting supplied by Illustra. See section 2.2.2.1 for further details.

2.3.3.2 Network isolation

It is best practice to deploy Illustra cameras to an isolated network to restrict available communication paths and prevent access to the wider Internet. Consult with a network professional for advice on how to provide this within the deployment environment of the camera.

2.3.4 Communication certificate support

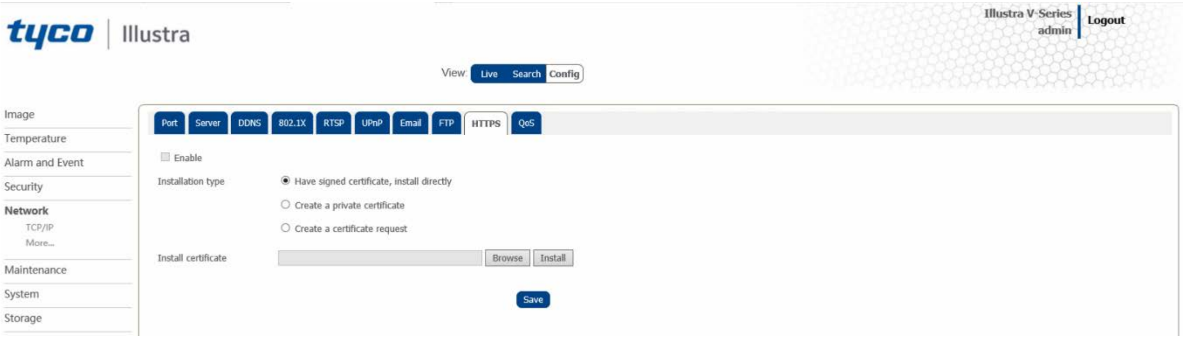
HTTPS encrypts web traffic, but does not verify the identity of the remote host without a properly configured digital certificate. Create a certificate that is unique to the individual camera so that your web browser or victor client can verify its identity. You may self-sign the certificate, or for more security-conscious customers, a trusted certificate authority can sign it.

To upload a certificate, complete the following steps:

1. Open **Illustra Connect**.
2. Click **Network**.
3. Click **HTTPS**.

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.



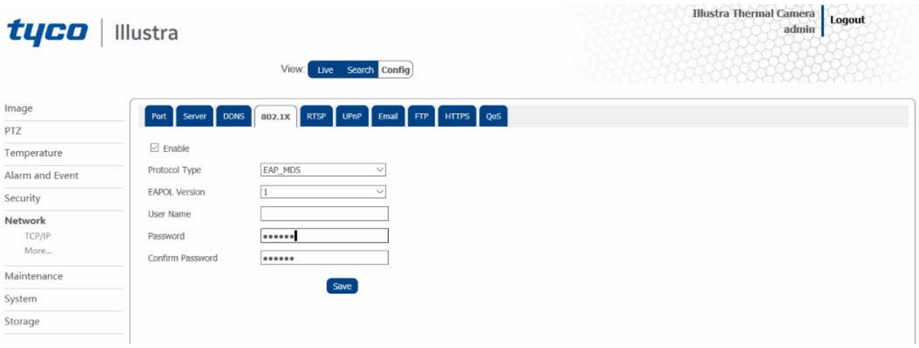
□ Enable

Installation type
● Have signed certificate, install directly
○ Create a private certificate
○ Create a certificate request

Install certificate

2.3.5 802.1X. Configuration

Configure 802.1X authentication through the relevant tab. The only EAP_MD5 is supported is EAPOL version 1.



☑ Enable

Protocol Type: EAP_MD5

EAPOL Version: 1

User Name:

Password: ••••••

Confirm Password: ••••••

2.4.0 Configuring security monitoring features

Illustra has logging capabilities.

2.4.1 Logs

Logs enable an operator to inspect the activity of an Illustra system, audit security of Illustra and monitor system events. Logging is enabled by default.

2.5.0 Availability hardening

Availability hardening is a process that ensures information the camera stores or creates is accessible. The Illustra backup and restore functionality supports availability hardening.

If you need to restore or replace a camera is important to have a backup of its configuration data to minimize the time it takes to restore functionality.

- To configure backup and restore settings click **Backup and Restore**.
- To download a settings file click **Export Settings**.
- To restore saved settings click **Import Settings**.

2.6.0 Privacy considerations

The capabilities and functionality of Illustra may require compliance by you or your organization with local, state, national and international laws and regulations. You or your organization are obligated to learn about and are solely responsible for compliance with all applicable laws and regulations relating to your use of those functions, including but not limited to those laws and regulations pertaining to personal data protection, privacy and security, any laws relating to the collection and sharing of personal data, including video and face detection with third parties, or any laws requiring notice to or consent of persons with respect to your use of the Illustra capabilities and functionalities.

3 Maintain

Use this section to monitor for potential cybersecurity issues and maintain protection levels as conditions change. Throughout the deployed lifetime of Illustra is it important to monitor and maintain it in addition to the network infrastructure it is deployed into.

An audit that produces a report indicating low cybersecurity risk is a very positive result and suggests that the deployment was conducted with a high degree of care and consideration. However, new attack vectors combined enhanced hacking tools and more advanced testing techniques may, in the future, disclose vulnerabilities with the technologies used.

The impacted technologies and their implementation may have been previously well regarded by cybersecurity experts. The discovery of vulnerabilities post the final deployment audit may not reflect the quality of the audit at the time.

You may require a higher degree of protection for Illustra's deployment environment as policies and regulations change over time.

3.1.0 Cybersecurity maintenance checklist

Continuously or periodically practise the following cybersecurity maintenance items. The frequency of their execution depends on the policies and regulations which govern the site. The following maintenance periods are a starting point. Adjust to best suit the target conditions of the deployed environment:

1	Backup configuration data	Quarterly (or as required)
2	Test backup data	Quarterly (or as required)
3	Disable user accounts of terminated employees	Immediately
4	Remove inactive user accounts	Monthly
5	Update user account roles and permissions	Quarterly
6	Disable unused features, ports and services	Quarterly
7	Check for and prioritize advisories	Weekly
8	Plan and execute advisory recommendations	Based on priority
9	Check and prioritize software patches and updates	Weekly
10	Plan and execute software patches and updates	Based on priority
11	Review updates to organizational policies	Annually

12	Review updates to regulations	Annually
13	Conduct security audits	Annually
14	Update password policies	Annually
15	Update as build documentation	As changes are made or annually
16	Update standard operating procedures	Annually
17	Renew licensing agreements	Annually (or as required)
18	Renew support contracts	Annually
19	Check for end-of-life announcements and plan for replacements	Quarterly
20	Periodically delete sensitive data in accordance to policies or regulations	As required
21	Monitor for cyber attacks	Continuously

3.1.1 Backup configuration data

If you need to restore or replace a camera is important to have a backup of its configuration data to minimise the time required to restore functionality.

- To configure backup and restore settings click **Backup and Restore**.
- To download a settings file click **Export Settings**.
- To restore saved settings click **Import Settings**.

3.1.2 Test backup data

Test backups to provide assurance that the data backups contain the expected data and integrity.

3.1.3 Disable accounts on termination of employment

Disable user accounts of personnel who voluntarily or non-voluntarily are terminated from employment immediately.

3.1.4 Remove inactive user accounts

While an employee may still be employed by an organization that owns, manages, or services the system, they may not have used it for a long period. This suggests that they do not have a need to use the system and you should remove their user account. This is sometimes referred to as a use it, or lose it policy. This best practice reduced the amount of active user accounts in the system and therefore lowers the potential attack footprint.

3.1.5 Update user account roles and permissions

While an employee may still be employed by an organization that owns, manages, or services the system, they may have changed roles or have increased or decrease their need to use the system. When you add a role or a permission to a user's account when that user is granted new authorizations due to an organizational role change, be sure to remove the camera's roles and permissions no longer required or used in their new role.

3.1.6 Disable unused features, ports and services

If you no longer require optional features, ports, and services disable them. This practice lowers the attack surface of Illustra resulting in a higher level of protection.

3.1.7 Check for and prioritize advisories

Find cybersecurity advisories for Illustra on www.illustracameras.com. Determine if Illustra is impacted by the conditions outlined in the advisories. Based on how you deploy, configure, and use Illustra system, the advisory may not be of concern. To help with your assessment refer to as-built documentation of the Illustra system. A good set of as-built documentation will identify the number of components impacted and when they are located. While advisories call attention to a cybersecurity issue, it is not always possible to take immediate action or execute the full recommendation described in the advisories. Address any impacting your system in order of priority. Consult with the respective vendor to check for advisories from third party components such as networking equipment and operating systems.

3.1.8 Plan and execute advisory recommendations

If Illustra is impacted by the conditions outlined in the advisories, including those from third party components, then action must be taken to mitigate the issues raised. The specific action is based upon the content of the advisories distributed and depends upon the environment Illustra is deployed into. Plans for executing the advisory recommendations must consider the operating environment and usage of Illustra.

3.1.9 Check and prioritize patches and updates

While an Illustra patch or update may or may not relate to an advisory, it is always best practice to apply the most current patches and updates. These patches and updates can include cybersecurity enhancements and fixes to known issues. Review the release notes and prioritize the benefits of the patch or update. The overall benefit should include the improved protection that lowers the cybersecurity risk. Be sure also to check for updates and patches of third party components such as networking equipment and operating systems by consulting with the respective vendor.

3.1.10 Plan and execute software patches and updates

Create a plan to apply software updates on a regular basis. This plan should include provisions for the unlikely event of service impact. Make considerations regarding schedule and deployed environment in order to minimise service disruptions.

3.1.10.1 Update process

To update the camera complete the following steps.

1. Check the Illustra cameras website (www.illustracameras.com) for the latest official release for your product.
2. Download the file.

3. Open **Illustra Connect**.
4. Click **Update**.
5. Select your firmware image.

3.1.11 Review organizational policy updates

Organizations may update their policies which include cybersecurity requirements. Changes to these policies can impact systems which were in compliance prior to the change. Periodically check for policy changes and re-assess compliance with those policies.

3.1.12 Review updates to regulations

If Illustra is deployed in a location that is governed by regulation, it is important to check to see if there are any updates to those regulations. In some cases, new regulations are introduced. Whether it is a review of an updated regulation to maintain compliance and a new regulation, an assessment of the changes should be conducted periodically.

3.1.13 Update as-built documentation

As-built documentation refers to the environment the Illustra solution is deployed into, this may include but is not limited to: network infrastructure and external integrations. Changes and updates to the operating environment should be recorded and assessed for potential security vulnerabilities.

3.1.14 Conduct security audits

Periodic security audits are necessary as cybersecurity guidance, organizational policies, regulations, auditing processes, system use and configuration and threats have likely changed since the last audit. If you conduct periodic security audits, you can apply the latest knowledge and conditions and reveal gaps in protection previously undetected or created by changes in system use of configuration.

3.1.15 Update password policies

Guidance on password policies evolves. Periodically re-assess password policies to make sure the right policy is in place for the target environment based on current organizational policies, regulations and guidance from standards organizations such as NIST.

Frequency - Annually

3.1.16 Update as-build documentation

Update as-built documentation if the deployment architecture or component configuration changes. Some configuration changes happen without a formal project or plan and if such cases it may be common to negate updating the as-built documentation. Schedule a full update of the as-built documentation on a regular basis to ensure that all changes are documented.

Frequency - As changes are made or quarterly

3.1.17 Update standard operating procedures

Including best practices for cybersecurity in standard operating procedures can complement the protection that the system can deliver on its own. Depending on the procedures an operator uses they can prevent, create, or close a gap in protection. It is important to update standard operating procedures periodically.

Frequency - Annually

3.1.18 Monitor for cyber attacks
Monitor site perimeters, networks and end-points for cyber-attacks. Many tools are available to assist with real-time analytics-based detection. Frequency - continuously

3.2.0 Patch policy

The policy documented here sets forth the current internal operating guidelines and process in regards to Illustra, 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 endeavours to address issues that arise within Illustra with the severity that they warrant.

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 reasonable practicable.

When non-CRITCIAL vulnerabilities are discovered within Illustra cameras, Johnson Controls, Inc. 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 the latest version of the released product.

3.3.0 Release schedule

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

No Illustra update is released without undergoing extensive quality assurance testing.

3.4.0 Recovery and factory reset

To reset the camera complete the following steps:

1. Open **Illustra Connect**.
2. Click **Maintenance**.

Click **Backup and Restore**.

There is also a hardware reset button to complete the same task. Refer to the user manual for its use and location.

3.5.0 Illustra testing process

Vulnerability assessment is a continuous process in which the camera is subject to penetration testing and vulnerability scanning. This includes the use of tools including: p0f, Nessus, and Black Duck.

3.5.1 Vulnerability assessment

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

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

3.5.2 Vulnerability assessment – third party components

Johnson Controls uses commercially reasonable efforts to monitor third party and open source software included within Illustra 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 the Illustra NVR.

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.

3.6.0 Illustra vulnerability reporting

If you believe you have discovered a vulnerability Illustra or any Johnson Controls product, contact the Cyber Protection Program through its website https://www.johnsoncontrols.com/cyber-solutions/cyber-response or at the email address productsecurity@jci.com.

Additionally, Johnson Controls Technical Support staff have direct access to the Cyber Protection team to help assess and resolve any issues (illustrasupport.tyco@jci.com).