

# Connect+

Administrator User Guide



# Contents

<b>1 Getting Started with Connect+</b> .....	<b>1</b>
1.1 What Connect+ Can Do.....	1
<b>2 Onboard Stores</b> .....	<b>2</b>
2.1 Become Familiar with Store Assets Hierarchy.....	2
2.2 Onboard Directories.....	2
2.2.1 Add Parent Directory.....	2
2.2.2 Add Subdirectory .....	3
2.3 Adding Sites .....	3
2.4 Add Control System and Obtain Controller Information.....	5
2.4.1 Configuring the Site Supervisor/E3 and E2 to Communicate with Connect+ Mixed Sites .....	6
2.5 Verify Control System Connection.....	9
2.6 Verify Tree Structure & Enterprise Summary .....	10
<b>3 Onboard Users</b> .....	<b>11</b>
3.1 Create User Group to define Privilege and Sites Access .....	11
3.2 Create User.....	13
3.3 User Expiration .....	15
3.3.1 Configure User Expiration Type.....	15
3.3.2 Reactivate User .....	16
3.4 User Lockout .....	16
<b>4 Complex Password</b> .....	<b>17</b>
4.1 Enable Complex Password .....	17
4.2 Configure Password.....	17
<b>5 Configure Advisory Receiving and Advisory View</b> .....	<b>18</b>
5.1 Get Familiar with Advisories.....	18
5.2 Configure Advisories Received from Controller .....	18
5.3 Advisory Receiver Commission .....	20
5.4 Enable Advisory Map .....	22
<b>6 Configure Advisory &amp; Graph Map Manager</b> .....	<b>23</b>
6.1 Advisory & Graph Mapping.....	23
6.2 Point & Critical Information Mapping.....	24
<b>7 Configure XWEB Mapping</b> .....	<b>26</b>
7.1 Download XWEB Server Device Map File.....	26
7.2 Configure XWEB Server Device Map File .....	27
7.2.1 Configure DixellEVOApplicationTypeMap.csv file.....	27
7.2.2 Configure DixellEVOUIDMapping.csv file .....	28
7.2.3 Configure DixellEVOSetpointTemplate.csv file .....	28
7.2.4 Configure Aliases File.....	31
7.3 Upload XWEB Server Device Map File.....	31

- 8 System Schedule Configuration..... 32
- 9 Enable Advanced Security for Admin organization (Optional) ..... 34
  - 9.1 Multi-Factor Authentication ..... 34
    - 9.1.1 Configure Multi-Factor Authentication ..... 34
    - 9.1.2 Login with Multi-Factor Authentication ..... 34
  - 9.2 Single Sign-on ..... 35
    - 9.2.1 Configure Single Sign-on ..... 35
    - 9.2.2 Login with Single Sign-on ..... 36
    - 9.2.3 Privilege of New User Login with Single Sign-on..... 37
    - 9.2.4 Auto-binding SSO User Account with Connerct+ User ..... 37
- 10 Configure Energy Analysis Report ..... 38
- Appendix A: Group Privileges, Descriptions, and Protocol Access Levels ..... 39

# 1 Getting Started with Connect+

## 1.1 What Connect+ Can Do

Connect+ is designed for **Store Manager, Technician, Food Safety Manager, Energy Manager and Regional Managers** to monitor, control or manage their store's or region's information. Connect+ enables a quick store crisis diagnosis and provides data-driven store optimization in a secure and easy way.

This guide provides a **step-by-step guide for Administrators** on how to configure Connect+ for the Enterprise before other users can access the software.



## 2 Onboard Stores

### 2.1 Become Familiar with Store Assets Hierarchy

This section will introduce the basic Store Hierarchy in Connect+. As Administrators can see from the **Navigation Tree** of the Connect+ landing page interface, a Store Hierarchy is reflected by the navigation tree comprising **Directory, Site, Control System, Unit, Application Type, Application and Point Levels**.

#### Directory

A Directory is the region where a customer is located. Connect+ offers a sub-directory under the parent directory to reflect a customer's own organization structure.

#### Sites

Sites are stores within a customer's organization. One site belongs to only one Directory.

#### Control System

A control system is a set of controllers within one localized store. A typical grocery store control system might contain Building Management Controllers and Refrigeration Controllers.

#### Unit

A unit is an individual controller at a site belonging to a control system. There may be more than one unit in each control system. One controller would be configured as the gateway in the control system to communicate with Connect+.

#### Application Type

An application type is the type of application that has been set up inside a unit (controller). There can be many types of applications programmed into the controller. Application types can range from air handlers, standard circuits, analog and digital combiners, zones, power monitoring, global data, sensor control, time schedules, user access, and more. All application types contain applications that belong to the same application type.

#### Application Instance

An application instance shows the application (if available) that has been programmed inside a controller to access a physical device or define the controller setting. Through application instance, user can either access a physical device's data points, such as an ice cream case controller. Or access to applications that are programmed to configure the controller, such as user access.

#### Point

Application points are attributes that have been programmed inside a controller application. Access to application points allows the user to view details about the points, graph points, retrieve logs, and make changes. In Connect+ there are three categories of points. **Input, Output or Parameters**. Administrators can enter the name of the input or output that the Administrator would like the current point to send or get its value from. Connect an input point to an output point of the same data type, and vice versa (for example, digital outputs to digital inputs, analog inputs to analog outputs). An input point cannot be associated to another input point, and likewise, an output point cannot be hooked to another output point.

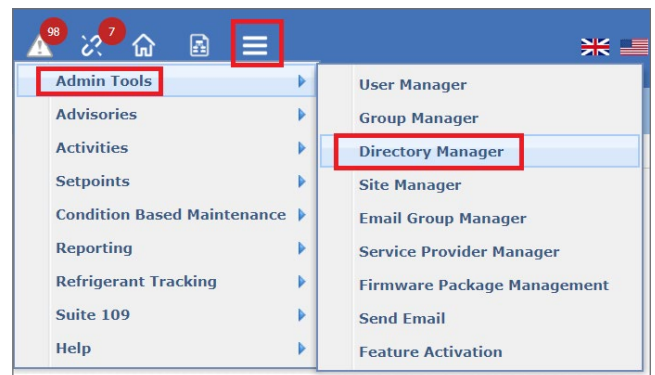
### 2.2 Onboard Directories

#### 2.2.1 Add Parent Directory

An Administrator can either right-click on the root of Connect+ or choose **Add Directory**.



Or go to **Top Menu > Admin Tools > Directory Manager**.

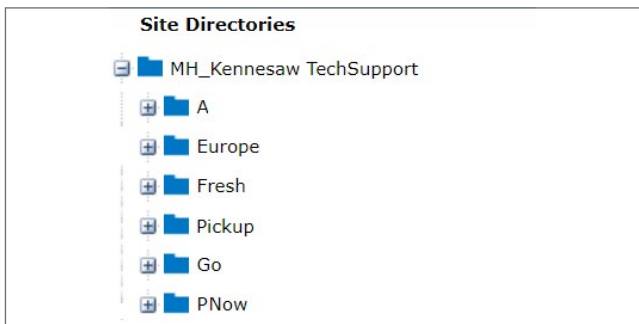




Then fill in the information for Admin organization's headquarters. Leave the parent directory blank, then this directory would be Admin root directory.

### 2.2.2 Add Subdirectory

Under the parent directory, the Admin can add multiple subdirectories to reflect a regional or organizational structure.

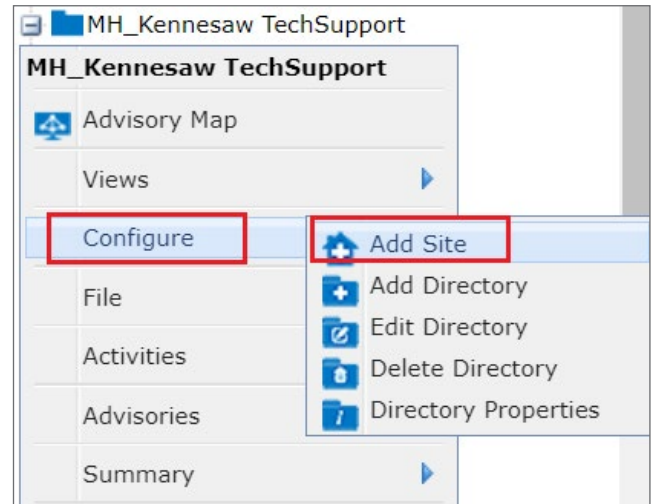


Fill in the subdirectory information and choose one parent directory to set up the correct hierarchy.

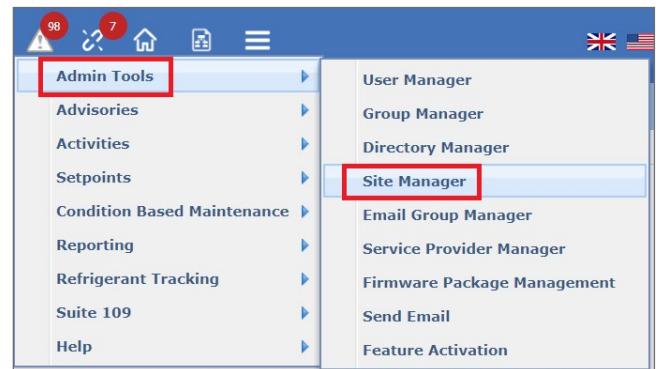
If you access the Directory Configuration page from the right-click menu, the parent directory will be automatically filled in with the directory you choose from the tree.

## 2.3 Adding Sites

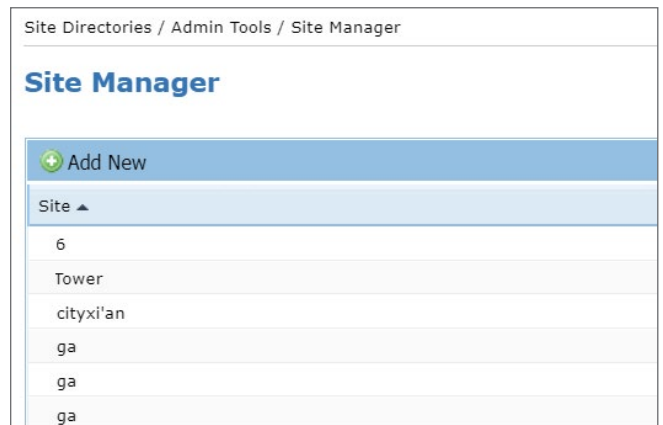
After setting up Directories, the Admin can add sites to each subdirectory by right-clicking the **Configure > Add Site** menu on directory level.



Or click **Top Menu > Admin Tools > Site Manager**.



Click the **Add New** button from the Site Manager table, you will be directed to **Site Configuration** page.



Fill the Site Information based on the field's explanation below:

### Site Configuration

<b>Name</b>	<input type="text"/>
<b>Number</b>	<input type="text"/>
<b>Parent Directory</b>	Dir <span style="float: right;">▼</span>
<b>Address Search</b>	Enter your address and autocomplete with Google Maps <span style="float: right;">/</span>
<b>Address 1</b>	<input type="text"/>
<b>Address 2</b>	<input type="text"/>
<b>Country</b>	United States <span style="float: right;">▼</span>
<b>City</b>	<input type="text"/>
<b>State/Province/Region</b>	Alabama <span style="float: right;">▼</span>
<b>Zip/Postal Code</b>	<input type="text"/>
<b>Voice Phone</b>	<input type="text"/>
<b>Refrigeration Service Provider</b>	<input type="text"/> <span style="float: right;">▼</span>
<b>Lighting Service Provider</b>	<input type="text"/> <span style="float: right;">▼</span>
<b>HVAC Service Provider</b>	<input type="text"/> <span style="float: right;">▼</span>
<b>Time Zone</b>	... <span style="float: right;">▼</span>

Cancel

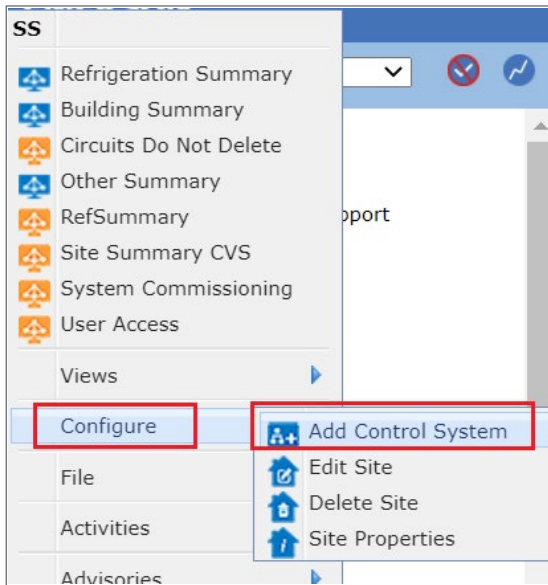
Save

Field	Validation	Notes
Name	Required	Unique, limit 50 characters
Number	Optional	Site number
Parent Directory	Required	Select only one from the drop-down.
Address Search	Required	Administrators can configure Google Map Address Search in the superuser property. If it is configured, this field is required.
Address 1 Address 2	Required	These fields are required and auto-filled by the Address Search if Google Map Address Search is configured. Or users need to manually input the address, which is optional.
Voice Phone	Optional	Site phone number
Service Provider	Optional	This field is used in Setpoint Management. If customer does not enable Setpoint Management and onboard Service Providers, the Service Provider information would be associated with Sites.
Time zone	Required	Site located time zone. <b>Note:</b> The time zone should be the same as the controller time zone that you want to add. Or the data might not be accurate for some functions. For example, advisory, point log, etc.
MSS Site Name	Optional	This is the site name of MSSR. It is used to receive alarms from the Alarm Infrastructure service.

## 2.4 Add Control System and Obtain Controller Information

After Sites have been added, the Admin needs to add Control Systems that are installed on Customer Premise. Right-click on desired sites, select **Configure > Add Control System**.

Enter **Protocol Type, Connection Type, IP Address, Port & Advisory Commissioning Port**. Contact Technical Support 833-409-7505 for more information if needed.



### Control System Configuration

**Name**

**Protocol Type**

**Connection Type**

**IP Address**  Validate IP Address

**Port**

**Advisory Commissioning Port**

**Obtain Controller Information Now**

---

**Optional**  Use this protocol user information for access to the devices at this Control System

**Protocol Username**

**Protocol Password**

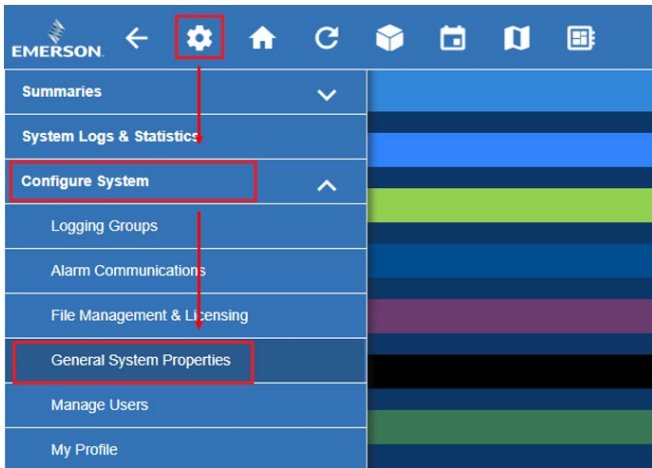
Field	Validation	Notes
Name	Required	Unique
Protocol Type	Required	E2, Site Supervisor, E3, Xweb, TAC, Danfoss, etc.
Connection Type	Required	Default is IP
IP Address	Required	Controller IP address which Connect+ can connect.
Validate IP Address	Optional	If this check-box is enabled (default), only a valid IP address will be accepted. If an invalid address is entered, a message will appear to notify you that an invalid address has been entered.
Port	Required	The port number of devices to which you are connecting, you can check it on the device. (Please refer to "Appendix A: Group Privileges, Descriptions, and Protocol Access Levels").
Advisory Commissioning Port	Required	The port used for receiving advisories after commissioning is complete.
Obtain Controller Information Now	Optional	The check-box appears only when adding a new control system (not available on Edit Control System). If this check-box is enabled (default), Connect+ will automatically connect to the control system and refresh all Units, Applications and Point lists under that controller.
Protocol	Optional	If this protocol check-box is enabled at the control system level, Connect+ will use <b>Protocol Username</b> and <b>Protocol Password</b> entered on this page and bypass the information at the Group level for <i>only the units located under this control system</i> . Normally, security settings for Connect+ are defaulted at the Group Configuration level.



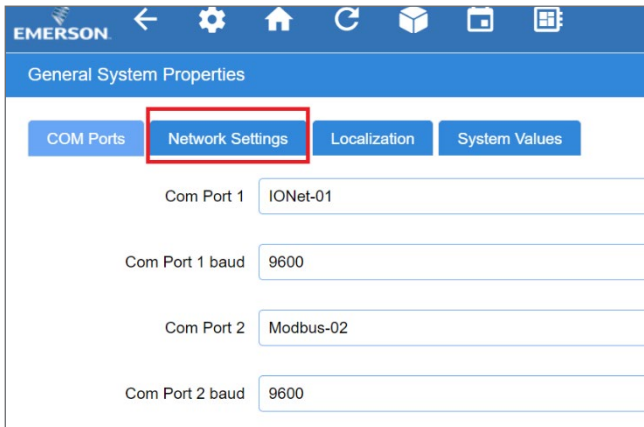
## 2.4.1 Configuring the Site Supervisor/E3 and E2 to Communicate with Connect+ Mixed Sites

For controllers to be functional, they must be configured at the controller and Connect+.

1. You can log into Site Supervisor or E3, click on the Main Menu, **Configure System** and then select **General System Properties**. This will take you to the Network configuration.



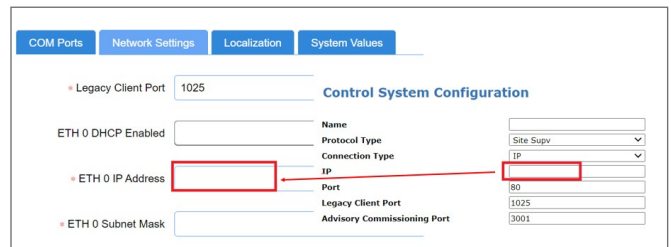
2. At the Network Configuration screen, click the **Network Settings** tab to access the TCP/IP settings of the controller.



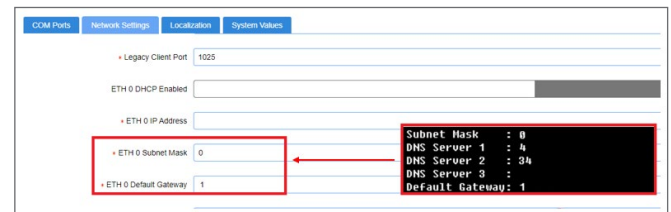
3. Click the **Advanced** options button on the upper right corner of the screen. This will enable Advanced options.



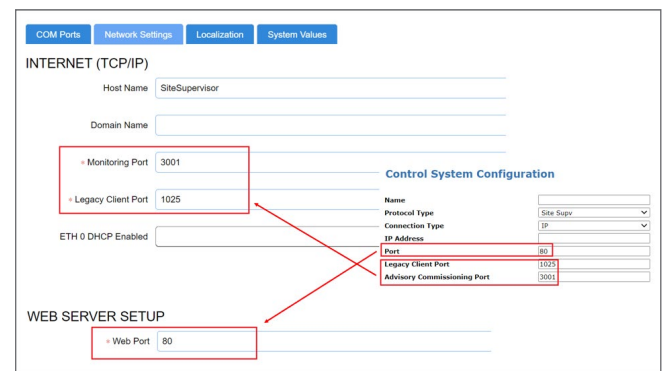
4. The IP address for ETH 0 should be the same IP address used in the control system settings of Connect+. The Site Supervisor or E3 should be the gateway controller in this setup. Contact [ColdChain.TechnicalServices@Emerson.com](mailto:ColdChain.TechnicalServices@Emerson.com) to obtain the gateway IP address to be used.



5. The ETH 0 Subnet Mask and Default Gateway should match the E2 controller on site. To get to the TCP/IP settings of the E2, press **Menu** > **7** > **3** > **1** from the Home screen. Press **F2** three (3) times to go to the **TCP/IP** tab.

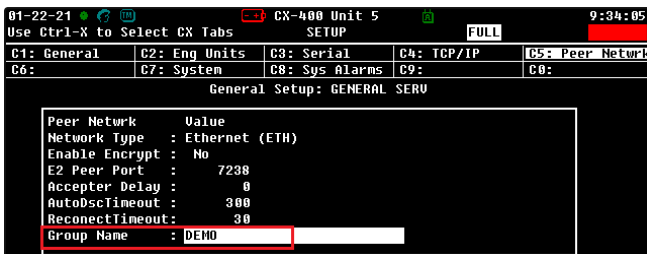


6. Configure the following additional settings values.
  - a. Monitoring Port
  - b. Legacy Client Port
  - c. Web Port

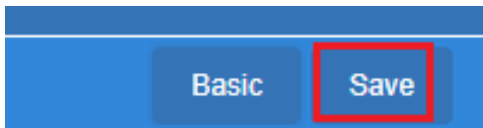


- Click the **System Values** tab. Configure the Site Name and Unit, then edit the Group Name to match the existing E2 controllers on site.

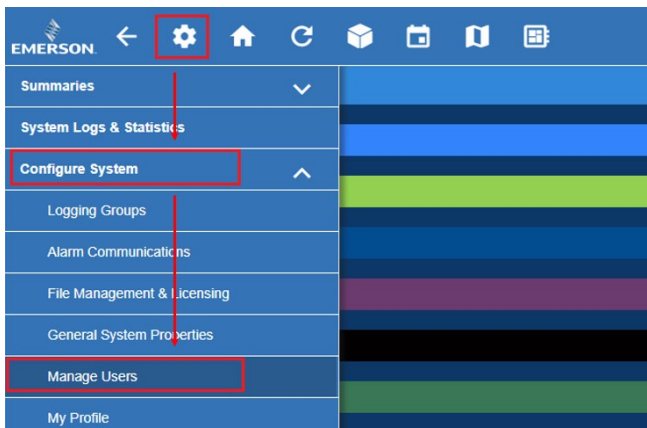
To view the Group Name of the existing E2 controllers on site, press **Menu** > **7** > **3** > **1** from the Home screen. Press **F2** four (4) times to go to the **Peer Network** tab.



- Save the changes by clicking the **Save** button on the upper right corner of the screen.



- The user credentials of both Site Supervisor/E3 and E2 must be modified to accommodate the login protocol of Connect+. To create a new user on the Site Supervisor/E3. Click on the **Main Menu** icon, expand **Configure System** and finally to the **Manage Users**.



- Click the **Create a User** button. A window will appear where **Username** and **Password** information can be entered. Both username and password are case sensitive.

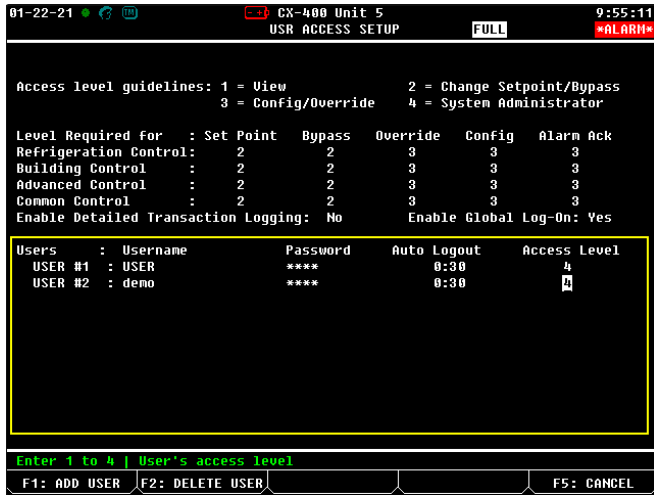


Choose the user role for the user account created.

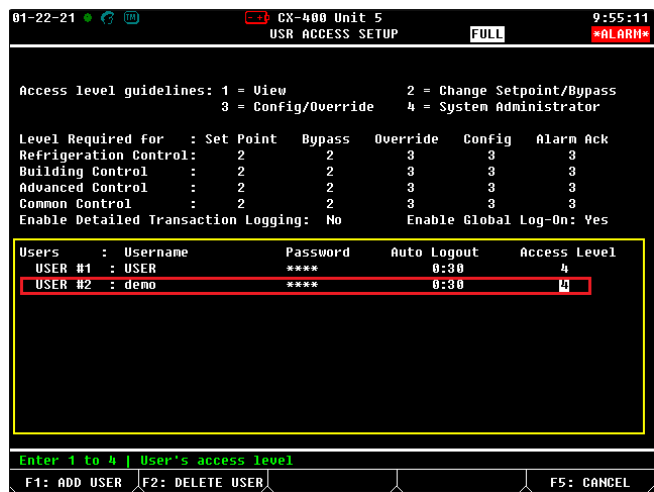
- Click the **Save** button on the upper right corner of the screen to save the changes.



12. On the existing E2 controllers on site, additional user credentials must be setup. To do this, press **Menu** > **7** > **3** > **3** from the Home screen. This will take you to the **User Access Level** screen.



13. Press the down arrow button until you are in the User List section. Press **F1** to add a new User. Enter the following for the **Username** and **Password**, then set the Access Level to 4. Press the **Save** button to save. The newly added account should be the same as Site Supervisor/E3.



14. The login credentials of the control system must be updated with the correct username and password used. Make sure the “use this protocol user information” check-box is checked is enabled and enter the username and password of gateway.

### Control System Configuration

Name: Site Supv

Protocol Type: Site Supv

Connection Type: IP  HTTP  HTTPS

IP Address:   Validate IP Address

Port: 80

Legacy Client Port: 1025

Advisory Commissioning Port: 3001

Obtain Controller Information Now:

---

Optional  Use this protocol user information for access to the devices at this Control System

Protocol Username: demo

Protocol Password: \*\*\*\*

Cancel Save

15. Ensure that the E2 controllers on site are running upgraded to use the 4.09F01 firmware. If an earlier version of the firmware is being used, the controller on site must be upgraded to the latest firmware.
16. **Obtain Controller Information Now** is checked by default. Click the Save button after the configuration is done. Obtain Controller Information will be run automatically.

### Control System Configuration

Name: Site Supv

Protocol Type: Site Supv

Connection Type: IP  HTTP  HTTPS

IP Address:   Validate IP Address

Port: 80

Legacy Client Port: 1025

Advisory Commissioning Port: 3001

Obtain Controller Information Now:

---

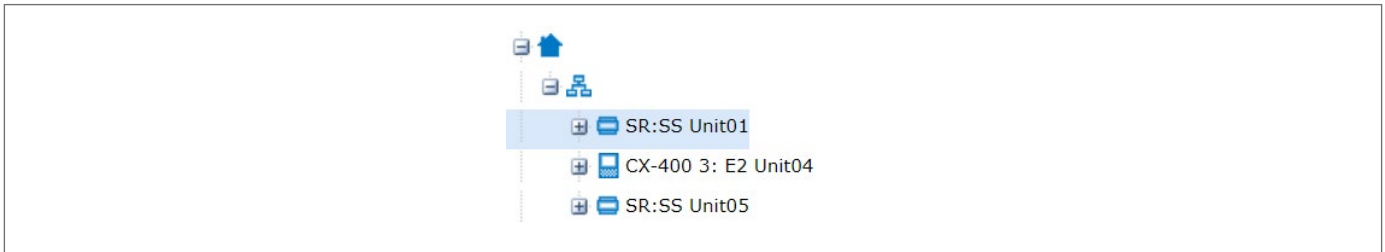
Optional  Use this protocol user information for access to the devices at this Control System

Protocol Username: demo

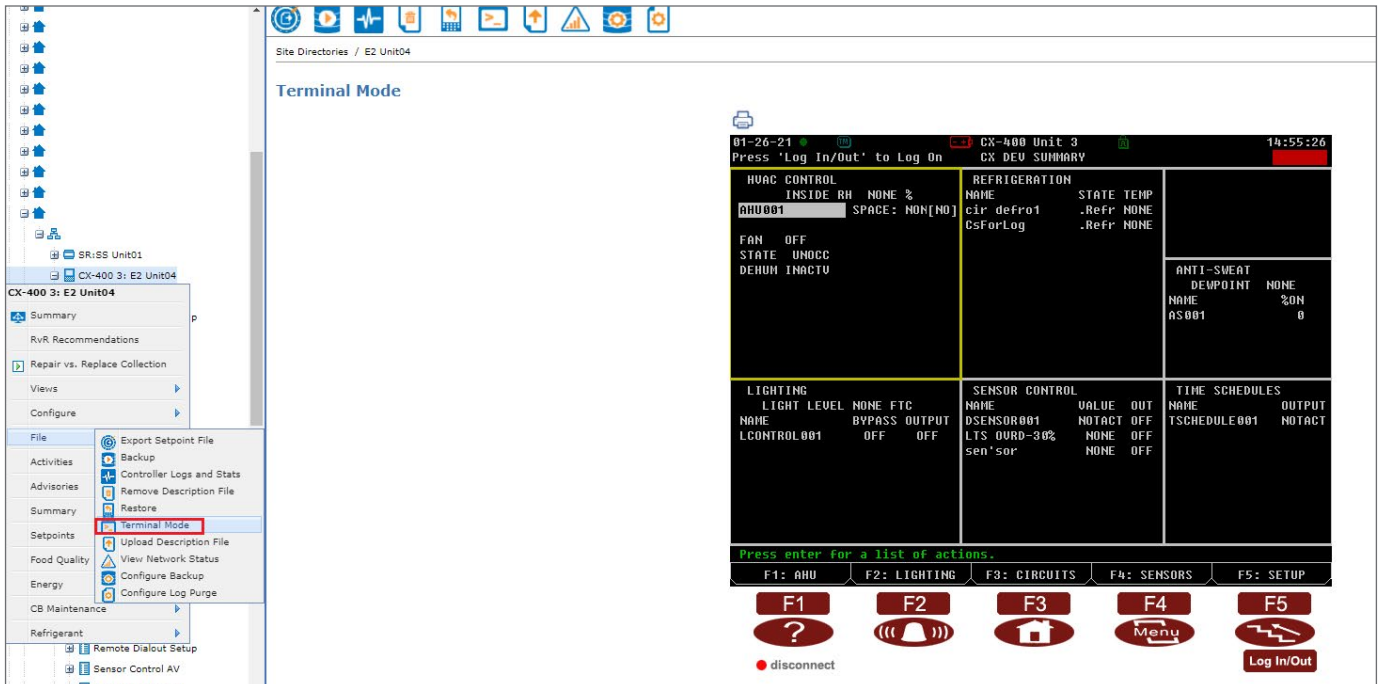
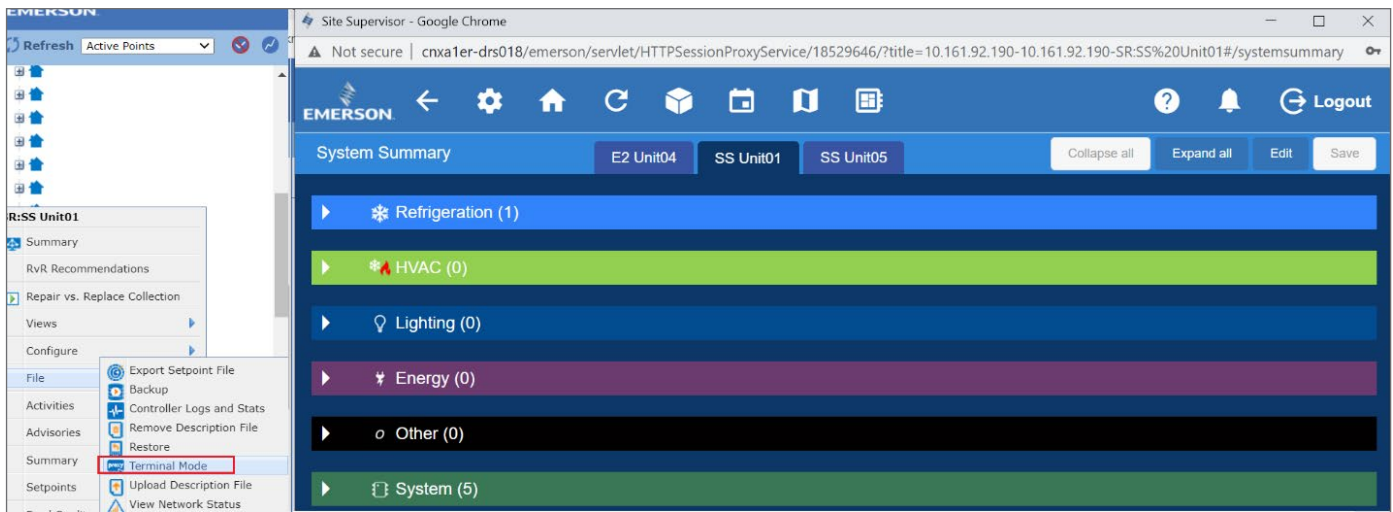
Protocol Password: \*\*\*\*

## 2.5 Verify Control System Connection

Once Obtain Controller Information is completed, you will see controllers are visible on the navigation tree.

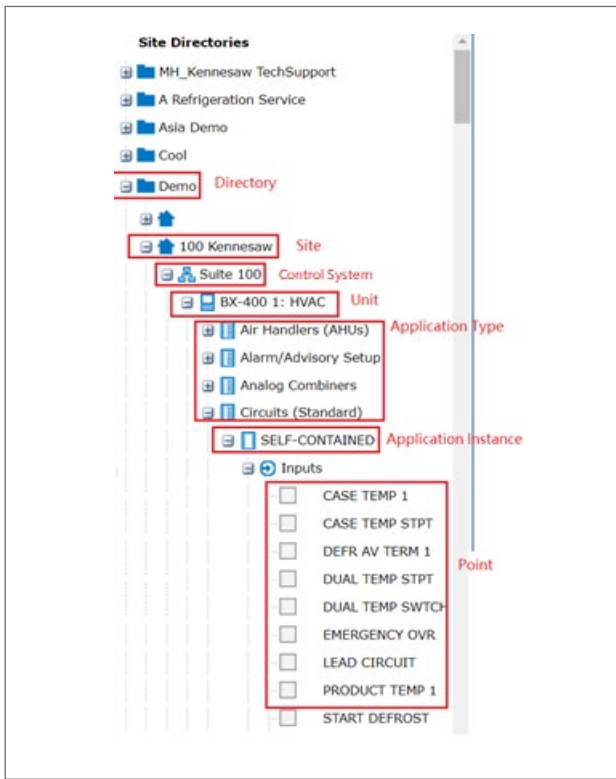


Usually, you can validate the Controller Connection by accessing the **File > Terminal Mode** from the right-click menu of the Site Supervisor, E3 or E2 once Obtain Controller Information is successful.

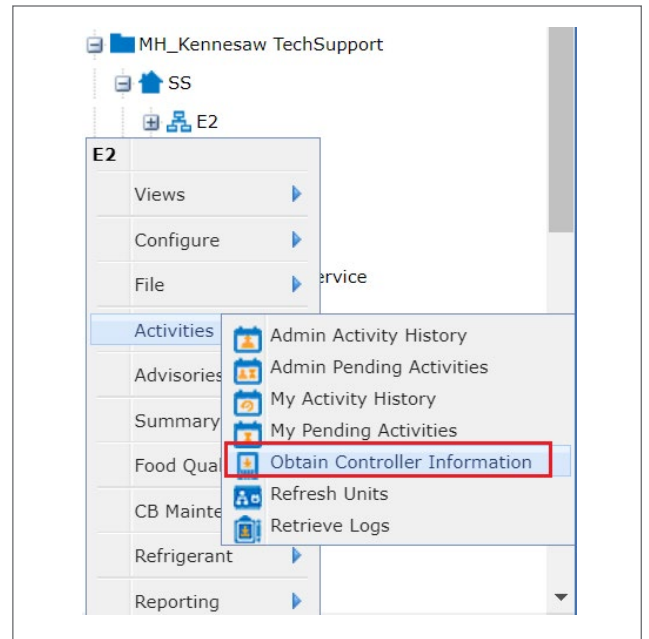


## 2.6 Verify Tree Structure & Enterprise Summary

Once the controller is connected, you can view the tree structure from the navigation frame.



If you cannot drill down to show the tree structure, you can select **Activities > Obtain Controller Information** from right-click menu of directory, site, or control system level.



The **Enterprise Summary** page also can provide summary information of directories, sites, control systems, and units configured in Connect+, shows the overall topography of the program, and the applications inside controllers that are connected to the system.

You can go to Enterprise Summary page by clicking **Enterprise Summary** icon from top bar.



The page displays all directories by default, including all parent and descendant directories. You can toggle the radio button on the top of the table to view the information of different level.

**Enterprise Summary**

View By:  Directory  Site  Control System  Unit  Application Type  Application Instance  Show 25

Directory	Parent Directory	Address 1	Country	City	State/Province/Region	Zip/Postal Code	Number of
Mexico	Mexico		Mexico				0
A M			United States		Georgia		6
MH_Kennesaw...			United States		Georgia	30144	0
Refrigeration ...			United States		New York		0
AA	A		Singapore				0
A	A		United Kingdom				5
Fresh	A		United States		Washington		0
Fresh Pick...	A		United States		Alabama		0
Go	A		United States		Alabama		0
	A		United States		Washington		0
Asia Demo			India				0

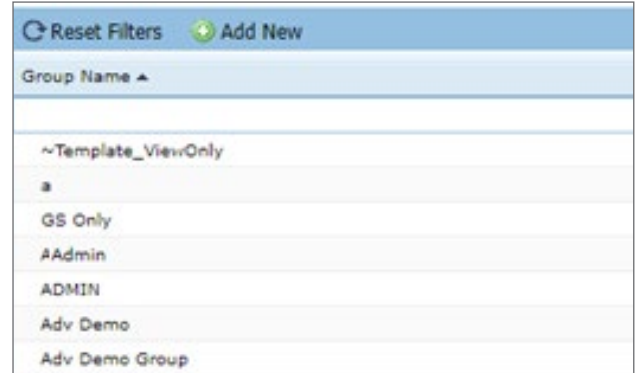
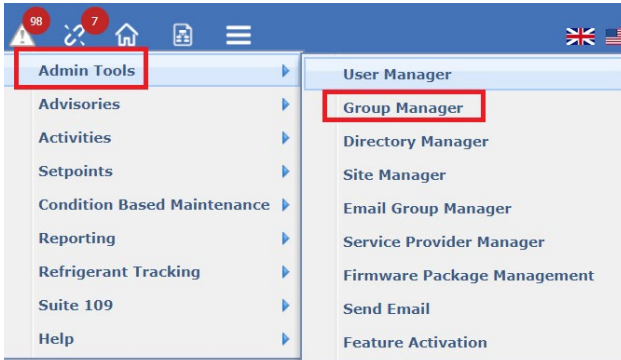


## 3 Onboard Users

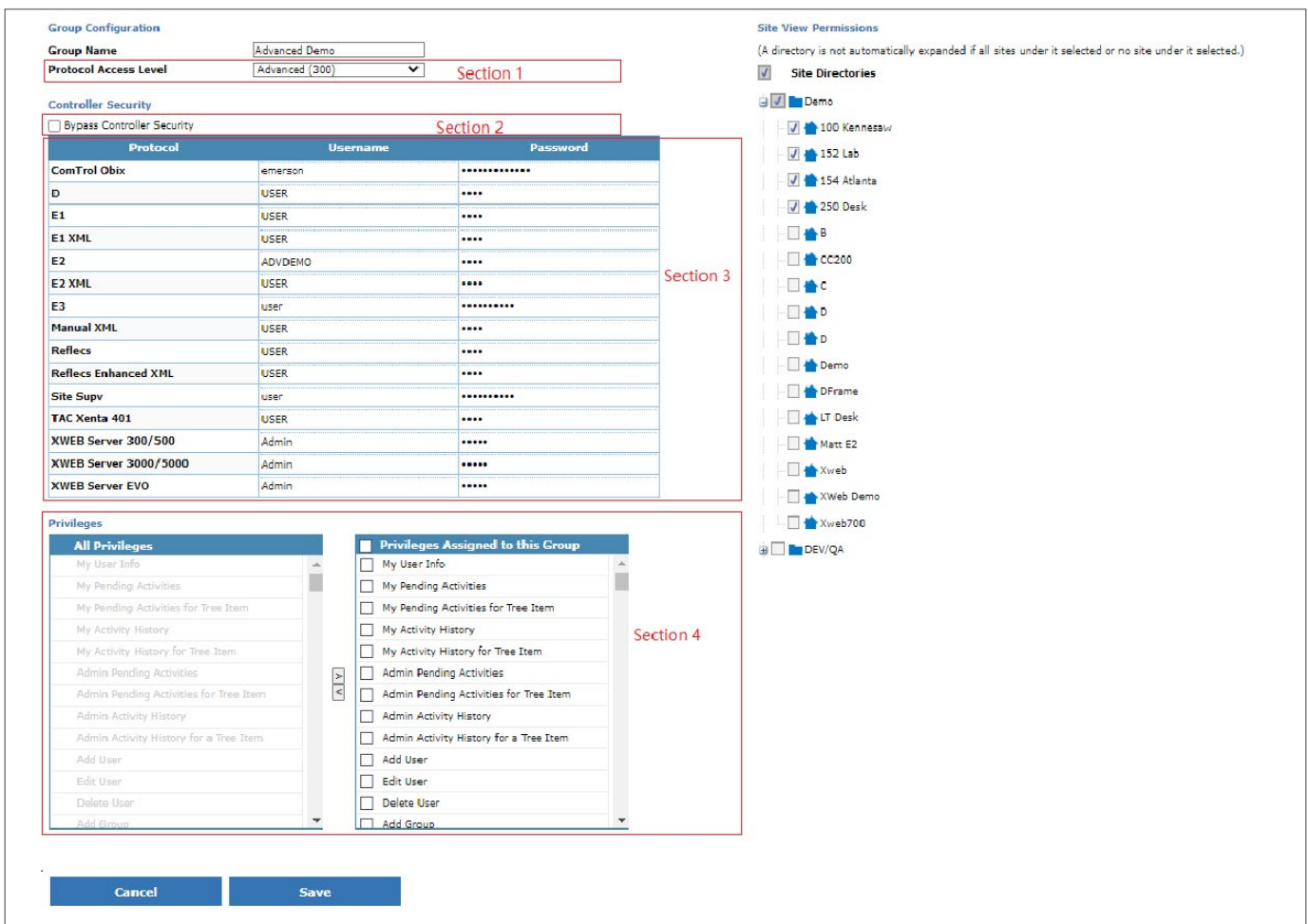
### 3.1 Create User Group to define Privilege and Sites Access

Connect+ manage user privilege and site access by Group Manager. You can access to Group Manager by clicking Top Menu > **Admin Tools** > **Group Manager**.

Click the **Add New** button from the Group Manager table, you will be directed to **Group Configuration** page.



Fill in Group Name, Controller Access Level and select Connect+ Privileges and Sites Access for the group:



All privileges can be added or subtracted for a user at the admin level on this page. To add or subtract privileges for a user, highlight the privilege in the left column and click the left and right arrows. The right arrow on the top will assign privileges, the left or bottom arrow will unassigned the privilege. Hover your mouse over each privilege to see its definition.



Name the new Group by entering it into the **Group Name** field.

Next, set the desired Protocol Access Level that will apply to the group.

1. The Protocol Access Level (PAL) determines what Connect+ activities are available to the users in a group. The available activities will identify what menus and sub-menus will be available to the users in that group. The PAL can be driven either at the Group level or at the Control System level. Normally, the Protocol Access Level is defaulted at the Group configuration level. The configurations set at the Control System level will bypass those set at the Group level. This allows users to “manage by exception” the security settings for their network of controllers. For example:
  - a. If each Control System in the Directory does not have a username and password configured, Connect+ will use the username and password at the Group level to log into the system.
  - b. For only some specific Control Systems for which the administrator wants to lock out some activities, the administrator can configure a user with a lower PAL (and consequently, lower activities access) and allowing the Group level settings (with a user with a higher PAL) to log in and execute activities in all other Control Systems that do not have a user/password set up.

**Control System Configuration**

Name: Site Supv  
Protocol Type: Site Supv  
Connection Type: IP  HTTP  HTTPS  
IP Address:   
Port: 80  
Legacy Client Port: 1025  
Advisory Commissioning Port: 3001  
Obtain Controller Information Now:

**Optional**  Use this protocol user information for access to the devices at this Control System  
Protocol Username: demo  
Protocol Password: \*\*\*\*\*

Cancel Save

2. The Group PAL configuration has three sections that can drive the PAL that will be applied when logging into the controller:
  - a. The PAL selected for the Group is the “Connect+ Group’s Protocol Access Level.” Special rules apply to determine how the menus will behave when this PAL differs from the PAL belonging to the Username/Password set at the Group or Control System level, whichever prevails (as explained in the step b below).
  - b. The PAL configured for a User/Password already set in the controller for a specific protocol as entered in the User/Password pane and bypass those set at the Control System level (if there is any).
  - c. Alternatively, if the **Bypass Controller Security** option is enabled, the system will use the PAL set in the Protocol Access Level drop-down. Enabling this option will also hide and bypass the User/ Pass.

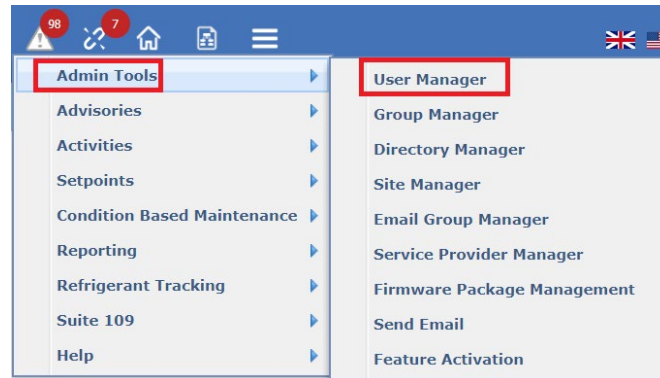
**NOTE: The bypass Controller Security option is only available for E2.**

**Assigning Privileges:** To enable users in a group to use an activity, privileges must be selected for the group under the **Privileges Assigned to this Group**. Use the left arrow button to select (right arrow button to remove) which privileges will be assigned to the Group (the privileges that are assigned will be grayed out so they cannot be assigned twice). A privilege is any activity that can be performed in Connect+. At least one privilege must be assigned.

**Site View Permissions:** you can assign permissions (which directories and sites) to each Group by enabling the check-boxes next to them.

## 3.2 Create User

You can access to User Manager by clicking Top Menu > **Admin Tools** > **User Manager**.



Click the **Add New** button from the **User Manager** table, and you will be directed to **User Configuration** page.

### User Manager

Reset Filters Add New

Username	First Name	Last Name	E-mail	Group Name
1	1	1	username@emerson.com	ADMIN
administrator	System	Administrator	username@emerson.com	ADMIN
bypass	bypass	bypass		bypass

In this page, you can configure user-basic information, preferences, and Engineering unit information.

Site Directories / Admin Tools / Setup / User Manager / User Configuration

### User Configuration

**Login ID**   
**First Name**   
**Last Name**   
**New Password (case sensitive)**   
**E-mail**   
**Group Name**   
**User Expiration Type**

### Preferences

Show GS Screen Edit Tool  
 Enable Home Page  
 Hide Nav Frame  
 Enable GS Screen Auto Log Off

**Cancel** **Save**

### Units

	English	Metric	Global
<b>Temperature</b>		Fahrenheit (DF)	
<b>Temp. Change</b>		Delta Fahrenheit (DDF)	
<b>Temp. Rate Change</b>		degrees F/hour (DFH)	
<b>Pressure, Large</b>		pound/sq in (PSI)	
<b>Pressure, Small</b>		in of water (INW)	
<b>Velocity, Air</b>		feet/minute (FPM)	
<b>Velocity, Liquid</b>		gallons/minute (GPM)	
<b>Liquid Volume</b>		gallons (GAL)	
<b>Volume Flow</b>		cubic feet/minute (CFM)	
<b>Current</b>		amperes (A)	
<b>Light</b>		foot-candles (FTC)	
<b>Weight</b>		pounds (LBS)	
<b>Enthalpy</b>		Btu/lb	

**Basic Information:** Enter Login ID, Name, E-mail address, user group, and user expiration information.

Field	Validation	Notes
Name	Required	Unique
First Name	Required	Enter the first name of the user in this field.
Last Name	Required	Enter the last name of the user in this field.
New Password (case sensitive)	Required	Provide a login password. It is case sensitive.
Email	Optional	Enter the email address of the user. If your company uses multi-factor to login Connect+, email is required.
Group Name	Required	Enter the name of the group to which this user has been associated.
User Expiration Type	Optional	See Section 3.3 User Expiration.
User Expiration Date	Optional	See Section 3.3 User Expiration.

**Preferences:** Check the check-box to enable the convenience features.

- **Show GS Screen Edit Tool:** If this check-box is enabled, the GS menus will become visible on the right-click menu of Navigation tree. If it is disabled, the menu will not show even you configure the privilege to this user.
- **Enable Home Page:** If this check-box is enabled, it will set the GS screen you choose as your system home page on start-up.
- **Hide Nav Frame:** The navigation tree will be hidden each time you log in if it is enabled. The selected home page can now be viewed on a full screen.
- **Enable GS Screen Auto Log Off:** This check-box is enabled by default. It allows the GS Screen page auto log off if this page is inactive for specific time duration (default 30 minutes).

**Engineering Units Information:** Engineering units can be set to English or Metric depending on the unit of measure the user requires. Administrator can also configure their own Engineering Units and set it as Global. And users can select the Global button for user's engineering units.

### How to configure Engineering Units as Global:

Login Connect+ as a super user. Select Top Menu > **Super User** > **Properties Editor**. Set each **GlobalEngineeringUnits** as your own.

The screenshot shows the 'Properties Manager' window with the title 'Jarú Properties Viewer and Installation Override Manager'. It displays '14 properties found.' and a table of properties. A red box highlights the table content.

Category	Key	Value
JaruSystem	GlobalEngineeringUnits.Current	amperes (A)
JaruSystem	GlobalEngineeringUnits.Heat	Btu/lb
JaruSystem	GlobalEngineeringUnits.Light	foot-candles (FTC)
JaruSystem	GlobalEngineeringUnits.LiquidVolume	gallons (GAL)
JaruSystem	GlobalEngineeringUnits.PressureLarge	pound/sq in (PSI)
JaruSystem	GlobalEngineeringUnits.PressureSmall	in of water (INW)
JaruSystem	GlobalEngineeringUnits.TempChange	Delta Fahrenheit (DDF)
JaruSystem	GlobalEngineeringUnits.TempRateChange	degrees F/hour (DFH)
JaruSystem	GlobalEngineeringUnits.Temperature	Fahrenheit (DF)
JaruSystem	GlobalEngineeringUnits.VelocityAir	feet/minute (FPM)
JaruSystem	GlobalEngineeringUnits.VelocityLiquid	gallons/minute (GPM)
JaruSystem	GlobalEngineeringUnits.VolumeFlow	cubic feet/minute (CFM)
JaruSystem	GlobalEngineeringUnits.Weight	pounds (LBS)
JaruSystem	useSiteTreeAndGlobalSearchSecurity	false

### 3.3 User Expiration

The configuration of user information. When a user account has expired, the user cannot log into the Connect+ anymore. They will need to contact Administrator for help.

#### 3.3.1 Configure User Expiration Type

In the user configuration page, you can configure the user expiration type to limit user's use duration.

**Security Mode**  
 Local Security  LDAP Integration

**User Configuration**

Login ID:   
First Name:   
Last Name:   
New Password (case sensitive):   
E-mail:   
Group Name:   
User Expiration Type:  (dropdown menu open showing: Never Expired, Never Expired, Expire By Calendar, Auto Expire By Interval)

**Preferences**

- **Auto Expire By Interval:** User account will expire if the interval between the current date and the last login date is more than the expiration interval or the current date is equal to the expiration date. When selecting **Auto Expire By Interval**, the **User Expiration Interval** and **User Expiration Date** are required.

**Security Mode**  
 Local Security  LDAP Integration

**User Configuration**

Login ID:   
First Name:   
Last Name:   
New Password (case sensitive):   
E-mail:   
Group Name:   
User Expiration Type:  (dropdown menu open showing: Auto Expire By Interval, -- select one --, User Expiration Date\*)

User Expiration Interval including 1 month, 3 months, 6 months

There are three kinds of user expiration types:

- **Never Expired:** User account will never expire.
- **Expire By Calendar:** User account will be expire at expiration date. **User Expiration Date** is required when selecting expiration calendar.

**Security Mode**  
 Local Security  LDAP Integration

**User Configuration**

Login ID:   
First Name:   
Last Name:   
New Password (case sensitive):   
E-mail:   
Group Name:   
User Expiration Type:  (dropdown menu open showing: Expire By Calendar, User Expiration Date\*)

User Expiration Date\*:

**User Configuration**

Login ID:   
First Name:   
Last Name:   
New Password (case sensitive):   
E-mail:   
Group Name:   
User Expiration Type:   
User Expiration Interval:  (dropdown menu open showing: -- select one --, -- select one --, 1 Months, 3 Months, 6 Months)

User Expiration Date\*:

**Preferences**

The User Expiration Date should be greater than the current date plus expiration interval, otherwise message will be prompted when clicking **Save** button.

For example, if the Current Date is 2019/4/15, and the User Expiration Interval is 3 months, the User Expiration Date should be greater than 2019/7/15 (2019/4/15 push 3 months). Otherwise, the below message will be prompted when clicking **Save** button.

Site Directories / Admin Tools / Setup / User Manager / User Configuration

User Expiration Date must greater than Expiration Interval

### User Configuration

**Login ID**   
**First Name**   
**Last Name**   
**New Password (case sensitive)**   
**E-mail**   
**Group Name**   
**User Expiration Type**   
**User Expiration Interval**   
**User Expiration Date\***

### Example of Auto Expire By Interval:

If a user is configured to use Auto Expire By Interval at 2019/4/15, and the User Expiration Interval is configured as 1 month, the User Expiration Date is 2019/9/20.

Connect+ will start to check the user login from the configured date (2019/4/15) every month. If user does not have a login record during a 1 month period, the user account will expire. Otherwise the user account will expire at configured User Expiration Date 2019/9/20.

1 Month Duration	Login Status	Expire Status
2019/4/15 - 2019/5/15	Login	No
2019/5/15 - 2019/6/15	Login	No
2019/6/15 - 2019/7/15	No Login	Yes (Expire at 2019/7/15)

### 3.3.2 Reactivate User

If the user account has expired, when the user attempts to log into Connect+, a message will display to indicate the account has expired and to contact their Administrator.

## Login

Enter a valid Login ID and password

**Login ID**

**Password**

**Login**

Administrator can re-activate the user from User Configuration page:

1. Check the **User Expiration Date**. If the date has expired, the administrator needs to extend the expiration date and click the Save button to re-activate the user.
2. If the **User Expiration Date** is not in the system yet, the expired account will prevent the user from logging into the instance during the **User Expiration Interval**. In this case, the administrator must verify if the account needs to be re-activated because the user has not logged into Connect+ for at least 1 month.
3. To re-activate this user, the administrator should go to the User Configuration page, and change the User Expiration Interval, then **Save** the configuration. Connect+ will start recalculating the expiration interval after saving.

## 3.4 User Lockout

For security considerations, the administrator could set the number of times a password can be entered incorrectly.

Log into Connect+ with superuser credentials, set the **LimitNumberOfLogin** property as **True** on the Properties Manager page, and configure the attempt limit **numberOfLoginTimes**. The default value is 5.

Category	Key	Value
	login	
JaruStatsProperties	limitNumberOfLogin	true
JaruStatsProperties	numberOfLoginTimes	5

Once the properties are configured, the user account will be locked out if the user enters the wrong password more than the set configured number of times

## Login

Number of login attempts exceeded, your account is locked.  
 To unlock your account, please reset your login ID or password by clicking the below link.  
 Or login after 24 hours.

**Login ID**  
[Forgot Login ID?](#)

**Password**  
[Forgot Password?](#)

**Login**

Users need to wait for 24 hours to get another attempt. Or users could reset their password by clicking **Forgot Password**.

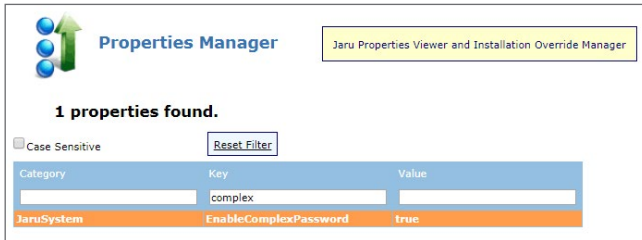
When user click the link, system will send a temporary password to the user's email address to log into the Connect+ with this temporary password and reset it.

## 4 Complex Password

User password configuration. User cannot log into Connect+ and need to reset the password when the password has expired.

### 4.1 Enable Complex Password

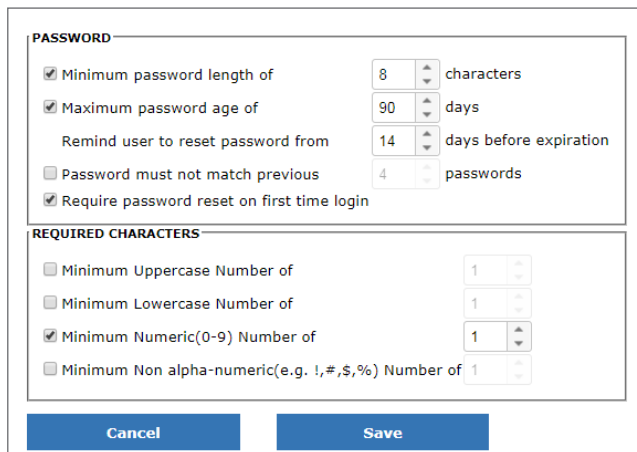
Log into Connect+ with superuser, set the **EnableComplexPassword** property as **True** on the Properties Manager page:



The screenshot shows the Properties Manager interface. At the top, it says "1 properties found." Below this, there is a table with columns for Category, Key, and Value. The table contains one row: JaruSystem, EnableComplexPassword, true. There are also checkboxes for "Case Sensitive" and a "Reset Filter" button.

### 4.2 Configure Password

Select Top Menu > **Admin Tools** > **Setup** > **Password Rule Manager** and configure the rule you want to apply on your instance.



The screenshot shows the Password Rule Manager configuration dialog. It has two sections: "PASSWORD" and "REQUIRED CHARACTERS".

**PASSWORD**

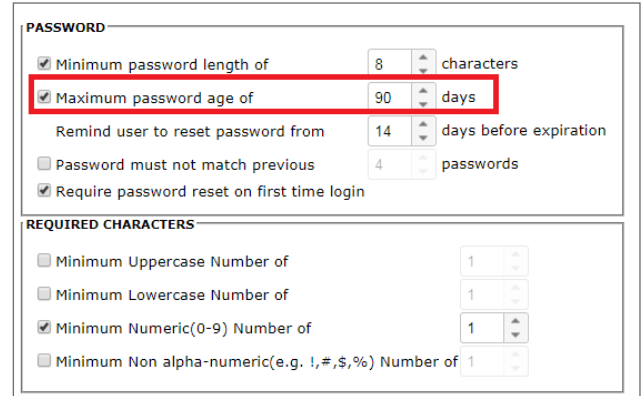
- Minimum password length of 8 characters
- Maximum password age of 90 days
- Remind user to reset password from 14 days before expiration
- Password must not match previous 4 passwords
- Require password reset on first time login

**REQUIRED CHARACTERS**

- Minimum Uppercase Number of 1
- Minimum Lowercase Number of 1
- Minimum Numeric(0-9) Number of 1
- Minimum Non alpha-numeric(e.g. !, #, \$, %) Number of 1

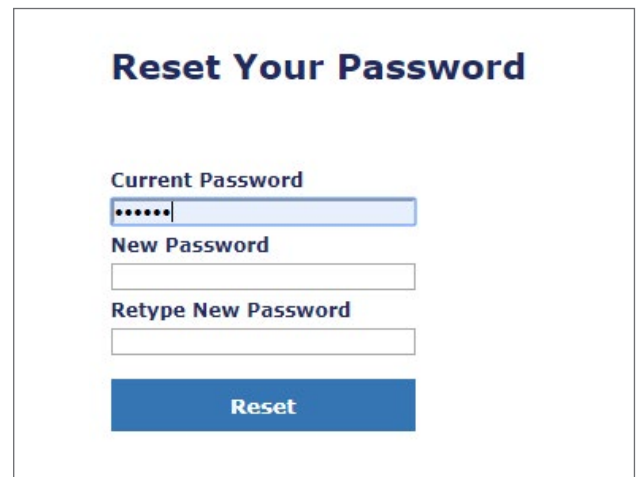
Buttons: Cancel, Save

**Maximum password age of:** When a user configures Maximum password age of XX days. (for example, 90 days), the password will expire 90 days later from when the new user created date or when the complex password rule configured date for existing user.



This is a partial view of the Password Rule Manager configuration dialog, showing the "PASSWORD" section. The "Maximum password age of" field is highlighted with a red box and set to 90 days. Other fields include "Minimum password length of" (8 characters), "Remind user to reset password from" (14 days before expiration), "Password must not match previous" (4 passwords), and "Require password reset on first time login" (checked).

When password expires, reset password is required when the user logs into the Connect+. After the password is reset, the user can login again using the new password.



The screenshot shows the "Reset Your Password" form. It has three input fields: "Current Password" (masked with dots), "New Password", and "Retype New Password". A blue "Reset" button is at the bottom.



## 5 Configure Advisory Receiving and Advisory View

### 5.1 Get Familiar with Advisories

An advisory is defined as the notifications or alarms generated from controllers to report store setting deviations. In Connect+, an Advisory can have **State, Type, Priority and Urgency Level**.

#### **Advisory State:**

An advisory would remain active until the condition to generate the advisory returns to normal. This is defined as Advisory State in Connect+ for all controllers.

#### **Type:**

- E2: Alarm, Device Failure, Notice
- Site Supervisor: Critical, Non-Critical, Notice
- Dixell: NA
- Danfoss: Severe, Critical, Normal, Log Only

#### **Priority:**

- E2 1-99
- Site Supervisor NA
- Dixell 1-99
- Danfoss NA

#### **Urgency Level**

When administrators have multiple controllers across the organization, it can be difficult to tell which Advisory needs immediate attention with a non-standard Advisory definition. In order to solve this problem, Connect+ has defined Urgency Levels as shown below. This allows users to have a consistent view of advisory's severity. The definitions below are default settings in Connect+:

- E2

Advisory Urgency Level	State	Type	Priority
High	Active	Fail or Alarm	1-20
Medium	Active	Notice	1-50
		Fail or Alarm	21-50
Low	Active	All	51-99
	Return to Normal	All	1-00

- Site Supervisor

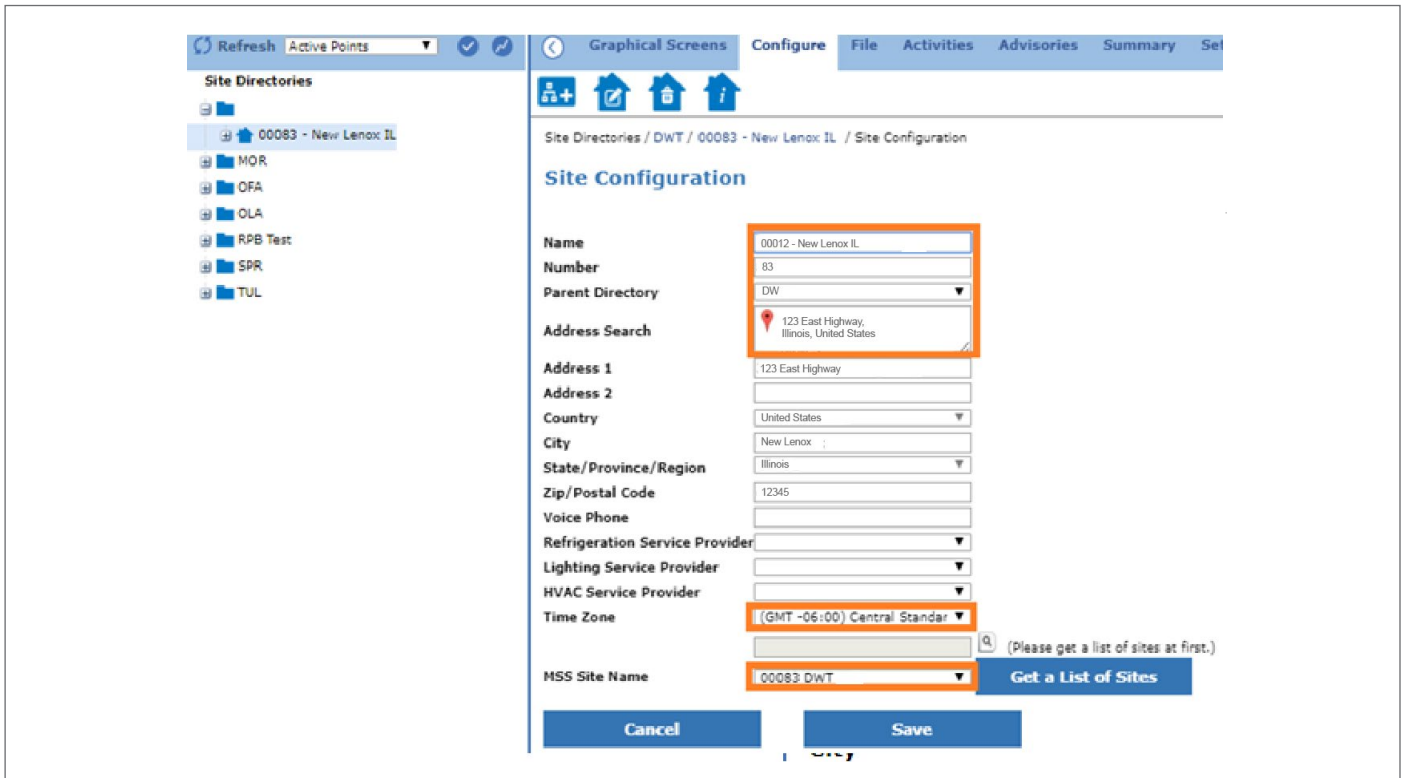
Advisory Urgency Level	State	Type	Priority
High	Active	Critical	NA
Medium	Active	Non-Critical	NA
		Critical	NA
Low	Return to Normal	Non-Critical	NA
	Active	Notice	NA

- Danfoss

Advisory Urgency Level	State	Type	Priority
High	Active	Severe or Critical	NA
Medium	Active	Normal	NA
Low	Active	Log Only	NA
	Return to Normal	All	NA

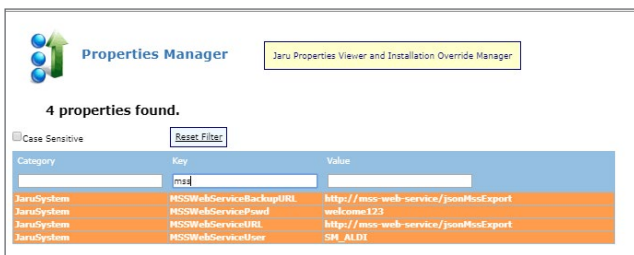
### 5.2 Configure Advisories Received from Controller

1. Customer added to MDM.
2. Sites with addresses and time zones added to MDM.
3. Sites set to be subscribed to Alarm Web service if not purchasing either Alarm Basic or Resolution at contract fee and terms. Note Alarm Web will be required at a minimum to enable Advisory receiving.
4. Sites set to be subscribed to Hosted Connect+/Site Manager service at contract fee and terms.
5. Sites added to Connect+ with store number and addresses entered and confirmed using Google address field



6. Sites MSS Site Names mapped in Connect+. Note MSS Web Service must be configured in Connect+ Properties Manager using customers MSS account credentials provided by PSC Service Activation team. If a problem occurs, enter a support ticket with escalation to Tier 2 Connect+ Application Support.

Sample of MSS Web Service:



7. Enter a support ticket to enable AI to C+ service for customer and assign to Tier 2 Connect+ Application Support.

8. Sites Advisories Commissioned from customer instance of Connect+.

Note customers may specify Alarm Filter Pries and number of Daily Test Alarms. Note that Return-to-Normal Advisories should be checked to be received. Primary and Secondary Receiver IP's vary according to customer connectivity:

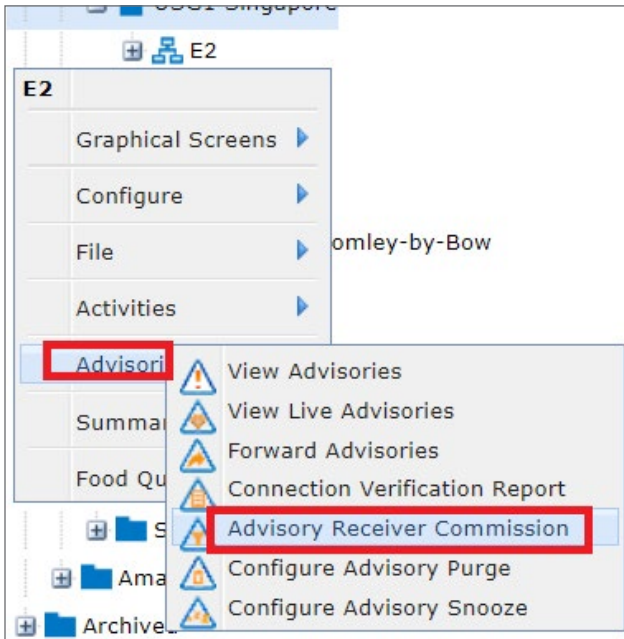
Internet: 12.155.208.49:3001  
 VPN: 12.155.208.137:3001 Primary  
 12.155.208.138:3001 Secondary  
 AT&T Cell Modem: 10.56.1.33:3001

9. Verify Advisories are being received by AI/ UARD using PSC Consoler.
10. After confirmation of AI to C+ service enabled, verify Advisories are being received by Connect+. If a problem occurs, enter support ticket with escalation to Tier 2 Connect+ Application Support.

### 5.3 Advisory Receiver Commission

The **Advisory Receiver Commission** page allows you to set advisory configurations such as connection test time and advisory filter priorities for alarms, failures, and notices. This user-specified data is sent to the controller so that the controller will know where to send advisories and what filters to use.

Right-click the menu at Controller Level on the navigation tree and choose **Advisory > Advisory Receiver Commission**:



The information below is required and will be displayed by default:

Retrieved Parameters	
	Advanced Parameters? Show Hide
Daily Connection Test Time:	11:07 AM
Alarm Filter Priority:	20
Fail Filter Priority:	20
Notice Filter Priority:	20
Control System Id:	594850252
Original Primary Destination Address:	
*New* Primary Destination Address:	SKAR
Original Backup Destination Address:	
*New* Backup Destination Address:	SKAR

Field	Validation	Notes
Daily Connection Test Time	Required	Connect+ will test the connection with the controller every day. It is the date and time when Connect+ will try to connect to the controller.
Alarm Filter Priority	Required	The priority should be 1-99.

Field	Validation	Notes
Fail Filter Priority	Required	The priority should be 1-99.
Notice Filter Priority	Required	The priority should be 1-99.
Control System ID	Required	It is the unique identifier for that set of controllers configured with monitoring. This will be set automatically by Connect+ if there is no unique ID in the system.
Original Primary Destination Address	Required	This field information is received from the controller. It cannot be edited.
*New* Primary Destination Address	Required	It is identified as where the controller will send an advisory if an advisory occurs.
Original Backup Destination Address	Required	This field information is received from the controller. It cannot be edited.
*New* Backup Destination Address	Required	The backup address. If the advisory cannot send to the primary address, it will send to the backup address.

The user can also configure Connection Verification advanced parameters by clicking **Show**.

The screenshot shows the 'Advisory Receiver Commission' configuration window. The 'Advanced Parameters?' section is expanded, revealing various settings. A red box highlights the advanced parameters section, which includes fields for Connection Delay, Maximum Connection Time, Modem Init String, Modem Baud Rate, Maximum Modem Connect Time, Dial-Out Prefix, and several checkboxes for transmission and retry settings.

Field	Validation	Notes
Connection Delay	Optional	It is used to make controller send alarm to the Connect+ after configured delay time.
Maximum Connection Time	Optional	If the controller failed to send an alarm to the Connect+, it will be connected to <b>Maximum Connection Time</b> .
Transmit Alarms	Optional	Checked by default. It allows the controller to transmit Alarm type advisory to Connect+.
Transmit Fails	Optional	Checked by default. It allows the controller to transmit Fails type advisory to Connect+.
Transmit Notices	Optional	Checked by default. It allows the controller transmit Notices type advisory to Connect+.
Return to Normal	Optional	Checked by default. It allows the controller to transmit return to normal advisory to Connect+.
Randomize Retry Time	Optional	If the option is set to true, it will not use Maximum Connection Time, controller will randomly retry if controller failed to send the alarm to Connect+.
Number of Daily Connection Tests	Optional	It defines how many times the Connect+ will be connected to the controller. For example, if it set as 2, Connect+ will be connected to the controller every 12 hours which start from <b>Daily Connection Test Time</b> .

After the configuration is done, click the **Commission** button to see the message if the Advisory Receiver Commission is completed.

### Advisory Receiver Commission

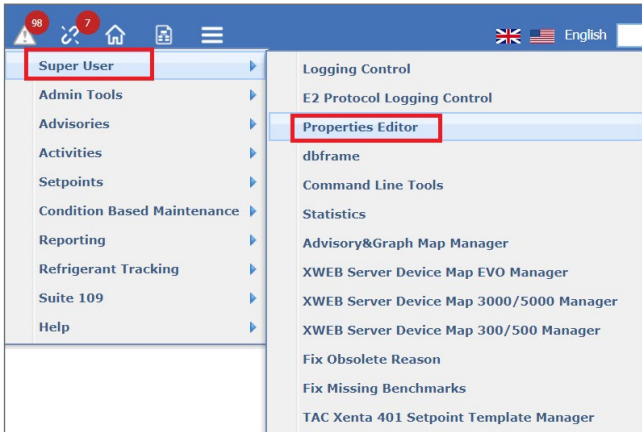
Advisory Receiver Commission activity was completed successfully.

Daily Connection Test Time:	3:38 AM
Alarm Filter Priority:	20
Fail Filter Priority:	20
Notice Filter Priority:	20
Control System Id:	
Original Primary Destination Address:	
Original Backup Destination Address:	

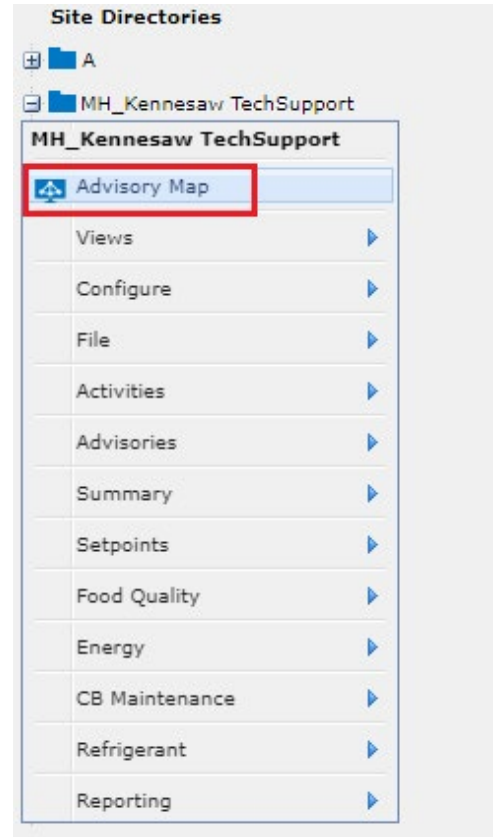
To check the advisories received in the controller, go to the **Advisory View** page.

## 5.4 Enable Advisory Map

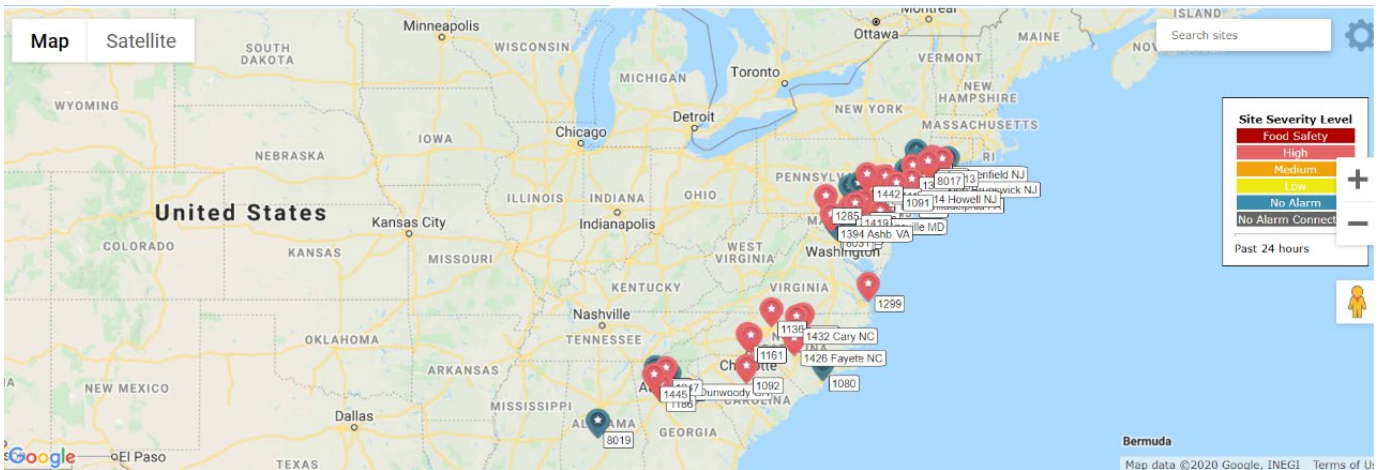
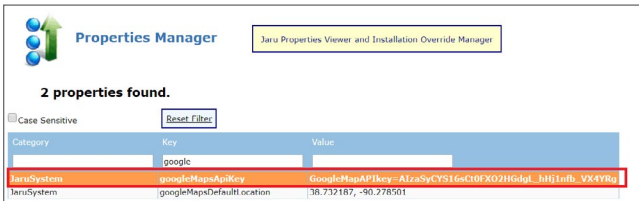
Login to the Connect+ with the super user. Select the Top Menu > **Super User** > **Properties Editor**.



Once it is configured. You will see the **Advisory Map** displayed on the right-click menu of the directory level.



Set the **JaruSystem.googleMapsApiKey**. This is provided by Google to access the Google Maps on the site.





## 6 Configure Advisory & Graph Map Manager

### 6.1 Advisory & Graph Mapping

In the **Advisory View** page, to view the point log of one alarm point, click the link of **Advisory Message**.

**Advisories View**

High **260** | Food Safety **4** | Medium **3** | Low **5** | All

Occurrence Date:  | Time Perspective:

[Reset Filters](#) | [Refresh Advisories](#) | [Restore Default Format](#)

Ad...	Occurrence Date	Age	Received Date	Site	Type	State	Source	Prior...	Advisory Message	Source Ty
	11/4/2020 8:10 AM	19.7 d	11/4/2020 8:13 AM	Store #1	Alarm	Active	CASE TEMP 6	20	<a href="#">Case Temp Hi Limit Exceeded</a>	Device
	11/4/2020 7:15 AM	19.8 d	11/4/2020 7:18 AM	Store #1	Alarm	Active	CASE TEMP 1	20	<a href="#">Case Temp Hi Limit Exceeded</a>	Device
	11/4/2020 7:14 AM	19.8 d	11/4/2020 7:15 AM	Store #1	Alarm	Active	FILTERED PRES	20	High Suction Limit Exceeded	Device
	11/4/2020 6:14 AM	19.8 d	11/4/2020 6:15 AM	Store #1	Fail	Active	RX-300 1: RACK A	20	Device absent from network	Device
	11/4/2020 6:14 AM	19.8 d	11/4/2020 6:15 AM (2)	Store #1	Fail	Active	RX-300 1: RACK A	20	Device absent from network	Device

To enable the link, administrator will need to log into the super user, select the Top Menu > **Super User** > **Advisory & Graph Map Manager** to see the **Advisory & Graph Mapping** section.

The screenshot shows the Super User menu with the following items: Logging Control, E2 Protocol Logging Control, Properties Editor, dbframe, Command Line Tools, Statistics, **Advisory&Graph Map Manager** (highlighted), XWEB Server Device Map EVO Manager, XWEB Server Device Map 3000/5000 Manager, XWEB Server Device Map 300/500 Manager, Fix Obsolete Reason, Fix Missing Benchmarks, and TAC Xenta 401 Setpoint Template Manager.

The screenshot shows the **Advisory & Graph Mapping** section with the following content:

**Download** the currently active Advisory&Graph Mapping.csv file.

**Delete** the overridden Advisory&Graph Mapping.csv file. created 08/14/2019 10:51:07

**Upload** **Browse...** No file selected.

**Point & Critical Information Mapping**

**Download** the currently active Default Point&CriticalInfoMapping.csv file.

**Upload** **Browse...** No file selected.

Download the default template by clicking the **Download** button. You could configure which type of advisories will show with the link in the downloaded **Advisory & Graph Mapping.csv**.

Protocol	Application Type	Advisory message	Action	Execution_info
E2	Circuits (Standard)	Case Temp Hi Limit Exceeded	graph point	CASE TEMP 1;DEFROST;Case Alarm Hi
E2	Circuits (Standard)	Case Temp Low Limit Exceeded	graph point	CASE TEMP 1;DEFROST;Case Alarm Low



Field	Validation	Notes
Protocol	Required	E2, Site Supervisor, XWEB Server 300/500, XWEB Server 3000/5000 or XWEB Server EVO.
Application Type	Required	It is the application type for which the advisory was generated.
Advisory message	Required	The message for one advisory. You could get it from Advisory Message column in Advisories View page.
Action	Required	The graph point.
Execution info	Required	It defines which points will be displayed together with the advisory point in log graph.

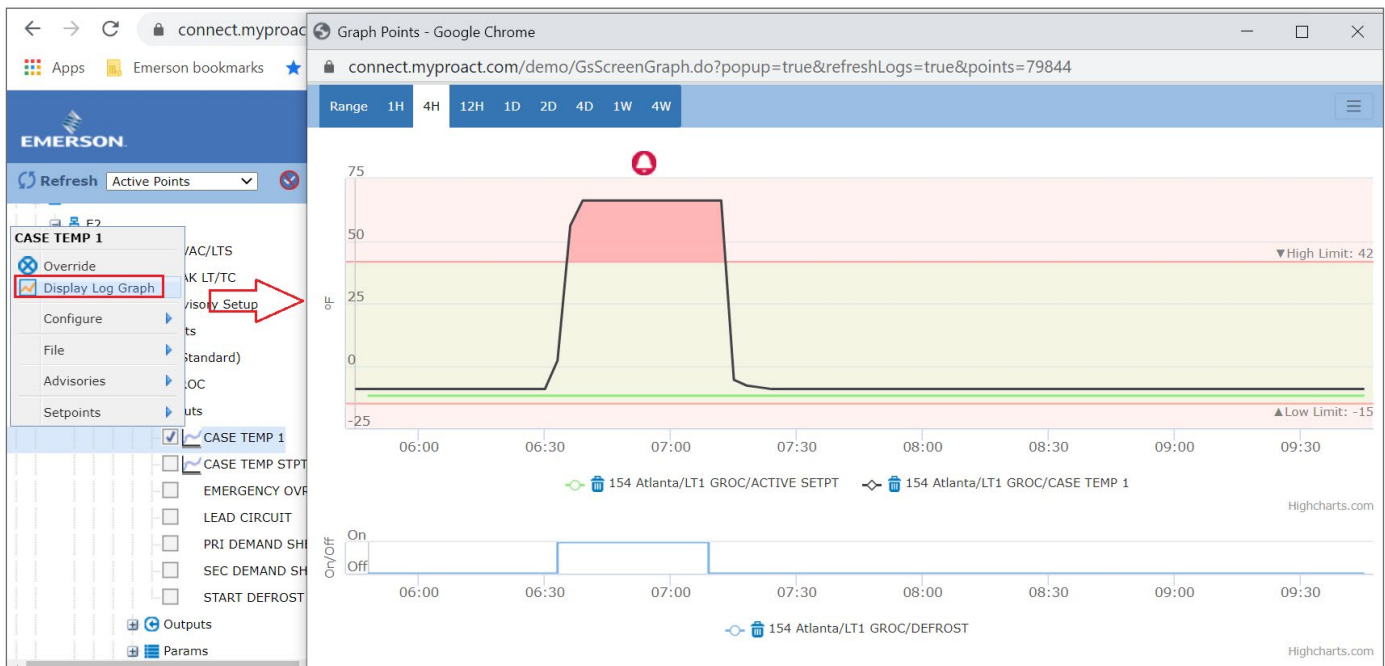
When configuration is done, you can click **Browse** button to choose your file, then click **Upload**.

Go to **Advisory View** page to see the configured advisory link on **Advisory Message** field. Click the link to go to the log graph page.

High 16		Medium 0		Low 0		All			
Food Safety 16									
Occurrence Date	Custom Range	Time Perspective:	Site Time	from	11/01/20	to	01/14/21	Go	
<a href="#">Reset Filters</a> <a href="#">Refresh Advisories</a> <a href="#">Restore Default Format</a> <a href="#">Terminal Mode</a>									
Ad...	Occurrence Date	Age	Received Date	Site	Type	State	Source	Prior...	Advisory Message
	11/25/2020 11:09 AM	1.7 mo	11/25/2020 11:11 AM	Store #1	Alarm	Active	CASE TEMP 1	20	<a href="#">Case Temp Hi Limit Exceeded</a>
	11/25/2020 11:09 AM	1.7 mo	11/25/2020 11:11 AM	Store #1	Alarm	Active	CASE TEMP 1	20	<a href="#">Case Temp Hi Limit Exceeded</a>
	11/25/2020 11:08 AM	1.7 mo	11/25/2020 11:08 AM	Store #1	Alarm	Active	CASE TEMP 4	20	<a href="#">Case Temp Hi Limit Exceeded</a>
	11/25/2020 11:06 AM	1.7 mo	11/25/2020 11:08 AM	Store #1	Alarm	Active	CASE TEMP 3	20	<a href="#">Case Temp Hi Limit Exceeded</a>

## 6.2 Point & Critical Information Mapping

This configuration will show relative points in the log graph. If you want to see other relative points in the log graph, select one point to configure.



Same with the Advisory & Graph Mapping, you can select Top Menu > **Super User** > Advisory & **Graph Map Manager** to see the **Point & Critical Information Mapping** section.

### Advisory & Graph Mapping

Download

the currently active Advisory&Graph Mapping.csv file.

Delete

the overridden Advisory&Graph Mapping.csv file. created 08/14/2019 10:51:07

Upload

Browse...

No file selected.

### Point & Critical Information Mapping

Download

the currently active Default Point&CriticalInfoMapping.csv file.

Upload

Browse...

No file selected.

Click the **Download** button to download the default file. You can also configure the points in the file.

A	B	C	D	E	F	G	H	I	J
Protocol	Application Type	Point	Setpoint	High limit	Low limit	Defrost	Defrost Timeslot		
E2	Circuits (Standard)	CASE TEMP 1	ACTIVE SETPT	Case Alarm Hi	Case Alarm Lo	DEFROST	Defrost Time 1:Defrost Time 2:D		
E2	Circuits (Standard)	CASE TEMP 2	ACTIVE SETPT	Case Alarm Hi	Case Alarm Lo	DEFROST	Defrost Time 1:Defrost Time 2:D		
E2	Circuits (Standard)	CASE TEMP 3	ACTIVE SETPT	Case Alarm Hi	Case Alarm Lo	DEFROST	Defrost Time 1:Defrost Time 2:D		
E2	Circuits (Standard)	CASE TEMP 4	ACTIVE SETPT	Case Alarm Hi	Case Alarm Lo	DEFROST	Defrost Time 1:Defrost Time 2:D		
E2	Circuits (Standard)	CASE TEMP 5	ACTIVE SETPT	Case Alarm Hi	Case Alarm Lo	DEFROST	Defrost Time 1:Defrost Time 2:D		
E2	Circuits (Standard)	CASE TEMP 6	ACTIVE SETPT	Case Alarm Hi	Case Alarm Lo	DEFROST	Defrost Time 1:Defrost Time 2:D		
E2	Circuits (Standard)	CASE TEMP 7	ACTIVE SETPT	Case Alarm Hi	Case Alarm Lo	DEFROST	Defrost Time 1:Defrost Time 2:D		
E2	Circuits (Standard)	CASE TEMP 8	ACTIVE SETPT	Case Alarm Hi	Case Alarm Lo	DEFROST	Defrost Time 1:Defrost Time 2:D		
E2	Circuits (Standard)	CASE TEMP 9	ACTIVE SETPT	Case Alarm Hi	Case Alarm Lo	DEFROST	Defrost Time 1:Defrost Time 2:D		
E2	Circuits (Standard)	CASE TEMP 10	ACTIVE SETPT	Case Alarm Hi	Case Alarm Lo	DEFROST	Defrost Time 1:Defrost Time 2:D		
E2	Circuits (Standard)	CASE TEMP 11	ACTIVE SETPT	Case Alarm Hi	Case Alarm Lo	DEFROST	Defrost Time 1:Defrost Time 2:D		
E2	Circuits (Standard)	CASE TEMP 12	ACTIVE SETPT	Case Alarm Hi	Case Alarm Lo	DEFROST	Defrost Time 1:Defrost Time 2:D		
E2	Circuits (Standard)	PRODUCT TEMP 1	ACTIVE SETPT	Product Alm Hi	Product Alm Lo	DEFROST	Defrost Time 1:Defrost Time 2:D		

Field	Validation	Notes
Protocol	Required	E2, Site Supervisor, XWEB Server 300/500, XWEB Server 3000/5000 or XWEB Server EVO.
Application Type	Required	The application type which advisory generated for.
Point	Required	Defines the original point you need to select.
Setpoint	Optional	The relative setpoint will show the selected point.
High Limit	Optional	The relative high limit point of selected point, if the selected point value is higher than high limit, the advisory will be generated.
Low Limit	Optional	The relative low limit point of selected point, if the selected point value is lower than low limit, the advisory will be generated.
Defrost	Optional	The relative defrost point will show the selected point.

The default file will configure Case Temp and Product Temp for Circuits (Standard), Circuits (Case), Circuits (XM) of E2 and Site Supervisor.

Once the configuration is done, select the file by clicking **Browse** then click **Upload**. The configuration will be applied.

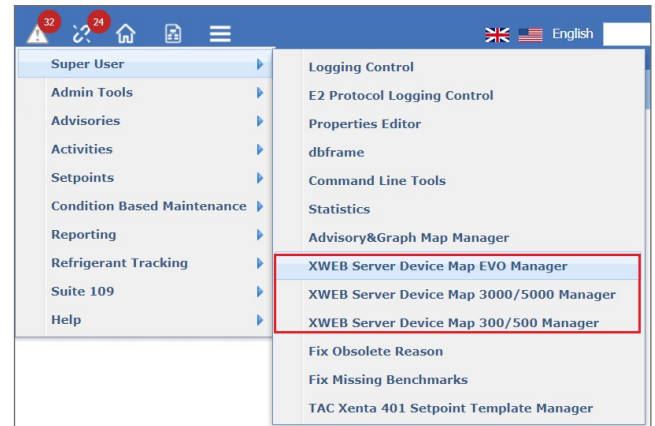
## 7 Configure XWEB Mapping

### 7.1 Download XWEB Server Device Map File

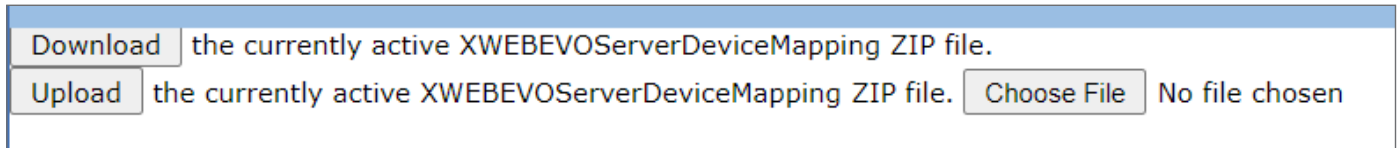
Select the Top Menu > **Super User** to see **XWEB Server Device Map Manager** menu for each Model. Currently, Connect+ support 3 models for Xweb device:

- Xweb EVO
- Xweb 3000/5000
- Xweb 300/500

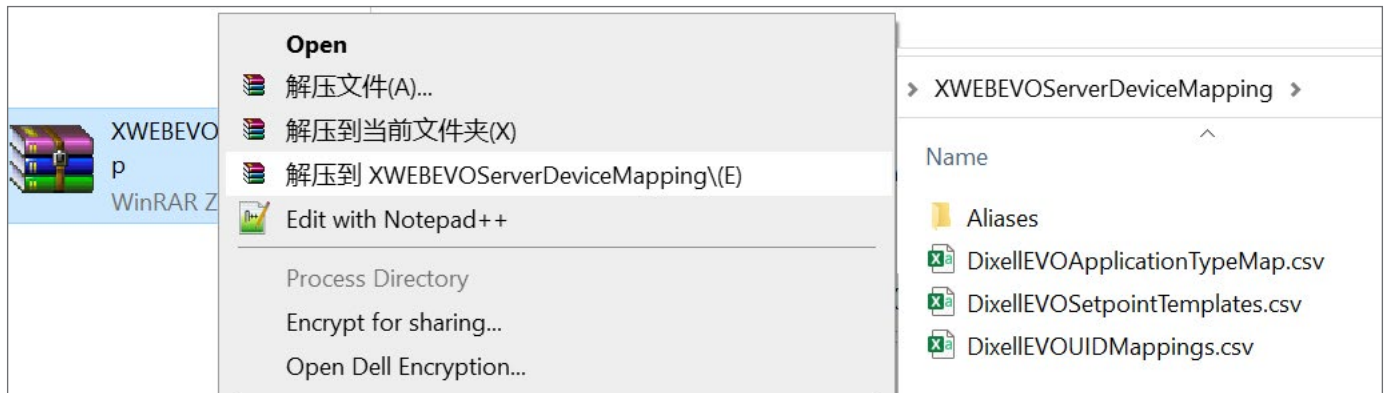
Select the **XWEB Server Device Map EVO Manager** menu for instance.



You can download the default template by clicking the **Download** button, The zip file **XWEBEVOServerDeviceMapping.zip** will be downloaded.



In the zip file, you will see below files:



File	Notes
DixellEVOApplicationTypeMap	Used to configure the mapping of the XWEB device and Connect+ application type.
DixellEVOSetpointTemplate	Configured to monitor and manage the setpoint changes
DixellEVOUIDMapping	Defines the point mapping relationship.
Aliases	Used to configure the point aliases for each device.

## 7.2 Configure XWEB Server Device Map File

### 7.2.1 Configure DixellEVOApplicationTypeMap.csv file

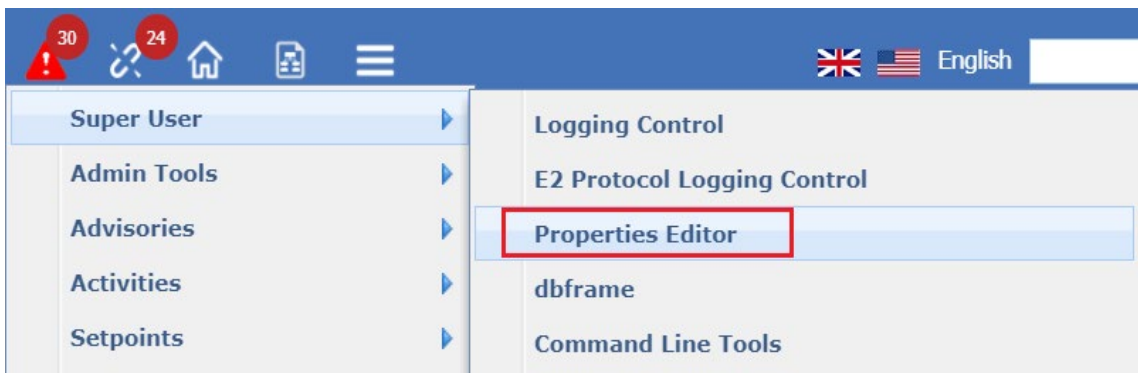
To add a new device support in the Connect+, map new devices in **DixellEVOApplicationTypeMap.csv** file. The devices added in the file will be shown in Connect+ navigation tree.

There are four columns in the file.

Field	Validation	Notes
dixellDeviceType	Required	The Dixell device model. Add new device model name in this column.
unifiedAppTypeName	Required	The mapped application type name in Connect+ defines which application type you want your new device to be mapped.
nativeAppTypeName	Required	The name displayed in the Application Name should match with the one in Connect+. Usually, it is the same as unifiedAppTypeName.
appTypeProtocolUniqueld	Required	The unique application type ID in Connect+.

### How to get ProtocolUniqueld

Login as the super user, Select Top Menu > **Superuser** > **Properties Editor**.



Find **JaruSystem.isDebugMode** and change the value to true.

## Properties Manager

Jaru Properties Viewer and Installation Override Manager

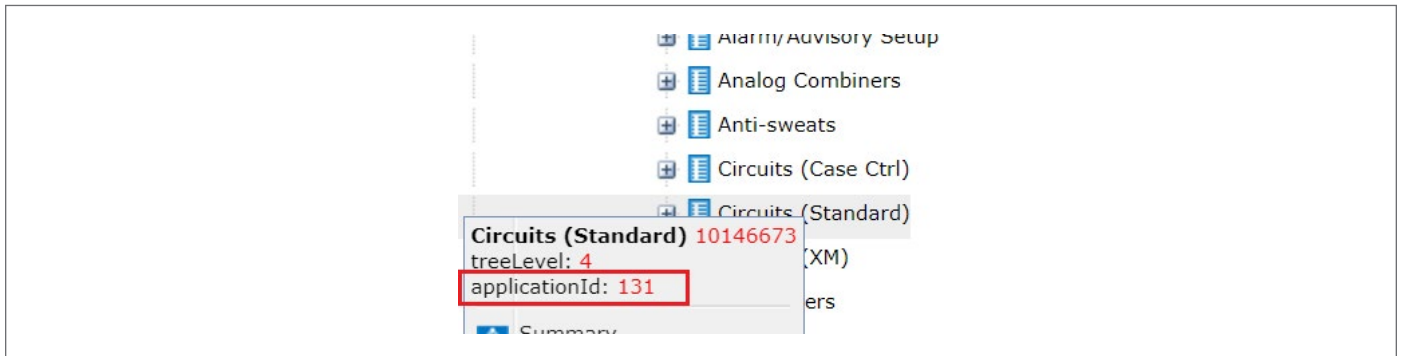
**7 properties found.**

Case Sensitive Reset Filter

Category	Key	Value
	deb	
DataCollection	QA.Debug	false
GatherEstimationStatistics	isEstimateDebugEnabled	off
JaruSystem	isDebugMode	true
SyncActivity	isDebugMode	false
XWebServerConfigs	enableDebug	false
XWebServerConfigs	gateway.json.debugContent	false
XWebServerConfigs	proxy.debugProxyContent	false

Re-login to the Connect+ and find the application type from navigation tree that you want to map in the Connect+. For example. Circuit (Standard), right-click on the application type to see the **applicationId**.

Write this ID in appTypeProtocolUniqueld column.



### 7.2.2 Configure DixellEVOUIDMapping.csv file

It defines the point mapping relationship for XWEB 300/500 and XWEB3000/5000. This mapping will be used to show which points will be shown from the Connect+ navigation tree. But for XWEB EVO and Connect+ all points will be shown from XWEB device in navigation tree. This mapping can only be used for Setpoint Management.

Field	Validation	Notes
appTypeProtocolUniqueld	Required	The unique application type ID in the Connect+ (See above steps).
unifiedAppTypeName	Required	The mapped application type name in the Connect+. You can define which application type you want your new device to be mapped.
pointProtocolUniqueld	Required	You can give a unique ID number to each point.
deviceType	Required	The device model such as, XR75, XM679, etc.
pointOriginalUniqueld	Required	Point name starts with _@, like _@SEt, _@Hy, etc.

### 7.2.3 Configure DixellEVOSetpointTemplate.csv file

In order for the user to monitor the points change in the Setpoint management, you need to configure DixellEVOSetpointTemplate.csv file. The points configured in the file will generate an exception if the Connect+ detect the point value changes.

Field	Validation	Notes
protocolName	Required	XWEB Server EVO
pointProtocolUniqueld	Required	This ID should be same as the pointProtocolUniqueld configured in DixellEVOUIDMapping.csv file.
appTypeProtocolUniqueld	Required	The unique application type ID in Connect+ (see above steps).
unifiedAppTypeName	Required	The mapped application type name in Connect+ defines which application type you want your new device to be mapped.
unifiedPointName	Required	Configured as the point name display in Connect+ setpoint report, map the device real point name, which is configured in nativePointName field to this field. For example, you can configure the Setpoint as the Connect+ displayed name in this field, and configure the device point name SET in nativePointName to match them.
typeFormat	Required	Point type format. It could be %f (float), %s (string), or a list, like {On, Off}.
possiblePointer	Required	Defined as if the point will be a pointer of other points. Usually, it is set as FALSE.
energyCritical	Required	<p><b>Setpoint Category</b></p> <p>Set it to TRUE for one point and select the Energy Critical Setpoint in the setpoint configuration. Setpoint exception will be generated if the point value is changed.</p> <div style="border: 1px solid black; padding: 10px;"> <p>- OR - <input checked="" type="radio"/> Enter values specifically for this item: <b>Directory - Demo</b></p> <p><input checked="" type="checkbox"/> Enable Setpoint Resolution</p> <p>Service Interval</p> <p><input checked="" type="radio"/> <b>Energy Critical Setpoints</b></p> <p>Average Price of Power</p> <p>Average Rack Design Load</p> <p>Average Lighting Design Load</p> <p>Average Anti-Sweat Design Load</p> <p><input type="radio"/> Alarm Critical Setpoints</p> </div>
alarmSetpoint	Required	<p><b>Setpoint Category</b></p> <p>Set it to TRUE for one point and select the Alarm Critical Setpoint in the setpoint configuration. Setpoint exception will be generated if the point value is changed.</p> <div style="border: 1px solid black; padding: 10px;"> <p>- OR - <input checked="" type="radio"/> Enter values specifically for this item: <b>Directory - Demo</b></p> <p><input checked="" type="checkbox"/> Enable Setpoint Resolution</p> <p>Service Interval</p> <p><input type="radio"/> Energy Critical Setpoints</p> <p><input checked="" type="radio"/> <b>Alarm Critical Setpoints</b></p> <p><input type="radio"/> Energy Critical and Alarm Critical Setpoints</p> <p><input type="radio"/> Setpoint Configuration Profile</p> </div>

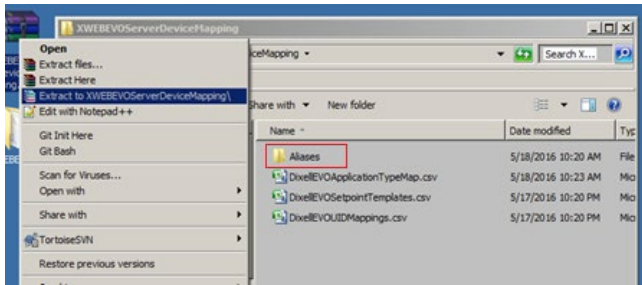


Field	Validation	Notes																																																																																																
checkOverride	Required	It should be TRUE or FALSE. If it is TRUE, it will get the point's override value as the point value. If it is FALSE, the original value will be retrieved as the point value.																																																																																																
nativeAppTypeName	Required	It is the application name which is identified in the Connect+. For example, Anti-sweat, Circuit (Standard), etc.																																																																																																
nativePointName	Required	Refer to unifiedPointName.																																																																																																
nativePointCategory	Required	It should be POINT_CATEGORY_INPUT, POINT_CATEGORY_OUTPUT, or POINT_CATEGORY_PARAMETER.																																																																																																
nativePointType	Required	It defined as number 1 = digital input, 2 = digital output, 3 = digital status, 4 = digital alarm, 10 = analogic input, 11 = analogic output, 12 = analogic setpoint, 20 = command, 50 = parameter point																																																																																																
deviceUnits	Required	The unit of the points. It begin with REU_ , for example, REU_BAR, REU_ON_OFF, REU_CCF, REU_KPA, etc.																																																																																																
returnUnits	Required	Same as device Units.																																																																																																
notes	Optional	You can add notes here.																																																																																																
supportedDevicePoint	Optional	Identified as the device name: point name, it is used to configure the mapping between the Connect+ and device. For example, XH50:Set. This field is required for XWEB 300/500, but not need for XWEB 3000/5000 and XWEB EVO.																																																																																																
setpointServiceSupported	Required	<p>Set the value as TRUE, it will show the point in Setpoint Profile, then you can decide which points will be monitored when the setpoint is changed in profile configuration. If the value is set as FALSE, the point will not be displayed.</p> <div data-bbox="656 993 1495 1673" data-label="Form"> <p><b>Custom Profile</b></p> <p>Profile Name <input type="text"/></p> <p>Average Price of Power <input type="text"/> \$/KWH</p> <p>Average Rack Design Load <input type="text"/> KW <input type="button" value="v"/></p> <p>Average Lighting Design Load <input type="text"/> KW</p> <p>Average Anti-Sweat Design Load <input type="text"/> KW</p> <p> <input type="button" value="Select all Energy Critical Setpoint"/> <input type="button" value="Select all Alarm Setpoint"/> <input type="button" value="Select All"/> <input type="button" value="Unselect All"/> </p> <table border="1"> <thead> <tr> <th colspan="2">Application Type</th> <th>Protocol</th> <th></th> </tr> </thead> <tbody> <tr><td><input checked="" type="checkbox"/></td><td>Anti-Sweat</td><td>XWEB Server 300/500</td><td></td></tr> <tr><td><input checked="" type="checkbox"/></td><td>Circuits (Case Ctrl)</td><td>XWEB Server 300/500</td><td></td></tr> <tr><td><input checked="" type="checkbox"/></td><td>Circuits (Standard)</td><td>XWEB Server 300/500</td><td></td></tr> <tr><td><input checked="" type="checkbox"/></td><td>Expansion Valve</td><td>XWEB Server 300/500</td><td></td></tr> <tr><td><input checked="" type="checkbox"/></td><td>Rack Control</td><td>XWEB Server 300/500</td><td></td></tr> <tr><td><input checked="" type="checkbox"/></td><td>Suction Group</td><td>XWEB Server 300/500</td><td></td></tr> <tr><td><input checked="" type="checkbox"/></td><td>Anti-Sweat</td><td>XWEB Server 3000/5000</td><td></td></tr> <tr><td><input checked="" type="checkbox"/></td><td>Circuits (Case Ctrl)</td><td>XWEB Server 3000/5000</td><td></td></tr> <tr><td><input checked="" type="checkbox"/></td><td>Circuits (Standard)</td><td>XWEB Server 3000/5000</td><td></td></tr> <tr><td><input checked="" type="checkbox"/></td><td>Expansion Valve</td><td>XWEB Server 3000/5000</td><td></td></tr> <tr><td><input checked="" type="checkbox"/></td><td>Rack Control</td><td>XWEB Server 3000/5000</td><td></td></tr> <tr><td><input checked="" type="checkbox"/></td><td>Suction Group</td><td>XWEB Server 3000/5000</td><td></td></tr> <tr><td><input checked="" type="checkbox"/></td><td>Anti-Sweat</td><td>XWEB Server EVO</td><td></td></tr> <tr><td><input type="checkbox"/></td><td></td><td></td><td>Alarm Delay</td></tr> <tr><td><input checked="" type="checkbox"/></td><td></td><td></td><td>Defrost Interval</td></tr> <tr><td><input checked="" type="checkbox"/></td><td></td><td></td><td>Energy Setpoint Diff</td></tr> <tr><td><input type="checkbox"/></td><td></td><td></td><td>High Alarm Limit</td></tr> <tr><td><input type="checkbox"/></td><td></td><td></td><td>Low Alarm Limit</td></tr> <tr><td><input checked="" type="checkbox"/></td><td></td><td></td><td>Setpoint</td></tr> <tr><td><input checked="" type="checkbox"/></td><td>Circuits (Case Ctrl)</td><td>XWEB Server EVO</td><td></td></tr> <tr><td><input checked="" type="checkbox"/></td><td>Circuits (Standard)</td><td>XWEB Server EVO</td><td></td></tr> <tr><td><input checked="" type="checkbox"/></td><td>Expansion Valve</td><td>XWEB Server EVO</td><td></td></tr> <tr><td><input checked="" type="checkbox"/></td><td>Rack Control</td><td>XWEB Server EVO</td><td></td></tr> </tbody> </table> </div>	Application Type		Protocol		<input checked="" type="checkbox"/>	Anti-Sweat	XWEB Server 300/500		<input checked="" type="checkbox"/>	Circuits (Case Ctrl)	XWEB Server 300/500		<input checked="" type="checkbox"/>	Circuits (Standard)	XWEB Server 300/500		<input checked="" type="checkbox"/>	Expansion Valve	XWEB Server 300/500		<input checked="" type="checkbox"/>	Rack Control	XWEB Server 300/500		<input checked="" type="checkbox"/>	Suction Group	XWEB Server 300/500		<input checked="" type="checkbox"/>	Anti-Sweat	XWEB Server 3000/5000		<input checked="" type="checkbox"/>	Circuits (Case Ctrl)	XWEB Server 3000/5000		<input checked="" type="checkbox"/>	Circuits (Standard)	XWEB Server 3000/5000		<input checked="" type="checkbox"/>	Expansion Valve	XWEB Server 3000/5000		<input checked="" type="checkbox"/>	Rack Control	XWEB Server 3000/5000		<input checked="" type="checkbox"/>	Suction Group	XWEB Server 3000/5000		<input checked="" type="checkbox"/>	Anti-Sweat	XWEB Server EVO		<input type="checkbox"/>			Alarm Delay	<input checked="" type="checkbox"/>			Defrost Interval	<input checked="" type="checkbox"/>			Energy Setpoint Diff	<input type="checkbox"/>			High Alarm Limit	<input type="checkbox"/>			Low Alarm Limit	<input checked="" type="checkbox"/>			Setpoint	<input checked="" type="checkbox"/>	Circuits (Case Ctrl)	XWEB Server EVO		<input checked="" type="checkbox"/>	Circuits (Standard)	XWEB Server EVO		<input checked="" type="checkbox"/>	Expansion Valve	XWEB Server EVO		<input checked="" type="checkbox"/>	Rack Control	XWEB Server EVO	
Application Type		Protocol																																																																																																
<input checked="" type="checkbox"/>	Anti-Sweat	XWEB Server 300/500																																																																																																
<input checked="" type="checkbox"/>	Circuits (Case Ctrl)	XWEB Server 300/500																																																																																																
<input checked="" type="checkbox"/>	Circuits (Standard)	XWEB Server 300/500																																																																																																
<input checked="" type="checkbox"/>	Expansion Valve	XWEB Server 300/500																																																																																																
<input checked="" type="checkbox"/>	Rack Control	XWEB Server 300/500																																																																																																
<input checked="" type="checkbox"/>	Suction Group	XWEB Server 300/500																																																																																																
<input checked="" type="checkbox"/>	Anti-Sweat	XWEB Server 3000/5000																																																																																																
<input checked="" type="checkbox"/>	Circuits (Case Ctrl)	XWEB Server 3000/5000																																																																																																
<input checked="" type="checkbox"/>	Circuits (Standard)	XWEB Server 3000/5000																																																																																																
<input checked="" type="checkbox"/>	Expansion Valve	XWEB Server 3000/5000																																																																																																
<input checked="" type="checkbox"/>	Rack Control	XWEB Server 3000/5000																																																																																																
<input checked="" type="checkbox"/>	Suction Group	XWEB Server 3000/5000																																																																																																
<input checked="" type="checkbox"/>	Anti-Sweat	XWEB Server EVO																																																																																																
<input type="checkbox"/>			Alarm Delay																																																																																															
<input checked="" type="checkbox"/>			Defrost Interval																																																																																															
<input checked="" type="checkbox"/>			Energy Setpoint Diff																																																																																															
<input type="checkbox"/>			High Alarm Limit																																																																																															
<input type="checkbox"/>			Low Alarm Limit																																																																																															
<input checked="" type="checkbox"/>			Setpoint																																																																																															
<input checked="" type="checkbox"/>	Circuits (Case Ctrl)	XWEB Server EVO																																																																																																
<input checked="" type="checkbox"/>	Circuits (Standard)	XWEB Server EVO																																																																																																
<input checked="" type="checkbox"/>	Expansion Valve	XWEB Server EVO																																																																																																
<input checked="" type="checkbox"/>	Rack Control	XWEB Server EVO																																																																																																

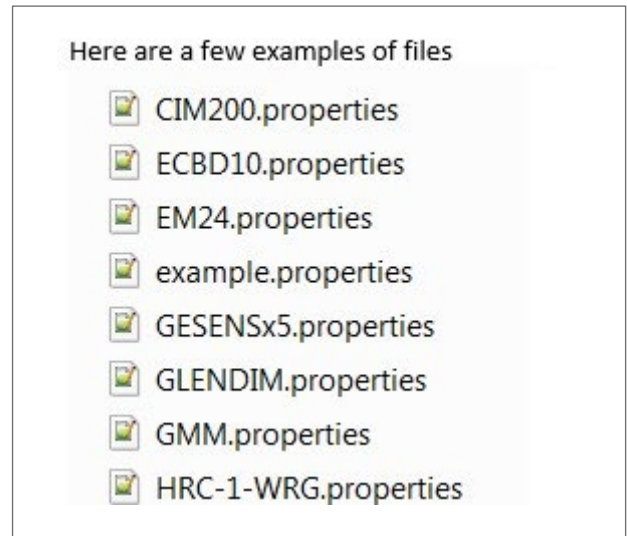
## 7.2.4 Configure Aliases File

You can change the point displayed name in the Connect+, to configure it. Follow below steps:

1. In XWEBEVOserverDeviceMapping.zip file, you will see an Aliases folder.



2. Add property files for each device type under this folder.

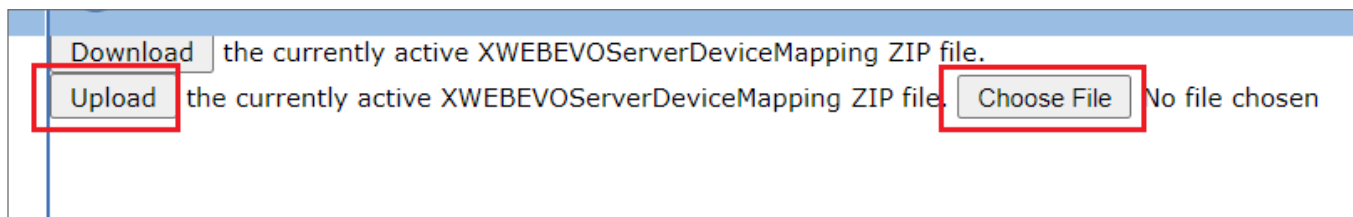


3. Configure customized point name and follow below rules:

```
#RULE1, THIS PROPERTY FILE NAME MUST BE DEVICE TYPE LIKE XR75. IF THERE ARE MULTIPLE
#      DEVICE TYPES, ONE SHOULD CREATE MULTIPLE PROPERTY FILES.
#RULE2, THE CONTENT MUST BE NAME=VALUE. FOR EXAMPLE, IF ONE WANTS TO NAME
#      "SET POINT-F" AS "SET POINT", THE CONTENT SHOULD BE SET POINT-F=SET POINT.
#NOTE, IF ORIGINAL NAME CONTAINS BLANK, IT MUST BE ESCAPED BY USING SLASH SIGN (\) .
#      FOR EXAMPLE, IF ORIGINAL NAME IS "% AVERAGE", IN THIS PROPERTY FILE IT MUST
#      BE WRITE AS "%\ AVERAGE". IF ORIGINAL NAME CONTAINS A SLASH SIGN, IT ALSO
#      SHOULD BE ESCAPED BY USING SLASH SIGN. FOR EXAMPLE, "PROBE 1\F" SHOULD BE
#      "PROBE\ 1\F".
```

## 7.3 Upload XWEB Server Device Map File

After you finish the configuration, save the file and re-compress them. Select the Top Menu > **Super User** > **XWEB Server Device Map EVO Manager**. Click the **Choose File** button to select your new zip file and click Upload button to upload it to the server.



After tomcat is restarted, the files will be working.

## 8 System Schedule Configuration

In Connect+, some schedules are automatically set up for system job after the installation. The system schedules cannot be edited by users.

All schedules are executed based on the server's time zone. The server's time zone will be displayed to the user at the top of the screen under the Schedule Manager heading.

You can access the schedule manager page by clicking the Top Menu > **Activities** > **Schedule Manager**. Check **Show System Schedules** check-box to show the system schedules.

**Schedule Manager**  
All schedules are based on the server's time zone: (GMT -05:00) Cuba Standard Time - America/Havana (CST) (DST)

Show System Schedules

+ Add New    Reset Filters

Name	Type	User	Schedule	Next Run Time
InboundAdvisoryQueueToAdvisoryJob	system	system	Every 1 minute	2/4/21 3:20

You can get system schedule description and recommend default setting from the below table:

Schedule Name	Description	Recommended Default Setting
CheckConnectionTestJob	Configure to check if advisory can be received at the prescribed time. If not, a controller offline alarm will be generated.	Disabled
GatherEstimationStatisticsJob	Gather an activity statistic for estimation.	Disabled
LogPartitionJob	Move the data before latest 13 months log to a new tables in the database to improve the performance.	Disabled
ProblemSiteReportEmailJob	Configure to run and send a report (via email) listing the problem sites that occurred over a set period of time.	Disabled
Sync Server Time To TAC Controllers	Configure to sync the TAC controller time with the server time.	Disabled
FQRDataGatheringJob	Gather food quality related points data and log. Like Case Temp, Product Temp, etc. It gives you the ability to generate the report after the data gathering is completed.	Disabled
FQRReportEmailJob	Configure to send out FQR exceptions/full/summary reports.	Recommend setting the time to run at an hour after the FQR Data Gathering and Report Generation has been finished.
InboundAdvisoryQueueToAdvisoryJob	Configure to show advisory in the Connect+ and forward advisory to email or UARD.	Every 1 minute
Address Pending Fixed	Configure to update the Pending Fixed status to Fixed for Setpoint Resolution	Every 30 minutes
AdvisoryPurgeJob	Configure to purge old advisories based on the configuration in the Configure Advisory Purge page.	Every 2 hours

Schedule Name	Description	Recommended Default Setting
HandleUserJob	Configure to disable the schedule for expired user and delete the schedule for the deleted user	Every Day at midnight
AutoDeleteDumpFilesJob	Configure to delete dump files and release server space. It will keep latest 1 dump file and delete others.	Recommend setting the time to run once a week at midnight.
GlobalSearchIndexJob	Configure to update the global search list.	Every Day
SetpointResolutionRegenerateFailuresSystemJob	Configure to generate the Setpoint Resolution Failures report.	Every 168 hours
UpdateExceptionsContractorSystemJob	Configured to update the service provider in the Setpoint Exception report if service provider is changed or the responsible for service provider has been modified.	Every Day

## 9 Enable Advanced Security for Admin organization (Optional)

### 9.1 Multi-Factor Authentication

If the company has security requirement for the Connect+ login, the administrator can use Multi-Factor Authentication function for double verification.

#### 9.1.1 Configure Multi-Factor Authentication

To turn on the Multi-Factor function, you need to log into the Connect+ with super user. Select **Super User > Properties Editor**.

Change JaruSystem. “**multiFactorAuthenticationModel**” to **Multi-Factor**.

Properties Manager

Jaru Properties Viewer and Installation Override M

4 properties found.

Case Sensitive

Category	Key	Value
	factor	
CondenserMaintenance	slopFactor	0.2
EconomicAlg	SetpointCondenserAlg.climate_factor	0.50
JaruSystem	Cluster.barometerAlarmCsLoadFactor	30.0
JaruSystem	multiFactorAuthenticationModel	None

JaruSystem.**multiFactorAuthenticationModel** =

Create/Update Override Value

default (lowest possible effective override level)

C:\Program Files\Tomcat 9.0\webapps\emerson\Jaruovertides.properties

JaruOverrides.properties

[database]

After the Multi-Factor is enabled, all Connect+ user needs to do Multi-Factor Authentication for the first-time login.

But you can also configure it to make some groups skip the Multi-Factor Authentication. Set JaruSystem.byPassMFAGroups property, configure the group name which you want to skip Multi-Factor Authentication in this field, if you want to add more than 1 group, you separate the group name by commas.

JaruSystem.**byPass2FAGroups** =

Create/Update Override Value

default (lowest possible effective override level)

C:\Program Files\Tomcat 9.0\webapps\emerson\Jaruovertides.properties

JaruOverrides.properties

[database]

#### 9.1.2 Login with Multi-Factor Authentication

The user will see the Multi-Factor Authentication that appears after first login.

##### Login with Email

If your user login account has a configured email, you will be required to send a security code to your email by clicking the **Send Security Code** button.

Login

User Authentication

Multi-Factor Authentication has been turned on for your account. To secure your account, we will send you a security code to verify your account.

Login ID

Password

Forgot Password? | Forgot Login ID?

Email:

Please enter your security code:

After clicking, the Connect+ will wait 3 minutes for the user to input the security code. If you miss filling in your security code within 3 minutes, you will need to click the **Send Security Code** button again to receive another security code to your email.

Once you received the security code in your email, enter it in the **Security Code** field and click **Submit**. After the successful authentication, you can start logging into the Connect+. If authentication fails, you need to check the security code and re-enter it again. Connect+ will restrict the failed authentication after 5 times. The administrator can change the value of **numberOfLoginTimes** in the superuser property.

Your account will be temporary locked if failed authentication times have exceeded. You can re-login after 24 hours.

User Authentication

Multi-Factor Authentication has been turned on for your organization. Security code would be sent to your email: [juan.guo@emerson.com](mailto:juan.guo@emerson.com)

Number of login attempts exceeded, your account is locked. Please login after 24 hours.

Security Code

## Login without Email

You cannot log in if account is not configured with email. Please contact your administrator.

### User Authentication

Multi-Factor Authentication has been turned on for your organization. Email is required to receive the Security Code. Please contact Administrator to update your user profile with valid email. You will be forwarded to login page after 10 seconds.

**Security Code**

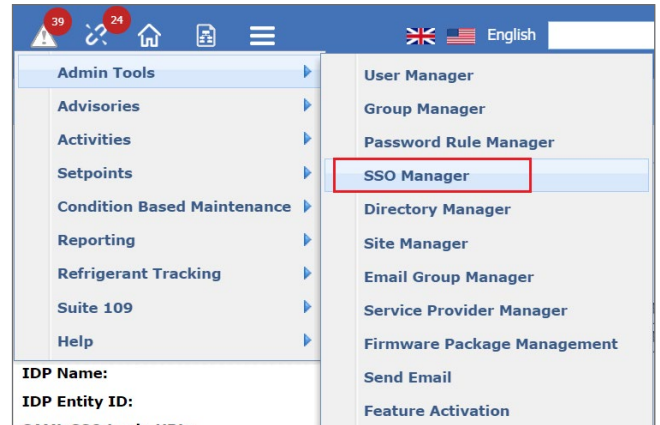
After passing the Multi-Factor authentication, you will not need to pass the authentication again for next login because the authentication information is recorded in the browser cookies. If you change a browser or change a device, you will need to verified again.

## 9.2 Single Sign-on

Single Sign-on allow you to log into the Connect+ using the company credential.

### 9.2.1 Configure Single Sign-on

Select the Top Menu > **Admin Tools** > **SSO Manager** to see the **SSO Configuration** page.



You can enable SSO and configure the properties from this page to establish the connection between the Connect+ and IDP server.

### Connect+ SSO Configuration

SSO Enabled:

SP Entity ID:

ASC (Consumer) URL:

IDP Name:

IDP Entity ID:

SAML SSO Login URL:

X.509 Certificate: 

```
-----BEGIN CERTIFICATE-----
o36f%poc4Jw#oR*Iz68nujP
vBcZTWUNov4o36f%poc4J
#oR*Iz68nujPvBcZTWUNo4
o36f%poc4Jw#oR*Iz68nujPv
BcZTWUNov4o36f%poc4Jw#
#oR*Iz68nujPvBcZTWUNov
o36f%poc4Jw#oR*Iz68nujP
vBcZTWUNov44ghfjnPhdji
```

Need to provide by customer and configure in Connect+

Attribute Keys(Optional):

firstName	<input type="button" value="Copy"/>
lastName	<input type="button" value="Copy"/>
email	<input type="button" value="Copy"/>

### IDP Server SAML Settings

GENERAL

Single sign on URL:

Use this for Recipient URL and Destination URL:

Allow this app to request other SSO URLs:

Audience URI (SP Entity ID):

Default RelayState:

Name ID format:

Application username:

ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Value
firstName	Unspecified	user.firstName
lastName	Unspecified	user.lastName
email	Unspecified	user.email

Copy from Connect+ and configure in IDP Server

Copy Attribute Keys from Connect+ to IDP Server



Field	Validation	Notes
SSO Enabled	Required	Check the property to enable the Single Sign-on.
SP Entity ID	Required	The Service Provider's (Connect+) Entity ID, which is a readonly field. Admin should copy this value to the IDP's App metadata configuration page in admin console. For example, <a href="http://www.customerdomain.com/emerson">http://www.customerdomain.com/emerson</a>
ASC (Consumer) URL	Required	The Service Provider's (Connect+) Consumer URL, which is a read-only field. Admin should copy this value to the IDP's App metadata configuration page in admin console. For example, <a href="http://www.customerdomain.com/emerson/consumer">http://www.customerdomain.com/emerson/consumer</a>
IDP Name	Required	IDP name. For example, Okta, salesforce, etc.
IDP Entity ID	Required	IDP Entity ID value, it is provided by IDP.
SAML SSO Login URL	Required	Single sign on service URL, it is provided by IDP.
X.509 Certificate	Required	The public key certificate provided by IDP.
Attribute Keys	Optional	In your IDP server, you need to add three Attribute Key: first name, last name and email. The added key should be same as the Connect+ provided. You can copy the properties and paste them to your IDP server. If you configure them, Connect+ can retrieve the first name, last name and email for your IDP account.

### 9.2.2 Login with Single Sign-on

The company user can now log into the Connect+ with the company credential.

In the login page, you will see a **Login** with XXX (XXX is the IDP Name which is configured in SSO configuration) button.

Click **Login** with XXX button to be redirected to company IDP Login page.

Input the company username and password then click the **Sign In** button. For the first time login, you will be redirected to the Connect+ user binding page after logging in to the company credential. The propose of this is to associate the Connect+ user with your company IDP user. After association, the existing Connect+ user's properties, like privilege, site permission, customized GS screen, will be assigned to the company IDP user.

Input Connect+ Login ID and Password, then click the **Login** button to log into the Connect+ successfully. If you do not have a Connect+ account, click the **Don't have a Connect+ Account?** link under **Login** button.

The Connect+ user will automatically create an account with your First Name, Last Name and Email which is configured in IDP Server. You can also modify your user profile after login. Click the **OK** button in the pop-up message to log into the Connect+.

### 9.2.3 Privilege of New User Login with Single Sign-on

There is a default group for Basic SSO Group defined in the Connect+. This group will be assigned to the new Connect+ user by default which is automatically created for the IDP user.

The group has been assigned with some basic privileges and there is no Site permission assigned.

Administrator needs to assign the site permission for the group, or the new user will not see any site after login.

Administrator can modify the privilege or assign the user to another group.

### 9.2.4 Auto-binding SSO User Account with Connerct+ User

If your SSO username is in email format or the SSO user email is configured in IDP server, the user binding indicated in 9.2.2 will be skipped. Connect+ could do the auto-binding through the unique email address.

To achieve auto-binding, you must make sure your SSO account username is in email format, or the primary email is configured.

Then, configure the IDP username format as an email address on the IDP server.

SAML Settings		Edit
GENERAL		
Single Sign On URL	http://sampleonly123.emerson.org/emerson/ssoConsumer.d	o
Recipient URL	http://sampleonly123.emerson.org/emerson/ssoConsumer.d	o
Destination URL	http://sampleonly123.emerson.org/emerson/ssoConsumer.d	o
Audience Restriction	http://sampleonly123.emerson.org/emerson	
Default Relay State		
Name ID Format	Email Address	
Response	Signed	
Assertion Signature	Signed	

User Name  
username@emerson.com

Reset Password More Actions

User Active View Logs

Applications Groups Profile

#### Attributes

Username	username@emerson.com
login	
First name	User First Name
firstName	
Last name	User Last Name
lastName	
Middle name	
middleName	
Honorific prefix	
honorificPrefix	
Honorific suffix	
honorificSuffix	
Primary email	username@emerson.com
email	

#### Profile

A profile is a collection of attributes that describe a user in Okta. Some apps and directories can sync attributes with Okta.

User Name  
username@emerson.com

Reset Password More Actions

User Active View Logs

Applications Groups Profile

#### Attributes

Username	username@emerson.com
login	
First name	User First Name
firstName	
Last name	User Last Name
lastName	
Middle name	
middleName	
Honorific prefix	
honorificPrefix	
Honorific suffix	
honorificSuffix	
Primary email	username@emerson.com
email	

#### Profile

A profile is a collection of attributes that describe a user in Okta. Some apps and directories can sync attributes with Okta.

## 10 Configure Energy Analysis Report

To enable the **Energy Analysis** report, log into Connect+ using superuser credentials.

Go to Top Menu > **Super user** > **Properties Editor**, configure Domo client ID, Domo security and customer name.

Category	Key	Value
	domo	
Reporting	Domo.credential.clientID	f27439c1-ee49-46d4-8d2c-c632f0fbdd17
Reporting	Domo.credential.clientSec	
Reporting	Domo.credential.customer	FOODSERVICE
Reporting	Domo.message.Unauthorized	Wrong Client ID or Client Secrete.
Reporting	Domo.template.request	{"sessionLength":1440,"authorizations":[{"token":"%ReportPath%"}]}
Reporting	Domo.template.response	<html><body><form id="form" action="%Report_Path%" rname="embedToken" value="%Embed_Token%" /></form></script></body></html>
Reporting	Domo.uri.accessToken	https://api.domo.com/oauth/token?grant_type=client_crede
Reporting	Domo.uri.embedToken	https://api.domo.com/v1/stories/embed/auth
Reporting	Domo.uri.report	https://public.domo.com/embed/

Then go to Top Menu > **Reporting** > **Reporting Manager**. You will see **Energy Analysis Report for Directory** and **Energy Analysis Report for Site** listed in the table.

Report Name	Last Updated	Description	Tree Level	Enabled
Advisory Analysis		Advisory Analysis	Directory	True
Energy Analysis Report for Directory		Energy Analysis Report (Directory) from Domo	Directory	False
Energy Analysis Report for Site		Energy Analysis Report (Site) from Domo	Site	False

Edit these two reports by double clicking the report name. Enable the report by checking the Enable check-box from the **General Information** tab.

Switch to **Report Template** tab, and configure the External Report URL. Energy reports are displayed on the right-click menu.

Reporting Configuration	
General Information	Report Template
Report Name	Energy Analysis Report for Directory
Description	Energy Analysis Report (Directory) from Domo
Basic Report	<input checked="" type="checkbox"/> (Check this box if report does not utilize a Report Data Collection Job)
Enabled	<input checked="" type="checkbox"/> (If not checked, this report will not be included in the list of reports to run)

Reporting Configuration	
General Information	Report Template
Enable Upload Customized Template	<input type="checkbox"/>
Tree Level	Directory
Report Type	Domo
External Report URL	https://public.domo.com/embed/pages/M8VWQ

## Appendix A: Group Privileges, Descriptions, and Protocol Access Levels

Table A-1 contains the privileges that can be assigned to a Group from the Group Configuration page and their corresponding descriptions. A privilege is an activity that can be performed in Connect+.

Privilege	Description
My User Info	Users can change their password and set personal system settings.
My Pending Activities	Users can view activities that are waiting to start or in progress that have been initiated by the user.
My Pending Activities for Tree Item	Users can view activities from a tree node that are waiting to start or in progress that have been initiated by the user.
My Activity History	Users can view activities initiated by the user.
My Activity History for Tree Item	Users can view activities from a tree node that have been initiated by the user.
Admin Pending Activities	Users can view activities that are waiting to start or in progress that have been initiated by all users of the system.
Admin Pending Activities for Tree Item	Users can view activities from a tree node that are waiting to start or in progress that have been initiated by all users of the system.
Admin Activity History	Users can view activities initiated by all users.
Admin Activity History for Tree Item	Users can view activities from a tree node initiated by all users of the system.
Add User	Users can add users to the system.
Edit User	Users can edit users of the system.
Delete User	Users can delete users from the system.
Add Group	Users can add groups and assign privileges as well as set site and directory permissions for each group. Users may perform activities depending on what group type they are assigned to.
Edit Group	Users can edit groups by adding or removing privileges and change their site and directory permissions.
Delete Group	Users can delete existing groups.
Add Service Provider	Users can add service providers to the system.
Edit Service Provider	Users can edit service providers in the system.
Delete Service Provider	Users can delete service providers in the system.
Service Provider Properties	Users can view detailed information about service providers.
Add Scheduled Activities	Users can add scheduled activities to the system. Activities, such as backups, and retrieve logs can be scheduled to run based on a schedule set by the user. Users will be allowed to create user schedules and not system schedules.
View All Scheduled Activities	Users can view all configured scheduled activities created by all users of the system.
Edit My Scheduled Activities	Users can view and edit only scheduled activities they created.
Edit Any Scheduled Activities	Users can view and edit all scheduled activities that were created by all users of the system.
Delete My Scheduled Activities	Users can delete only scheduled activities they created.
Delete Any Scheduled Activities	Users can delete all scheduled activities that were created by all users of the system.
View Directory Properties	Users can view information that is related to a directory, including subdirectories, sites, activities, and configuration information.
Add Directory	Users can add directories to the system. Directories are the top-most level of the navigation tree.
Edit Directory	Users can edit existing directories in the system.
Delete Directory	Users can delete existing directories from the system. Deleting a directory will delete everything within the directory.
View Site Properties	Users can view information that is related to a site, including subdirectories, activities, and configuration information.
Add Email Group	Users can add email group.
Edit Email Group	Users can edit existing email group.
Delete Email Group	Users can delete existing email group.

Privilege	Description
Copy Email Group	Users can copy the existing email group.
Add Site	Users can add sites to the system. Sites are at the second level of the navigation tree.
Edit Site	Users can edit existing sites in the system.
Delete Site	Users can delete existing sites from the system.
View Control System Properties	Users can view information related to the control system including units, activities that can be performed, configurations and details.
Add Control System	Users can add control systems to the system. Control systems are at the third level of the navigation tree.
Edit Control System	Users can edit existing control systems in the system.
Delete Control System	Users can delete existing control system from the system.
View Unit Properties	Users can view information related to the unit including application, activities, configurations and details.
View Application Type Properties	Users can view details about the application and make changes to the application.
View Application Instance Properties	Users can view the number of points in the application (if available) that have been programmed inside a controller.
View Point Properties	Users can view details about controller points, graph points, retrieve logs, and make changes.
Display Log Graph	Users can view graphical representation of the data.
View Real-time Graph	Users can view real-time graph of the data.
Watch Points	Users can select multiple points from the tree and view the real-time values for those points.
GS Screen Edit	Users can modify graphical status screens.
GS Set Home Page	Users can set a graphical status screen as the first page they see when they log into the system.
Add GS Screen	Users can create graphical status screens.
Import GS Screen	Users can bring graphical status screens into the system that were created on another system or by another user of the system.
Copy & Paste GS Screen	Users can copy an existing graphical status screen and paste it to another tree node of same level.
Associate GS Screen	Users can connect a graphical status screen to a node on the tree.
Advisory Receiver Commissioning	Users can set advisory configurations such as connection test time and advisory filter priorities for alarms, failures, and notices.
Firmware Package Management	Users can manage firmware files.
View Advisories	Users can view historical advisories (alarms, fails, notices, warnings) from the database.
Acknowledge Live Advisories	Users can Acknowledge Live Advisories.
Clear Live Advisories	Users can Clear Live Advisories.
Reset Live Advisories	Users can Reset Live Advisories.
Mute Live Advisories	Users can Mute Live Advisories.
Forward Advisories	Users can forward advisories to email addresses and/or users in the system.
Connection Verification Report	Users can view inbound connections to determine which sites in the navigation tree are in good communication status and which sites are not.
Purge Inbound Connection Records	Users can set purge configurations for inbound connection records.
Feature Activation	Users can view the license page as well as add feature activation keys.
Help Contents	Users can view the system help including the help provided on each page.
Add Private List	Users can create a list of points that will only be visible to them.
Edit Private List	Users can edit a list of points only visible to them that they created.
Delete Private List	Users can delete a list of points that the user created.
Add Public List	Users can create a list of points that will be visible to all users of the system.
Edit Public List	Users can modify any public list of points that was created.
Delete Public List	Users can remove a list of points that was created and will no longer be visible to all users of the system.

Privilege	Description
View Setpoint Broadcast Activity History	Users can view Setpoint Broadcast activity History.
Admin SSO Manager	Users can configure and use Company account (Single Sign-on).
Revert Setpoint Broadcast	Users can revert the point value which already been broadcasted.
Activity History Configuration	Users can purge activity history in the database.
Admin Send Email	Send Email
View Enterprise Summary	Users can view your enterprise assets.
Manage Password Rule	Users can configure your password rule.
Export Setpoint File	Users can download Setpoint File from the controller.
View Audit Log	Users can view the audit log.
Obtain Controller Information	Retrieves all information possible for current level.
Backup	Back up one or more controllers at a given level.
Controller Logs and Stats	Retrieves log data for various diagnostic information types from the controller.
Terminal Mode	Shows the native UI for the current controller
Retrieve Logs	Retrieves Point Logs for current level requested.
Configure Advisory Purge	Users can choose to store a certain number of advisories in the system for the tree node selected.
Utility	Utility Group
Upload Description File	Users can send a Description File to a controller.
Remove Description File	Users can remove Description File from a controller.
Firmware Transfer	Transfer firmware to a set of controllers.
Restore	Restore setpoints to a controller.
Firmware Apply	Applies the Firmware to a controller.
Firmware Transfer	Transfer the firmware file to the a controller.
Add Application	Adds one or more applications to a controller.
Refresh Point List	Retrieves the listing of points for the current level.
Configure Unit Backup	Users can choose to store a certain number of backups in the system for the unit selected.
Edit Application Instance	Edit an application instance which will be saved on a controller.
Get Live Advisories	Users can use the retrieve advisories for the controller.
Manual Defrost	Users can start a defrost for a freezer or refrigerated case that is outside its normally scheduled routine.
Modify Point	Modifies a point value.
Override	Overrides a point value.
View Network Status	Users can view the connected devices of a controller.
Setpoint Broadcast	Broadcasts setpoint functionality.
Delete Application Instance	Users can delete an application instance from a controller.
Configure Log Purge	Users can configure purging for point logs.
Configure Advisory Snooze	Users can set a snooze duration for the selected node in the tree.

Table A-1



Table A-2, Table A-3 and Table A-4 list the privileges (activities) that can be assigned to a Group at the Group configuration level and the minimum Protocol Access Level required to run the activity.

Activity	Minimum Protocol Access Level needed to run this Activity
Watch Points	100
Export Setpoint File	300
Modify Point	300
Obtain Controller Information	100
Backup	200
Controller Logs and Stats	100
Terminal Mode	100
Retrieve Logs	100
Upload Description File	400
Remove Description File	400
Firmware Transfer	400
Restore	300
Override	300
Refresh Units	100
Refresh Applications	100
Firmware Apply	400
Add Application	300
Refresh Point List	100
Edit Application Instance	300
Get Live Advisories	100
Manual Defrost	400
Setpoint Broadcast	400
Delete Application Instance	300

Table A-2

Activity	Minimum Protocol Access Level needed to run this Activity
Watch Points	100
Export Setpoint File	100
Modify Point	100
Obtain Controller Information	100
Backup	100
Controller Logs and Stats	100
Terminal Mode	100
Retrieve Logs	100
Upload Description File	100
Remove Description File	100
Firmware Transfer	100
Restore	100
Override	100
Refresh Units	100
Refresh Applications	100
Firmware Apply	100
Add Application	100
Refresh Point List	100
Edit Application Instance	100
Get Live Advisories	100
Manual Defrost	100
Setpoint Broadcast	100
Delete Application Instance	100

Table A-3

Activity	Minimum Protocol Access Level needed to run this Activity
Watch Points	100
Retrieve Logs	100
Refresh Units	100
Refresh Applications	100
Refresh Point List	100
Terminal Mode (HttpSessionProxyActivity)	100

Table A-4

The contents of this publication are presented for informational purposes only and they are not to be construed as warranties or guarantees, express or implied, regarding the products or services described herein or their use or applicability. Emerson reserves the right to modify the designs or specifications of such products at any time without notice. Responsibility for proper selection, use and maintenance of any product remains solely with the purchaser and end-user.

[Climate.Emerson.com](https://Climate.Emerson.com)

026-1025 R2 | Emerson is a trademark of Emerson Electric Co. or one of its affiliated companies. ©2023 Emerson Digital Cold Chain, Inc. All rights reserved.

**EMERSON. CONSIDER IT SOLVED.™**