# Illustra Standard HD Camera Hardening guide


GPS0052-CE-EN
Version ISHD 1.0
Rev A
Revised 2024-04-10

# Table of Contents

# 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 user accounts, permissions and roles, and backup and restore.

This Johnson Controls **Illustra Standard HD Camera Hardening guide** is broken down into three main sections depicting the overall process for hardening:

| 1. Planning | 2. Deployment | 3. Maintain |
|---|---|---|
| Provides an introduction, general knowledge, and overall guidance for you to prepare your system for security and hardening | Guides you through the execution and hardening steps based on the products and security features of the target system components | Provides a checklist for future checkpoints to keep your system safe and secure |

Appendixes are included at the end for additional information about account access, event actions, settings, health monitor and log files.

## 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 guarantee 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.

Illustra IP cameras integrate seamlessly with Johnson Control hardware and software video clients such as victor, VideoEdge, and exacqVision. 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

Illustra cameras can be deployed in many ways. Figures 1.1.1.1 and 1.1.1.2 illustrate architectures using an internal network or connectivity to the internet.

Figure 1.1.1.1 Typical Illustra deployment architecture.

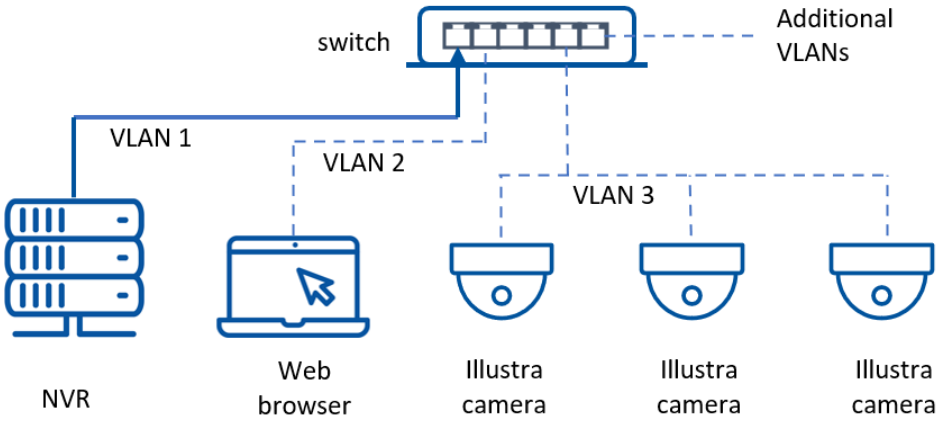
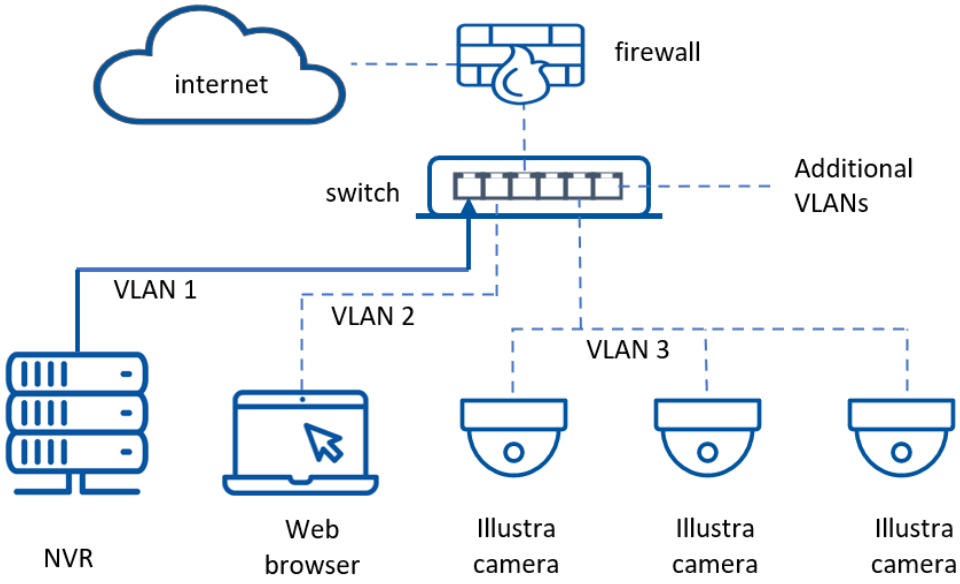


Figure 1.1.1.2 Illustra deployment with Internet connectivity.




### 1.1.2 Components

Illustra Standard HD Camera. A motorized variable-focus (V/F) Infrared (IR) Smart Dome Camera by Tyco comes with several intelligent functions built-in for high-quality video surveillance. Additionally, this high definition (HD) camera comes with a rich feature-set that includes true Wide Dynamic Range (WDR), Power-Over-Ethernet (PoE), and 3D Digital Noise Reduction (DNR) to meet a wide variety of video surveillance applications capturing high quality, color images in back light environment.

### 1.1.3 Supporting components

Illustra cameras seamlessly integrate with Johnson Controls components but can also work with third party components and systems.

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.

Web Browser. You can configure an Illustra camera through a web browser. See the compatibly list included with the datasheet for the supported web browsers. You can find this on the Illustra website at https://illustracameras.com/cameras/.

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 PoE.

### 1.2.0 Security feature set

This document details the extensive security features available across the Illustra product range.

Individual features may vary, depending on camera model and firmware version.

- User accounts, including roles
- User account management
- Password strength enforcement
- IP address allow list or deny list
- MAC address allow list or deny list
- Encrypted communication
- Network protocol configuration
- Logging

Table 1.2.0.1 Security features

| Section | Type | Feature name |
|---|---|---|
| **1.2.1** | Dashboard | Security overview |
| **1.2.2** | User Account Support | User accounts |
| **1.2.3** | | User authorization |
| **1.2.4** | | Automatic Logoff feature |
| **1.2.5** | User Password Support | User password policy |
| **1.2.6** | | User authentication |
| **1.2.7** | Authentication safeguards | Machine authorization |
| **1.2.8** | | Network Time Protocol |
| **1.2.9** | Secure Communications | Secure Communications |
| **1.2.10** | | Digital certificate management |
| **1.2.11** | | Encryption/hash algorithms |
| **1.2.12** | Alarms and Events | Logs |
| **1.2.13** | | Alarms and alerts |
| **1.2.14** | | Timely response to events |
| **1.2.15** | Backup and Restore | Availability assurance |
| **1.2.16** | | Resource availability |
| **1.2.17** | Software updates | Encrypted software updates |

### 1.2.1 Security overview

The web GUI shows the security status, and security options of your camera. For more information on managing security settings see section 2.2.2.1.

### 1.2.2 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 sections 2.2.4 and 2.2.4.

### 1.2.3 User authorization

To control the level of user authorization, use the principle of separation of duties and divide accounts into user types. For more information see sections 2.2.4 and 2.2.4.

### 1.2.4 Automatic Logoff feature

Illustra has an automatic logoff feature. For more information see section 2.2.2.4

### 1.2.5 User password policy

Illustra enforces strong passwords by default. Passwords must be 8 – 16 characters long (Johnson Controls recommends a minimum of 15) and have at least four characters from the following character groups:

- Upper case letters

- Lower case letters
- Numbers
- Special characters

### 1.2.6 User authentication

User authentication requires a username and password combination across all functions, by default, this includes video streaming.

### 1.2.7 Machine authorization

Illustra allows for certificate-based device authentication. For more information see sections 2.4.3 and 2.4.4.

### 1.2.8 Network Time Protocol (NTP)

Illustra has a Network Time Protocol (NTP) synchronization feature.
For more information see section 2.2.2.5

### 1.2.9 Secure communications

Illustra supports TLS 1.2, SNMPv3, and has a set of built-in firewall capabilities. See section 2.4.2 for SNMP configuration and section 2.4.5 for built-in firewall configuration. If paired with a compatible system encrypted video streaming is available.

### 1.2.10 Digital certificate management

Customers should install a suitable certificate signed by a Certificate Authority (CA). You can update this certificate, see section 2.3.4. Web browsers highlight self-signed certificates as insecure because they are inadequate for authentication. The certificates are valid for encryption purposes.

### 1.2.11 Encryption/hash algorithms

Here are the supported ciphers for TLS v1.2:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

### 1.2.12 Logs

The following logs are enabled by default: Security, Audit, Fault, System, and Boot. You can also create user defined Event Logs that use advanced features, for example, motion detection. For more information about specific logs see sections 2.4.2 through 2.4.7.

If required, logs can be exported from web GUI.

### 1.2.13 Alarms and alerts

You can 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 or on the web GUI, see section 2.4.0.

### 1.2.14 Timely response to events
If the device is integrated with a supported system, alerts and events may appear immediately to operators of those systems. Email alert functionality, transfer of events to network storage, and alarm output is also available.

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

### 1.2.16 Resource availability
To export camera settings, navigate to the Back Up and Restore page on the web GUI. You can restore settings using an exported file.

To record video, use an SD card. You can configure video to respond to events including analytics triggers and alarm input. If the camera is integrated with an NVR, you can use the NVR to record video. If equipped with an SD card and with NVR access video backfill may be used. If network connection is lost the backfill will continue to record video locally. Transferring the recorded data to an NVR when the connection is restored.

### 1.2.17 Encrypted software updates
Software upgrades are provided as an encrypted and signed file. For more information on the update procedure see section **Error! Reference source not found.**.

### 1.3.0 Intended environment
You can install Illustra cameras in a range of environments, including internally 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
Connecting any Operational Technology (OT) system to the internet always increases cybersecurity risk. Illustra cameras do not need Internet connectivity to function. To harden your system, Johnson Controls recommends that you do not connect Illustra cameras to the internet. Illustra cameras need access to a local area network (LAN) to leverage the full feature set. The camera may require Internet connectivity to allow the function of optional features, such as dynamic DNS.

### 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, for example using an NVR, or external NTP.
If NTP is required, a default server of us.pool.ntp.org is provided. This URL setting can be modified by the customer as necessary.

### 1.4.0 Patch policy

It is best practice to upgrade the camera with the latest Illustra firmware to install the most recent security fixes.

When we discover a critical security vulnerability, we use commercially reasonable efforts to:

- Issue a **critical update** for the current version of the product as soon as is reasonably practicable

When we discover non-critical security vulnerability, we use commercially reasonable efforts to:

- Apply fixes for **high severity** vulnerabilities in the next immediate release

  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.

### 1.4.1 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.

### 1.5.0 Hardening methodology

Illustra has many on board 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.

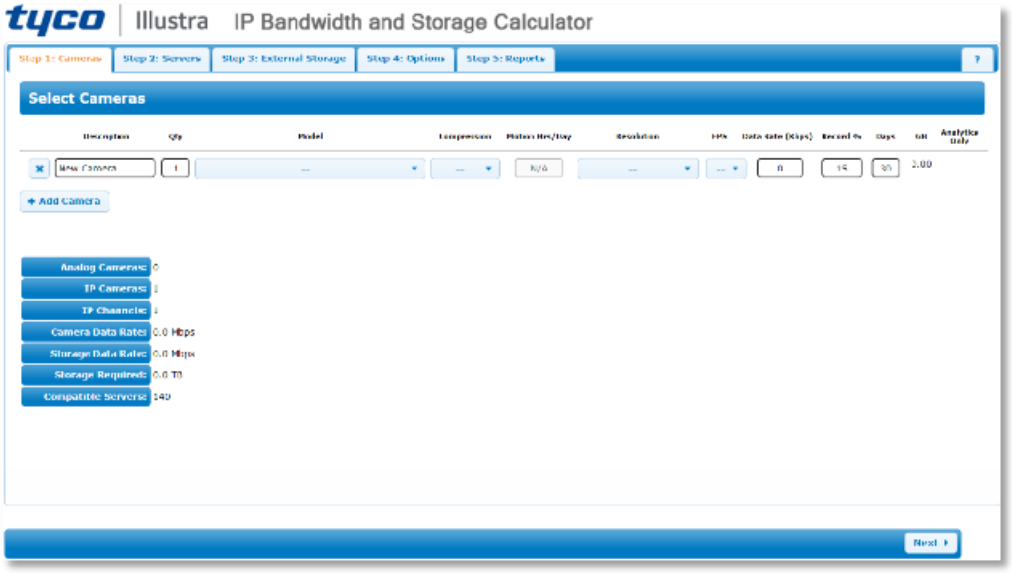
### 1.6.0 Communication paths table

| 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 |
| **RTSP** | Video streaming | Enabled | Yes | Yes | TCP or UDP | 554 | 1 – 65535 |
| **UPnP** | Automatic IP discovery and setup | Enabled | Yes | Yes | TCP or UDP | 49152 | N/A |
| **SMTP** | Sending of security events | Disabled | No | Yes | TCP | 25 | 10 – 65535 |
| **FTP** | Sending of events and events triggered video captures | Disabled | No | Yes | TCP | 21 | 0 – 65535 |
| **SFTP** | Secure sending of events and events triggered video captures | Disabled | No | Yes | TCP | 21 | 0 – 65535 |
| **HTTP** | Communication to the Web GUI | Enabled | Yes | Yes | TCP | 80 | 1 – 65535 |
| **HTTPS** | Secure communication to the Web GUI | Enabled | No | Yes | TCP | 443 | 1 – 65535 |
| **Websockets Secure** | Communication with no plug-in data | Enabled | Yes | Yes | TCP | 7681 | 1 – 65535 |
| **NTP** | Network time synchronisation | Disabled | No | Yes | UDP | 123 | N/A |
| **ONVIF** | Camera discovery and setup | Disabled | No | Yes | UDP | 3702 | N/A |
| **Data port** | Video streaming | Enabled | Yes | Yes | TCP | 9008 | 1 – 65535 |
| **Long Polling Port** | transfer intelligent data by http | Enabled | Yes | Yes | TCP | 8080 | 1 – 65535 |
| **Multicast** | Search devices | Enabled | Yes | Yes | UDP | 23456 | N/A |

### 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.

# 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

A deployment of Illustra should employ a VLAN with access restricted to systems and components required for operation. See section 1.1.1 for examples of deployment.

### 2.1.1 Getting started

Before installing an Illustra camera, consider the guidance outlined in the following sections.

### 2.1.2 Physical installation considerations

Cameras are designed to be placed in open areas where they can capture the best video footage. The physical access to the device and physical installation of the device can impact the cybersecurity. When possible, install cameras in a location that is difficult to reach without a ladder or has added physical protection which does not obstruct the camera's line of sight.

#### *2.1.2.1 Tamper detection*

You can configure tamper detection as a blur detection analytics event, see section **Error! Reference source not found.**.

### 2.1.3 Default security behavior

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 default password must be changed. Password restrictions ensure password strength.

### 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. Navigate to the web GUI
2. Navigate to the Web User Interface banner and click **Config**
3. Click **Maintenance**
4. Click **Backup & Restore**
5. Click the "Load Default" button and then verify the password to restore all system settings to the default factory settings except those you want to keep

   Optional: Select Network Config, Security Configuration, Image Configuration  Preserve IP address

There is also a hardware reset button. See the User Guide for details on its operation and location.

### 2.1.5 Recommended knowledge level

The person executing the proper hardening steps in this guide must have Illustra administration and networking technologies experience.

### 2.1.6 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.

### 2.2.0 Hardening

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

### 2.2.1 Hardening checklist

To harden this product, complete the following tasks:

- Hardening Step 1: Change all default credentials
- Hardening Step 2: Perform firmware updates
- Hardening Step 3: Disable unused ports
- Hardening Step 4: Enable RTSP authentication with Digest
- Hardening Step 5: Encrypted Communications
    - Hardening Step 5.1: Setup HTTPS
    - Hardening Step 5.2: Setup Secure FTP
    - Hardening Step 5.2: Setup SNMPv3
- Hardening Step 6: Update the SSL certificate
- Hardening Step 7: Enable IEEE 802.1X
- Hardening Step 8: Backup and restore camera setting

### 2.2.2 Administration

To access Illustra settings complete the following steps:

1. Navigate to the web GUI
2. Log on as an administrator
3. Navigate to the Web User Interface banner and click **Config**

There are seven main areas of administration, **Image**, **Alarm and Event, Security, Network, Maintenance, System** and **Storage**:

- Use the **Image** menu to configure display settings and so on
- Use the **Alarm and Event** menu to configure motion detective and so on
- Use the **Security** menu to configure various security settings and add or modify user accounts
- Use the **Network** menu to configure basic network settings, networking protocols, and allowing individual protocols to be enabled or disabled
- Use the **Maintenance** menu to upgrade or reboot the camera and so on
- Use the **System** menu to configure options for maintenance and monitoring
- Use the **Storage** menu to manage SD card and so on

#### *2.2.2.1 Security*

To access security settings, complete the following steps:

1. Navigate to the web GUI
2. Navigate to the Web User Interface banner and click **Config**
3. Click **Security**
4. Click **User**

You can enable or disable video authentication.

#### *2.2.2.2 Network*

To access the **Network** settings, complete the following steps:

1. Navigate to the web GUI
2. Navigate to the Web User Interface banner and click **Config**
3. Click **Network**

The **Network** submenu has a list of user configurable network protocols.

#### *2.2.2.3 System*

To access the **System** settings, complete the following steps:

1. Navigate to the web GUI
2. Navigate to the Web User Interface banner and click **Config**
3. Click **System**

The **System** submenu has options for backup or upgrades, **Date Time** configuration, logs (see section **Error! Reference source not found.**), and system information.

#### *2.2.2.4 Automatic Logoff feature*

To configure automatic log off complete the following steps:

1. Open the web GUI
2. Navigate to the Web User Interface banner and click **Config**
3. Click **Security**
4. Click **Security Management**
5. Type and adjust the **Logout Time (Seconds)**

**Note:** The default value is 300 seconds.

#### *2.2.2.5 Network Time Protocol*

To configure NTP time synchronization, complete the following steps:

1. Open the web GUI
2. Navigate to the Web User Interface banner and click **Config**
3. Click **System**
4. Click **Date and Time**
5. Select **Synchronize with NTP server** in **Time Mode**
   **Optional**: To change the NTP server, type **NTP Server**

### 2.2.3 User management overview

Hardening Step 1: Change all default credentials.

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 normal user. The roles are briefly outlined here, for a detailed list of permissions, Appendix A.

- **Admin** – This user has access to the full functionality of the camera and may change any setting. Only use admin roles when absolutely necessary.
- **Advanced user** – This user can change non-security-based configuration. For example, video and picture settings.
- **Normal user** – This user is limited to read access.

To ensure you follow security best practices configure individual user accounts properly. Best practices for account management are described in section 2.2.4.

### 2.2.4 User management best practices

To improve the security for Illustra cameras, 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 detect suspicious administrative actions more easily.

#### *2.2.4.4 Strong passwords*

By default, the camera enforces a strong password policy for users. It is recommended that this is unchanged. 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. Navigate to the web GUI
2. Navigate to the Web User Interface banner and click **Config**
3. Click **Security**
4. Click **Users**
   **Optional:** To add a user click **Add**
   **Optional:** To change a password click **Modify**

Use unique accounts during all phases of operation for Illustra. Installers, technicians, auditors, and other deployment phase users must not 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 Password policy configuration*

By default, Illustra follows a strong password policy.

#### *2.2.5.3 Change default passwords*

During initial commissioning the user is asked to change the password for the default admin account once they log on to the web GUI. For further user accounts that are added to Illustra it is advised that the user manually change their own password on initial log on.

#### *2.2.5.4 Assign roles*

Roles limit the actions a user can take, see section 2.2.3. You can assign roles when you create a user account.

### 2.3.0 Updating firmware process

Use Illustra firmware to upgrade the firmware or through Illustra Connect. Refer to the Illustra Connect User Guide for further information.

**Note:** All existing camera settings are maintained when the firmware is upgraded.

#### Hardening Step 2: Perform firmware updates

To manually update the firmware, complete the following steps:

1. Navigate to the web GUI
2. Navigate to the Web User Interface banner and click **Config**
3. Click **Maintenance**
4. Click **Upgrade**
5. Click **Browse**. The Choose file to Upload dialog displays
6. Browse to the firmware file
7. Click the firmware file
8. Click **Open**
9. Click **Upload**

The file transfer begins. Do not disconnect power to the camera during the upgrade process. The camera restarts automatically after the updates, this can take from 1 to 10 minutes. Once complete the Log in page displays.

### 2.4.0 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.

### 2.4.1 Communication port configuration

Ensure that the ports corresponding to your Illustra camera from section 1.6.0 are open that need to be open based on the features being used.  Unused ports should be closed unless they are specifically needed.

#### Hardening Step 3: Disable unused ports

To harden your system, block all ports that are not in use.

The **Network** displays a list of configurable ports. To open **Network** complete the following steps:

1. Navigate to the web GUI
2. Navigate to the Web User Interface banner and click **Config**
3. Click on **More**

By default, the minimum number of ports for essential functionality are open. To harden security do not enable additional ports unless necessary, disable any services not required during operation, and to enable encryption wherever possible.

#### *2.4.1.1 RTSP Authentication*

#### Hardening Step 4: Enable RTSP authentication with Digest

By default, access to Real Time Streaming Protocol (RTSP) streams require user authentication. To change the status of RTSP authentication, navigate to the **Network** page.

1. Select "Enable" to enable the RTSP function
2. Port: Access port of the streaming media. The default number is 554.
3. RTSP Address: The RTSP address (unicast) format that can be used to play the stream in a media player

Multicast Addresses:

- Main stream: The address format is “rtsp://IP address: rtsp port/profile1?transportmode=mcast”
- Sub stream: The address format is “rtsp://IP address: rtsp port/profile2?transportmode=mcast”
- Third stream: The address format is “rtsp://IP address: rtsp port/profile3?transportmode=mcast”

Audio: Having entered the main/sub stream in a VLC player, the video and audio will play automatically.

If “Allow anonymous login…” is checked, there is no need to enter the username and password to view the video.

If “auto start” is enabled, the multicast received data should be added into a VLC player to play the video.

Notes:

1. This camera supports local video preview through a VLC player. Enter the RTSP address (unicast or multicast, e.g., rtsp://192.168.226.201:554/profile1?transportmode=mcast) in a VLC player to realize the simultaneous video preview with the web client.

2. The IP address mentioned above cannot be the address of IPv6.

3. Avoid the use of the same multicast address in the same local network.

4. When playing the video through the multicast streams in a VLC player, please pay attention to the mode of the VLC player. If it is set to TCP mode, the video cannot be played.

5. If the coding format of the video of the main stream is MJPEG, the video may be disordered at some resolutions.

It is best practice to use digest authentication to enable RTSP authentication.

#### *2.4.1.2 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.

### 2.4.2 Encrypted communications

#### Hardening Step 5: Encrypted Communications

Encrypted communications can help prevent attacks by preventing simple connection eavesdropping. Access to Illustra should be through HTTPS. If your deployment requires FTP or SNMP, it is best practice to use Secure FTP and SNMPv3.

#### Hardening Step 5.1: Setup HTTPS

To access HTTP/HTTPS configuration complete the following steps:

1. Navigate to the web GUI
2. Navigate to the Web User Interface banner and click **Config**
3. Click **Network**
4. Click **More**
5. Click **HTTP/HTTPS**

Here you can change port numbers and upload certificates. For more information see section 2.4.3.

#### Hardening Step 5.2: Setup Secure FTP

To configure FTP, complete the following steps:

1. Navigate to the web GUI
2. Navigate to the Web User Interface banner and click **Config**
3. Click **Network**
4. Click **More**
5. Click **FTP**

#### Hardening Step 5.3: Setup SNMPv3

To configure SNMP, complete the following steps:

1. Navigate to the web GUI
2. Navigate to the Web User Interface banner and click **Config**
3. Click **Network**
4. Click **More**
5. Click **SNMP**

### 2.4.3 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 client can verify its identity. You may self-sign the certificate, or for more security-conscious customers, a trusted certificate authority can sign it.
**Note:** Johnson Controls recommends using a trusted certificate authority.

There is a certificate installed by default. Once the function is enabled and saved, the camera can be accessed by entering https://IP: https port via the web browser (e.g., https://192.168.226.201:443).

#### Hardening Step 6: Update the SSL certificate

The next three sections will guide you through the process for doing the following:

- Upload a signed certificate
- Create a private certificate
- Generate a certificate request

*Signed Certificate*

To upload a signed certificate, complete the following steps:

1. Navigate to the web GUI.
2. Navigate to the Web User Interface banner and click **Config**
3. Click **Network**
4. Click **More**
5. Click **HTTPS**
6. Click **Delete** to cancel the default certificate
7. Click **Install** and browse to the certificate location
8. Click **Save**

*Private Certificate*

To Create a private certificate, complete the following steps:

1. Navigate to the web GUI
2. Navigate to the Web User Interface banner and click **Config**
3. Click **Network**
4. Click **More**

5. Click **HTTPS**
6. Click **Delete** to cancel the default certificate
7. Click **Create a private certificate**
8. Click **Create** to create a private certificate
9. Type in country (only two letters available), domain (camera's IP address/domain), validity date, password, province/state, region, etc.
10. Click **OK**

**Note:** The camera only accepts .pem format certificates. The certificate must have the server certificate and private key combined. The private key must NOT be password protected.

*Generating a Certificate Signing Request*

The camera may also create a Certificate Signing Request that may be given to a signing authority.

1. Navigate to the web GUI
2. Navigate to the Web User Interface banner and click **Config**
3. Click **Security**
4. Click **Network**
5. Click **More**
6. Click **HTTPS**
7. Click **Delete** to cancel the default certificate
8. Click **Create a Certificate Request**
9. Click **Create** to create the certificate request. Then download the certificate request and submit it to the trusted certificate authority for signature. After receiving the signed certificate, import the certificate to the device
10. Complete the following fields (no field is mandatory)
    a. Two letter **Country** code
    b. **Province**
    c. **Locality**
    d. **Organization**
    e. **Organizational Unit**
    f. **Common Name**
11. The first **Subject Alternative Name** drop-down menu and textbox contain text. To add further entries, complete the following steps:
    a. Click the **Subject Alternative Name** drop-down menu and choose from **IP** or **DNS** for IP address or domain name respectively
    b. Type the IP address or domain name into the textbox
12. Click **Apply**

A certificate request generates in the text field on the right of the page. You can send this to a signing authority. You can upload a signed certificate using the same procedure outlined in the steps to upload a certificate.

**Note:** The certificate from the signing authority does not contain a private key. You can ignore the private key requirement for certificates generated from a Certificate Signing Request.

### 2.4.4 802.1X configuration

The IEEE 802.1X security feature provides port-based network access control typically used when securing corporate networks from the attachment of unauthorised devices.

### Hardening Step 7: Enable IEEE 802.1X

To enable IEEE 802.1X complete the following steps:

1. Navigate to the web GUI
2. Navigate to the Web User Interface banner and click **Config**
3. Click **Security**
4. Click **More**
5. Click **IEEE 802.1x**
6. To enable IEEE802.1x security select **Enable**
7. Click **Protocol Type**
8. Click **EAPOL Version**
9. Type in **Username / Password / Confirm Password**
10. Click **Save**

### 2.4.5 Built-in firewall

Illustra' s built-in firewall provides basic filters and allow listing or deny listing functionality that filters device access by IP address.

#### *2.4.5.1 Basic Filters*

The following filter is available:

Block and Allow Lists. This filter can be accessed with the following steps:

1. Navigate to the web GUI
2. Navigate to the Web User Interface banner and click Config
3. Click **Security**
4. Click **Block and Allow Lists**
5. Select **Block/Allow the following address, IPv4/IPv6**
6. Type IP address in the address box
7. Click **Add**

### 2.4.6 Mass configuration

Mass configuration simplifies the management of components connected to the system and reduces the risk of misconfiguration. For mass configuration Illustra cameras may be configured using Illustra Connect. Refer to the Illustra Connect User Guide for further information.

### 2.5.0 Operation Log

The operation log contains alarm, abnormal, operation, information logs.

1. Navigate to the web GUI
2. Navigate to the Web User Interface banner and click **Config**
3. Select **Maintenance**
4. Select **Operation Log**
5. Select the main type, sub type, start and end time
6. Click "Search" to view the operation log
7. Click "Export" to export the operation log

### 2.6.0 Availability hardening

Availability hardening is a process that ensures information the camera stores or creates is accessible. Illustra provides several features to ensure availability of data including, backup and restore functionality, network storage, and video backfill. If you need to restore or replace a camera it is important to have a backup of its configuration data to minimise the time it takes to restore functionality.

#### Hardening Step 8: Backup and restore camera setting

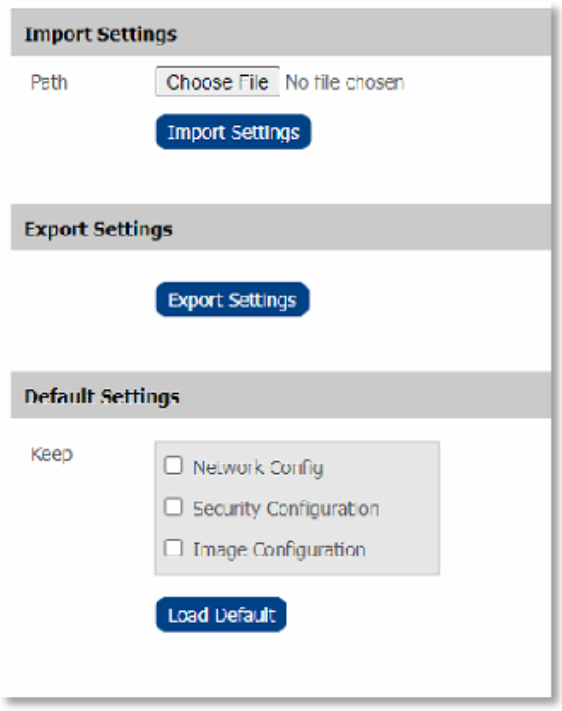
Backup

1. Navigate to the web GUI
2. Navigate to the Web User Interface banner and click **Config**
3. Click **Maintenance**
4. Click **Backup & Restore**
5. Click **Export Settings** (as shown in figure 2.6.0.1)
6. Save the file according to the company's backup policies

Restore

1. Navigate to the web GUI
2. Navigate to the Web User Interface banner and click **Config**
3. Click **Maintenance**
4. Click **Backup & Restore**
5. Select a file that was created during the backup process above
6. Click **Import Settings** (as shown in figure 2.6.0.1)

Figure 2.6.0.1



### 2.7.0 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

In section 1 we learned that many components work together to provide a custom solution.  This section addresses how to monitor for potential cybersecurity issues and maintain protection levels as conditions change.  From the research you gathered in Section 1, determine the items in table 3.1.1 that apply to your system and focus on only those items.

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:

Table 3.1.1

| Item | Description | Immediate | Base on Priority | Daily | Weekly | Monthly | Quarterly | Annual |
|---|---|---|---|---|---|---|---|---|
| **1** | *Backup configuration data* | | | | | | ✓ | |
| **2** | *Test backup data* | | | | | | ✓ | |
| **3** | *Disable user accounts of terminated employees* | ✓ | | | | | | |
| **4** | *Remove inactive user accounts* | | | | | ✓ | | |
| **5** | *Update user account roles and permissions* | | | | | | ✓ | |
| **6** | *Disable unused features, ports, and services* | | | | | | ✓ | |
| **7** | Check for and prioritise advisories | | | | ✓ | | | |
| **8** | Plan and execute advisory recommendations | | ✓ | | | | | |
| **9** | Check and prioritise software patches and updates | | | | ✓ | | | |
| **10** | Plan and execute software patches and updates | | ✓ | | | | | |
| **11** | Review updates to organisational policies | | | | | | | ✓ |
| **12** | Review updates to regulations | | | | | | | ✓ |
| **13** | Update as-built documentation | ✓ | | | | | ✓ | |
| **14** | Conduct security audits | | | | | | | ✓ |
| **15** | Update password policies | | | | | | | ✓ |
| **16** | Update standard operating procedures | | | | | | | ✓ |
| **17** | Monitor for cyber attacks | ✓ | | | | | | |

### 3.1.1 Backup configuration data

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

| Action | Details | Suggested frequency |
|---|---|---|
| Backup configuration data | Create a backup of your data | Quarterly |

### 3.1.2 Test backup data

After completing step 3.1.1, test backups to provide assurance that the data backups contain the expected data and integrity.

| Action | Details | Suggested frequency |
|---|---|---|
| Test backup data | Test the data created in step 3.1.1 | Quarterly |

### 3.1.3 Disable accounts on termination of employment

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

| Action | Details | Suggested frequency |
|---|---|---|
| Disable accounts | Disable user accounts that are no longer needed | 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.

| Action | Details | Suggested frequency |
|---|---|---|
| Remove inactive user accounts | Disable or remove user accounts that are no longer needed | Monthly |

### 3.1.5 Update user account roles and permissions

While an employee may still be employed by an organisation 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 authorisations due to an organisational role change, be sure to remove the camera’s roles and permissions no longer required or used in their new role.

| Action | Details | Suggested frequency |
|---|---|---|
| Update user account roles and permissions | Review employee accounts and update as needed | Quarterly |

### 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. Refer to section 2.4.1

| Action | Details | Suggested frequency |
|---|---|---|
| Disable unused features, ports, and services | Review features ports and services. | Quarterly |

### 3.1.7 Check for and prioritise 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.

| Action | Details | Suggested frequency |
|---|---|---|
| Check for and prioritize advisories | Refer to the link above that hosts advisories and explore each week | Weekly |

### 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.

| Action | Details | Suggested frequency |
|---|---|---|
| Plan and execute advisory recommendations | Plan as described above and execute advisory recommendations | Based on priority |

### 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.

| Action | Details | Suggested frequency |
|---|---|---|
| Check and prioritize software patches and updates | Explore available patches and updates each week | Weekly |

### 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 to minimise service disruptions. See section 2.3.0 for the firmware update process.

| Action | Details | Suggested frequency |
|---|---|---|
| Plan and execute software patches and updates | Explore available patches and updates each week | Based on priority |

### 3.1.11 Review organizational policy updates

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

| Action | Details | Suggested frequency |
|---|---|---|
| Review updates to organizational policies | Collect most recent security policies for your organization | Annual |

### 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.

| Action | Details | Suggested frequency |
|---|---|---|
| Review updates to regulations | Collect most recent copies of regulations as applicable. Perform a gap analysis against the deployed configuration. | Annual |

### 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. Schedule a full update of the as-built documentation on a regular basis to ensure that all changes are documented.

| Action | Details | Suggested frequency |
|---|---|---|
| Update as-built documentation | Update as-built documentation if the system architecture or component configuration significantly changes | Immediate |

### 3.1.14 Conduct security audits

Periodic security audits are necessary as cybersecurity guidance, organisational 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.

| Action | Details | Suggested frequency |
|---|---|---|
| Conduct security audits | Perform the tasks listed on your Security audit checklist | Annual |

### 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 organisational policies, regulations, and guidance from standards organisations such as NIST.

| Action | Details | Suggested frequency |
|---|---|---|
| Update password policies | Review internal password policies and the section on passwords | Annual |

### 3.1.16 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.

| Action | Details | Suggested frequency |
|---|---|---|
| Update standard operating procedures | Collect standard operating procedures for use within the organization | Annual |

### 3.1.17 Monitor for cyber attacks

Monitor site perimeters, networks, and endpoints for cyber-attacks. Many tools are available to assist with real-time analytics-based detection.

| Action | Details | Suggested frequency |
|---|---|---|
| Monitor for cyber attacks | Determine which security monitoring tools and services to implement | Run continuously once implemented |

### 3.2.0 Recovery and factory reset

To recovery or factory reset the device use the web GUI or hardware reset button. For more information see section 2.1.4.

### 3.3.0 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 but not limited to: p0f, Nessus, and Black Duck.

### 3.3.1 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 |

### 3.3.2 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 Illustra.

| 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.

### 3.4.0 Illustra vulnerability reporting

If you believe you have discovered a vulnerability in 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 to help assess and resolve any issues (illustrasupport.tyco@jci.com).

## Appendix A – User account access

| Camera Menu | Sub Menu | Tab | Admin | Advanced User | Normal User |
|---|---|---|---|---|---|
| **Live** | Live View | | √ | √ | √ |
| **Search** | SD Card Record/Picture searching | | √ | √ | √ |
| **Config** | image | Display setting | √ | √ | √ |
| | | Video/Audio | √ | √ | √ |
| | | OSD | √ | √ | √ |
| | | Video Mask | √ | √ | √ |
| | | ROI Config | √ | √ | √ |
| | Alarm and Event | Motion Detection | √ | √ | √ |
| | | Anomaly | √ | √ | √ |
| | | Alarm Server | √ | √ | √ |
| | | Object Abandoned/Missing | √ | √ | √ |
| | | Video Exception | √ | √ | √ |
| | | Line Crossing | √ | √ | √ |
| | | Region Intrusion | √ | √ | √ |
| | Security | User | √ | √ | √ |
| | | Online User | √ | √ | √ |
| | | Block and Allow Lists | √ | √ | √ |
| | | Security Management | √ | √ | √ |
| | Network | TCP/IP | √ | √ | √ |
| | | More... | √ | √ | √ |
| | Maintenance | Backup and Restore | √ | √ | √ |
| | | Reboot | √ | √ | √ |
| | | Upgrade | √ | √ | √ |
| | | Log | √ | √ | √ |
| | System | Basic Information | √ | √ | √ |
| | | Date and Time | √ | √ | √ |
| | | Local Config | √ | √ | √ |
| | Storage | Config | √ | √ | √ |

| | | | | | |
|---|---|---|---|---|---|
| | | Download | √ | √ | √ |
| | Other | Remote storage settings | √ | √ | × |
| | | Remote image settings | √ | √ | √ |
| | | Remote PTZ control | √ | √ | √ |
| | | Remote alarm server configuration | √ | √ | √ |
| | | Remote intelligent event configuration | √ | √ | √ |
| | | Remote network advanced configuration | √ | √ | × |
| | | Remote security management | √ | √ | × |
| | | Remote configuration backup and recovery | √ | √ | × |
| | | Remote restart and upgrade | √ | √ | × |
| | | Remote view logs | √ | √ | √ |
| | | Remote voice intercom | √ | √ | √ |
| | | Remote preview | √ | √ | √ |
| | | Remote playback | √ | √ | √ |
| | | Remote storage settings | √ | √ | × |

*Note: The default administrator account cannot be deleted, administrator can select the user permissions for advanced or normal user.*

# Appendix B Configuring event actions

You can configure the camera to carry out a specified operation when an analytic alert is triggered. Analytic alerts are defined using event actions. You can configure multiple event actions.

Use event actions to configure any combination of the following actions:

- Record a clip to microSD Card
- Send an external alarm using email that includes alarm detail, where to retrieve the AVI video file and one JPEG picture of the event if recording MJPEG to microSD Card. If MJPEG is not being recorded on microSD Card, then no JPEG picture is sent
- Send an AVI video file to a pre-configured external FTP server. The video file contains pre and post alarm video buffer

**Note:** You must use a microSD Card to send an SMTP email, video files and images from triggered analytic alerts.

## Appendix B.1 Creating an event action

Configure an event action which can be triggered by an analytic alert.

1. Navigate to the web GUI
2. Navigate to the Web User Interface banner and click **Config**
3. Click **Alarm and Events**
4. Click **Event Actions**
5. Select an **Event Action**
6. Click **enable**
7. Select **Trigger SD Card Snapshot**: The system will capture images and save the images on an SD card
8. Select **Trigger SD Card Recording**: Video will be recorded on an SD card
9. Select **Trigger Email**: If “**Trigger Email**” and “**Attach Picture**” are checked (email address must be set first in the Email configuration interface), the captured pictures and triggered event will be sent into those addresses
10. Select **Trigger FTP**: If “**Trigger FTP**” and “**Attach Picture**” are checked, the captured pictures will be sent into FTP server address

**Notes:**

- If **Record** is selected, the AVI clip is saved to the microSD card, and it must be removed from the camera to view the video file.
- The selected pre and post event duration buffer is included in any video clips sent using FTP.

## Appendix B.2 Editing an event action

To modify the details of an existing event action, complete the following steps:

1. Navigate to the web GUI
2. Navigate to the Web User Interface banner and click **Config**
3. Click **Alarm and Events**
4. Click **Event Actions**
5. Click an entry on the event actions list, you can edit the following:
    - Enable

- Trigger SD Snapshot
- Trigger SD Recording
- Trigger Email
- Trigger FTP

### Appendix B.3 Supported events

| Event Actions | Description |
|---|---|
| Output | The camera can enable an output for an event action |
| Record | Event to record upon fault action will be enabled |
| Email | Email notification of fault |
| FTP | FTP upload of fault notification |
| **Analytics** | **Description** |
| ROI | A region of interest is a defined area of the camera view which is 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 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 blurred, (such as: redirection, blocking, or defocusing). |

# Appendix C Configure SMTP Settings

Configure the SMTP settings to allow email alerts sent from the camera when an analytic alert is triggered. To configure SMTP, complete the following steps:

1. Navigate to the web GUI
2. Navigate to the Web User Interface banner and click **Config**
3. Click **Network**
4. Click **More**
5. Click **Email**
   Use the following parameters to complete configuring the SMTP settings:

   - **Sender Address:** sender's e-mail address.
   - **Username and password:** sender's username and password
     *(you don't have to enter the username and password if "Anonymous Login" is enabled).*
   - **Server Address:** The SMTP server IP address or host name. Select the secure connection type at the "**Secure Connection**" pull-down list according to what's required.
   - **SMTP Port:** The SMTP port.
   - **Send Interval(s):** The time interval of sending email. For example, if it is set to 60 seconds and multiple motion detection alarms are triggered within 60 seconds, they will be considered as only one alarm event and only one email will be sent. If one motion alarm event is triggered and then another motion detection alarm event is triggered after 60 seconds, two emails will be sent. When different alarm types are triggered at the same time, multiple emails will be sent separately.
   - Click the **"Test"** button to test the connection of the account.
   - **Recipient Address:** receiver's e-mail address.

# Appendix D Configure FTP Settings

Configure the FTP settings for the FTP server this sends video files from triggered analytic alerts.

1. Navigate to the web GUI
2. Navigate to the Web User Interface banner and click **Config**
3. Click **Network**
4. Click **More**
5. Click **FTP**
6. Click “**Add"** to add the information of the FTP. After that, click “**Save**” to save the settings
   Use the following parameters to complete configuring the FTP settings:
   - **Server Name**: The name of the FTP server
   - **Server Address**: The IP address or host name of the FTP server
   - **Upload Path**: The directory where files will be uploaded to
   - **Port**: The port of the FTP server
   - **Username and Password**: The username and password that are used to login to the FTP server
   - **Server Type**: three options: FTP, FTPS, SFTP

# Appendix E Health Monitor

The following list contains the information displayed by the Health Monitor:

- User Resets
- Power Resets
- Total Disk Size
- Disk Usage
- Video Streams Playing

# Appendix F Audit Log Details

The Audit Log logs details of changes in the following format: source, class, result, user, and a description of the change. The audit log displays changes made in the following areas of the Web User Interface including:

- Changes in FTP, SMTP, IPV4, IPV6, DNS and SNMP are logged under class **Maintenance**
- Changes in Stream are logged under class **Maintenance**
- Changes in Reboot, Reset and Upgrade are logged under class **Maintenance**
- Changes in ROI are logged under **Maintenance**

## Appendix G Fault Log Details

Any system or environmental faults display in the Fault Log with the following information:

- **Fault** - a description of the fault
- **Date created** - the time and date when the fault occurred