# Smart Connected Chillers Hardening Requirements


GPS0030-CE-20220429-EN
Rev A

Johnson Controls

## Introduction

Our practices provide peace of mind to our customers with a holistic cyber mind set beginning at initial project design concept, and is supported through deployment, including a rapid incident response to meet comprehensive and evolving cybersecurity environments.

This hardening document intends to provide cybersecurity requirements used in planning, deployment, and maintenance periods for the Smart Connected Chiller solution.

As cybersecurity threats affect 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 requirements for configuration and maintenance, including the user accounts, 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 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 unauthorized access or damage caused by a cybersecurity incident. This guide is provided “as is”, and Johnson Controls makes no representation or warranty, expressed or implied, as to the efficacy of the cybersecurity practices or recommendations described within. Johnson Controls disclaims all liability for any damages that may occur because of, or despite, reliance on this guide or compliance with any cybersecurity practices or recommendations set forth herein.

# Contents

# 1 Planning

This section helps plan for the implementation of security requirement for the Smart Connected Chiller solution.

### 1.1.0 Smart Connected Chiller Solution overview

Smart connected chillers from Johnson Controls are revolutionizing how chillers are serviced. This solution gathers data from your equipment, analyzes it and then informs you of the best time to make upgrades or perform maintenance, validate the performance results you expected from operating the equipment, and minimize your costs.

- Predictive Maintenance - Automatically gathers data from your equipment and informs you about the best time to upgrade or perform maintenance.
- Reduces Downtime - Anticipates problems using AI-based algorithms to reduce the amount of time your chiller is out of commission.
- Improves Efficiency - Facilitates more efficient operations, minimizing costs, and extending the life of your equipment.

Technologies shaping connected buildings and services include:

- A new generation of building automation systems (BAS) delivers greater knowledge and control
- Smart equipment brings intelligence to building devices boosting building performance
- Cloud-based technologies and solutions enhance management of buildings and portfolios
- Mobility tools help service technicians and facility managers stay connected

These technologies provide historical and predictive data that make smart connected services possible.

### 1.1.1 Deployment architecture

The Smart Connected Chiller solution is comprised of several components to provide options for wired and wireless communications within the building and to cloud services which provide analytics and remote access for chiller monitoring.

The current Smart Connected Chiller solution does not support third party chillers. Support for third party chillers will be added in a future release which will sufficiently address the security for the additional communication risk associated with its configuration.

Figure 1.1.1 on the following page shows the full solution. The gateway and modem are highlighted in this architecture to indicate the scope of components which require hardening. It is these components which enable building to cloud communications.

Figure 1.1.1: Smart Connect Chiller architecture

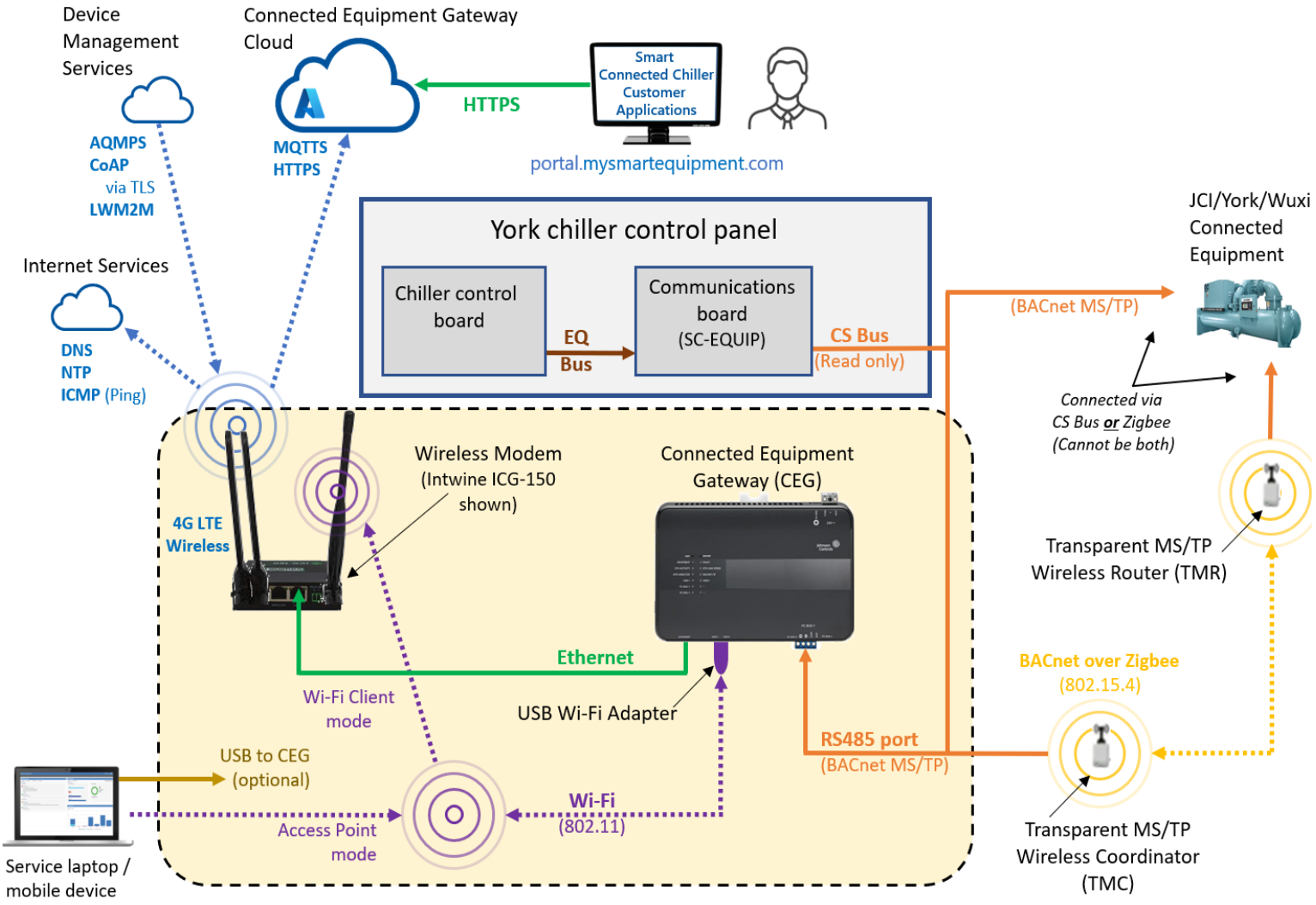



Figure 1.1.1 above reflects a scenario with Johnson Controls only devices such as York and Wuxi connected equipment. The CS bus is active on the SC-EQUIP board, while the BAS Port / FC bus is not used to connect chiller equipment. Optionally, the BAS Port / FC bus may be used for Metasys connectivity independent of the connected solution.

### 1.1.2 Components

The Smart Connected Chiller solutions consists of the following components which require hardening on premises:

*Connected Equipment Gateway (CEG)*

The Connected Equipment Gateway (CEG) streams data from BACnet® MS/TP compatible equipment to the modem via a wired Ethernet or wireless Wi-Fi connection. The CEG is compatible with Johnson Controls® and third party manufactured chillers, roof top units, input output modules, and air handling units. The CEG supports selecting up to eight chillers to monitor from a single gateway, via wired or wireless BACnet network. Wireless equipment connects to the CEG using the Transparent MS/TP Wireless Router (TMR). Equipment connected to the CEG is self-discovered. The CEG includes a local user interface (UI) for basic commissioning and configuration.

*USB Wi-Fi adapter*

The Wi-Fi Access Point (AP) adapter connects to one of the CEG USB ports and can serve as either an access point, a Wi-Fi client or both:

- **Access Point mode** – Mobile devices and laptops can connect to the CEG
- **Wi-Fi Client mode** – Wirelessly connects the CEG to a single modem

The USB Wi-Fi adapter is either included as part of panel kit along with the CEG or sold separately (product code ACC-WFUSB-0)

*Transparent MS/TP Wireless Coordinator (optional)*

The CEG can communicate to the TMR Wireless Field Bus System with the optional Transparent MS/TP Wireless Coordinator (TMC). The adapter uses low power 802.15.4 mesh technology to monitoring of HVAC equipment that uses the BACnet over Zigbee protocol. The wireless system creates a wireless mesh network and provides a reliable, resilient self-healing network by automatically updating transmission paths for the data.

When the TMC is plugged into one of the CEG's RS-485 ports, the CEG can communicate to equipment connected using Transparent MS/TP Routers (TMRs) that are within signal range and share a common Personal Area Network (PAN) identifier.

*Modem*

Several approved 4G LTE modems are available from Johnson Controls which support this application. The modem establishes internet connectivity for transmission of CEG data to the Johnson Controls Cloud which host services for Smart Connected Chiller customer applications. Availability of modem models is country dependent.

Standard modem offerings:

- Digi WR11-M600-DE1-XB – 4G LTE wireless no local Wi-Fi
- Intwine ICG-150 – 4G LTE wireless with local Wi-Fi

International modem offerings:

- Teltonika RUT950 for Asian countries excluding China and Hong Kong
- Robustel R1510 for China & HK

### 1.1.3 Supporting components

Supporting components are those which are necessary for system operations but are not within the targeted scope of this document. This solution is supported by the following components:

*York Chiller Control Panel*

The York chiller control panel provides runtime control of the local chiller and can provide chiller status information to connected equipment via the SC-EQUIP communication board.

*Smart Chiller Equipment communications board (SC-EQUIP)*

SC-EQUIP is the Smart Chiller Equipment communications board which connects directly to a York chiller control board to provide an RS-485 based interfaces for ASHRAE® BACnet MS/TP communications. The SC-EQUIP provides two RS-485 ports, one for the SC Bus and one for a BAS Bus. The SC Bus is used when communicating to only JCI branded equipment while the BAS Bus is support Metasys integrations. The SC bus connects the local chiller panel to the CEG as well as other equipment within the facility.

*Service laptops / mobile devices*

Service personnel can connect laptops or mobile devices to the CEG when the CEG has a Wi-Fi adapter installed and configured to run in Access Point mode.

*Johnson Controls Cloud Services*

The Johnson Controls Cloud is hosted in a Microsoft Azure environment which receives data from Smart Connected Chillers sent from the CEG via the modem. The Johnson Controls Cloud also host the Smart Connected Chiller Customer Applications which users can access remotely via the internet. All connections to the cloud are via TLS secured communications.

### 1.2.0 Security feature set

Johnson Controls products are designed with built-in cybersecurity features out of the box. Some features are included and note set up by default while other features need the reader to go through steps for advanced hardening.

### 1.3.0 Intended environment

Physical access and installation of devices can greatly impact cybersecurity. Components are designed to be operated in an indoor, dry environment. However, components at each level will possess varying degrees of access. Here is some general guidance based on typical environments per component type:

Most components are designed to be installed within a user supplied panel or enclosure usually in an upright orientation. Install in areas free of corrosive vapors and where the ambient temperature stays below 122 degrees F (50 degrees C).

Please refer to the CEG Installation Guide (Part number 24-11460-00034) for additional details.

### 1.3.1 Internet connectivity

Connected Chillers are designed to require internet access. Internet access increases your cybersecurity footprint and attack area which requires additional hardening steps. The hardening steps in section 2 must be taken to limit external access.

### 1.4.0 Hardening methodology

While most building automation products provide onboard security safeguards, including many secure-by-default settings, we recommend that the device is hardened according to the guidance outlined in section 2, deployment.

Generally, you should aim for a defense-in-depth strategy employing standard IT hardening methods and compensating controls as needed to compliment the base security features of each component.

### 1.5.0 Data flow diagram

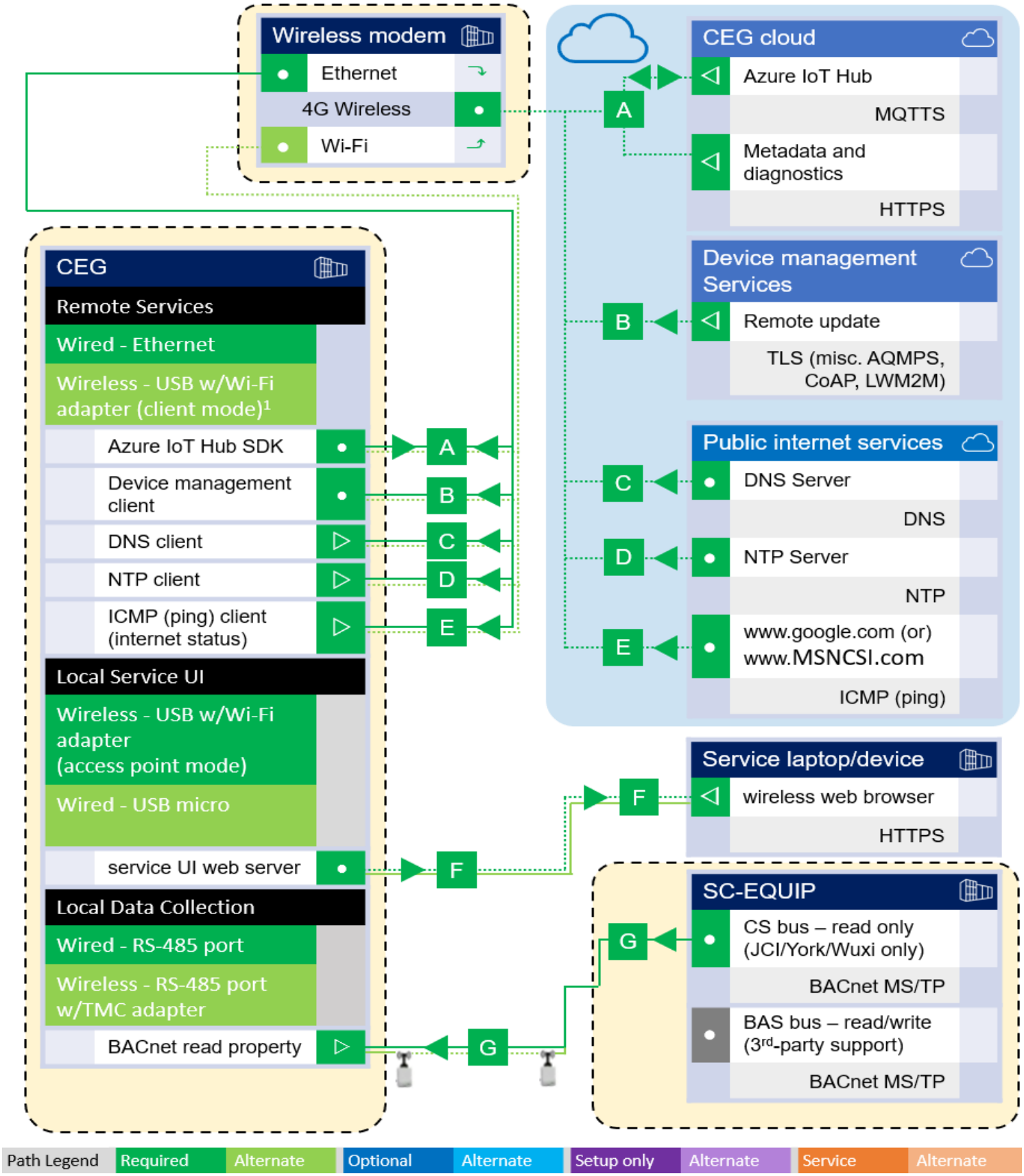
A data flow diagram is a detailed view of the architecture which will show each communication path and flow direction. This resource will be used to aid in the configuration of network security settings (rules) within routers, firewalls and zero-trust architectures.

The use requirements of each path should be identified as:

- Required – this path must be established for the solution to function for all supported applications.
- Optional – this path is optionally required depending on the functions that will be enabled (e.g., webserver, email)
- Setup only – this path is only needed during the setup and configuration and disabling during normal operations is recommended.
- Service – this path is only needed for service. A service path is typically a temporary remote service connection which is disabled during non-service periods.

It is useful for someone who is not as familiar with the process to break the communication paths to understand the processes for the basic to the more complex applications. It is helpful to group paths by function. Communication paths should be labelled so they can be referenced within the document.

Figure 1.5.0 Data Flow Diagram



[1]Wi-Fi support limited to modems with capability.

- Intwine ICG-150 - supports Wi-Fi
- Digi WR11 - does not support Wi-Fi

### 1.5.1.1 Communication paths table

This table is useful to IT security groups and those configuring network devices such as switches, router, firewalls, etc. When monitoring network traffic, the paths below illustrate the expected behavior in the system.

Figure 1.5.1.1 Communications Path Table

| Path | Connected Equipment Gateway (CEG) | | | | | | Direction / use requiement[2] | | Connecting Component | | Notes |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Function | Interface | Default Port Assignment | Protocol | Default Port State[1,2] | Port Activity (if enabled) | | | Default Port Assignment [3,4] | Internet access[4] | |
| **A** | **Azure IoT Hub SDK** | | | | | | Required | | **CEG cloud** | | |
| | Data to cloud | Ethernet or USB-Wi-Fi[5] | 443 | MQTTS | Enabled | ∞ | ▶ | | - | 4G LTE | [5]Wi-Fi in client mode |
| **B** | **Device Management Client** | | | | | | Required | | **Device Management services** | | |
| | Firmware update (FOTA) | Ethernet or USB-Wi-Fi | - | LWM2M with DTLS | Enabled | On demand | | ◀ | 5671 | 4G LTE | CoAP, AQMPS used as required |
| | Secure Bootstrapping and Provisioning | Ethernet or USB-Wi-Fi | - | LWM2M with DTLS | Enabled | On demand | | ◀ | 5684 | 4G LTE | CoAP, AQMPS used as required |
| **C** | **DNS Client** | | | | | | Required | | **Public Internet – DNS Server** | | |
| | DNS Client | Ethernet or USB-Wi-Fi | 53 | DNS | Enabled | On demand | | ◀ | 53 | 4G LTE | |
| **D** | **NTP Client** | | | | | | Required | | **Public Internet – NTP Server** | | |
| | NTP Client | Ethernet or USB-Wi-Fi | 123 | NTP | Enabled | On demand | | ◀ | 123 | 4G LTE | |
| **E** | **ICMP Client** | | | | | | Required | | **Public Internet –Status check** | | |
| | ICMP Client (Ping) | Ethernet or USB-Wi-Fi | NA | ICMP (ping) | Enabled | On demand | | ◀ | NA | 4G LTE | www.google.com (or) www.MSNCSI.com |
| **F** | **Local Service UI** | | | | | | Required | | Service laptop / device | | |
| | Service UI webserver | USB-Wi-Fi adapter access point mode | 443 | HTTPS | Enabled | On demand | ▶ | | - | No | |
| **G** | **Local Data Collection** | | | | | | Required | | SC-EQUIP | | |
| | BACnet read property | RS-485 port or RS-485 port w/ TMC | N/A RS-485 Serial | BACnet/ MSTP | Enabled | ∞ | | ◀ | N/A RS-485 Serial | No | |

# 2 Deployment

This section is designed to help execute the deployment phase of your system. The contents within this section address how to initiate secure deployment for new installations, how to harden your attack surface and additional steps after commissioning required before the new or upgraded system is turned over to runtime operations.

### 2.1.0 Deployment overview

Security hardening begins prior to deployment with careful planning as outlined in section 1 of this guide. It is a good practice to review sections prior to deployment to fully understand the security feature set, its architecture, data flow and requirements before physically installing and making application specific configuration changes.

In this section more details are provided to help the installer prepare for deployment:

- Physical installation considerations
- Default security behavior
- Resetting factory defaults
- Considerations for commissioning
- Recommended knowledge level

Before you start the installation of your solution, consider the guidance in the following sections.

### 2.1.1 Physical installation considerations

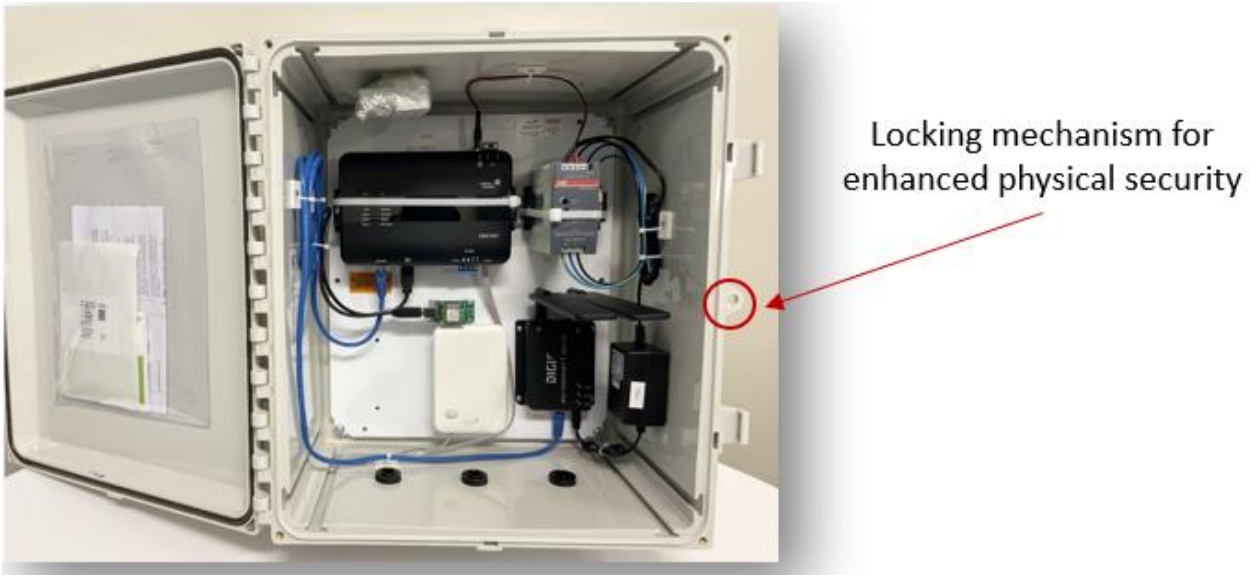
Install hardware using the instructions provided in the installation guide. Keep in mind that the physical access to the device and physical installation of the device can impact the cybersecurity.

Physical access to certain devices enable actions that cannot be authenticated and logged electronically through the capabilities of this product. To prevent unauthorized access, be sure to place the device in a room, cabinet or enclosure that can restrict access (for example, mechanical lock or physical access control).

Some products are equipped with an optical tamper switch that you can use to send and log electronic alerts regarding physical tampering of the installation. Consider using protective electric wire conduits when communication wires with paths through areas of lower trust.

The CEG is packaged and sold as a panelized solution, complete with power supply and cellular modem in an outdoor rated enclosure, with the option of a wireless TMR. The panel mounting hardware provides flexibility in the installation location within the chiller plant and provides a layer of physical hardening when the case is locked shut.

Figure 2.1.2.1 – Locking enclosure




### 2.1.2 Default security behavior

On the initial startup, certain functions will be enabled to facilitate the most common commissioning tasks. Examples may include

- User account settings (example: changing password on first login)
- Enhanced password validation
- A configuration webpage

### 2.1.3 Considerations for commission

In some applications the default settings may not be sufficient to fully commission the system. Functions that will not be used during the commissioning process should be disabled.

In the commissioning phase, a less secure configuration may be used before the full infrastructure is available to speed up the deployment process (for example, using wireless). Once the commissioning phase is complete, be sure to remove the temporary infrastructure and harden the system further before turning over to full runtime operations.

### 2.1.4 Recommended knowledge level

The person confirming that the proper hardening steps are executed should be experienced in your product's administration and networking technologies. If training for your product(s) exist, completion of the basic installation course is required, and any advanced installation course is recommended.

### 2.2.0 Hardening

While many products include secure-by-default safeguards, additional hardening is usually required to meet the security requirements of the target environment. It is important to apply to the correct level of protection as warranted by the customer policies and government regulations that may govern the application security settings for this deployment.

### 2.2.1 Hardening checklist

While Connected Chillers components have several secure-by-default safeguards, we recommend additional hardening to meet the security requirements of the target environment. This checklist provides an example list of hardening steps you may select to go through. The actual steps you will take is based upon the features included within your specific environment as gathered in Section 1.3.0.

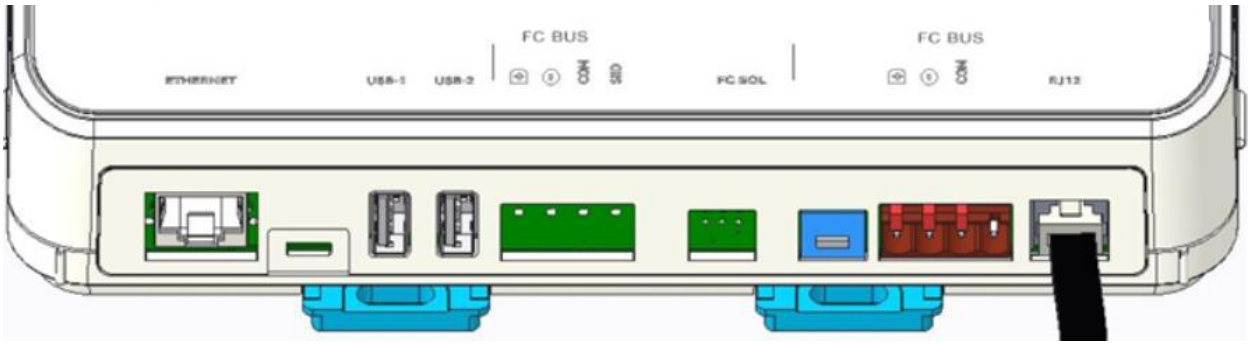
- For steps that are not applicable to your instance, check off the “N/A” column
- As you complete the remaining steps, check off or include the date these were completed

| Hardening Step | Status | |
|---|---|---|
| | Complete | N/A |
| **1. CEG Hardening** | - | - |
| 1.1: Remove USB Wi-Fi adapter if wireless is not permitted (conditional) | ☐ | ☐ |
| 1.2: Secure USB cable within enclosure (conditional) | ☐ | ☐ |
| 1.3: Change connection defaults (admin user / wireless) | ☐ | - |
| 1.3.1 Changing Wi-Fi Access Point settings after initial logon (optional) | ☐ | ☐ |
| 1.4: Create unique user accounts | ☐ | ☐ |
| 1.5: Configure modem communication mode (wired or wireless) | ☐ | - |
| 1.6: Update software (manual only if required) | ☐ | - |
| 1.7: Review supporting functions | - | - |
| 1.7.1 - Audit Logs | ☐ | - |
| 1.7.2 - Reset Functions | ☐ | - |
| | | |
| **2. SC-Equip Hardening** | - | - |
| 2.1: Inventory equipment connected to the MS-TP and MTR networks | ☐ | - |
| 2.2: Verify SC-Equip bus used for the MS-TP network | ☐ | - |
| 2.3: Confirm firmware version and bus status for each SC-Equip | ☐ | - |
| | | |
| **3. Document Deployment Details** | ☐ | - |
| | | |

**CEG hardening**

To harden the CEG, it is necessary to log on to the CEG through its User Interface, the CEG UI. The technician uses the CEG UI to make the necessary configuration changes which strengthen the security of the CEG's IP enabled interfaces. These interfaces are used for local administration and internet-facing cloud services. It is important to minimize the attack surface and ensure that the remaining active interfaces have the appropriate level of protection.

Figure 2.2.1.1 – CEG ports




### 2.2.2 Determine internal communication types

The CEG can be configured for wired or wireless communications for service and modem connections as described in this table:

Table 2.2.2.1 – CEG Connections

| CEG Connection | Wireless path | Wired path | Preferred path |
|---|---|---|---|
| Service laptop/mobile device | USB Wi-Fi adapter (access point mode) | micro-USB port | Wireless |
| Modem | USB Wi-Fi adapter (client mode)[1] | Ethernet | Wired |

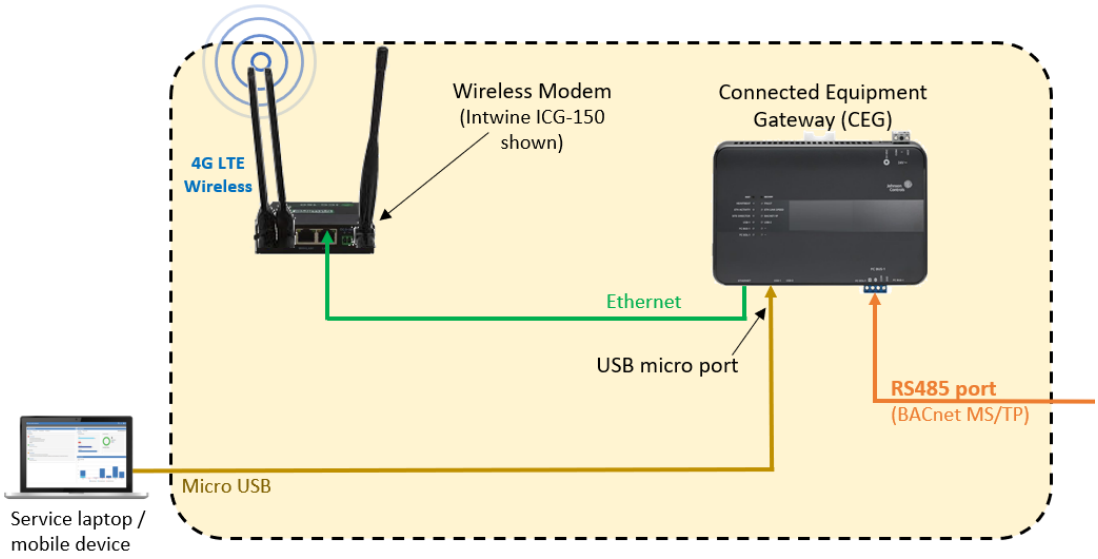
[1]Wi-Fi client mode requires use of modem with Wi-Fi capability (e.g. Intwine ICG-150)
NOTE: Digi WR11 modems do not support this communication mode.

Both forms of Wi-Fi communication are enabled by plugging the USB Wi-Fi adapter into the CEG USB port.

Step 1.1 – Remove USB Wi-Fi adapter if wireless is not permitted (conditional)

If the customer does not permit wireless in the environment, wired connections must be established for each path and the USB Wi-Fi adapter should be removed from the CEG.

Figure 2.2.2.1 – Service laptop / Mobile device connection




### Step 1.2 – Secure USB cable within enclosure (conditional)

If a wired service connection is utilized, ensure that the micro-USB cable is secured inside the lockable CEG enclosure to prevent unauthorized use of the service interface. Technicians should be instructed to always return the cable to its secure location and lock inside the CEG enclosure before leaving.

## 2.2.3 Changing connection defaults (admin user / wireless)

Before you begin, locate the factory printed default Wi-Fi parameters label within Connected Equipment Gateway CEG1001 Quick Start Guide (Part No. 24-11460-00042). This document comes with the CEG and will be used for reference throughout this procedure.

Figure 2.2.3.1 CEG Factory Printed Label

**Wi-Fi SSID:** CEG-GATEWAY

**Wi-Fi Passphrase:** Place label here

**UI Username:** admin

**UI Password:** Place label here

**Device ID:** Place label here

### Step 1.3 - Change connection defaults (admin user / wireless)

For the initial access to the CEG UI, execute the following steps:

1. Establish the respective connection between the Laptop/Service Device and the CEG (see wireless and wired instruction within table:

| **Wi-Fi service connections -** | **USB service connections –** |
|---|---|
| a) Plug the Wi-Fi adapter into the USB port. | a) Ensure the CEG is powered off |
| b) Verify that the Wi-Fi AP LED is flashing. | b) Connect a laptop to the CEG using a USB cable between the device and CEG USB port |
| c) Access the Wi-Fi settings on your Wi-Fi connected mobile phone, tablet, or computer. | c) Power up the CEG |
| d) Click the default Wi-Fi SSID and enter the Wi-Fi Passphrase (see factory label figure 2.2.3.1). | e) The Remote Network Driver Interface Specification (RNDIS) driver should be installed automatically. If it does not, then the RNDIS will need to be manually installed |
| | f) Verify you're connected with a static IP configuration by viewing your network setting properties (i.e., 192.168.142.2) |

2. Open a web browser and enter https://cegwy.jci.com or **192.168.142.1** as the browser address.

   **Note:** Ignore the "***Your connection is not private***" warning and proceed to https://cegwy.jci.com.

3. Use the factory default UI Username and UI Password.

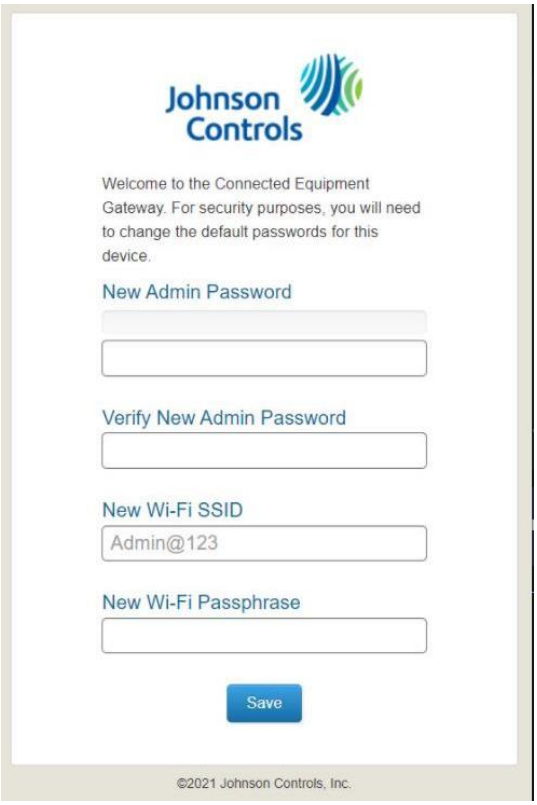
4. Read and accept the CEG license agreement.

   The first time you log on to the CEG, you must change the following:

   - CEG UI Admin password
   - USB Access Point Wi-Fi SSID
   - USB Access Point Wi-Fi passphrase

   NOTE: It is still necessary to configure Wi-Fi parameters for installations not utilizing Wi-Fi as part of the initialization process.

Figure 2.2.3.1 –CEG Logon screen




See figure 2.2.3.2 for guidance:

Figure 2.2.3.2 –CEG field formation rules

| | UI Admin password | Wi-Fi SSID | Wi-Fi Passphrase |
|---|---|---|---|
| Length (permitted) | 8-32 characters | 2-32 characters | 8-63 characters |
| Minimum | 8 | To accommodate non-guessable values | 8 |
| Recommended | 12+ | | 12+ |
| Supported character types | printable characters plus the space (ASCII 0x20), @, ?, ", $, [, \, ], and + | printable characters plus the space (ASCII 0x20) | printable characters plus the space (ASCII 0x20) |
| Unsupported character types | N/A | ?, ", $, [, \, ], and + | ?, ", $, [, \, ], and + |
| Case-sensitive | Yes | Yes | Yes |
| Formation guidance | Avoid guessable values – Use a mix of case, alpha, numeric and special characters, and randomness to make entries harder to guess | | |
| Formation rules | Yes | Not enforced | Not enforced |
| Mixed case | At least one upper and lower case | | |
| Numbers | At least one number | | |
| Blocked | Common passwords | | |

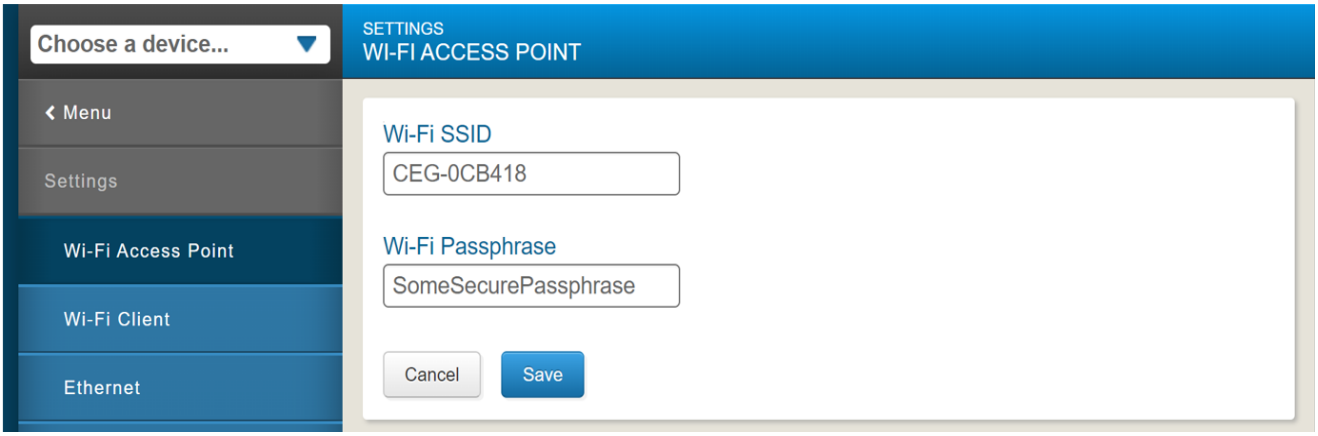
**Important for Wi-Fi connections:** After you change the Wi-Fi passphrase and SSID, the web server restarts, and you need to re-establish connection to the CEG. If using Wi-Fi be sure to use the new SSID and passphrase. On some computers and mobile devices, click on the original Wi-Fi network before you rejoin the network with the new passphrase.

#### Step 1.3.1 – Changing Wi-Fi Access Point settings after initial logon (optional)

To change the Wi-Fi Access Point settings after the first logon, select **Settings> Wi-Fi Access Point** from the CEG UI menu.

The Wi-Fi SSID and Passphrase may be modified from this menu by users assigned the “Admin” or “Tech” roles.

Figure 2.2.3.3 – Wi-Fi Access Point screen




### 2.2.4 CEG User Management

The **Admin** account should only be used for the initial configuration. Each CEG user should be given their own unique user account, including administrators. Use of unique user accounts is necessary for proper tracking of user activity which is captured in the audit log.

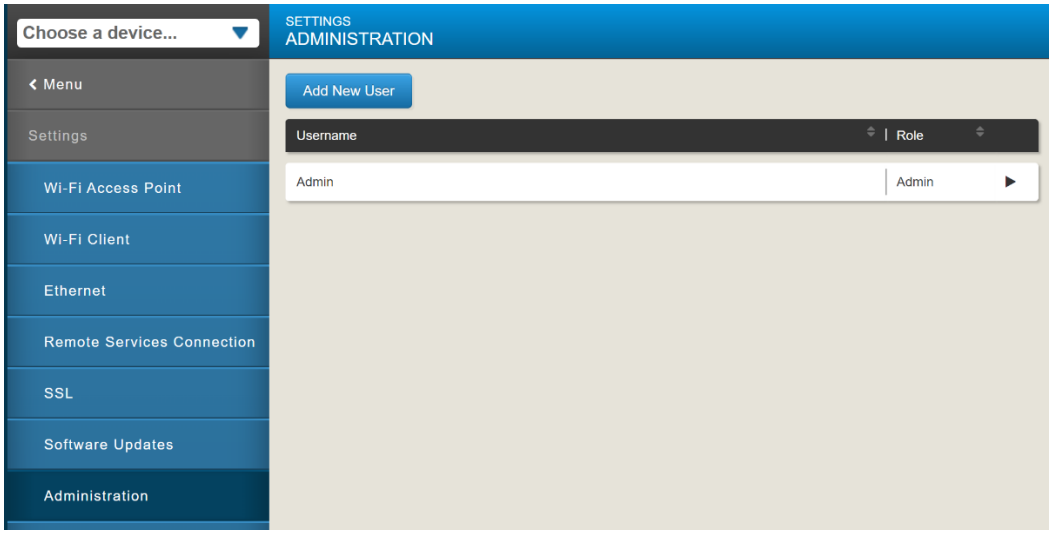
#### Step 1.4 – Create unique user accounts

To manage user accounts, select **Settings> Administration** from the CEG UI menu.

The Administration Settings screen requires Administrator access. On this screen an administrator can add or delete users, define user roles, and change passwords.

From the Administration Settings screen, you can add/modify user accounts.

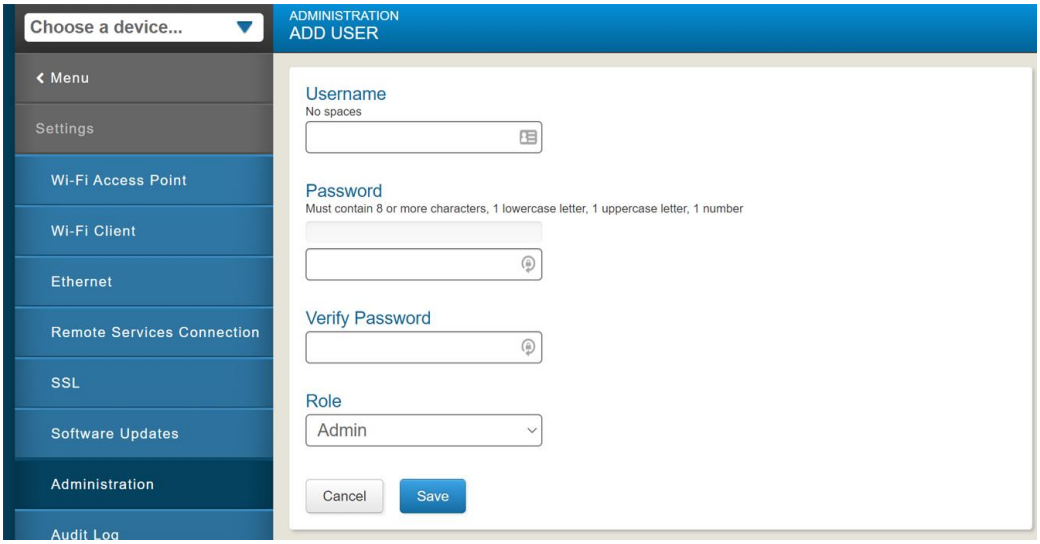
Figure 2.2.4.1 – CEG Administration screen

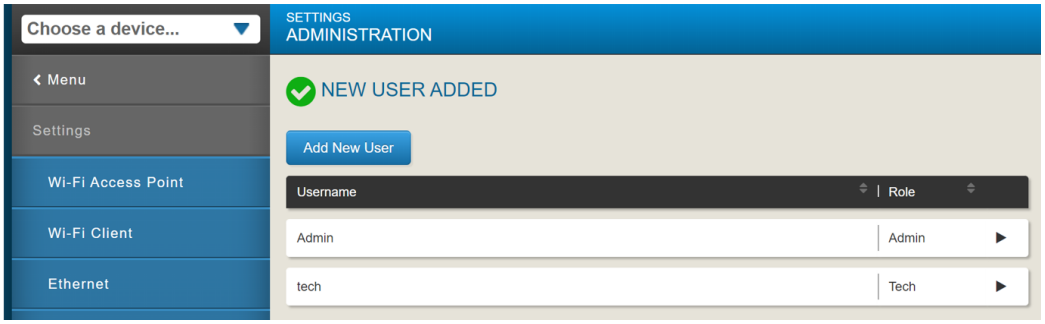



When editing a user, you can set the password and user role. The following user roles are available:

- **Admin** – user have full access including user management
- **Tech** – user can modify the configuration, but cannot manage user accounts
- **Tenant** – role is not used.

Figure 2.2.4.2 – CEG Add User screens



### 2.2.5 CEG – Configure Modem Communication Mode

The CEG uses an internet connection to stream telemetry data to the cloud. The CEG is connected to the internet through an Ethernet or Wi-Fi connected modem.

You will need to determine how the CEG will communicate with the Modem. To reduce security risk, modem communications should be set as wired or wireless but not both. Wired Ethernet connections are more secure than Wi-Fi connections as a physical connection to the network is required.

#### Step 1.5 – Configure modem communication mode (wired or wireless)

Option 1 – Ethernet (preferred)

- To enable wired Ethernet communications to the modem:
    a. Log on to the CEG local UI using the CEG Wi-Fi connection
    b. To configure a wired Ethernet connection, select **Settings > Ethernet**, and enter the necessary data as outlined in the following table:

| Field | Setting |
|---|---|
| Ethernet | On (default) |
| Auto DNS Configure | On (default) |

Option 2 – To enable wireless Wi-Fi Client Mode communications to the modem:

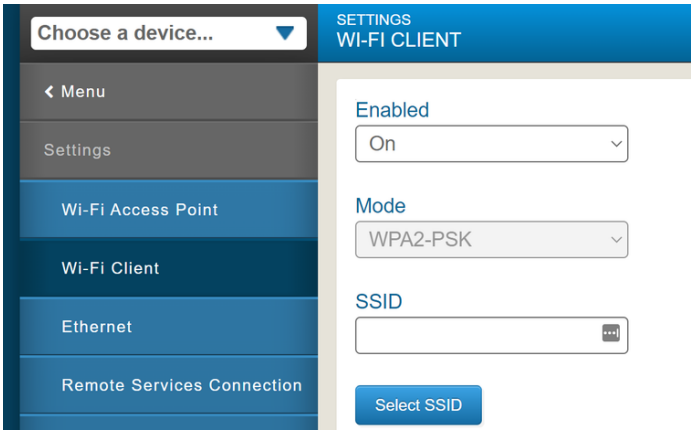
1) Disable Ethernet communications first to prevent a dual path between the modem and CEG –
    a. Log on to the CEG local UI using the CEG Wi-Fi connection
    b. To configure an Ethernet cable connection, select **Settings > Ethernet**, and set the “Ethernet” field to “Off”:

| Field | Setting |
|---|---|
| Ethernet | Off |

2) To enable wireless Wi-Fi communications to the modem via Wi-Fi Client mode:
    a. Ensure the CEG Wi-Fi adapter is connected to a USB port on the CEG
    b. Select **Settings > Wi-Fi Client** from the CEG UI.
    c. At the top of the “Wi-Fi Client” page, use the dropdown menu to set the “Wi-Fi Client” field to “On”.

| Field | Setting |
|---|---|
| Wi-Fi client | On |

Figure 2.2.5.1 – CEG Wi-Fi Client screen

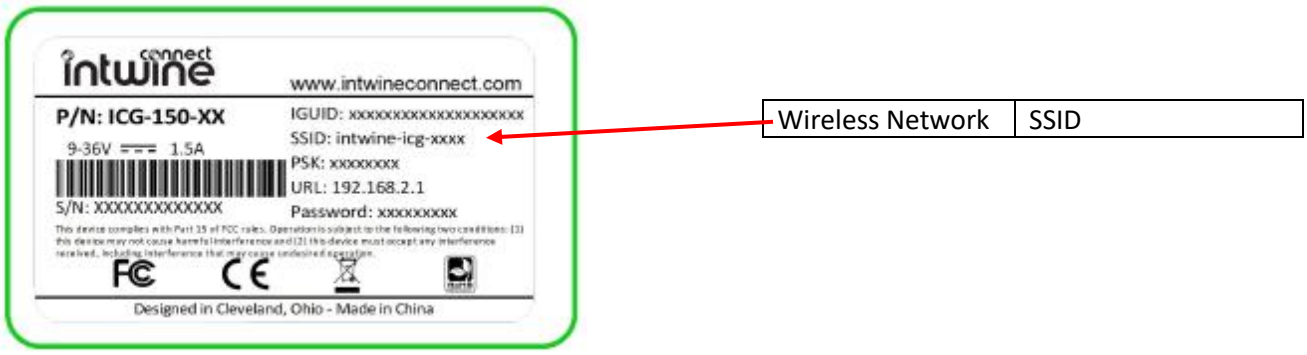



d. In the field “Client SSID”, enter the SSID of the wireless network that the CEG will be connecting to. In the field “Passphrase”, enter the passphrase for the wireless network the CEG will be connecting to.

| Field | Setting |
|---|---|
| Client SSID | As configured in the modem |
| Passphrase | As configured in the modem |

If your site is using the Intwine ICG-150 modem, the default SSID is located on the device label.

Figure 2.2.5.2 – Intwine ICG-150 product connection details label




e. At the bottom of the screen, click “Save”. Once the changes have saved, the “Authentication Status” and “Connection Status” fields will indicate if the CEG has connected to the wireless network successfully.

### 2.2.6 CEG –Software Updates

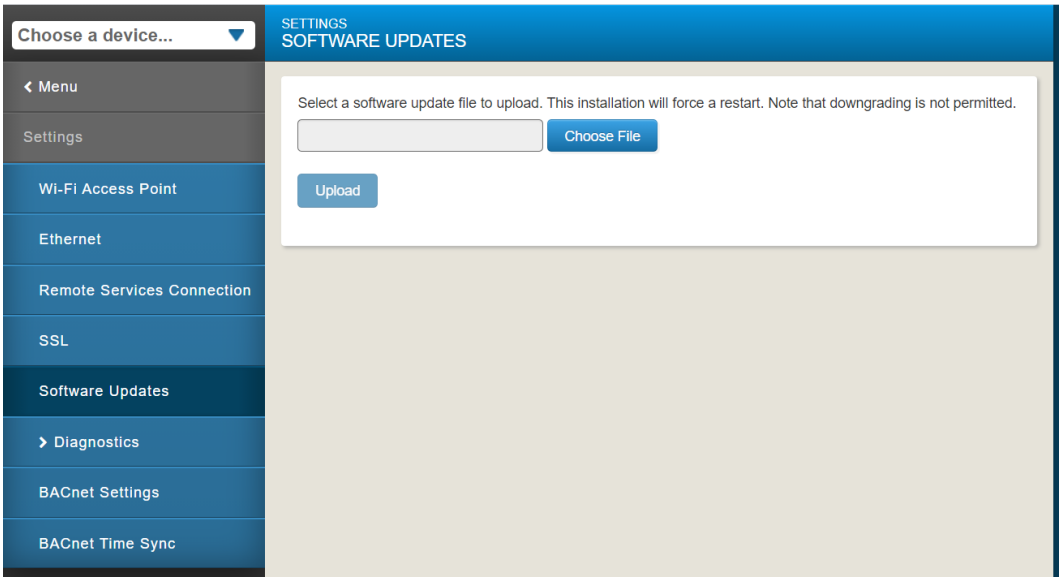
CEG device also receives software upgrade automatically from cloud when new version of software is available via the remote services connection. CEG checks for software upgrade package during startup, when remote connection is re-established and periodically during an established connection.

#### Step 1.6 – Update software (manual only if required)

With the cloud service, local updates of the CEG are not required. However, it is possible to manually update the CEG. This may be necessary if an update is required before a connection to the cloud can be established.

1) Log on to the CEG local UI using the CEG Wi-Fi connection
2) Select **Settings > Software Update and s**elect **Choose File**
3) Select a file that is accessible from the laptop or mobile device connecting to the CEG.
4) Select **Upload** from the Software Update screen to transfer the file to the CEG.

Figure 2.2.6.1 – CEG Software Updates screen




5) Click the **Install Button** to have CEG use the new file.
6) The CEG goes offline temporarily while the updates are applied, during which time you may see a **Connection Problem** message.

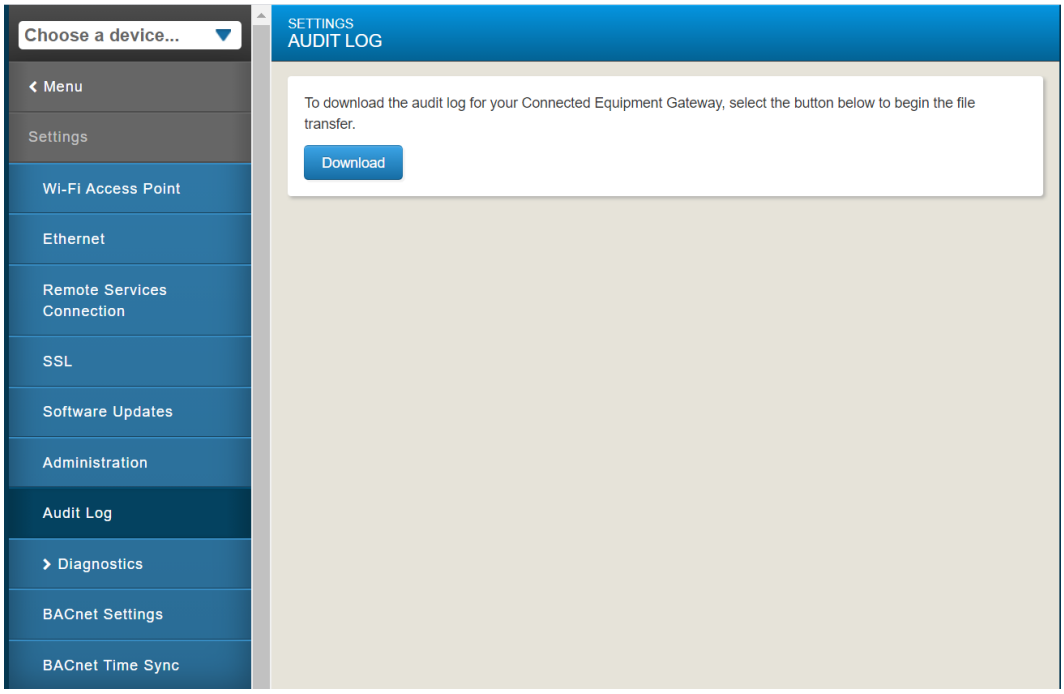
### 2.2.7 CEG – Audit Log

The audit log provides valuable information that can be used for both functional troubleshooting and security investigations.

#### Step 1.7.1 – Review support functions – Audit Logs

The audit log provides a user readable text file that shows actions taken on the local CEG user interface:

Figure 2.2.7.1 – CEG Audit Log screen




The audit log may be downloaded to the laptop or mobile device connecting to the CEG by selecting the **Download** button

Figure 2.2.7.2 - Example Audit Text File

```
Aug 19 16:25:39 CEG00108D0CB40E node[1414]: 2021-08-19T16:25:39.529Z CEG00108D0CB40E tangerine[1414]:Admin logged in.
Aug 19 17:13:46 CEG00108D0CB40E node[1414]: 2021-08-19T17:13:46.827Z CEG00108D0CB40E tangerine[1414]:Admin logged out. (session timed out)
Aug 20 18:33:50 CEG00108D0CB40E node[1414]: 2021-08-20T18:33:50.117Z CEG00108D0CB40E tangerine[1414]:Admin logged in.
Aug 27 17:26:17 CEG00108D0CB40E node[1414]: 2021-08-27T17:26:17.787Z CEG00108D0CB40E tangerine[1414]:Admin logged in.
Aug 27 17:27:48 CEG00108D0CB40E node[1414]: 2021-08-27T17:27:48.005Z CEG00108D0CB40E tangerine[1414]:[10.9.140.5] Admin uploaded a software update package ceg-test-1.0.0.1411.cgi
Aug 27 17:27:51 CEG00108D0CB40E node[1414]: 2021-08-27T17:27:51.983Z CEG00108D0CB40E tangerine[1414]:[10.9.140.5] CEG Upgrade from version 1.0.0.1392 to 1.0.0.1411 was initiated by Admin
Aug 27 17:29:32 CEG00108D0CB40E node[1414]: 2021-08-27T17:29:32.229Z CEG00108D0CB40E tangerine[1414]:Provision Progress 5% Complete
Aug 27 17:29:43 CEG00108D0CB40E node[1414]: 2021-08-27T17:29:43.809Z CEG00108D0CB40E tangerine[1414]:Provision Progress 10% Complete
Aug 27 17:29:56 CEG00108D0CB40E node[1414]: 2021-08-27T17:29:56.829Z CEG00108D0CB40E tangerine[1414]:Provision Progress 15% Complete
Aug 27 17:30:08 CEG00108D0CB40E node[1414]: 2021-08-27T17:30:08.517Z CEG00108D0CB40E tangerine[1414]:Provision Progress 20% Complete
Aug 27 17:30:18 CEG00108D0CB40E node[1414]: 2021-08-27T17:30:18.586Z CEG00108D0CB40E tangerine[1414]:Provision Progress 25% Complete
Aug 27 17:30:27 CEG00108D0CB40E node[1414]: 2021-08-27T17:30:27.217Z CEG00108D0CB40E tangerine[1414]:Provision Progress 30% Complete
Aug 27 17:30:33 CEG00108D0CB40E node[1414]: 2021-08-27T17:30:33.290Z CEG00108D0CB40E tangerine[1414]:Provision Progress 35% Complete
Aug 27 17:30:39 CEG00108D0CB40E node[1414]: 2021-08-27T17:30:39.393Z CEG00108D0CB40E tangerine[1414]:Provision Progress 40% Complete
Aug 27 17:30:45 CEG00108D0CB40E node[1414]: 2021-08-27T17:30:45.396Z CEG00108D0CB40E tangerine[1414]:Provision Progress 45% Complete
Aug 27 17:31:06 CEG00108D0CB40E node[1414]: 2021-08-27T17:31:06.643Z CEG00108D0CB40E tangerine[1414]:Provision Progress 50% Complete
Aug 27 17:31:21 CEG00108D0CB40E node[1414]: 2021-08-27T17:31:21.212Z CEG00108D0CB40E tangerine[1414]:Provision Progress 55% Complete
Aug 27 17:31:34 CEG00108D0CB40E node[1414]: 2021-08-27T17:31:34.164Z CEG00108D0CB40E tangerine[1414]:Provision Progress 60% Complete
Aug 27 17:31:45 CEG00108D0CB40E node[1414]: 2021-08-27T17:31:45.845Z CEG00108D0CB40E tangerine[1414]:Provision Progress 65% Complete
Aug 27 17:32:03 CEG00108D0CB40E node[1414]: 2021-08-27T17:32:03.265Z CEG00108D0CB40E tangerine[1414]:Provision Progress 70% Complete
Aug 27 17:32:13 CEG00108D0CB40E node[1414]: 2021-08-27T17:32:13.239Z CEG00108D0CB40E tangerine[1414]:Provision Progress 75% Complete
Aug 27 17:32:23 CEG00108D0CB40E node[1414]: 2021-08-27T17:32:23.188Z CEG00108D0CB40E tangerine[1414]:Provision Progress 80% Complete
Aug 27 17:32:34 CEG00108D0CB40E node[1414]: 2021-08-27T17:32:34.452Z CEG00108D0CB40E tangerine[1414]:Provision Progress 85% Complete
Aug 27 17:32:46 CEG00108D0CB40E node[1414]: 2021-08-27T17:32:46.387Z CEG00108D0CB40E tangerine[1414]:Provision Progress 90% Complete
Aug 27 17:33:02 CEG00108D0CB40E node[1414]: 2021-08-27T17:33:02.410Z CEG00108D0CB40E tangerine[1414]:Provision Progress 95% Complete
Aug 27 17:33:12 CEG00108D0CB40E node[1414]: 2021-08-27T17:33:12.302Z CEG00108D0CB40E tangerine[1414]:Provision Progress 100% Complete
Aug 27 17:33:30 CEG00108D0CB40E device_manager[1197]: Rebooting Now - Graceful
Aug 30 18:04:11 CEG00108D0CB40E node[1492]: 2021-08-30T18:04:11.511Z CEG00108D0CB40E tangerine[1492]:Admin logged in.
Aug 30 18:52:18 CEG00108D0CB40E node[1492]: 2021-08-30T18:52:18.621Z CEG00108D0CB40E tangerine[1492]:Admin logged out. (session timed out)
Aug 30 20:06:11 CEG00108D0CB40E node[1492]: 2021-08-30T20:06:11.766Z CEG00108D0CB40E tangerine[1492]:Admin logged in.
Aug 30 20:06:24 CEG00108D0CB40E node[1492]: 2021-08-30T20:06:24.861Z CEG00108D0CB40E tangerine[1492]:Admin logged out.
Aug 30 20:07:18 CEG00108D0CB40E node[1492]: 2021-08-30T20:07:18.369Z CEG00108D0CB40E tangerine[1492]:Admin logged in.
Aug 30 20:55:21 CEG00108D0CB40E node[1492]: 2021-08-30T20:55:21.818Z CEG00108D0CB40E tangerine[1492]:Admin logged out. (session timed out)
Sep  1 13:13:23 CEG00108D0CB40E node[1492]: 2021-09-01T13:13:23.375Z CEG00108D0CB40E tangerine[1492]:Admin logged in.
Sep  1 13:20:02 CEG00108D0CB40E node[1492]: 2021-09-01T13:20:02.774Z CEG00108D0CB40E tangerine[1492]:User Tenant is created by Admin.
Sep  1 13:20:05 CEG00108D0CB40E node[1492]: 2021-09-01T13:20:05.426Z CEG00108D0CB40E tangerine[1492]:Admin logged out.
```

### 2.2.8 CEG –Reset Functions

Use the following reset functions of the CEG if you are unable to communicate to the CEG or cannot logon do to lost credentials. There are two types of reset functions:

- Network Reset – only the network settings are reset
- Factory Defaults – all settings are restored to factory defaults

Step 1.7.2 – Review support functions – Reset Functions

Use the instructions in the following sections according to the type of reset you require. For both resets, the following information applies:

- The reset button is located on the front of the device. To reach the reset button, use a small screwdriver or similar tool.
- If the CEG is connected to the network when you press the reset button, it disconnects from the network.
- If you press and hold the reset button for more than nine seconds, the reset operation cancels.
- If a fault condition already exists, the reset button does not work.

**Network Reset**

The Network Reset function resets Wi-Fi and Ethernet settings. Use this function if you forget your Wi-Fi connection information. To reset the Wi-Fi and Ethernet settings, complete the following steps:

1. Press and hold the RESET button for two seconds. The FAULT LED flickers slowly.
2. Release the RESET button within three seconds. The FAULT LED continues to flicker slowly.
3. Within five seconds, press the RESET button again, and then immediately release it to confirm that you want to reset the Wi-Fi and Ethernet settings. If you do not press the RESET button to confirm within five seconds, the reset operation is canceled.

The Wi-Fi SSID, passphrase, and Ethernet are set to factory defaults. The LEDs stop flickering for two seconds, then the LEDs return to normal operation based on the current state of the device.

**Reset to factory defaults**

The Reset to Factory Defaults function resets all device settings including user profiles. The function also resets your SSL certificate to the Johnson Controls self-signed certificate that is included in the device. This function is for administrators who want to clear all user profiles from a device. The Reset to Factory Defaults function does not change the version of the software. If you run a software upgrade, the CEG retains the upgraded software version and does not reset to the factory default version.

To reset to factory defaults, complete the following steps:

1. Press and hold the RESET button for six seconds. After two seconds, the FAULT LED flickers slowly. After an additional four seconds of holding the RESET button, the FAULT LED changes to a faster flicker.

2. Release the RESET button within three seconds of seeing a fast flicker. The FAULT LED continues to flicker quickly.
3. Within five seconds, press the RESET button again, and then immediately release it to confirm that you want to reset to factory defaults. If you do not press the RESET button to confirm within five seconds, the reset operation is canceled.

All device settings reset to factory defaults. The LEDs stop flashing for two seconds, and then the LEDs return to normal operation based on the current state of the device.

### 2.2.8 SC-Equip Hardening

Each connected JCI/York/Wuxi branded chiller is equipped with SC-Equip board which enables BACnet communications to those chillers. The SC-Equip board has two RS-485 bus network ports, the CS bus and the BAS/FC bus. Only one bus throughout the system should be utilized to ensure all equipment on these BACnet networks are accessible. The bus type to use is determined by the following guidance:

| Bus Type | Equipment Brands | Security |
|---|---|---|
| CS Bus | Use only when **ALL** connected equipment is JCI, York or Wuxi branded | **Read-only Protected** – The SC-Equip board limits communication to the chillers to read-only commands. This mode is not supported by third-party devices. |
| BAS (FC) Bus | Must be used if any equipment on the BACnet network is from a third-party | **No protection** – The SC-Equip permits both read and write commands. This mode is necessary for third-party device support. |

#### Step 2.1 - Inventory equipment connected to the MS-TP and MTR networks

To ensure that the correct bus type is utilize, inventory all BACnet connected equipment.

#### Step 2.2 - Verify SC-Equip bus used for the MS-TP network

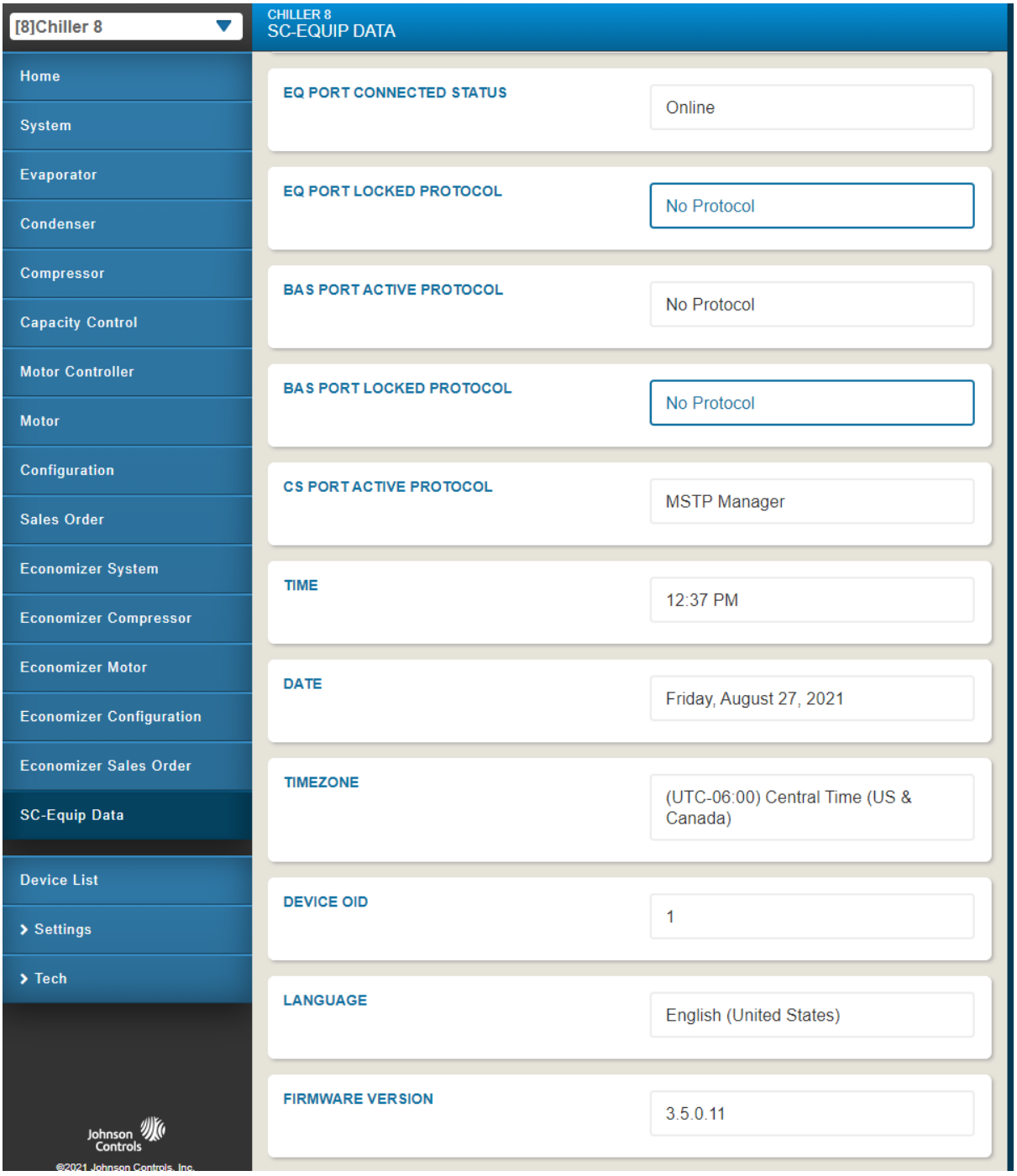
Review the inventory of connected equipment. If all devices are JCI, York or Wuxi branded, the BACnet/MSTP network should be wired to CS Bus port on each SC-Equip board. Otherwise, the BACnet/MSTP network should connect to the BAS (FC) Bus port on each SC-Equip board.

#### Step 2.3 – Confirm firmware version for each SC-EQUIP

The SC-EQUIP firmware should be confirmed via the CEG UI for each SC-Equip controller.  The minimum FW version recommended on SC-Equip is 3.5.x.x.

Select **SC-Equip Data** from the menu:

Figure 2.2.8.2 – CEG SC-EQUIP Data screen




.

### 2.2.9 Security audits and documentation

A well-documented deployment of the solution will be useful in security audits, and a security audit can expose errors in the system documentation and identifying gaps in protection. Each task feeds the other and it may be necessary to repeat hardening step 19, after an audit is complete and the gaps are addressed.

#### Hardening step 22: Security documentation

Document deployment once hardening is sufficient for run-time operations. When updates are released, or security advisories are published this documentation will be useful. The documentation will allow for quick assessment to determine if the deployment is impacted by the issues described in a security advisory and requires a configuration change, software update or patch.

Include the following details in creating as-built security documentation:

- As-built architecture drawing of system
- For all system components record:
  - Component identification
    - Name
    - Description
    - Device Type
    - Location
    - Vendor
    - Model
    - IP address
    - MAC address
  - Support details
    - Software version
    - Hardware version
    - Licenses
    - Installation date
  - Communication configuration details
    - Enabled Ports and protocols
    - Encryption settings