USER GUIDE

Connect+

Administrator User Guide

COPELAND

TABLE OF CONTENTS

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

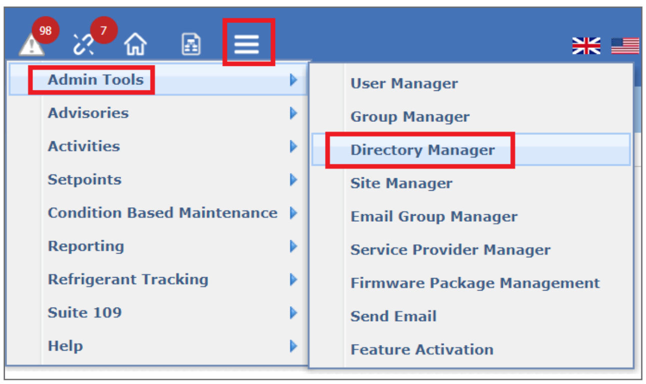
Application points are attributes that have been programmed inside a controller application. Access to application points allows the user to view details about the points, graph points, retrieve logs, and make changes. In Connect+ there are three categories of points. **Input, Output** or **Parameters**. 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

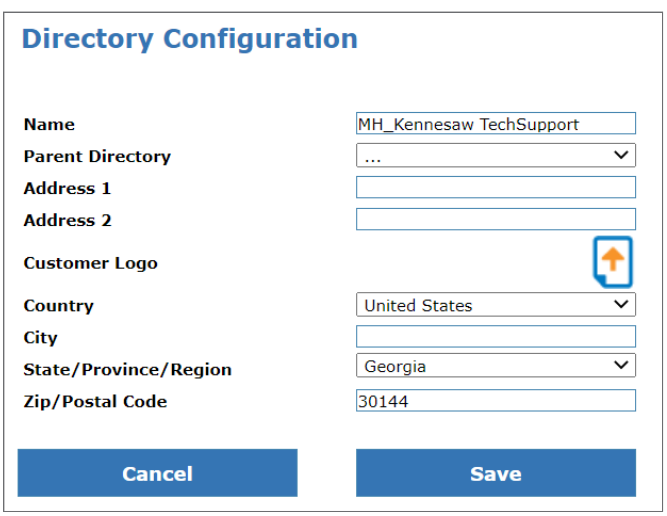
2.2.1 Add Parent Directory

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

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

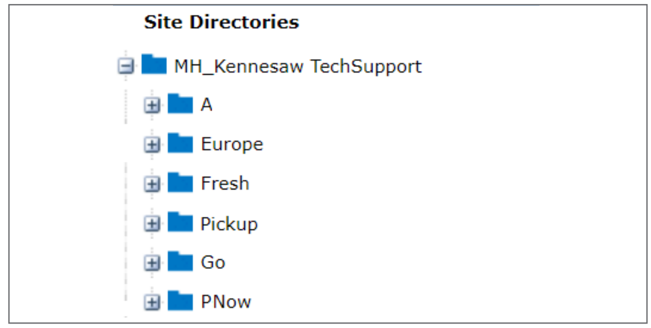


Then fill in the information for Admin organization's headquarters. Leave the parent directory blank, then this directory would be Admin root directory.



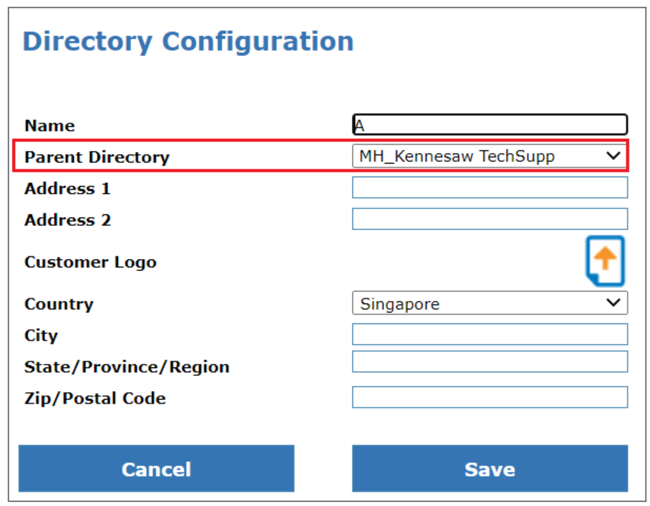
2.2.2 Add Subdirectory

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



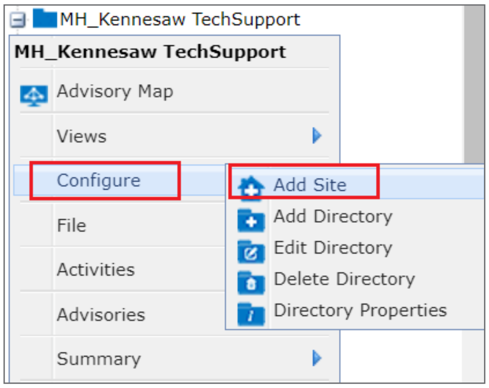
Fill in the subdirectory information and choose one parent directory to set up the correct hierarchy.

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.

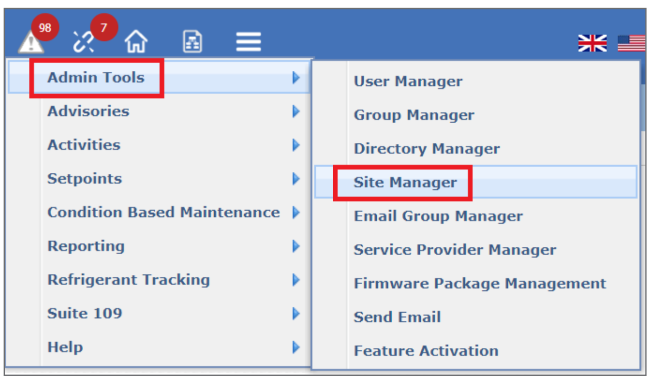


2.3 Adding Sites

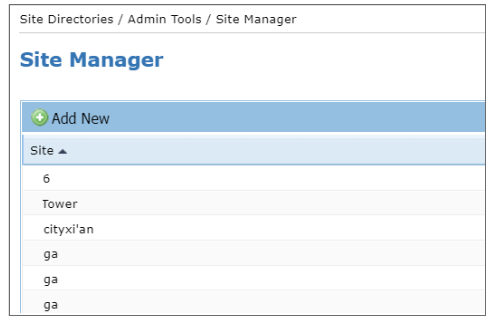
After setting up Directories, the Admin can add sites to each subdirectory by right clicking the **Configure** > **Add Site** menu on directory level.



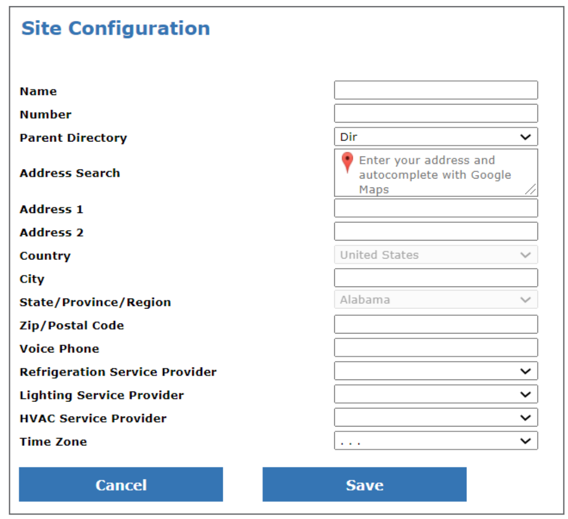
Or click **Top Menu** > **Admin Tools** > **Site Manager.**



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



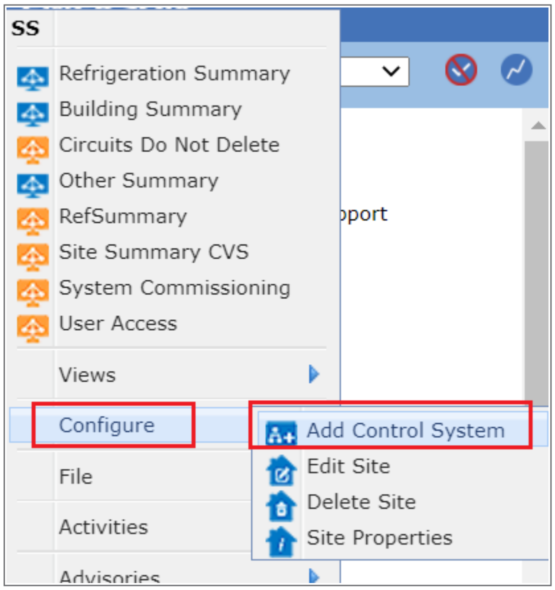
Fill the Site Information based on the field's explanation below:



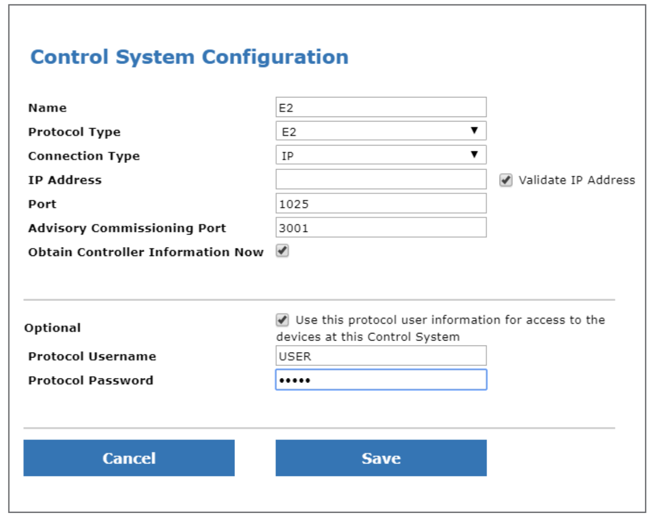
Field	Validation	Notes
Name	Required	Unique, limit 50 characters
Number	Optional	Site number
Parent Directory	Required	Select only one from the drop-down.
Address Search	Required	Administrators can configure Google Map Address Search in the superuser property. If it is configured, this field is required.
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. ***NOTE:*** *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 or *ColdChain.TechnicalServices@Copeland.com* for more information if needed.

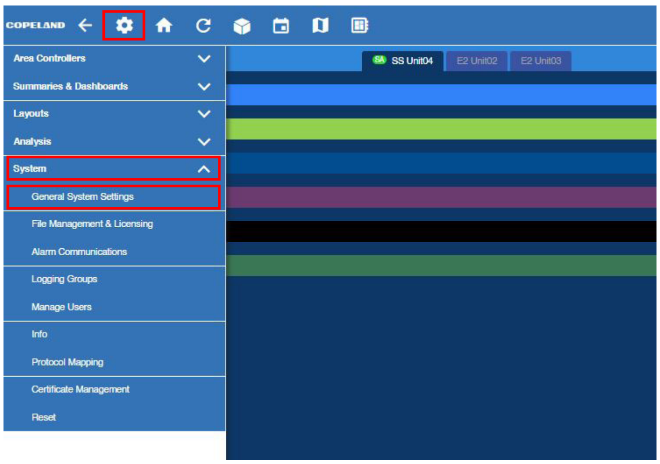


Field	Validation	Notes
Name	Required	Unique
Protocol Type	Required	E2, Site Supervisor, E3, XWEB, TAC, Danfoss, etc. The protocol type cannot be changed once the controller is connected.
Connection Type	Required	Use IP as the connection type. You can select HTTP or HTTPS connection according to your controller connection.
IP Address	Required	Controller IP address to which Connect+ can connect.
Validate IP Address	Optional	If this checkbox 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 check it on the device. (refer to *"2.4.1 Configuring the Site Supervisor/E3 and E2 to Communicate with Connect+ Mixed Sites"*).
Advisory Commissioning Port	Required	The port used for receiving advisories after commissioning is complete. (refer to *"2.4.1 Configuring the Site Supervisor/E3 and E2 to Communicate with Connect+ Mixed Sites"*).
Obtain Controller Information Now	Optional	The checkbox appears only when adding a new control system (not available on Edit Control System). If this checkbox 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 checkbox is enabled at the control system level, Connect+ will use **Protocol Username** and **Protocol Password** entered on this page and bypass the information at the Group level for only the units located under this control system. Normally, security settings for Connect+ are defaulted at the Group Configuration level.

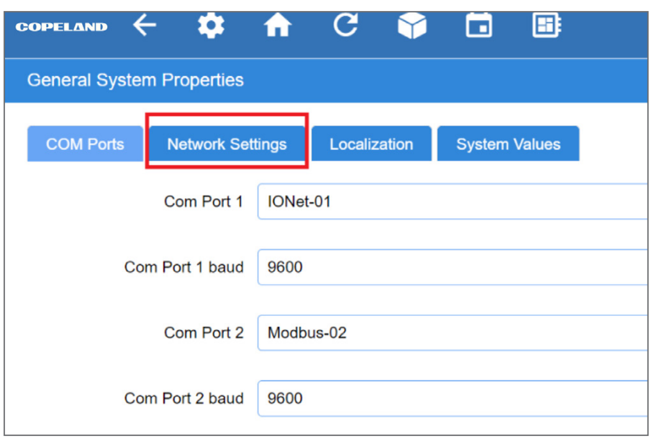
2.4.1 Configuring the Site Supervisor/E3 and E2 to Communicate with Connect+ Mixed Sites

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.

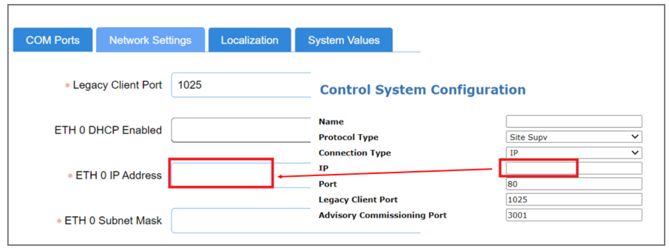


2. At the Network Configuration screen, click the **Network Settings** tab to access the TCP/IP settings of the controller.

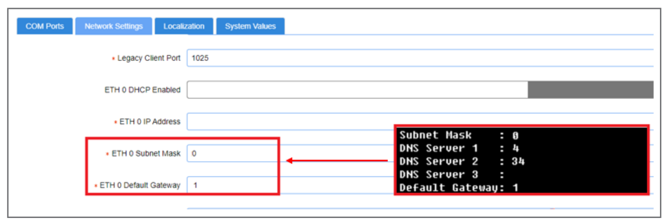


3. Click the **Advanced** options button on the upper right corner of the screen. This will enable Advanced options.

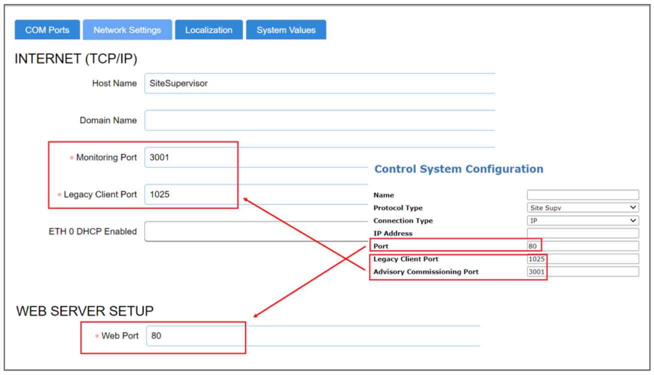
4. The IP address for ETH 0 should be the same IP address used in the control system settings of Connect+. The Site Supervisor or E3 should be the gateway controller in this setup. Contact *ColdChain.TechnicalServices@Copeland.com* to obtain the gateway IP address to be used.



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.

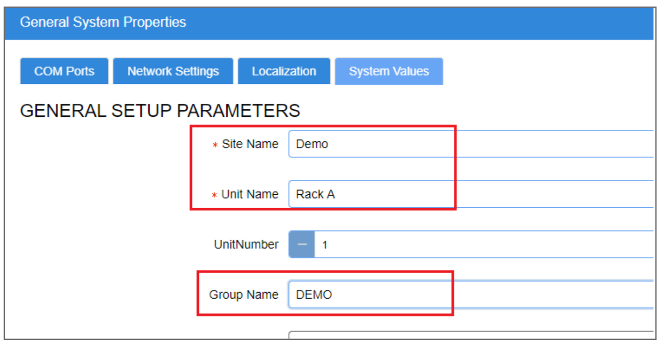


6. Configure the following additional settings values.
   a. **Monitoring Port** - The Monitoring Port is used for alarm dial-outs to remote monitoring. If using Copeland Monitoring with TCP/IP alarm dial-out, DO NOT change this port number without contacting Copeland Monitoring first. Changing this port without authorization will result in loss of communication with Monitoring.
   b. **Legacy Client Port**
   c. **Web Port** - The Web Port is the port number used by controller's Web Services feature. The default port number, 80, is the industry standard port number for web servers and should be used in most cases. If this port is a number other than the default 80, most browsers will require you to include the port number in the controller's web address, separated from the IP address by a colon. For example, if the IP address is 10.10.64.196 and the Web Port field is 8080, to access this controller via Web Services you would have to enter http://10.10.64.196:8080 in the browser's Address field.

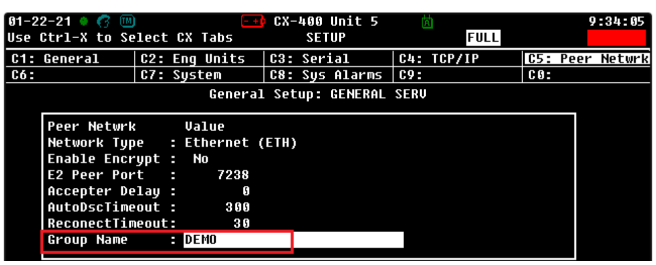


NOTE: In general, the default Monitoring port is 3001. If your Site Supervisor/E3 firmware version is 2.25F01, the default Monitoring Port is set to 0. It MUST be changed to 3001 (recommended) or other than 0 to make sure the connection is available.

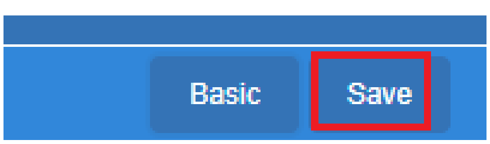
4. Click the **System Values** tab. Configure the Site Name and Unit, then edit the Group Name to match the existing E2 controllers on site.



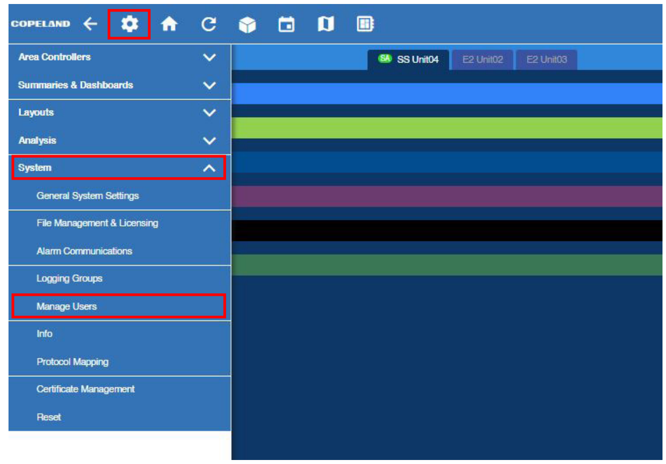
To view the Group Name of the existing E2 controllers on site, press Menu > 7 > 3 > 1 from the Home screen. Press F2 four (4) times to go to the **Peer Network** tab.



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

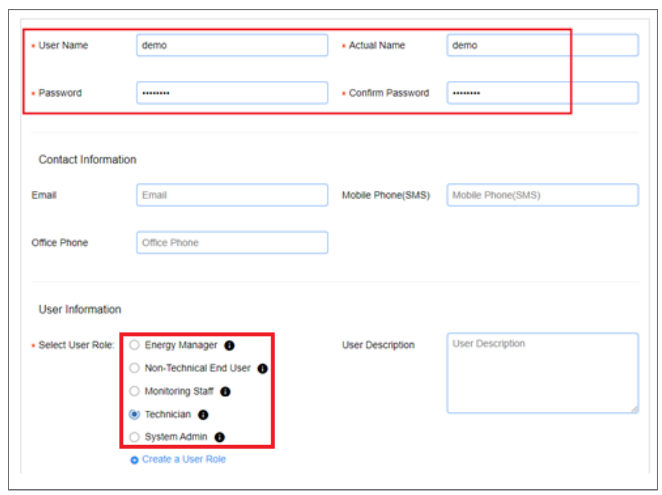


6. The user credentials of both Site Supervisor/E3 and E2 must be modified to accommodate the login protocol of Connect+. To create a new user on the Site Supervisor/E3, click on the **Main Menu** icon, expand **Configure System** and **Manage Users**.

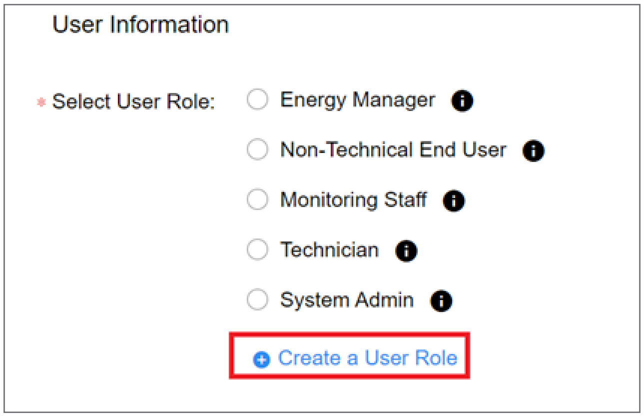


7. Click the **Create a User** button. A window will appear where **Username** and **Password** information can be entered. Both username and password are case sensitive.

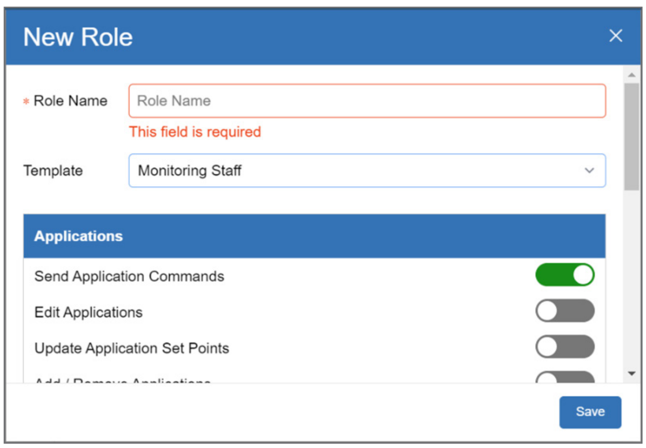
Choose the user role for the user account created.



You can create a new user role by clicking **Create a User Role.**



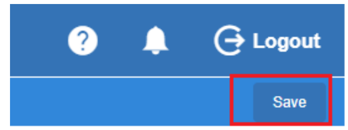
Add a Role name and assign the privileges to this role.



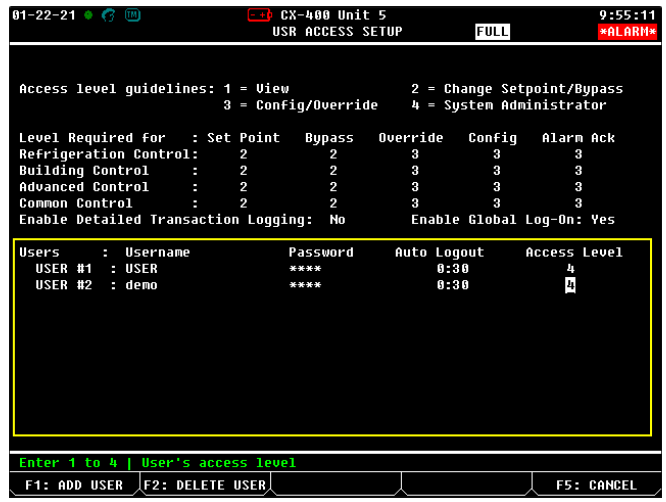
Some of Connect+ functions not only need the controller credential, but also needs both Site Supervisor/E3 privileges assigned.

Connect+ Permission	SS/E3 Permission
Add Application	Add/Remove Applications
Delete Application	Add/Remove Applications
Override	Override Application Setting
Modify	Override Application Setting
Manual Defrost	Send Application Command
Edit Application Instance	Edit Application
Setpoint Broadcast	Edit Application
Mute Live Advisories	Mute Alarms
Reset Live Advisories	Reset Alarms
Acknowledge Live Advisories	Acknowledge Alarms

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

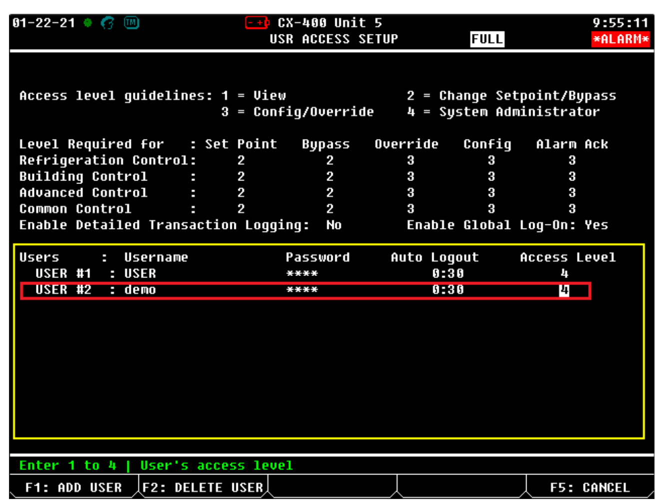


8. On the existing E2 controllers on site, additional user credentials must be setup. To do this, press Menu > 7 > 3 > 3 from the Home screen. This will take you to the **User Access Level** screen.

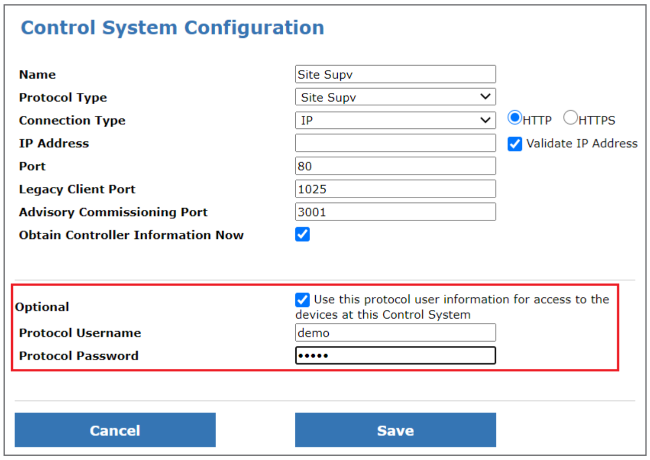


Press the down arrow button until you are in the User List section. Press F1 to add a new User. Enter the following information for the **Username** and **Password,** then set the Access Level to 4. Press the button to save. The E2 account will be bypassed if the gateway is Site Supervisor/E3, so this newly added account will not be used in the connection of the E2 in this group, but it might be used when you view the terminal mode.

NOTE: Perform the above steps prior to upgrading the Firmware version of the E2.



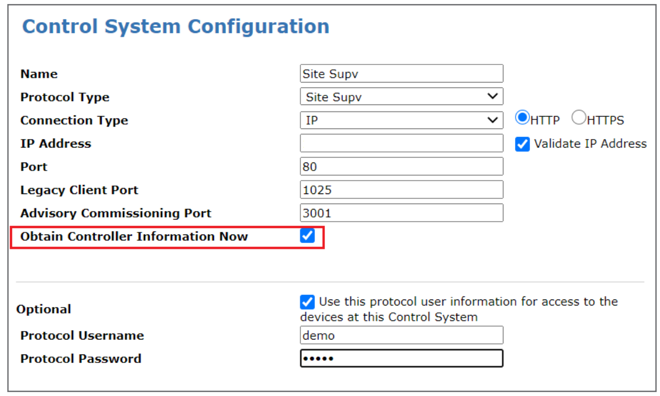
9. The login credentials of the control system must be updated with the correct username and password used. If your gateway credential is different from the credential that configured in Group Manager, make sure the “Use this protocol user information” checkbox is enabled and enter the username and password of the gateway.



10. Add the basic information of the gateway.

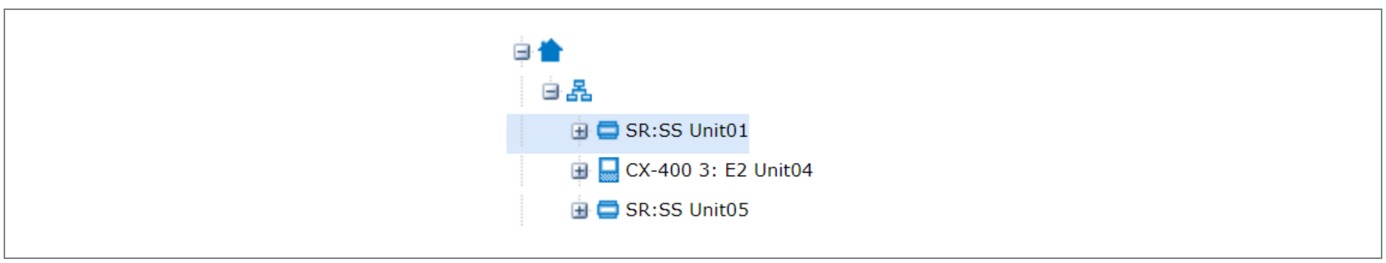
11. Ensure that the E2 controllers on site are running upgraded to use the 4.09F01 firmware. If an earlier version of the firmware is being used, the controller on site must be upgraded to the later Firmware.

12. Obtain Controller Information Now is checked by default. Click the Save button after the configuration is done. Obtain Controller Information will be run automatically.

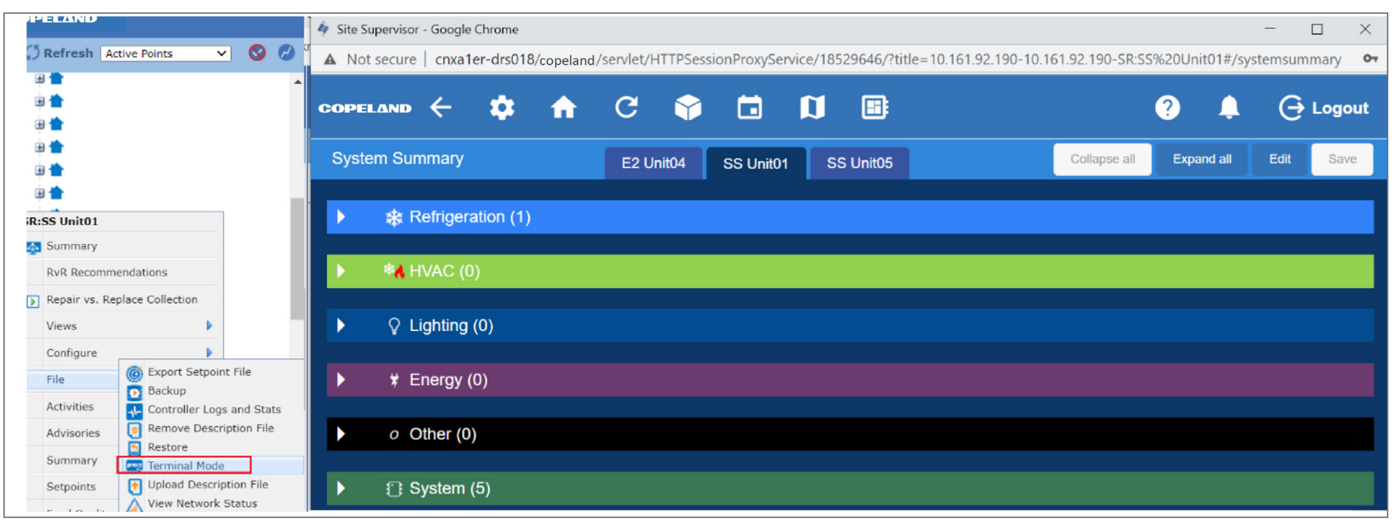


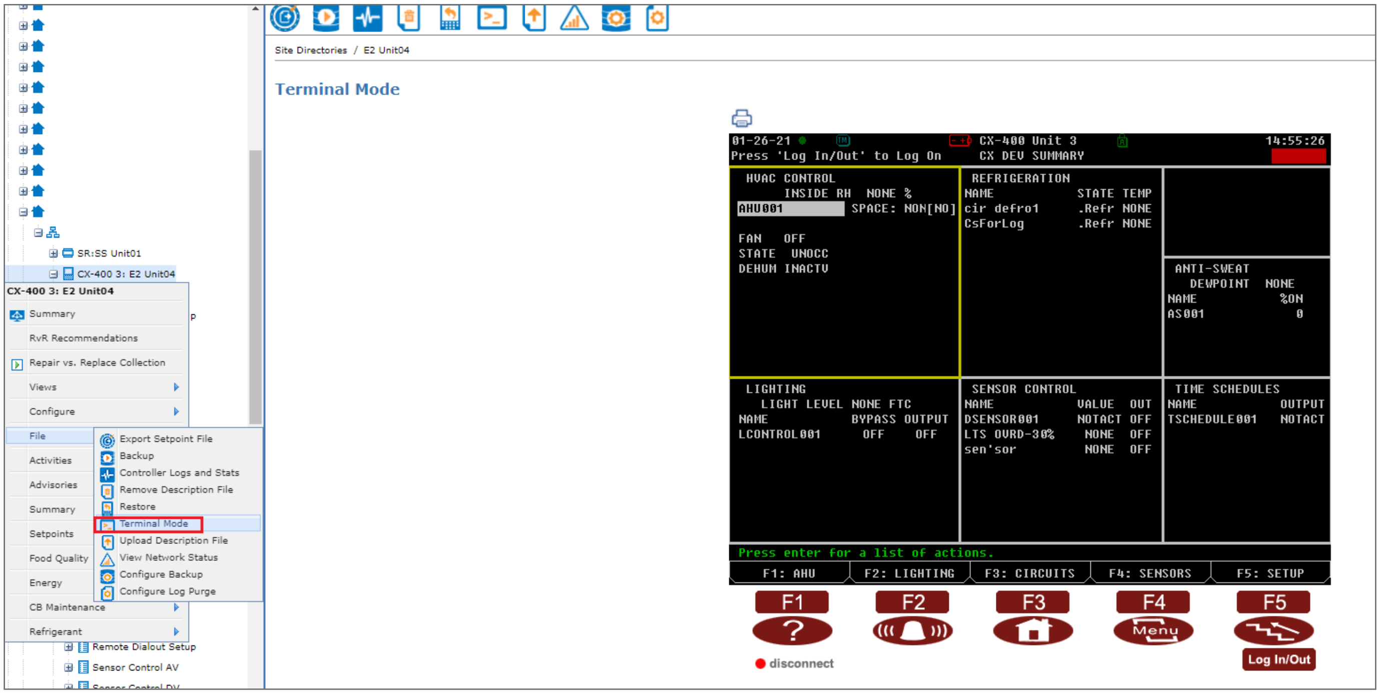
A. Verify Control System Connection

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



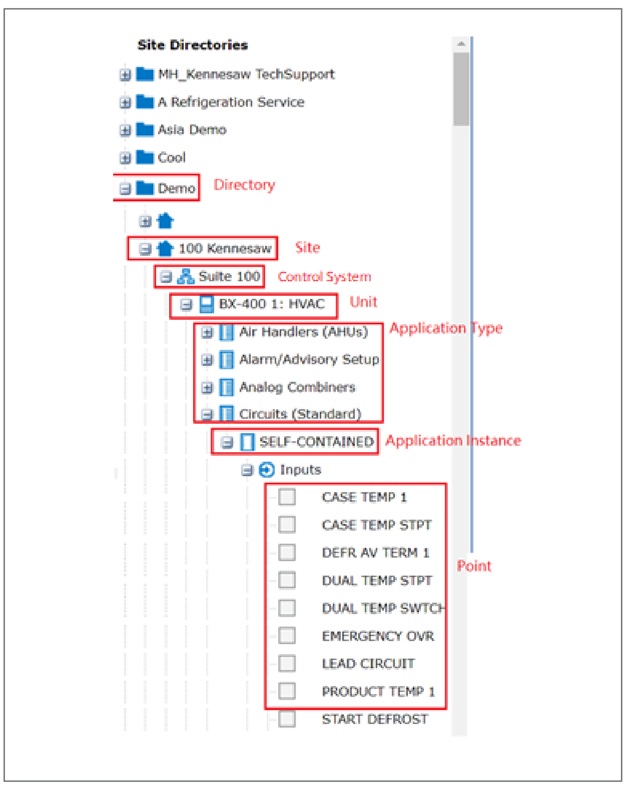
Usually, you can validate the Controller Connection by accessing the **File** > **Terminal Mode** from the right-click menu of the Site Supervisor, E3 or E2 once Obtain Controller Information is successful.



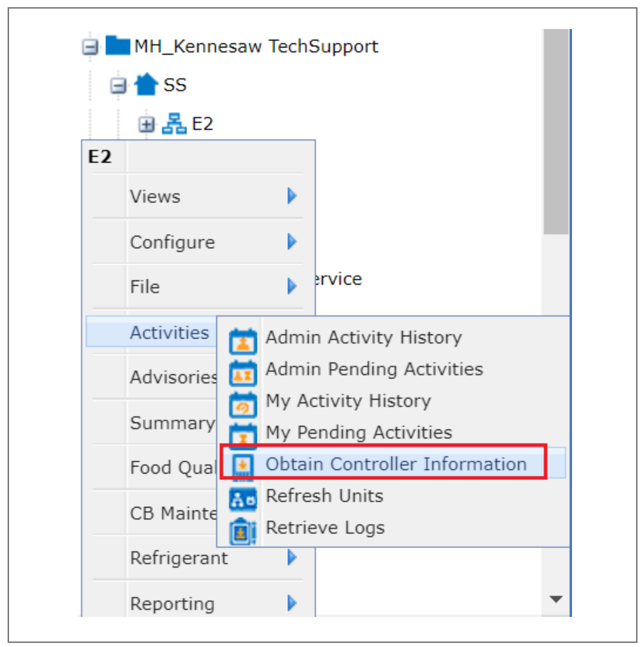


B. Verify Tree Structure and Enterprise Summary

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



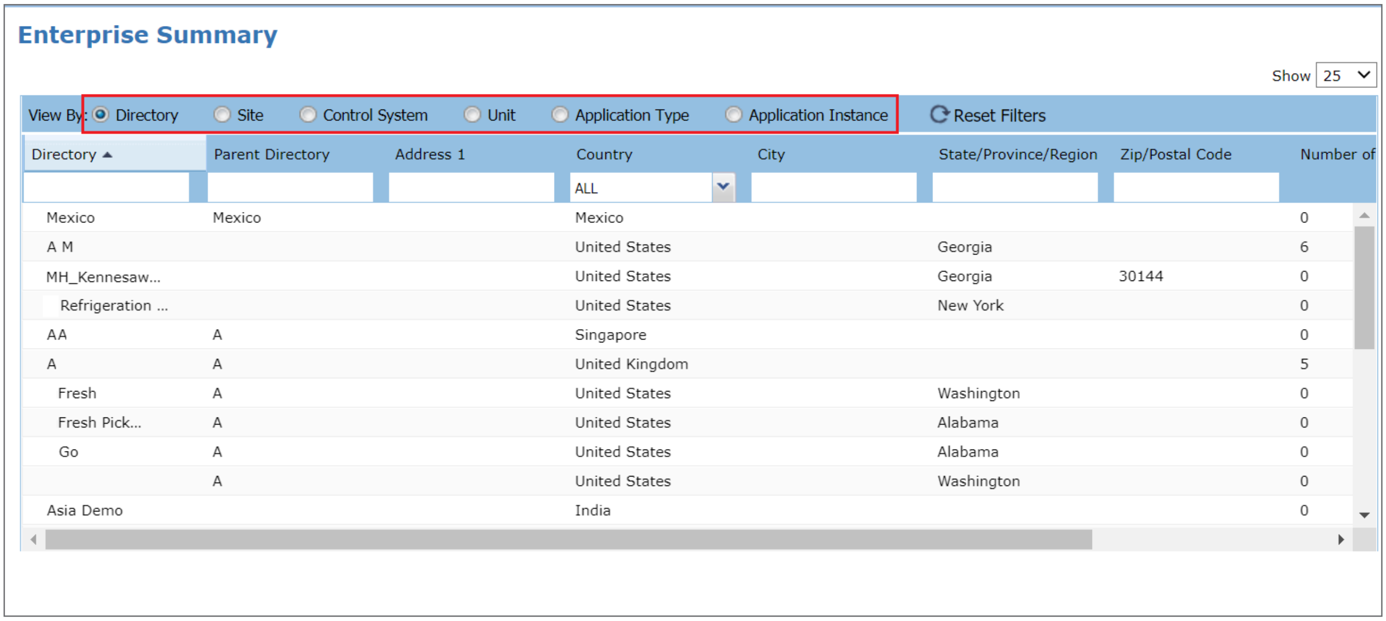
If you cannot drill down to show the tree structure, you can select **Activities** > **Obtain Controller Information** from right-click menu of directory, site, or control system level.



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.



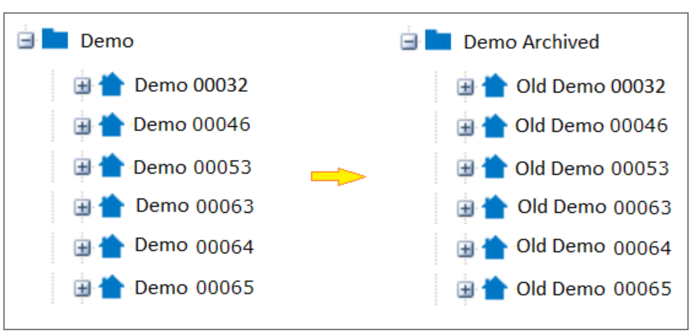
2.4.2 Replace the Controller with New Protocol

As business needs and products are updated, sometimes you need to replace your old device with a new one. Follow the below steps to replace the controllers.

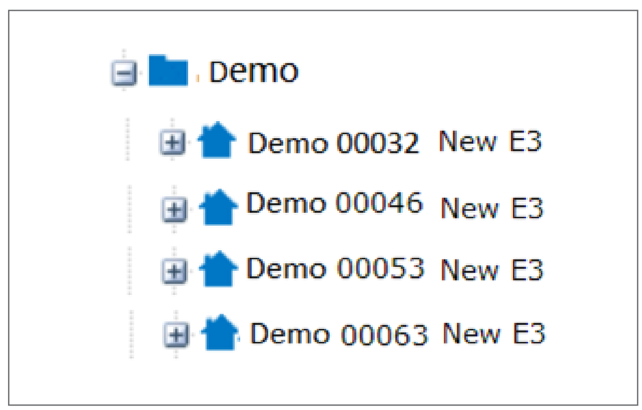
1. Archive your existing data.

   The protocol type in Connect+ cannot be changed once the controller data has been retrieved. Therefore, you cannot directly replace an existing controller with a new protocol device. For example, replacing the E2 with E3.

   Change the existing directory and site names that you want to replace as archives. The existing data will not be lost and can be used for later review.

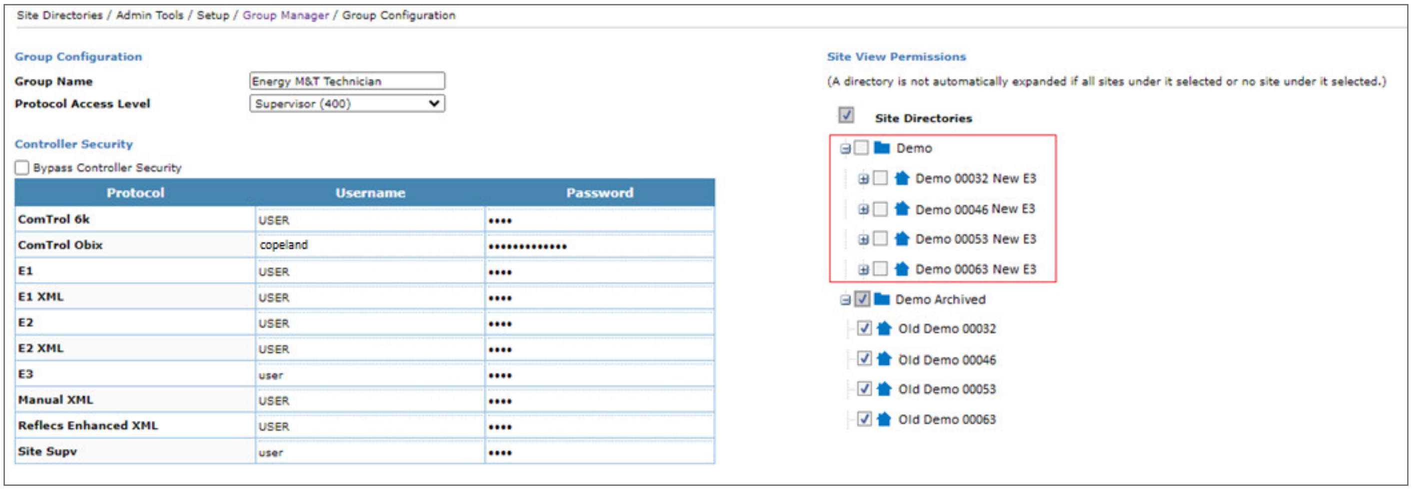


2. Create a new directory/site for the new connection. Using a similar name with the archived directory/site is recommended.



3. Choose the new protocol when adding a control system (refer to Section *"2.4 Add Control System and Obtain Controller Information"*). If you are connected to a group consisting of E2's and Site Supervisors or E3's, then one of the Site Supervisors or E3's should be the gateway.

4. Add the newly created directory/site to the existing group.

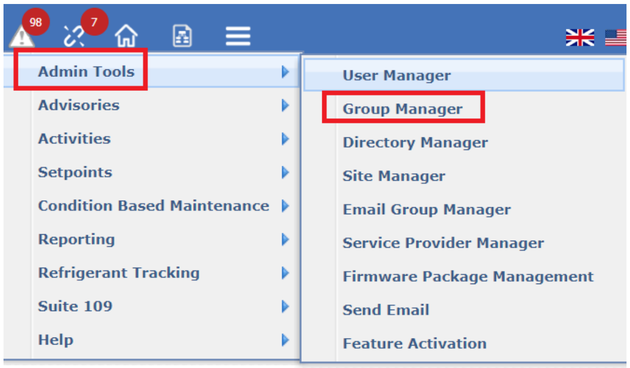


3. Onboard Users

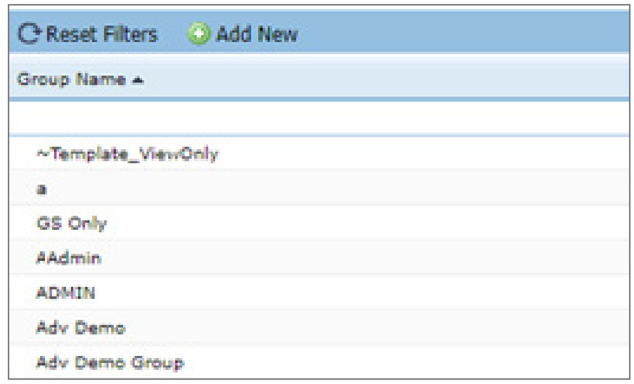
3.1 Create User Group to define Privilege and Sites Access

After you create the user on controllers, you need to add the credentials in Connect+ to make it connect.

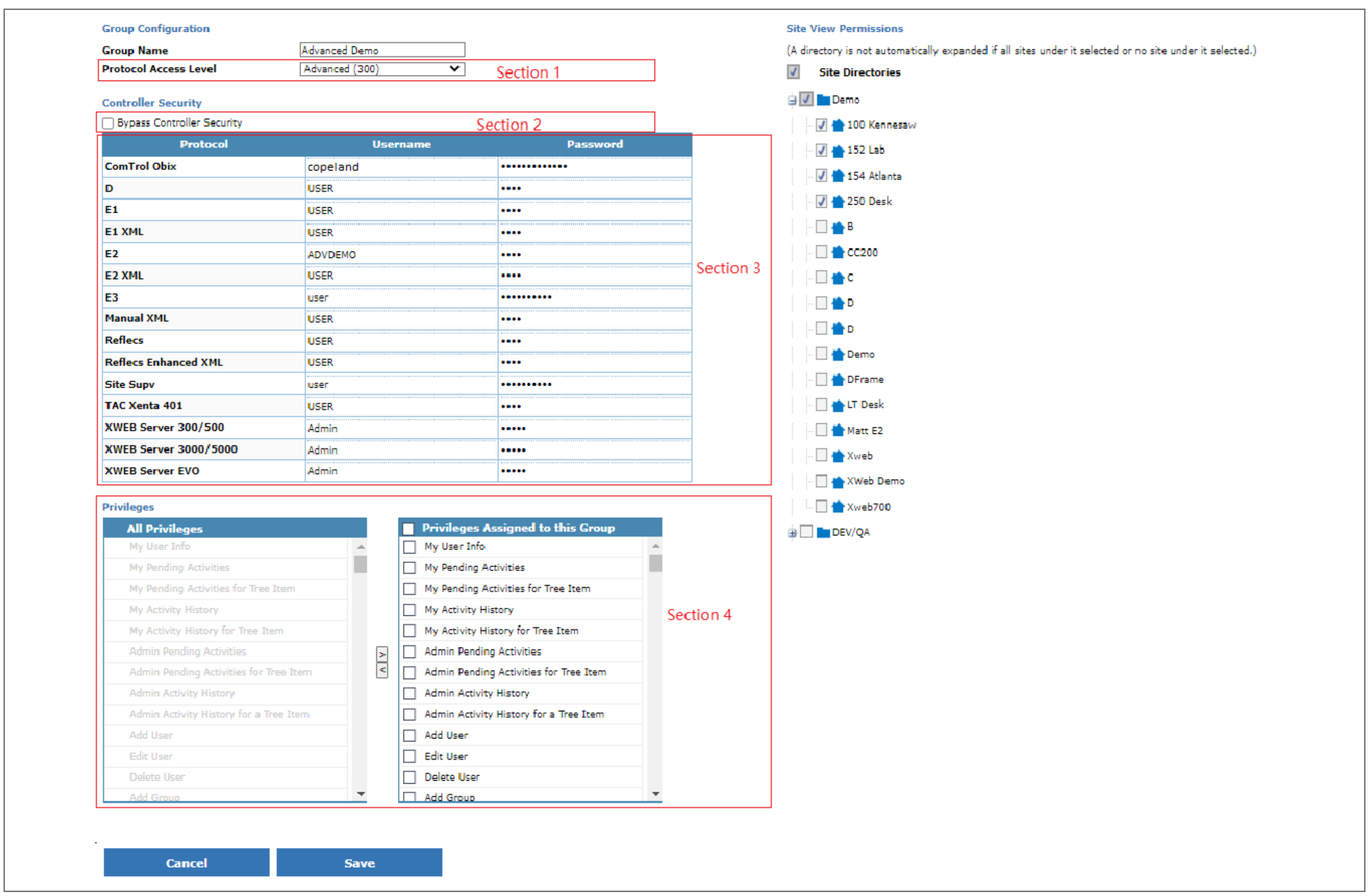
Connect+ manage user privilege and site access and controller credential by Group Manager. You can access to Group Manager by clicking **Top Menu** > **Admin Tools** > **Group Manager**.



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:



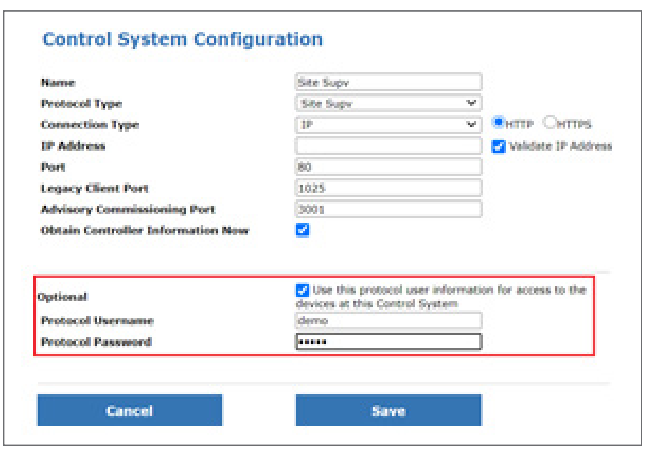
All privileges can be added or subtracted for a user at the admin level on this page. To add or subtract privileges for a user, highlight the privilege in the left column and click the left and right arrows. The right arrow on the top will assign privileges, the left or bottom arrow will unassigned the 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 (***<u>Recommended</u>***). 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.



2. The PAL selected for the Group is the "Connect+ Group's Protocol Access Level." (Section 1 of the image) Special rules apply to determine how the menus will behave. (refer to *"Appendix A: Group Privileges, Descriptions, and Protocol Access Levels"* Table 2 – Table 4)

3. You need to enter the protocol credentials in the Controller Security part (Section 3 of the image). All of your controllers will be connected using the credentials configured in this place.

   If some of your specific controller credentials are different from this configuration, you can add the individual credentials in the control system configuration. Usually, the initial Site Supervisor and E3 credentials will be configured as user/supervisor (case Sensitive), you need to manually configure it.

4. If you want to bypass the E2 credential, you can check the **Bypass Controller Security** check-box (Section 1 of the image). After this checkbox is checked, the protocol credential table (Section 3 of the image) will be hidden. You still need to add your Site Supervisor/E3 credentials from the control system configuration.

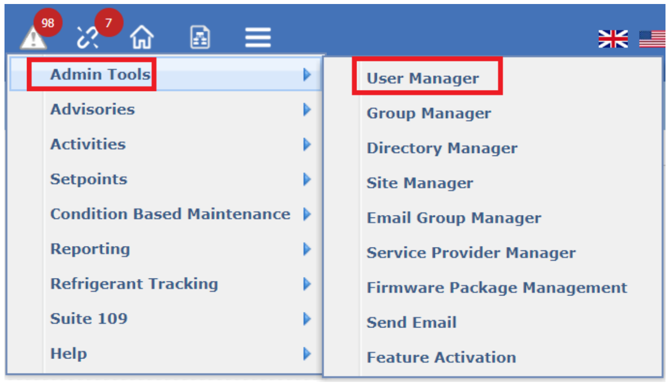
NOTE: The bypass Controller Security option is only available for E2.

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.

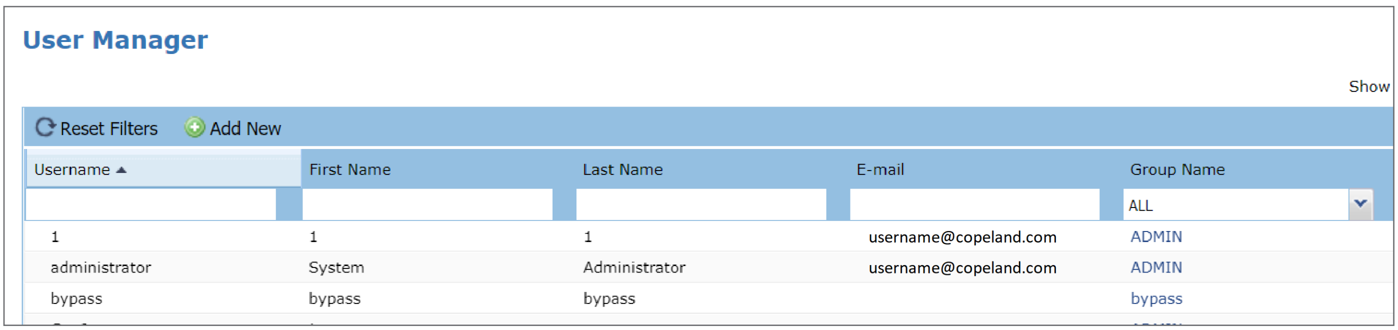
Site View Permissions: you can assign permissions (which directories and sites) to each Group by enabling the checkboxes next to them.

3.2 Create User

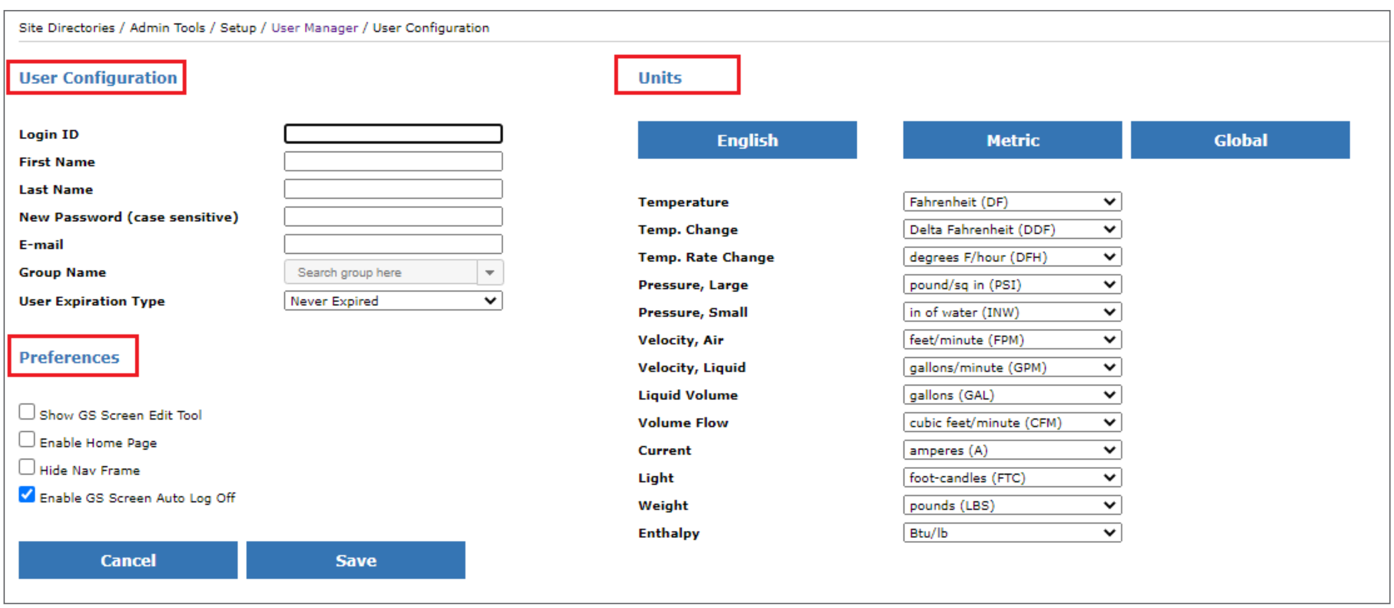
You can access to User Manager by clicking **Top Menu** > **Admin Tools** > **User Manager.**



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



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



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"

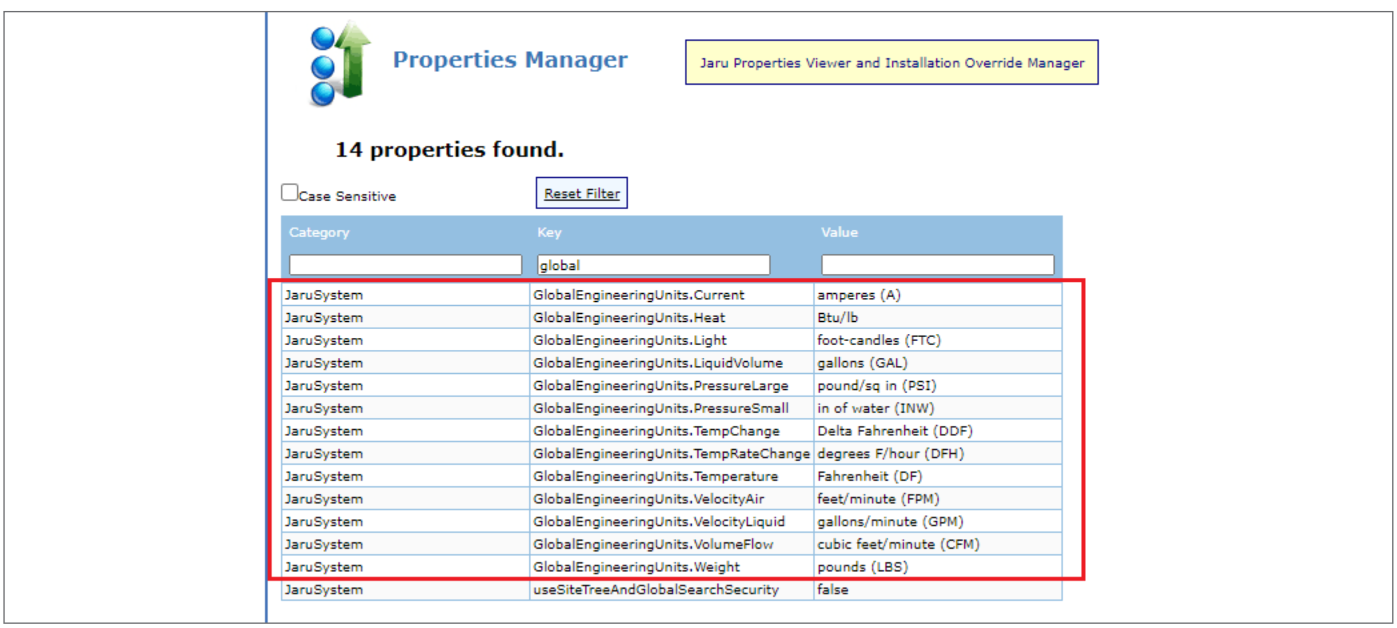
Preferences: Check the checkbox to enable the convenience features.

- **Show GS Screen Edit Tool:** If this checkbox 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 checkbox 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 checkbox 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.



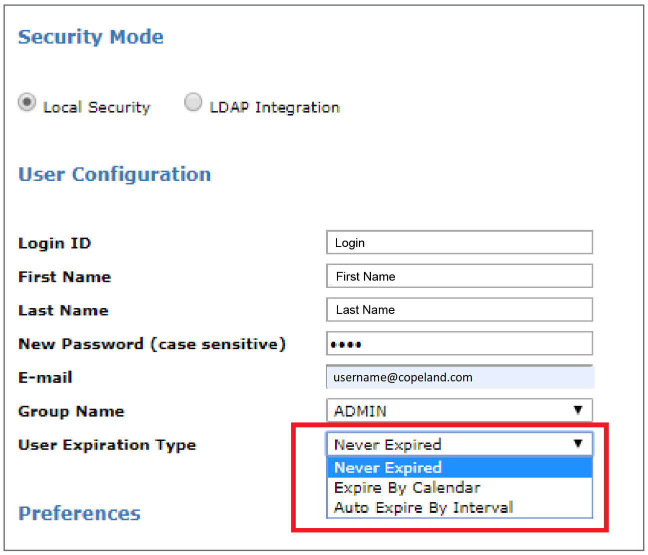
Category	Key	Value
JaruSystem	GlobalEngineeringUnits.Current	amperes (A)
JaruSystem	GlobalEngineeringUnits.Heat	Btu/lb
JaruSystem	GlobalEngineeringUnits.Light	foot-candles (FTC)
JaruSystem	GlobalEngineeringUnits.LiquidVolume	gallons (GAL)
JaruSystem	GlobalEngineeringUnits.PressureLarge	pound/sq in (PSI)
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.

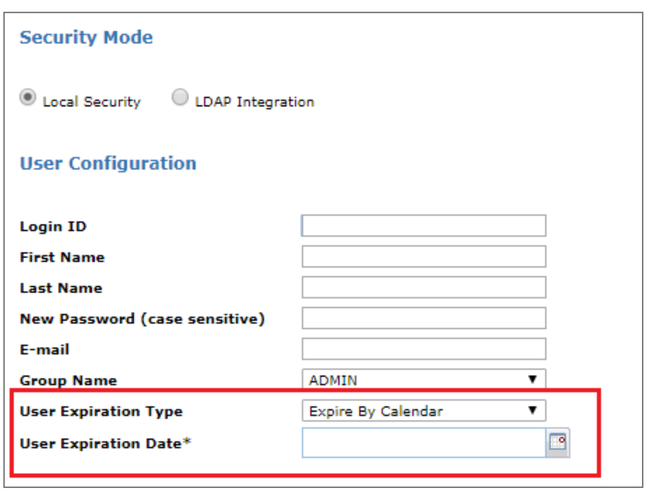
3.3.1 Configure User Expiration Type

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

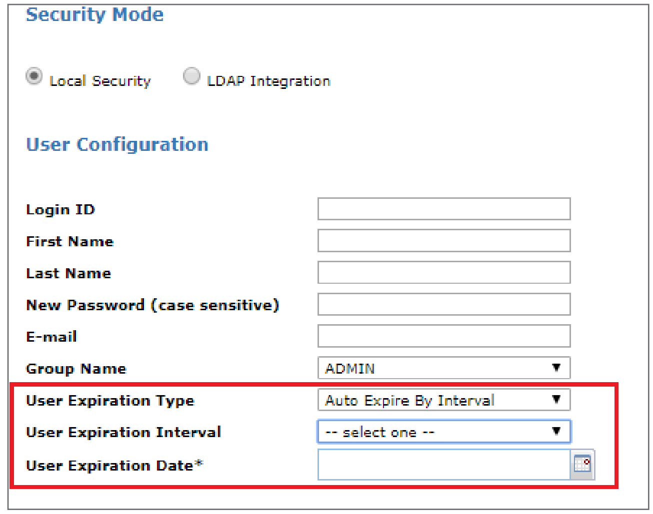


There are three kinds of user expiration types:

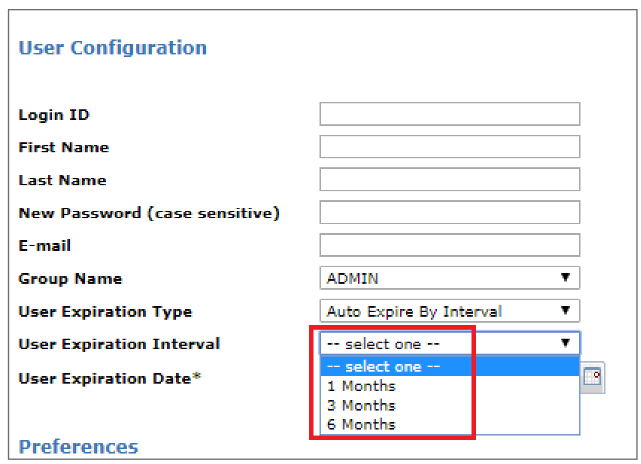
- **Never Expired:** User account will never expire.
- **Expire By Calendar:** User account will be expire at expiration date. **User Expiration Date** is required when selecting expiration calendar.



- **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.
  User Expiration Interval including 1 month,

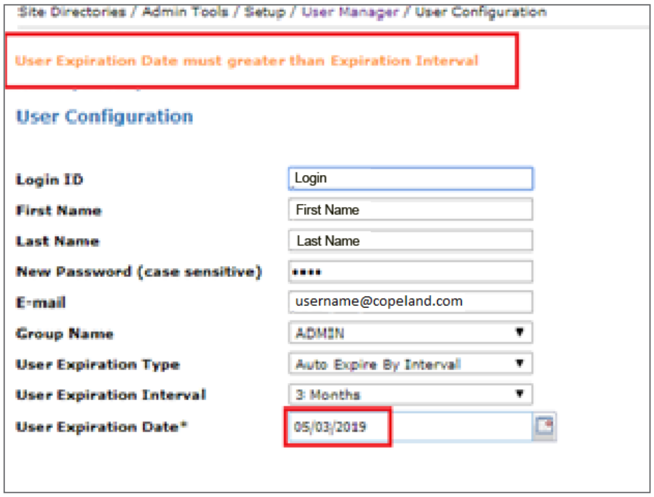


3 months, 6 months
The User Expiration Date should be greater than the



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.



Example of Auto Expire By Interval:

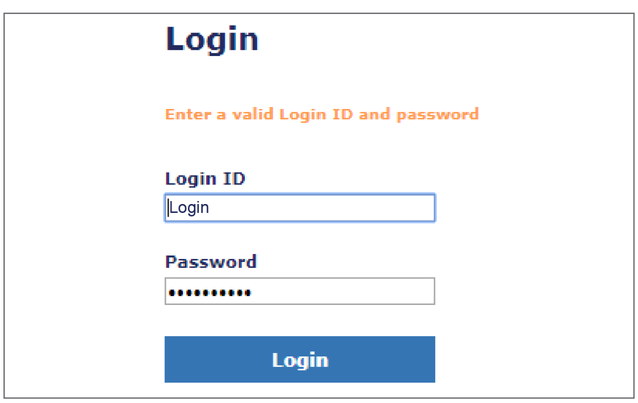
If a user is configured to use Auto Expire By Interval at 2019/4/15, and the User Expiration Interval is configured as 1 month, the User Expiration Date is 2019/9/20.

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.



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.

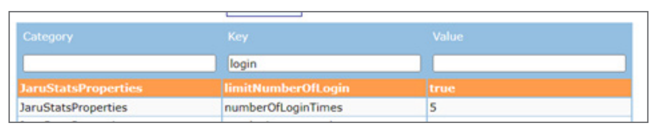
2. If the **User Expiration Date** is not in the system yet, the expired account will prevent the user from logging into the instance during the **User Expiration Interval**. In this case, the administrator must verify if the account needs to be re-activated because the user has not logged into Connect+ 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.

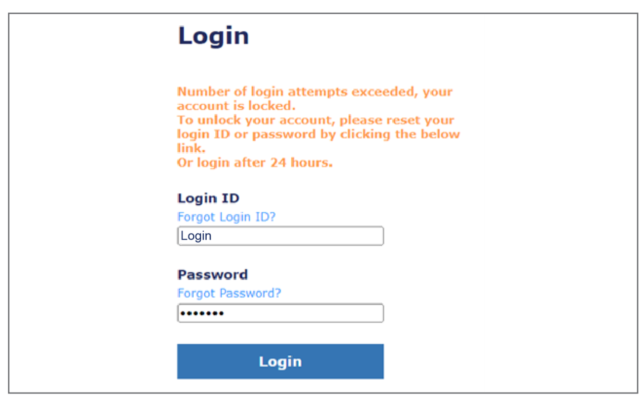
3.4 User Lockout

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.



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.



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

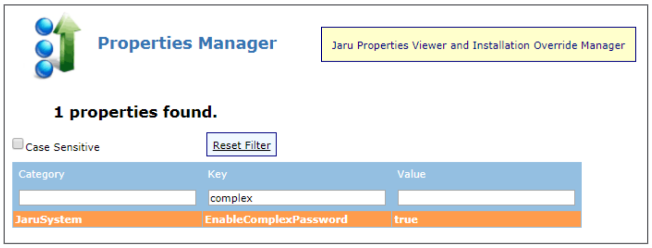
When user click the link, system will send a temporary password to the user's email address to log into the Connect+ with this temporary password and reset it.

4. Complex Password

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

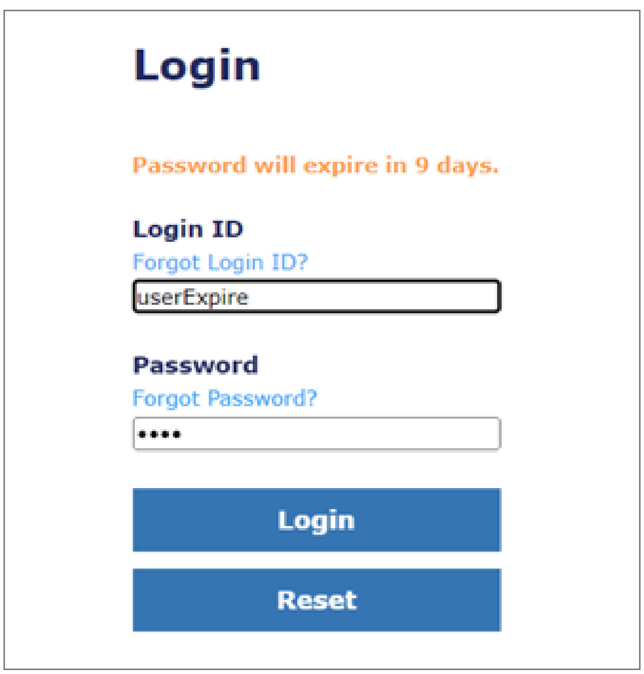
4.1 Enable Complex Password

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



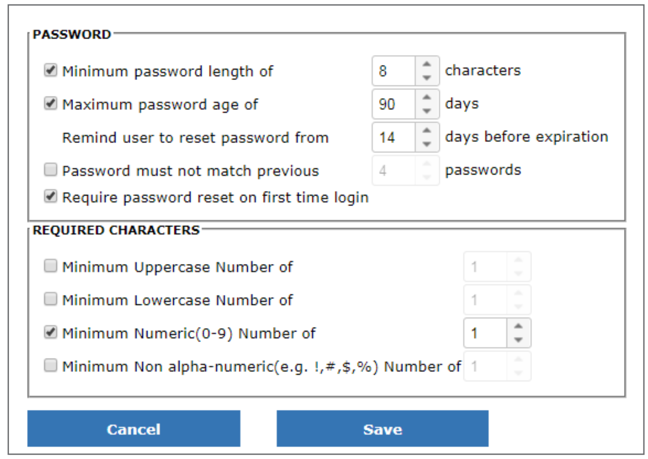
Remind user to reset password from: This option together with the “Maximum password age of” option is enabled.

When the password is about to expire, the user will see the option to reset the password when logging in within the configured reminder date, and the user can reset the password in advance.

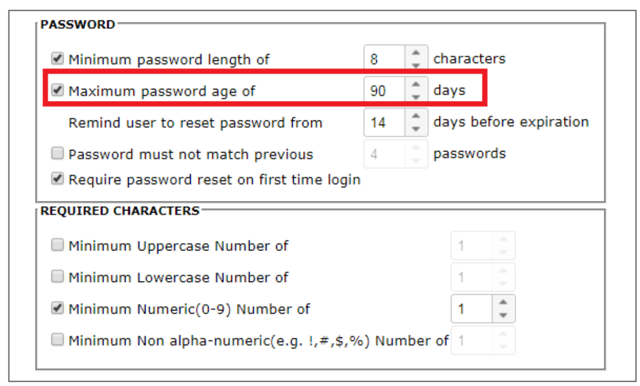


4.2 Configure Password

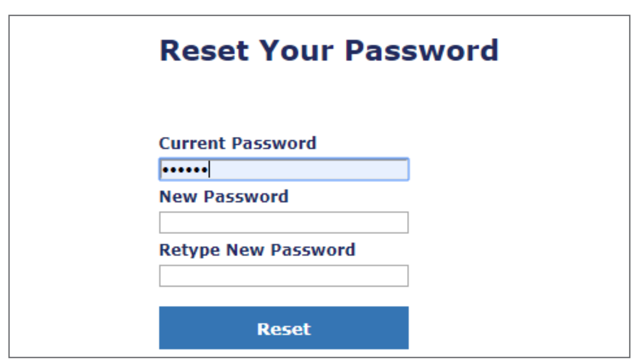
Select **Top Menu** > **Admin Tools** > **Setup** > **Password Rule Manager** and configure the rule you want to apply on your instance.



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.



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.



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
- XWEB: NA
- Danfoss: Severe, Critical, Normal, Log Only

Priority:

- E2 1-99
- E3 & Site Supervisor 1-99
- XWEB 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+:

Table: E2, E3, Site Supervisor and XWEB

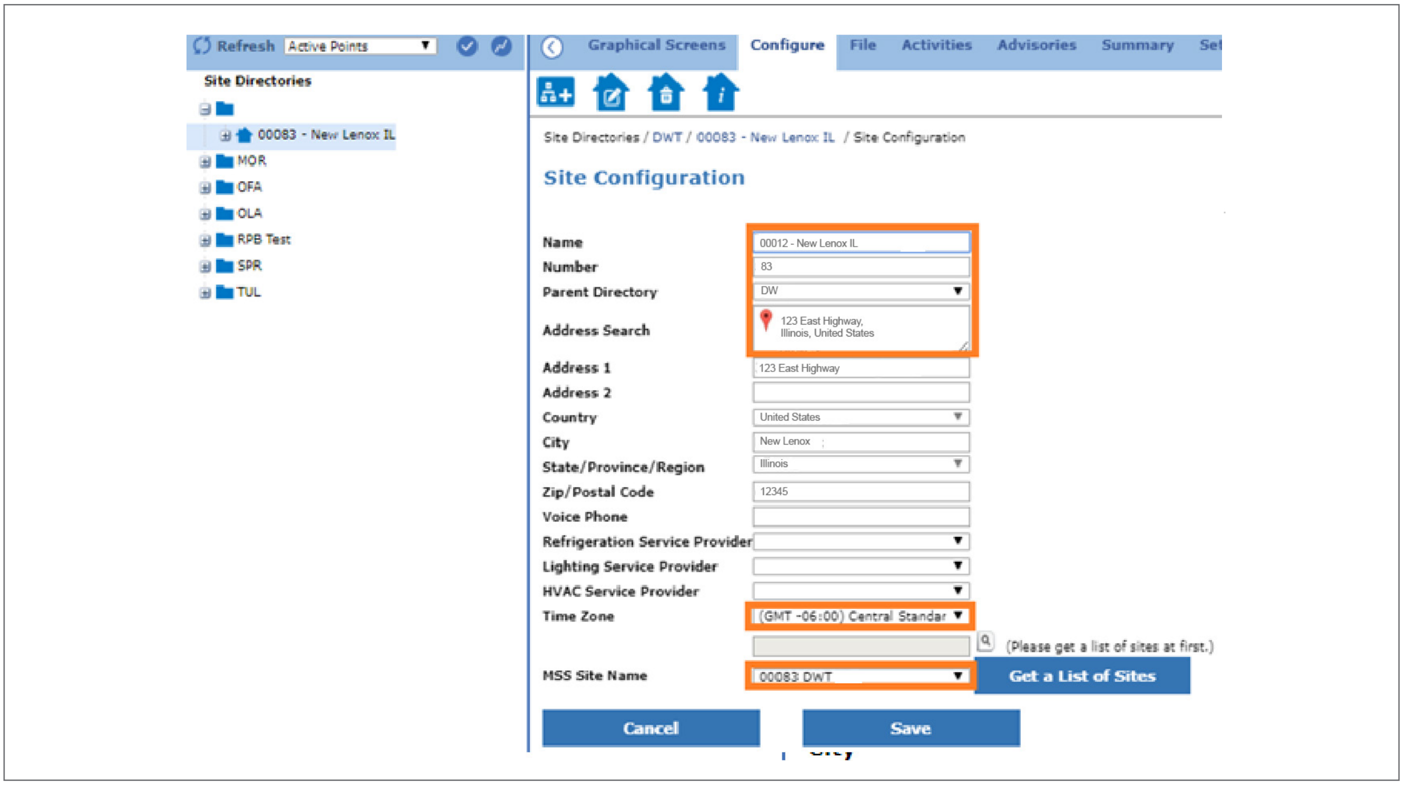
Advisory Urgency Level	State	Type	Priority
High	Active	Fail or Alarm	1-20
Medium	Active	Notice	1-50
		Fail or Alarm	21-50
Low	Active	All	51-99
	Return to Normal	All	1-00

Table: 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

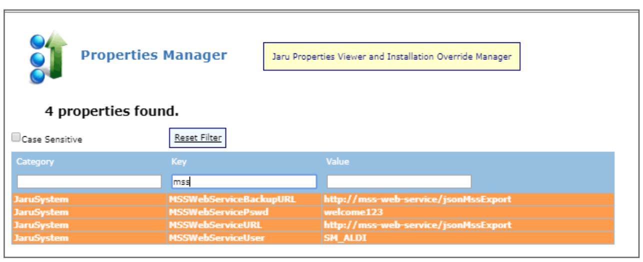
5.2 Configure Advisories Received from Controller

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 Priories 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

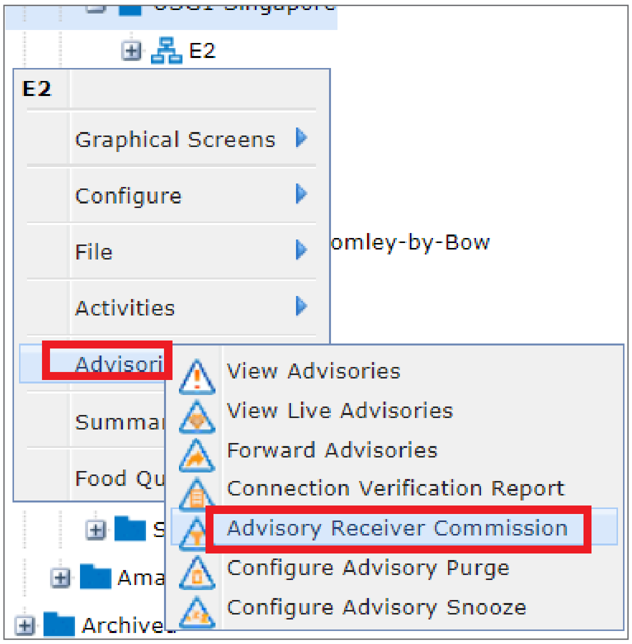
9. Verify Advisories are being received by AI/ UARD using PSC Consoler.

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.

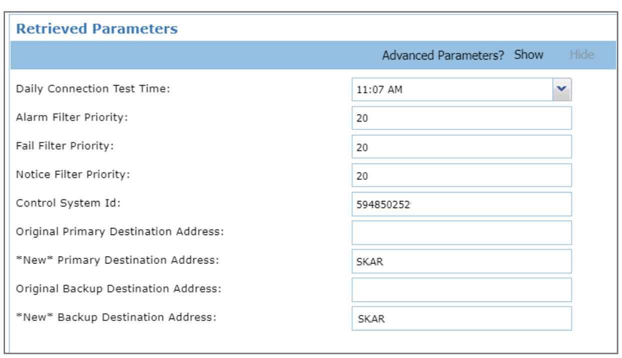
5.3 Advisory Receiver Commission

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**:

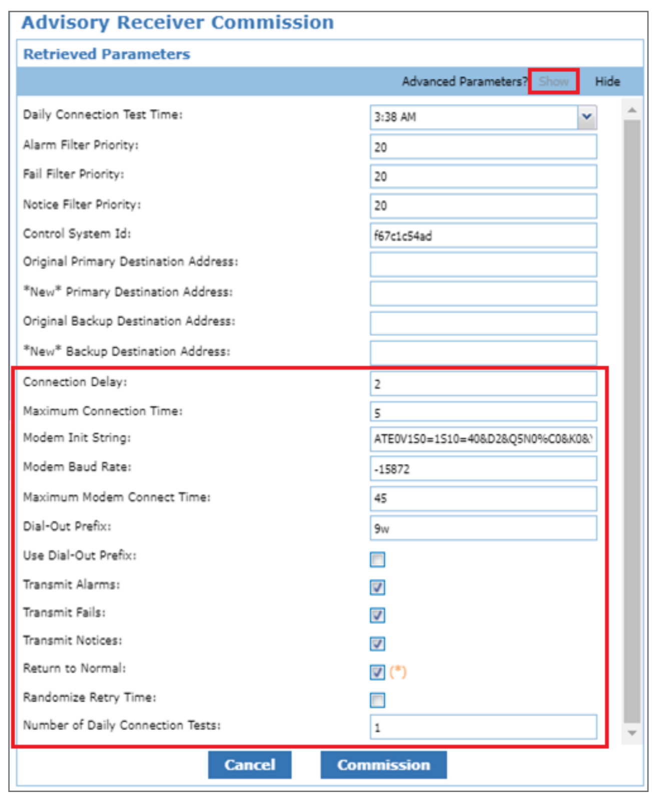


The information below is required and will be displayed by default:



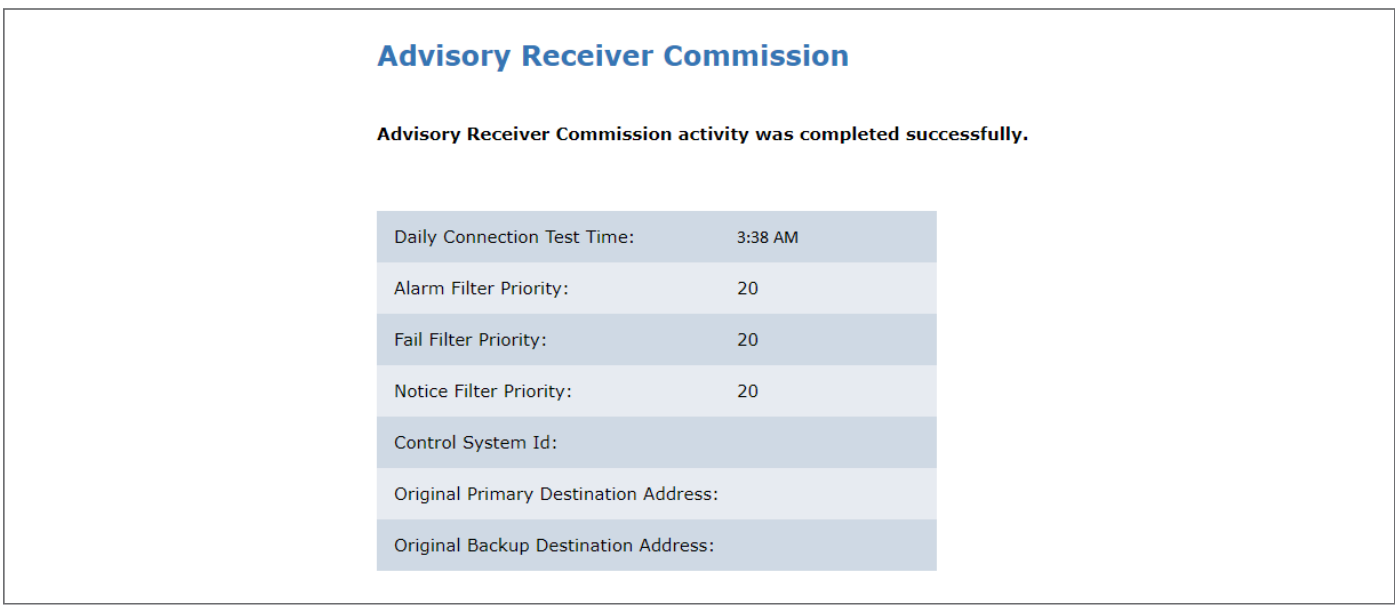
Field	Validation	Notes
Daily Connection Test Time	Required	Connect+ will test the connection with the controller every day. It is the date and time when Connect+ will try to connect to the controller.
Alarm Filter Priority	Required	The priority should be 1-99.
Fail Filter Priority	Required	The priority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



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 **Maximum Connection Time**.
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 **Daily Connection Test Time**.

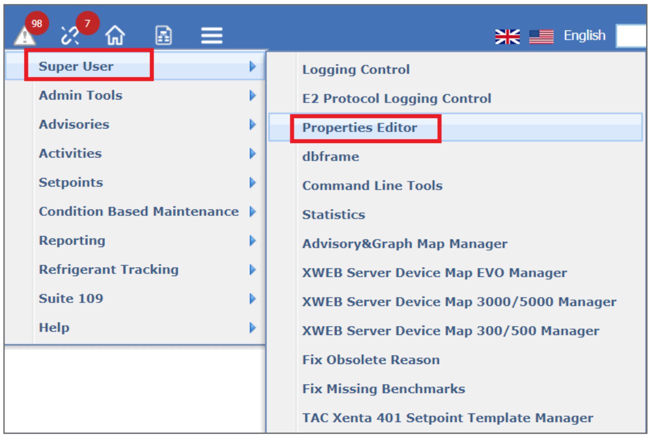
After the configuration is done, click the **Commission** button to see the message if the Advisory Receiver Commission is completed.



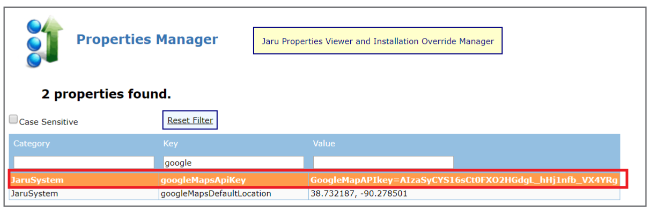
To check the advisories received in the controller, go to the **Advisory View** page.

5.4 Enable Advisory Map

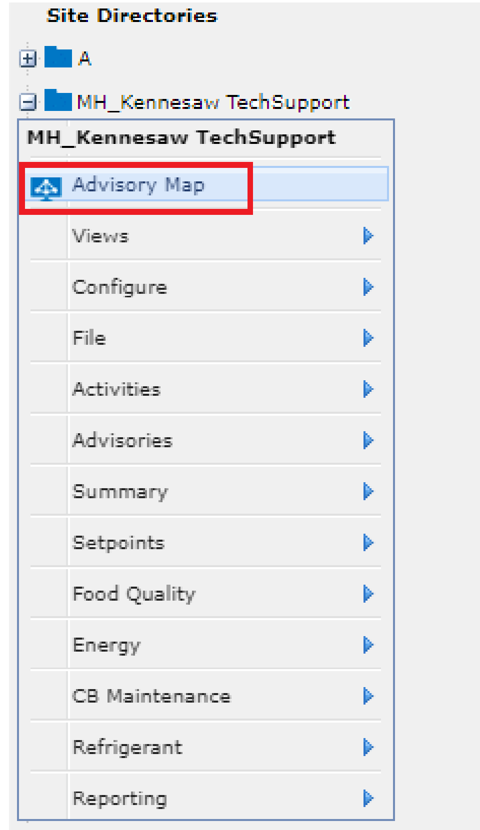
Login to the Connect+ with the super user. Select the **Top Menu** > **Super User** > **Properties Editor**.

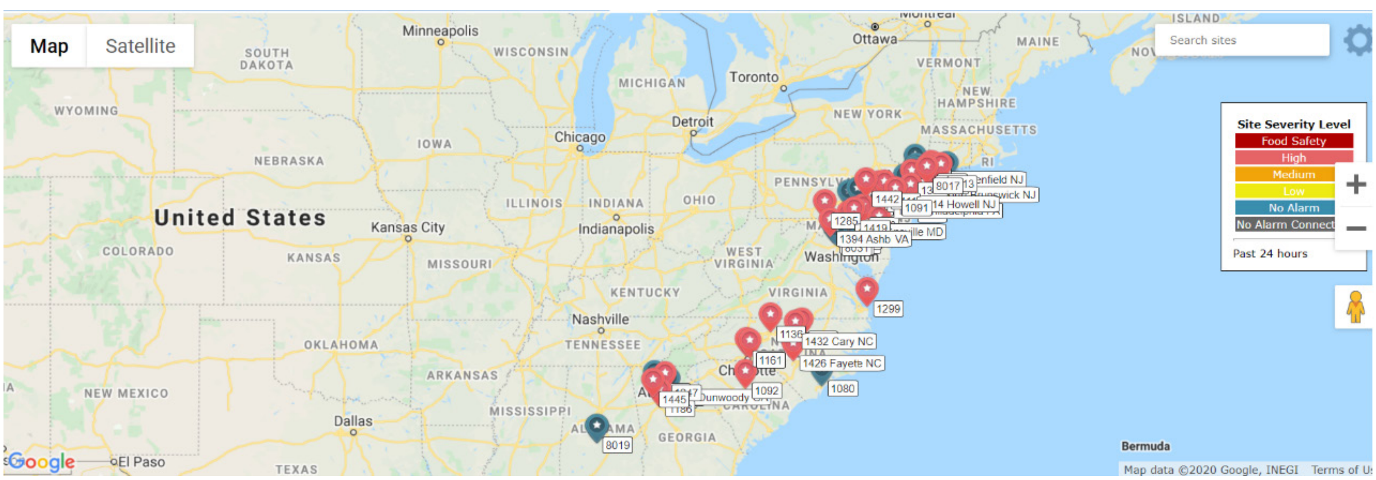


Set the **JaruSystem.googleMapsApiKey**. This is provided by Google to access the Google Maps on the site.



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

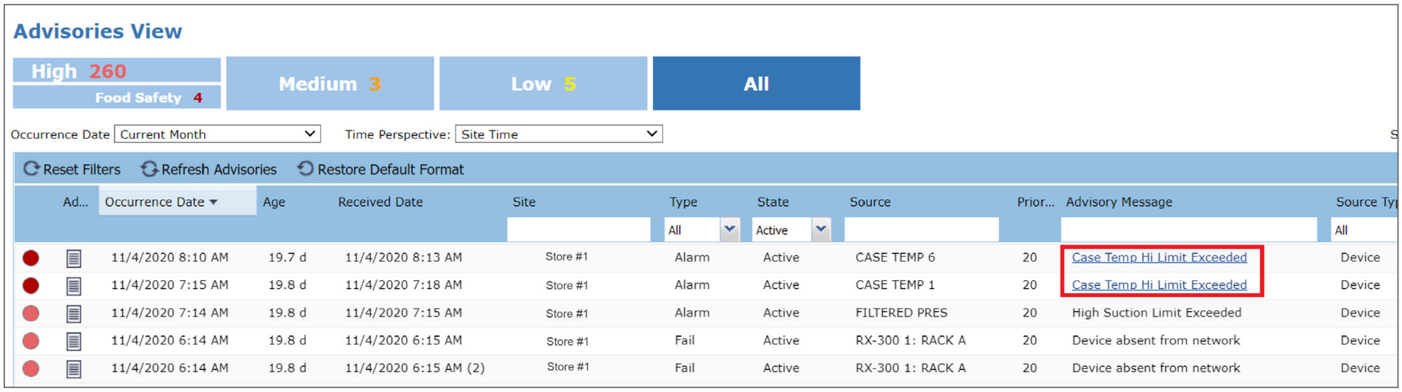




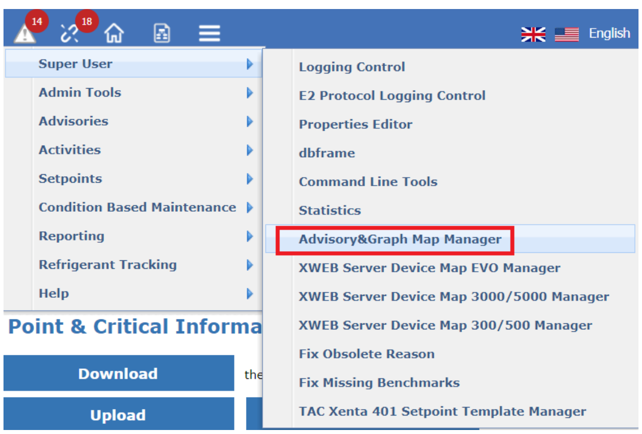
6. *Configure Advisory & Graph Map Manager*

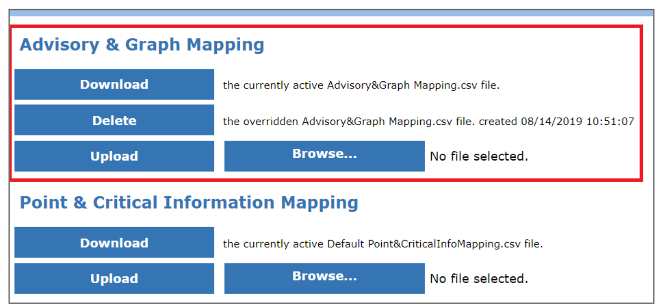
6.1 Advisory & Graph Mapping

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



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.





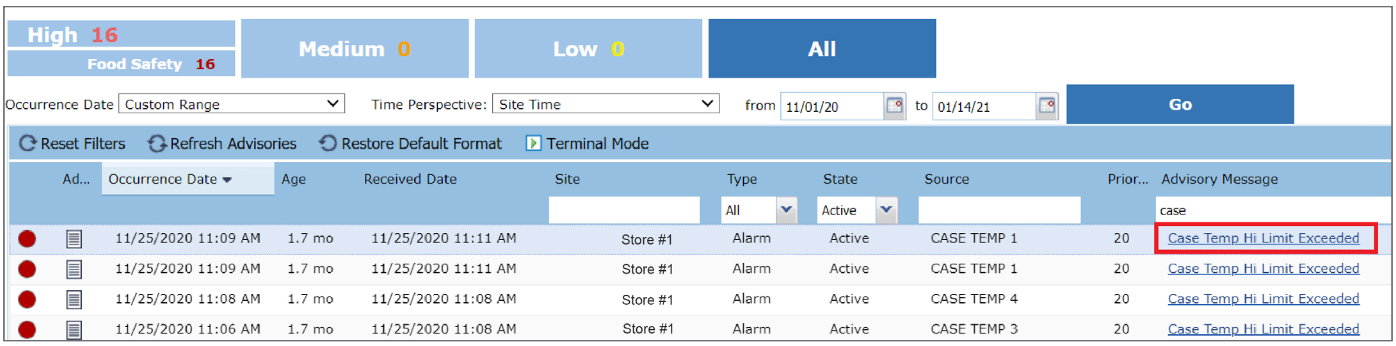
Download the default template by clicking the **Download** button. You could configure which type of advisories will show with the link in the downloaded **Advisory & Graph Mapping.csv**.

A	B	C	D	E
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.

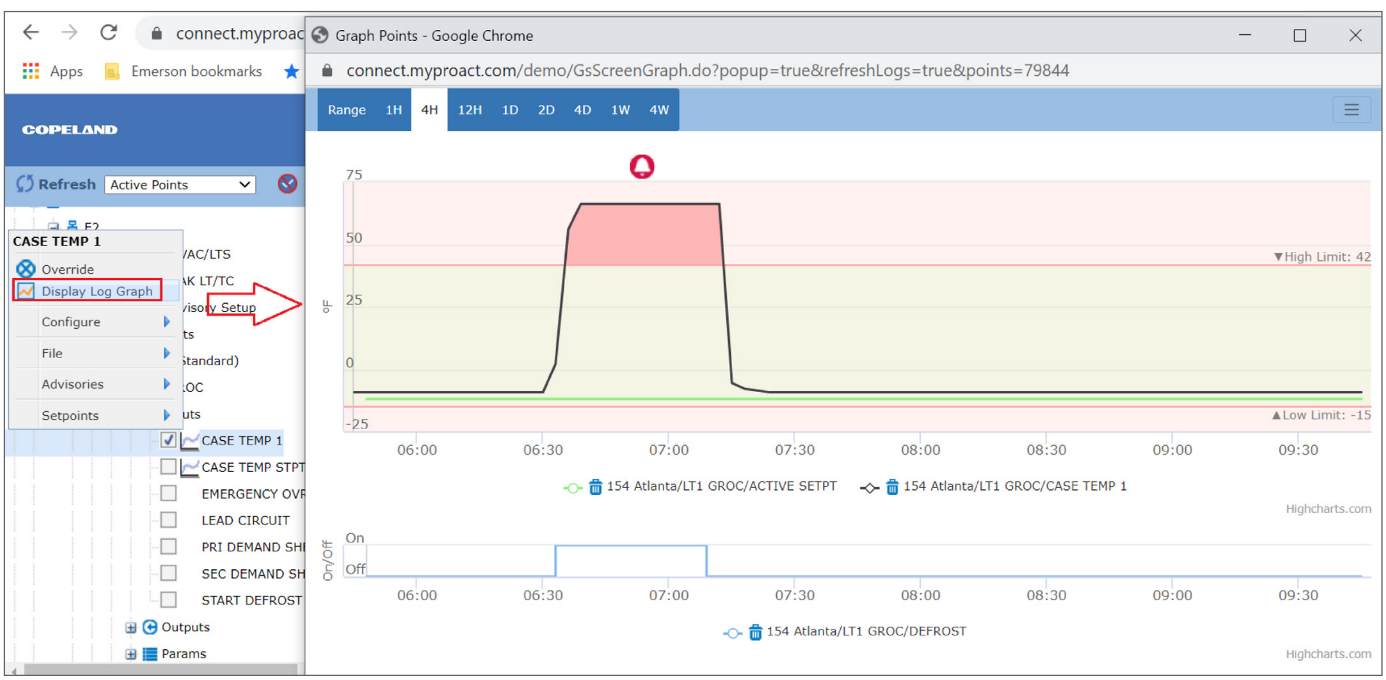
When configuration is done, you can click **Browse** button to choose your file, then click **Upload**.

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.

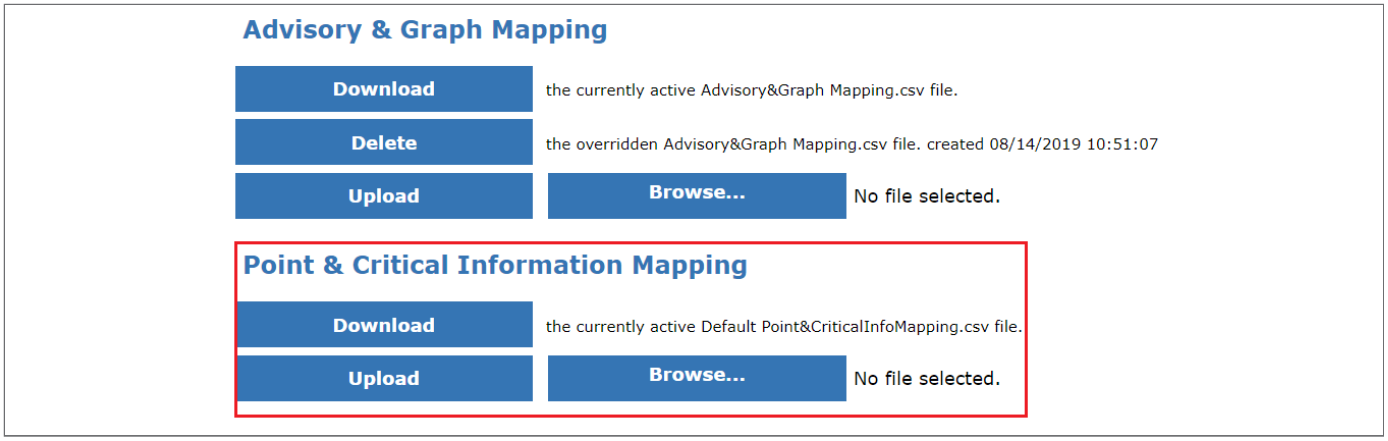


6.2 Point & Critical Information Mapping

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.



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 Alrm Hi	Product Alrm 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.

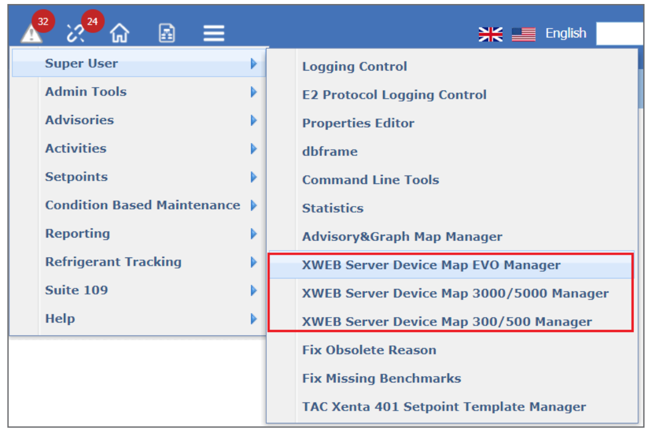
7. Configure XWEB Mapping

7.1 Download XWEB Server Device Map File

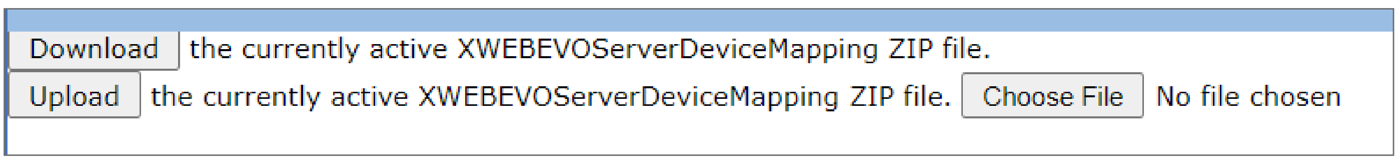
Select the **Top Menu** > **Super User** to see **XWEB Server Device Map Manager** menu for each Model. Currently, Connect+ support 3 models for Xweb device:

- XWEB EVO
- XWEB 3000/5000
- XWEB 300/500

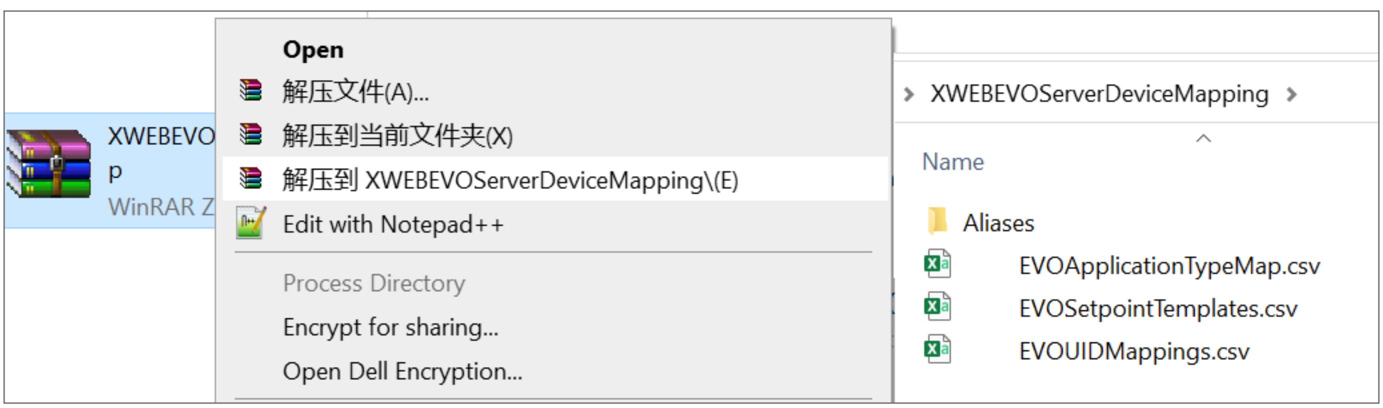
Select the **XWEB Server Device Map EVO Manager** menu for instance.



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
XWEBEVOApplicationTypeMap	Used to configure the mapping of the XWEB device and Connect+ application type.
XWEBEVOSetpointTemplate	Configured to monitor and manage the setpoint changes
XWEBEVOUIDMapping	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 XWEBEVOApplicationTypeMap.csv file

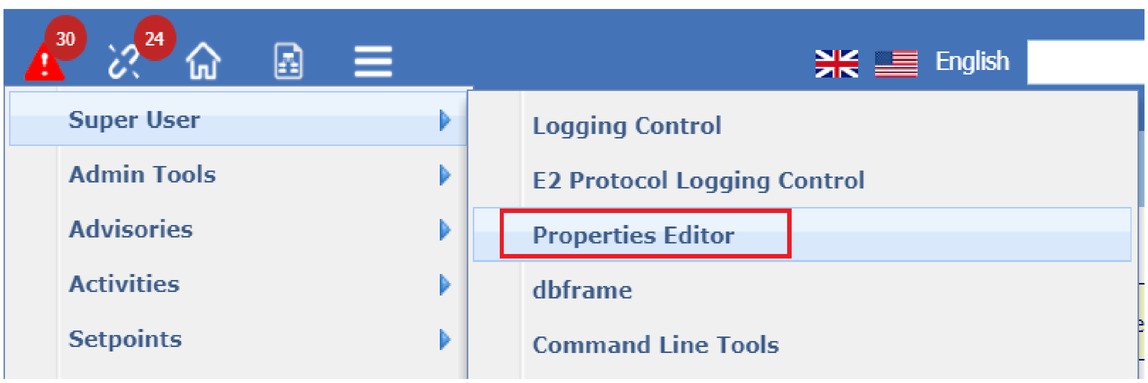
To add a new device support in the Connect+, map new devices in **XWEBEVOApplicationTypeMap.csv** file. The devices added in the file will be shown in Connect+ navigation tree.

There are four columns in the file.

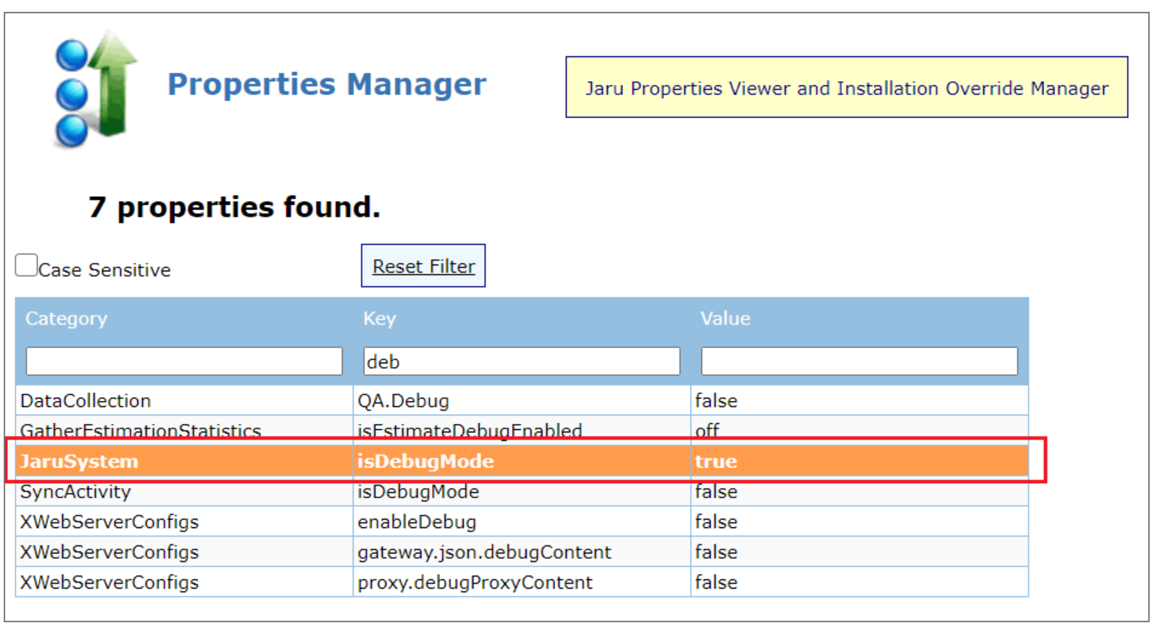
Field	Validation	Notes
XWEBDeviceType	Required	The XWEB device model. Add new device model name in this column.
unifiedAppTypeName	Required	The mapped application type name in Connect+ defines which application type you want your new device to be mapped.
nativeAppTypeName	Required	The name displayed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

How to get ProtocolUniqueId

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

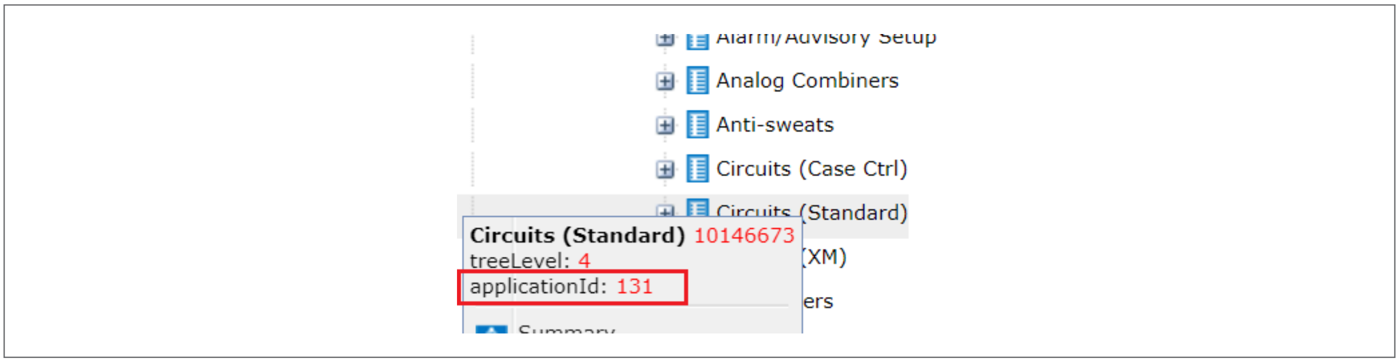


Find **JaruSystem.isDebugMode** and change the value to true.



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 appTypeProtocolUniqueId column.



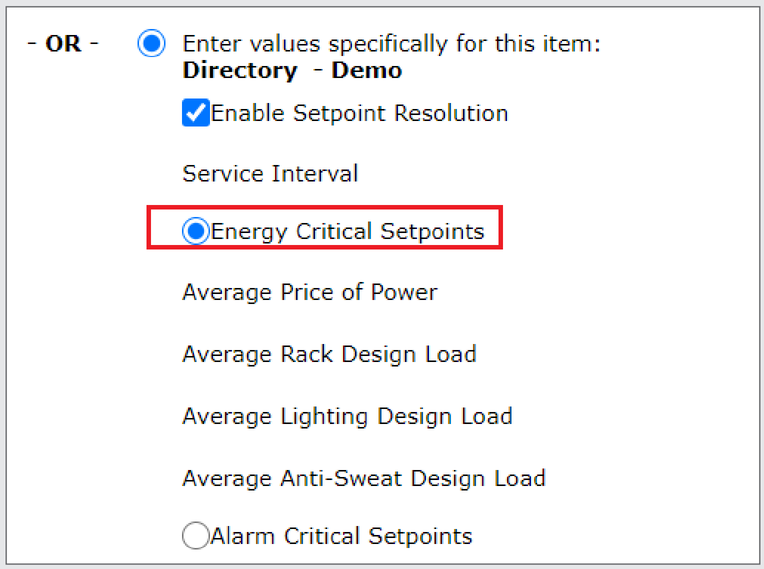
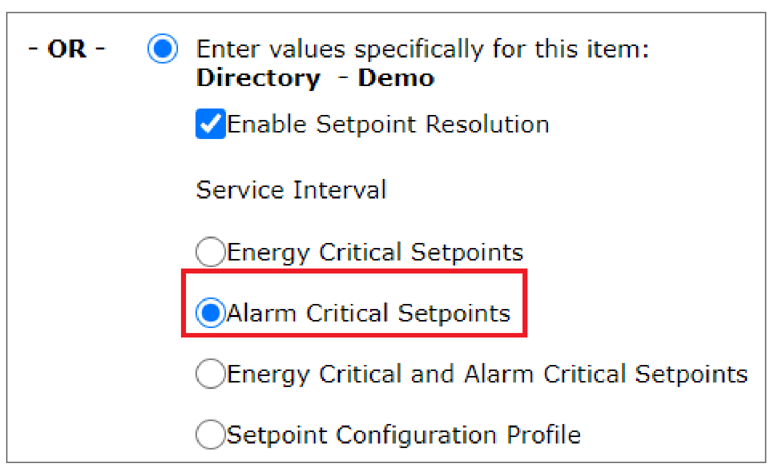
7.2.2 Configure XWEBEVOUIDMapping.csv file

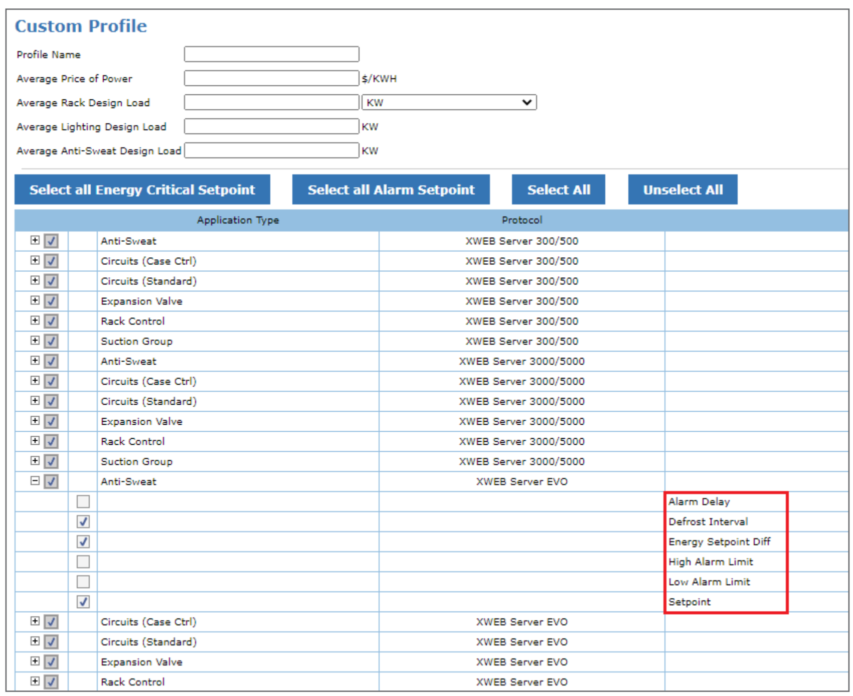
It defines the point mapping relationship for XWEB 300/500 and XWEB3000/5000. This mapping will be used to show which points will be shown from the Connect+ navigation tree. But for XWEB EVO and Connect+ all points will be shown from XWEB device in navigation tree. This mapping can only be used for Setpoint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

Field	Validation	Notes
appTypeProtocolUniqueId	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.
pointProtocolUniqueId	Required	You can give a unique ID number to each point.
deviceType	Required	The device model such as, XR75, XM679, etc.
pointOriginalUniqueId	Required	Point name starts with _@, like _@SEt, _@Hy, etc.

7.2.3 Configure XWEBEVOSetpointTemplate.csv file

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

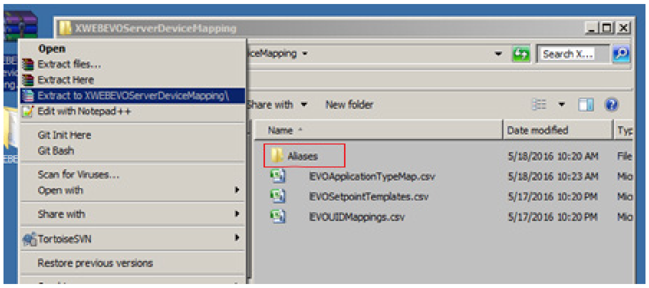
Field	Validation	Notes
protocolName	Required	XWEB Server EVO
pointProtocolUniqueId	Required	This ID should be same as the pointProtocolUniqueId configured in XWEBEVOUIDMapping.csv file.
appTypeProtocolUniqueId	Required	The unique application type ID in Connect+ (see above steps).
unifiedAppTypeName	Required	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	**Setpoint Category** 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. 
alarmSetpoint	Required	**Setpoint Category** 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. 

Field	Validation	Notes
checkOveride	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	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. 

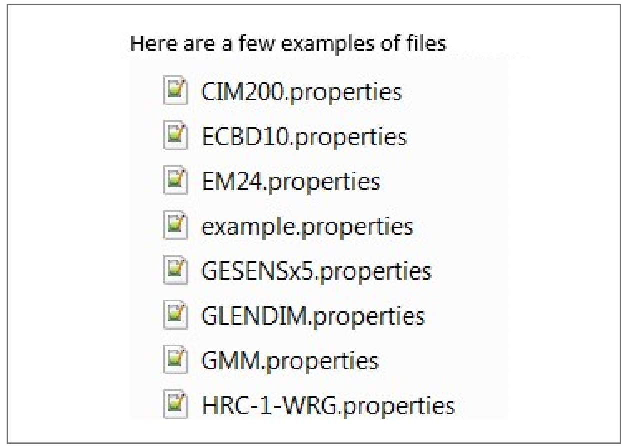
7.2.4 Configure Aliases File

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.

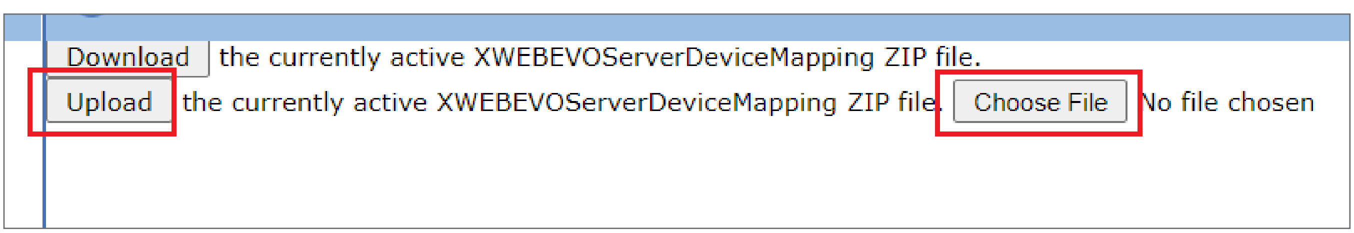


3. Configure customized point name and follow below rules:

```
#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.



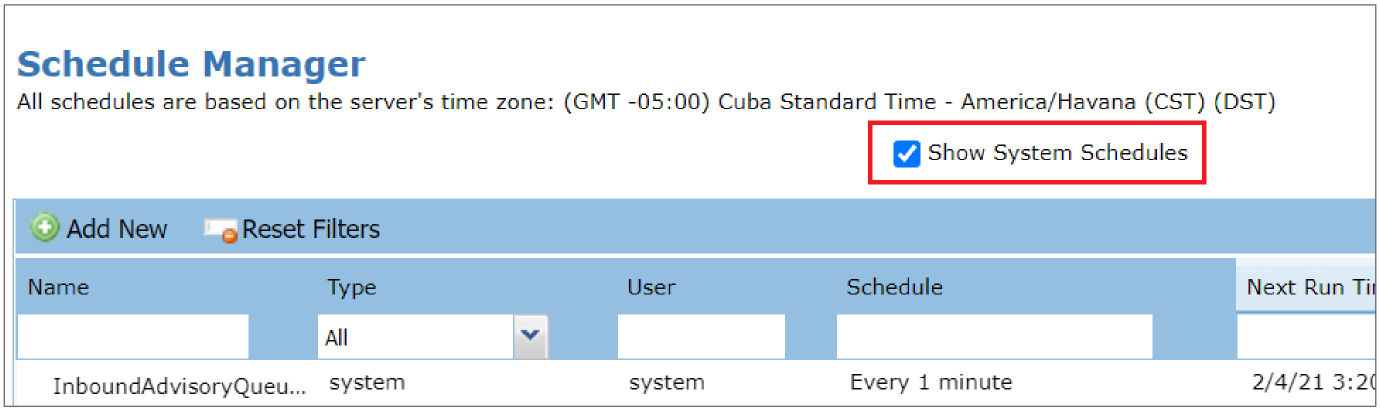
After Tomcat® is restarted, the files will be working.

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** checkbox to show the system schedules.



You can get system schedule description and recommended 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.
InboundAdvisoryQueueToAdivisoryJob	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

Schedule Name	Description	Recommended Default Setting
AdvisoryPurgeJob	Configure to purge old advisories based on the configuration in the Configure Advisory Purge page.	Every 2 hours
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)

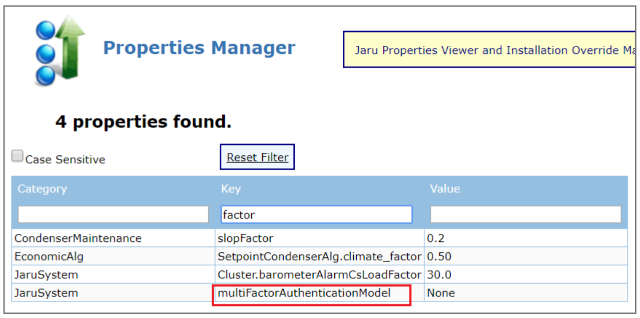
9.1 Multi-Factor Authentication

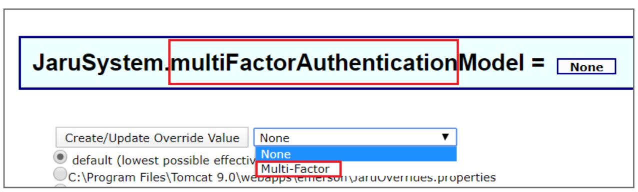
If the company has security requirement for the Connect+ login, the administrator can use Multi-Factor Authentication function for double verification.

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**.

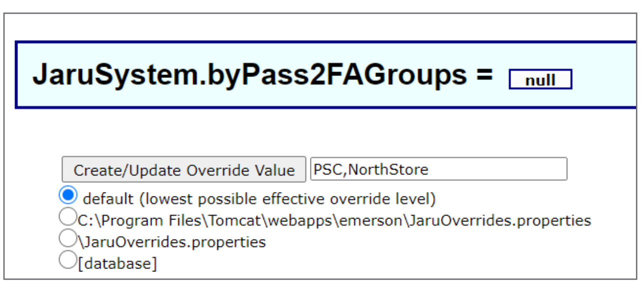
Change JaruSystem. **"multiFactorAuthenticationModel" to Multi-Factor**.





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.

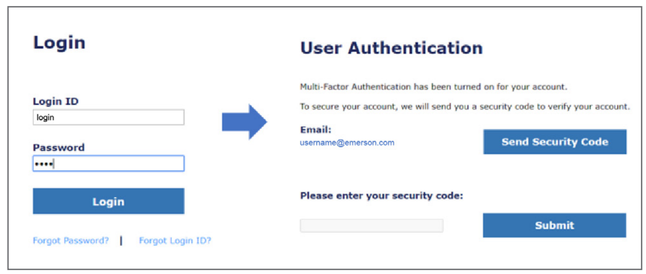


9.1.2 Login with Multi-Factor Authentication

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

Login with Email

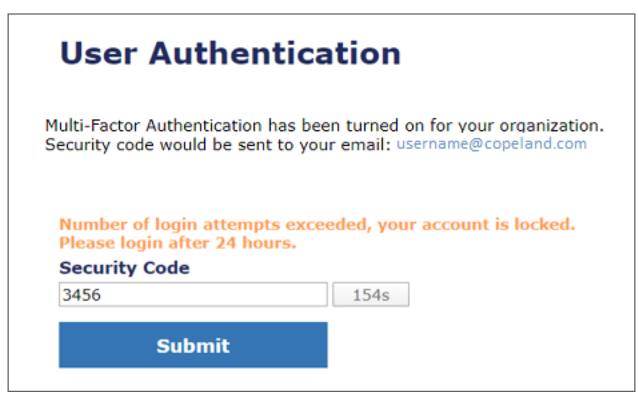
If your user login account has a configured email, you will be required to send a security code to your email by clicking the **Send Security Code** button.



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.

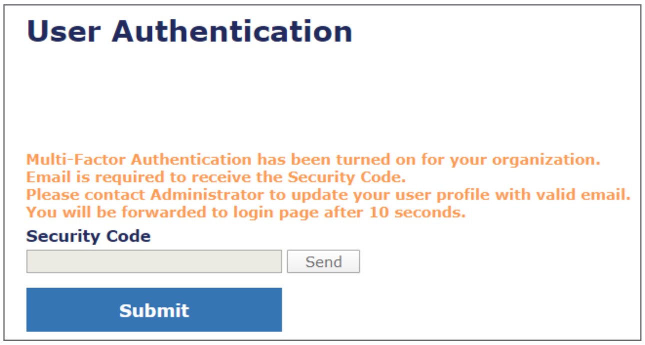
Once you received the security code in your email, enter it in the **Security Code** field and click **Submit**. After the successful authentication, you can start logging into the Connect+. If authentication fails, you need to check the security code and re-enter it again. Connect+ will restrict the 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.



Login without Email

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



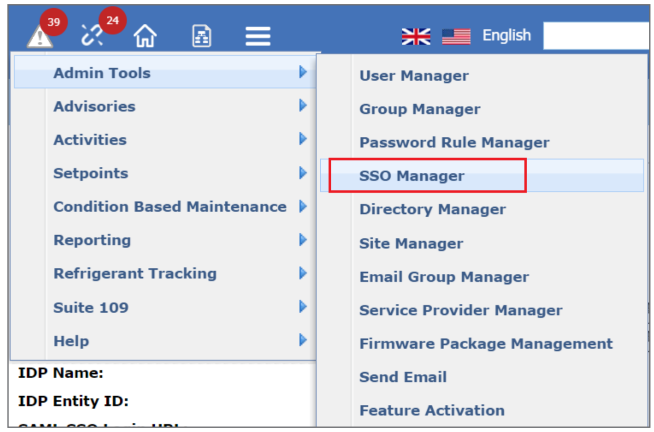
After passing the Multi-Factor authentication, you will not need to pass the authentication again for next login because the authentication information is recorded in the browser cookies. If you change a browser or change a device, you will need to verify again.

9.2 Single Sign-on

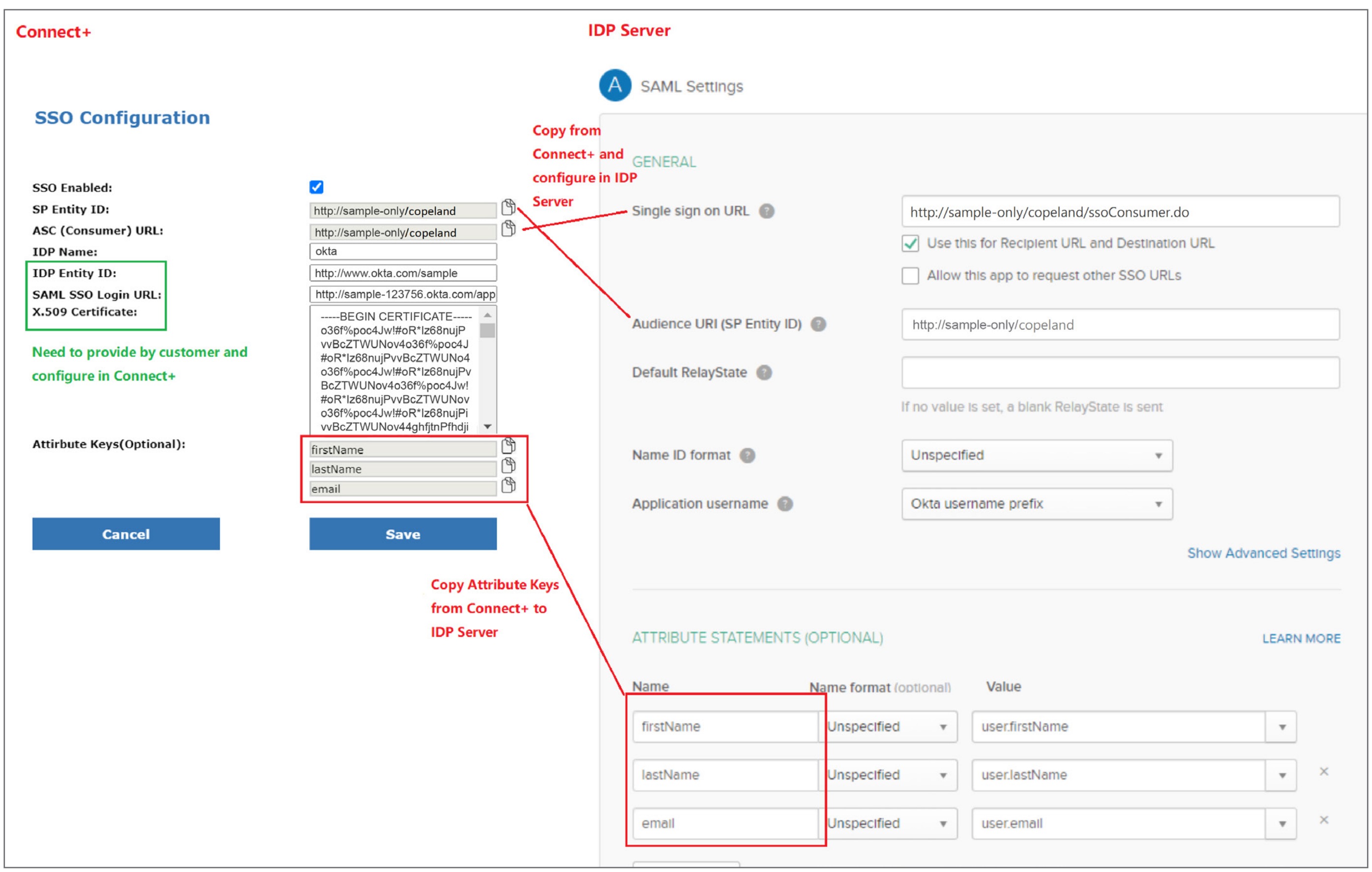
Single Sign-on allow you to log into the Connect+ using the company credential.

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.

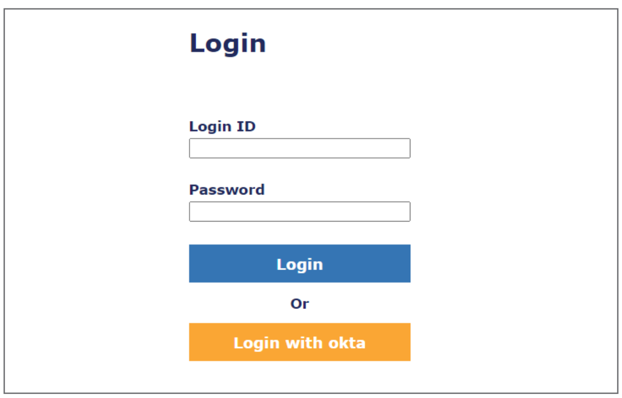


Field	Validation	Notes
SSO Enabled	Required	Check the property to enable the Single Sign-on.
SP Entity ID	Required	The Service Provider's (Connect+) Entity ID, which is a read only field. Admin should copy this value to the IDP's App metadata configuration page in admin console. For example, http://www.customerdomain.com/copeland
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, http://www.customerdomain.com/copeland/consumer
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.

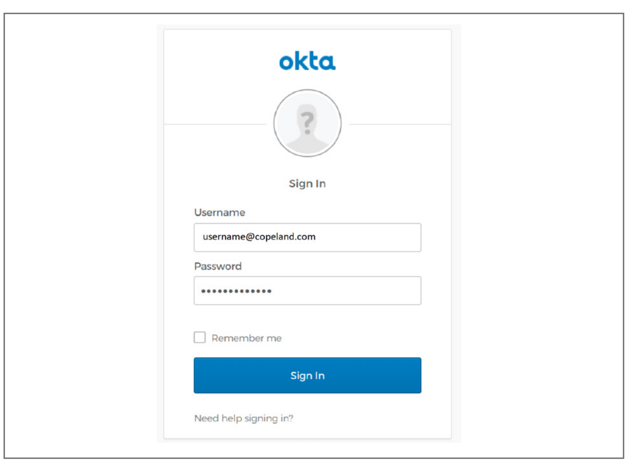
9.2.2 Login with Single Sign-on

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

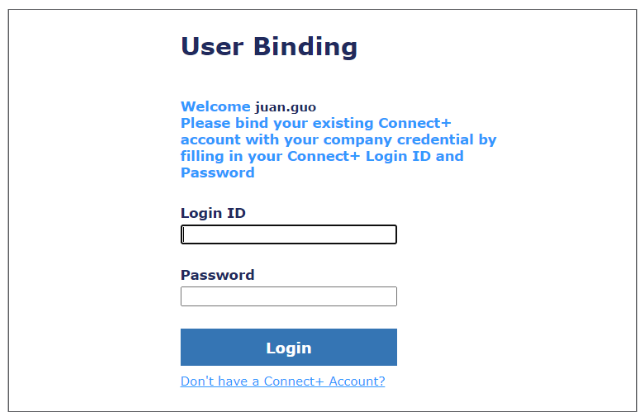
In the login page, you will see a **Login** with XXX (XXX is the IDP Name which is configured in SSO configuration) button.



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.

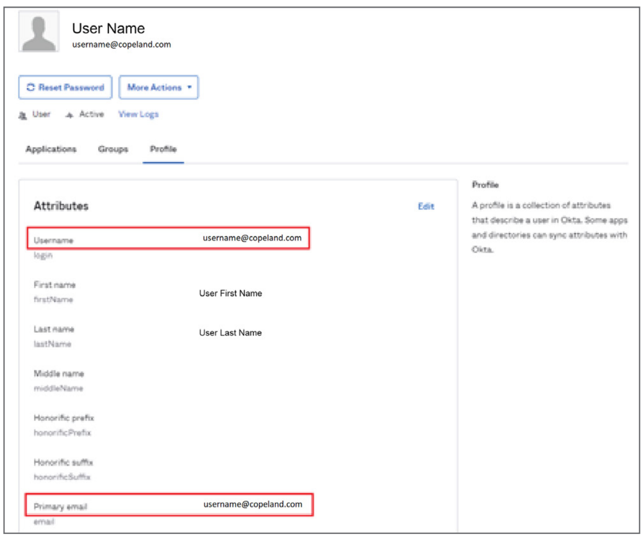
Administrator needs to assign the site permission for the group, or the new user will not see any site after login.

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

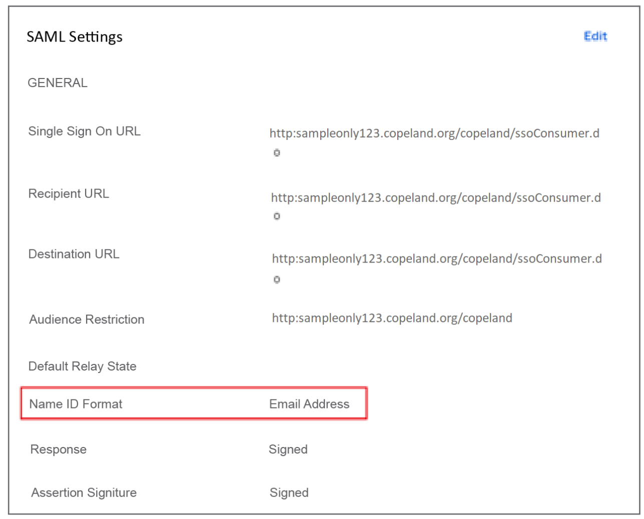
9.2.4 Auto-binding SSO User Account with Connect+ User

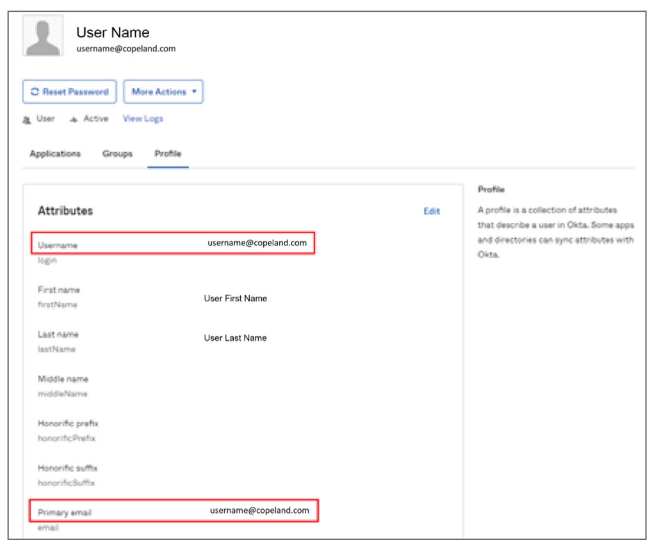
If your SSO username is in email format or the SSO user email is configured in IDP server, the user binding indicated in section *"9.2.2 Login with Single Sign-on"* will be skipped. Connect+ could do the auto-binding through the unique email address.

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.



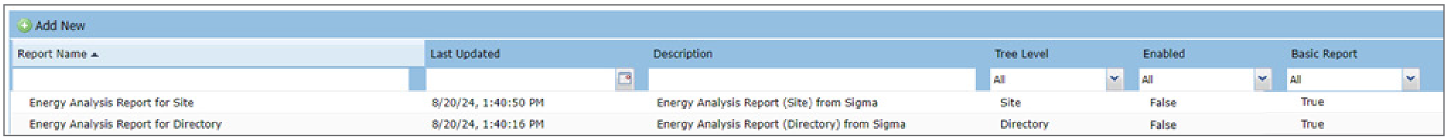


10. Configure Report

Connect+ supports four reports - Advisory Analysis, Energy Analysis, Alarm Summary and Insight Enterprise report. These reports can provide multiple perspectives on different data.

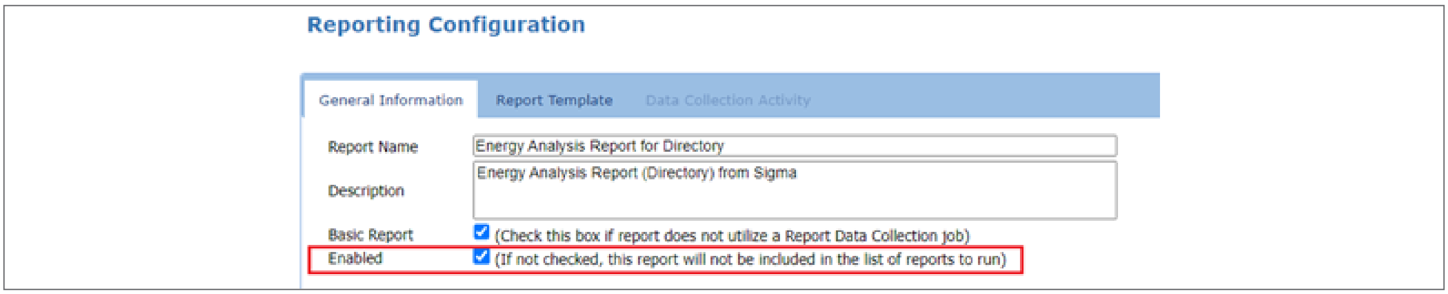
10.1 Configure Energy Analysis Report

To enable the reports, log into Connect+ using superuser credentials. 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. They are disabled by default.

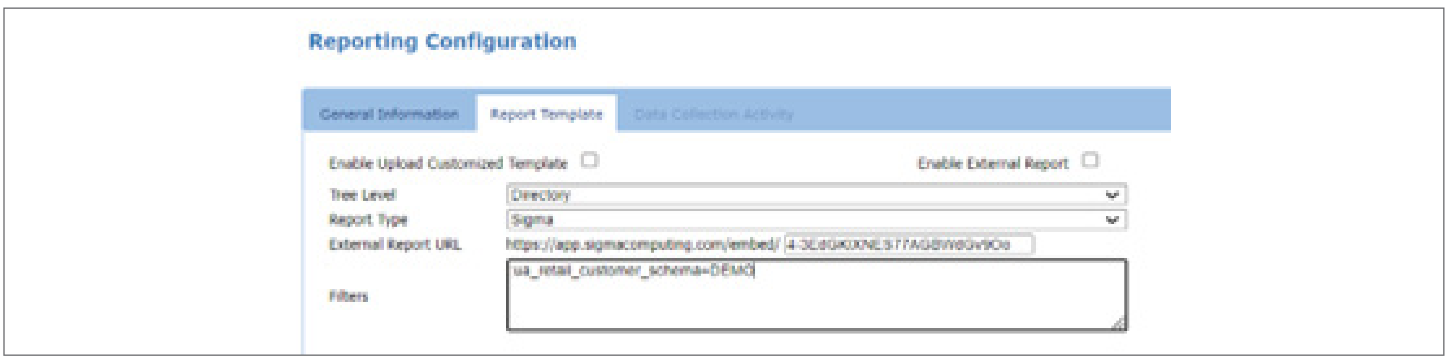


Report Name	Last Updated	Description	Tree Level	Enabled	Basic Report
			All	All	All
Energy Analysis Report for Site	8/20/24, 1:40:50 PM	Energy Analysis Report (Site) from Sigma	Site	False	True
Energy Analysis Report for Directory	8/20/24, 1:40:16 PM	Energy Analysis Report (Directory) from Sigma	Directory	False	True

Edit these two reports by double clicking the **Report Name**. Enable the report by checking the **Enable** checkbox from the **General Information** tab.



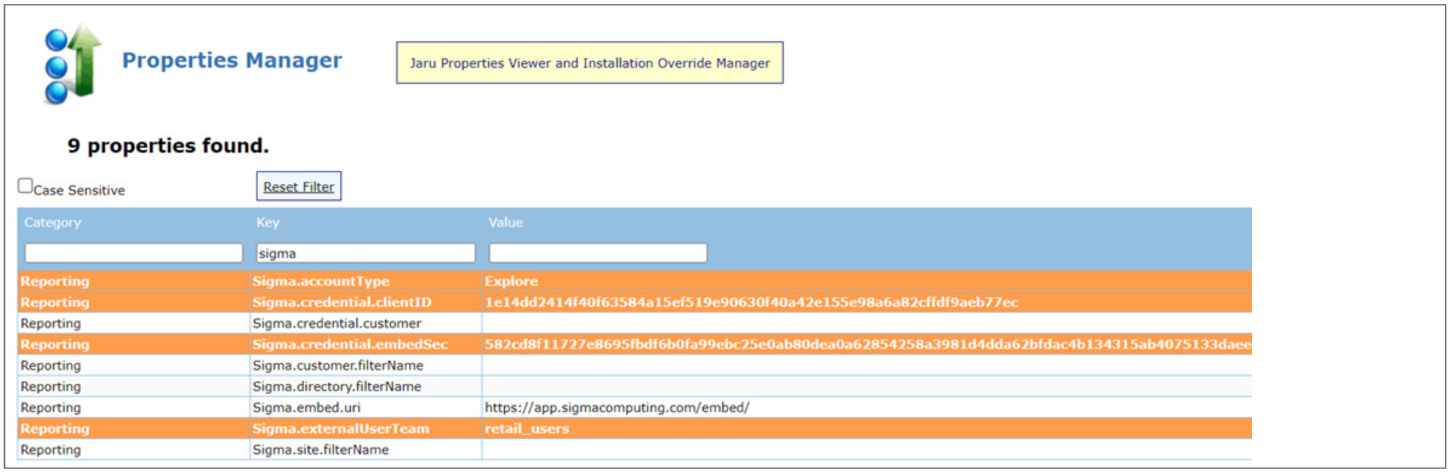
Switch to **Report Template** tab and configure the External Report URL with *4-3EdGKIXNES77AGBWdGv9Oo*.



Please contact 833-409-7505 or *ColdChain.TechnicalServices@Copeland.com* for the ua_retail_customer_schema configuration in the Filters field.

After that, go to Top Menu > **Super user** > **Properties Editor**, configure the properties as below:

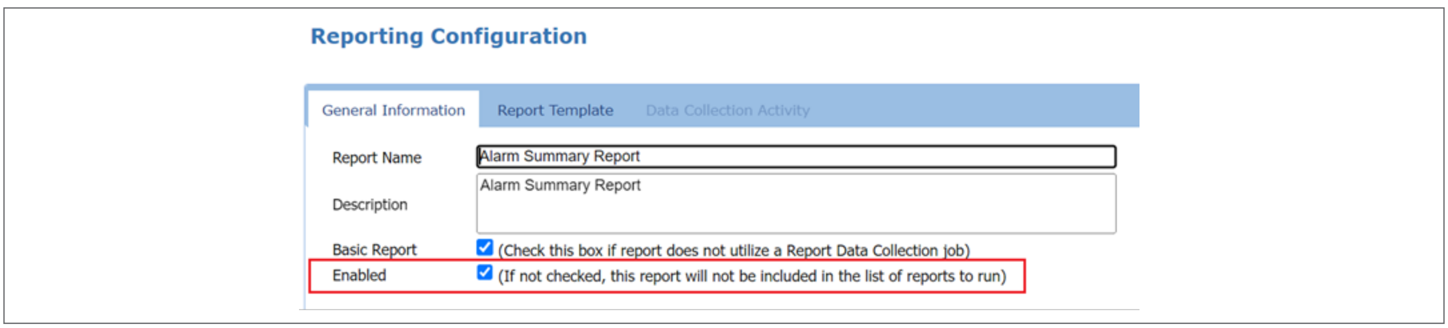
- Reporting.Sigma.accountType = **Explore**
- Reporting.Sigma.credential.clientID = **1e14dd2414f40f63584a15ef519e90630f40a42e155e98a6a82cffdf9aeb77ec**
- Reporting.Sigma.credential.embedSec = **582cd8f11727e8695fbdf6b0fa99ebc25e0ab80dea0a62854258a3981d4dda62bfdac4b134315ab4075133daee c743c94b301178c8e5c58e0ddd14db10eecb00**
- Reporting.Sigma.externalUserTeam = **retail_users**



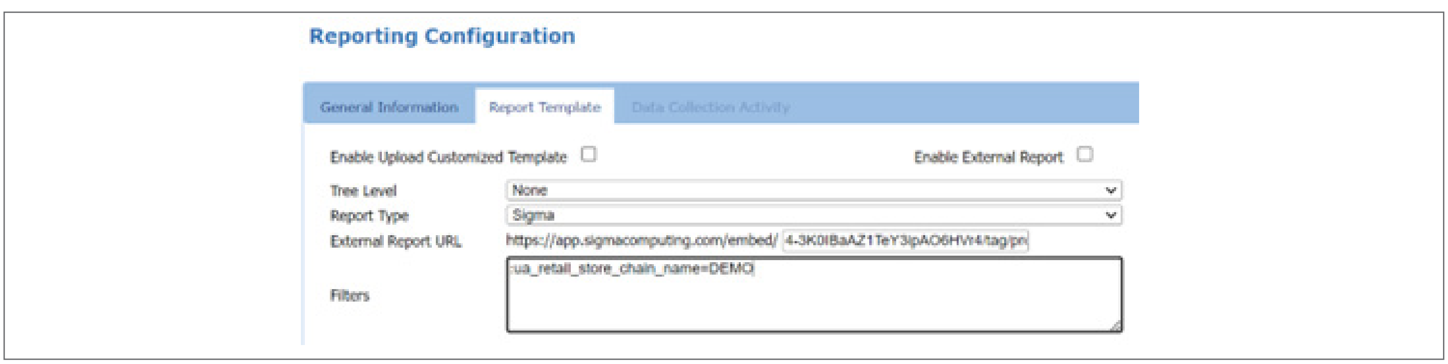
Once all configurations are complete, Energy reports will be displayed on the right-click menu and energy data can be successfully displayed based on accumulated logs for specific Power Monitoring points.

10.2 Configure Alarm Summary Report

You can configure and view the Alarm Summary Report once your company purchases it. Log into Connect+ using superuser credentials, go to Top Menu > **Reporting** > **Reporting Manager**, you will see the **Alarm Summary Report** in the table. Double click the report to go the configuration page. Check the **Enabled** checkbox in **General Information** tab.



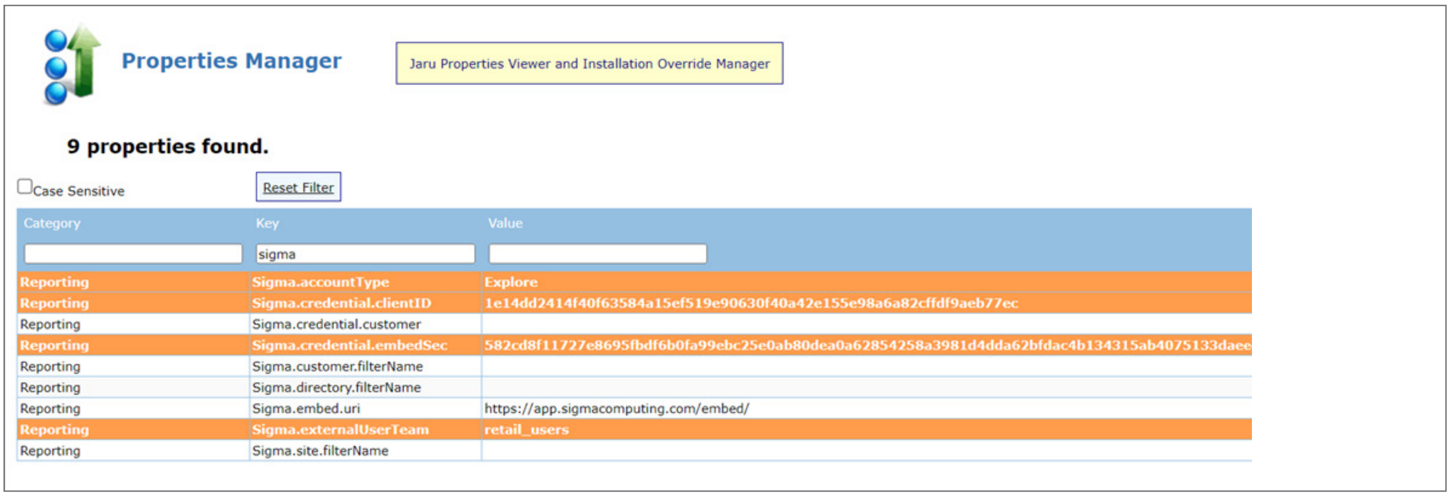
Then go to the **Report Template** tab, fill in the External Report URL parameter with *4-3K0IBaAZ1TeY3ipAO6HVr4/tag/prod*.



Please contact 833-409-7505 or *ColdChain.TechnicalServices@Copeland.com* for the ua_retail_customer_schema configuration in the Filters field.

Same as Energy Report, you also need to go to Top Menu > **Super user** > **Properties Editor**, configure the properties below, these configurations are same as Energy Report, if you have configured it, please ignore it.

- Reporting.Sigma.accountType = **Explore**
- Reporting.Sigma.credential.clientID = **1e14dd2414f40f63584a15ef519e90630f40a42e155e98a6a82cffdf9aeb77ec**
- **Reporting.Sigma.credential.embedSec** = **582cd8f11727e8695fbdf6b0fa99ebc25e0ab80dea0a62854258a3981d4dda62bfdac4b134315ab4075133daeec743c94b301178c8e5c58e0ddd14db10eecb00**
- Reporting.Sigma.externalUserTeam = **retail_users**



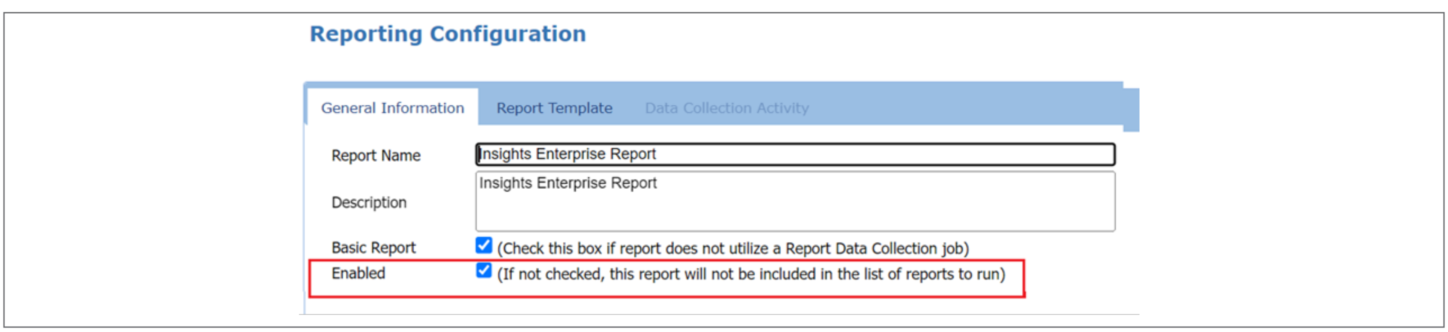
Once all configurations are complete, Alarm Summary report will be displayed under Top Menu > **Reporting** and alarm summary data can be successfully displayed based on the alarm received in Connect+.

10.3 Configure Insight Enterprise Report

Like the Alarm Summary Report, the Insight Enterprise Report requires an additional purchase.

Go to Top Menu > **Reporting** > **Reporting Manager**. You will see the **Insight Enterprise Report** in the table. Double click the report to go the configuration page.

Check the Enabled checkbox in **General Information** tab.



Then go to the **Report Template** tab, fill in the External Report URL parameter with *4-7hjl7r1xFCaql02KAeuhtf/tag/prod*.

Please contact 833-409-7505 or *ColdChain.TechnicalServices@Copeland.com* for the ua_retail_customer_schema configuration in the Filters field.

Below are the common configurations, if you have configured it for other report, you can ignore it.

Go to Top Menu > **Super user** > **Properties Editor**, configure the properties below:

- Reporting.Sigma.accountType = **Explore**
- Reporting.Sigma.credential.clientID = **1e14dd2414f40f63584a15ef519e90630f40a42e155e98a6a82cffdf9aeb77ec**
- Reporting.Sigma.credential.embedSec = **582cd8f11727e8695fbdf6b0fa99ebc25e0ab80dea0a62854258a3981d 4dda62bfdac4b134315ab4075133daeec743c94b301178c8e5c58e0ddd14db10eecb00**
- Reporting.Sigma.externalUserTeam = **retail_users**

Once all configurations are complete, Insight Enterprise report will be displayed under Top Menu > **Reporting** and cases and racks status data will be calculated and displayed in the report.

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	Access Needed
My User Info	Users can change their password and set personal system settings.	Connect+
My Pending Activities	Users can view activities that are waiting to start or in progress that have been initiated by the user.	Connect+
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.	Connect+
My Activity History	Users can view activities initiated by the user.	Connect+
My Activity History for Tree Item	Users can view activities from a tree node that have been initiated by the user.	Connect+
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.	Connect+
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.	Connect+
Admin Activity History	Users can view activities initiated by all users.	Connect+
Admin Activity History for Tree Item	Users can view activities from a tree node initiated by all users of the system.	Connect+
Add User	Users can add users to the system.	Connect+
Edit User	Users can edit users of the system.	Connect+
Delete User	Users can delete users from the system.	Connect+
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.	Connect+
Edit Group	Users can edit groups by adding or removing privileges and change their site and directory permissions.	Connect+
Delete Group	Users can delete existing groups.	Connect+
Add Service Provider	Users can add service providers to the system.	Connect+
Edit Service Provider	Users can edit service providers in the system.	Connect+
Delete Service Provider	Users can delete service providers in the system.	Connect+
Service Provider Properties	Users can view detailed information about service providers.	Connect+
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.	Connect+
View All Scheduled Activities	Users can view all configured scheduled activities created by all users of the system.	Connect+
Edit My Scheduled Activities	Users can view and edit only scheduled activities they created.	Connect+
Edit Any Scheduled Activities	Users can view and edit all scheduled activities that were created by all users of the system.	Connect+
Delete My Scheduled Activities	Users can delete only scheduled activities they created.	Connect+
Delete Any Scheduled Activities	Users can delete all scheduled activities that were created by all users of the system.	Connect+
View Directory Properties	Users can view information that is related to a directory, including subdirectories, sites, activities, and configuration information.	Connect+

Table A-1

Privilege	Description	Access Needed
Add Directory	Users can add directories to the system. Directories are the top-most level of the navigation tree.	Connect+
Edit Directory	Users can edit existing directories in the system.	Connect+
Delete Directory	Users can delete existing directories from the system. Deleting a directory will delete everything within the directory.	Connect+
View Site Properties	Users can view information that is related to a site, including subdirectories, activities, and configuration information.	Connect+
Add Email Group	Users can add email group.	Connect+
Edit Email Group	Users can edit existing email group.	Connect+
Delete Email Group	Users can delete existing email group.	Connect+
Copy Email Group	Users can copy the existing email group.	Connect+
Add Site	Users can add sites to the system. Sites are at the second level of the navigation tree.	Connect+
Edit Site	Users can edit existing sites in the system.	Connect+
Delete Site	Users can delete existing sites from the system.	Connect+
View Control System Properties	Users can view information related to the control system including units, activities that can be performed, configurations and details.	Connect+
Add Control System	Users can add control systems to the system. Control systems are at the third level of the navigation tree.	Connect+
Edit Control System	Users can edit existing control systems in the system.	Connect+
Delete Control System	Users can delete existing control system from the system.	Connect+
View Unit Properties	Users can view information related to the unit including application, activities, configurations and details.	Connect+
View Application Type Properties	Users can view details about the application and make changes to the application.	Connect+
View Application Instance Properties	Users can view the number of points in the application (if available) that have been programmed inside a controller.	Connect+
View Point Properties	Users can view details about controller points, graph points, retrieve logs, and make changes.	Connect+
Display Log Graph	Users can view graphical representation of the data.	Connect+
View Real-time Graph	Users can view real-time graph of the data.	Connect+ & Controller
Watch Points	Users can select multiple points from the tree and view the real-time values for those points.	Connect+ & Controller
GS Screen Edit	Users can modify graphical status screens.	Connect+
GS Set Home Page	Users can set a graphical status screen as the first page they see when they log into the system.	Connect+
Add GS Screen	Users can create graphical status screens.	Connect+
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.	Connect+
Copy & Paste GS Screen	Users can copy an existing graphical status screen and paste it to another tree node of same level.	Connect+
Associate GS Screen	Users can connect a graphical status screen to a node on the tree.	Connect+
Advisory Receiver Commissioning	Users can set advisory configurations such as connection test time and advisory filter priorities for alarms, failures, and notices.	Connect+ & Controller
Firmware Package Management	Users can manage firmware files.	Connect+
View Advisories	Users can view historical advisories (alarms, fails, notices, warnings) from the database.	Connect+ & Controller
Acknowledge Live Advisories	Users can Acknowledge Live Advisories.	Connect+ & Controller
Clear Live Advisories	Users can Clear Live Advisories.	Connect+ & Controller

Table A-1

Privilege	Description	Access Needed
Reset Live Advisories	Users can Reset Live Advisories.	Connect+ & Controller
Mute Live Advisories	Users can Mute Live Advisories.	Connect+ & Controller
Forward Advisories	Users can forward advisories to email addresses and/or users in the system.	Connect+
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.	Connect+
Purge Inbound Connection Records	Users can set purge configurations for inbound connection records.	Connect+
Feature Activation	Users can view the license page as well as add feature activation keys.	Connect+
Help Contents	Users can view the system help including the help provided on each page.	Connect+
Add Private List	Users can create a list of points that will only be visible to them.	Connect+
Edit Private List	Users can edit a list of points only visible to them that they created.	Connect+
Delete Private List	Users can delete a list of points that the user created.	Connect+
Add Public List	Users can create a list of points that will be visible to all users of the system.	Connect+
Edit Public List	Users can modify any public list of points that was created.	Connect+
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.	Connect+
View Setpoint Broadcast Activity History	Users can view Setpoint Broadcast activity History.	Connect+
Admin SSO Manager	Users can configure and use Company account (Single Sign-on).	Connect+
Revert Setpoint Broadcast	Users can revert the point value which already been broadcasted.	Connect+ & Controller
Activity History Configuration	Users can purge activity history in the database.	Connect+
Admin Send Email	Send Email	Connect+
View Enterprise Summary	Users can view your enterprise assets.	Connect+
Manage Password Rule	Users can configure your password rule.	Connect+
Export Setpoint File	Users can download Setpoint File from the controller.	Connect+
View Audit Log	Users can view the audit log.	Connect+
Obtain Controller Information	Retrieves all information possible for current level.	Connect+ & Controller
Backup	Back up one or more controllers at a given level.	Connect+ & Controller
Controller Logs and Stats	Retrieves log data for various diagnostic information types from the controller.	Connect+ & Controller
Terminal Mode	Shows the native UI for the current controller	Connect+ & Controller
Retrieve Logs	Retrieves Point Logs for current level requested.	Connect+ & Controller
Configure Advisory Purge	Users can choose to store a certain number of advisories in the system for the tree node selected.	Connect+
Upload Description File	Users can send a Description File to a controller.	Connect+ & Controller
Remove Description File	Users can remove Description File from a controller.	Connect+ & Controller
Firmware Transfer	Transfer firmware to a set of controllers.	Connect+ & Controller
Restore	Restore setpoints to a controller.	Connect+ & Controller
Firmware Apply	Applies the Firmware to a controller.	Connect+ & Controller
Firmware Transfer	Transfer the firmware file to the a controller.	Connect+ & Controller
Add Application	Adds one or more applications to a controller.	Connect+ & Controller
Refresh Point List	Retrieves the listing of points for the current level.	Connect+ & Controller
Configure Unit Backup	Users can choose to store a certain number of backups in the system for the unit selected.	Connect+

Table A-1

Privilege	Description	Access Needed
Edit Application Instance	Edit an application instance which will be saved on a controller.	Connect+ & Controller
Get Live Advisories	Users can use the retrieve advisories for the controller.	Connect+ & Controller
Manual Defrost	Users can start a defrost for a freezer or refrigerated case that is outside its normally scheduled routine.	Connect+ & Controller
Modify Point	Modifies a point value.	Connect+ & Controller
Override	Overrides a point value.	Connect+ & Controller
View Network Status	Users can view the connected devices of a controller.	Connect+ & Controller
Setpoint Broadcast	Broadcasts setpoint functionality.	Connect+ & Controller
Delete Application Instance	Users can delete an application instance from a controller.	Connect+ & Controller
Configure Log Purge	Users can configure purging for point logs.	Connect+
Configure Advisory Snooze	Users can set a snooze duration for the selected node in the tree.	Connect+

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 - Privileges Versus E2 Protocols

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 - Privileges Versus E3 and Site Supervisor Protocols

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 - Privileges Versus XWEB Server Protocols

Visit our website at copeland.com/en-us/products/controls-monitoring-systems for the latest technical documentation and updates.
For Technical Support call 833-409-7505 or email **ColdChain.TechnicalServices@Copeland.com**

COPELAND