Connect+

Administrator User Guide

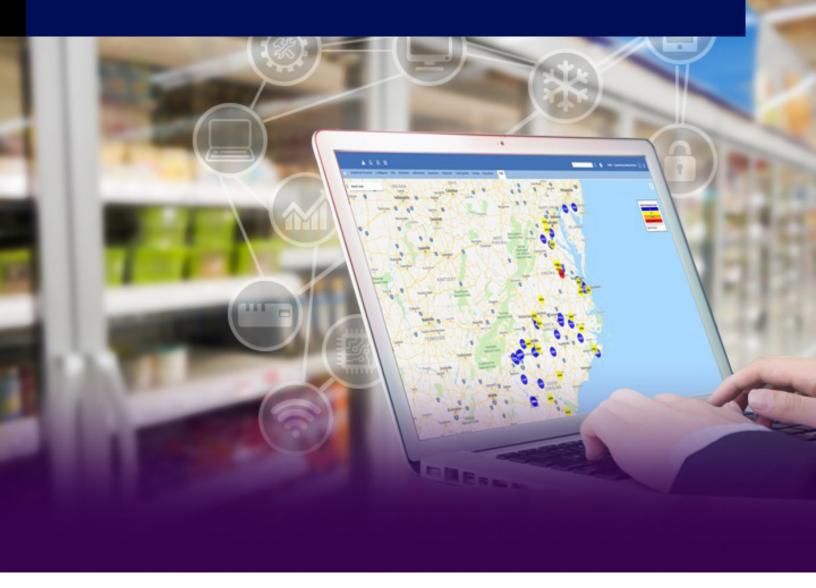




TABLE OF CONTENTS

1.	Getting Started with Connect+	1
	1.1 What Connect+ Can Do	1
2.	Onboard Stores	2
	2.1 Become Familiar with Store Assets Hierarchy	2
	2.2 Onboard Directories	3
	2.2.1 Add Parent Directory	3
	2.2.2 Add Subdirectory	3
	2.3 Adding Sites	4
	2.4 Add Control System and Obtain Controller Information	5
	2.4.1 Configuring the Site Supervisor/E3 and E2 to Communicate with Connect+ Mixed Sites	6
	2.4.2 Replace the Controller with New Protocol	11
3.	Onboard Users	13
	3.1 Create User Group to define Privilege and Sites Access	13
	3.2 Create User	15
	3.3 User Expiration	17
	3.3.1 Configure User Expiration Type	17
	3.3.2 Reactivate User	18
	3.4 User Lockout	18
4.	Complex Password	
	4.1 Enable Complex Password	19
	4.2 Configure Password	19
5.	Configure Advisory Receiving and Advisory View	20
	5.1 Get Familiar with Advisories	20
	5.2 Configure Advisories Received from Controller	20
	5.3 Advisory Receiver Commission	22
	5.4 Enable Advisory Map	24
6.	Configure Advisory & Graph Map Manager	25
	6.1 Advisory & Graph Mapping	25
	6.2 Point & Critical Information Mapping	26

7.	Со	onfigure XWEB Mapping	28
	7.1	1 Download XWEB Server Device Map File	28
	7.2	2 Configure XWEB Server Device Map File	29
		7.2.1 Configure XWEBEVOApplicationTypeMap.csv file	29
		7.2.2 Configure XWEBEVOUIDMapping.csv file	30
		7.2.3 Configure XWEBEVOSetpointTemplate.csv file	30
		7.2.4 Configure Aliases File	33
-	7.3	Upload XWEB Server Device Map File	33
8.	Sys	ystem Schedule Configuration	34
9.	En	nable Advanced Security for Admin Organization (Optional)	36
	9.1	1 Multi-Factor Authentication	36
		9.1.1 Configure Multi-Factor Authentication	36
		9.1.2 Login with Multi-Factor Authentication	36
	9.2	2 Single Sign-on	
		9.2.1 Configure Single Sign-on	37
		9.2.2 Login with Single Sign-on	38
		9.2.3 Privilege of New User Login with Single Sign-on	39
		9.2.4 Auto-binding SSO User Account with Connect+ User	39
10	. C	Configure Report	40
	10	0.1 Configure Energy Analysis Report	40
	10	0.2 Configure Alarm Summary Report	41
	10	0.3 Configure Insight Enterprise Report	42
Ap	per	endix A: Group Privileges, Descriptions, and Protocol Access Levels	44

1. Getting Started with Connect+

1.1 What Connect+ Can Do

Connect+ is designed for <u>Store Manager, Technician, Food Safety Manager, Energy Manager and Regional Managers</u> 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 **<u>step-by-step guide for Administrators</u>** 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 <u>Navigation Tree</u> of the Connect+ landing page interface, a Store Hierarchy is reflected by the navigation tree comprising <u>Directory, Site, Control</u> <u>System, Unit, Application Type, Application and Point Levels.</u>

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. <u>Input, Output</u> or <u>Parameters</u>. 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**.

COPE				
Site Directories				
Add Directory	Points	~	0	0
Site Directories				

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.

Directory Configuration				
Name	MH_Kennesaw TechSupport			
Parent Directory	🗸			
Address 1				
Address 2				
Customer Logo				
Country	United States 🗸			
City				
State/Province/Region	Georgia 🗸			
Zip/Postal Code	30144			
Cancel	Save			

2.2.2 Add Subdirectory

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

Site Directories
🖨 🖿 MH_Kennesaw TechSupport
🖶 🖿 A
🕀 💼 Europe
🕀 🛅 Fresh
🕀 💼 Pickup
🕀 🖿 Go
🛃 🚞 PNow

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.

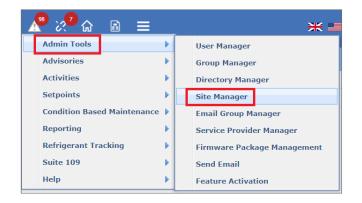
Directory Configuration			
Name	Α		
Parent Directory	MH_Kennesaw TechSupp 🗸 🗸		
Address 1			
Address 2			
Customer Logo	1		
Country	Singapore V		
City			
State/Province/Region			
Zip/Postal Code			
Cancel	Save		

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.

MH_Kennesaw TechSupport					
2	Advisory Map				
	Views		►		
	Configure		🔥 Add Si	te	
	File		🔂 Add Di	recto	ry
	Activities		👩 Edit Di		
	Activities		🛅 Delete	Dire	ctory
	Advisories		Directo	ory Pr	operties
	Summary		•		

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.

Site	e Directories / Admin Tools / Site Manager			
Site Manager				
(Add New			
Si	ite 🔺			
	6			
	Tower			
	cityxi'an			
	ga			
	ga			
	ga			

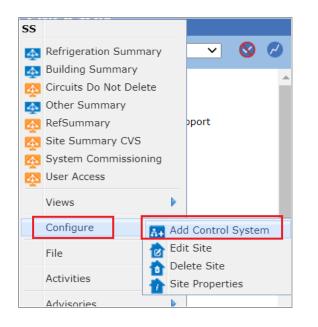
Fill the Site Information based on the field's explanation below:

Name	
Number	
Parent Directory	Dir 🗸
Address Search	 Enter your address and autocomplete with Google Maps
Address 1	
Address 2	
Country	United States 🗸 🗸
City	
State/Province/Region	Alabama 🗸
Zip/Postal Code	
Voice Phone	
Refrigeration Service Provider	~
Lighting Service Provider	~
HVAC Service Provider	~
Time Zone	· · · · · · · · · · · · · · · · · · ·

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.
		Site located time zone.
Time zone	Required	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.

	E2	
Protocol Type	E2	T
Connection Type	IP	T
IP Address		✓ Validate IP Addre
Port	1025	
Advisory Commissioning Port	3001	
Obtain Controller Information Now	 Image: A start of the start of	
	✓ Use this protocol user infor	
Optional	devices at this Control System	
Optional Protocol Username		

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+.

 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.

COPELAND 🔶 🏚 🏦	С	•	۵			
Area Controllers	~			SS Unit04	E2 Unit02	E2 Unit03
Summaries & Dashboards	~					
Layouts	~					
Analysis	~					
System	~					
General System Settings						
File Management & Licensing						
Alarm Communications						
Logging Groups						
Manage Users						
Info						
Protocol Mapping						
Certificate Management						
Reset						

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

COPELAND	÷ 🌣	Â	G	Ŷ		
General Syste	em Properties					
COM Ports	Network Se	ttings	Localiz	ation	System	Values
	Com Port 1	IONet	t-01			
C	om Port 1 baud	9600				
	Com Port 2	Modb	us-02			
C	om Port 2 baud	9600				

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

?	(11)	G	Logout
	Adva	nced	Save

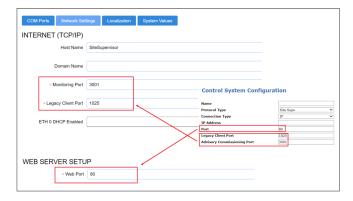
4. The IP address for ETH 0 should be the same IP address used in the control system settings of Connect+. The Site Supervisor or E3 should be the gateway controller in this setup. Contact *ColdChain.TechnicalServices@Copeland.com* to obtain the gateway IP address to be used.

COM Ports	Network Settings	Localization	System Values		
* Lega	acy Client Port 1025		Control System Confi	guration	
ETH 0 D	HCP Enabled		Name Protocol Type	Site Supv	
			Connection Type	IP	`
* ETH	H 0 IP Address	←	IP Port	80	
			Legacy Client Port	1025	

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 > 2 > 2 > 3 > 1 from the Home screen. Press = 2 three (3) times to go to the TCP/IP tab.

COM Ports Network Settings Localization System Values	
Legacy Client Port 1025	
ETH 0 DHCP Enabled	
+ ETH 0 IP Address	Subnet Hask : 0
ETH 0 Subnet Mask 0	DNS Server 1 : 4 DNS Server 2 : 34
+ ETH 0 Default Gateway 1	DNS Server 3 : Default Gateway: 1

- 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 dialout, 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.

General Syster	n Properties					
COM Ports	Network Set	tings Local	ization	System Values		
GENERAL SETUP PARAMETERS						
		* Site Name	Demo			
		* Unit Name	Rack A	\		
		UnitNumber	- 1		J	
		Group Name	DEMO			
			_			

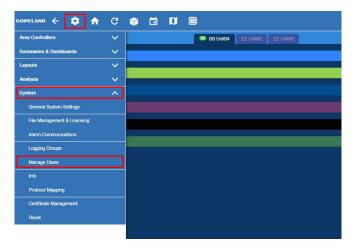
To view the Group Name of the existing E2 controllers on site, press > ? > ? > ? from the Home screen. Press F2 four (4) times to go to the **Peer Network** tab.

1-22-21 🔹 🥝 🛄 se Ctrl-X to Se		CX-400 Unit 5 SETUP	fi Full	9:34:05
C1: General	C2: Eng Units	C3: Serial	C4: TCP/IP	C5: Peer Netwr
C6:	C7: System	C8: Sys Alarms	C9:	C0:
	Gener	al Setup: GENERAL	SERV	
Enable Encr E2 Peer Por Accepter De	re : Ethernet Typt : No t : 7238 Play : 0 Pout : 300 Reout : 30			

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.

Ð	Create a User		
user	0	۴	Ú

Choose the user role for the user account created.

User Name	demo	Actual Name	demo
 Password 		Confirm Password	
Contact Informat	ion		
Email	Email	Mobile Phone(SMS)	Mobile Phone(SMS)
Office Phone	Office Phone		
User Information	1		
Select User Role:	Energy Manager	User Description	User Description
	Non-Technical End User ①		
	 Monitoring Staff 		
	🖲 Technician 🕚		
	System Admin ●		

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

User Information	
* Select User Role:	O Energy Manager
	Non-Technical End User 1
	O Monitoring Staff
	O Technician
	O System Admin
	Create a User Role

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

New Rol	e	×	
∗ Role Name	Role Name This field is required		
Template	Monitoring Staff	~	
Applications	1		
Send Applica	tion Commands		
Edit Application			
Update Application Set Points			
Add / Dama.	• • • • • • • • • • • • • • • • • • •	-	
		Save	

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.

?	۰	6	→ Logout
			Save

8. On the existing E2 controllers on site, additional user credentials must be setup. To do this, press >> >>
>> >> >> >> >> >> >> >> >>

01-22-21 🔹 🌈 🔟		-400 Unit ACCESS SI		FULL		9:55:11 <mark>*ALARM*</mark>
Access level guidelines: 1 3		g/Override			tpoint/B <u>m</u> inistra	
Level Required for : Set	Point	Bypass	Override	Config	Alarm	Ack
Refrigeration Control:	2	2	3	3	3	
Building Control :	2	2	3	3	3	
Advanced Control :	2	2	3	3	3	
Common Control :	2	2	3	3	3	
Enable Detailed Transaction	n Loggin	g: No	Enable	Global	Log-On:	Yes
Users : Username USER #1 : USER USER #2 : demo	*	assword *** ***	Auto Log 0:3 0:3	9	Access 4 1	evel.
Enter 1 to 4 User's acces	s level					
F1: ADD USER F2: DELETE	USER				F5:	CANCEL

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 **S** 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.

91-22-21 🗕 🌈 📧	E +∳ CX-4 USR A	00 Unit CCESS SE		FULL		9:55:11 <mark>*ALARM</mark> *
Access level guidelines: 1 3	= View = Config/	Override	2 = Ch 4 = Sy		tpoint/B <u>m</u> inistra	
Level Required for : Set	Point B	ypass	Override	Config	Alarm	Ack
Refrigeration Control:	2	2	3	3	3	
Building Control :	2	2	3	3	3	
Advanced Control :	2	2	3	3	3	
Common Control :	2	2	3	3	3	
Enable Detailed Transaction	n Logging:	No	Enable	Global	Log-On:	Yes
Users : Username USER #1 : USER	Pas ***	sword	Auto Log 0:3		Access 4	Level
USER #2 : demo	***	×	0:3	8	4	7
Enter 1 to 4 User's acces	s level					
F1: ADD USER F2: DELETE					F5:	CANCEL

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.

Name	Site Supv		
Protocol Type	Site Supv	~	
Connection Type	IP	~	●http ○https
IP Address			🗸 Validate IP Addre
Port	80		
Legacy Client Port	1025		
Advisory Commissioning Port	3001		
Obtain Controller Information Now	<		
Optional Protocol Username	Use this protocol devices at this Contr		on for access to the
Protocol Password	••••		

- 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.

Control System Configu	uration	
Name	Site Supv	
Protocol Type	Site Supv	~
Connection Type	IP	V OHTTP OHTTPS
IP Address		Validate IP Addres
Port	80	
Legacy Client Port	1025	
Advisory Commissioning Port	3001	
Obtain Controller Information Now		
Optional	✓ Use this protocol devices at this Conti	user information for access to the rol System
Protocol Username	demo	
Protocol Password		

A. Verify Control System Connection

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



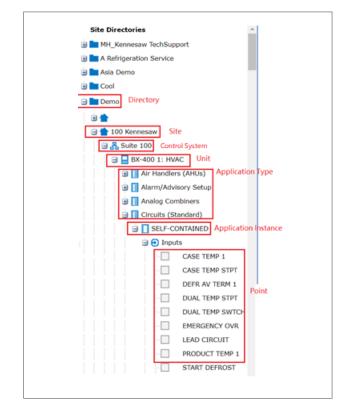
Usually, you can validate the Controller Connection by accessing the **File** > **Terminal Mode** from the right-click menu of the Site Supervisor, E3 or E2 once Obtain Controller Information is successful.

PELAND	🏘 Site Supervisor - Google Chrome	- 🗆 ×
🗇 Refresh 🛛 Active Points 🛛 🗸 🔇	🔰 🔺 Not secure cnxa1er-drs018/copeland/servlet/HTTPSessionProxyService/18529646/?title=10.161.92.190-10.161.92.190-SR:SS%20Unit01#/sys	temsummary
😐 💼		
😐 🚖	copeland — 🏟 🏦 C 🧊 🖬 🗊 📰 🛛 🤶 🌲	🕞 Logout
😐 📥		C
😐 📥		
😐 📥	System Summary E2 Unit04 SS Unit01 SS Unit05 Collapse all Expand all	Edit Save
😐 📥		
R:SS Unit01	Refrigeration (1)	
Summary		
RvR Recommendations	▶ * A HVAC (0)	
Repair vs. Replace Collection		
Views 🕨	► ♀ Lighting (0)	
Configure		
File Export Setpoint File	▶ ★ Energy (0)	
Activities Controller Logs and Stats		
Advisories	▶ o Other (0)	
Summary Restore		
Setpoints Upload Description File	▶ (} System (5)	

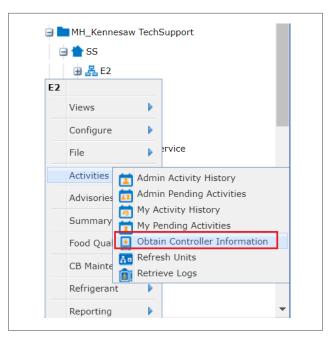
	Î 🎯 🕑 💤 🕘 🔛 🕈 🕼 🥺 🙆
۰	Site Directories / E2 Unit04
😟 🏠	
۵	Terminal Mode
🖷 🌰	
۵	
۵	01-26-21 0 00 cz (X-400 Unit 3 0 14:55:26 Press 'Log In/Out' to Log On CX DEV SUMMARY
👜 🌰	HUAC CONTROL REFRIGERATION
😐 📥	INSIDE RH NOME % NAME STATE TEMP
ė 🛨	AHU001 SPACE: NON[NO] cir defrot .Refr NONE CSForLog .Refr NONE
Ġ "Я	FAN OFF CSTOLOG
🖶 🚍 SR:SS Unit01	STATE UNOCC
🖃 🔜 CX-400 3: E2 Unit04	DEHUM INACTV ANTI-SUKAT DEVPOINT NONE
CX-400 3: E2 Unit04	NAME &ON
Summary p	AS 801 8
RvR Recommendations	
Repair vs. Replace Collection	
Views	LIGHTING SENSOR CONTROL TIME SCHEDULES
Configure 🕨	LIGHT LEVEL NONE FTC NAME VALUE OUT NAME OUTPUT NAME BYPASS OUTPUT DSENSOR001 NOTACT OFF TSCHEDULE001 NOTACT
File () Export Setpoint File	LCONTROL001 OFF LTS OVRD-30% NONE OFF
Activities Backup	sen'sor' NONE OFF
Advisories Controller Logs and Stats	
Summary Restore	
Terminal Mode	
Setpoints Upload Description File Food Quality View Network Status	Press enter for a list of actions.
Configure Backup	\sim F1: AHU \perp F2: Lighting \downarrow F3: circuits \downarrow F4: sensors \downarrow F5: setup $_{ m 2}$
Configure Log Purge	F1 F2 F3 F4 F5
CB Maintenance	
Refrigerant 🕨	
Remote Dialout Setup Sensor Control AV	disconnect Log In/Out
B Sancar Control DV	

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.

'iew B <mark>y</mark> :	🔘 Site 🛛 🔘 Contr	ol System 🛛 🔘 Unit	Application Type	Application Instance	C Reset Filters			
Directory 🔺	Parent Directory	Address 1	Country	City	State/Province/Region	Zip/Postal Code	Num	nbe
			ALL	*				
Mexico	Mexico		Mexico				0	
AM			United States		Georgia		6	
MH_Kennesaw			United States		Georgia	30144	0	
Refrigeration			United States		New York		0	
AA	A		Singapore				0	
А	А		United Kingdom				5	
Fresh	А		United States		Washington		0	
Fresh Pick	A		United States		Alabama		0	
Go	A		United States		Alabama		0	
	А		United States		Washington		0	
Asia Demo			India				0	

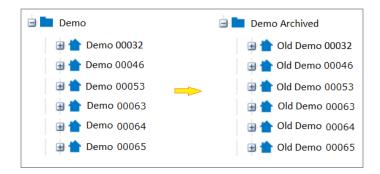
2.4.2 Replace the Controller with New Protocol

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.

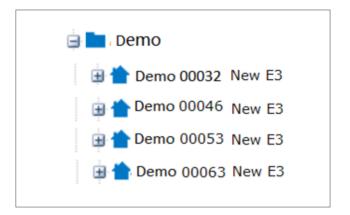
1. Archive your existing data.

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.

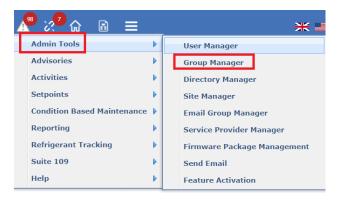
Group Configuration Group Name Protocol Access Level Controller Security	Energy M&T Technician Supervisor (400)		Site View Permissions (A directory is not automatically expanded if all sites under it selected or no site under Site Directories Demo Demo Demo Demo 00032 New E3
Protocol	Username	Password	
ComTrol 6k	USER		🗃 🗔 譮 Demo 00046 New E3
ComTrol Obix	copeland		🔀 🗌 🁚 Demo 00053 New E3
E1	USER		😠 🛄 🁚 Demo 00063 New E3
E1 XML	USER		🖃 🗹 🖿 Demo Archived
E2	USER		Vid Demo 00032
E2 XML	USER		☑ 📩 DId Demo 00046
E3	user		
Manual XML	USER		- 🗹 🁚 Old Demo 00053
Reflecs Enhanced XML	USER		- 🗹 👚 Old Demo 00063
Site Supv	user		

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.

e	Reset Filters 🛛 🔾 Add New
Gro	up Name 🔺
~	Template_ViewOnly
a	
G	S Only
A	Admin
A	DMIN
A	dv Demo
A	dv Demo Group

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

Controller Security Protocol ComTrol Obix ComTrol Obix ComTrol Obix C E1 SML E2 SML E3 Manual XML U Reflecs U	copeland USER USER USER ADVDEMO USER	-ernam	Sec	Section 1 tion 2 Password			Site Directories
Bypess Controller Security Protocol Com Trol Obix Cr D U E1 U E1 XML U E2 XML U E3 U Renual XML U Reflecs U	copeland USER USER USER ADVDEMO USER	sernam	e	Password			
Protocol ComTrol Obix c D E1 E1 XML U E2 E2 E3 Manual XML U Reflecs U	copeland USER USER USER ADVDEMO USER	sernam	e	Password			\ominus 🔽 🛅 Demo
ComTrol Obix c D U E1 A U E1 XML U E2 XML U E2 XML U E3 U Manual XML U Reflecs U	copeland USER USER USER ADVDEMO USER	sernam		•••••			– 📝 ╆ 100 Kennesaw
D U E1 U E1 XML U E2 XML 4 E2 XML 4 E3 U Manual XML U Reflecs U	USER USER USER ADVDEMO USER						- 🗸 🌰 152 Lab
E1 U U U U U U U U U U U U U U U U U U U	USER USER ADVDEMO USER						V 📥 154 Atlanta
EI XML U E2 A E2 XML U E3 u Manual XML U Reflecs U	USER ADVDEMO USER						
E2 A E2 XML U E3 U Manual XML U Reflecs U	ADVDEMO USER			••••			250 Desk
E2 XML U E3 u Manual XML U Reflecs U	USER			••••			🗔 🌰 B
E3 u Manual XML U Reflecs U				••••			- 🗌 📥 CC200
Manual XML U Reflecs U						Section 3	- 🗌 🌰 C
Reflecs U	user			•••••			- D
-	USER			••••			
	USER			••••			
Reflecs Enhanced XML U	USER			••••			🔄 📥 Demo
Site Supv u	user						- 🗌 🃥 DFrame
TAC Xenta 401 U	USER			••••			– 🗌 📥 LT Desk
XWEB Server 300/500 A	Admin			••••			- 🗌 🏪 Matt E2
XWEB Server 3000/5000 A	Admin						Xweb
XWEB Server EVO A	Admin			••••			Xweb Demo
Privileges							- 🗌 🌰 Xweb700
All Privileges My User Info		_	Privileges Ass My User Info	signed to this Group	A		🖶 📃 🖿 DEV/QA
My Pending Activities			My Pending Acti	ivities	_		
My Pending Activities for Tree Item	- 1	_		ivities for Tree Item	- 1		
My Activity History		_	My Activity Hist		_		
My Activity History for Tree Item		_		ory for Tree Item	Se	ection 4	
Admin Pending Activities		_	Admin Pending				
Admin Pending Activities for Tree Item	>			Activities for Tree Item			
Admin Activity History		_	Admin Activity H				
Admin Activity History for a Tree Item		_		History for a Tree Item			
Add User		_	Add User				
Edit User			Edit User				
Delete User			Delete User				
Add Group	-		Add 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.

 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 (*Recommended*). 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.

	Site Supv	
Protocol Type	Site Supv	•
Connection Type	[]P	BHTTP CHITPS
IP Address	(Validate IP Address
Port	80	
Legacy Client Port	1025	
Advisory Commissioning Port	3001	
Obtain Controller Information Now		
	Use this protocol user informa	tion for access to the
	devices at this Control System	-
Optional Protocol Username Protocol Password]

- 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)
- 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.

User Manag	jer					
						Show
C Reset Filters	📀 Add New					
Username 🔺		First Name	Last Name	E-mail	Group Name	
					ALL	*
1		1	1	username@copeland.com	ADMIN	
administrator		System	Administrator	username@copeland.com	ADMIN	
bypass		bypass	bypass		bypass	

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

Site Directories / Admin Tools / Setup /	User Manager / User Configuratio	n			
User Configuration		Units			
Login ID			English	Metric	Global
First Name			Lingitsii	Pictru	Ciobul
Last Name		Temperatu	e	Fahrenheit (DF)	~
New Password (case sensitive)		Temp. Char	ge	Delta Fahrenheit (DDF)	~
E-mail		Temp. Rate	Change	degrees F/hour (DFH)	~
Group Name	Search group here	 Pressure, L 	arge	pound/sq in (PSI)	~
User Expiration Type	Never Expired	♥ Pressure, S	mall	in of water (INW)	~
		Velocity, Ai	,	feet/minute (FPM)	~
Preferences		Velocity, Li	lnid	gallons/minute (GPM)	∨
		Liquid Volu	me	gallons (GAL)	∨
Show GS Screen Edit Tool		Volume Flo	N	cubic feet/minute (CFM)	v
Enable Home Page		Current		amperes (A)	~
Hide Nav Frame		Light		foot-candles (FTC)	~
Enable GS Screen Auto Log Off		Weight		pounds (LBS)	~
		Enthalpy		Btu/lb	~
Cancel	Save				

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.

Proper	ties Manager Jaru Properties V	Viewer and Installation Override	e Manager
14 propertie	es found.		
Case Sensitive	Reset Filter		
Category			
	global		
JaruSystem	GlobalEngineeringUnits.Current	amperes (A)	
JaruSystem	GlobalEngineeringUnits.Heat	Btu/lb	
JaruSystem	GlobalEngineeringUnits.Light	foot-candles (FTC)	
JaruSystem	GlobalEngineeringUnits.LiquidVolume	gallons (GAL)	
JaruSystem	GlobalEngineeringUnits.PressureLarge	pound/sq in (PSI)	
JaruSystem	GlobalEngineeringUnits.PressureSmall	in of water (INW)	
JaruSystem	GlobalEngineeringUnits.TempChange	Delta Fahrenheit (DDF)	
JaruSystem	GlobalEngineeringUnits.TempRateChange	degrees F/hour (DFH)	
JaruSystem	GlobalEngineeringUnits.Temperature	Fahrenheit (DF)	
JaruSystem	GlobalEngineeringUnits.VelocityAir	feet/minute (FPM)	
JaruSystem	GlobalEngineeringUnits.VelocityLiquid	gallons/minute (GPM)	
JaruSystem	GlobalEngineeringUnits.VolumeFlow	cubic feet/minute (CFM)	
JaruSystem	GlobalEngineeringUnits.Weight	pounds (LBS)	
JaruSystem	useSiteTreeAndGlobalSearchSecurity	false	

3.3 User Expiration

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

3.3.1 Configure User Expiration Type

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

Security Mode	
Local Security DLDAP Integ	ration
User Configuration	
Login ID	Login
First Name	First Name
Last Name	Last Name
New Password (case sensitive)	••••
E-mail	username@copeland.com
Group Name	ADMIN V
User Expiration Type	Never Expired 🔻
Preferences	Never Expired Expire By Calendar Auto Expire By Interval

There are three kinds of user expiration types:

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

Security Mode	
Local Security OLDAP Integration	on
User Configuration	
Login ID	
First Name	
Last Name	
New Password (case sensitive)	
E-mail	
Group Name	ADMIN
User Expiration Type	Expire By Calendar 🔻
User Expiration Date*	

• 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,

Local Security O LDAP Integration User Configuration	n
Jser Configuration	
ogin ID	
First Name	
ast Name	
New Password (case sensitive)	
-mail	
Group Name	ADMIN 🔻
Jser Expiration Type	Auto Expire By Interval 🔻
Jser Expiration Interval	select one 🔻
Jser Expiration Date*	

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

User Configuration	
Login ID	
First Name	
Last Name	
New Password (case sensitive)	
E-mail	
Group Name	ADMIN V
User Expiration Type	Auto Expire By Interval
User Expiration Interval	select one 🔻
User Expiration Date*	Select one Months Months Months Months
Preferences	

current date plus expiration interval, otherwise message will be prompted when clicking **Save** button.

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

Site Directories / Admin Tools / Setu	p / User Manager / User Configuration
User Expiration Date must greate	r than Expiration Interval
User Configuration	
Login ID	Login
First Name	First Name
Last Name	Last Name
New Password (case sensitive)	••••
E-mail	username@copeland.com
Group Name	ADMIN T
User Expiration Type	Auto Expire By Interval
User Expiration Interval	3 Months *
User Expiration Date*	05/03/2019

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.

Enter a valid Login ID and password	rd
Login ID	
Login	
Password	
•••••	

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.

			-
	login		
JaruStatsProperties	numberOfLoginTimes	5	

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

_ogin
lumber of login attempts exceeded, count is locked. o unlock your account, please reset ogin ID or password by clicking the nk. Ir login after 24 hours.
ogin ID
orgot Login ID?
ogin
assword
orgot Password?

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:

Prope	rties Manager Jaru Pr	operties Viewer and Installation Override Manage
1 properties	s found.	
Case Sensitive	Reset Filter	
Category		Value
	complex	
JaruSystem	EnableComplexPassword	true

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.

Login	
Password w	ill expire in 9 day
Login ID	
Forgot Login 1	(D?
userExpire	
Password Forgot Passwo	ord?
	Login
	Reset

4.2 Configure Password

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

Minimum password length of	8	-	characters	
Maximum password age of	90	-	days	
Remind user to reset password from	14	-	days before expirat	tion
Password must not match previous	4		passwords	
REQUIRED CHARACTERS			1	
Minimum Uppercase Number of			1	
Minimum Lowercase Number of			1 🛫	
🗹 Minimum Numeric(0-9) Number of			1 🌐	
Minimum Non alpha-numeric(e.g. !,#,\$,	%) Nu	nbe	er of 1	

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.

Minimum password length of	8	÷	charact	ers
🗹 Maximum password age of	90	*	days	
Remind user to reset password from	14	*	days be	efore expiration
Password must not match previous 4 🗘 passwords			rds	
Require password reset on first time log	gin			
EQUIRED CHARACTERS				
Minimum Uppercase Number of			1	
Minimum Lowercase Number of				
✓ Minimum Numeric(0-9) Number of				
Minimum Non alpha-numeric(e.g. !,#,\$				

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.

Reset Your Password	
Current Password	
•••••]
New Password	1
Retype New Password	-
Reset	

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 <u>State, Type, Priority</u> <u>and Urgency Level</u>.

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	Туре	Priority
High	Active	Fail or Alarm	1-20
Medium	Active	Notice	1-50
weatum	Active	Fail or Alarm	21-50
	Active	All	51-99
Low	Return to Normal	All	1-00

Table: Danfoss

Advisory Urgency Level	State	Туре	Priority
High	Active	Severe or Critical	NA
Medium	Active	Normal	NA
	Active	Log Only	NA
Low	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.

🔇 Refresh Active Points 🔻 🥑 💋	Graphical Screens	Configure	File	Activities	Advisories	Summary	Set
Site Directories	日合合合						
÷ 🖿							
🕀 🌰 00083 - New Lenox IL	Site Directories / DWT / 00083	- New Lenox IL	/ Site C	onfiguration			
🗎 🖿 MOR							
😟 📩 OFA	Site Configuration						
🗄 🚞 OLA							
🕀 🛅 RPB Test	Name	00012 - New Len	ox IL				
🗉 🚞 SPR	Number	83					
🗄 🛅 TUL	Parent Directory	DW					
	Address Search	123 East Hig Illinois, Unite	jhway, id States				
	Address 1	123 East Highway	ý				
	Address 2						
	Country	United States		Ŧ			
	City	New Lenox					
	State/Province/Region	Illinois		Ŧ			
	Zip/Postal Code	12345					
	Voice Phone						
	Refrigeration Service Provide	BR		•			
	Lighting Service Provider			T			
	HVAC Service Provider			•			
	Time Zone	(GMT -06:00) Centra				
				0	인 (Please get a	list of sites at f	ìrst.)
	MSS Site Name	00083 DWT		T	Get a List	of Sites	
	Cancel		100	Save			

 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.

Prope	rties Manager Jaru f	Properties Viewer and Installation Override Manager
4 propertie	s found.	
Case Sensitive	Reset Filter	
Category		
	mss	
JaruSystem	MSSWebServiceBackupURL	http://mss-web-service/jsonMssExport
JaruSystem		
JaruSystem		
JaruSystem	MSSWebServiceUser	SM ALDI

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:

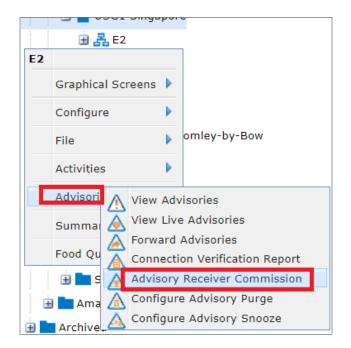
Internet	12.155.208.49:3001
VPN	12.155.208.137:3001 Primary 12.155.208.138:3001 Secondary
AT&T Cell Modem	10.56.1.33:3001

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

5.3 Advisory Receiver Commission

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

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



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

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

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

Field	Validation	Notes		
Fail Filter Priority	Required	The priority should be 1-99.		
Notice Filter Priority Required		The priority should be 1-99.		
Control System ID	Required	It is the unique identifier for that set of controllers configured with monitoring. This will be set automatically by Connect+ if there is no unique ID in the system.		
Original Primary Destination Address	Required	This field information is received from the controller. It cannot be edited.		
New Primary Destination Address		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		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**.

Retrieved Parameters	
	Advanced Parameters? Show Hide
Daily Connection Test Time:	3:38 AM 👻
Alarm Filter Priority:	20
Fail Filter Priority:	20
Notice Filter Priority:	20
Control System Id:	f67c1c54ad
Original Primary Destination Address:	
New Primary Destination Address:	
Original Backup Destination Address:	
New Backup Destination Address:	
Connection Delay:	2
Maximum Connection Time:	5
Modem Init String:	ATE0V150=1510=408.D28.Q5N0%C08.K08.1
Modem Baud Rate:	-15872
Maximum Modem Connect Time:	45
Dial-Out Prefix:	9w
Use Dial-Out Prefix:	
Transmit Alarms:	V
Transmit Fails:	
Transmit Notices:	₹
Return to Normal:	(*)
Randomize Retry Time:	
Number of Daily Connection Tests:	1

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.

Advisory Receiver (Commission
Advisory Receiver Commission	activity was comple
Daily Connection Test Time:	3:38 AM
Alarm Filter Priority:	20
Fail Filter Priority:	20
Notice Filter Priority:	20
Control System Id:	
Original Primary Destination Add	lress:
Original Backup Destination Add	ress:

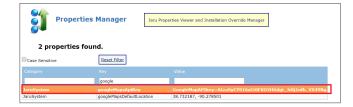
To check the advisories received in the controller, go to the **Advisory View** page.

5.4 Enable Advisory Map

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

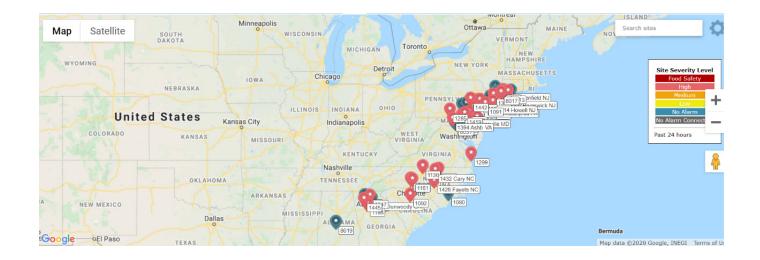
Super User	Þ	Logging Control
Admin Tools	×.	E2 Protocol Logging Control
Advisories	Þ	Properties Editor
Activities	×.	dbframe
Setpoints	×.	Command Line Tools
Condition Based Maintena	nce 🕨	Statistics
Reporting	×.	Advisory&Graph Map Manager
Refrigerant Tracking	•	XWEB Server Device Map EVO Manager
Suite 109	×.	XWEB Server Device Map 3000/5000 Manage
Help	×.	XWEB Server Device Map 300/500 Manager
		Fix Obsolete Reason
		Fix Missing Benchmarks
		TAC Xenta 401 Setpoint Template Manager

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

Site Directories					
🗄 🔚 A					
🗐 🗖 MH_Kennesaw TechSupport					
MH_Kennesaw TechS	upport				
\land Advisory Map					
Views	F				
Configure	F				
File	F				
Activities	F				
Advisories	F				
Summary	F				
Setpoints	Þ				
Food Quality	F				
Energy	F				
CB Maintenance	F				
Refrigerant	F				
Reporting	F				



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.

Adv	isoı	ies View									
Hig		260 Food Safety 4	Medi		Low 5		All				
-		ate Current Month	~	Time Perspective:	L	~					
C Re	eset F	Ilters G Refresh Ad	visories 🕤 R	Received Date	at Site	Туре	State	Source	Deise	Advisory Message	Course 3
	Au	Occurrence Date +	Age	Received Date	Site		 Active 		PHOT	Auvisory message	Source T All
•		11/4/2020 8:10 AM	19.7 d	11/4/2020 8:13 A	M Store #1	Alarm	Active	CASE TEMP 6	20	Case Temp Hi Limit Exceeded	Device
٠		11/4/2020 7:15 AM	19.8 d	11/4/2020 7:18 A	M Store #1	Alarm	Active	CASE TEMP 1	20	Case Temp Hi Limit Exceeded	Device
		11/4/2020 7:14 AM	19.8 d	11/4/2020 7:15 A	M Store #1	Alarm	Active	FILTERED PRES	20	High Suction Limit Exceeded	Device
		11/4/2020 6:14 AM	19.8 d	11/4/2020 6:15 A	M Store #1	Fail	Active	RX-300 1: RACK A	20	Device absent from network	Device
		11/4/2020 6:14 AM	19.8 d	11/4/2020 6:15 A	M (2) Store #1	Fail	Active	RX-300 1: RACK A	20	Device absent from network	Device

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

🗶 🔊 🕼 🗈 🔳		💥 📕 English
Super User	•	Logging Control
Admin Tools	Þ	E2 Protocol Logging Control
Advisories	Þ	Properties Editor
Activities	Þ	dbframe
Setpoints	₽	Command Line Tools
Condition Based Maintenance	•	Statistics
Reporting	Þ	Advisory&Graph Map Manager
Refrigerant Tracking	₽	XWEB Server Device Map EVO Manager
Help	₽	XWEB Server Device Map 3000/5000 Manager
Point & Critical Infor	ma	XWEB Server Device Map 300/500 Manager
		Fix Obsolete Reason
Download	the	Fix Missing Benchmarks
Upload		TAC Xenta 401 Setpoint Template Manager

Advisory & Graph Mapping							
Download	the currently active Advisory&Gra	the currently active Advisory&Graph Mapping.csv file.					
Delete	the overridden Advisory&Graph M	the overridden Advisory&Graph Mapping.csv file. created 08/14/2019 10:51:07					
Upload	Browse No file selected.						
Point & Critical Information Mapping							
Download	the currently active Default Point8	the currently active Default Point&CriticalInfoMapping.csv file.					
Upload	Browse	No file selected.					

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

ry message Ad	ction	Execution_info
emp Hi Limit Exceeded g	graph point	CASE TEMP 1;DEFROST;Case Alarm Hi
emp Low Limit Exceeded g	graph point	CASE TEMP 1;DEFROST;Case Alarm Low
(emp Hi Limit Exceeded	emp Hi Limit Exceeded graph point

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.

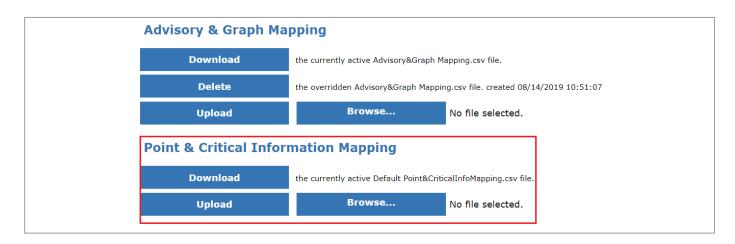
Hi	gh 1 Fa	6 ood Safety 16	Medi	um 0	Low	0		All			
ccurre	ence Da	te Custom Range	~	Time Perspectiv	e: Site Time		✓ from 11	1/01/20	9 to 01/14/21		Go
Ċ R	eset Fil	ters 🖸 Refresh Advis	ories 🕤 R	estore Default For	mat 下 Termina	al Mode					
	Ad	Occurrence Date 🔻	Age	Received Date	Site		Туре	State	Source	Prior	Advisory Message
							All 🗸	Active 💌			case
•		11/25/2020 11:09 AM	1.7 mo	11/25/2020 11:	11 AM	Store #1	Alarm	Active	CASE TEMP 1	20	Case Temp Hi Limit Exceeded
•		11/25/2020 11:09 AM	1.7 mo	11/25/2020 11:	11 AM	Store #1	Alarm	Active	CASE TEMP 1	20	Case Temp Hi Limit Exceeded
•		11/25/2020 11:08 AM	1.7 mo	11/25/2020 11	08 AM	Store #1	Alarm	Active	CASE TEMP 4	20	Case Temp Hi Limit Exceeded
		11/25/2020 11:06 AM	1.7 mo	11/25/2020 11:	08 AM	Store #1	Alarm	Active	CASE TEMP 3	20	Case Temp Hi Limit Exceeded

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.

Α	В	С	D	E	F	G	Н		J
Protocol	Application Type	Point	Setpoint	High limit	Low limit	Defrost	Defrost Ti	meslot	
E2	Circuits (Standard)	CASE TEMP 1	ACTIVE SETPT	Case Alarm Hi	Case Alarm Lo	DEFROST	Defrost Ti	me 1;Defros	t Time 2;D
E2	Circuits (Standard)	CASE TEMP 2	ACTIVE SETPT	Case Alarm Hi	Case Alarm Lo	DEFROST	Defrost Ti	me 1;Defros	t Time 2;D
E2	Circuits (Standard)	CASE TEMP 3	ACTIVE SETPT	Case Alarm Hi	Case Alarm Lo	DEFROST	Defrost Ti	me 1;Defros	t Time 2;D
E2	Circuits (Standard)	CASE TEMP 4	ACTIVE SETPT	Case Alarm Hi	Case Alarm Lo	DEFROST	Defrost Ti	me 1;Defros	t Time 2;D
E2	Circuits (Standard)	CASE TEMP 5	ACTIVE SETPT	Case Alarm Hi	Case Alarm Lo	DEFROST	Defrost Ti	me 1;Defros	t Time 2;D
E2	Circuits (Standard)	CASE TEMP 6	ACTIVE SETPT	Case Alarm Hi	Case Alarm Lo	DEFROST	Defrost Ti	me 1;Defros	t Time 2;D
E2	Circuits (Standard)	CASE TEMP 7	ACTIVE SETPT	Case Alarm Hi	Case Alarm Lo	DEFROST	Defrost Ti	me 1;Defros	t Time 2;D
E2	Circuits (Standard)	CASE TEMP 8	ACTIVE SETPT	Case Alarm Hi	Case Alarm Lo	DEFROST	Defrost Ti	me 1;Defros	t Time 2;D
E2	Circuits (Standard)	CASE TEMP 9	ACTIVE SETPT	Case Alarm Hi	Case Alarm Lo	DEFROST	Defrost Ti	me 1;Defros	t Time 2;D
E2	Circuits (Standard)	CASE TEMP 10	ACTIVE SETPT	Case Alarm Hi	Case Alarm Lo	DEFROST	Defrost Ti	me 1;Defros	t Time 2;D
E2	Circuits (Standard)	CASE TEMP 11	ACTIVE SETPT	Case Alarm Hi	Case Alarm Lo	DEFROST	Defrost Ti	me 1;Defros	t Time 2;D
E2	Circuits (Standard)	CASE TEMP 12	ACTIVE SETPT	Case Alarm Hi	Case Alarm Lo	DEFROST	Defrost Ti	me 1;Defros	t Time 2;D
F2	Circuits (Standard)	PRODUCT TEMP 1	ACTIVE SETPT	Product Alrm Hi	Product Alrm Lo		Defrost Ti	me 1.Defros	t 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.

Super User	•	Logging Control
Admin Tools	₽	E2 Protocol Logging Control
Advisories	₽	Properties Editor
Activities	₽	dbframe
Setpoints	•	Command Line Tools
Condition Based Maintenanc	e 🕨	Statistics
Reporting	•	Advisory&Graph Map Manager
Refrigerant Tracking	₽	XWEB Server Device Map EVO Manager
Suite 109	₽	XWEB Server Device Map 3000/5000 Manage
Help	₽	XWEB Server Device Map 300/500 Manager
	-	Fix Obsolete Reason
		Fix Missing Benchmarks
		TAC Xenta 401 Setpoint Template Manager

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

Download the currently active XWE	BEVOServerDeviceMapping ZIP fil	le.
Upload the currently active XWEBE	VOServerDeviceMapping ZIP file.	Choose File No file chosen

In the zip file, you will see below files:

		Open		
)	解压文件(A)	> X	WEBEVOServerDeviceMapping >
XWEBEVO	1	解压到当前文件夹(X)		^
р		解压到 XWEBEVOServerDeviceMapping\(E)	Na	ame
WinRAR Z	ш	Edit with Notepad++		Aliases
		Process Directory		
		Encrypt for sharing		
		Open Dell Encryption		EVOUIDMappings.csv

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.

³⁰ 次 ²⁴ 谕		🕂 📑 English
Super User	Þ	Logging Control
Admin Tools	Þ	E2 Protocol Logging Control
Advisories		Properties Editor
Activities	Þ	dbframe
Setpoints	Þ	Command Line Tools

Find JaruSystem.isDebugMode and change the value to true.

Propertie	es Manager Jaru Pro	operties Viewer and Installation Override Manage
7 properties fo	ound.	
Case Sensitive	Reset Filter	
Category	Кеу	Value
	deb	
DataCollection	QA.Debug	false
GatherEstimationStatistics	isEstimateDebugEnabled	off
JaruSystem	isDebugMode	true
SyncActivity	isDebugMode	false
XWebServerConfigs	enableDebug	false
XWebServerConfigs	gateway.json.debugContent	false
XWebServerConfigs	proxy.debugProxyContent	false

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

Write this ID in appTypeProtocolUniqueId column.

🖿 🛅 Alarm/ Advisory Setup
🗄 📘 Analog Combiners
🗃 📘 Anti-sweats
🔢 📘 Circuits (Case Ctrl)
Circuits (Standard) 10146673
treeLevel: 4 [XM]
applicationId: 131 ers

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.		
unnedPointName		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. - OR - Enter values specifically for this item: Directory - Demo Enable Setpoint Resolution Service Interval Energy Critical Setpoints Average Price of Power Average Rack Design Load Average Anti-Sweat Design Load Alarm Critical Setpoints		

Setpoint Category

Required

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.



alarmSetpoint

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.	
		It defined as number:	
nativePointType	Required	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.	
	Optional	Identified as the device name: point name, it is used to configure the mapping between the Connect+ and device. For example, XH50:Set.	
supportedDevicePoint		This field is required for XWEB 300/500, but not need for XWEB 3000/5000 and XWEB EVO.	
		Sat the value as TRUE, it will show the point in Satpoint Profile, then you can decide	

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.

Profile Name	•				
Average Pric	e of Power		(WH		
-	k Design Load	K		~	
-	-			·	
	hting Design Load	KW			
Average Ant	i-Sweat Design Load	KW	1		
Select	all Energy Critical Setpoint	Select all A	Alarm Setpoint	Select All	Unselect All
	Application Typ)e	1	Protocol	
± 🗸	Anti-Sweat		XWEB S	erver 300/500	
± 🗸	Circuits (Case Ctrl)		XWEB S	erver 300/500	
+ 🗸	Circuits (Standard)		XWEB S	erver 300/500	
+ 🗸	Expansion Valve		XWEB S	erver 300/500	
+ 🗸	Rack Control		XWEB S	erver 300/500	
+ 🗸	Suction Group		XWEB S	erver 300/500	
+ 🗸	Anti-Sweat		XWEB Se	rver 3000/5000	
+ 🗸	Circuits (Case Ctrl)		XWEB Se	rver 3000/5000	
+ 🗸	Circuits (Standard)		XWEB Se	rver 3000/5000	
+ 🗸	Expansion Valve		XWEB Se	rver 3000/5000	
÷ 🗸	Rack Control		XWEB Se	rver 3000/5000	
÷ 🗸	Suction Group		XWEB Se	rver 3000/5000	
- 🗸	Anti-Sweat		XWEE	Server EVO	
					Alarm Delay
	✓				Defrost Interval
	√				Energy Setpoint Dif
					High Alarm Limit
					Low Alarm Limit
	✓				Setpoint
± 🗸	Circuits (Case Ctrl)		XWEE	Server EVO	
± 🗸	Circuits (Standard)		XWEE	Server EVO	
	Expansion Valve			Server EVO	

setpointServiceSupported

Required

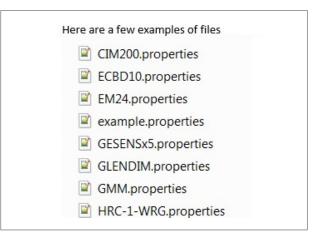
7.2.4 Configure Aliases File

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.

Open Extract files Extract Here	ceMapping •	👻 🚺 Search X 🛃
Extract to XWEBEVOServerDeviceM	spping) Share with 👻 New folder	iii • 🔟 🛛
Git Init Here Git Bash	Name ~	Date modified Ty
Scan for Viruses	Alases EVOApplcationTypeMap.csv	5/18/2016 10:20 AM Fil 5/18/2016 10:23 AM Mi
Open with	EVOSetpointTemplates.csv	5/17/2016 10:20 PM M
Share with	EVOUIDMappings.csv	5/17/2016 10:20 PM M
R TortoiseSVN	•	
Restore previous versions		

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.

Schedule Manager All schedules are based on the server's time zone: (GMT -05:00) Cuba Standard Time - America/Havana (CST) (DST) Show System Schedules						
😳 Add New 🛛 🧤 🕞	Reset Filters					
Name	Туре		User	Schedule	Next Run Ti	
	All	*				
InboundAdvisory	Queu system		system	Every 1 minute	2/4/21 3:20	

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.

Propert	ies Manager	Jaru Properties Viewer and Installation Override
4 properties f	ound.	
Case Sensitive	Reset Filter	
Category	Кеу	Value
	factor	
CondenserMaintenance	slopFactor	0.2
EconomicAlg	SetpointCondenserAlg.c	climate_factor 0.50
JaruSystem	Cluster.barometerAlarm	nCsLoadFactor 30.0
JaruSystem	multiFactorAuthentication	ionModel None

JaruSystem.multiFactorAuthenticationModel =					
Create/Update Overn	ide Value None 🔻				

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.

aruSystem.byPas	s2FAGroups = <u>null</u>
Create/Update Override Value	PSC,NorthStore
 default (lowest possible effec C:\Program Files\Tomcat\web JaruOverrides.properties [database] 	

9.1.2 Login with Multi-Factor Authentication

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

Login with Email

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

Login	L L	Jser Authenticat	tion
Login ID		Iulti-Factor Authentication has been	turned on for your account. I you a security code to verify your acco
login			I you a security code to verify your acco
Password		mail: sername@emerson.com	Send Security Code
••••			
Login	P	Please enter your security coo	de:
			Submit

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

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

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

User Authentication			
Multi-Factor Authentication has been turned on for your organization. Security code would be sent to your email: username@copeland.com			
Number of login attempts exceeded, your account is locked. Please login after 24 hours.			
Security Code			
Security Code 3456	154s		

Login without Email

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

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

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.

🔏 🖉 🏠 🔳 🚍		 💥 🛄 English	۱
Admin Tools	Þ	User Manager	
Advisories	Þ	Group Manager	
Activities	▶	Password Rule Manag	ger
Setpoints	Þ	SSO Manager	
Condition Based Maintenance	▶	Directory Manager	
Reporting	₽	Site Manager	
Refrigerant Tracking	₽	Email Group Manager	
Suite 109	▶	Service Provider Man	ager
Help	Þ	Firmware Package Ma	anagement
IDP Name:	1	Send Email	
IDP Entity ID:		Feature Activation	

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

Connect+	II	DP Server		
SSO Configuration	Copy fron Connect+	A SAML Settings		
SSO Enabled: SP Entity ID: ASC (Consumer) URL: IDP Name:	configure http://sample-only/copeland http://sample-only/copeland bttp://sample-only/copeland okta		http://sample-only/copeland/ssoConsumer.do	
IDP Entity ID: SAML SSO Login URL: X.509 Certificate: Need to provide by customer and configure in Connect+	http://www.okta.com/sample http://sample-123756.okta.com/app 	Audience URI (SP Entity ID) 💿 Default RelayState 💿	Allow this app to request other SSO URLs	
Attirbute Keys(Optional):	doR*iz58nujPvBcZTWUNov o36f%pocJwH6Pt258nujPi vvBcZTWUNov44ghfjnPfhdji ▼ firstName lastName email	Name ID format 🚳	If no value is set, a blank RelayState is sent Unspecified	
Cancel	Save Copy Attribute Keys from Connect+ to IDP Server	ATTRIBUTE STATEMENTS (OPTIONAL		LEARN MORE
		Name Name form	nat (optional) Value fied v user.firstName	Ŧ
		lastName Unspecifier		• × • ×

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	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.

Login	
Login ID	
Password	
Login	
Or	
Login with okta	

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

	okta
	Sign In
Usernar	ne
usernai	me@copeland.com
Passwor	rd
•••••	
🗌 Rem	ember me
	Sign In
Need he	Ip signing in?

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.

User Binding
Welcome juan.guo Please bind your existing Connect+ account with your company credential by filling in your Connect+ Login ID and Password
Login ID
Password
Login Don't have a Connect+ Account?

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.

User _+ Active View	re Actions *		
Applications Groups	Profile		Profile
Attributes		Edit	A profile is a collection of attributes that describe a user in Okta. Some ap
Username	username@copeland.com		and directories can sync attributes wi
login			Okta.
First name firstName	User First Name		
Last name lastName	User Last Name		
Middle name middleName			
The second second			
Honorific prefix honorific Prefix			

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

SAML Settings	Edit
GENERAL	
Single Sign On URL	http:sampleonly123.copeland.org/copeland/ssoConsumer.d 0
Recipient URL	http:sampleonly123.copeland.org/copeland/ssoConsumer.d
Destination URL	http:sampleonly123.copeland.org/copeland/ssoConsumer.d
Audience Restriction	http:sampleonly123.copeland.org/copeland
Default Relay State	
Name ID Format	Email Address
Response	Signed
Assertion Signiture	Signed

User Name username@copelar			
User & Active View L	e Actions *		
Applications Groups	Profile		
Attributes		Edit	Profile A profile is a collection of attributes that describe a user in Okta. Some ap
Username	username@copeland.com		and directories can sync attributes w
login			Okta.
First name			
firstName	User First Name		
Last name	User Last Name		
lastName			
Middle name			
middleName			
Honorific prefix			
honorificPrefix			
Honorific suffix honorificSuffix			

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.

Add New									
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.

Reporting Con	figuration
General Information	Report Template Data Collection Activity
-	Energy Analysis Report for Directory Energy Analysis Report (Directory) from Sigma
Description Basic Report	Check this box if report does not utilize a Report Data Collection job)
Enabled	(If not checked, this report will not be included in the list of reports to run)

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

Reporting Config	uration	
General Information	eport Template Data Collection	Activity .
Enable Upload Customized	d Template	Enable External Report
Tree Level	Deectory	~
Report Type	Signa	v
External Report URL	https://app.sigmacomputing.com/em	bed/ 4-3E4GKXNES17AG8WeGV9Oa
Fibers	ua_retal_customer_schema+DEM	9

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

Properties	Manager Jaru Prop.	erties Viewer and Installation Override Manager
9 properties fou	nd.	
Case Sensitive	Reset Filter	
Category		
	sigma	
Reporting		Explore
Reporting	Sigma.credential.clientID	1e14dd2414f40f63584a15ef519e90630f40a42e155e98a6a82cffdf9aeb77ec
Reporting	Sigma.credential.customer	
Reporting	Sigma.credential.embedSec	- 582 cd8 f11727 e8695 fb df 6b0 fa 99 ebc 25 e0 a b 80 de a 0 a 62854258 a 3981 d4 da 62 b fd a c4 b 134315 a b 4075133 da e e c a caracterizaria da cara
Reporting	Sigma.customer.filterName	
Reporting	Sigma.directory.filterName	
Reporting	Sigma.embed.uri	https://app.sigmacomputing.com/embed/
Reporting		
Reporting	Sigma.site.filterName	

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.

Reporting Con	figuration
General Information	Report Template Data Collection Activity
Report Name	Alarm Summary Report
Description	Alarm Summary Report
Basic Report	Check this box if report does not utilize a Report Data Collection job)
Enabled	(If not checked, this report will not be included in the list of reports to run)

Then go to the Report Template tab, fill in the External Report URL parameter with 4-3KOIBaAZ1TeY3ipAO6HVr4/tag/prod.

Reporting Conf	guration	
General Information	Report Template Data Colle	ction Activity
Enable Upload Custom	zed Template	Enable External Report
Tree Level	None	
Report Type	Sigma	
External Report URL	https://app.sigmacomputing.c	om/embed/ 4-3K0IBaAZ1TeY3ipAO6HVr4/tag/pn
	ua_retail_store_chain_name	=DEMO
Filters		
	1	

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 = 582cd8f11727e8695fbdf6b0fa99ebc25e0ab80dea0a62854258a
 3981d4dda62bfdac4b134315ab4075133daeec743c94b301178c8e5c58e0ddd14db10eecb00
- Reporting.Sigma.externalUserTeam = retail_users

Properties Manager Jaru Properties Viewer and Installation Override Manager				
9 properties found.				
Case Sensitive	Reset Filter			
Category	Кеу	Value		
	sigma			
Reporting	Sigma.accountType	Explore		
	Sigma.credential.clientID	1e14dd2414f40f63584a15ef519e90630f40a42e155e98a6a82cffdf9aeb77ec		
Reporting	Sigma.credential.customer			
Reporting	Sigma.credential.embedSec	582cd8f11727e8695fbdf6b0fa99ebc25e0ab80dea0a62854258a3981d4dda62bfdac4b134315ab4075133daee		
Reporting	Sigma.customer.filterName			
Reporting	Sigma.directory.filterName			
Reporting	Sigma.embed.uri	https://app.sigmacomputing.com/embed/		
Reporting	Sigma.externalUserTeam	retail_users		
Reporting	Sigma.site.filterName			

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.

Reporting Configuration	
General Information	Report Template Data Collection Activity
Report Name	Insights Enterprise Report
Description	Insights Enterprise Report
Basic Report	Check this box if report does not utilize a Report Data Collection job
Enabled	If not checked, this report will not be included in the list of reports to run)

Then go to the **Report Template** tab, fill in the External Report URL parameter with 4-7hjl7r1xFCaqI02KAeuhtf/tag/prod.

Reporting Configuration			
General Information	Report Template	Data Collection Activity	
Enable Upload Customi	zed Template	Enable External Report	
Tree Level	None		×
Report Type	Sigma		~
External Report URL	https://app.sign	acomputing.com/embed/ 4-7hji7r1xFCaqI02KAeuhtt/tag/prod	
	:ua_retail_custo	omer_schema=DEMO	
Filters			

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.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+

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

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+

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	Activity
Vatch Points	100	Watch Points
Export Setpoint File	300	Export Setpoint File
Modify Point	300	Modify Point
Obtain Controller Information	100	Obtain Controller Information
ackup	200	Backup
ontroller Logs and Stats	100	Controller Logs and Stats
Ferminal Mode	100	Terminal Mode
etrieve Logs	100	Retrieve Logs
pload Description File	400	Upload Description File
emove Description File	400	Remove Description File
irmware Transfer	400	Firmware Transfer
estore	300	Restore
verride	300	Override
efresh Units	100	Refresh Units
efresh Applications	100	Refresh Applications
irmware Apply	400	Firmware Apply
dd Application	300	Add Application
efresh Point List	100	Refresh Point List
dit Application Instance	300	Edit Application Instance
et Live Advisories	100	Get Live Advisories
Manual Defrost	400	Manual Defrost
Setpoint Broadcast	400	Setpoint Broadcast
Delete Application Instance	300	Delete Application Instance

Table A-2 - Privileges Versus E2 Protocols

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

The contents of this publication are presented for informational purposes only and they are not to be construed as warranties or guarantees, express or implied, regarding the products or services described herein or their use or applicability. Copeland reserves the right to modify the designs or specifications of such products at any time without notice. Responsibility for proper selection, use and maintenance of any product remains solely with the purchaser and end-user. ©2024 Copeland is a trademark of Copeland LP.

