DISTECH CONTROLS™

ECLYPSE APEX

User Guide

Connecting People with
Intelligent Building Solutions

Document Revision History

- Version 1.0 – Sept 2021
  - Release to market
- Version 1.1 – April 2022
- Version 1.2 – February 2023
  - New Secure Connect tab in BACnet Settings to support BACnet/SC features (BETA)

Copyright

©, Distech Controls Inc., 2021. All rights reserved.

While all efforts have been made to verify the accuracy of information in this manual, Distech Controls is not responsible for damages or claims arising from the use of this manual. Persons using this manual are assumed to be trained HVAC professionals and are responsible for using the correct wiring procedures, correct override methods for equipment control and maintaining safe working conditions in fail-safe environments. Distech Controls reserves the right to change, delete or add to the information in this manual at any time without notice.

Distech Controls, the Distech Controls logo, Allure, and Allure UNITOUCH are registered trademarks of Distech Controls, Inc. BACnet is a registered trademark of ASHRAE. The *Bluetooth*® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks is under license. All other trademarks are property of their respective owners.

Table of Contents

CHAPTER 1

Introduction 9

Overview 9
- About the ECLYPSE APEX Controller 9
- About the IP Protocol Suite 9
- About BACnet® 9

About This User Guide 9
- Purpose of the User Guide 9
- Referenced Documentation 9
- ECLYPSE Introduction 10
- Network Security 10
- Intended Audience 10
- Conventions Used in this Document 10
- Related Documentation 10

Acronyms and Abbreviations Used in this Document 11

CHAPTER 2

Internet Protocol Suite Fundamentals 12

About the Internet Network 12

Internet Protocol Suite Overview 12

CHAPTER 3

IPv4 Communication Fundamentals 14

DHCP Versus Manual Network Settings 14
- Dynamic Host Configuration Protocol (DHCP) 14
- Fixed IP Address or Hostname Management 15

Networking Basics 15
- IP Addressing 15
- About the Subnetwork Mask 15
- CIDR Addressing 16
- Private IPv4 Address Ranges 16
- Reserved Host Addresses 16
- Default Gateway 17
- Domain Name System (DNS) 17

About Routers, Switches, and Hubs 18
- Connecting a Router 18
- Network Address Translation / Firewall 18
- IP Network Segmentation 19

CHAPTER 4

IP Network Protocols and Port Numbers 20

About Port Numbers 20

IP Network Port Numbers and Protocols 20

ECLYPSE Services that Require Internet Connectivity 22

CHAPTER 5

Connecting IP Devices to an IP Network 23
Connecting the IP Network 23
Wired Network Cable Requirements 23
About the Integrated Ethernet Switch 24
Spanning Tree Protocol (STP) 24
Connecting the Network Cable to the Controller 25
Wireless Network Connection 25
About the 2.4 GHz ISM Band 26
Distance Between the Wi-Fi Adapter and Sources of Interference 26
About Wi-Fi Network Channel Numbers 26
Radio Signal Range 27
Radio Signal Transmission Obstructions 27
Where to Locate Wireless Adapters 28
Transmission Obstructions and Interference 28
ECLYPSE Wi-Fi Adapter Mounting Tips 28
Planning a Wireless Network 30
ECLYPSE Wi-Fi Adapter Connection Modes 32
Wi-Fi Client Connection Mode 32
Wi-Fi Access Point 33
Wi-Fi Hotspot 34
Wireless Bridge 34
Wireless Network Commissioning Architectures 36
Client to Access Point Configuration 36
Client to Hotspot Configuration 37

CHAPTER 6

First Time Connection to an ECLYPSE Controller 38
Connecting to the Controller 38
Controller Identification 38
Ethernet Network Connection 39
Network Connections for ECY Series Controllers 39
Wi-Fi Network Connection 40
Configuring the Controller 41
Using the XpressNetwork Utility 41
Using the Controller's Factory-default Hostname in the Web Browser 41
Using the Controller's IP Address in the Web Browser 42
Connecting to the Controller's Configuration Web Interface 42
Next Steps 42

CHAPTER 7

Supported RADIUS Server Architectures 43
Overview 43
Authentication Fallback 43
RADIUS Server Architectures 44
Local Credential Authentication 44
ECLYPSE-Based Centralized Credential Authentication 45
EC-Net-Based Centralized Credential Authentication 46
Configuring the EC-Net Station's RestService 47

Configuring the EC-Net Station's RadiusService 47
Information Technology Department-Managed Centralized Credentials Authentication 48

CHAPTER 8

ECLYPSE Web Interface 49

Overview 49
Web Interface Main Menu 50
Home Page 50
User Profile and Login Credentials 50

Network Settings 52
Ethernet 52
Wireless Configuration 53
Network Diagnostics 55

BACnet Settings 57
General 57
Routing 58
Network IP Ports 58
Network MS/TP Ports 60
Secure Connect 61
Diagnostics 62

User Management 63
Server/Client User Configuration 63
Password Policy 68

Radius Server/Client Settings 69
RADIUS Server Settings 69
RADIUS Client Settings 70

Single Sign On (SSO) Settings 71
SSO Server Settings 72
SSO Client Settings 72
Setting Up the SSO Functionality 74
Setting Up the SSO Functionality through a Radius Server 77
Certificate Authentication with SSO 80

System Settings 81
Device Information 81
Updating the Firmware 82
Export Audit Log 82
Extensions 83
Location and Time 84
Web Server Access 85
Licenses 90
Backup and Restore 91

IoT 97
IoT Configuration 97
IoT Best Practices 99
Docker Container Deployment Example 100

BLE Room Devices 101
BLE Room Devices 102
Beacons 106

CHAPTER 9

Configuring the ECLYPSE Wi-Fi Adapter Wireless Networks **109**
Setting up a Wi-Fi Client Wireless Network 109
Setting up a Wi-Fi Access Point Wireless Network 110
Setting up a Wi-Fi Hotspot Wireless Network 112

CHAPTER 10

Securing an ECLYPSE Controller **114**
Introduction 114
Passwords 114
Change the Default Platform Credentials 114
Use Strong Passwords 114
Account Management and Permissions 114
Use a Different Account for Each User 114
Use Unique Service Type Accounts for Each Project 115
Disable Known Accounts When Possible 115
Assign the Minimum Required Permissions 115
Use Minimum Possible Number of Admin Users 115
HTTPS Certificates 115
Certificates 115
Additional Measures 115
Update the Controller's Firmware to the Latest Release 115
External Factors 115
Install Controllers in a Secure Location 115
Make Sure that Controllers are Behind a VPN 116

CHAPTER 11

BACnet MS/TP Communication Data Bus Fundamentals **117**
BACnet MS/TP Data Transmission Essentials 117
BACnet MS/TP Data Bus is Polarity Sensitive 117
Maximum Number of BACnet MS/TP Devices on a Data Bus Segment and Baud Rate 118
Data Bus Segment MAC Address Range for BACnet MS/TP Devices 119
Device Loading 119
Data Bus Physical Specifications and Cable Requirements 121
Data Bus Topology and EOL Terminations 121
Function of EOL Terminations 121
When to Use EOL Terminations 122
When to use EOL Terminations with BACnet MS/TP Thermostats 122
About Setting Built-in EOL Terminations 123
Only a Daisy-Chained Data Bus Topology is Acceptable 124
Data Bus Shield Grounding Requirements 124
ECB 24V-Powered Controller Data Bus Shield Grounding Requirements 125
ECB-PTU Line-Powered Data Bus Controller Shield Grounding Requirements 126
Data Bus Shield Grounding Requirements When Mixing Both ECB 24V-Powered Controllers and ECB-PTU Line-Powered Controllers 126
Using Repeaters to Extend the Data Bus 127
Device Addressing 129

About the MAC Address ... 129
BACnet MS/TP Data Bus Token-Passing Overview ... 130
About Tuning the Max Info Frames Parameter ... 130
About Tuning the Max Master Parameter ... 131
Setting the Max Master and Max Info Frames ... 131
Default Device Instance Number Numbering System for Distech Controls' Controllers ... 131
Adopting a Numbering System for MAC Addresses, Device Instance Numbers, and Network Numbers ... 131
Setting the Controller's MAC Address ... 132
Inter-Building BACnet Connection ... 133
BACnet/IP Broadcast Management Device Service (BBMD) ... 133

Power Supply Requirements for 24VAC-Powered Controllers ... 134
BACnet MS/TP is a Three-Wire Data Bus ... 134
Avoid Ground Lift ... 134
Techniques to Reduce Ground Lift ... 135
About External Loads ... 135
Transformer Selection and Determining the Maximum Power Run Length ... 135
Recommended 24V Power Cable ... 135
24VAC Power Supply Connection ... 136
Power Wiring with APEX ... 136

CHAPTER 12

Subnetwork Installation Guidelines ... 138

About the Subnetwork Data Bus ... 138
Subnetwork Connection Method ... 138

Subnetwork Module Compatibility and Supported Quantity Charts ... 138
Subnetwork Module Connection ... 139
Subnetwork Data Bus Length ... 140

Cat 5e Cable Subnetwork Data Bus ... 142
Cat 5e Cable Subnetwork Data Bus Cable Requirements ... 142
Cat 5e Cable Subnetwork Bus Topology and End-of-Line Terminations ... 144
Setting the Subnet ID Addressing for Room Devices ... 146

Setting the Allure UNITOUCH Sensor Subnet ID Address ... 147

Setting the Allure EC-Smart-Vue Sensor's Subnet ID Address ... 149

Setting the Allure EC-Smart-Air and EC-Smart-Comfort Communicating Sensor Series' Subnet ID Address ... 150

Setting the EC-Multi-Sensor Series' Subnet ID Address ... 152

Setting the EC-Multi-Sensor-BLE Subnet ID Address ... 152

Setting the ECx-Light and ECx-Blind Series' Subnet ID Address ... 153
Auto-assigned Subnet ID Address for Light and Blind Expansion Modules ... 154
Auto Learn Light and Blind/Shade Expansion Modules in EC-gfxProgram ... 154

Commissioning a Connected VAV Controller with an Allure EC-Smart-Vue Sensor ... 155

CHAPTER 13

Modbus TCP Configuration ... 156

Controller Modbus Support ... 156

Modbus TCP Device Connection ... 156

Device Addressing ... 156

About Device Addressing 156

CHAPTER 14

Modbus RTU Communication Data Bus Fundamentals 158

Controller Modbus Support 158

Modbus RTU Data Transmission Essentials 158

Modbus RTU Data Bus is Polatiry Sensitive 158

Maximum Number of Modbus RTU Devices on a Data Bus Segment and Baud Rate 159

Data Bus Segment Addressing Range for Modbus RTU Devices 159

Data Bus Physical Specifications and Cable Requirements 160

Data Bus Topology and EOL Terminations 161

When to Use EOL Terminations 161

About Setting Built-in EOL Terminations 162

Only a Daisy-Chained Data Bus Topology is Acceptable 162

Data Bus Shield Grounding Requirements 163

Modbus RTU Data Bus Shield Grounding Requirements 163

Device Addressing 164

CHAPTER 15

Resetting or Rebooting the Controller 165

Resetting or Rebooting the Controller 165

CHAPTER 16

ECY Controller Troubleshooting 166

CHAPTER 17

Allure EC-Smart-Vue Communicating Sensor Troubleshooting 169

CHAPTER 18

Wi-Fi Network Troubleshooting Guide 171

CHAPTER 19

Single Sign On (SSO) Troubleshooting 172

CHAPTER 1
Introduction

Overview

This document describes best practices, specifications, wiring rules, and application information to implement robust and reliable communications networks.

About the ECLYPSE APEX Controller

The ECLYPSE APEX Controller is a modular and scalable platform that is used to control a wide range of HVAC applications. It uses IP protocol to communicate on wired Ethernet networks and Wi-Fi to communication on wireless networks.

This user guide also explains how to connect to the ECLYPSE controller's configuration interfaces.

About the IP Protocol Suite

Distech Controls' ECLYPSE Series controllers use a widely used IP protocol to communicate with each other and with other applications for control and supervision. What is commonly referred to as IP is actually a multi-layered protocol suite that reliably transmits data over the public Internet and privately firewalled-off intranets. As integral part of our interconnected world, this protocol is used by applications such as the World Wide Web, email, File Transfer Protocol (FTP), datashares, and so on.

ECLYPSE Series controllers are able to work across geographic boundaries as a unified entity for control and administration purposes.

About BACnet®

The BACnet® ANSI/ASHRAE™ Standard 135-2008 specifies a number of Local Area Network (LAN) transport types. Distech Controls' controllers support both BACnet/IP and BACnet Master-Slave/Token-Passing (MS/TP) communications data bus (based on the EIA-485 medium) as a local network for inter-networking of supervisory controllers and field controllers.

About This User Guide

Purpose of the User Guide

This user guide does not provide and does not intend to provide instructions for safe wiring practices. It is the user's responsibility to adhere to the safety codes, safe wiring guidelines, and safe working practices to conform to the rules and regulations in effect in the job site jurisdiction. This user guide does not intend to provide all the information and knowledge of an experienced HVAC technician or engineer.

This user guide shows you how to integrate ECLYPSE controllers into your IP network environment while enforcing standard network security practices.

Referenced Documentation

The follow documentation is referenced in this document.

- Controller Hardware Installation Guides: These documents are available from the Distech Controls Software Center

- Xpress*Network* Utility User Guide: This document is available on Distech Controls SmartSource website
- EC-*gfx*Program User Guide: This document is available on Distech Controls SmartSource website

ECLYPSE Introduction

The ECLYPSE series is a modular and scalable platform that is used to control a wide range of HVAC applications. It supports BACnet/IP communication and is a listed BACnet Building Controller (B-BC).

The ECLYPSE APEX Controller consists of an automation and connectivity server with built-in power supply, and I/O extension modules.

This programmable controller provides advanced functionality such as customizable control logic, Web-based design and visualization interface (ENVYSION embedded), logging, alarming, and scheduling.

This user guide also explains how to configure the ECLYPSE controller's configuration interfaces.

Network Security

Maintaining the highest level of network security, especially when IP devices are connected to the Internet requires specially trained personnel who are aware of the necessary techniques to ensure continued protection. This must include the implementation of a Virtual Private Network (VPN) to connect with IP controllers over the Internet. It is also important to coordinate with Information Technology (IT) department personnel the use of shared network resources.

At the first connection to an ECLYPSE Controller you will be forced to change the password to a strong password for the admin account to protect access to the controller.

Intended Audience

This user guide is intended for system designers, integrators, electricians, and field technicians who have experience with control systems, and who want to learn about how to make a successful IP network installation. It is recommended that anyone installing and configuring the devices specified in this user guide have prior training in the usage of these devices.

Conventions Used in this Document

This is an example of Note text. Wherever the note-paper icon appears, it means the associated text is giving a time-saving tip or a reference to associated information of interest.

This is an example of Caution or Warning text. Wherever the exclamation icon appears, it means that there may be an important safety concern or that an action taken may have a drastic effect on the device, equipment, and/or network if it is improperly carried out.

Related Documentation

The follow documentation is referenced in this document. These documents are available on Distech Controls SmartSource website.

- Always refer to the Hardware Installation Guide for the devices you are installing.
- EC-*gfx*Program User Guide
- Open-to-Wireless™ Application Guide
- Network Guide

Acronyms and Abbreviations Used in this Document

Acronym	Definition
ASHRAE	American Society of Heating, Refrigeration, and Air-Conditioning Engineers
AP	Access Point
APDU	Application Protocol Data Units
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
BACnet®	Building Automation and Control Networking Protocol
BAS	Building Automation System
B-BC	BACnet Building Controller
BBMD	BACnet/IP Broadcast Management Device
CIDR	Classless Inter-Domain Routing
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EOL	End Of Line
FTP	File Transfer Protocol
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HVAC	Heating, Ventilating, and Air Conditioning
ID	Identifier
IP	Internet Protocol
IPv4	Internet Protocol version 4
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
MAC	Media Access Control
MB	Megabyte
MHz	Megahertz
MS/TP	Master-Slave/Token-Passing
NAT	Network Address Translation
NTP	Network Time Protocol
PC	Personal Computer
RADIUS	Remote Authentication Dial-In User Service
REST	Representational State Transfer
RTU	Remote Terminal Unit (for Modbus)
SSID	Service Set IDentification
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
WAN	Wide Area Network
WPA	Wi-Fi Protected Access
WWW	World Wide Web

CHAPTER 2
Internet Protocol Suite Fundamentals

This chapter describes the Internet protocol operating principles necessary to configure the IP parameters of an IP controller.

About the Internet Network

The Internet is the world-wide interconnection of networks. At its root however, it is not one big network, but a group of networks that communicate between each other by using standard protocols and by using gateways between these networks called routers.

The structure of the Internet is decentralized and non-hierarchical. On the Internet, all communication uses the Internet Protocol (IP) to communicate and all connected devices are identified by their IP address. An Internet Registry allocates IP addresses to internet service providers to be used by their users.

Data is sent across the network in packets. Each packet has a header that identifies the sender's and intended receiver's IP addresses.

Internet Protocol Suite Overview

Internet Protocol (IP) is part of a multi-layered suite that together enables data communication. The following descriptions are an overview of the IP suite protocol layers as used by IP devices:

- Physical layer (bits): This is the physical and device-to-device electrical connection layer otherwise known as Ethernet. This layer defines:
  - The requirements for the physical connection between devices (the signal medium). For example, RJ-45 connectors (attached per TIA/EIA-568-A,), using Cat 5e data cable. The maximum cable length between devices is 328 ft. (100 m) at 100 MB/s data rate.
  - The electrical signal requirements for data packet transport.
  - The data packet structure including data payload and the source and destination device's MAC addresses.

In the case of Wi-Fi connected devices, the link layer is the air interface defined by the Wi-Fi standard, such as radio frequencies, data rates, authentication, data channel encryption, and so on.

- Data Link layer: This layer implements the ability for two devices to exchange data with each other.
- Network layer: This layer implements the ability to connect multiple distinct networks with each other. It provides the internetworking methods that allow data packets to travel from the source device to a destination device across network boundaries, such as a router through the use of an IP address. See *About Routers, Switches, and Hubs*.
- Transport Layer (segments): This layer provides end-to-end communication data stream connection between two or more devices through a variety of protocols. However, it is the Transmission Control Protocol (TCP), the most commonly used internet transport protocol that is used by Distech Controls IP controllers to communicate with each other. TCP creates a connection-oriented channel between two applications; that is to say the data stream is error-checked, is sorted into the correct sequence (missing data packets are re-transmitted) and this data stream has a port number for addressing a specific application at the destination host computer.
- Session layer (data): This layer implements the protocol to open, close, and manage a session between applications such that a dialog can occur.

- Presentation layer: This layer implements the display of media such as images and graphics.
- Applications layer: This layer implements the process-to-process communications protocol that includes among other services the BACnet/IP protocol, programming, debugging, WWW, and so on.

All of the above IP suite protocol layers must be fully functional for any two devices or controllers to communicate with each other.

CHAPTER 3
IPv4 Communication Fundamentals

This chapter describes IPv4 Communication operating principles.

DHCP Versus Manual Network Settings

The following methods can be used to set the network settings:

- Manually set network settings allow precise control over the network's configuration. This option may require an in-depth understanding of arcane networking details – much of which is covered in this guide. See *Networking Basics*.
- Use the router's DHCP setting to automatically connect devices to the network by negotiating the appropriate settings with the device. This option may not be applicable to all networks; for example, the network administrator does not want to use DHCP and has supplied information to manually configure the device's IP interface.

No matter which option is chosen, it will be necessary to coordinate with Information Technology (IT) department personnel the use of shared network resources.

Dynamic Host Configuration Protocol (DHCP)

The Dynamic Host Configuration Protocol (DHCP) is a router feature that dynamically allocates configuration parameters to connected devices such as IP, DNS, and default gateway addresses. Enabling DHCP on a router normally eliminates the need to manually configure network settings on connected devices. The implementation of DHCP on most routers allows a device to be assigned a fixed IP address by associating a specific IP address to a device's MAC address.

Devices that use ECLYPSE's internal router with the DHCP option (Hotspot/AP mode) cannot be assigned fixed IP addresses according to the device's MAC address.

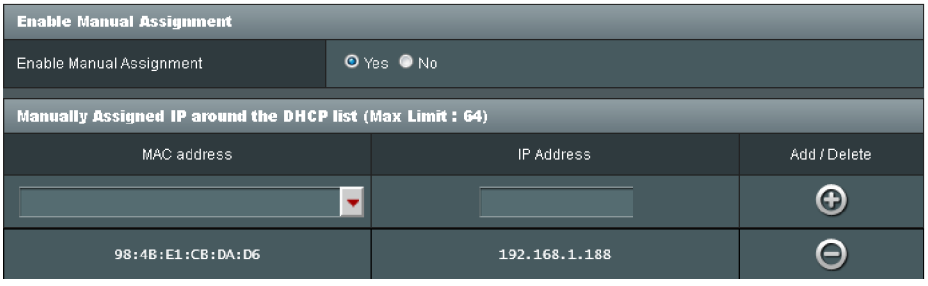


Figure 1: Typical Router Configuration to Assign a Device's MAC Address to a Fixed IP Address

If your router supports DHCP and you have access to the router's configuration interface, this is the most straight-forward way to configure your network. Ensure that all devices that require a fixed IP address use a manually assigned IP address.

Fixed IP Address or Hostname Management

Why should ECLYPSE IP controllers use a fixed IP address or use hostname Management? To program or to access an IP controller, you must be able to connect to it. Like a postal address, a fixed IP address that is always assigned to the same device allows you to consistently connect to and work with the same device.

An alternative to using a fixed IP address is to use the controller's Hostname Management which allows a controller to be identified by a nickname such as ***Office_205*** instead of the controller's IP address. The hostname can be used in a Web browser's address bar or in the EC-*gfx*Program's **Connect to** screen.

Networking Basics

When manually configuring the TCP/IP interface on an ECLYPSE IP controller (the DHCP option is not used), an IP address, subnetwork mask, and a default gateway are required in the Network Settings.

IP Addressing

The most widely used internet addressing scheme is IPv4. It codes an IP address in 32 bits.

An IPv4 address is made up of two parts defined by a subnetwork mask; the network portion (which identifies a specific network or subnetwork) and the host portion (which identifies a specific device).

About the Subnetwork Mask

Devices on the same sub-network can address IP packets to each other directly without routing. The range of IP addresses available in a sub-network is defined by the subnetwork mask. This is also called the subnetwork mask's 'address space'. The subnetwork mask is coded in 32 bits as follows.

An IP packet addressed to a device on another network portion will have to be routed through the router's WAN port as such an address is not local. BACnet/IP broadcast discovery messages such as "Who-Is" do not pass through network routers that separate subnetworks. This means that BACnet/IP controllers on different subnetworks will not normally communicate with each other.

BBMD allows broadcast message to pass through a router: on each subnet, a single device has BBMD enabled. Each BBMD device ensures BACnet/IP connectivity between subnets by forwarding broadcast messages found on its subnetwork to each other, and then onto the local subnetwork as a broadcast message. See *BBMD Settings*.

Network Class	CIDR	Subnetwork Mask	Block Size	Number of Subnetworks according to the Network Type			Number of Hosts according to the Network Type		
				Class A	Class B	Class C	Class A	Class B	Class C
←Class A Network→	/8	255.0.0.0	256	1			16777214		
	/9	255.128.0.0	128	2			8388606		
	/10	255.192.0.0	64	4			4194302		
	/11	255.224.0.0	32	8			2097150		
	/12	255.240.0.0	16	16			1048574		
	/13	255.248.0.0	8	32			525286		
	/14	255.252.0.0	4	64			262142		
	/15	255.254.0.0	2	128			131070		
←Class B Network→	/16	255.255.0.0	256	256	1		65534	65534	
	/17	255.255.128.0	128	512	2		32766	32766	
	/18	255.255.192.0	64	1024	4		16382	16382	
	/19	255.255.224.0	32	2048	8		8190	8190	
	/20	255.255.240.0	16	4096	16		4094	4094	
	/21	255.255.248.0	8	8192	32		2046	2046	
	/22	255.255.252.0	4	16384	64		1022	1022	
	/23	255.255.254.0	2	32768	128		510	510	
←Class C Network→	/24	255.255.255.0	256	65536	256	1	254	254	254
	/25	255.255.255.128	128	131072	512	2	126	126	126
	/26	255.255.255.192	64	262144	1024	4	62	62	62
	/27	255.255.255.224	32	524288	2048	8	30	30	30
	/28	255.255.255.240	16	1048576	4096	16	14	14	14
	/29	255.255.255.248	8	2097152	8192	32	6	6	6
	/30	255.255.255.252	4	4194304	16384	64	2	2	2

CIDR Addressing

Another way to express the subnetwork mask is through CIDR addressing (Classless Inter-Domain Routing) which is written as a slash and a number which represents the number of true bits set in the subnetwork mask. For example, the subnetwork mask 255.128.0.0 is 11111111 10000000 00000000 00000000 in binary or /9.

An IP address can be expressed with its CIDR subnetwork mask in the form of 192.168.0.0/24 for example.

Private IPv4 Address Ranges

Each IP address class has a private address range. Private IPv4 addresses cannot be routed over the Internet.

Distech Controls IP controllers will normally be assigned to a private IP address and are connected to the LAN ports of a router, thereby keeping them behind a firewall from the internet while allowing them to freely communicate to each other and to other trusted devices.

The following IPv4 address ranges are reserved for private networks.

Network Class	IP Address Range	Number of Addresses	Largest CIDR Block (subnetwork mask)
A	10.0.0.0 - 10.255.255.255	16,777,216	10.0.0.0/8 (255.0.0.0)
B	172.16.0.0 - 172.31.255.255	1,048,576	172.16.0.0/12 (255.240.0.0)
C	192.168.0.0 - 192.168.255.255	65,536	192.168.0.0/16 (255.255.0.0)

Reserved Host Addresses

The first and the last IP addresses are reserved for special use on all subnetwork IP address ranges:

The first IP Address is the Network ID. Networks with different network IDs are considered to be distinct. By default, no direct communication can take place between two networks that have different Network IDs. This prevents computers on one network from being accessed by computers on another network. When one department or organization is on one network, it is segregated from computers on other networks.

Last IP Address is the Broadcast Address: this is used for a specific type of network traffic that is destined to every host in the subnetwork range of IP addresses. For example, the device's DHCP client uses the broadcast address to find the network's DHCP server.

For Example, with a typical class C private network:

Subnetwork Mask = 255.255.255.0

Network ID = 192.168.1.0

Gateway = 192.168.1.1

Broadcast Address = 192.168.1.255

Usable IP Addresses = 192.168.1.2 - 192.168.1.254

Default Gateway

Two hosts on the same subnetwork can directly communicate with each other. When a host wants to communicate to an IP address that is not in the subnetwork address range, the host sends the packet to the default gateway. The default gateway is usually the router's IP address and is usually set in the routers administration interface. For more information about IP routing, see *About Routers, Switches, and Hubs*.

Certain ECLYPSE controller services use the default gateway. See *ECLYPSE Services that Require Internet Connectivity*.

Domain Name System (DNS)

When you want to connect to another computer or service on the Internet (to a Website for example), rarely would you want to use the IP address to make the connection as it would be a pain to remember the numeric IP address for each and every site you want to visit. The Domain Name System (DNS) was created to allow internet users to take advantage of a meaningful Uniform Resource Locator (URL) such as *http://www.distech-controls.com/* to connect to an IP address without having to know the server's or computer's numerical IP address. The DNS does this by looking up the URL and providing the numeric IP address to the requesting computer. Should the IP address of a computer/server be changed, the DNS server can be updated with its new IP address, thereby ensuring that other networked computers can still find this computer/server through its URL.

Set the DNS IP address of the Domain Name System (DNS) servers in routers and in IP controllers that have manually-configured IP parameters. Between one and three DNS IP address is usually provided by the Internet Service Provider (ISP). The second and third DNS addresses are for failover should the first DNS become unavailable.

If you do not know the address of your DNS server(s), try the following publicly-available DNS server addresses: primary = 8.8.8.8 and secondary = 4.4.4.4

Some ECLYPSE controller services use DNS to resolve Web addresses thereby allowing the service to operate. See *ECLYPSE Services that Require Internet Connectivity*.

About Routers, Switches, and Hubs

The differences between a hub, switch, and router are discussed in the table below.

Device Type	Description
Hub	Every incoming data packet is repeated on every other port on the device. Due to this, all traffic is made available on all ports which increase data packet collisions that affect the entire network, thus limiting its data carrying capacity.
Switch	A switch creates a one-to-one virtual circuit that directs IP packets directly to the port that the destination computer is connected to.
Router	Like a switch, a router learns the IP addresses of all devices connected to any of its RJ-45 ports to create a routing table. If a data packet arrives at the router's port with a destination IP address that is: – Found in the router's routing table, the router forwards the data packet to the appropriate port for the device that has this IP address. – For a network with a different network ID than the current network ID, the router forwards the data packet to the uplink port where the next router will again either recognize the network ID and route the data packet locally or again forwards the data packet to the uplink port. By being exposed to traffic, a router adds to its routing table the pathways necessary to resolve a data packet's pathway to its final destination, by passing through one or more routers if necessary.

Connecting a Router

The way a router is connected to other devices changes its function.

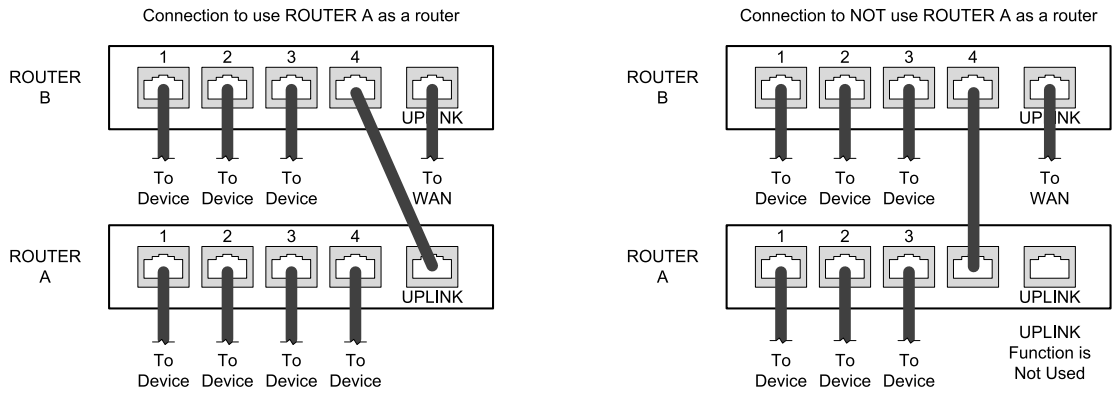


Figure 2: The Way a Router is Connected Changes its Function

On some routers, the uplink port is marked as WAN (Wide Area Network) and the numbered ports are to be connected to the LAN (Local Area Network) devices.

Network Address Translation / Firewall

A router's uplink port provides Network Address Translation (NAT) and firewall functions.

NAT is a method to hide the private IP addresses of a range of devices (connected to LAN ports) behind a single IP address presented at the WAN uplink port. NAT uses a mechanism to track requests to WAN IP addresses and readdresses the outgoing IP packets on exit, so they appear to originate from the router itself. In the reverse communications path, NAT again readdresses the IP packet's destination address back to the original source private IP address.

Due to this tracking mechanism, only requests originating from the LAN side can initiate communications. A request from the WAN to the router cannot be mapped into a private address as there is no outbound mapping for the router to use to properly readdress it to a private IP address. This is why a NAT acts as a firewall that blocks unsolicited access to the router's LAN side.

Most routers allow you to open a port in the firewall so that WAN traffic received at a specific port number is always forwarded to a specific LAN IP address. The standard port numbers used by ECLYPSE controllers is explained in chapter *IP Network Protocols and Port Numbers*.

IP Network Segmentation

For efficient network planning, normally the IP controllers will be assigned to their own network segment of an IP network or subnetwork. This is done as shown in the figure below.

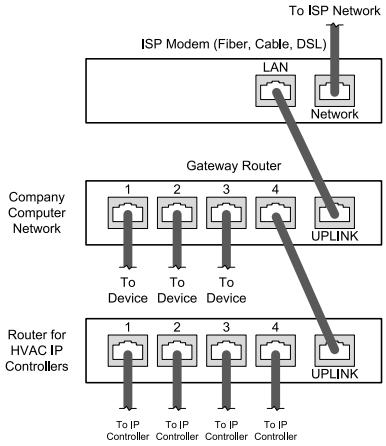


Figure 3: Network Segment for HVAC IP Controllers

For certain wireless topologies, a wireless router can be used to connect to the controller. In this scenario, a wireless operator interface (laptop or tablet) can be used for commissioning as shown in the figure below. If the laptop has a Supervisor installed, it can be used to program ECB series controllers connected to the RS-485 port of the Connected System Controller.

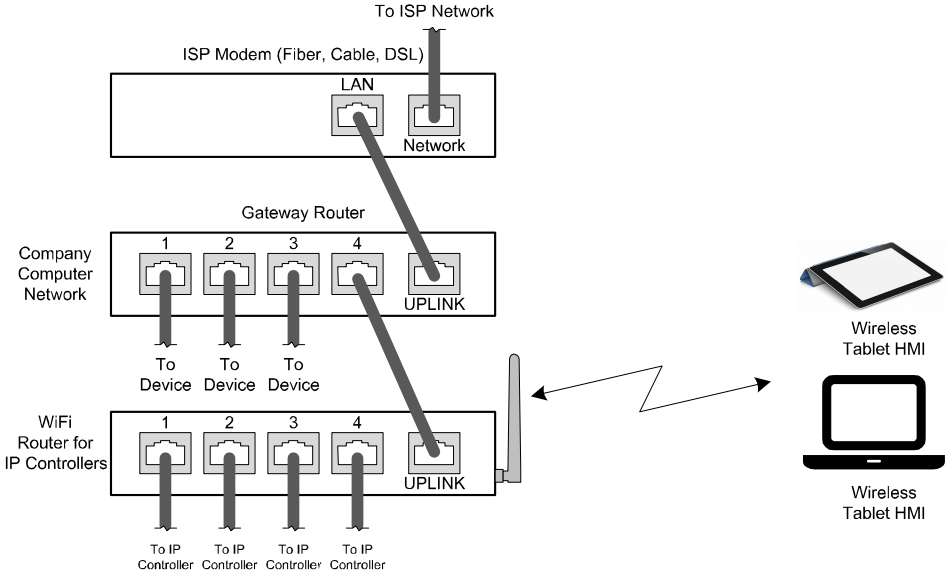


Figure 4: Network Segment for HVAC IP Controllers with a Wireless Access Point

If a wireless router is unavailable or is out-of-range, an ECLYPSE Wi-Fi adapter can be connected to an controller's USB port to add wireless connectivity. See *Wireless Network Connection*.

CHAPTER 4

IP Network Protocols and Port Numbers

This chapter describes the IP Network Protocols and Port Numbers used by the ECLYPSE controller.

About Port Numbers

In an IP packet, a port number is an extension of the packet's IP address and completes the destination address for a communications session. By convention, the packet's port number is associated with a protocol used between software applications and is used to uniquely identify a communications endpoint for a specific application or process running on a computer. This allows a multitude of applications to share a single physical connection to the Internet while allowing distinct communication channels between different applications.

For example, your web browser listens to port 80 on your computer to receive HTML web pages sent from a web server on port 80.

The standard port numbers used by controllers is explained in *IP Network Port Numbers and Protocols*.

Sometimes, two applications might use the same port number to communicate. To sort out this conflict, the following methods can be used.

- In the configuration of some applications, the port number can be changed from its default setting. Should you change it, you must also change it on the corresponding application also so that the port numbers will match.
- Routers have features such as port forwarding that can change an incoming packet's port number coming from the Wide Area Network (WAN) to another port number on the Local Area Network or vice versa.

IP Network Port Numbers and Protocols

This section lists the IP Network Protocols to communicate over IPv4 networks. The corresponding default in-bound port number is also shown.

Service	Default Port Number (Protocol)	Description	Where can this port number be changed?
SMTP	25 (TCP)	Outgoing Email server port number.	See the EC-*gfx*Program User Guide, Resources Configuration.
DNS	53 (TCP, UDP)	Domain Name Server URL lookup.	–
DHCP	67 (UDP)	The router's DHCP service that allows a device to auto-configure a devices' IP settings.	–
HTTP	80 (TCP)	**EC-*gfx*Program Debugging Values (REST service)**: After the control logic or code has been sent to the controller, a live debugger allows programmers to execute code, view input/output values, and troubleshoot errors in real-time. **ENVYSION**: The ENVYSION server presents system status, trending visualization, real-time equipment visualization, schedule configuration, alarm monitoring, and dashboard functions to a Web browser operator interface. **Web Configuration Interface**: This is the network configuration interface for wired and wireless IP network interfaces.	See *System Settings*. If this is used with EC-Net, this parameter can be changed in the **RestService** and **WebService**.

Service	Default Port Number (Protocol)	Description	Where can this port number be changed?
HTTPS	443 (TCP)	**Secure EC-*gfx*Program Debugging Values (REST service):** After the control logic or code has been sent to the controller, a live debugger allows programmers to execute code, view input/output values, and troubleshoot errors in real-time. **Secure ENVYSION**: The ENVYSION server presents system status, trending visualization, real-time equipment visualization, schedule configuration, alarm monitoring, and dashboard functions to a Web browser operator interface. **Secure Web Configuration Interface:** This is the network configuration interface for wired and wireless IP network interfaces.	See *System Settings*. If this is used with EC-Net, this parameter can be changed in the **RestService** and **WebService**.
Radius Server	1812 (UDP)	Authentication Port: This is the port on which authentication requests are made.	
Radius Server	1813 (UDP)	Accounting Port: This is the port on which accounting requests are made. This is only used to receive accounting requests from other RADIUS servers.	
Radius Server	1814 (UDP)	Proxy Port: This is an internal port used to proxy requests between a local server and a remote server.	See *User Management*. If this is used with EC-Net, these parameters must be set in the RadiusService.
BACnet/IP	47808 (UDP)	The BACnet over IP protocol.	See *BACnet Settings*.
Secure MQTT	8883 (TCP)	The “nLight gateway” service is provided by three application processes running on the Eclypse-nECY. MQTT publish/subscribe protocol on port 8883 is used to communicate configuration and status info to the Distech Eclypse applications running on the Eclypse-nECY that require this information. Secure MQ Telemetry Transport. This is an internal port that facilitates communication with the nLight Gateway.	
Zeroconf/ mDNS	5353 (UDP)	Used for mDNS discovery of the Eclypse controller on the network.	
nLight	5551 (TCP)	TCP port 5551 is the primary means of communication between SensorView and the nLight gateway application running on the Eclypse-nECY. TCP port 5551 is also used for nECY -to- nECY nLight communications. nLight global control channel packets and nLight profile control command packets are exchanged on this port.	
nLight	7 (UDP)	UDP port 7 is used to facilitate the SensorView auto discovery of Eclypse-nECY nLight-enabled controllers on the subnet.	
nLight	5555 (UDP)	UDP port 5555 is used to facilitate the Eclypse-nECY nLight gateway auto discovery of X-Point bridge devices on the subnet.	
nLight	5556 (UDP)	UDP port 5556 is used by the Eclypse-nECY nLight gateway to route nLight global control channel broadcast packets to X-Point bridge devices on the subnet.	
nLight	5551 (UDP)	UDP port 5551 is used by the Eclypse-nECY nLight gateway to send/receive nLight unicast packets to X-Point bridge devices on the subnet.	

ECLYPSE Services that Require Internet Connectivity

In order to operate, the following out-bound services require:

- A working DNS. See *Domain Name System (DNS)*.
- The default gateway / router to be configured. See *Default Gateway*.
- Internet connectivity.

The corresponding default out-bound port number is also shown.

Service	Default Port Number (Protocol)	Description
SMTP	25 (TCP)	Outgoing Email server port number.
Network Time Protocol (NTP)	123 (UDP)	Used to set the controller's real-time clock.
DNS server	53 (UDP, TCP)	Used to provide URL name resolution. The controller by default uses an internet DNS. If the local network has a DNS, set its IP address in *Network Settings*.
Weather Service	443 (TCP)	Weather Service requires internet access through port 443 to receive information.

CHAPTER 5
Connecting IP Devices to an IP Network

An IP network requires infrastructure such as Ethernet cable, routers, switches, or Wi-Fi hotspots in order to work. The following topics discuss the fundamentals of such a network.

Connecting the IP Network

There are two methods to connect a device to an IP Network:

- Wired (Ethernet connection with the PRI and SEC ports).
- Wireless (when the Wi-Fi Adapter is connected to the controller).

Wired Network Cable Requirements

Wired networks use commonly available Cat 5e structural cabling fitted with RJ-45 connectors. If you make your own patch cable, use Category 5e cable and crimp the RJ-45 connectors at both ends of the cable either as T568A or T568B.

Parameter	Details
Media	Cat 5e Cable; four (4) pairs of wires with RJ-45 Connectors (standard straight patch cable)
RJ-45 Pin Configuration	Straight-through wiring. Crimp connectors as per T568A or T568B (both cable ends must be crimped the same way).
Characteristic impedance	100-130 Ohms
Distributed capacitance	Less than 100 pF per meter (30 pF per foot)
Maximum Cat 5e Cable length between IP devices	328 ft. (100 m) maximum. See *About the Integrated Ethernet Switch*.
Polarity	Polarity sensitive
Multi-drop	Daisy-chain (no T-connections) ECLYPSE IP devices have two RJ-45 female RJ-45 connectors that provide IP packet switching to support follow-on devices.
Daisy-chain limit, APEX	Up to 20 devices can be daisy-chained per network switch port.
Daisy-chain limit, ECY-CSC	Up to 20 devices can be daisy-chained per network switch port.
Daisy-chain limit, ECY-VAV, ECY-303 and ECY-PTU Controllers	Up to 50 devices can be daisy-chained per network switch port.
Spanning Tree Protocol (STP) limit, ECY-VAV, ECY-303 and ECY-PTU Controllers	Distech Controls recommends a maximum of 25 devices to be connected in a ring and must use two network switch ports.
EOL terminations	Not applicable
Shield grounding	Not applicable

Table 1: Wired Network Cable Physical Specifications and Requirements

Bus and Cable Types	Non-Plenum Applications (Use in Conduit - FT4)		Plenum Applications (FT6)	
	Part Number	O.D. (Ø)[1]	Part Number	O.D. (Ø)[1]
300 m (1000 feet), Cat 5e Yellow Jacket Cable - Without Connectors	CB-W244P-1446YLB	4.6mm (0.18in.)	CB-W244P-2175YEL	4.6mm (0.18in.)
100 Crimp RJ 45 Connectors	CB-W5506E	N/A	CB-W5506E	N/A

Table 2: Distech Controls Recommended Cable Types to use for the Cat 5e Cable Subnetwork Bus

1. Outer cable diameter – This does not take into account the RJ-45 connector.

About the Integrated Ethernet Switch

The 2-port wired interface uses a switch to forward packets addressed to IP devices connected to it. This allows controllers to be daisy-chained together to extend the IP network's physical range and to reduce the amount of network cable required as each controller no longer has to make a home run to the network switch.

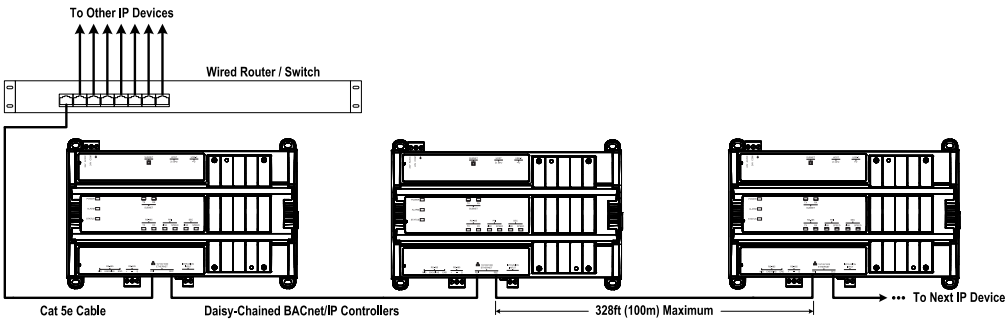


Figure 5: Wired Network Connection - Daisy-Chained

Spanning Tree Protocol (STP)

Switches and routers that support Spanning Tree Protocol (are IEEE 802.1D certified) are able to detect and eliminate a loop from being formed on the network by disabling any port on the router that is causing a loop. Such switches can be used to enhance network availability by allowing you to create a ring network of controllers that is resistant to a single point network failure (a cut wire for example).

In this scenario APEX controllers are connected in a loop (or ring) such that the last controller is connected back to the switch / router. Under normal operation, the switch / router disables one of the ports to prevent a packet storm. This is shown below.

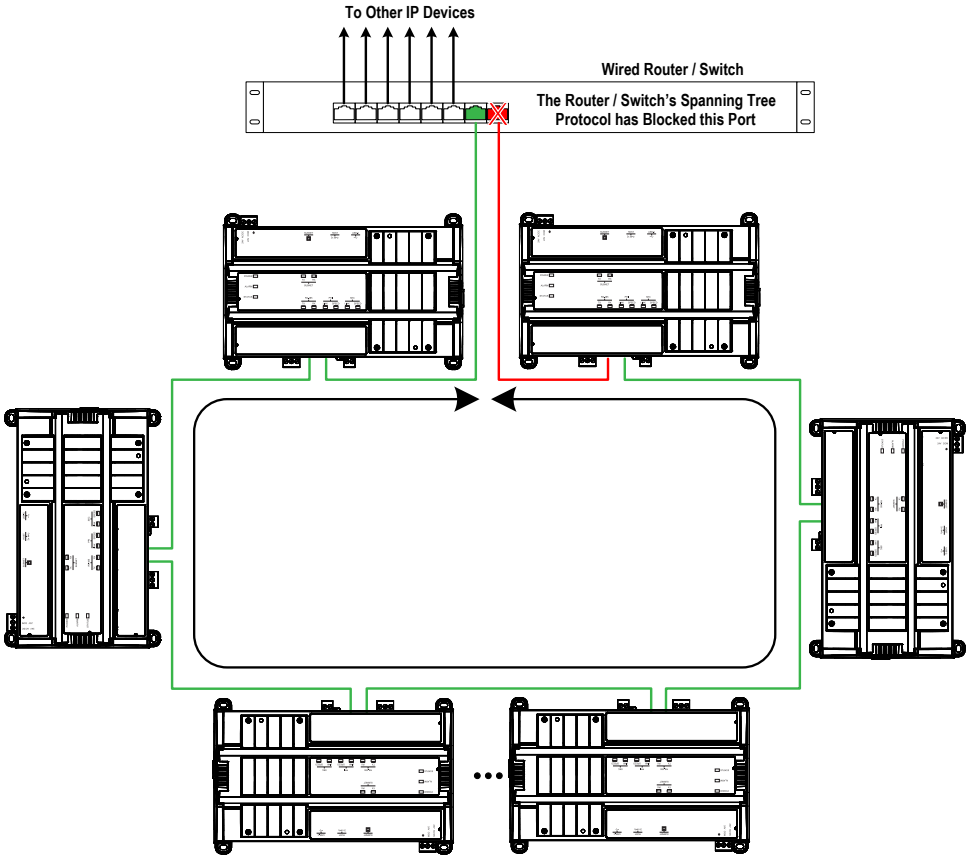


Figure 6: Wired Network Connection: Spanning Tree Protocol – Normal Operation

When a network wire is cut, the ring is split into two – the switch / router automatically enables the port to maintain service. This is shown below.

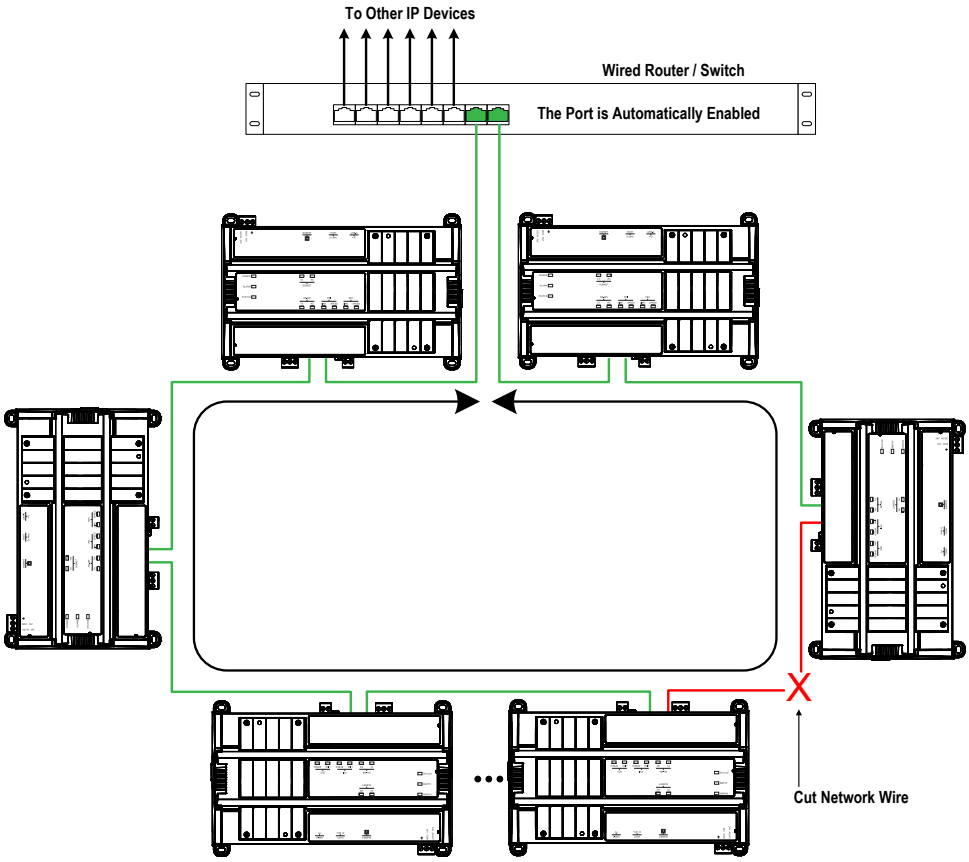


Figure 7: Wired Network Connection: Spanning Tree Protocol – Failover Operation

The switch / router can be configured to send an email message when port blocking is disabled thus signaling that a network wire has been cut.

Connecting the Network Cable to the Controller

To connect controllers to an Ethernet network and then discover them, see chapter *First Time Connection to an ECLYPSE Controller*.

Wireless Network Connection

The ECLYPSE Wi-Fi adapter connects to an ECLYPSE controller's USB port.

Figure 8: Wi-Fi Adapter

It adds wireless IP connectivity to controllers and it can be used in many wireless topologies and applications.

To wirelessly connect to a controller for the first time, see *First Time Connection to an ECLYPSE Controller*.

To configure a Wi-Fi adapter, see *Network Settings*. See also chapter *Configuring the ECLYPSE Wi-Fi Adapter Wireless Networks*.

Recommendations are provided regarding the radio signal obstructions and factors that should be avoided to obtain the best Wi-Fi radio signal transmission and reception. Walls attenuate radio wave propagation by an amount that varies with the construction materials used. See *Radio Signal Transmission Obstructions* for more information on wall materials that can reduce range transmission.

About the 2.4 GHz ISM Band

The 2.4 GHz ISM (Industrial, Scientific and Medical) band has been allocated worldwide for the use of radio frequency energy by industrial, scientific, and medical purposes as part of the device's method of internal operation and as such may have powerful emissions that cause interference to radio communications.

For example, microwave ovens operate in the 2.4 GHz ISM band with about 1000W emitted power and a fraction of a percent of that energy does leak from the oven. While this is not a health risk, Wi-Fi networks operate at even lower power levels to communicate and can be overwhelmed by this source of interference.

When setting up a 2.4 GHz band Wi-Fi network, you must take into consideration any equipment that operates in the 2.4 GHz ISM band such as medical and laboratory equipment. Other sources of interference are other telecommunications equipment such as cell phones, GSM/DECT, cordless phones, RFID reader, Bluetooth devices, walkie-talkies, baby monitors, and so on. Note that equipment that transmits in other frequency bands do emit spurious emissions at low levels over a wide spectrum so that a radio transmitter that is in close proximity to the ECLYPSE Wi-Fi adapter can cause interference, even if its operating frequency is 1.9 GHz for example.

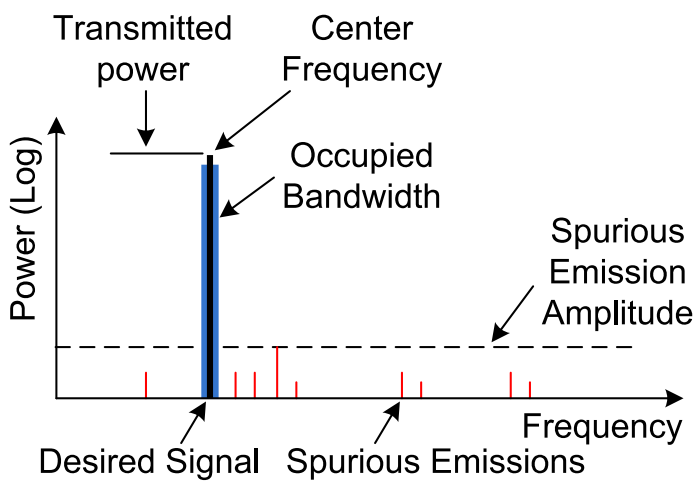


Figure 9: Typical Radio Transmitter Spurious Emissions

Distance Between the Wi-Fi Adapter and Sources of Interference

Unrelated transmitters should be more than 6.5 feet (2 m) away from the Wi-Fi Adapter to avoid possible interference.

About Wi-Fi Network Channel Numbers

Wi-Fi communications use a slice of radio spectrum or channel width for data transmission. In general terms, the amount of channel width required is proportional to the data transmission rate. Wi-Fi networks operate in a number of different frequency ranges or bands such as the 2.4 GHz band. Each band is divided into a number of industry-standard channels that represent a center frequency for data transmission. In practice, the center frequency is the mid-point between the upper and lower cutoff frequencies of the channel width.

When the channel width is larger than the channel spacing (the space between channels), overlap between the channels can occur, resulting in inter-channel interference that lowers overall network throughput. This is shown in the diagram below. For example, in the 2.4 GHz band using 802.11g, the channel width is 20 MHz while the channel spacing is 5 MHz. If one Wi-Fi network is using channel 1 that is in close proximity to another Wi-Fi network that is using channel 2, there will be significant inter-channel overlap and interference. Data throughput is reduced as a result.

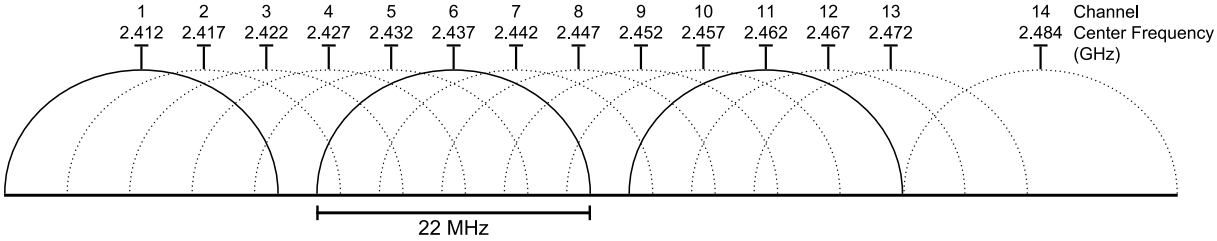


Figure 10: 2.4 GHz Band 802.11g Radio Spectrum Showing Inter-Channel Overlap

For a 20 MHz channel width in the 2.4 GHz band using 802.11g, the best channels to use to avoid inter-channel overlap are channels 1, 6, and 11. For a 40 MHz channel width in the 2.4 GHz band using 802.11g, the best channels to use to avoid inter-channel overlap are channels 3 and 11.

For a 20 MHz channel width in the 2.4 GHz band using 802.11n, the best channels to use to avoid inter-channel overlap are channels 1, 6, and 11. For a 40 MHz channel width in the 2.4 GHz band using 802.11g, the best channel to use to avoid inter-channel overlap is channel 3.

For industrial / commercial environments, it is recommended to avoid using a 40 MHz channel width in the 2.4 GHz band as it occupies a large part of the available radio spectrum. This means that it will be difficult to co-exist with other networks while avoiding interference, especially from devices that use mixed mode 802.11 b/g which significantly degrades 802.11n performance. One solution is to disable the 802.11 b/g mode on all hotspots to force all wireless clients to 802.11n mode, thereby forbidding the use of legacy devices.

Radio Signal Range

Range is dependent upon many environmental variables that are present in buildings. In normal conditions, a radio signal is transmitted at a maximum range between Wi-Fi Adapters of 50 feet (15 m) at 2.4 GHz (IEEE 802.11b/g/n).

In certain cases where there are obstructions, the range could be less.

Because radio signals and transmission range can vary according to building and office setup, you can troubleshoot Wi-Fi network performance issues by running a Wi-Fi surveying or Wi-Fi stumbling tool on a laptop computer. This software shows the currently operating Wi-Fi networks operating within range, their signal strength, and their channel number so as to make the best configuration choices.

Radio Signal Transmission Obstructions

Radio signals are electromagnetic waves; hence the further they travel, the weaker the signal becomes thereby limiting effective range of operation. Coverage is further decreased by specific materials found in the direction of the transmission. For example, while radio waves can penetrate a wall, they are dampened more than if the waves were on a direct line-of-sight (LoS) path.

The following table shows the different types of building materials and range reduction:

Wall Material	Range Reduction vs. LoS
Wood, drywall, glass (uncoated, without metal)	0 – 10%
Brick, particle board	5 – 35%
Metal, steel-reinforced concrete, mirrors. See *Where to Locate Wireless Adapters*	10 – 90%

Where to Locate Wireless Adapters

When installing the wireless adapter, it is important to ensure that distances and obstructions do not impede transmission. Metallic parts, such as steel reinforcement in walls, machinery, office furniture, etc. are major sources of field strength dampening. Furthermore, supply areas and elevator shafts should be considered as complete transmission screens, see following figure.

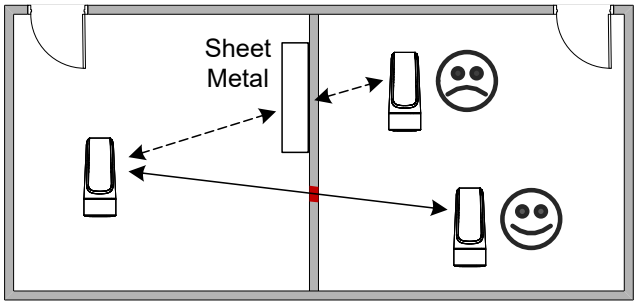


Figure 11: Screening of Radio Waves

Transmission Obstructions and Interference

One way to get around an obstruction, such as a duct, is to place the wireless adapter on the side of the obstruction that is nearer to the coordinating wireless device, even if the controller is on the opposite side of the obstruction. But always keep in mind that the wireless adapter performs best when it is away from metal objects or surfaces (more than 1" (2.5 cm)).

For more examples on how to position the wireless adapter, see *ECLYPSE Wi-Fi Adapter Mounting Tips*.

In addition to obstructions, the angle with which the transmission travels through the obstruction has a major influence on the field strength. The steeper the angle through an obstruction, the radio wave has to travel through more material resulting in the field strength reduction (See figure below). Therefore, it is preferable that the transmission be arranged so that it travels straight and perpendicularly through the obstruction.

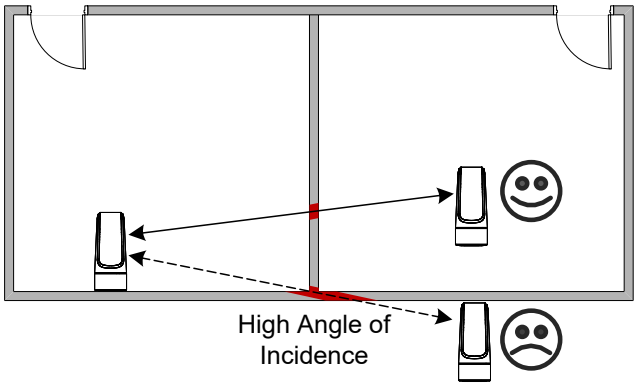


Figure 12: Angle of Radio Waves

A solution to avoid an obstruction is to add another wireless router located closer to the controller(s).

ECLYPSE Wi-Fi Adapter Mounting Tips

This section provides information and examples on how to properly position the Wi-Fi Adapter to ensure reliable wireless communication. The most common guidelines to remember when installing the Wi-Fi Adapter is to keep it at least 1” (2.5 cm) away from metal, and never install the Wi-Fi Adapter inside a metal enclosure (relay panels, junction box, etc.).

Typical Metal Relay Panel/Utility Box Installation

The following image shows where to install an Wi-Fi Adapter on a metal relay panel or utility box with a controller inside the panel/box. To maximize wireless range, the Wi-Fi Adapter must be installed on the top or side of the panel.

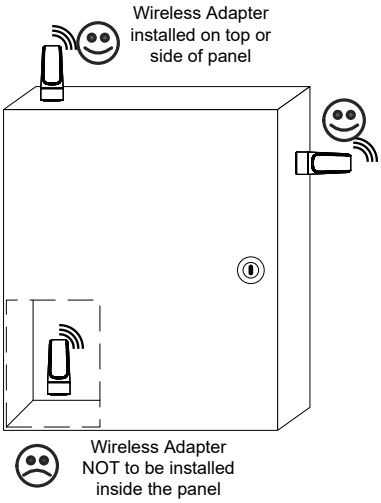


Figure 13: Wi-Fi Adapter Position with Metal Relay Panel/Utility Box

Typical Fan Coil Unit Installation

The following example shows where to install an Wi-Fi Adapter on a fan coil unit with a controller inside the unit. The Wi-Fi Adapter must be installed on the top or side of the unit with the antenna straightened out and away from the metal. The Wi-Fi Adapter and antenna should never be installed inside the metal enclosure.

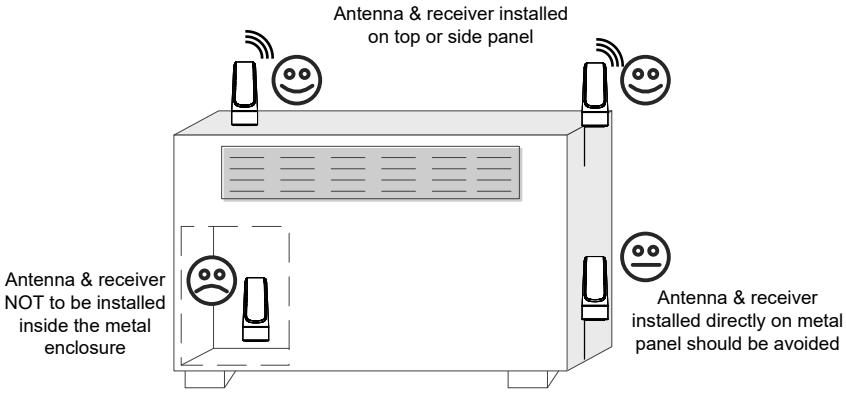


Figure 14: Wi-Fi Adapter Position on Fan Coil Unit

Planning a Wireless Network

A wireless network can be installed in many different types of floor spaces, large or small: office space, commercial space, residential space, etc. The following provides an example on how to start planning a wireless network such as a large office space. This type of planning can also be used with smaller areas.

1. Retrieve a copy of your floor plans and a compass.

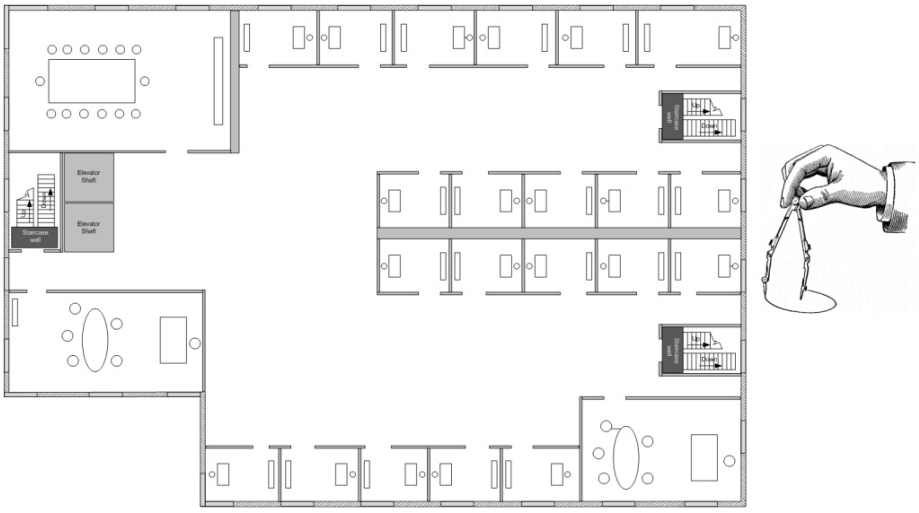


Figure 15: Copy of floor plan and a compass

2. Mark relevant radio shadings into floor plan such as: fire protection walls, lavatories, staircases, elevator shafts and supply areas.

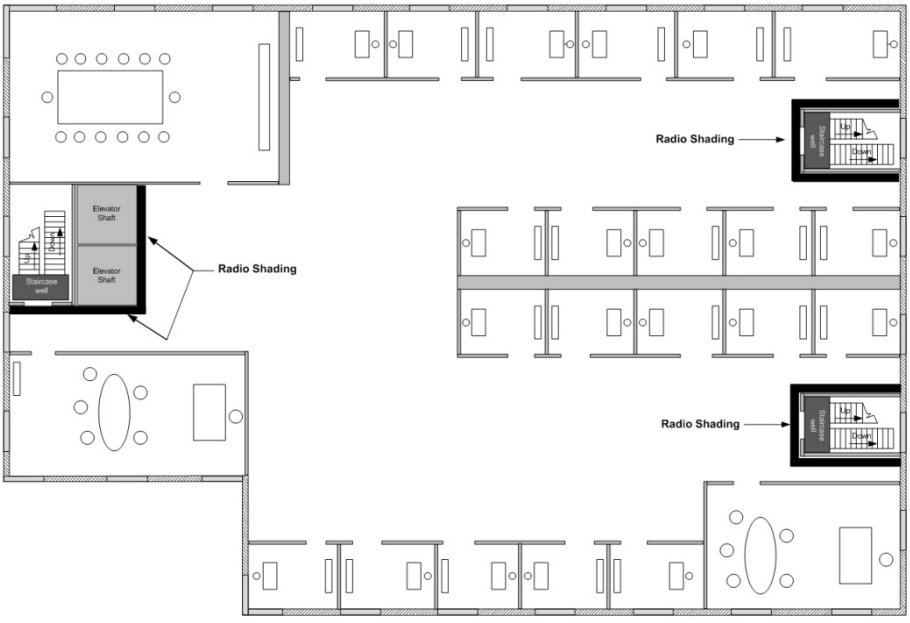


Figure 16: Mark relevant radio shadings

3. Draw circles to locate the ideal positions for your Wi-Fi Adapter as shown below:

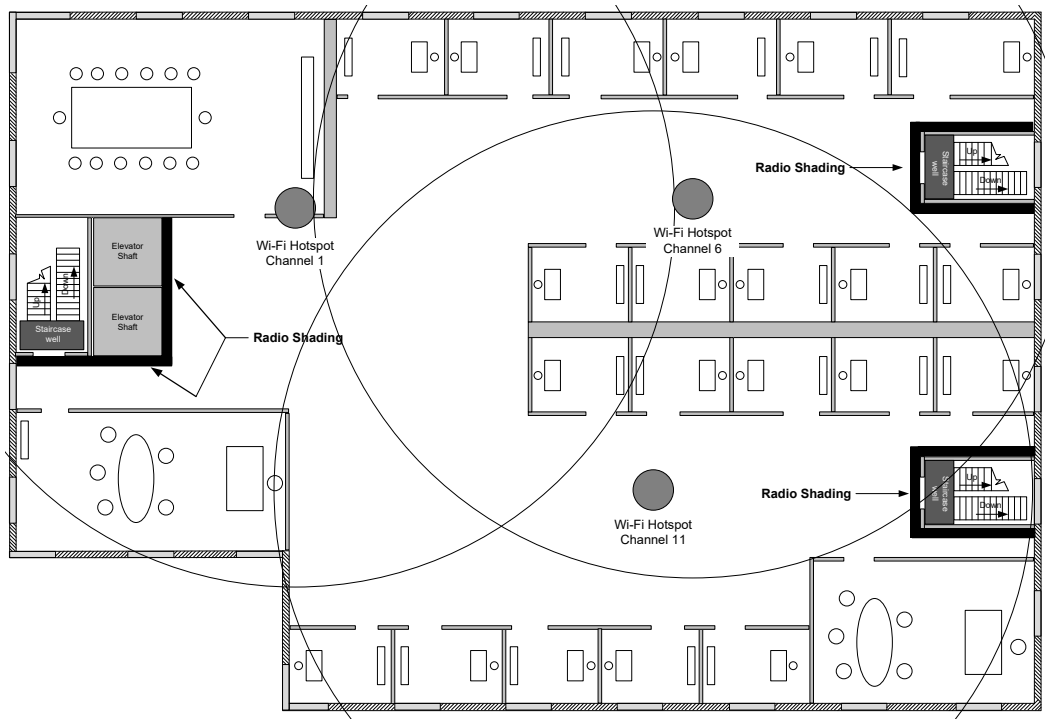


Figure 17: Radio Wi-Fi Adapter Location

- Make sure that the Wi-Fi Adapter is positioned in a way such that no screens block the connection to any corner inside the fire safety section (potential sensor positions).
- For reliable range planning, the unfavorable conditions should be detected at the beginning but often come from later changes to the environment (room filled with people, alteration of partition walls, furniture, room plants, etc.).
- Even after careful planning, range and signal tests should be done during installation to verify proper reception at the Wi-Fi Adapter positions. Unfavorable conditions can be improved by changing the antenna position or by adding a router closer to the controller(s).

For reliable range planning, the unfavorable conditions should be detected at the beginning but often come from later changes to the environment (room filled with people, alteration of partition walls, furniture, room plants, etc.).

Even after careful planning, range and signal tests should be done during installation to verify proper reception at the Wi-Fi Adapter positions. Unfavorable conditions can be improved by changing the antenna position or by adding a router closer to the controller(s).

ECLYPSE Wi-Fi Adapter Connection Modes

The Wi-Fi adapter supports a number of connection modes shown in the table below:

Connection Mode	Description	Max Number of Wireless Clients or Nodes
Client	This sets the mode of the Wi-Fi adapter to connect the controller as a client of a Wi-Fi access point. This interface can auto-configure its IP parameters when the connected network that has a DHCP server. When an ECLYPSE controller is a Wi-Fi client, the Ethernet ports can be used to provide network connectivity to another ECLYPSE or to a laptop for example. Each connected device counts towards the “Maximum Number of Wireless Clients or Nodes”. See *Wireless Bridge* for more information.	16
Access Point	This sets the mode of the Wi-Fi adapter to be a Wi-Fi access point. This access point operates off of the same subnetwork and has the same IP connectivity that the controller has with its wired network connection. For example, if the controller’s wired connection is to a network that has an active DHCP server, access point clients can also use this DHCP server to automatically configure their IP connection parameters.	16
Hotspot (default)	This sets the mode of the Wi-Fi adapter to be a Wi-Fi hotspot with a router. This puts the hotspot into a separate subnetwork with a DHCP server to provide IP addresses to any connected device. Wide area network (WAN) connectivity is through the wired connection.	16

Typical application examples are shown below.

Wi-Fi Client Connection Mode

Cut installation costs by leveraging existing wireless infrastructure and by eliminating the need for Ethernet cables. This architecture is characterized by the point-to-point connection between an access point and a client-controller.

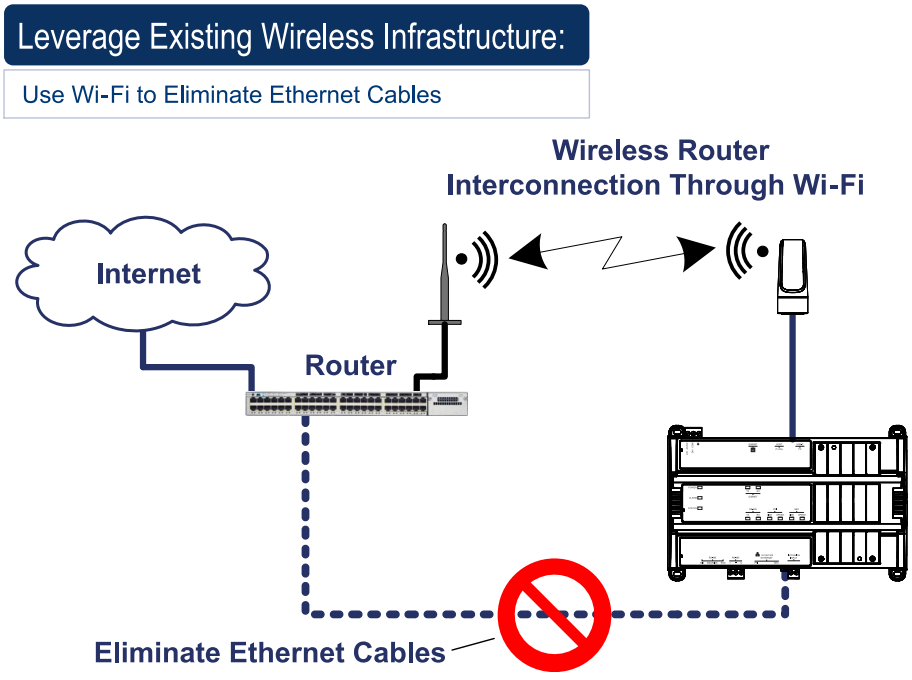


Figure 18: Leveraging Existing Wireless Infrastructure by Eliminating Ethernet Cables

To configure the Wi-Fi client connection mode, see *Setting up a Wi-Fi Client Wireless Network*.

Wi-Fi Access Point

Should there be no available access point; an ECLYPSE controller can be configured as a wired-to-wireless bridge to create an access point which can provide Wi-Fi access to other Wi-Fi enabled clients. This access point operates off of the same subnetwork and has the same IP connectivity that the controller has with its wired network connection. The Wi-Fi adapter can also be temporarily added to a controller for wireless commissioning purposes. A variety of software applications are available for system monitoring and override, commissioning, configuration and programming. To configure the Wi-Fi access point connection mode, see *Setting up a Wi-Fi Access Point Wireless Network*.

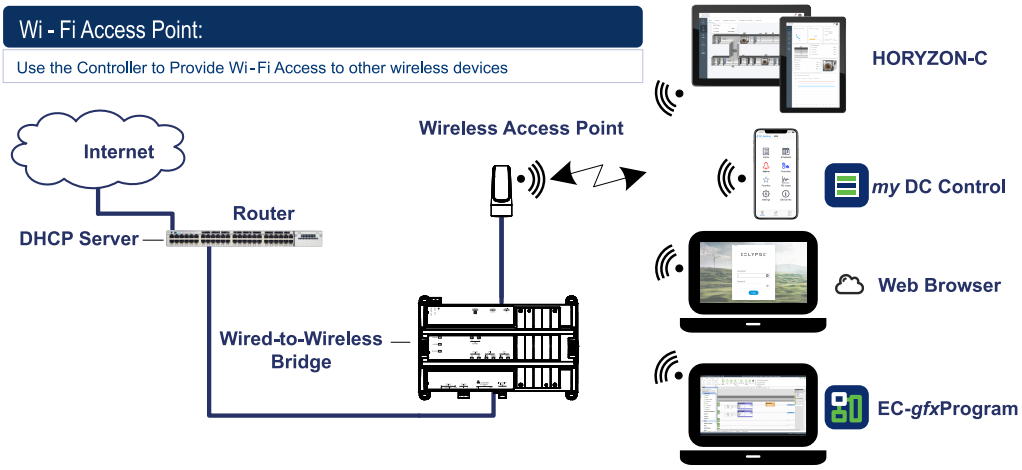


Figure 19: Using an APEX Controller to Create an Access Point

A second ECLYPSE controller can be configured as a wireless client. This can be used as a solution to 'jump' architectural features that are not compatible with wires such as glass atrium and the like. To configure the Wi-Fi client connection mode, see *Setting up a Wi-Fi Access Point Wireless Network*.

An access point can provide Wi-Fi access to other Wi-Fi enabled clients and controllers.

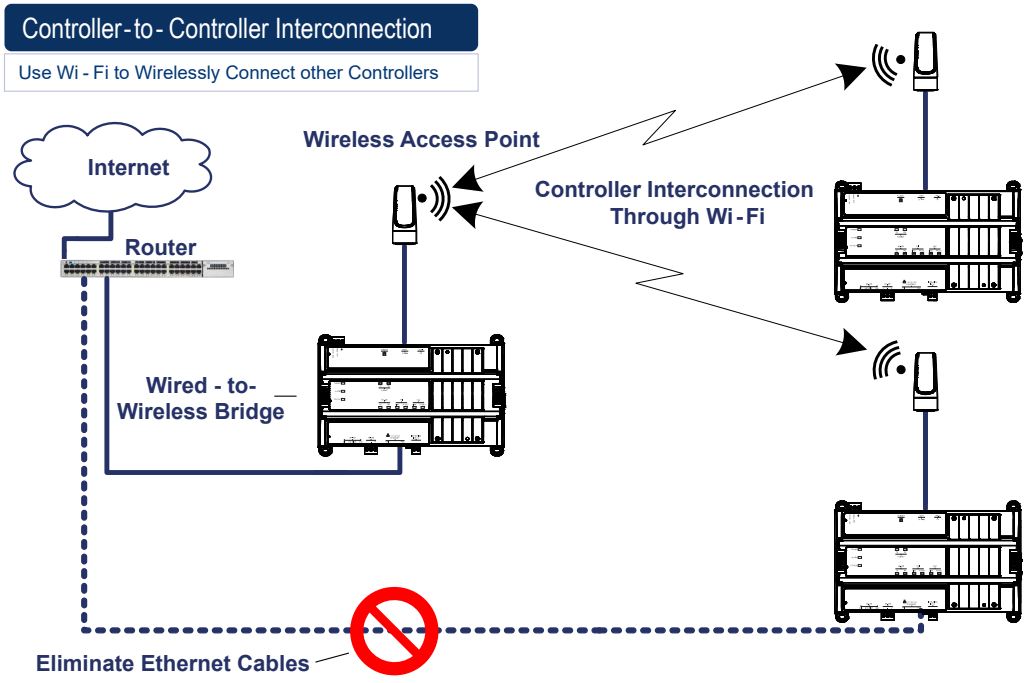


Figure 20: Using an APEX Controller as a Wireless Bridge

Wi-Fi Hotspot

Should the wired network not use a DHCP server (uses fixed IP addresses); an ECLYPSE controller can be configured to create a hotspot with a router that creates its own subnet and DHCP server which can provide Wi-Fi access to other Wi-Fi enabled clients. This is the default connection method when a Wi-Fi adapter is connected to an ECLYPSE controller. The Wi-Fi adapter can also be temporarily added to an ECLYPSE controller for wireless commissioning purposes. A variety of software applications are available for system monitoring and override, commissioning, configuration and programming. To configure the Wi-Fi hotspot connection mode, see *Setting up a Wi-Fi Hotspot Wireless Network*.

A hotspot creates a subnetwork. As a result, any connected BACnet device will not be able to discover BACnet devices on any other LAN subnetwork.

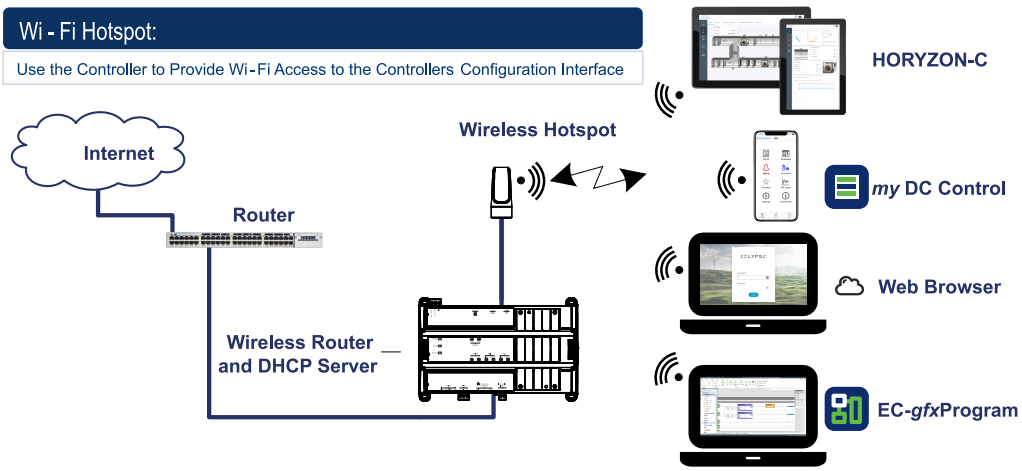


Figure 21: Using an APEX Controller to Create a Hotspot

Wireless Bridge

A second controller can be configured as a wired-to-wireless bridge to allow the connection of wired IP devices to the bridged controller's Ethernet ports. This can be used as a solution to 'jump' architectural features that are not compatible with wires such as glass atrium and the like.

The access point / hotspot can provide Wi-Fi access to other Wi-Fi enabled clients.

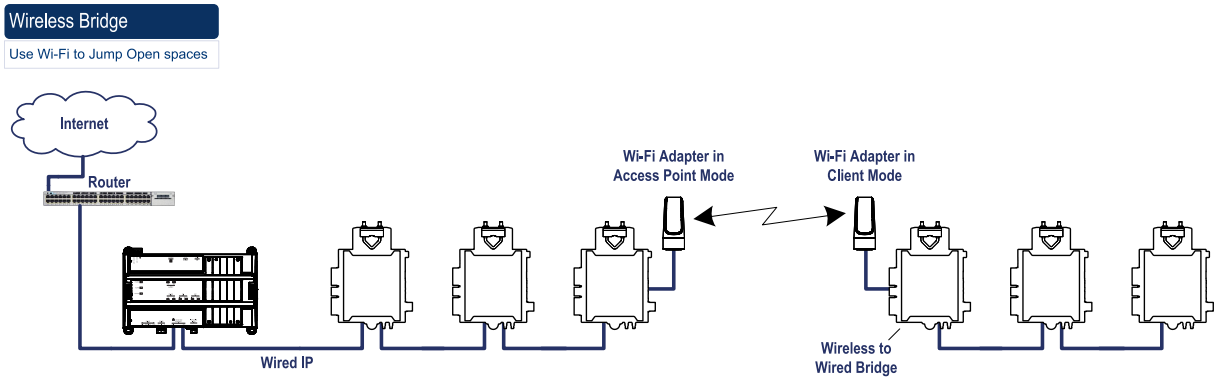


Figure 22: Using an ECLYPSE Controller as a Wireless Bridge

Maximum Number of Wireless Clients or Nodes for an Access Point

A wireless access point can service a maximum of 16 clients or nodes in total. The following examples show what this limit can be composed of:

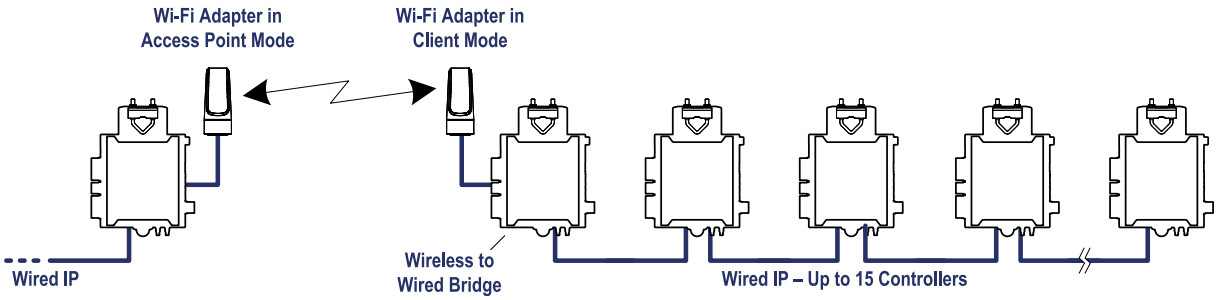


Figure 23: Using an ECLYPSE Controller as a Wireless Bridge

- One wireless bridged controller is connected to as many as 15 daisy-chained wired devices.

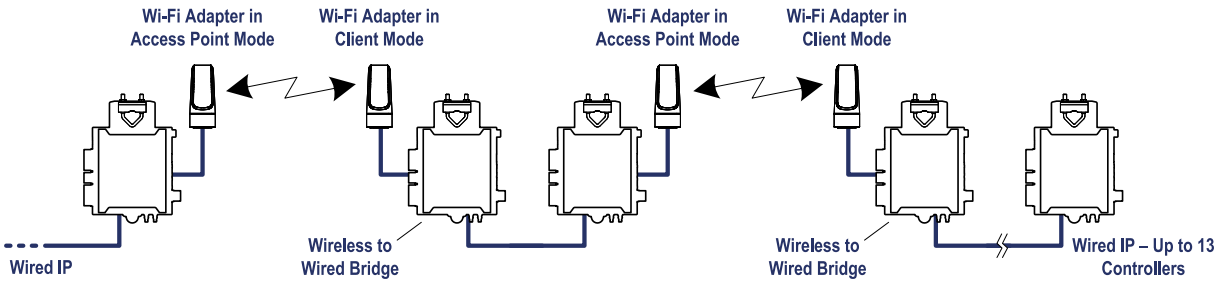


Figure 24: Using an ECLYPSE Controller as a Wireless Bridge

- One wireless bridged controller is connected to one wired controller that is wirelessly connected to one wireless bridge that is then connected 13 daisy chained wired devices.

If the access point is a Wi-Fi router:

1. The number of devices is limited by the total number of clients the router is able to support.
2. It can support many controllers acting as wireless to wired bridges.
3. Each wireless to wired bridge controller can support up to 15 controllers.

Wireless Network Commissioning Architectures

Client to Access Point Configuration

A laptop is connected through Wi-Fi, as a Wi-Fi client, to any ECLYPSE Connected VAV controller that has its wireless settings configured as an Access Point. The other ECLYPSE Connected VAV controllers are configured as Wi-Fi Clients and are wirelessly connected to the same Access Point.

With this configuration, the laptop and all the controllers are on the same subnet, so either laptop user has access to all networked controllers.

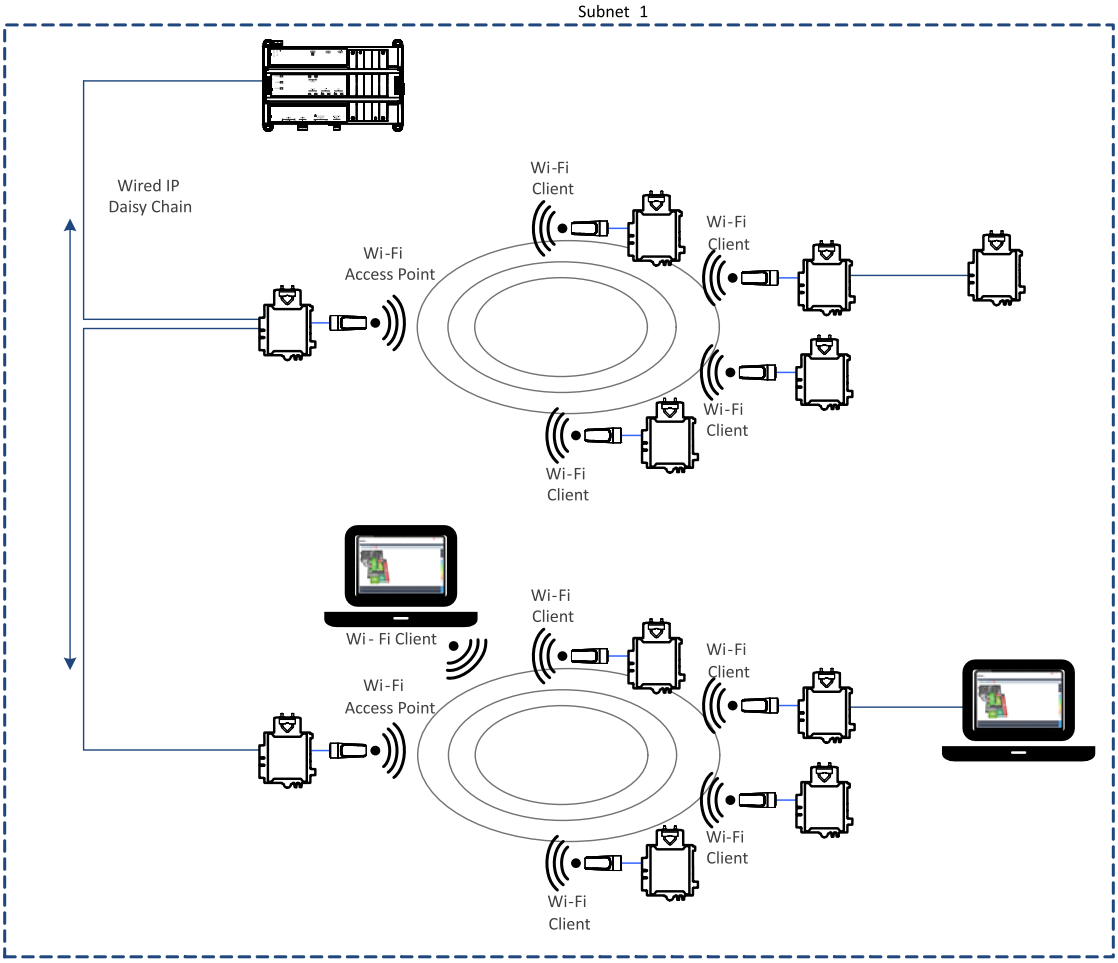


Figure 25: Client to Access Point Configuration

Client to Hotspot Configuration

Laptop 1 is connected as a Wi-Fi client to an ECLYPSE Controller that has its wireless settings configured as a Hotspot (Subnetwork 2). The ECLYPSE Connected VAV controllers that are part of the wired network are configured, on their wireless side as a Wi-Fi Access Point (Subnetwork 1).

The remaining ECLYPSE Connected VAV controllers are configured as a Wi-Fi Client and are wirelessly connected to a VAV controller's Access Point.

With this configuration, laptop 1 is on the same subnet as the ECLYPSE Connected System Controller (Subnetwork 2 created by the Hotspot), but all the Connected VAV Controllers are on a different Subnet (Subnetwork 1), so the laptop 1 user only has access to the Connected System Controller on its same subnet. This is because BACnet/IP broadcast discovery messages such as "Who-Is" do not pass through network routers that separate subnetworks. In the example shown below, the Connected System Controller acts as a router between the Wi-Fi hotspot clients and the wired network. This means that BACnet/IP controllers on different subnetworks will not normally communicate with each other. The laptop 2 user has access to both the Connected VAV controllers and the Connected System Controller. A solution is to use BBMD on both Laptop 1 (using EC-Net for example) and on the Connected System Controller. See *BACnet/IP Broadcast Management Device Service (BBMD)*.

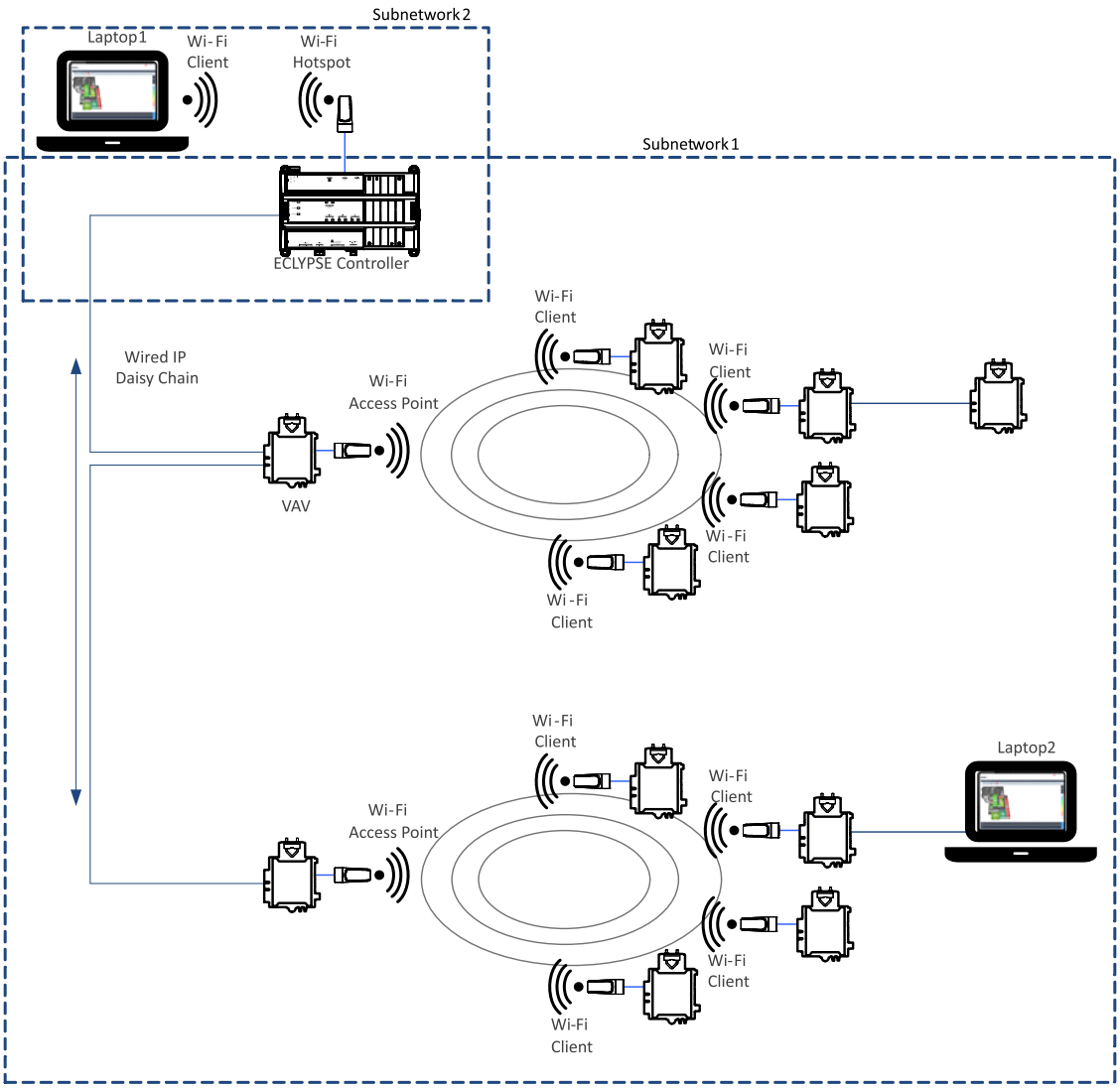


Figure 26: Client to Hotspot Configuration

CHAPTER 6
First Time Connection to an ECLYPSE Controller

This chapter describes how to get started with an ECLYPSE controller. This includes connecting to the factory-default IP address to gain access to the controller's configuration interfaces.

Connecting to the Controller

When connecting to the controller for the first time, the goal is to gain access to the controller so that you can configure it to work in its future network environment. To do so, you must connect the controller to form a network.

The Xpress*Network* Utility allows you to discover all ECLYPSE controllers connected to an IP network's subnetwork and to perform a range of operations on many controllers at once: you can set each controller's Hostname and IP address, launch EC-*gfx*Program to program the controller, or you can access the controller's Web interface. It is a software application that runs on a PC that is connected to the same subnetwork as the controllers. See the Xpress*Network* Utility User Guide for more information.

ECY Series Controller configuration can also be made through the controller's configuration Web interface that is accessed through the Xpress*Network* Utility. This Web interface is used to set all the controller's configuration parameters including the controller's IP address according to your network planning. See *ECLYPSE Web Interface*.

There are two networking methods to connect to a controller:

- Wired (Ethernet connection) with a PC.
- Wireless (when the Wi-Fi Adapter is connected to the controller) with a PC. See *Wi-Fi Network Connection*.

Once you have connected the controller(s) to a network, configure the controller. See *Configuring the Controller*.

Controller Identification

Controllers are uniquely identified on the network by their MAC address. This identifier is printed on a label located on the side of the controller and another is on the controller's box. Get a printed copy of the building's floor plan. During controller installation, peel the MAC address sticker off the controller's box and put it on the floor plan where the controller has been installed.

This MAC address is used as part of the controller's factory-default Wi-Fi access point name and its hostname.

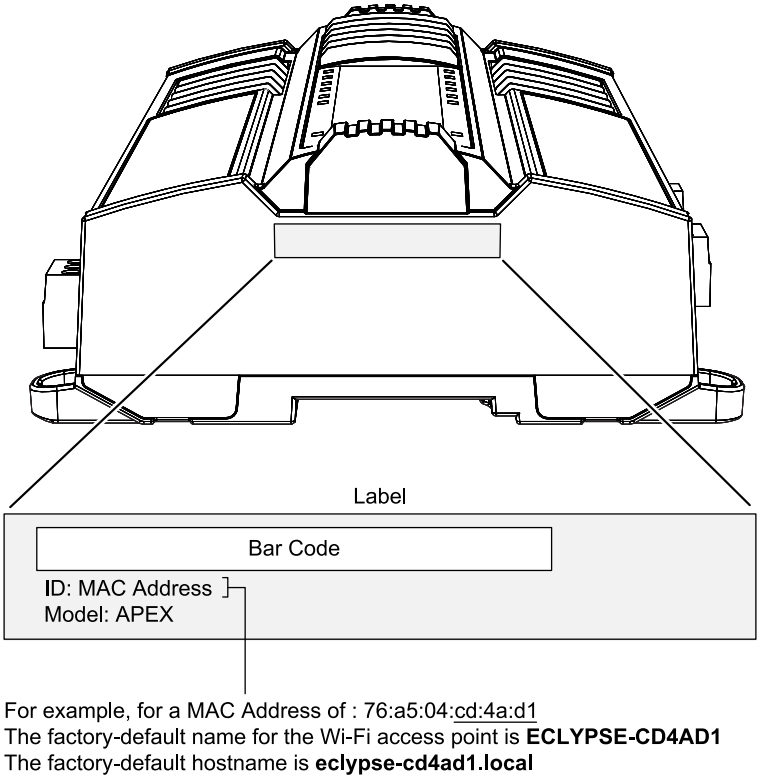


Figure 27: Finding the Controller's MAC Address

Ethernet Network Connection

Depending on the controller model, the way the controller is connected to the network will change according to whether the controller is a Power over Ethernet (PoE) model or not.

- For non-PoE controller models, see *Network Connections for ECY Series Controllers*.
- For the ECY-VAV-PoE controller, see Network Connections for ECY-VAV-PoE Model Controllers.

See also *Connecting IP Devices to an IP Network* for network wiring considerations.

Network Connections for ECY Series Controllers

Connect the controller to the network as follows:

1. Connect your PC's network card to the controller's PRI Ethernet port using a Category 5e Ethernet cable.

If you are commissioning more than one controller, connect the controllers and PC to a network switch. Two or more controllers can be connected to the network by daisy-chaining them together by using Cat 5e network Cables to connect the **Ethernet Switch Sec**(ondary) connector of one controller to the **Ethernet Switch Pri**(mary) connector of the next controller.

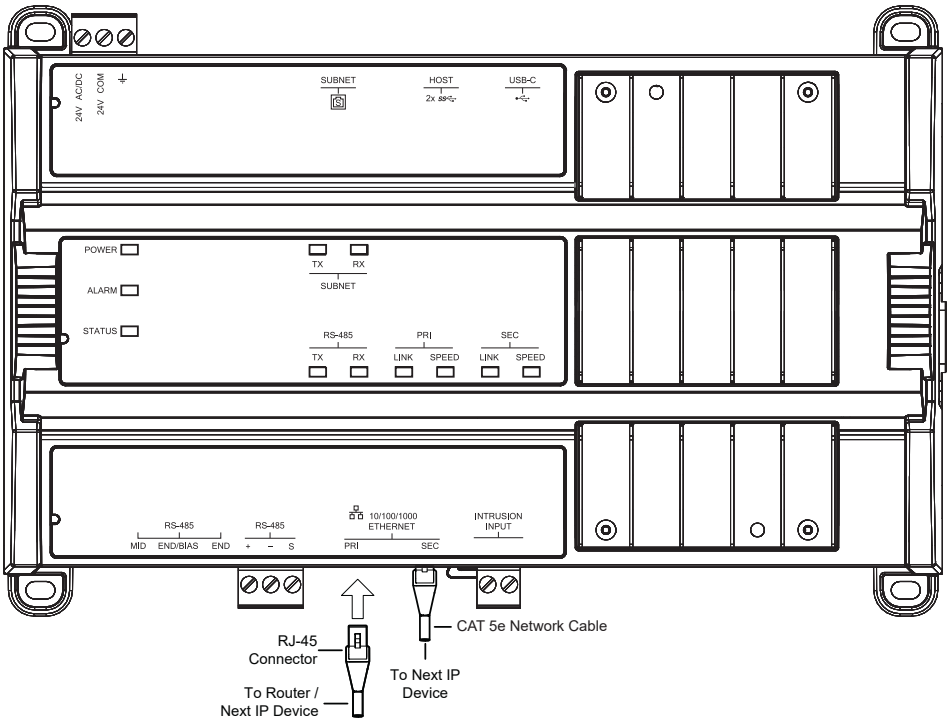


Figure 28: APEX Wired Network Connection: Cat 5e Cables with RJ-45 Connectors are used

2. Connect power to the controller(s). See the controller's Hardware Installation Guide for how to do so.

Wi-Fi Network Connection

Once the ECLYPSE Wi-Fi Adapter has been connected to a powered controller, a Wi-Fi hotspot becomes available that allows you to connect to the controller's configuration Web interface with your PC.

On your PC's wireless networks, look for an access point named **ECLYPSE-XXYYZZ** where **XXYYZZ** are the last 6 hexadecimal characters of the controller's MAC address.

To find the controller's MAC address, see *Controller Identification*. The default password for the wireless network is: **eclypse1234.**

Either of the controller's two USB HOST ports can be used to connect the wireless adapter.

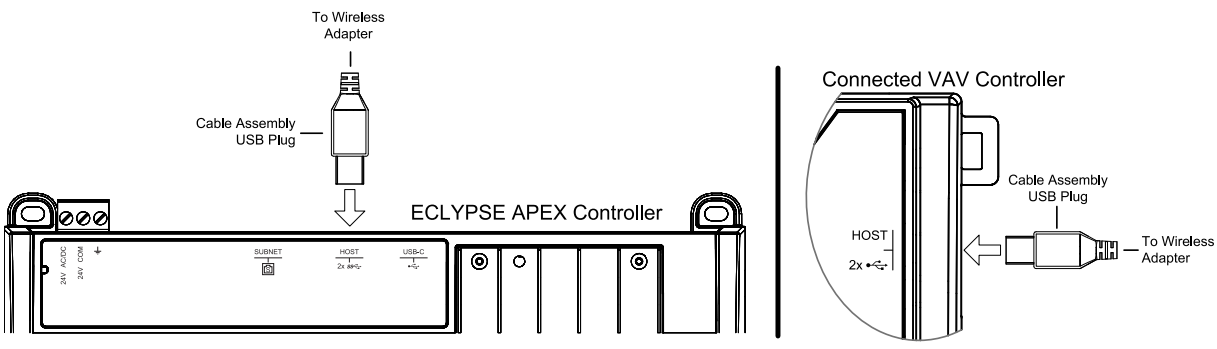


Figure 29: Connecting the Wireless Adapter to the Controller's USB HOST Port

Configuring the Controller

Any of the following methods can be used to connect to the controller's interface in order to configure it:

- ☐ Using the XpressNetwork Utility
- ☐ Using the controller's factory-default Hostname in the Web browser
- ☐ Using the controller's IP address in the Web browser

Using the XpressNetwork Utility

The Xpress*Network* Utility is a software application that runs on a PC that allows you to discover all ECY Series controllers connected to an IP network's subnetwork or Wi-Fi network and to perform a range of operations on many controllers at once: you can set each controller's Hostname and IP address, launch EC-*gfx*Program to program the controller, or you can access the controller's configuration Web interface.

The XpressNetwork Companion mobile app can be installed on your smartphone and it works with the QR code marked on the controller's faceplate which encodes the controller's MAC address and host ID. By scanning the QR code, the app records this information to which you assign a hostname. Once the QR codes for all controllers have been read in, the app's information is transferred to the Xpress*Network* Utility where it is used to populate the relevant data fields.

See the Xpress*Network* Utility User Guide for more information.

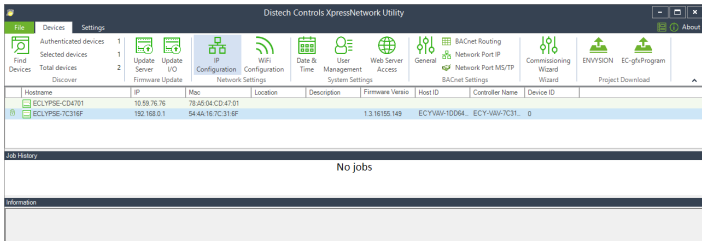


Figure 30: XpressNetwork Utility Discovers the Network-Connected Controllers

Using the Controller's Factory-default Hostname in the Web Browser

Controllers have a factory-default hostname that you can use instead of an IP address to connect to it. The hostname can be used in a Web browser's address bar or in the EC-*gfx*Program's **Connect to** screen. When installing the latest version of EC-*gfx*Program and your PC does not have the Bonjour service installed, a link to install the Bonjour service is provided. The Bonjour service must be installed on your PC to allow your PC to discover controllers by their hostname.

If your PC is unable to resolve the controller's hostname, you must connect your PC to the controller through Ethernet or Wi-Fi so that your PC only sees the controller network. For example, in this case, your PC must be disconnected from all other networks such as a corporate network or the Internet. If necessary, temporarily disconnect your PC's network cable from its Ethernet port.

The controller's factory-default hostname is **eclypse-xxxxxx.local** where **xxxxxx** is the last 6 characters of the MAC address printed on a sticker located on the side of the controller. See *Controller Identification*.

For example, the sticker on the side of a controller shows that its MAC address is 76:a5:04:cd:4a:d1. Connect to the controller's Web interface as follows:

1. Open your Web browser.
2. In the Web browser's address bar, type **https://eclypse-cd4ad1.local** and click **Go**.

3. Login to the controller. Then set the controller's configuration parameters in the controller's configuration Web interface. See *Connecting to the Controller's Configuration Web Interface*.

The Hostname can be changed in the *System Settings*.

Using the Controller's IP Address in the Web Browser

Connect to a controller through its IP address as follows:

For a Wi-Fi network connection

1. Open your Web browser.
2. In the Web browser's address bar, type **https://192.168.0.1** (the controller's factory-default wireless hotspot IP address) and click go.
3. Login to the controller. Then set the controller's configuration parameters in the controller's configuration Web interface. See *Connecting to the Controller's Configuration Web Interface*.

Not all smart phones/mobile devices have the Bonjour service installed and thus cannot use the hostname mechanism.

For an Ethernet network connection

You must know the controller's current IP address (from the DHCP server for example).

4. Open your Web browser.
5. In the Web browser's address bar enter the controller's IP address and click go.
6. Login to the controller. Then set the controller's configuration parameters in the controller's configuration Web interface. *Connecting to the Controller's Configuration Web Interface*.

Connecting to the Controller's Configuration Web Interface

The ECLYPSE Series Controller configuration can be made through the controller's configuration Web interface to set all the controller's configuration parameters including the controller's IP address according to your network planning.

At the first connection to an ECLYPSE Controller you will be forced to change the password to a strong password for the admin account to protect access to the controller.

It is important to create new user accounts with strong passwords to protect the controller from unauthorized access. See *User Management*, *Securing an ECLYPSE Controller*, *Supported RADIUS Server Architectures*.

Next Steps

In Network Settings, configure the controller's network parameters so that they are compatible with your network. See *ECLYPSE Web Interface*.

CHAPTER 7
Supported RADIUS Server Architectures

A RADIUS server is used to centralize user credentials (controller login username / password) across all devices. This chapter describes the supported RADIUS server architectures and how to configure a RADIUS server in EC-Net or in an ECLYPSE controller.

Overview

When network connectivity allows, an EC-*gfx*Program user can connect directly to an ECLYPSE controller or a user can connect to the ECLYPSE controller through an EC-Net station. No matter the connection method, a user has to authenticate themselves with their user credential (controller login username / password combination). Credentials can be held separately in each device (ECLYPSE controller / EC-Net station), though this is not recommended as maintaining user credentials among multiple devices is more labor intensive.

Under such circumstances, the preferred method is to centralize user credentials in a RADIUS server on one device or server. When a user connects to an ECLYPSE controller, the ECLYPSE controller connects to the remote RADIUS server to authenticate the user's credential. A RADIUS server uses a challenge/response mechanism to authenticate a user's login credentials. An unrecognized username or a valid username with an invalid password receive an 'access denied' response. A remote RADIUS server can be another ECLYPSE controller, Microsoft Windows Domain Active Directory Server, or a suitably-configured EC-Net / EC-BOS station.

Authentication Fallback

Should the connection to the remote RADIUS server be temporarily lost, ECLYPSE controllers have a fall back authentication mode: users that have already authenticated themselves with the remote RADIUS server and then the connection to the RADIUS server is lost, these users will still be able to login to the controller as their successfully authenticated credentials are locally cached.

The user profile cache is updated when the user authenticates themselves while there is a working RADIUS server connection. For this reason, at a minimum, admin users should log in to each ECLYPSE controller at least once, so their login can be cached on that controller. Otherwise, if there is a RADIUS server connectivity issue and a user who has never before connected to the ECLYPSE controller will be locked out from the controller. It is particularly important for admin user credentials to be cached on each controller as an admin user can change the controller's network connection parameters that may be at cause for the loss of connectivity to the RADIUS server.

RADIUS Server Architectures

Local Credential Authentication

Each device has its own credential database in the local credential authentication architecture. This approach is labor-intensive as multiple credential database instances must be maintained.

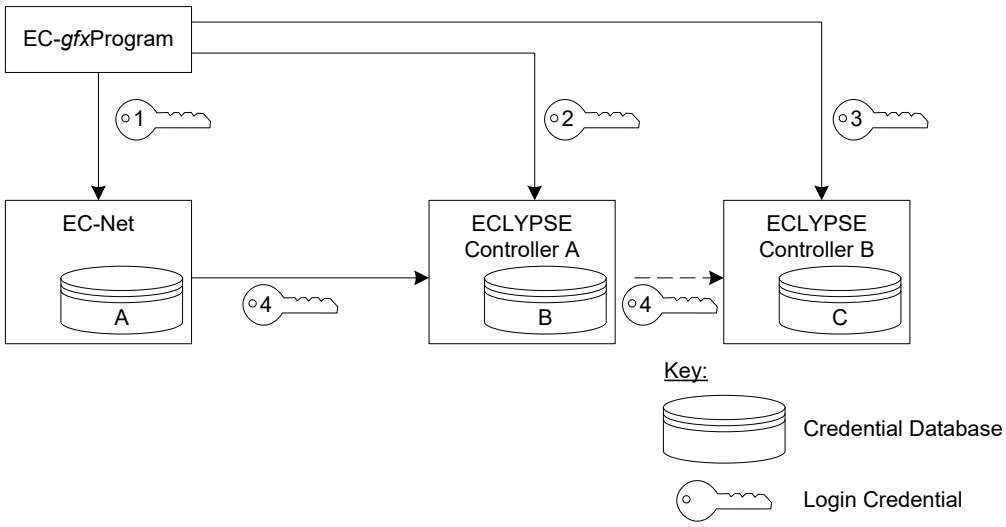


Figure 31: Local Credential Authentication

This authentication method has the following components.

Component	Description
Login Credential 1	This is the login credential used by an EC-*gfx*Program user to connect to the EC-Net station. This credential is managed in the EC-Net User Service.
Login Credential 2	This is the login credential used by an EC-*gfx*Program user to connect to ECLYPSE controller A. This credential is managed in controller's A *User Management* credential database.
Login Credential 3	This is the login credential used by an EC-*gfx*Program user to connect to ECLYPSE controller B. This credential is managed in controller's B *User Management* credential database.
Login Credential 4	This is the login credential used by the EC-Net station's RestService to connect to ECLYPSE controller A and B. To program an ECLYPSE controller with EC-*gfx*Program through EC-Net, the RestService must be configured on the EC-Net station with a login credential to all ECLYPSE controllers. This credential is managed in this controller's A and B *User Management* credential databases.
Credential Database A	This is the EC-Net station UserService credential database.
Credential Database B and C	This is the ECLYPSE controller A's credential database and ECLYPSE controller B's credential database. If EC-*gfx*Program users are to connect to either of these controllers through the EC-Net station, the controller's credential database must have the credentials for EC-Net station's RestService. Each credential database must also have the credentials for each user that will login to ECLYPSE controller A (for example, administrators, direct connection EC-*gfx*Program users, ENVYSION users, etc.). See *User Management*.

ECLYPSE-Based Centralized Credential Authentication

The credential database is centralized in an ECLYPSE controller that is configured as a RADIUS server, to authenticate login requests made directly to it, and by other subscribed ECLYPSE controllers. This architecture is ideal when you are not using EC-Net on your network.

EC-Net cannot subscribe to a remote RADIUS server. Due to this, you will have to add user credentials to both the ECLYPSE RADIUS server and to the EC-Net station. For this reason, if you are using EC-Net on your network, it is best to centralize credential authentication by using this EC-Net station as a RADIUS server. See *User Management*.

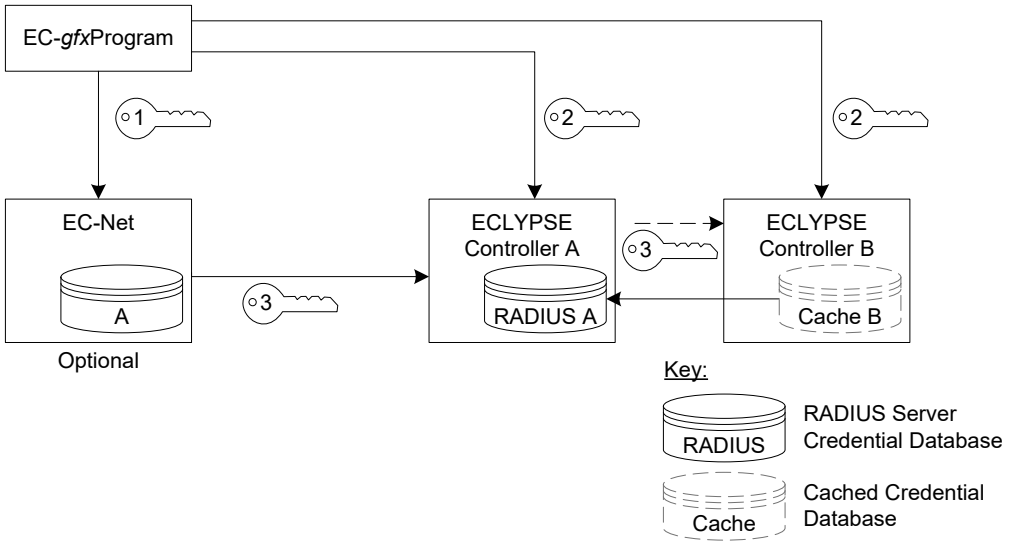


Figure 32: ECLYPSE-Based Centralized Credential Authentication

This authentication method has the following components.

Component	Description
Login Credential 1	This is the login credential used by an EC-*gfx*Program user to connect to the EC-Net station. This credential is managed in the EC-Net User Service.
Login Credential 2	This is the login credential used by an EC-*gfx*Program user to connect to ECLYPSE controller A. This credential is managed in controller's A *User Management* credential database.
Login Credential 3	This is the login credential used by the EC-Net station's RestService to connect to any ECLYPSE controller. To program an ECLYPSE controller with EC-*gfx*Program through EC-Net, the RestService must be configured on the EC-Net station with a login credential to all ECLYPSE controllers. This credential is managed in this ECLYPSE controller A's *User Management* RADIUS server credential database.
Credential Database A	This is the EC-Net station UserService credential database. This credential database is independent of all other credential databases.
RADIUS Server A Credential Database	This is the ECLYPSE controller A's RADIUS Server credential database. If EC-*gfx*Program users are to connect to this controller through the EC-Net station, this credential database must have the credentials for EC-Net station's RestService. This credential database must also have the credentials for each user that will login to any ECLYPSE controller (for example, administrators, direct connection EC-*gfx*Program users, ENVYSION users, etc.). See *User Management*.
Credential Database Cache B	This is the ECLYPSE controller B's cached credential database. If the connection to ECLYPSE controller A's RADIUS Server is lost, users that have previously authenticated themselves with the ECLYPSE controller A's RADIUS Server credential database on a given controller will still be able to login to those controllers as their credentials are locally cached.

EC-Net-Based Centralized Credential Authentication

The credential database is centralized in an EC-Net station to authenticate login requests made by all other subscribed ECLYPSE controllers.

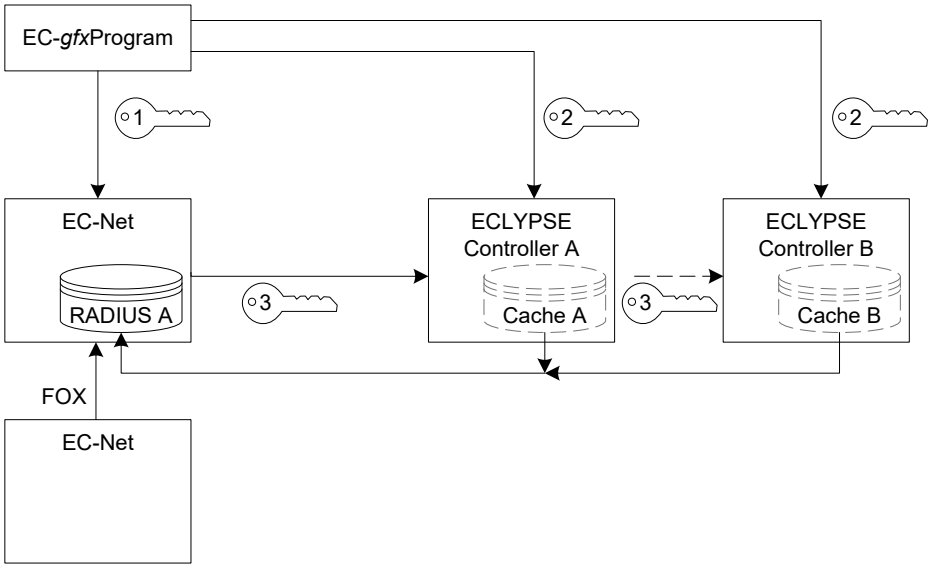


Figure 33: EC-Net-Based Centralized Credential Authentication

This authentication method has the following components.

Component	Description
Login Credential 1	This is the login credential used by an EC-*gfx*Program user to connect to the EC-Net station. This credential is managed in the EC-Net User Service.
Login Credential 2	This is the login credential used by an EC-*gfx*Program user to connect to any ECLYPSE controller. This credential is managed in the EC-Net User Service.
Login Credential 3	This is the login credential used by the EC-Net station's RestService to connect to any ECLYPSE controller. To program an ECLYPSE controller with EC-*gfx*Program through EC-Net, the RestService must be configured on the EC-Net station with a login credential to all ECLYPSE controllers. This credential is managed in the EC-Net User Service.
RADIUS Server A Credential Database	This is EC-Net station UserService credential database that is also a RADIUS Server credential database. If EC-*gfx*Program users are to connect to this controller through the EC-Net station, this credential database must have the credentials for EC-Net station's RestService. This credential database must also have the credentials for each user that will login to ECLYPSE controller A or B (for example, administrators, direct connection EC-*gfx*Program users, ENVYSION users, etc.). Note that other EC-Net stations can use FOX protocol to authenticate users on those stations.
Credential Databases Cache A and B	These are ECLYPSE controllers' cached credential databases. If the connection to the EC-Net station's RADIUS Server is lost, users that have previously authenticated themselves with EC-Net station's RADIUS Server credential database on a given controller will still be able to login to those controllers as their credentials are locally cached.

Configuring the EC-Net Station's RestService

To configure the REST service in EC-Net, refer to the EC-*gfx*Program Getting Started User Guide: Getting Started on EC-Net for ECB & ECY Series Controllers. Any ECLYPSE controller being connected to by the RestService must be able to authenticate the User name and password configured in the RestService configuration.

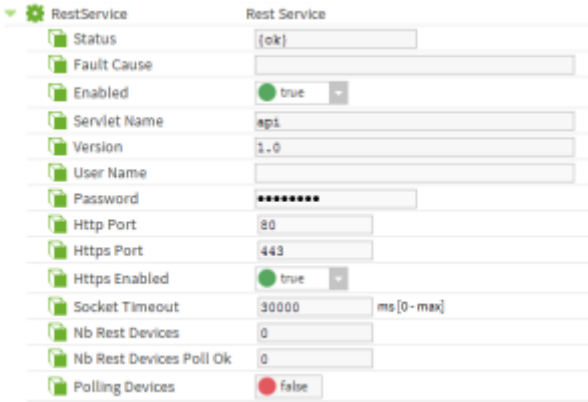


Figure 34: Typical RestService Configuration

Configuring the EC-Net Station's RadiusService

To configure the Radius Service in EC-Net, refer to the EC-*gfx*Program Getting Started User Guide: Getting Started on EC-Net for ECB & ECY Series Controllers.

A RADIUS server uses a challenge/response mechanism to authenticate a user's logon credentials (username and password). When one or more ECY Series controllers subscribe to a RADIUS server, this RADIUS server provides centralized user management to control which users have access to any of these ECY Series controllers.

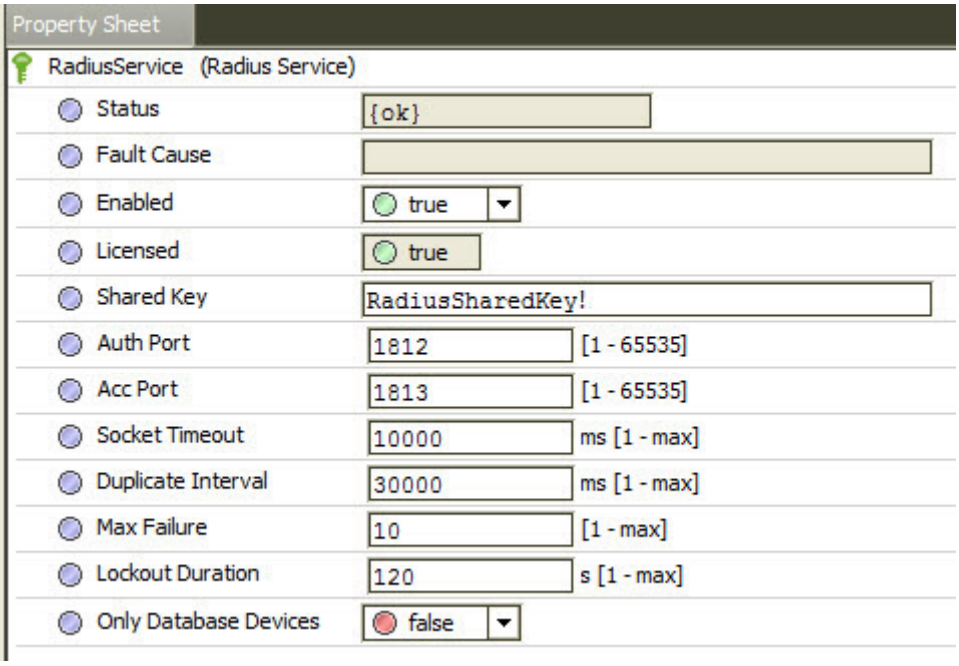


Figure 35: Typical Radius Service Configuration

See also *Setting Up the SSO Functionality through a Radius Server*

Information Technology Department-Managed Centralized Credentials Authentication

The credential database is centralized in a Microsoft Windows Domain Active Directory Server to authenticate login requests made by other subscribed ECLYPSE controllers and EC-Net stations.

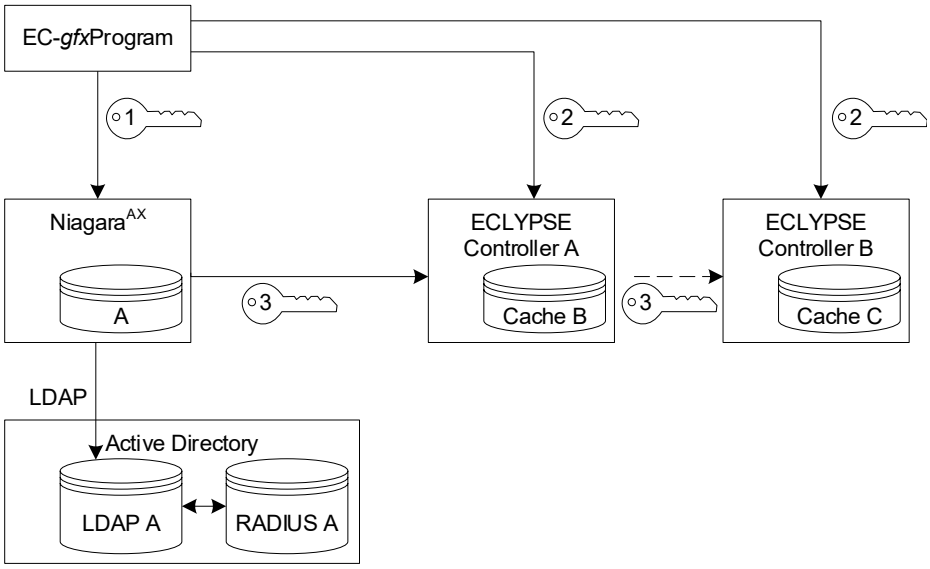


Figure 36: Information Technology Department-Managed Centralized Credentials Authentication

This authentication method has the following components.

Component	Description
Login Credential 1	This is the login credential used by an EC-*gfx*Program user to connect to the EC-Net station. This credential is managed in the EC-Net User Service. This credential must be added to the Active Directory LDAP credential database.
Login Credential 2	This is the login credential used by an EC-*gfx*Program user to connect to any ECLYPSE controller. This credential must be added to the Active Directory RADIUS credential database.
Login Credential 3	This is the login credential used by the EC-Net station's RestService to connect to any ECLYPSE controller. To program an ECLYPSE controller with EC-*gfx*Program through EC-Net, the RestService must be configured on the EC-Net station with a login credential to all ECLYPSE controllers. This credential must be added to the Active Directory RADIUS credential database.
LDAP A	This is the Microsoft Windows Domain Active Directory Server credential database that authenticates user credentials through both RADIUS and LDAP protocols for all ECLYPSE controllers and all subscribed EC-Net stations.
RADIUS A	This is EC-Net station UserService credential database that imports user credentials through an LDAP connection to the Active Directory. To program an ECLYPSE controller with EC-*gfx*Program through EC-Net, the RestService must be configured on the EC-Net station with a login credential to all ECLYPSE controllers. This credential must be added to the Active Directory credential database.
Credential Database A	These are ECLYPSE controllers' cached credential database. If the connection to the Active Directory is lost, users that have previously authenticated themselves with Active Directory Server credential database will still be able to login to the controller as their successfully authenticated credentials are locally cached.

To configure an EC-Net station to connect to an LDAP server, refer to the EC-Net LDAP Active Directory Configuration Guide and LDAP User Service.

CHAPTER 8
ECLYPSE Web Interface

This chapter describes the ECLYPSE controller's Web interface.

Overview

The ECLYPSE controller has a web-based interface that allows you to view system status, configure the controller, update the controller's firmware, and access applications associated to your projects.

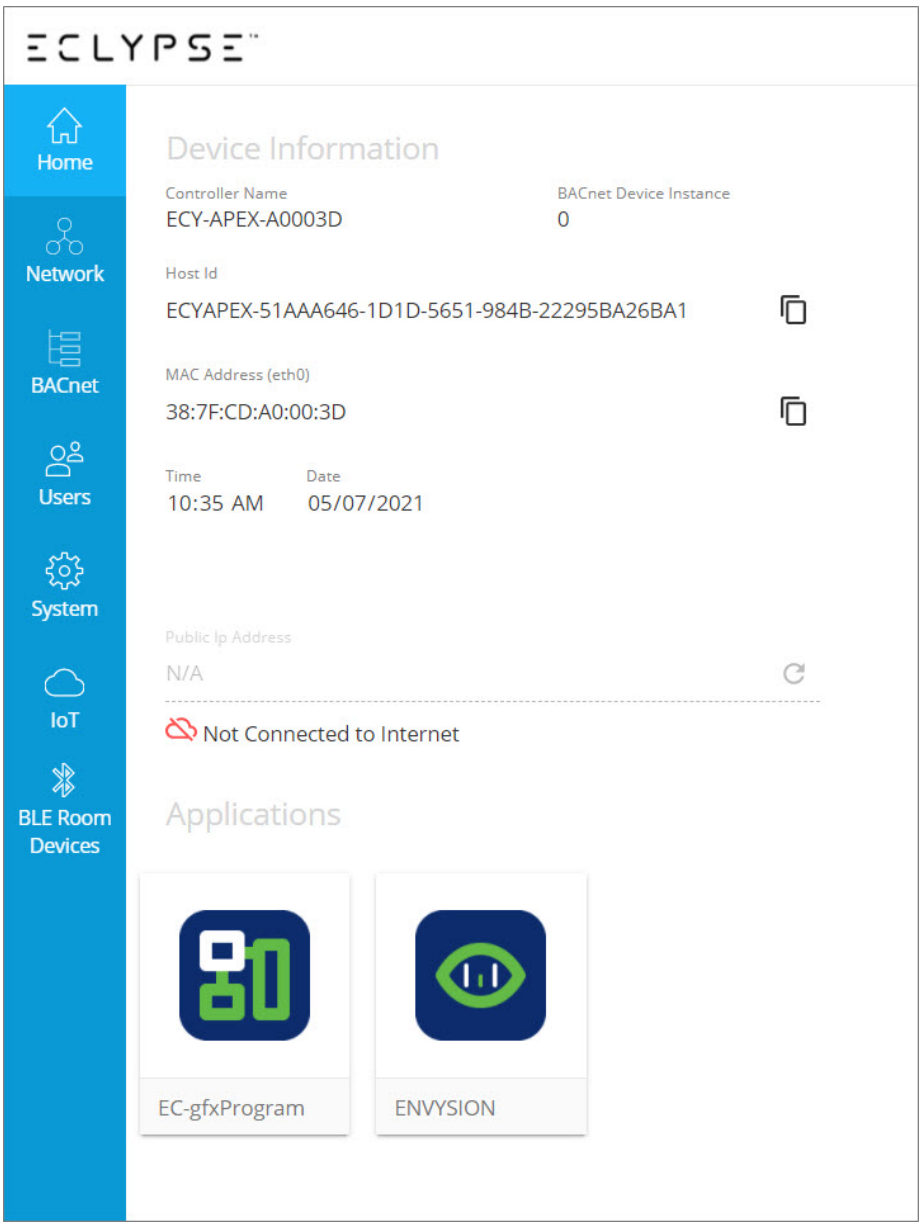


Figure 37: Example of an ECLYPSE Controller's Web Interface Welcome Home Page (options may vary)

Web Interface Main Menu

The sidebar contains the configuration menus that allow you to view and set the controller's configuration settings including its IP address, Wi-Fi settings, users, controller's firmware, and much more.

The menus may vary according to the associated device licenses and the user's access level. These configuration parameters are password protected.

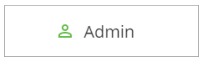
Home Page

The web interface home page consists of the following items:

Item	Description
Device Information	Basic information on the device such as controller name, device instance, host ID, MAC address, time, and date.
	Copy icon that allows you to copy the Host Id and/or the MAC address of the device to that you can quickly paste elsewhere as needed.
Public IP Address	IP address to access your ECLYPSE controller from a public network (e.g. Internet).
Connected/Not Connected to Internet	ECLYPSE controller Internet connection status.
Applications	Access different applications associated to your projects and controller license such as the following: ☐ **EC-*gfx*Program**: Access EC-*gfx*Program directly from the ECLYPSE Web Interface. Your password is required to allow access. ☐ **ENVYSION**: Embedded graphic design and visualization interface. Host system-based graphics such as Air Handling Units, Boiler Room, and more, directly from the controller. See the ENVYSION User Guide.

User Profile and Login Credentials

It is important to create new user accounts with strong passwords to protect the controller from unauthorized access.

The profile box 

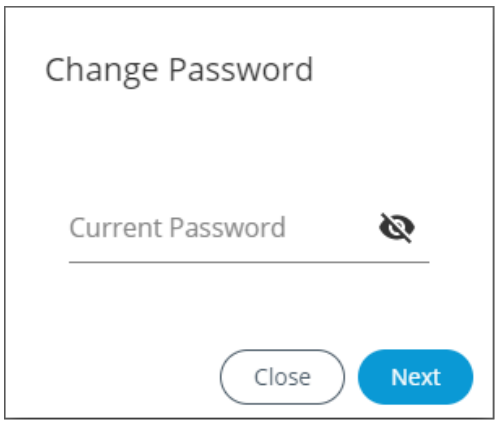
is used to change your password and logout from your ECLYPSE controller.

On your first login to an ECLYPSE controller, you will be prompted to change the factory default password. We recommend you choose a strong password for the 'admin' account as it gives full control over the controller.

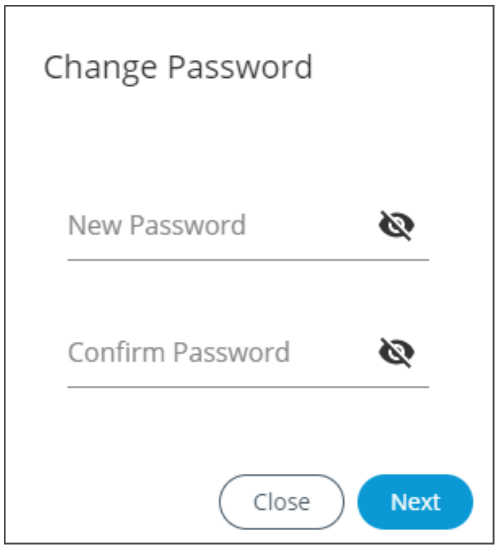
See *User Management*, *Securing an ECLYPSE Controller*, and *Supported RADIUS Server Architectures*.

To Change Your Password

1. To change your password, click the profile icon and select **Change Password**.



2. Enter your current password and click **Next**.



3. Enter the new password twice to confirm and click **Next**. Your password is changed.

Click the show password icon to see the password you are entering.

Network Settings

The **Network** menu is used to configure the ECLYPSE controller's network interface and setup the wired and wireless network configuration parameters. The available menus are:

- Ethernet
- Wireless
- Diagnostic

Ethernet

The Ethernet screen is used for any wired IP connections that are made through either one of the controller's **Ethernet Switch Pri**(mary) connector or **Ethernet Switch Sec**(ondary) connector. See *Network Connections for ECY Series Controllers*. The Wired IP parameters can be auto-configured when the connected network has a working DHCP server. The alternative is to manually configure the controller's IP parameters.

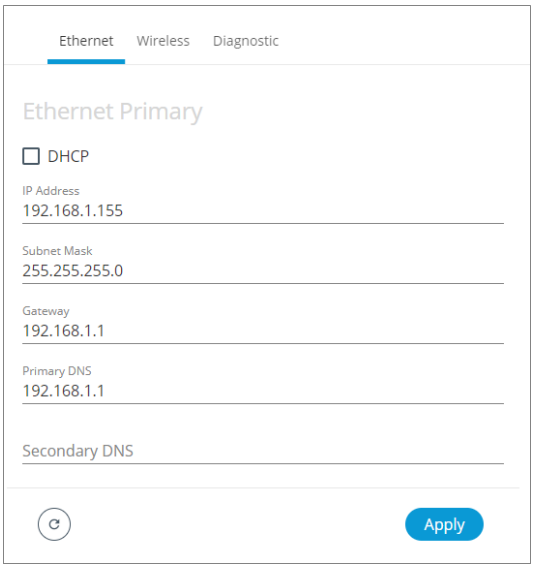


Figure 38: Primary Ethernet Configuration in ECLYPSE Web Interface

Option	DHCP Client: Enabled	DHCP Client: Disabled
DHCP	If the controller is connected to a network that has an active DHCP server, enabling this option will automatically configure the Wired IP connection parameters. The Wired IP parameters shown below are read only (presented for information purposes only).	If you want to manually configure the controller's network settings (to have a fixed IP address for example) or in the case where the network does not have a DHCP server, disable this option. In this case, you must set the Wired IP connection parameters shown below to establish network connectivity. See also *DHCP Versus Manual Network Settings*.
IP Address	IP Address provided by the network's DHCP server.	Set the IP address for this network device. See *IPv4 Communication Fundamentals*. Ensure that this address is unique from all other device on the LAN including any used for a hot spot's IP addressing.
Subnet Mask	Subnet mask provided by the network's DHCP server.	Set the connected network's subnetwork mask. See *About the Subnetwork Mask*.
Gateway	Gateway IP address provided by the network's DHCP server.	The IP address of the default gateway to other networks. This is usually the IP address of the connected network router. See *Default Gateway*.
Primary DNS Secondary DNS	Primary and secondary DNS IP Address provided by the network's DHCP server.	The connected network's primary and secondary IP address of the DNS servers. See *Domain Name System (DNS)*.

When making changes to the network settings, click **Apply** to apply and save the changes. You can click refresh to refresh the information in the screen.

Wireless Configuration

This configuration interface is for any ECLYPSE Wi-Fi Adapter connected to the **HOST** connector.

A hotspot creates a subnetwork. As a result, any connected BACnet device will not be able to discover BACnet devices on any other LAN subnetwork.

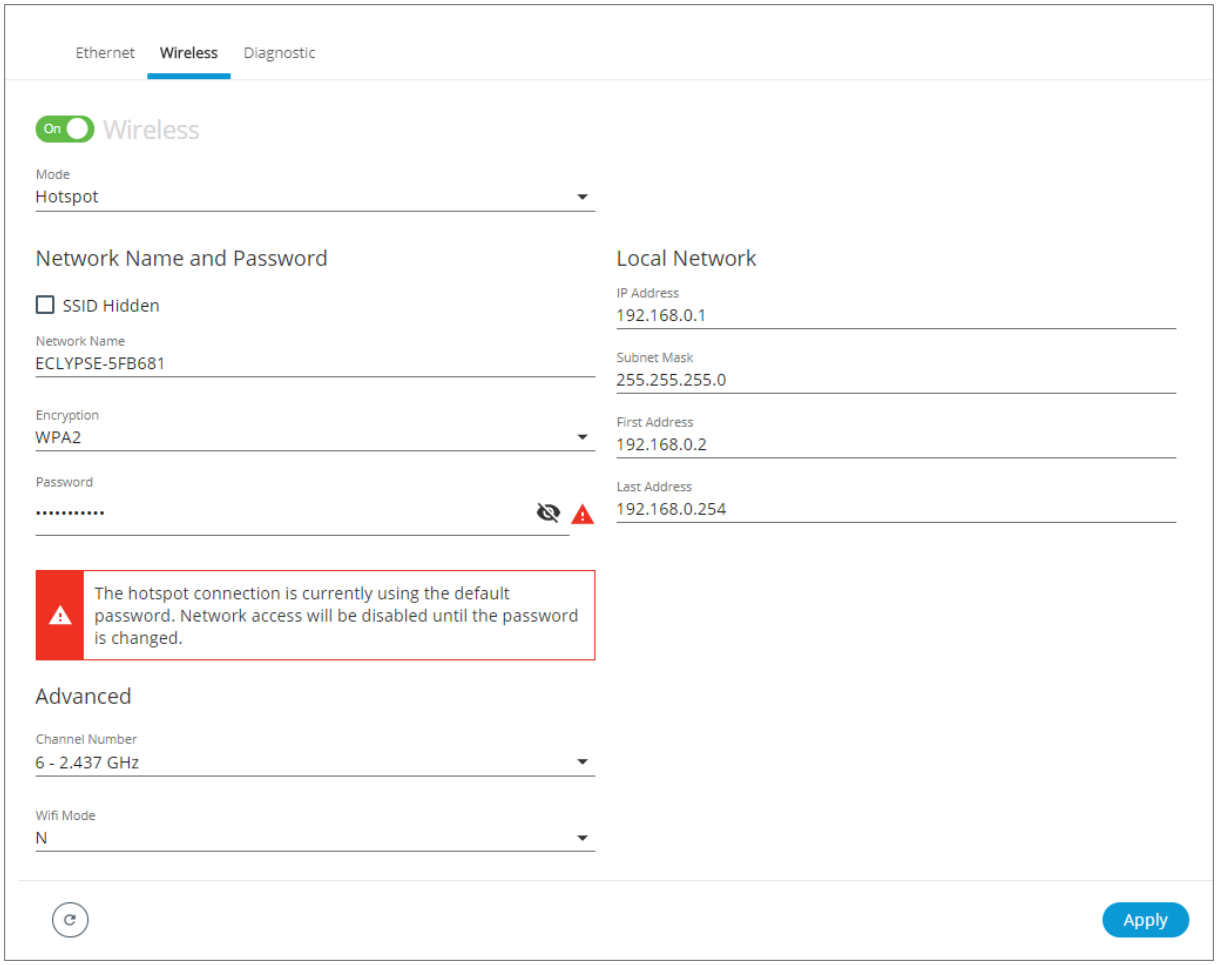


Figure 39: The Wi-Fi network operating modes: Hotspot, Access-Point, or Client.

The Wireless connection parameters can be set as follows.

Item	Description
On / Off On Off	Enable/disable the controller's wireless features.
Wireless Mode	Select the Wi-Fi network operating mode: Hotspot, Access-Point, or Client. **Hotspot**: This creates a Wi-Fi hotspot with a router. See *Setting up a Wi-Fi Hotspot Wireless Network* for how to configure this mode. **Access-Point**: This creates a Wi-Fi access point. See *Setting up a Wi-Fi Access Point Wireless Network* for how to configure this mode. **Client**: this connects the controller as a client of a Wi-Fi access point. See *Setting up a Wi-Fi Client Wireless Network* for how to configure this mode. See also *ECLYPSE Wi-Fi Adapter Connection Modes*.
SSID Hidden	Hide or show the Service Set IDentification (SSID).
Network Name	The Service Set IDentification (SSID) for a Wi-Fi hotspot. This parameter is case sensitive. When this controller's active mode is configured as a: For **Hotspot**: set a descriptive network name that other wireless clients will use to find this hotspot.

Item	Description
	For **Client**: select an available hotspot from the lists of access point connections that are within range. Click the Wi-Fi icon to select an available Wi-Fi network from the list of access points that are within range.
Encryption	Set the encryption method to be used by the Wi-Fi network: ☐ **Open**: this option should be avoided as it does not provide any wireless security which allows any wireless client to access the LAN ☐ **WPA2**: select the Wi-Fi Protected Access II option to secure the Wi-Fi network with a password. ☐ **WPA2E**: Use this option if you are connecting to an enterprise network that has a working RADIUS authentication server. This RADIUS server provides user authentication.
Password	When encryption is used, set the password to access the Wi-Fi network as a client or the password other clients will use to access this hotspot. Passwords should be a long series of random alphanumeric characters and symbols that are hard to guess. This parameter is case sensitive. If using a Hotspot connection, network access will be disabled until the default password is changed. If using an Access Point connection, the default password must be changed before you can save and apply your changes to this page.
	Click to show or hide the password.
IP Address	IP address for a Hotspot (or gateway address that wireless clients will connect to). Ensure that this address is: ☐ Not in the range of IP address set by **First Address** and **Last Address**. ☐ Not the same as the **IP address** set under IP Configuration for the wired network.
Subnet Mask	The hotspot's subnetwork mask. See *About the Subnetwork Mask*.
First Address Last Address	The range of IP addresses to be made available for Hotspot clients to use. The narrower the range, the fewer hotspot clients will be able to connect due to the lack of available IP addresses. For example, a range where First Address = 192.168.0.22 and Last Address = 192.168.0.26 will allow a maximum of 5 clients to connect to the hotspot on a first-to-connect basis.
Advanced	When a Hotspot or Access-point is configured, this sets the channel width and number the hotspot is to use. The wireless mode can also be set. See below.
Channel Number	Sets the center frequency of the transmission. If there are other Wi-Fi networks are nearby, configure each Wi-Fi network to use different channel numbers to reduce interference and network drop-outs. **NOTE:** The range of available channels may vary from country to country.
Wi-Fi Mode	Sets the wireless mode (wireless G or wireless N). Wireless N mode is backwards compatible with wireless G and B. Wireless G mode is backwards compatible with wireless B.
	Click to refresh the information in the list.
Apply	Click **Apply** to apply and save the changes

Network Diagnostics

The **Diagnostic** menu provides a number of tools to diagnose network connectivity issues between controllers.

- **Wi-Fi Monitor**: shows the current performance of a Wi-Fi connection with another controller.
- **Ping Monitor**: shows the round trip time it takes for a ping packet to go to an IP address and come back.

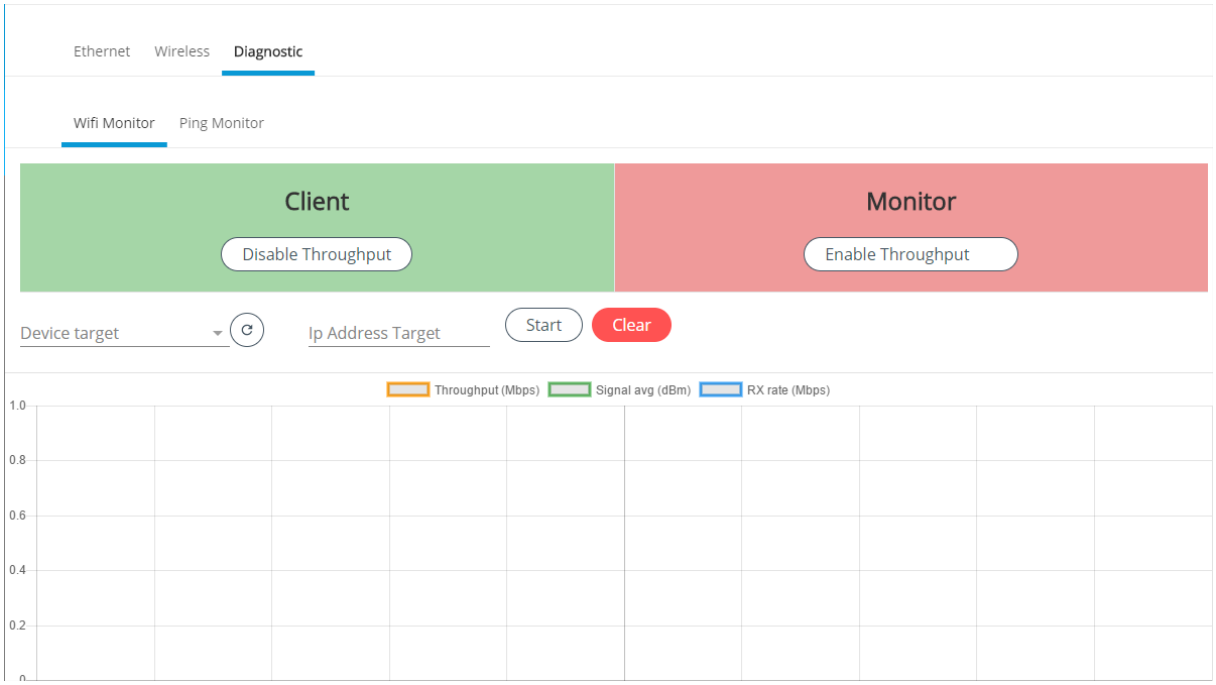


Figure 40: Network Diagnostics – Wi-Fi Monitor

Item	Description
Disable Throughput	Disables the Wi-Fi Monitoring throughput client service. For Wi-Fi monitor to work, this must be started.
Enable Throughput	Activates the Wi-Fi Monitoring throughput client service. For Wi-Fi monitor to work, this must be started.
Device Target	Select the corresponding controller's MAC address in the **Device Target** list.
Ip Address Target	Enter the corresponding controller's IP address for its Wi-Fi interface in **Ip Address Target**.
	Click to refresh the information in the **Device Target** list.
Start	Starts graphing the monitored data.
Clear	Clears the graph.
Throughput (Mbps)	Transmit datarate to the target.
Signal avg (dBm)	Current average received signal strength. **Note:** Signal strength is measured in negative units where the stronger the signal, the closer it is to zero. A weaker signal strength will have a more negative number. For example, a receive signal strength of -35 dBm is much stronger than a receive signal strength of -70 dBm.
RX rate (Mbps)	Receiving data rate from the target.

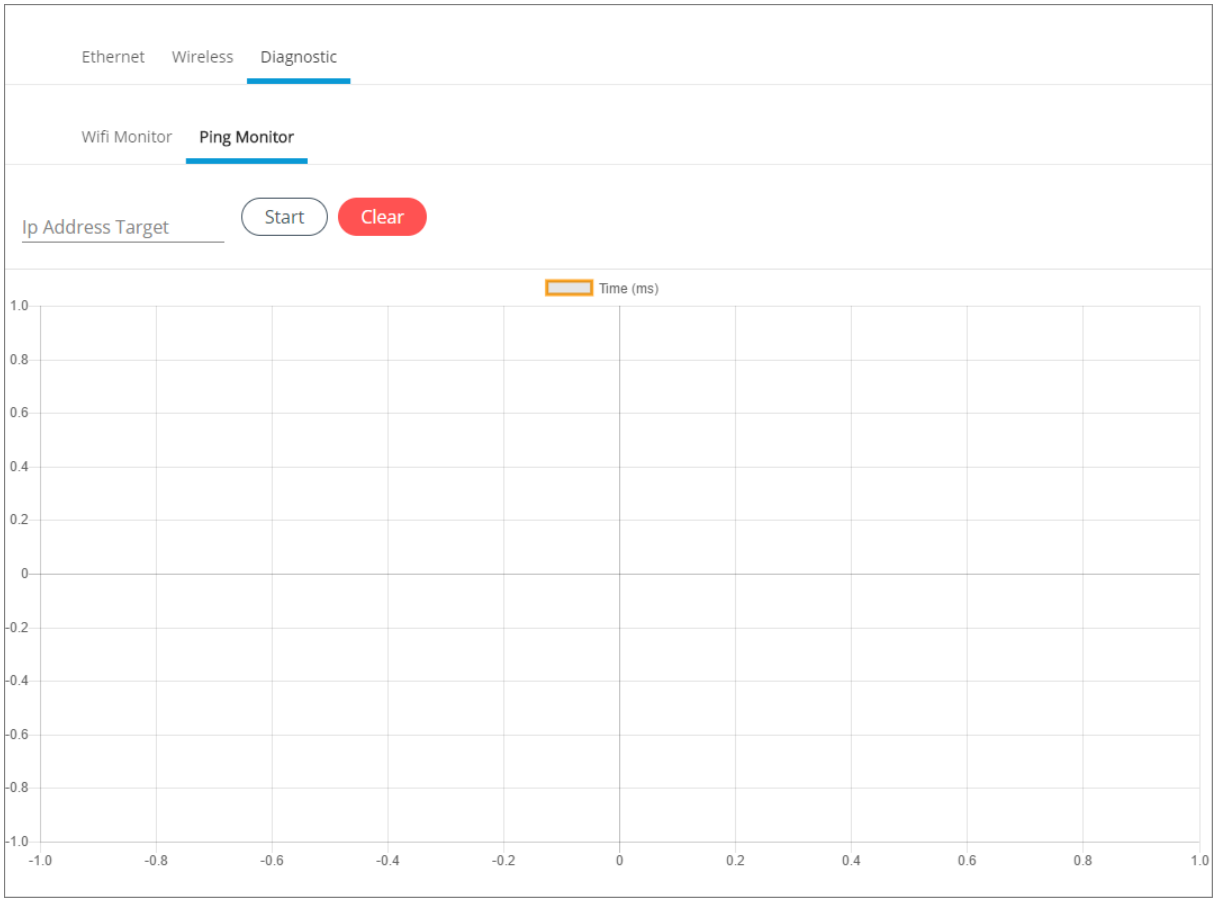


Figure 41: Network Diagnostics – Ping Monitor

Item	Description
Ip Address Target	Enter the corresponding controller's IP address for its Wi-Fi interface in **Ip Address Target**.
Start	Starts graphing the monitored data.
Clear	Clears the graph.

BACnet Settings

This is where the BACnet interface parameters are set.

General

This sets the controller's BACnet network parameters.

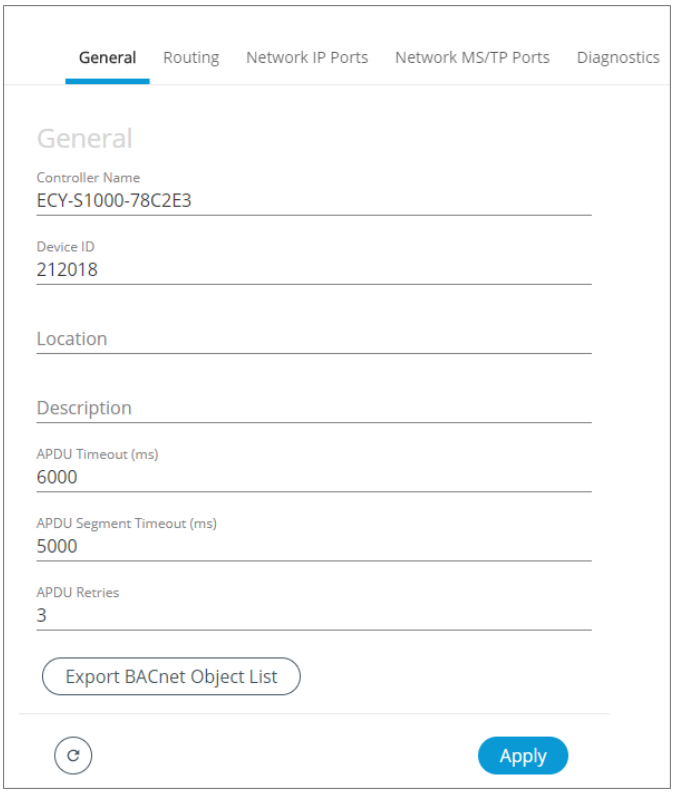


Figure 42: General BACnet Settings

Item	Description
Controller Name	Set a descriptive name by which this controller will be known to other BACnet objects.
Device ID	Each controller on a BACnet intra-network (the entire BACnet BAS network) must have a unique Device ID. Refer to the Network Guide for more information.
Location	Current controller's physical location. This is exposed on the BACnet network as a device object property.
Description	Description of the controller's function. This is exposed on the BACnet network as a device object property.
APDU Timeout (ms)	Maximum amount of time the controller will wait for an acknowledgment response following a confirmed request sent to a BACnet device before re-sending the request again or moving onto the next request. This property is exposed on the BACnet network as a device object property.
APDU Segment Timeout (ms)	Maximum amount of time the controller will wait for an acknowledgment response following a confirmed segmented request sent to a BACnet device before re-sending the segmented request again or moving onto the next request. This property is exposed on the BACnet network as a device object property.
APDU Retries	Sets the number of times to retry a confirmed request when no acknowledgment response has been received. This property is exposed on the BACnet network as a device object property.
Export BACnet Object List	Export all controller BACnet variables to a file (.csv).
↻	Click to refresh the information in the list.
Apply	Click **Apply** to apply and save the changes

Routing

This enables the routing of BACnet packets between BACnet MS/TP controllers connected to the ECLYPSE Connected System Controller's RS-485 port and BACnet/IP controllers connected to the ECLYPSE Connected System Controller's Ethernet Switch ports. For example, routing must be enabled for EC-Net to discover the BACnet MS/TP controllers connected to the ECLYPSE Connected System Controller's RS-485 port.

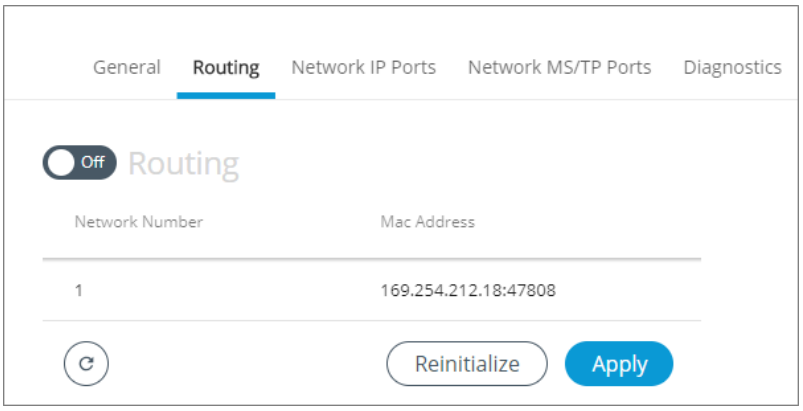


Figure 43: BACnet Routing Configuration

Item	Description
On / Off On Off	Enables/disable the routing of BACnet packets between BACnet MS/TP controllers connected to the ECLYPSE Connected System Controller's RS-485 port and BACnet/IP controllers connected to the ECLYPSE Connected System Controller's Ethernet Switch ports.
Network Number	Network number that identifies a LAN for routing purposes. All controllers with the same network number are members of the same logical BACnet network. See *Device Addressing*.
Mac Address	Device Mac address.
	Click to refresh the information in the list.
Apply	Click **Apply** to apply and save the changes.

Network IP Ports

This sets the IP network configuration parameters (on-board port) as well as the BACnet Broadcast Management Device (BBMD) and Foreign Device for intranetwork connectivity.

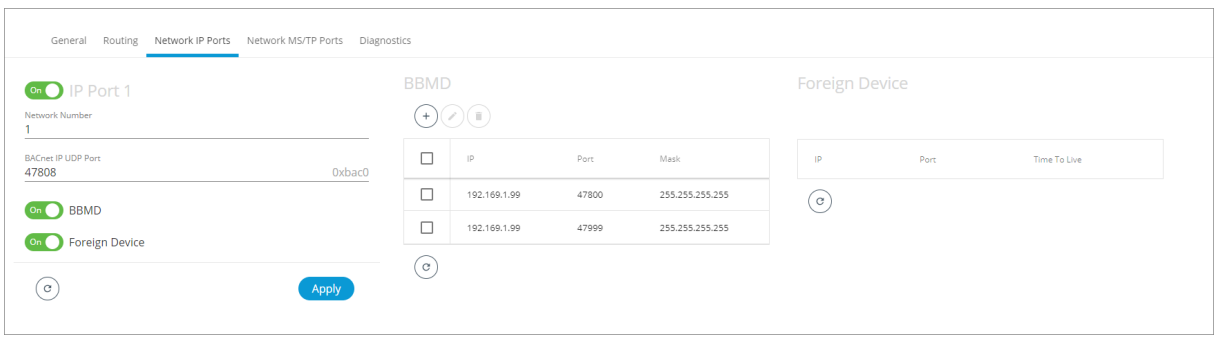


Figure 44: BACnet IP Configuration - Network IP Ports

On-Board Port

Item	Description
On / Off On Off	Enables/disables the routing of BACnet packets between BACnet MS/TP controllers connected to the ECLYPSE Connected System Controller's RS-485 port and BACnet/IP controllers connected to the ECLYPSE Connected System Controller's Ethernet Switch ports.
Network Number	Network number that identifies a LAN for routing purposes. All controllers with the same network number are members of the same logical BACnet network. See *Device Addressing*.
BACnet IP UDP Port	Standard BACnet/IP port number (UDP 47808) used by BACnet devices to communicate.
Enable BBMD	BBMD allows broadcast message to pass through a router. See *BBMD Settings*. To enable this feature, set **Enable BBMD** on only one device on each subnet.
Enable Foreign Devices	Foreign Device Registration allows a BACnet/IP device to send broadcast messages to a device with BBMD enabled. See *Foreign Device Settings*. To enable this feature, set **Enable Foreign Devices** on only one device on each subnet.
	Click to refresh the information in the list.
Apply	Click **Apply** to apply and save the changes.

BBMD Settings

BACnet/IP devices send broadcast discovery messages such as "Who-Is" as a means to discover other BACnet devices on the network. However, when there are two or more BACnet/IP subnetworks, broadcast messages do not pass through network routers that separate these subnetworks.

BBMD allows broadcast message to pass through a router: on each subnet, a single device has BBMD enabled. Each BBMD device ensures BACnet/IP connectivity between subnets by forwarding broadcast messages found on its subnetwork to each other, and then onto the local subnetwork as a broadcast message.

In the BBMD table, add the BBMD-enabled controllers located on other subnetworks. To add a BBMD:

1. Click .

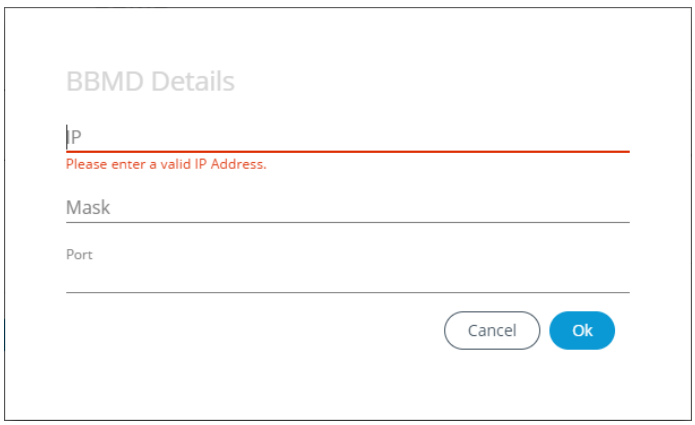


Figure 45: Adding a BBMD

2. In the **IP** field, enter IP address of the BBMD located on the other subnetwork.
3. In the **Mask** field, enter the subnetwork mask for the other subnetwork.
4. In the **Port** field, enter the port number for the BACnet service of the BBMD located on the other subnetwork.
5. Click **OK**.

You can also edit or delete a BBMD selected from the list using the Edit icon or Delete icon provided.

Foreign Device Settings

Some BACnet/IP devices also support a feature called Foreign Device Registration (FDR). FDR allows a BACnet/IP device to send broadcast messages to a device with BBMD enabled. The BBMD-enabled device will then forward these broadcast messages to all other BBMDs and onto all other FDR devices. If a subnet has only FDR supported devices, then it does not need a local BBMD. These devices can register directly with a BBMD on another subnetwork.

Item	Description
IP	IP address of a controller (foreign device) located on another subnetwork.
Port	Delay after which the foreign device is forgotten.
Time to Live	Time-to-live value that serves as a timestamp attached to the data. Once the timespan has elapsed, data is discarded.
	Click to refresh the information in the list.

Network MS/TP Ports

Some controller models support up to three RS-485 ports. Some controllers only support Modbus RTU on its RS-485 port. See the controller's datasheet for more information.

BACnet MS/TP and Modbus RTU communications are made by connecting directly to separate RS-485 ports. **On-board RS-485 Port** is the controller's onboard RS-485 port. When an ECY-RS485 expansion module is attached to the controller, **ECY-RS485 Module Port 1** is port #1 and **ECY-RS485 Module Port 2** is port #2 on that module. The following network configuration parameters are for an RS-485 port that is used to communicate with BACnet MS/TP controllers.

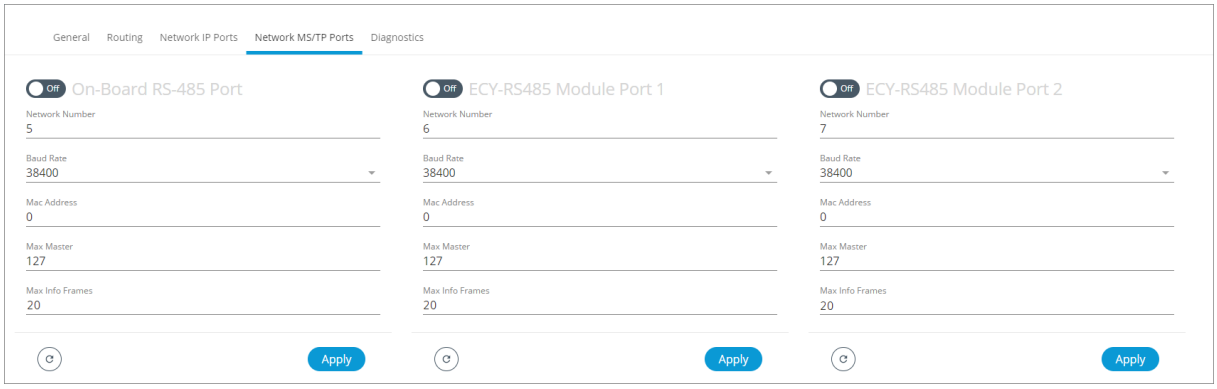


Figure 46: Network MS/TP Ports

Item	Description
On / Off On Off	Enables/disables the controller's BACnet MS/TP connection. If the controller has been configured to use Modbus RTU, this option cannot be enabled. First disable Modbus RTU in EC-gfxProgram.
Network Number	Network number identifies a LAN for routing purposes. All controllers with the same network number are members of the same logical BACnet network. See *Device Addressing*.
Baud Rate	Recommended baud rate setting is 38 400. See *Baud Rate*.
Mac Address	ECY series controller's MAC Address on the BACnet MS/TP Data Bus.
Max Master	When commissioning a BACnet MS/TP Data Bus, it is useful to start with the Max Master set to 127 so as to be able to discover all devices connected to the data bus. Then, once all devices have been discovered and the MAC Addressing is finalized by eliminating any gaps in the address range, set the Max Master (the highest MAC Address) to the highest Master device's MAC Address number to optimize the efficiency of the data bus. See *Setting the Max Master and Max Info Frames*.
Max Info Frames	For the ECY series controller, this should be set to 20. See *Setting the Max Master and Max Info Frames*.
	Click to refresh the information in the list.
Apply	Click **Apply** to apply and save the changes.

Secure Connect

This enables a secure connection to a hub on the BACnet/SC network.

The communications using BACnet/SC occur over TLS 1.3 (see Web Server Access). This is the worldwide IT standard for secure communication. Data sent via TLS is encrypted before being sent.

Hub-to-Node communications are fully encrypted. Since any platform using BACnet/SC is using a full TCP/IP stack with TLS, it's induced additional time for the Device to decrypt and encrypt all the data compared to standard BACnet communication working over UDP/IP.

Special care should be taken regarding the number of messages exchanged between devices (number of points, polling policies, etc.) With the current platform, we do not recommend having Communication above 900 messages per minutes (RX/TX) as shown in the BACnet Diagnostic page to avoid contingencies or bootup issues.

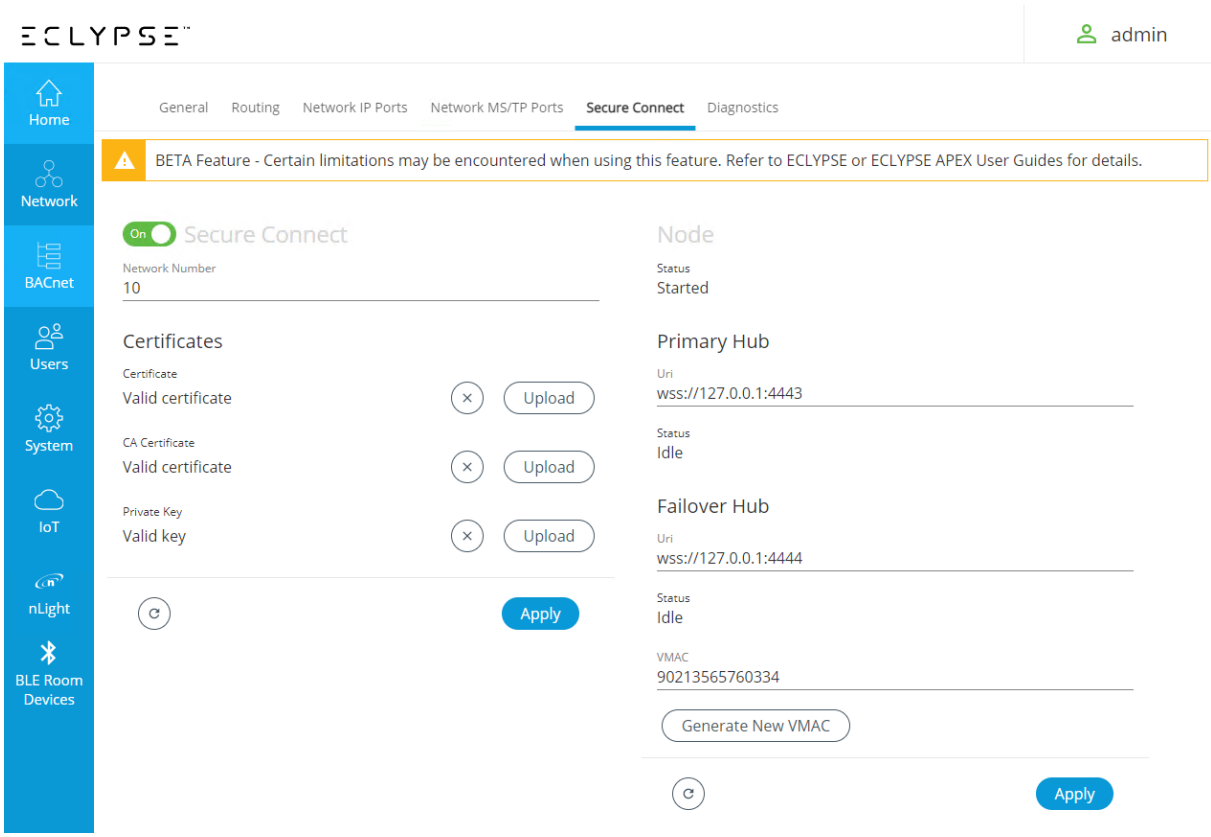


Figure 47: Secure Connect BACnet Settings

Item	Description
On / Off On Off	Enables/disables the controller's Secure Connect features.
Network Number	Enter a network number to identify a LAN for routing purposes. All controllers with the same network number are members of the same logical BACnet network. See Device Addressing.

Certificates

Certificates are required for the device to be authenticated on the BACnet/SC network.

Item	Description
Certificate	Upload a signed BACnet/SC client certificate to authenticate this device. File format is *.pem*.
CA Certificate	Upload the certificate used to sign the BACnet/SC client certificate for this device. File format is *.pem*.
Private Key	Upload the private key of the device's certificate. File format is *.key*.

Node

Item	Description
Status	Indicates the connection status of the network.

Primary Hub

Item	Description
URI	Uniform Resource Identifier (URI) identifies a resource and contains a URL and/or a URN. Specify the URI of the primary hub to connect (ex: wss://192.168.1.1/api/bacnet/sc/hub)
Status	Indicates the connection status of the Primary Hub.

Failover Hub

Item	Description
URI	Uniform Resource Identifier (URI) identifies a resource and contains a URL and/or a URN. Specify the URI of the failover hub to connect (ex: wss://192.168.1.1/api/bacnet/sc/hub)
Status	Indicates the connection status of the Failover Hub.

VMAC

Item	Description
VMAC	Configures a unique Virtual MAC (VMAC) address for the device. The driver initially sets this value to a random set of six bytes (six octets). Click Generate New VMAC if you need to change this number.

Diagnostics

Some controller models support up to three RS-485 ports. Some controllers only support Modbus RTU on its RS-485 port. See the controller's datasheet for more information.

BACnet MS/TP and Modbus RTU communications are made by connecting directly to separate RS-485 ports. On-board RS-485 Port is the controller's onboard RS-485 port. When an ECY-RS485 expansion module is attached to the controller, ECY-RS485 Module Port 1 is port #1 and ECY-RS485 Module Port 2 is port #2 on that module.

The following Diagnostics tab provides information on live values passing through the RS-485 ports. By default, the live values are displayed. You can stop and restart the streaming of the live values using the Stop Live Values/Start Live Values button.

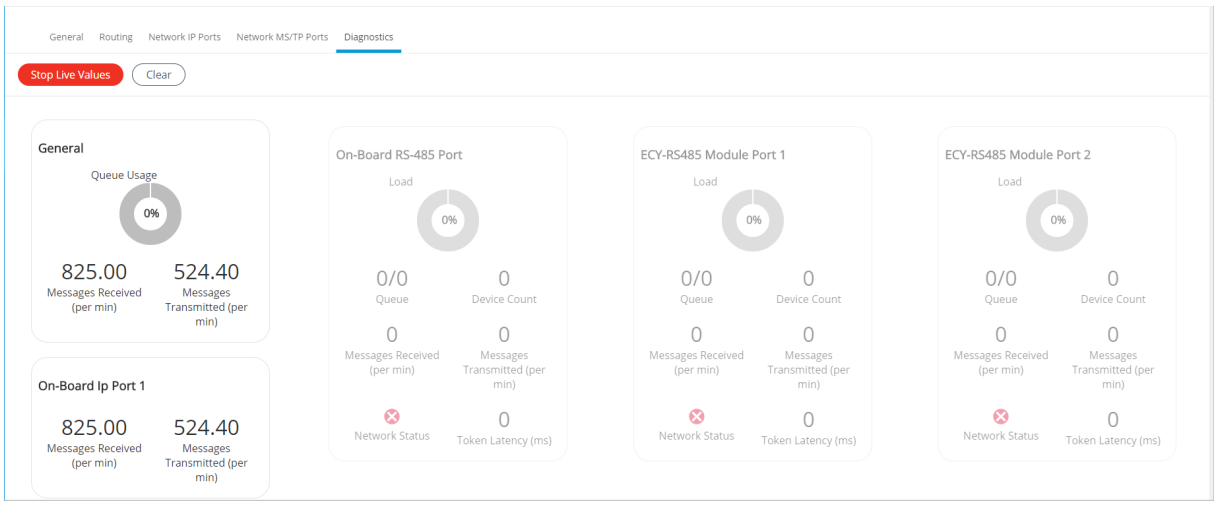


Figure 48: BACnet Diagnostics

User Management

User management is the control of who can access the controller by enforcing the authentication credentials users need to access the controller. User management can either be managed in *Server* or *Client* mode. You can also set the Welcome page a user will land on when they connect to the controller.

An ECLYPSE controller can manage users through several mechanisms. It can either be in *Server* mode that provides a user database to other ECLYPSE controllers and itself, or in Client mode for access to a remote user database.

You can provide appropriate privileges to users depending on the clearance level desired for each role. You can also modify user properties and customize the user experience by assigning a Welcome page to each user.

Server/Client User Configuration

When you configure an ECLYPSE controller in server mode, you can add new users, select their roles, and choose their custom Welcome page. This page will be the default page displayed after a user logs in to an ECLYPSE controller.

If you configure an ECLYPSE controller in client mode, you can only choose the Welcome page displayed to a user. Any other information will be retrieved from the remote server. The Welcome page chosen in client mode has priority over the one configured in the server.

Adding a User in Server Mode

Adding a user creates a user profile that allows a person to login to the controller with a username / password combination and to have access to certain controller software interfaces. These users will have login access to the controller. It is important to create new user accounts with strong passwords to protect the controller from unauthorized access. See also *Password Policy* and/or *Securing an ECLYPSE Controller*

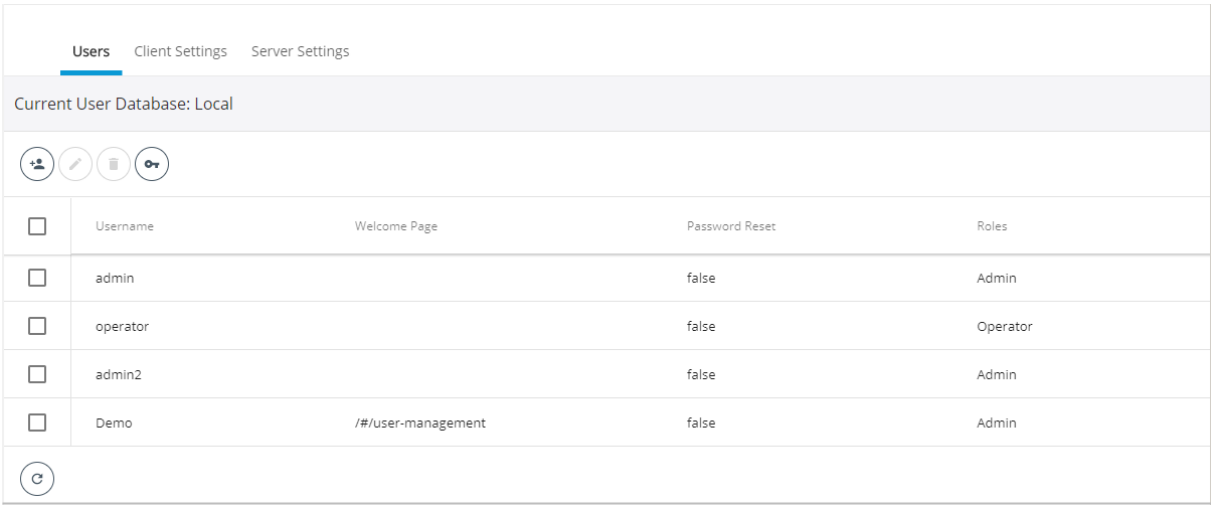


Figure 49: Adding Users in Server Mode

1. Click the Add User icon to add a new user or select a user and click edit to edit an existing user. The **User Details** window is displayed.

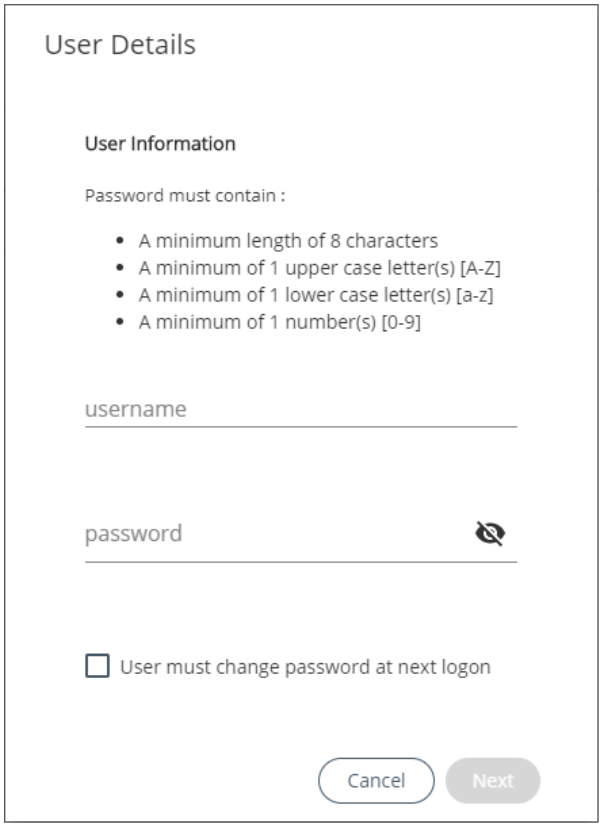


Figure 50: Adding a User

2. Enter the information as shown below:

Item	Description
Username	User's login credential.
Password	User's password credential.
	Show/Hide the user's password credential.
User must change password at next login	Select to force user to change their password at the next login.

3. Click Next. The Roles options are displayed.

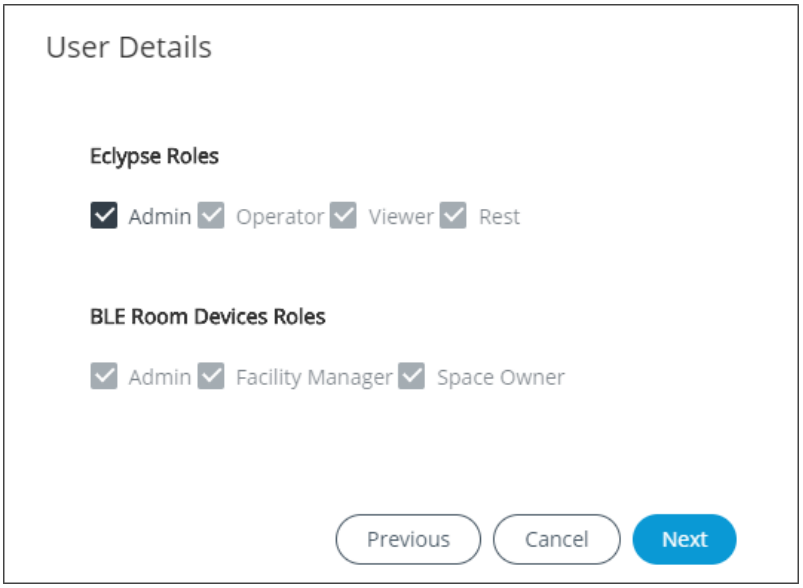


Figure 51: User Details - Roles

4. Select the access levels the user will be able to use. Set one or more options according to the user's role:

ECLYPSE Roles	Description
Admin	Allows user access to the ENVYSION studio and viewer. The user can also view and modify all configuration interface parameters and program the controller with EC-*gfx*Program. When this option is chosen, the user also receives Admin access for BLE Room Device Roles.
Operator	Allows user access to the ENVYSION interface in viewing mode as well as gives partial access to the ECLYPSE Web Configuration Interface. Certain configuration interface screens are unavailable such as User Management, Viewer Information, etc.
Viewer	Allows user access to the ENVYSION interface in Viewing mode. The user is not allowed to access the ECLYPSE Web Configuration Interface.
Rest	Allows a user to program the controller with EC-*gfx*Program. This user does not have access to the ECLYPSE Web Configuration Interface or ENVYSION.

Table 3: ECLYPSE Roles

BLE Room Device Roles	Description
Admin	Allows full read/write access to BLE room devices such as changing the Subnet ID, PIN Code, Advanced Settings, and Bluetooth settings.
Facilities Manager	Allows read/write access for the PIN Code, Advanced Settings, and Bluetooth settings.
Space Owner	Allows read access for the PIN Code, and read/write access for Advanced Settings.

Table 4: BLE Room Device Roles

5. Click **Next**. The **Welcome Page** screen is displayed allowing you to define the user's landing page that will be displayed when they login to the controller.

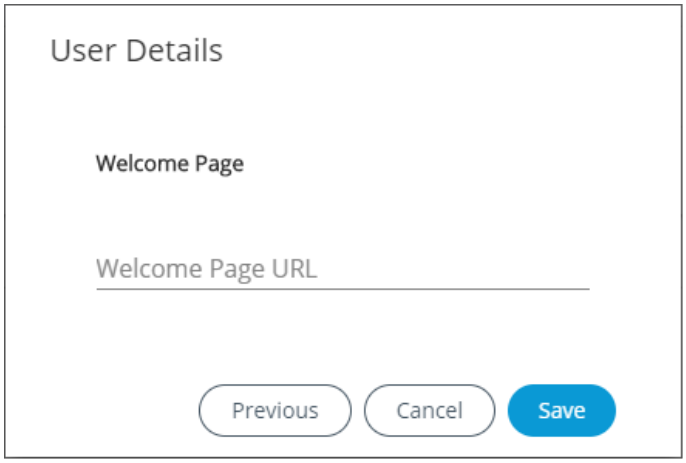


Figure 52: User Details - Welcome Page

6. Enter the URL of the web page you want to define as the landing page. The URL is the one found after the controllers' IP address or hostname. This should be copied from your Web browser's address bar when you have navigated to the target page.

   For example if the address for the user default web page is **HOSTNAME/eclypse/envysion/index.html** OR **192.168.0.10/#/bacnet.html**, remove the hostname or IP Address so that the URL becomes **/eclypse/envysion/index.html**, or **/#/bacnet**.

7. Click **OK**, and because authentication is required, enter your username and password.

The edit icon is used to edit a user's information. When editing user information, the user password is not shown therefore the field appears empty. You can leave the password as is or assign a new one.

Defining a User Welcome Page in Client Mode

In Client mode, you can only add a Welcome page to your user considering that the rest of the data is stored on the Server, essentially the credentials and roles (see *Adding a User in Server Mode*). This user's Welcome page however will have priority over the page defined in the Server mode.

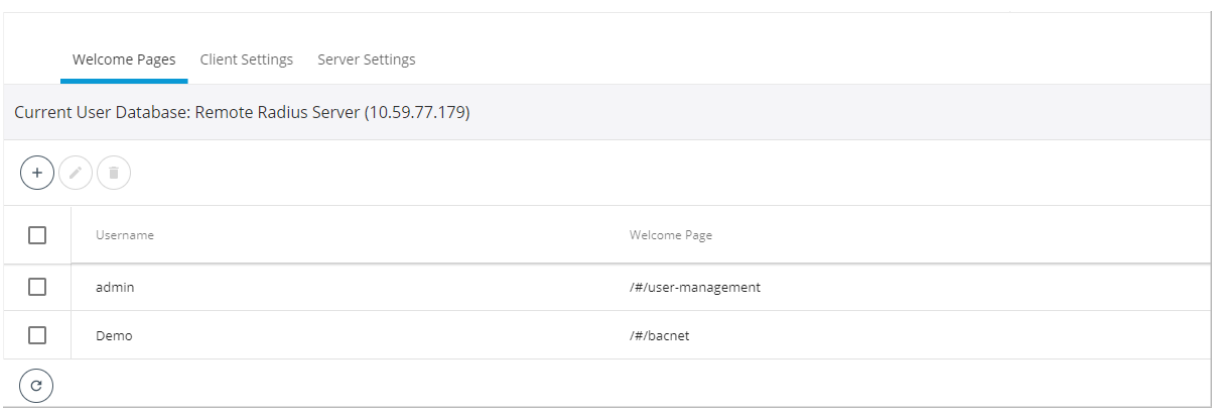


Figure 53: Adding a User in Client Mode

1. Click + to add a user and Welcome page. The **User Details** window is displayed.

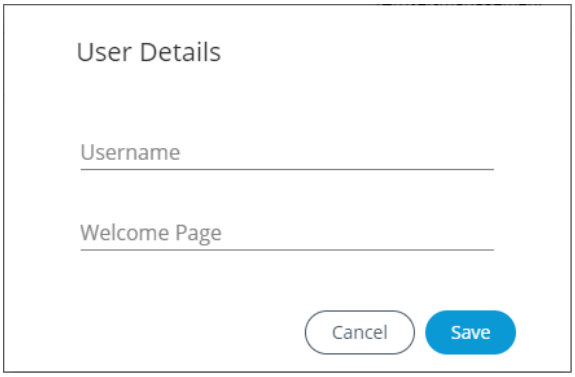


Figure 54: User Details

2. In **Username**, enter the name of the user.
3. In **Welcome Page**, enter the URL of the web page you want to define as the landing page. The URL is the one found after the controllers' IP address or hostname. This should be copied from your Web browser's address bar when you have navigated to the target page.

   For example if the address for the user default web page is **HOSTNAME/eclypse/envysion/index.html** OR **192.168.0.10/#/bacnet**, remove the hostname or IP Address so that the URL becomes **/eclypse/envysion/index.html** or **/#/bacnet**.
4. Click **Save**.

To edit an existing user, select the user from the list and click the edit icon and to remove, click the delete icon .

Password Policy

The password policy sets the minimum requirements for a valid password to help prevent common password cracking techniques. By requiring long passwords with a well-rounded composition of elements (uppercase and lowercase letters, numbers, and symbols) it makes the password harder to guess and makes a brute force attack less effective.

Click the key icon to display the **Password Policy** options:

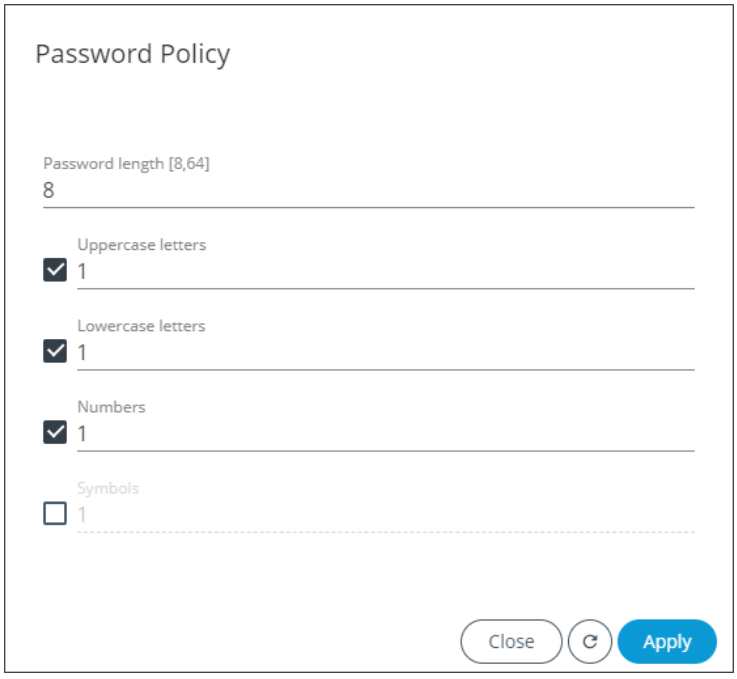


Figure 55: Password Policy Options

Item	Description
Password length (>8)	Minimum password length.
Uppercase letters	Minimum number of uppercase letters (A to Z) required to compose the password.
Lowercase letters	Minimum number of lowercase letters (a to z) required to compose the password.
Numbers	Minimum number of numbers (0 to 9) required to compose the password.
Symbols	Minimum number of symbols (for example, =, +, &, ^, $, etc.) required to compose the password.
	Click to refresh the information in the list.
Apply	Click **Apply** to apply and save the changes.

Radius Server/Client Settings

You can use the network's RADIUS Server for user authentication management.

RADIUS Server Settings

When **Radius Server** is selected in the **Server Settings** tab, this controller can be used as a RADIUS server by other controllers on the network. In this scenario, the other controllers must be configured to use the *Client* **RADIUS Server** mode with this controller's IP address. This centralizes access management on this controller thereby saving time by eliminating the need to add users to each controller individually. Set the port numbers and shared key that other controllers will use to connect to this controller. See *Supported RADIUS Server Architectures*.

The port values of 1812 for authentication and 1813 for accounting are standard RADIUS port numbers. However, other port numbers may be used. No matter which port numbers are used, make sure that the port numbers are unused by other services on this controller and that both the RADIUS server and the RADIUS clients use the same port number values. See also *IP Network Port Numbers and Protocols*.

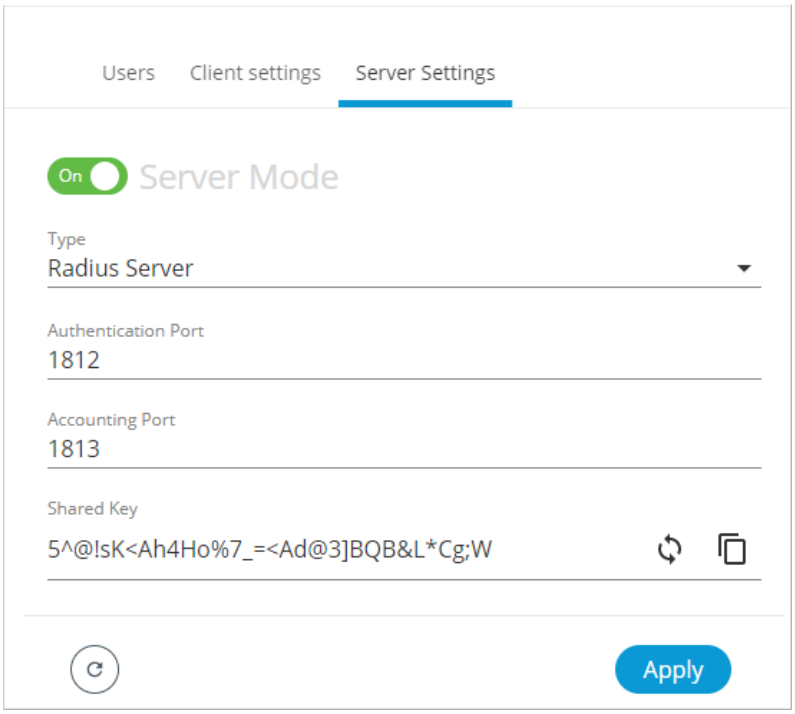


Figure 56: Radius Server Settings

To setup the RADIUS server settings, complete the parameters as described in the following table:

Item	Description
Authentication Port	RADIUS server authentication port number.
Accounting Port	RADIUS server accounting port number.
Shared Key	Encryption key that devices use to encrypt and decrypt user authentication credentials that are sent between devices. The shared key should be a long string made up of 16 to 132 random alphanumeric characters and symbols that would be difficult to guess. This same key must be copied to any RADIUS client.
	Click to copy the shared key to the clipboard.
	Click to refresh the information in the list.
Apply	Click **Apply** to apply and save the changes

RADIUS Client Settings

When **Radius Server** is selected in the **Client Settings** tab the following configuration parameters shown in the table below are available. This centralizes access management on the RADIUS server thereby saving time by eliminating the need to add users to each controller individually. The client RADIUS server can be another ECLYPSE controller, Microsoft Windows Domain Active Directory Server, or a suitably-configured EC-Net/EC-BOS station. See *Supported RADIUS Server Architectures*.

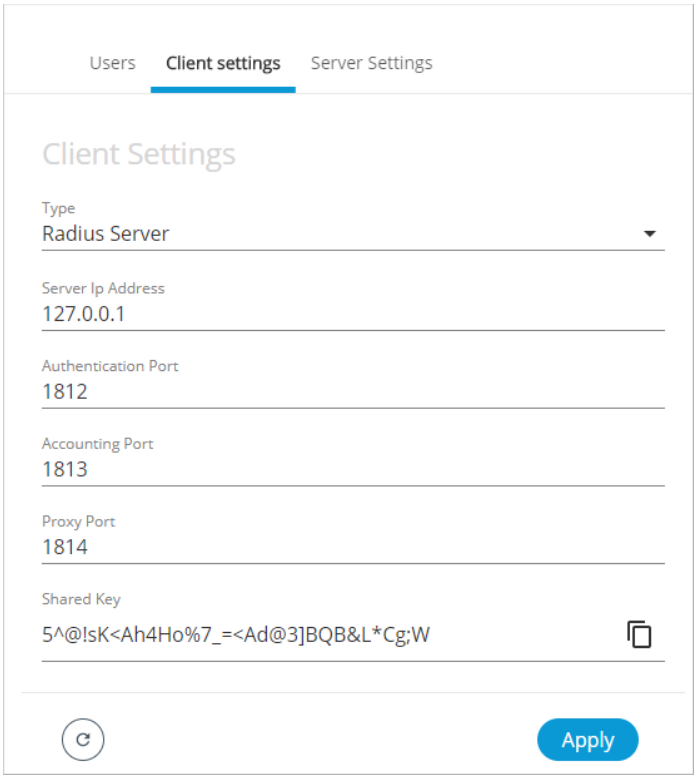


Figure 57: Radius Client Settings

To setup the RADIUS client settings, complete the parameters as described in the following table:

Item	Description
Server IP Address	IP address of the RADIUS server. This can be the IP address of an ECY series controller that is set as the Server Radius or a suitably-configured RADIUS server on an EC-Net / EC-BOS station.
Authentication Port	Port on which authentication requests are made.
Accounting Port	Port on which accounting request are made. This is only used to receive accounting requests from other RADIUS servers.
Proxy Port	Internal port used to proxy requests between a server mode and client mode.
Shared Key	Encryption key that devices use to encrypt and decrypt user authentication credentials that are sent between devices. The shared key should be a long string made up of 16 to 132 random alphanumeric characters and symbols that would be difficult to guess. If EC-Net is the RADIUS server, the same value must be copied to the **Shared Key** parameter in the **Radius Service**.
	Click to copy the shared key to the clipboard.
	Click to refresh the information in the list.
Apply	Click **Apply** to apply and save the changes

Should the connection to the RADIUS server be temporarily lost, ECLYPSE controllers have a fall back authentication mode: Users that have already authenticated themselves with the RADIUS server and then the connection to the RADIUS server is lost, these users will still be able to login to the controller as their successfully authenticated credentials are locally cached.

The user profile cache is updated when the user authenticates themselves while there is a working RADIUS server connection. For this reason, at a minimum, admin users should log in to each ECLYPSE controller at least once, so their login can be cached on that controller. Otherwise, if there is a RADIUS server connectivity issue, and a user who has never connected to the ECLYPSE controller before will be locked out from the controller. It is particularly important for admin user credentials to be cached on each controller as an admin user can change the controller's network connection parameters that may be at cause for the loss of connectivity to the RADIUS server.

The port values of 1812 for authentication and 1813 for accounting are RADIUS standard port numbers. However, other port numbers may be used. No matter which port numbers are used, make sure that the port numbers are unused by other services on this controller and that both the RADIUS server and the RADIUS clients use the same port number values. See also *IP Network Port Numbers and Protocols*.

Single Sign On (SSO) Settings

The **Single Sign On (SSO)** service allows a user to use one set of login credentials (e.g.username and password) to access multiple ECLYPSE controllers that are on the same network. This provides a secure centralized login method to authenticate users.

The basic functionality behind an SSO service with ECLYPSE controllers is the Client-Server architecture where one controller is defined as the Server dedicated to authentication/authorization purposes to access the Client controllers.

The SSO authenticates the user for all the controllers the user has been given rights to and eliminates further login prompts when the user accesses other controllers within the same session.

The session ends if you close the web browser or you log out. It is recommended that you close your web browser after logging out.

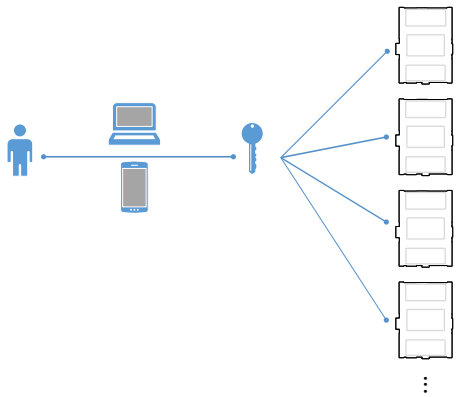


Figure 58: SSO Architecture

With the SSO service, you will be automatically redirected to the SSO server login page when you navigate to a SSO client web page. Once you are authenticated by the server, you will be redirected to the web page you requested on the client. If you requested the default page, you will be redirected to your Welcome page instead.

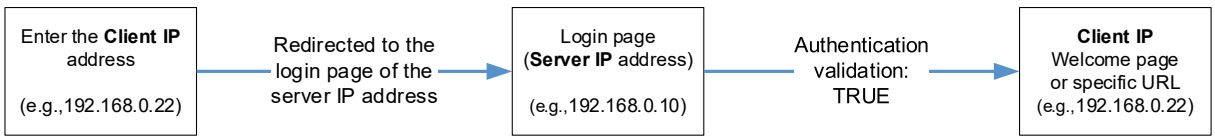


Figure 59: SSO Authentication Sequence

The Xpress*Network* Utility allows you to perform a range of operations on many controllers at once, so we highly recommend that you use xpress*Network* Utility when configuring the SSO parameters for your controllers.

The SSO requires HTTPS to function properly. HTTP cannot be enabled and will automatically be disabled when SSO is activated.

See also *Setting Up the SSO Functionality*.

SSO Server Settings

The **Server Settings** tab allows you to select the type of server mode for the Server controller. The available modes are **Single Sign On** or **Radius Server**.

When **Type** is set to **Single Sign On (SSO)**, the controller will be defined as the SSO Server dedicated to authentication purposes. Therefore, a single login to the server will authenticate user access to multiple ECLYPSE controllers that are on the same network.

An SSO server must be configured with a static IP address. If the SSO server IP address changes, you will have to reconfigure all SSO clients with the new IP address. See *Ethernet*.

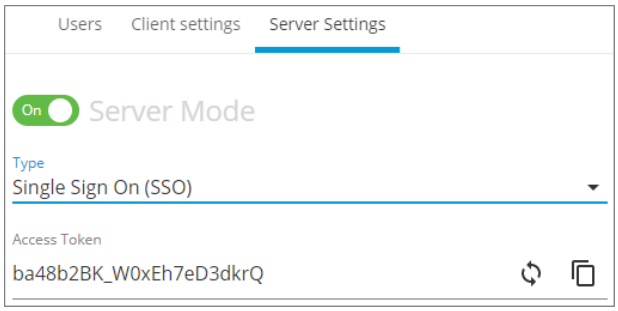


Figure 60: SSO Server Settings

Item	Description
Server Mode (On/Off) On Off	Enable or disable the functionality of the server. When set to OFF, the controller is no longer in server mode.
Type	Server type.
Access Token	Identifier used by the server that is handling the protected resource to lookup the associated authorization information. The access token is usually a long string made up of 16 to 132 random alphanumeric characters and symbols that would be difficult to guess. When the SSO service is selected, the access token ID is displayed by default. If required, you can generate a new code using the generate icon or manually enter an access token.
	Click to copy the access token to the clipboard.
	Click to refresh the information in the list.
Apply	Click **Apply** to apply and save the changes

See also *Setting Up the SSO Functionality*.

SSO Client Settings

whaThe **Client Settings** tab allows you to select the type of client mode for the Client controller(s). When **Type** is set to **Single Sign On (SSO)**, the controller will use the SSO server for authentication.

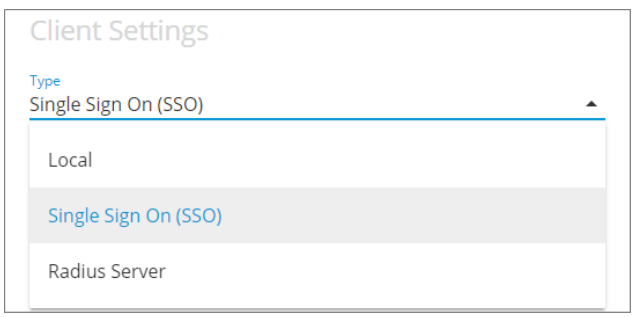


Figure 61: Client Settings - Type

When **Type** is set to **Local**, credentials are added to and managed by this controller.

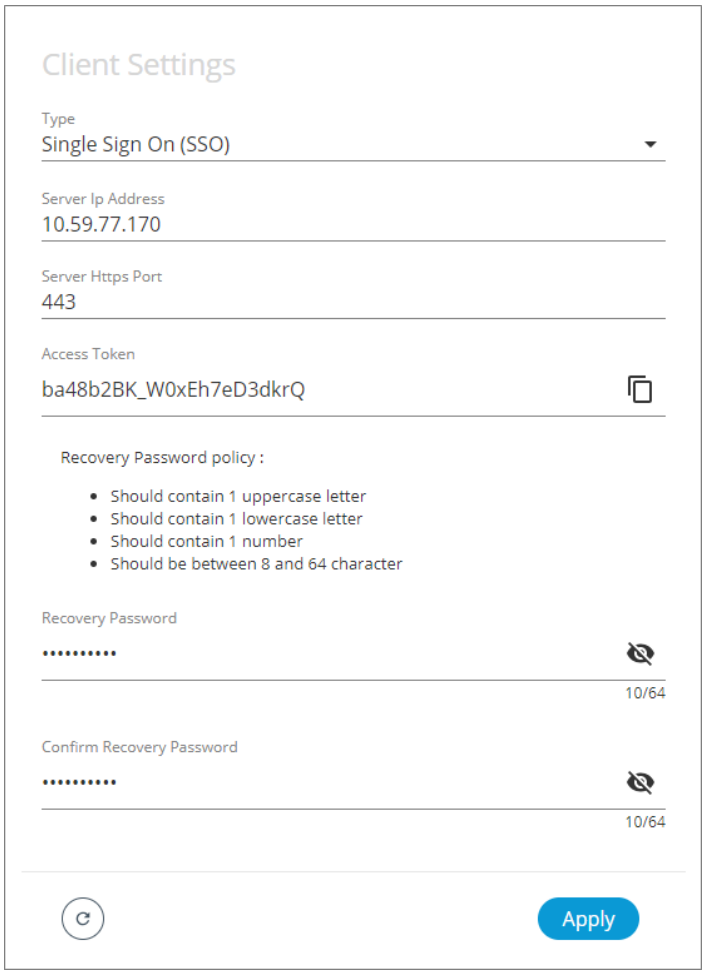


Figure 62: Client Settings - SSO

Item	Description
Type	Server type.
Server IP Address	Server IP address of the SSO server. This is the IP address of the ECLYPSE controller that was configured as the server. **Note:** An SSO server must be configured with a static IP address. If the SSO server IP address changes, you will have to reconfigure all SSO clients with the new IP address. See *Ethernet*.
Server Https Port	Server HTTPS port of the SSO server. By default, this port is set to 443.
Access Token	Server access token of the SSO server. If the server access token changes, this parameter should be updated by the user accordingly. In the **Access Token** field, enter the access token belonging to the Server. To do so, go to **Server Settings**, copy the access token using the copy icon and paste (CTRL+V) into the **Access Token** field in **Client Settings**.
Recovery Password / Confirm Recovery Password	Define a recovery password to access the controller in recovery mode if ever the server is unavailable. See *Single Sign On (SSO) Troubleshooting*. Click the show password icon to see the password you are entering. In order for the recovery to work, we highly recommend you do not forget your recovery password. If so, a factory reset will be required.

Item	Description
	Click to copy the access token to the clipboard.
	Click to refresh the information in the list.
Apply	Click **Apply** to apply and save the changes

Setting Up the SSO Functionality

This section explains how to setup the SSO functionality by setting up the SSO Server first, followed by the SSO Client. For more information, see *Single Sign On (SSO) Settings*.

An SSO server must be configured with a static IP address. If the SSO server IP address changes, you will have to reconfigure all SSO clients with the new IP address. See *Ethernet*.

SSO functionality is only available in HTTPS mode. See *Web Server Access* for more information on enabling HTTPS.

Setting up the SSO Server

1. Open a web browser.
2. Enter the IP address of the controller that will become the Server (e.g., 192.168.0.10). The ECLYPSE Login page is displayed.
3. Enter your credentials to log in. The ECLYPSE home page is displayed.
4. In the **Users** menu, select the **Server Settings** tab and make sure the **Server Mode** is set to **On**.

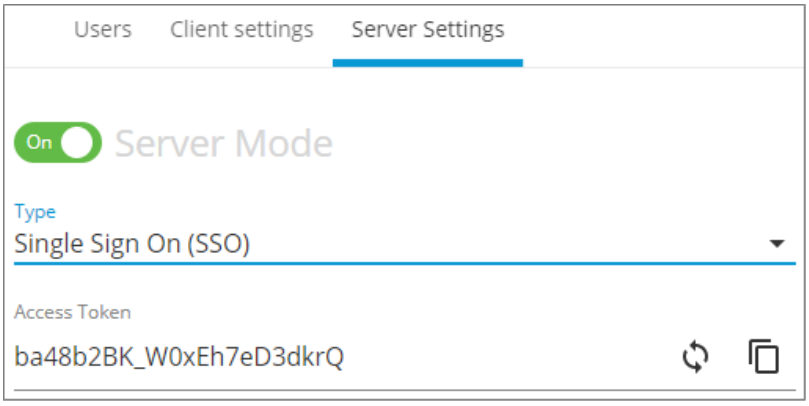


Figure 63: SSO Server Settings

5. In **Type**, select **Single Sign On (SSO)**.
6. In **Access Token**, an access token is displayed by default. If required, you can generate a new access token or manually enter a custom access token. This exact access token will be needed to setup the Client server (see next procedure *Setting Up the SSO Client*).
7. Click Apply.

Setting Up the SSO Client

1. Open a web browser or a new tab in the current Web browser.
2. Enter the IP address of the controller that will become the Client (e.g., 192.168.0.22). The ECLYPSE Login page is displayed.
3. Enter your credentials to log in. The ECLYPSE home page is displayed.

4. In the **Users** menu, select the **Server Settings** tab and make sure the **Server Mode** is set to **Off**. If not, set the **Server Mode** to **Off** and click **Apply** before proceeding.

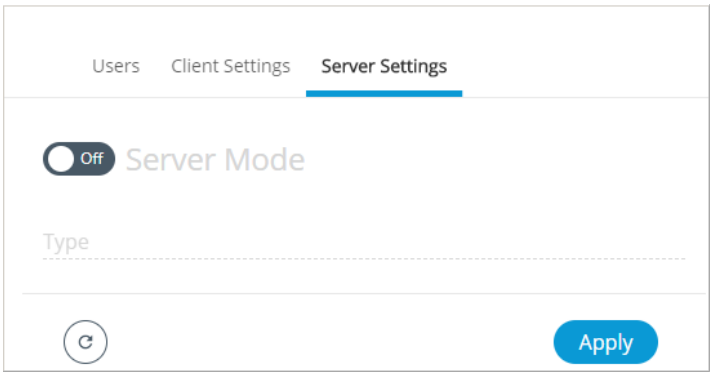


Figure 64: SSO Server Settings - Server Mode Off

5. Select the **Client Settings** tab to setup the SSO client.
6. In **Type**, select **Single Sign On**. Additional fields are displayed.

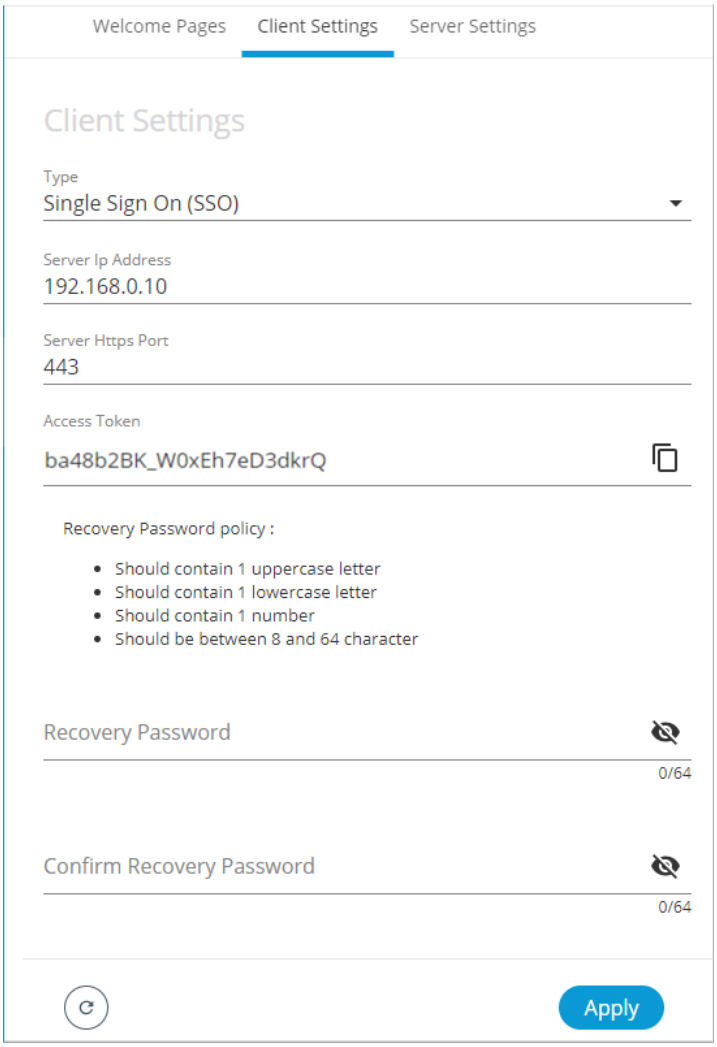


Figure 65: SSO Client Settings

7. In **Server IP Address**, enter the server IP address of the controller that is configured as the Server (e.g., 192.168.0.10).

8. In **Server Https Port**, verify that the port number matches the HTTPS port number of the SSO server in **System > Web Server** (e.g., 443).

9. In **Access Token**, you must enter the access token from the SSO Server. Copy the access token from the **Server Settings** (see above procedure *Setting up the SSO Server*) and paste in this field.

10. In **Recovery Password**, enter a recovery password that you will use in a case where the server is no longer available.

11. In **Confirm Recovery Password**, enter the password again.

12. Click **Apply** to apply and save the configuration.

13. When setting up a new SSO connection, a message is displayed to notify you that a new certificate has been detected. To validate the authenticity of the server, click **Continue**.

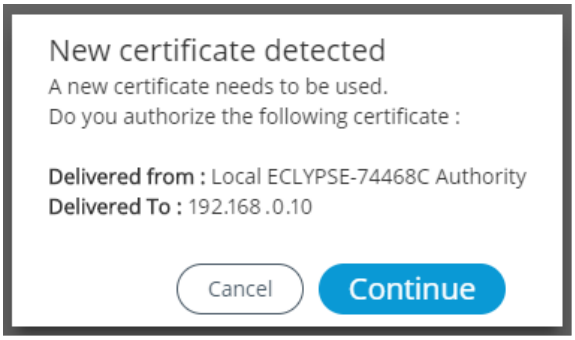
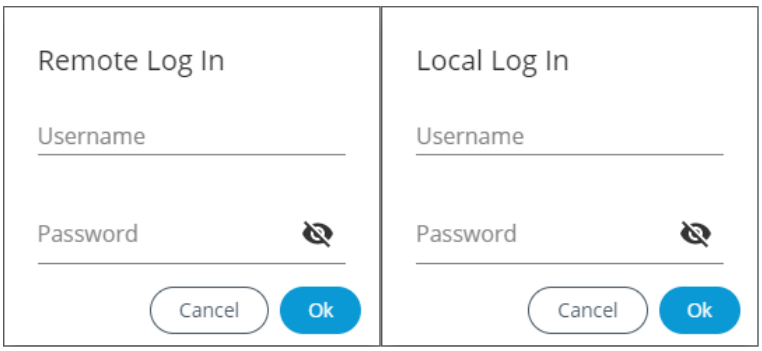


Figure 66: SSO New Certificate Detected

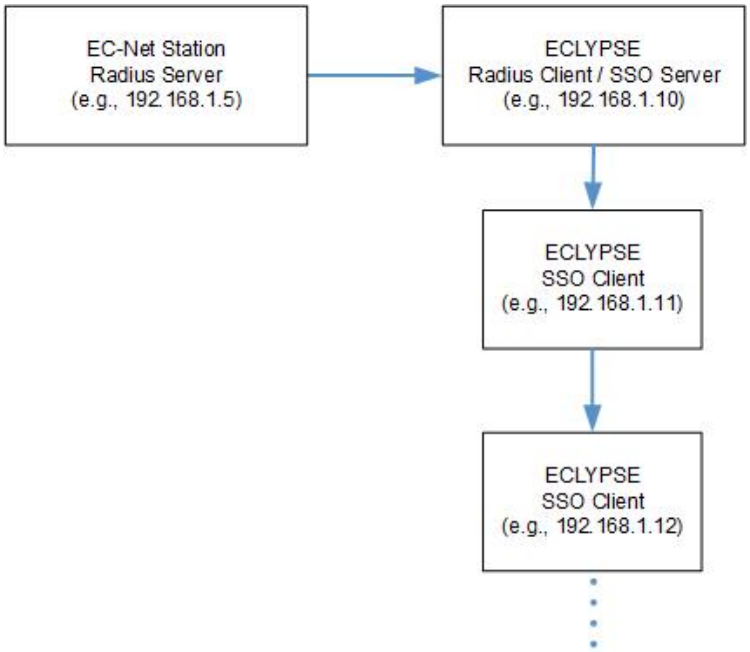
14. A new page is displayed confirming that the server settings are being applied. After approximately 1 minute, you can refresh your browser manually using the F5 key or close and reopen your browser.

To switch from the SSO Mode to Radius or Local Mode, you will be asked to log in to the remote or local server. These credentials are the ones associated to the server you wish to switch to.



Setting Up the SSO Functionality through a Radius Server

The following procedure will explain how to setup an EC-Net station as the Radius server. In turn, this will allow users residing in EC-Net to access the ECY Series controllers and the associated ENVYSION graphics on an SSO Client, through a web browser. The SSO client eliminates the need to login every time you are accessing an ENVYSION graphic in an ECLYPSE controller.



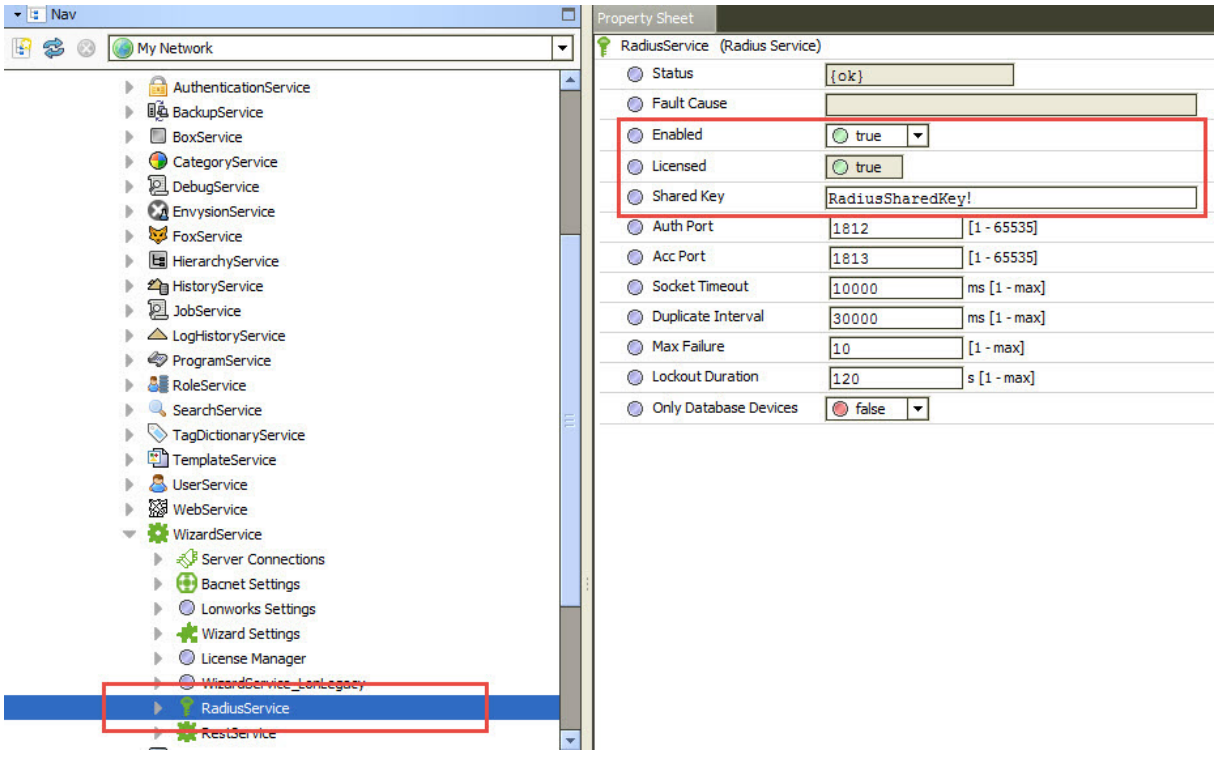
This procedure is explained in three parts, in the following order:

- Setting up the RADIUS server in EC-Net
- Setting up the Radius client/SSO server in the ECLYPSE Web configuration interface
- Setting up the SSO client

See also *Configuring the EC-Net Station's RadiusService*

Setting Up the RADIUS Server in EC-Net

1. In EC-Net, configure the RadiusService settings under **Station > Config> Services > WizardService**.

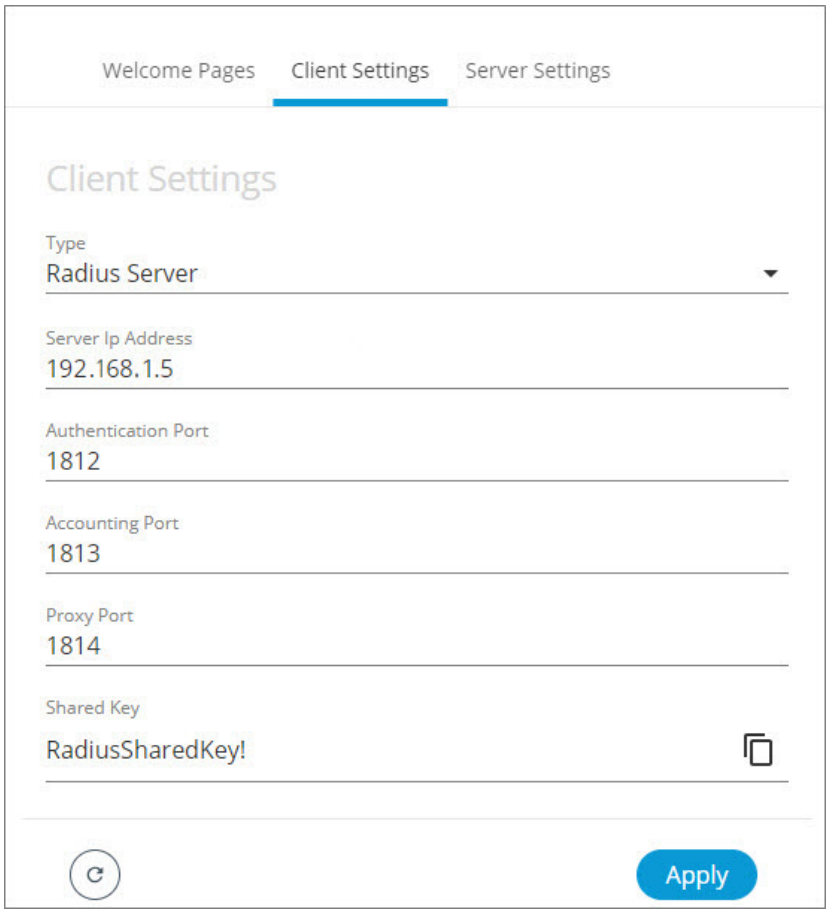


2. In **Shared Key**, enter a key that must contain between 16 and 132 random alphanumeric characters and symbols that would be difficult to guess. This exact key must be copied to the Shared Key parameter in the User Management screen of the ECLYPSE Web interface.
3. Make sure **Enabled** is set to **true** to enable the RadiusService.
4. Make sure that **Licensed** is set to **true**. This is true when the RadiusService is licenced on this station and is available. For more information about support pack licensing, see Licensing the EC-Net Support Package for a Non-Distech Controls Brand Station in the EC-*gfx*Program Getting Started Guide.
5. Click **Save**.

Setting Up the Radius Client/SSO Server in the ECLYPSE Web Configuration Interface

1. Open a Web browser.
2. Enter the IP address of the controller that will become the RADIUS client/SSO server (e.g., 192.168.1.10). The ECLYPSE Login page is displayed.
3. Enter your credentials to log in. The ECLYPSE home page is displayed.

4. In the **Users** menu, select the **Client Settings** tab.



5. In **Type**, select **Radius Server**.
6. In **Server IP Address**, enter the IP address of the EC-Net Radius Server.
7. Set the port numbers as needed. Port values 1812 and 1813 are standard RADIUS port numbers but other port number can be used. See RADIUS Server Settings.
8. In **Shared Key**, you must enter the same shared key as the one entered in EC-Net. See previous procedure: *Setting Up the RADIUS Server in EC-Net*.
9. Click **Apply**. You will be prompted to enter the Radius Server credentials. Once the credentials are granted the Radius client is setup.
10. Now to setup the SSO Server, select the **Server Settings** tab and make sure the **Server Mode** is set to **On**.
11. In **Type**, select **Single Sign On (SSO)**.
12. In **Access Token**, an access token is displayed by default. If required, you can generate a new one or manually enter a custom access token. This exact access token will be needed to setup the SSO clients (see *Setting Up the SSO Client*).
13. Click **Apply**.

Setting Up the SSO Client

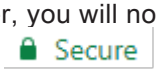
See *Setting Up the SSO Client*.

Certificate Authentication with SSO

To avoid getting certificate authentication messages:

Also see *Saving a Certificate*.

1. Go to the System menu and select the Web Server tab.
2. Click **Export Authority Public Key**. A certificate is downloaded (.crt file) and can be found in the **Downloads** folder.
3. Go to your browser settings. For the purpose of this procedure, Google Chrome web browser is used.
4. Scroll down to the bottom of the Chrome **Settings** page and select **Advanced**.
5. Select **Manage certificates**. The **Certificates** window is displayed.
6. Select the **Trusted Root Certification Authorities** tab.
7. Click **Import**.
8. Click **Next**.
9. Browse to the **Downloads** folder and select the certificate file (.crt) that was previously downloaded.
10. Click **Next** throughout the next windows and then click **Finish**.
11. A warning message is displayed. Click **Yes** to continue and apply the certificate.
12. Close all Google Chrome windows for the changes to be applied.

When restarting the Web browser, you will no longer get a message stating that your connection is NOT secure, but rather a Secure 

green padlock icon will appear in the URL bar to indicate a secure connection.

System Settings

This is where you configure the controller's date and time, Web interface, port numbers, secure web interface, and the license. A secure web interface requires a SSL certificate.

Device Information

This shows detailed information about the controller such as the firmware version, MAC address for each network interface, extension modules versions, and Wi-Fi information.

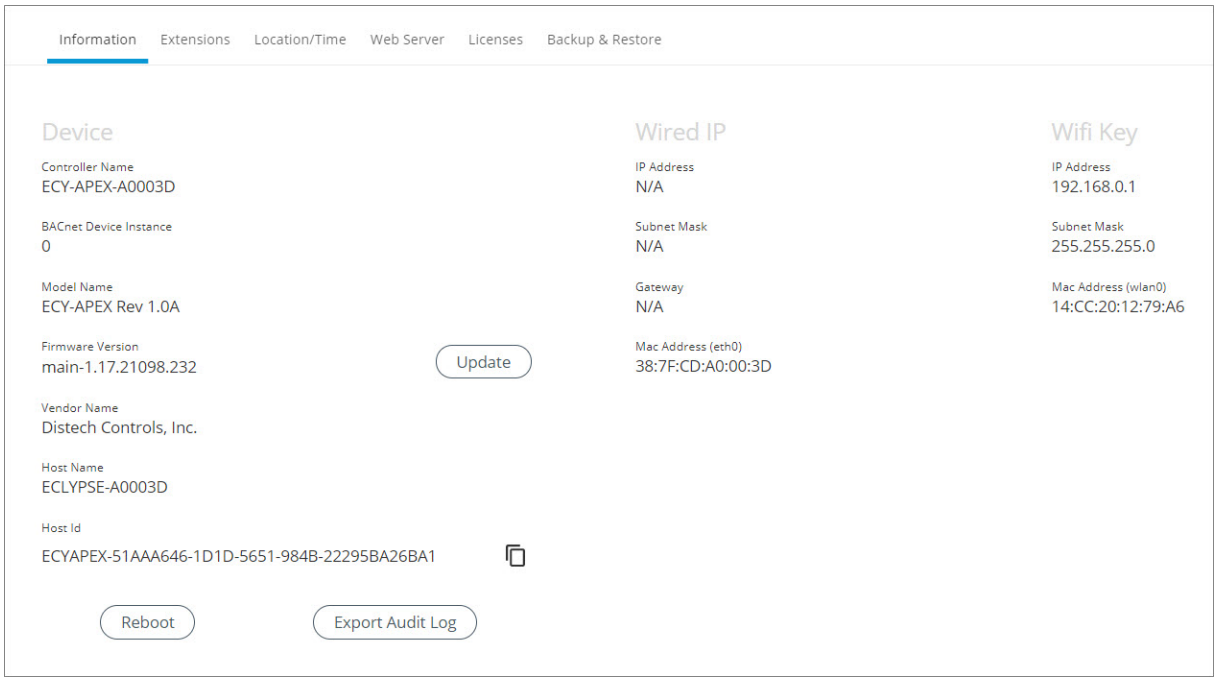


Figure 67: General Device Information

Item	Description
Update	The controller's firmware can be updated through the Firmware Update file upload interface. See *Updating the Firmware*. Also see *Extensions*.
Reboot	Click to reboot the controller. **Note:** Rebooting the controller will interrupt the operation of any connected equipment and the controller will be offline from the network for the duration of the reboot.
Export Audit Log	Export an audit log in .csv format showing auditable events such as account logins, event ID and description, event type, etc. See *Export Audit Log* for more information.

The **Wired IP** (wired Ethernet connection) and **Wifi Key** (wireless connection) sections provide information such as the IP address, subnet mask, gateway and Mac address

The Mac Address is the same for both Primary (PRI) Wired Ethernet connection (ETH0) and the Secondary (SEC) Wired Ethernet connection.

Updating the Firmware

The controller's firmware can be updated through the Firmware Update file upload interface for an ECLYPSE series controller.

1. In System settings under the **Information** tab, click **Update** located next to the firmware version. The Firmware Update window is displayed:

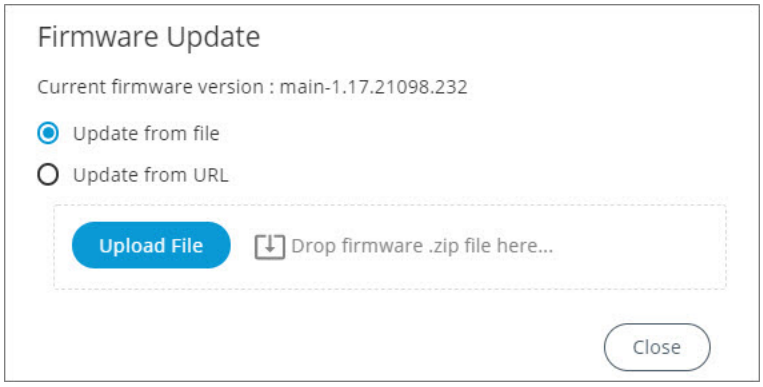


Figure 68: The Firmware Update File Upload Interface

2. Upload the firmware file using one of the following firmware upload methods:
   - Update from a file on your PC.
   - Update from a URL
   - In Windows Explorer, find the firmware file on your PC and drag and drop it in the dotted area.

The file upload starts followed by the firmware upgrade. Once the upgrade is complete, the controller will reboot. If you click Cancel, not only will the upload processed be canceled, but also the upgrade.

Do not remove power from the controller or interrupt the network connection to the controller during the firmware upgrade process. Failing to do so may render the controller unusable.

See also *Extensions* to update the ECLYPSE Controller's I/O extension modules.

Export Audit Log

Auditable events are authentication and authorization failures and all operations done in the users' configuration. The **Export Audit Log** is used to export a .csv file that details the auditable events that are audited by the device, and/or web application (account logins, event ID and description, event type, etc).

The following device auditable events are logged:

Event Types	Description
Authentication In	When a user logs in. Only unauthorized logins will be logged.
For the following event types, logging is done only on operations done in the users' configuration:	
Rest_Post	When a user sends a write/update action on the Rest API.
Rest_Put	When a user sends an update action on the Rest API.
Rest_Delete	When a user sends a delete action on the Rest API.
Rest_Get	When a user sends a read action on the Rest API.
Web_Interface	When a user performs an action on the Web interface.

The .csv file displays the event details in the following information columns:

Column Heading	Description
eventID	Sequential event number.
timestamp	Time of occurrence of a particular event (date and time of day) in GMT.
user	User ID or username.
ipAddress	IP address of the client making the request.
type	Event type as described in the previous table.
description	Event type description.
result	Result status for any of the event types: success, error, or unauthorized.
event	Action performed by the user. For an authentication event, the event column will indicate a Web or Rest API authentication. Other events shown in this column relate to User Management events such as editing, adding, or updating data such as passwords and users, and also unauthorized access attempts.

	A	B	C	D	E	F	G	H	I
1	eventID	timestamp	user	ipAddress	type	description	result	event	
2	1	5/16/2017 17:45	admin	10.59.76.27	REST_POST	User send a write/update action on the Rest API	SUCCESS	User management - User radius global configuration	
3	2	5/23/2017 13:42	admin	10.59.76.27	AUTHENTICATION_IN	User logged in	UNAUTHORIZED	Authentication - Web	
4									
5									
6									
7									
8									
9									
10									

auditLogs (2)

Figure 69: Example of an exported .csv file of auditable events

Extensions

The **Extensions** tab is used to update the ECY Series Controller's I/O extension modules. It also displays the extension module version and hardware ID.

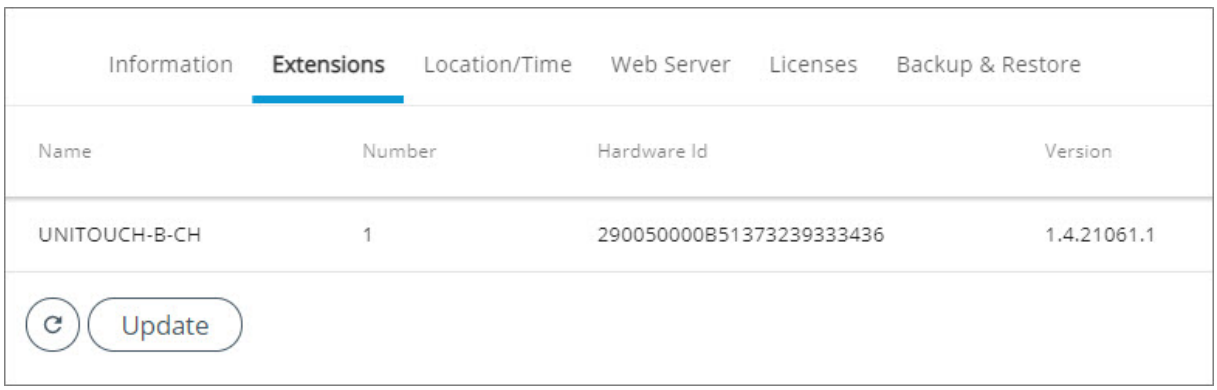


Figure 70: Extensions tab

1. In the **Extensions** tab, click **Update**. The **Extension Firmware Update** window is displayed.

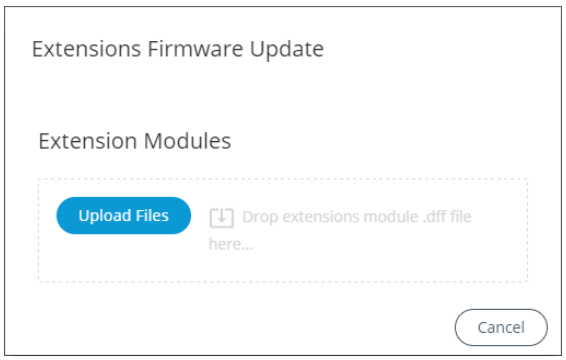


Figure 71: Extensions Firmware Update Window

2. Upload the firmware file using one of the following firmware upload methods:
   - Click Upload Files to find the firmware file on your PC.
   - In Windows Explorer, find the firmware file on your PC and drag and drop it in the dotted area.

The file upload starts followed by the firmware upgrade. If you click Cancel, not only will the upload processed be canceled, but also the upgrade.

Do not remove power from the controller or interrupt the network connection to the controller during the firmware upgrade process. Failing to do so may render the controller unusable.

3. Click refresh to refresh the information in the list.

Location and Time

The Location/Time tab is used to configure the system date and time as well as the weather and current location.

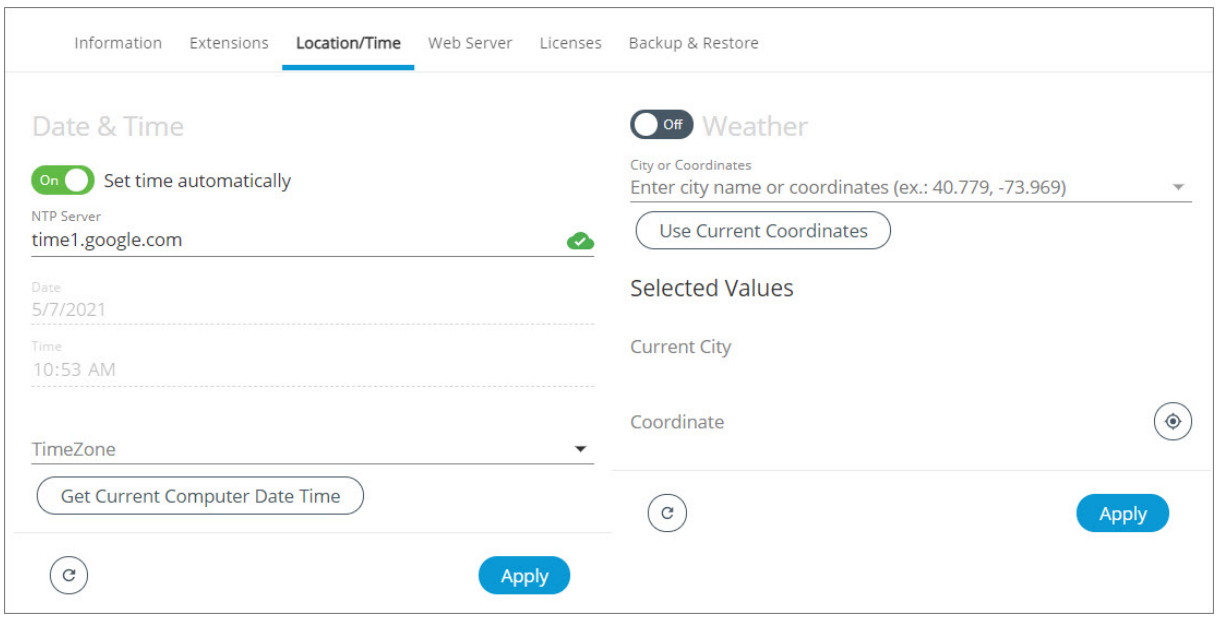


Figure 72: System Settings – Location, Date, and Time

Item	Description
Set Time Automatically On Off	Toggle On or Off to automatically set the time based on the NTP Server.
NTP Server	Input the desired Network Time Protocol (NTP) Server that will be used to automatically fetch time and date information. A successful connection will display the icon and an unsuccessful connection will display the icon. Internet connectivity is required for this feature to work.
Date	Set the controller's date.
Time and Time Zone	Set the controller clock's time and the time zone the controller is located in.
Get Current Computer Date Time	Click to get the current time and date from the computer being used to access the controller's web interface.
Weather On/Off On Off	Enable or disable the weather data fetching service for a specific location. If connected to an EC-BOS and weather is enabled, the ECLYPSE controller will override all weather information from the EC-BOS. The default weather service is Accuweather and is updated every hour. If weather is enabled, weather information is pushed to the weather block within EC-*gfx*Program, where it can be used in the control logic. It will also be pushed to the ECx-Display, if connected to the ECLYPSE controller.

Item	Description
	NOTE: Internet connectivity through port 443 is required for Weather Service functionality.
City	Set the city location from which the system will use weather data.
Current City	Displays the currently selected city,
Coordinate	Displays the latitude and longitude coordinates of the currently selected city. Click the coordinate icon to display to open the location in Google maps.
	Click to refresh the information in the list.
Apply	Click **Apply** to apply and save the changes

Web Server Access

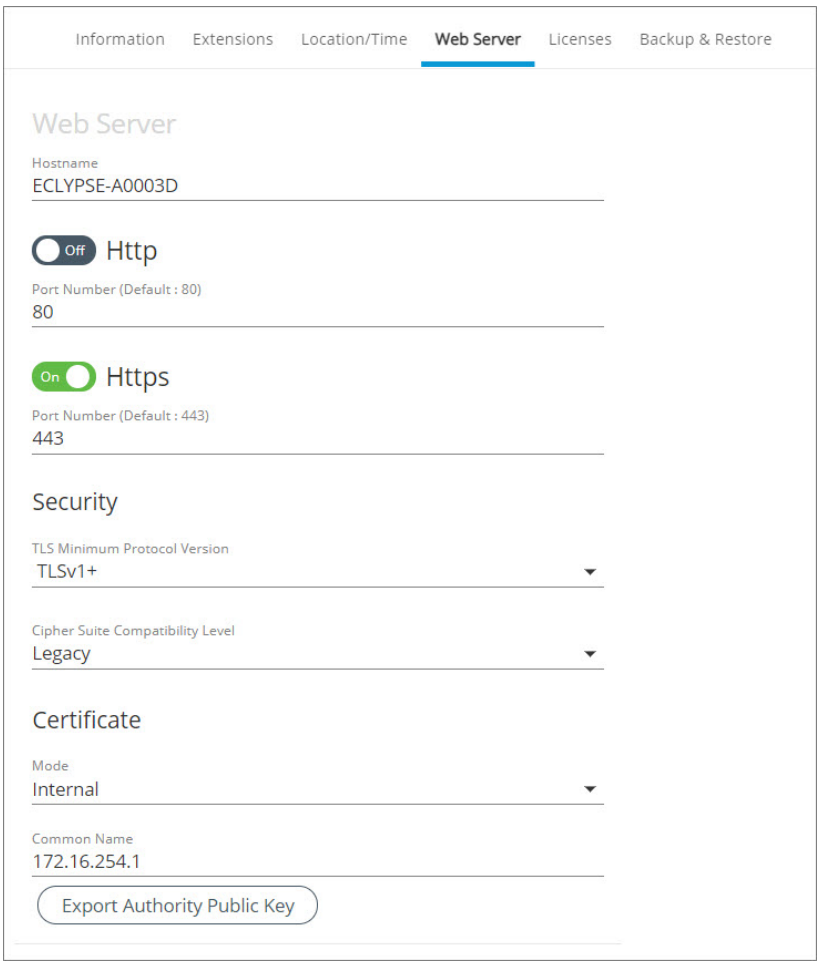


Figure 73: System Settings – Web Server Access

Item	Description
Hostname	Give this controller a label or nickname to identify it on the network. The hostname can be used in place of an IP address to identify this controller on the network. This hostname can be used in a Web browser's address bar or in the EC-*gfx*Program's **Connect to** screen for example. A hostname may contain only the ASCII letters 'a' through 'z' (case-insensitive), the digits '0' through '9', and the hyphen ('-'). A hostname cannot start with a hyphen and must not end with a hyphen. No other symbols, punctuation characters, or white space are permitted.
HTTP	Set this to enable the standard Webserver on this controller. When Single Sign On (SSO) is enabled, HTTP is not available.
HTTPS	Set this to enable the secure Webserver on this controller. Connections to this sever are encrypted which helps to prevent eavesdropping thereby keeping passwords secure.

Item		Description
Security		**TLS minimum Protocol Version:** ☐ Select the appropriate Transport Layer Protocol (TLSv1+, TLSv1.1+, TLSv1.2, or TLSv1.3) minimum version to be used for server authentication and secure encryption and decryption of data over the Internet. **Cipher Suite Compatibility Level:** ☐ Legacy: This is the default value and is used only if you need to support outdated client and browser versions (e.g., Internet Explorer 6, Client in Java 6). ☐ Recommended: This level provides a higher level of security but is only compatible with latest client and browser versions (e.g., Firefox 27+, Chrome 30+, Client in Java 8).
Certificate Mode		Select the type of certificate (Internal or Custom) to be used by the ECLYPSE controller. ☐ **Internal**: Use a self-signed certificate that has been created automatically by the ECLYPSE controller. ☐ **Custom**: Use a custom certificate. In this case, the user must import the custom certificate into the ECLYPSE controller.
Internal Certificate	Common Name	For HTTPS connections, a certificate must have the controller's current URL or IP address encoded into it to show to the connecting device that the connection corresponds to the certificate. Set the controller's current IP address, hostname, or DNS name.
	Export Authority Public Key	For HTTPS connections, click to export the public key from the local authority that generates the internal certificate to a file on your PC. You must import this certificate into all PCs that are going to connect to this controller as a trusted certificate. See *Saving a Certificate*.
Custom Certificate	Status	Displays the certificate status: ☐ **File not found**: No certificate has been imported. ☐ **Present**: A certificate has been imported.
	Import Custom Certificate	Upload a custom certificate. You can also drag and drop a certificate file in the dotted area.
	Password	The password for the imported certificate.
		Click to refresh the information in the list.
Apply		Click **Apply** to apply and save the changes

Saving a Certificate

When the HTTPS Certification has been configured, you can save the certificate on your PC. This certificate must be distributed to all PCs that will connect to this controller. It is this certificate that allows a trusted connection to be made between the two devices.

1. Enable Certificate Mode to **Internal**, and set this controller's IP address or DNS name in the **Common Name parameter**.
2. Click **Export Authority Public Key** to save the certificate on your PC.
3. Save the file on your PC.
4. Distribute this file to all PCs that will connect to this controller.
5. Install the certificate on the PC by double-clicking it in Microsoft Windows Explorer.
6. Click **Open**.

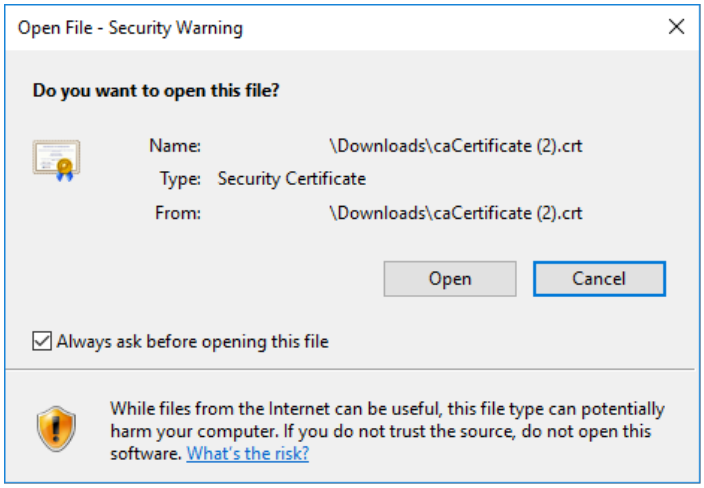


Figure 74: Certificate Security Warning

7. Install the certificate in the Trusted Root Certification Authorities store. Click **Install Certificate**.

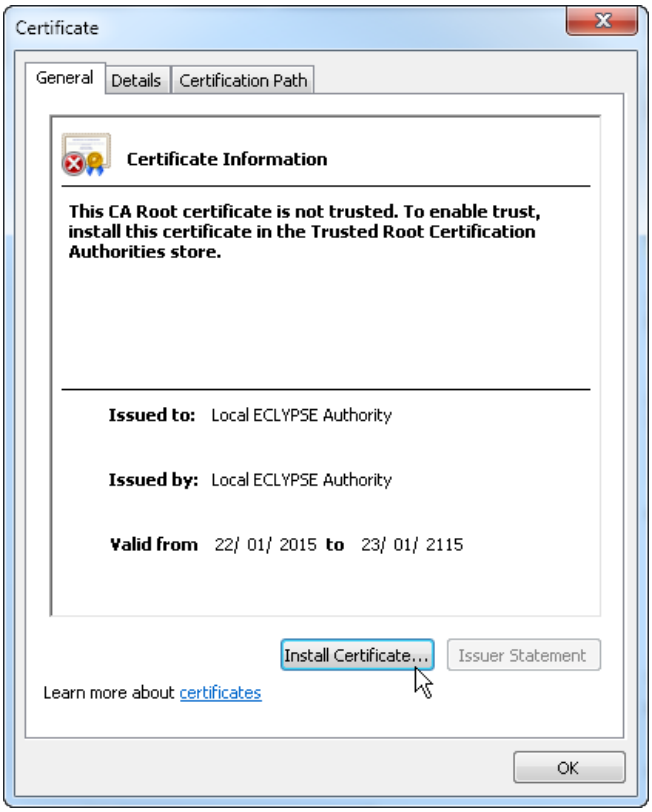


Figure 75: Installing the Certificate on the PC

8. Select **Place all certificates in the following store**. Click **Browse**.

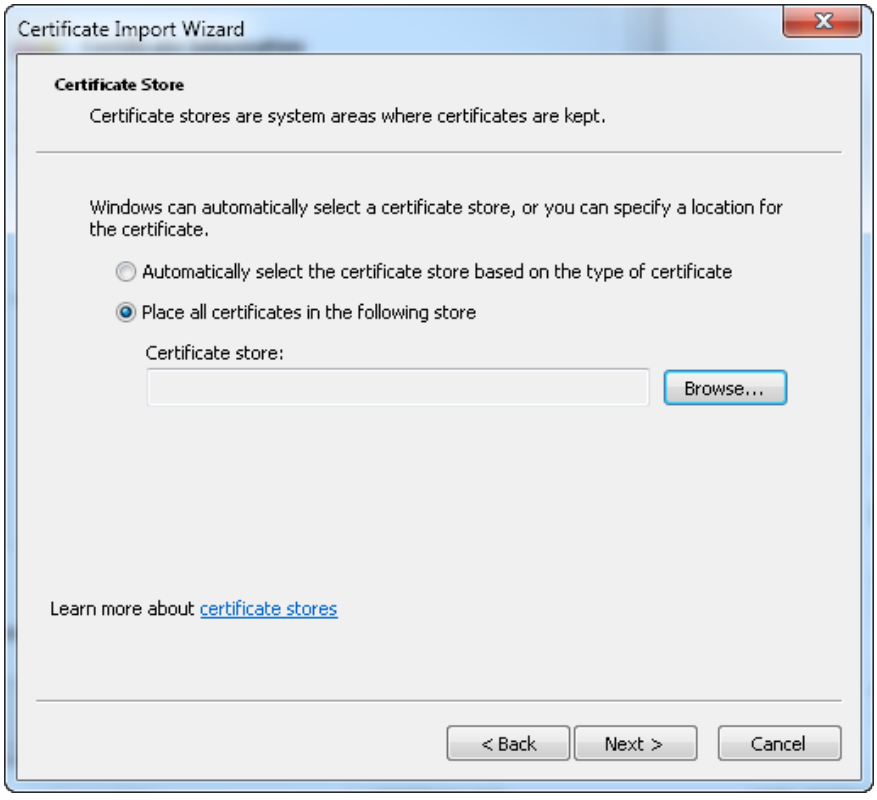


Figure 76: Selecting the Store

9. Select **Trusted Root Certificate Authorities** and click **OK**.

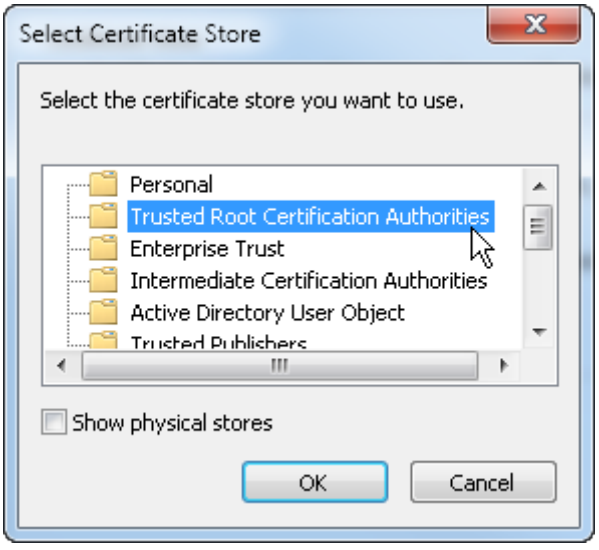


Figure 77: Selecting the Trusted Root Certification Authorities Store

10. Click **Next**. Click **Finish**.
11. Accept the warning. Click **Yes**.

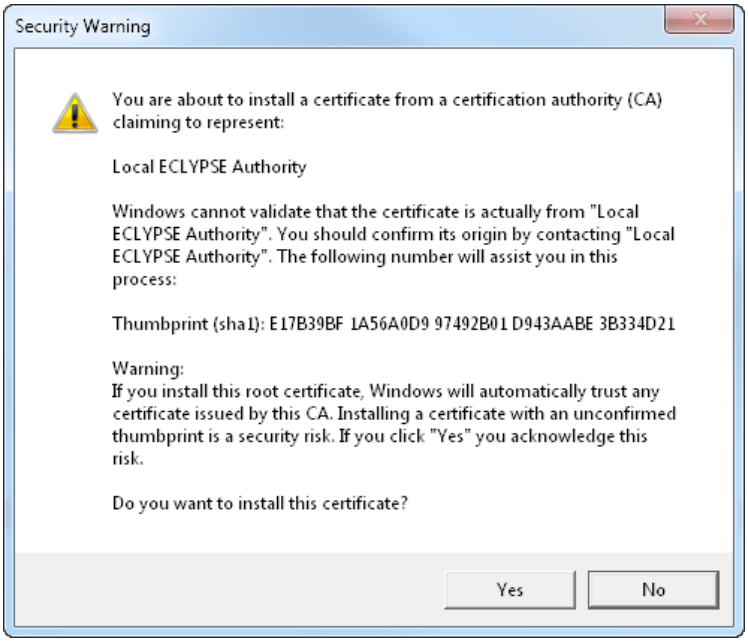


Figure 78: Accept the Warning

Removing a Certificate

After you hold the controller's reset button for 20 seconds, the controller's HTTPS security certificates will be regenerated. If you use HTTPS to connect to the controller, you will no longer be able to connect to the controller from any PC that was used in the past to connect to the controller unless you delete the old HTTPS security certificate from these PCs.

Security certificates are managed on a PC through the Certificate Manager. To delete an ECLYPSE controller's HTTPS security certificate from a PC, proceed as follows.

1. On the PC, open the Certificate Manager: click **Start** and type **certmgr.msc** into the search box and press **Enter**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
2. In the Certificate Manager, navigate to **Certificates - Current User\Trusted Root Certification Authorities\Certificates**. When you open this folder, certificates are displayed along with related details in the right pane.
3. Certificates for ECLYPSE controllers are named in the following ways:
   – Local ECLYPSE Authority
   – Local **ECLYPSE-XXXXXX Authority** where **XXXXXX** is the controller's MAC address. See *Controller Identification*.

     Backup the certificate in case it will be needed: right-click the certificate and select **All Tasks\Export**.
4. Delete the certificate: right-click the certificate and select **Delete**.

When you connect to the controller, your browser will ask you to accept the new HTTPS security certificate.

Licenses

You can import licenses from your PC or a Web server, as well as export an existing license.

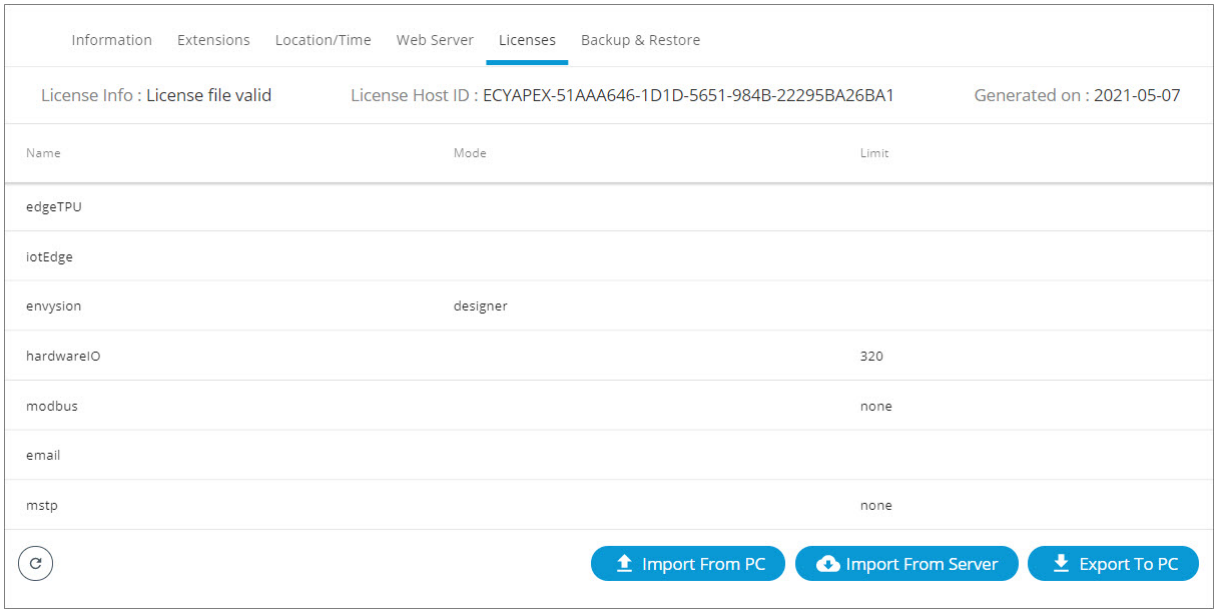


Figure 79: System Settings – Licenses

Item	Description
License Info	Basic license information.
License Host ID	License host ID.
Generated on	License generation date.
Name	The name of the licensed feature.
Mode	The feature's operating mode.
Limit	The quantity limited by the license. 'None' indicates that there is no limitation.
Import From PC	Imports a license file from your PC. 1. Click **Import from PC**. 2. Click **Upload File** to select a file from your PC or drag and drop the file in the dotted area.
Import From Server	Imports a license file directly from a Web server. Internet connectivity on the computer is required. Once connected to the Web server the license is imported and a message is displayed to confirm the successful file import.
Export To PC	Saves the controller's license file to your PC. Select **Export to PC** to download a .zip file of the license.
	Click to refresh the information in the list.

Backup and Restore

The **Backup and Restore** tab allows you to fully backup and restore the ECLYPSE controller such as the settings, extensions firmware, ENVYSION project, etc. The backup file is created on an ECLYPSE controller and can then be downloaded to the PC using the download option. The backup file can also be created on a USB key and then restored in a controller.

The backup file for an ECLYPSE controller can only be created on a FAT32-formatted USB flash drive.

The **Backup and Restore** window, shown below, is used to create a backup as well as import and restore a backup. When a backup is created, the file appears in the list as shown in the following figure.

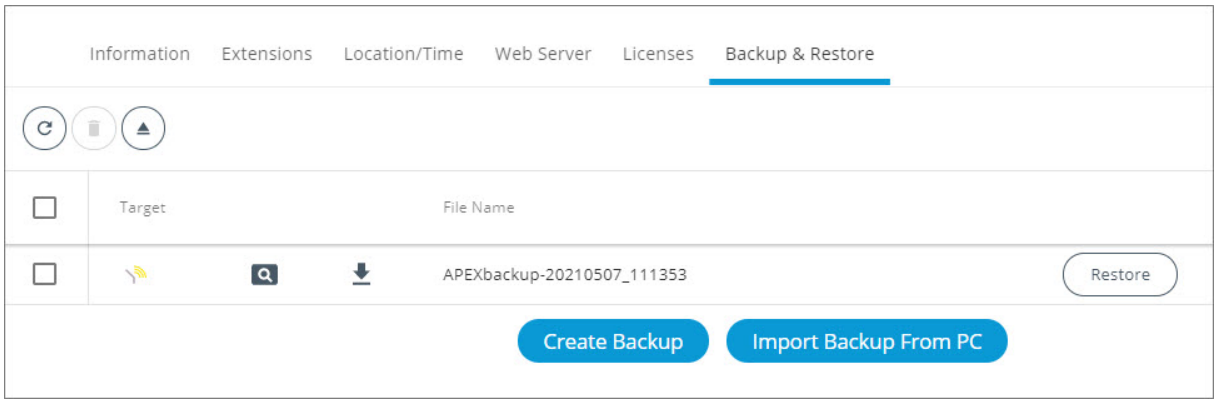


Figure 80: System Settings - Backup and Restore

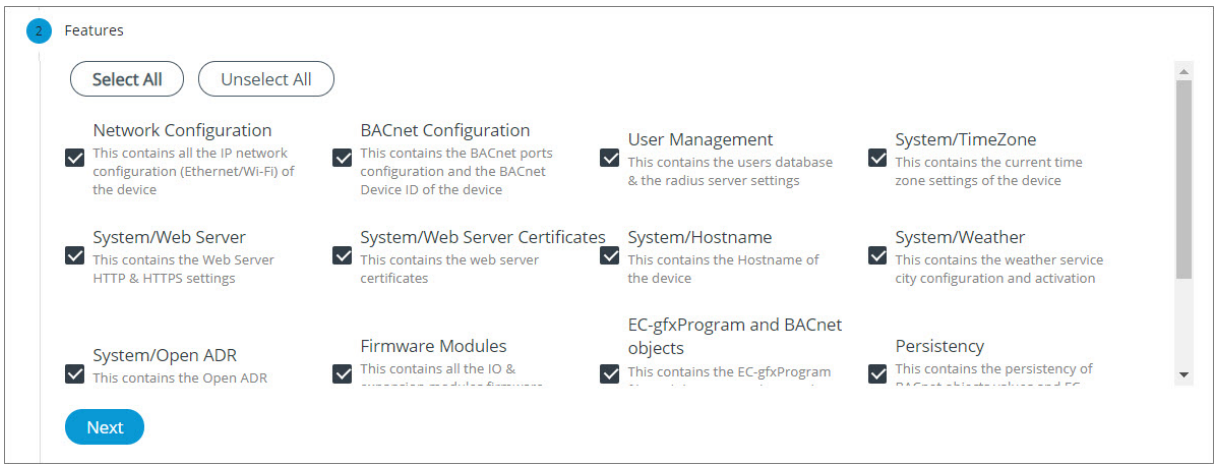
Item	Description
	Click to refresh the information in the list.
	Click to eject the USB key. This is highly recommended in order to avoid data corruption.
Checkbox	Select the checkbox next to the file or files you wish to delete. Select the main selection checkbox at the top left corner of the list to select all or deselect all items in the list.
Target	- Indicates that the backup is in the ECLYPSE controller - Indicates that the backup is in the USB key.
	Click to display a preview of the backup file information (name, status, model, firmware version, selected features, etc.). Directly from this preview window, you can choose to restore the file.
	Click to download the backup file (.ecybackup file) on your PC.
Filename	Name of the backup file.
Restore	Restore the selected backup file that is currently on your controller.
Create Backup	Start the backup process. See *Creating a Backup*.
Import Backup From PC	Import a backup from your PC.

Creating a Backup

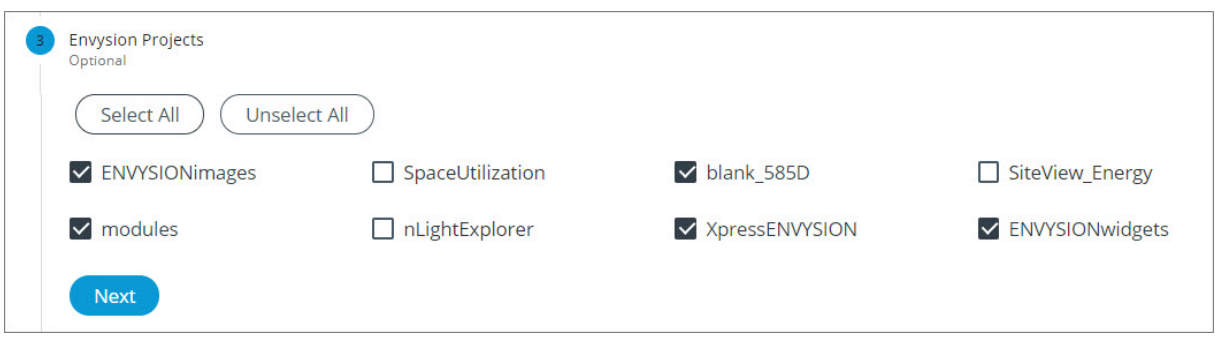
The backup functionality guides you through a series of well-defined steps to easily create the data backup.

1. In the Backup & Restore main screen, click **Create Backup**. The options to create a new backup are displayed.
2. In the **Backup File Name** section, enter the backup file name, and click **Next**.

3. In the **Features** section, select the data you wish to backup and click **Next**.

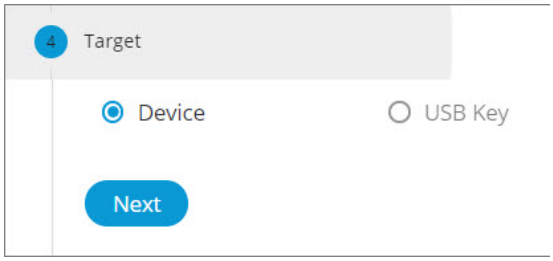


4. Select the ENVYSION projects you wish to backup and click **Next**.



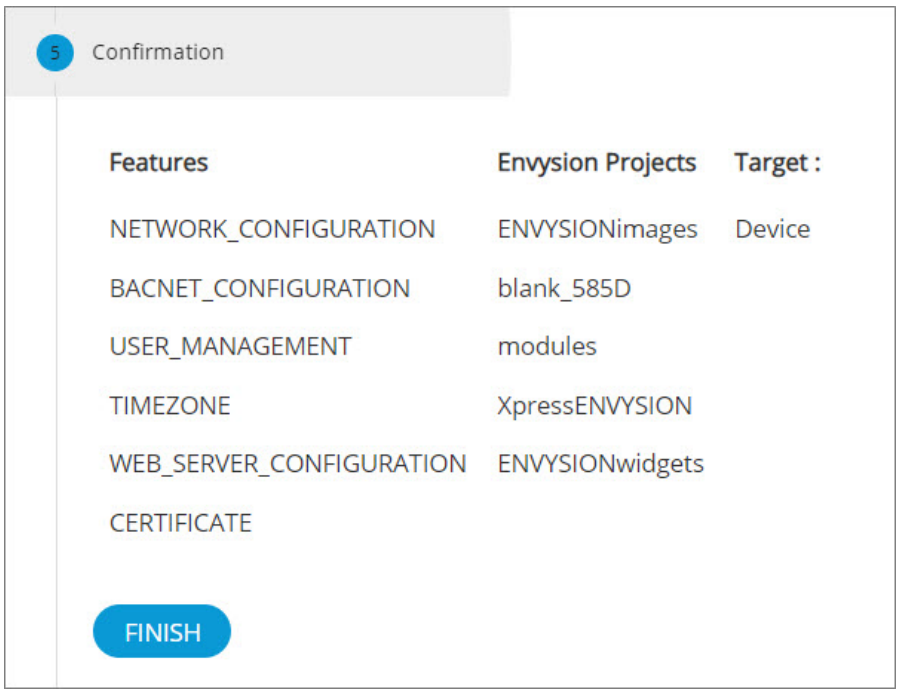
5. In the **Target** section, select to store the backup to the **Device** (Controller) or on a **USB key** plugged to the controller and click **Next**.

If no USB key is plugged in, the **USB key** option is grayed out. At this point you can insert a USB key but remember to refresh in order to make the option available.



6. In the **Confirmation** section, an overview of the data you selected to backup is displayed. Click **Finish** to create the backup.

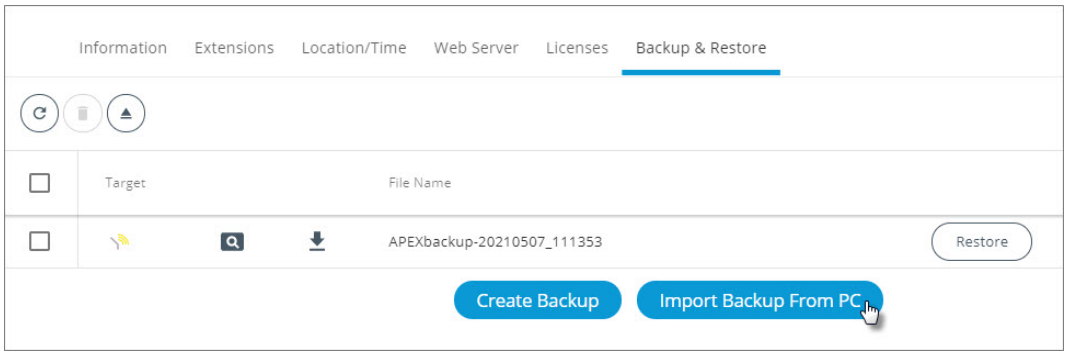
Keep in mind that space may be limited on your ECLYPSE controller therefore plan to remove the backup from the controller shortly after.



Importing a Backup from your PC or USB Key

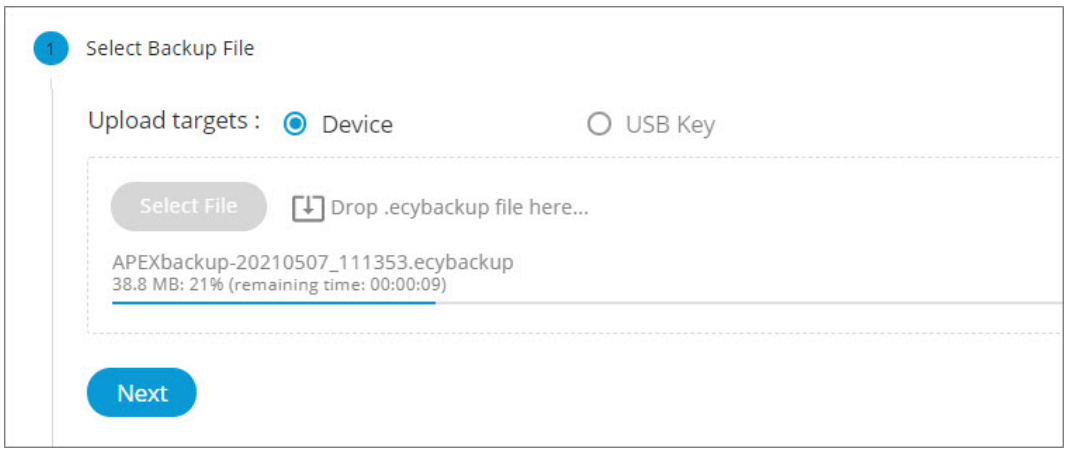
The Importing a Backup from your PC functionality guides you through a series of well-defined steps to easily import and restore a backup located on a USB drive plugged directly to the controller, or your PC.

1. In the **Backup & Restore** main screen, click **Import a Backup From PC**. The restore options are displayed.

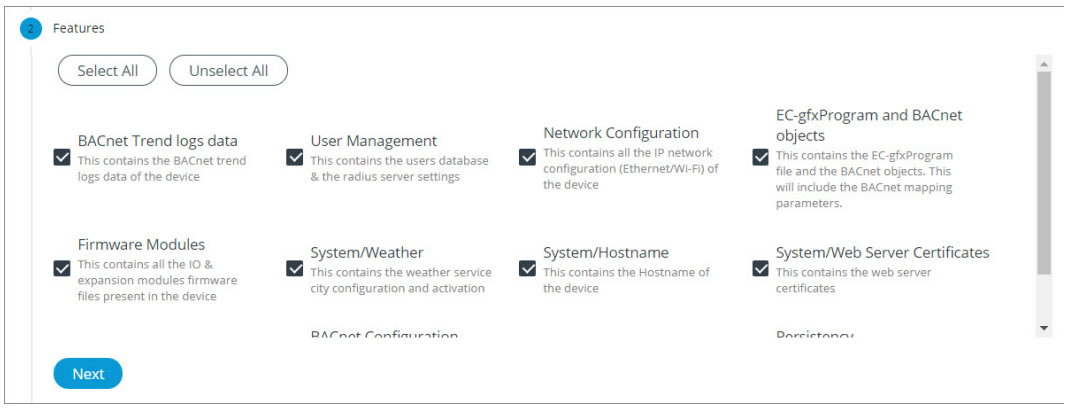


2. In the **Select Backup File** section select the upload target, either the **Device** (controller) or **USB Key**. Click **Select File** to select the backup file (.ecybackup) you wish to restore or drag and drop the backup file in the dotted area. Click **Next**.

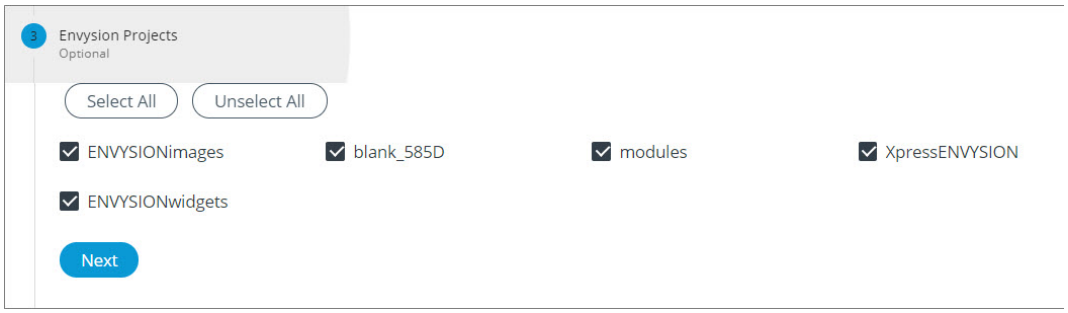
If no USB key is plugged in, the **USB key** option is grayed out. At this point you can insert a USB key but remember to refresh in order to make the option available.



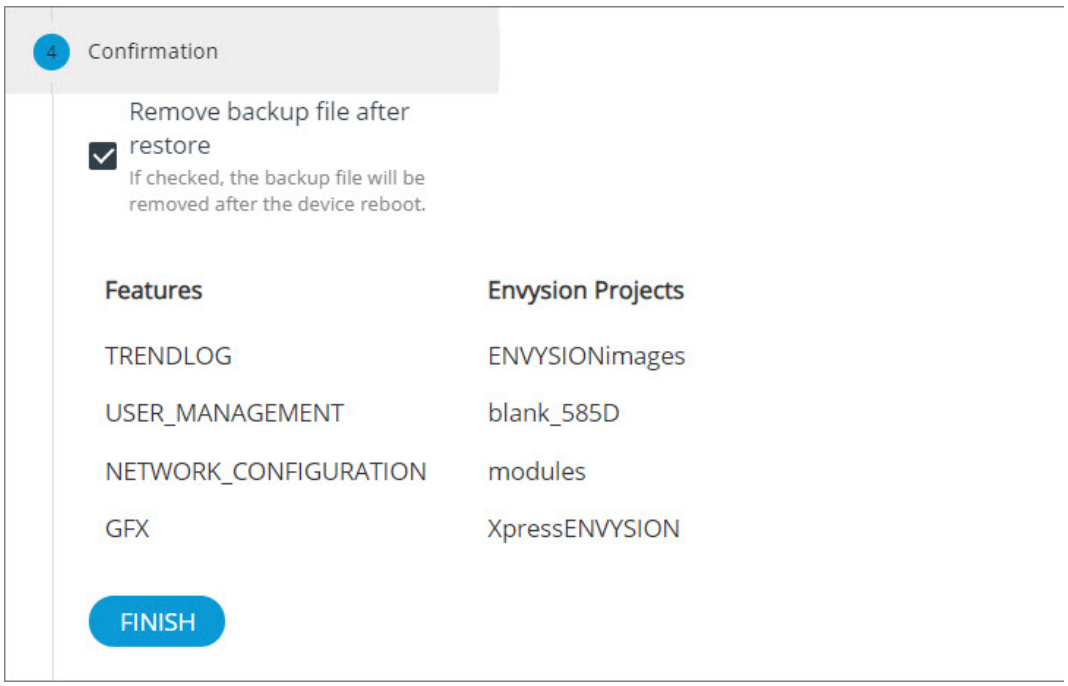
3. In the **Features** section, select the data you wish to backup and click **Next**.



4. Select the ENVYSION projects you wish to restore and click **Next**.



5. In the **Confirmation** section, an overview of the data you selected to restore is displayed and by default the **Remove backup file after restore** option is selected. When selected, the backup file will be removed after the device reboots.
   Click **Finish** to restore the backup. A status page is displayed to indicate that the data is being restored.

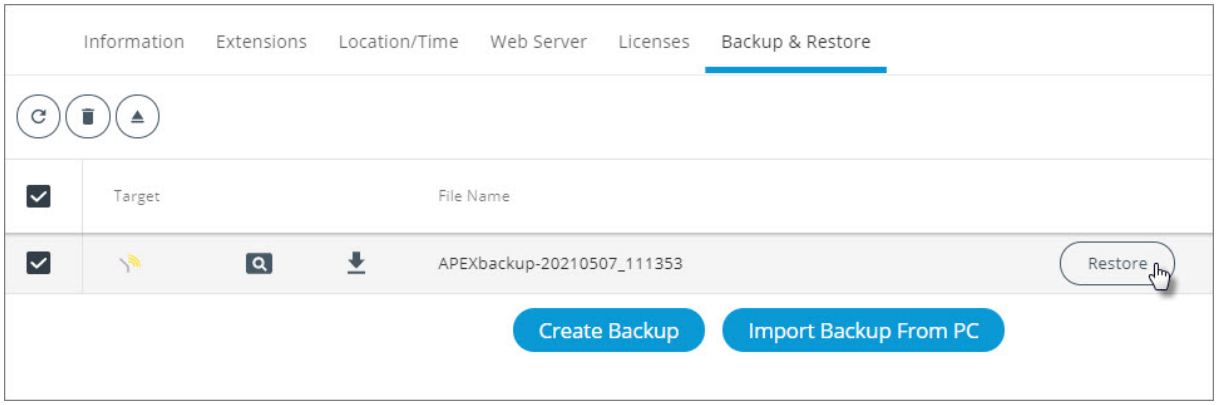


Do not power off the device or close the browser window. You will automatically be redirected to the login page once the device is ready.

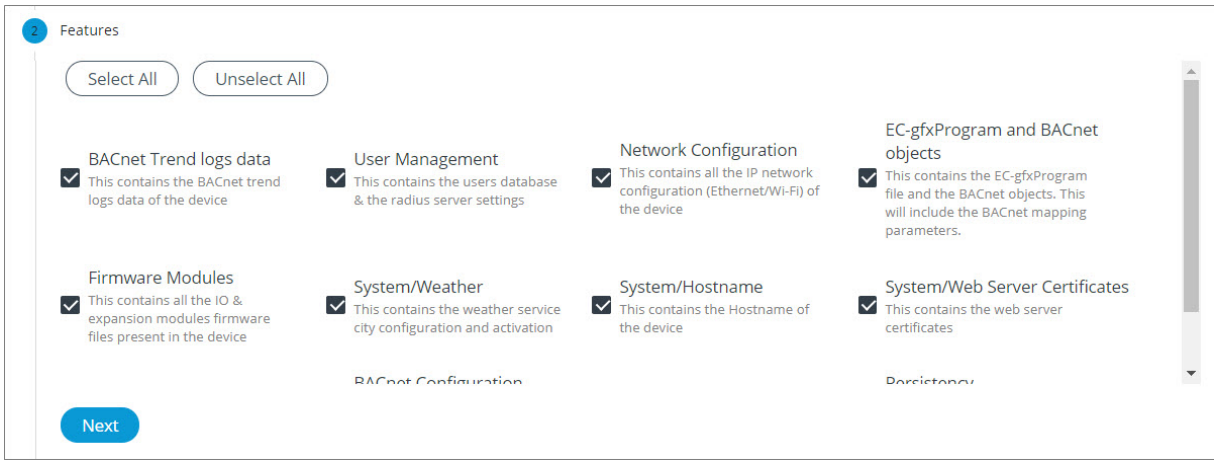
Restoring a Selected File

In the **Backup & Restore** main screen, a **Restore** button is available next to each backup file. This allows you to restore a selected backup file already available in the controller's internal memory.

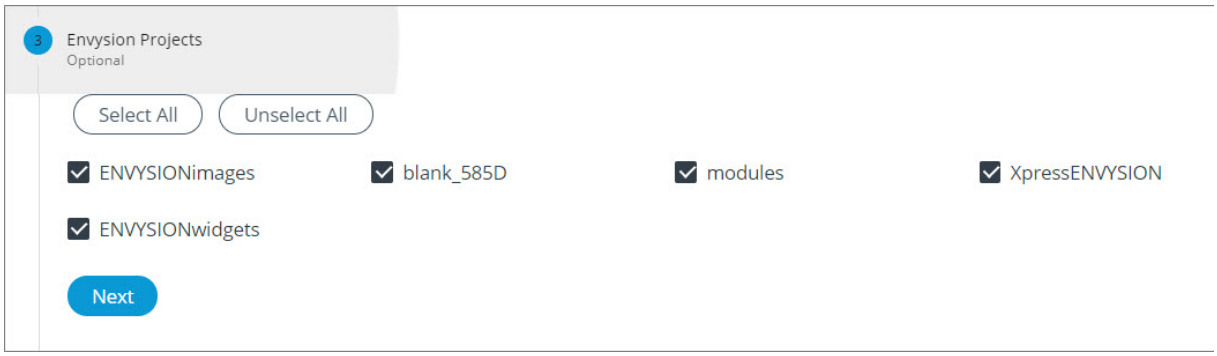
1. In the **Backup & Restore** main screen, select the backup file(s) you wish to restore from the list. Click **Restore** and the restore options are displayed.



2. Select the features you want to restore. By default, all features are selected. To unselect some of the features, simply click the checkbox or use the **Select All** or **Unselect All** options. Click **Next**.

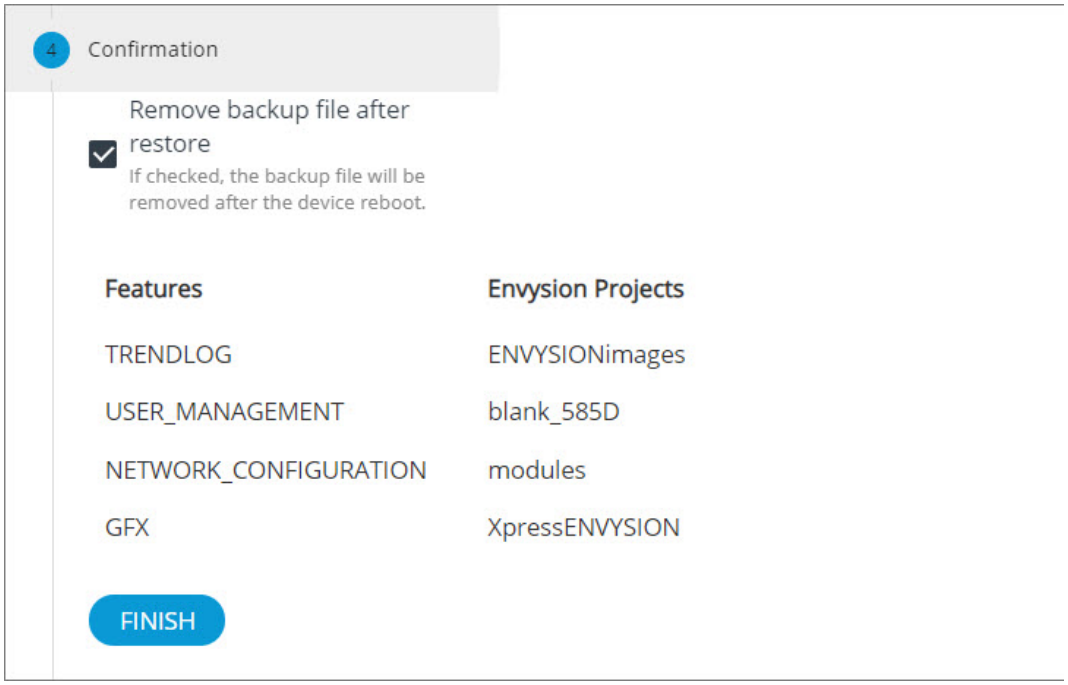


3. Select the ENVYSION projects to restore and click **Next**.



4. In the Confirmation section, review the selected features you selected and select **Remove backup file after restore** to remove the backup file from the device after reboot if you wish. Click **Finish**. The restore process may take a few minutes.

You cannot restore a backup which was created in a more recent firmware version than the one you are restoring to.

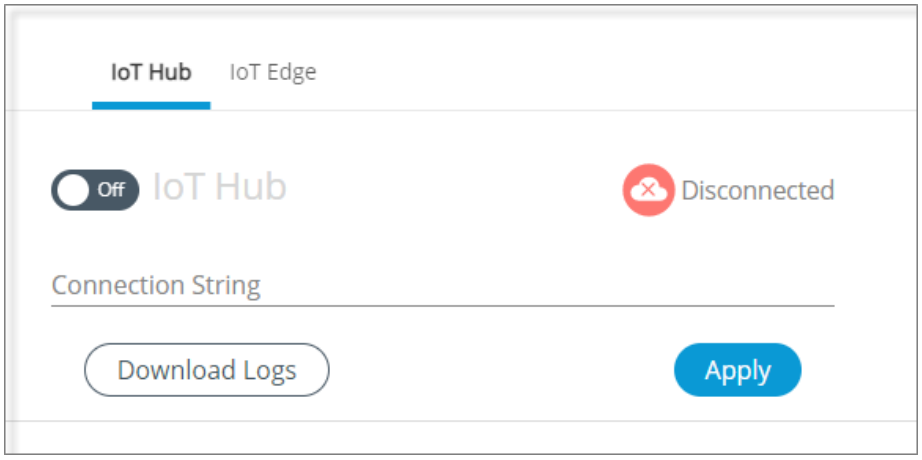


IoT

IoT Configuration

The IoT tab is used to connect to the cloud.

1. Select the **IoT** from the sidebar menu.
2. Select either the **IoT Hub** or **IoT Edge** tab.

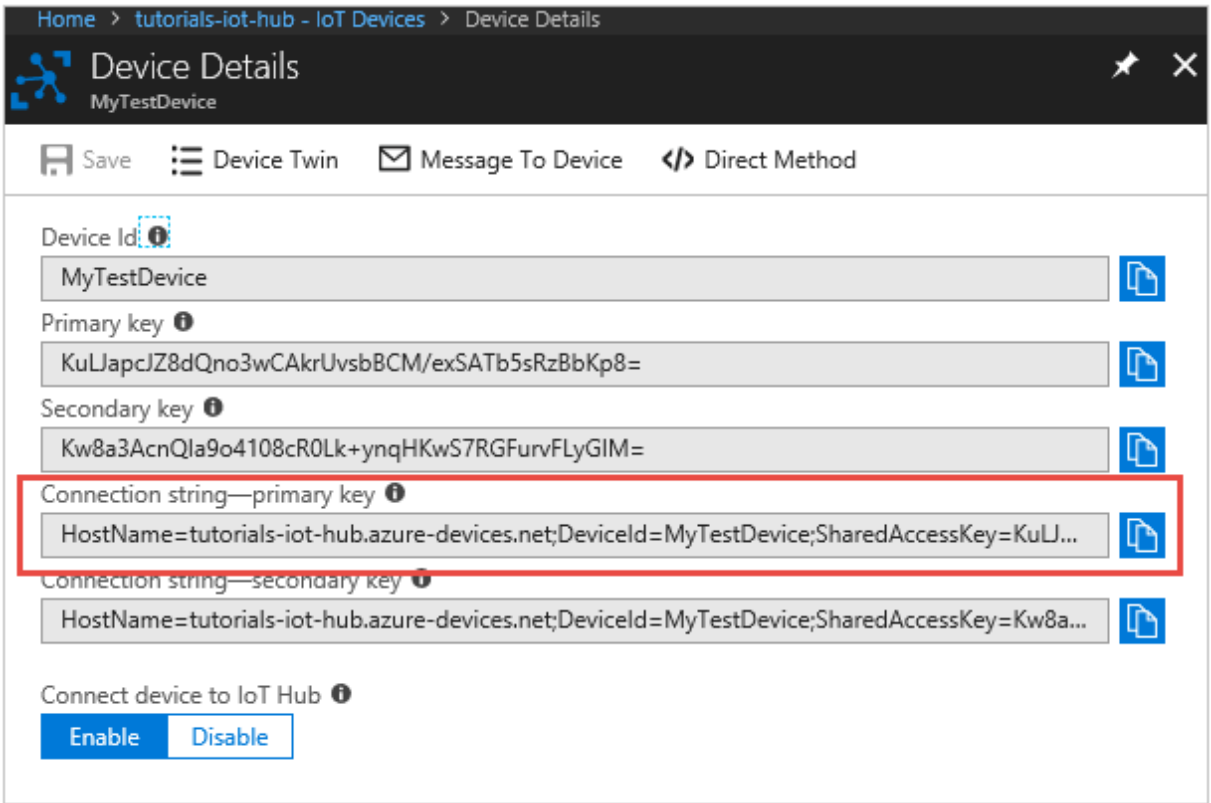


3. Enter the IoT Hub and/or Edge connection string and click **Apply**. A connection string contains the following information:

```
HostName=<hostname·of·IoT-Hub-instance>;DeviceID=<Eclypse·
Hostname>;SharedAccessKey=<Passphrase/password·assigned·to·eclypse·controller·via·
IoT·Hub>
```

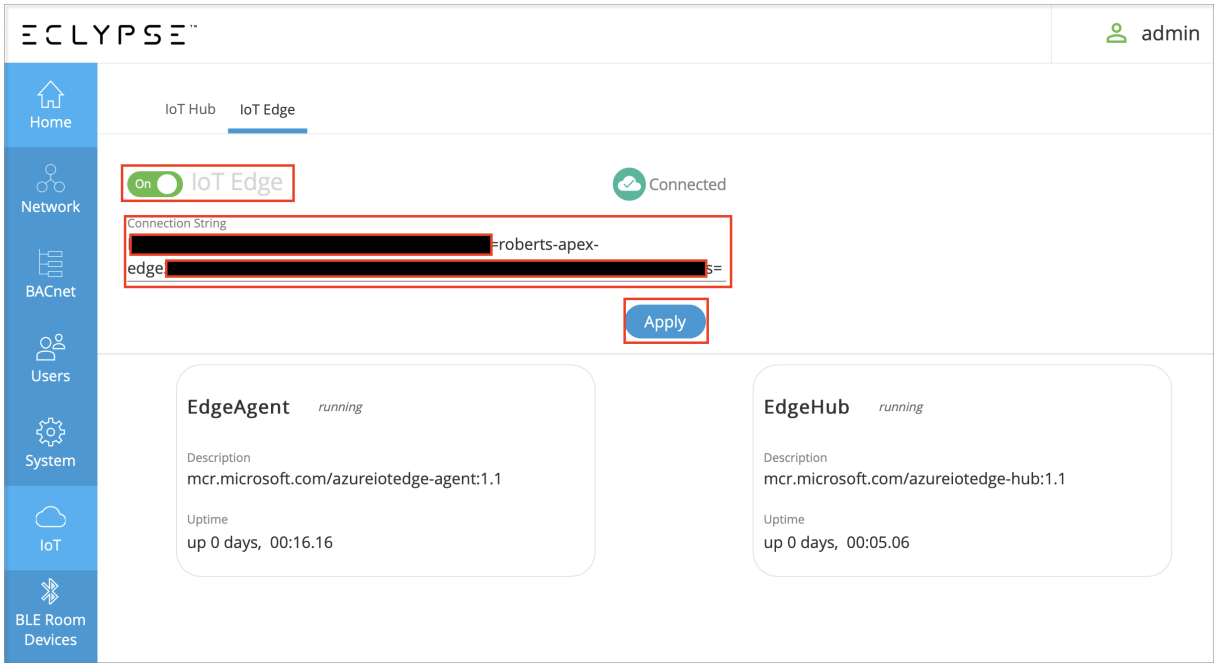
The connection string information can be found in the following locations:

- DeviceID: The host ID can be copied from the ECLYPSE Web interface home page (Host Id parameter). See *Overview*.
- Hostname and SharedAccessKey: These two strings can be retrieved from the Device Details window from the Azure portal. For more information, refer to the Microsoft Azure tutorial: *https://docs.microsoft.com/en-us/azure/iot-hub/tutorial-connectivity*



4. The device establishes a permanent connection to the IoT Hub or IoT Edge . To download the log files, click **Download Logs**. Log files contain information related to the connectivity of the controller to the cloud IoT Hub such as login attempts (success/failure) with timestamps: See the following example:

```
File  Edit  Format  View  Help
2019-01-10T15:50:58.015: CONNECTED - CONNECTION_OK
2019-01-11T08:41:00.371: DISCONNECTED_RETRYING - NO_NETWORK: Mqtt connection lost
2019-01-11T08:41:04.203: CONNECTED - CONNECTION_OK
2019-01-12T08:46:15.009: DISCONNECTED_RETRYING - NO_NETWORK: Mqtt connection lost
2019-01-12T08:46:18.787: CONNECTED - CONNECTION_OK
2019-01-13T08:51:29.127: DISCONNECTED_RETRYING - NO_NETWORK: Mqtt connection lost
2019-01-13T08:51:32.539: CONNECTED - CONNECTION_OK
2019-01-14T08:56:43.937: DISCONNECTED_RETRYING - NO_NETWORK: Mqtt connection lost
```



For more details on IoT connections, please refer to the Distech Controls Wiki at *https://wiki.distech-controls.com/en/Azure-IOT/IOT-Edge*.

IoT Best Practices

To ensure optimum EC-*gfx*Program and ENVYSION performance and long-term stability, controller memory resource recommendations should be followed.

ECY-APEX controllers have a maximum of 1024 MB of dedicated memory for containers, however, no more than 512 MB should be used. Containers are also limited to a maximum of two cores in total. It is recommended to use 512MB of memory so as to maintain performance quality and stability for other critical functions of the controller.

When deploying Docker containers, “Memory” should not surpass 512 MB in total for all containers, and “CpusetCpus” should be set to “0”, “1”, or “0,1” CPU cores.

Distech Controls recommends for developers using the ECY-APEX to always deploy a Netdata container for container monitoring, and to add no more than two additional containers (total: 3 Docker containers). More containers can be added but performance cannot be guaranteed. To increase controller performance and stability in cases of a high load, a second ECY-APEX can be added.

Docker Container Deployment Example

In the following container deployment example, two container applications running Netdata and Red Node are shown. Each container is allocated 256 MB of memory and are sharing the resources of the same CPU core. In this deployment, the total recommended memory limit of 512 MB has been reached and no additional containers should be added.

Netdata example:

```
## NetData
http://0.0.0.0:50099

### Image
`docker.io/netdata/netdata`


### Container Create
```JSON
{
    "HostConfig": {
        "Memory": 268435456,
        "CpuPeriod": 25000,
        "CpuQuota": 50000,
        "CpusetCpus": "0",
        "LogConfig": {
            "Type": "none",
            "Config": { }
        },
        "PortBindings": {
            "19999/tcp": [{
                "HostPort": "50099"
            }]
        },
        "Mounts": [{
            "Target": "/etc/netdata",
            "Source": "netdataConfig",
            "Type": "volume",
            "ReadOnly": false,
            "Consistency": "default"
        }]
    }
}
```
```

Node Red Example:

```
## Node-RED
http://0.0.0.0:50080

### Image
`docker.io/nodered/node-red`

### Variables
`NODE_TLS_REJECT_UNAUTHORIZED` `Number` `0`
`NODE_OPTIONS`  `Text`  `--max_old_space_size=128`
`TZ` `Text` `America/New_York`

### Container Create
```JSON
{
    "HostConfig": {
        "Memory": 268435456,
        "CpuPeriod": 25000,
        "CpuQuota": 50000,
        "CpusetCpus": "0",
        "PortBindings": {
            "1880/tcp": [{
                "HostPort": "50080"
            }]
        },
        "Mounts": [{
            "Target": "/data",
            "Source": "node-red",
            "Type": "volume",
            "ReadOnly": false,
            "Consistency": "default"
        }]
    }
}
```

BLE Room Devices

The **BLE Room Devices** tab enables web configuration of Distech Controls line of *Bluetooth*® low energy technology enabled devices, namely the Allure UNITOUCH™, the EC-Multi-Sensor-BLE, or the UNIWAVE. All devices must first be correctly programmed into the controller using EC-*gfx*Program before they will appear in this tab.

The BLE Room Devices tab consists of two main screens: BLE Room Devices and Beacons.
```

BLE Room Devices

The **BLE Room Devices** main screen presents the details of the Bluetooth enabled room devices currently programmed in your ECLYPSE controller.

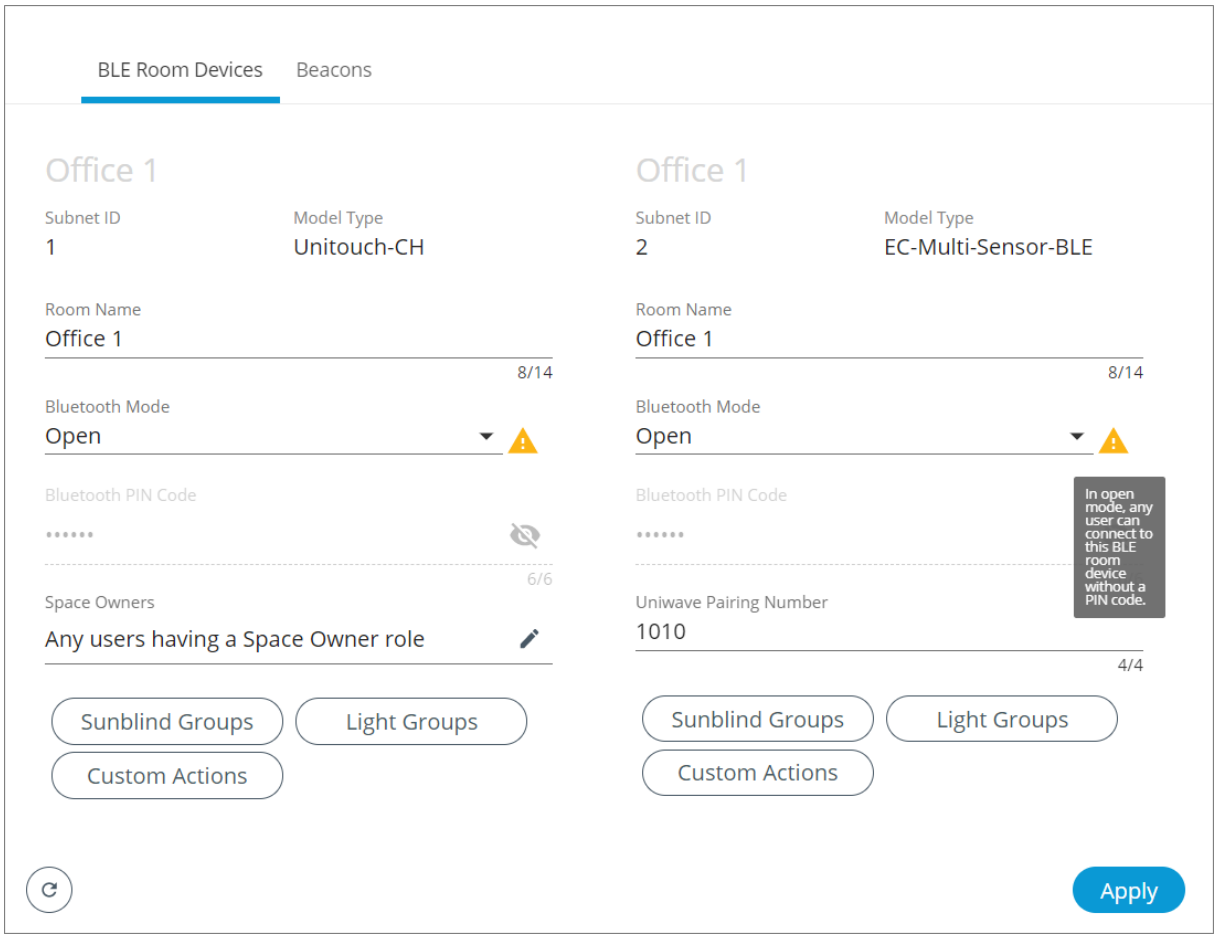


Figure 81: BLE Room Devices Web Page

Item	Description
Subnet ID	This indicates the current subnet ID assigned to the device.
Model Type	This indicates the model of the BLE enabled device.
Room Name	Enter a description of the room or location of where the device is located. This name will appear on either the UNITOUCH screen or UNIWAVE device as well as in the *my* PERSONIFY mobile application device list.
Bluetooth Mode	Choose the Bluetooth mode required for the device. ☐ **Commissioning**: Bluetooth connection is used for commissioning the device. This option is the factory default mode (default PIN code 999995) and has short range for commissioning purposes only. ☐ **Disabled:** Bluetooth connection is disabled and does not allow any wireless connections to the device. ☐ **Open**: Bluetooth connection is open and is not authenticated with a PIN code. We recommend this option for rooms or areas that are accessible to anyone. ☐ **Private**: Bluetooth connection is authenticated with a six (6) digit PIN code. When this mode is selected, you will be prompted to change the PIN code as the default PIN code is not allowed while using Private mode. We recommend this option for private rooms and areas.
Bluetooth PIN Code	If Private Bluetooth mode is enabled, choose the PIN code required to wirelessly connect to the device using a smartphone or tablet. When Private mode is selected, you will be prompted to enter a minimum six (6) digit PIN code which must be different that the default PIN code. Use the icons to show or hide the PIN code.
Space Owners	Use the icon to add, edit, delete, and assign users as a space owner. See *Space Owners* for more information.
UNIWAVE Pairing Number	The UNIWAVE pairing number can be changed here. This pairing number is required to connect a UNIWAVE device and must be input directly in the device as well.
Sunblind Groups	Define display names and enable or disable the sunblind groups. Sunblind groups must first be added and configured in EC-*gfx*Program. See the EC-*gfx*Program User Guide for more information.
Light Groups	Define display names and enable or disable the light groups. Light groups must first be added and configured in EC-*gfx*Program. See the EC-*gfx*Program User Guide for more information.
Custom Actions	Define display names and enable or disable Custom Actions. Custom Actions must first be added and configured in EC-*gfx*Program. See the EC-*gfx*Program User Guide for more information.
	Click to refresh the information in the list.
Apply	Click **Apply** to apply and save all changes.

Table 5: BLE Room Device Configuration

Space Owners

A Space Owner can have certain advanced controls over the UNITOUCH based on roles assigned to that person upon being added as a user in the Current User Database. To access the advanced settings on the UNITOUCH, a space owner requires knowledge of the *exact name* and *password* from the Current User Database that was assigned to that specific user. See *User Management* and *Adding a User in Server Mode* for more information users and roles. See the Allure UNITOUCH User Guide for more detailed information on how to access advanced settings on the UNITOUCH.

Upon clicking the icon, the Space Owners dialogue box appears.

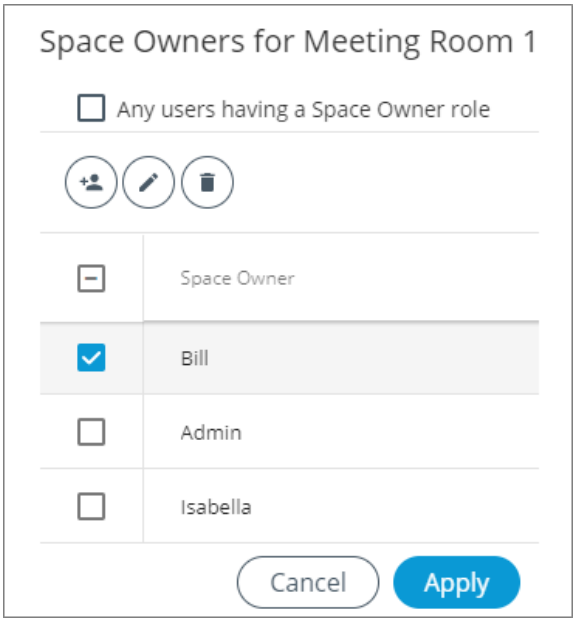


Figure 82: Space Owner Dialogue Box

Item	Description
Any users having a Space Owner role	This option gives access to anyone within the Current User Database that has been assigned a Space Owner role but is not necessarily in the list of Space Owners in the Space Owner dialogue box.
	Add a person as a Space Owner for the UNITOUCH. This name must be an exact match to the name in the Current User Database. The space owner should also know their password that was assigned in the Current User Database to be able to access advanced settings on the UNITOUCH. **Note:** The name of the person added must also be added as a user to the Current User Database and have correctly assigned roles. See *Adding a User in Server Mode*.
	Edit the Space Owner name. Select one Space Owner at a time and click the edit icon to change the Space Owner name.
	Delete a space owner. Select one or more Space Owners from the list and click the delete icon to delete them.
Cancel	Click to cancel all changes and close the dialogue box.
Apply	Click **Apply** to apply and save the changes.

Table 6: Space Owners Options and Configuration

If the Space Owner dialogue box is unpopulated (completely empty) and "**Any users having a Space Owner role**" is unchecked for an Allure UNITOUCH, any person can have read access to the PIN code. This means that any person can potentially have unauthorized wireless access to temperature, lighting, and sunblind settings. Therefore, an unpopulated Space Owner list is not recommended and should be avoided.

Groups and Actions

Sunblind Groups, Lighting Groups, and Custom Actions must first be added and configured with EC-*gfx*Program. See the EC-*gfx*Program User Guide for more information. Once they have been added, configured, and synchronized with the controller, they will now be visible in the Web Configuration page.

After clicking the Sunblind Groups, Light Groups, or Custom Actions buttons, a dialogue window shows the options available.

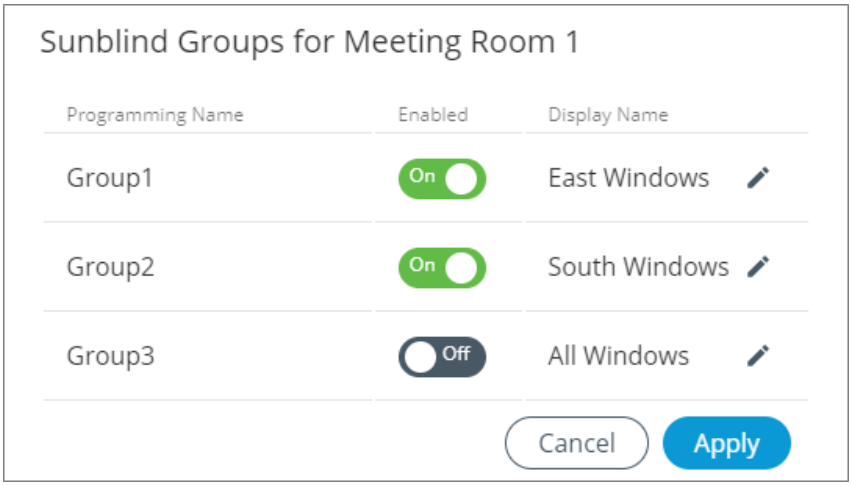


Figure 83: Sunblind Groups Dialogue Box

Item	Description
Programming Name	This displays the name given in the EC-*gfx*Program programming sheet. This name can only be edited in EC-*gfx*Program.
Enabled On Off	Enable or disable the group from being visible on the UNITOUCH and the *my* PERSONIFY mobile application.
Display Name	The Display Name will be displayed on the UNITOUCH screen, the *my* PERSONIFY mobile application, or on a UNIWAVE device. By default, the Display Name is the same as the Programming Name. The Display Name can be edited using the icon, however there is a 14 character limit. When creating custom actions, it is recommended that you assign descriptive names with a maximum of 13 characters for the UNIWAVE and 15 characters for the UNITOUCH, to ensure that the name is fully visible on the display.
Cancel	Click **Cancel** to abort all changes and close the dialogue box.
Apply	Click **Apply** to apply and save the changes.

Beacons

The beacon option, commonly used for indoor positioning, is available in certain countries only.

The **Beacons** screen presents all beacon-enabled EC-Multi-Sensor-BLE devices declared for your ECLYPSE controller. It is displayed within the **BLE Room Devices** tab as soon as you have defined one or more EC-Multi-Sensor-BLE devices via EC-*gfx*Program, even if they are not physically connected to the controller. This allows you to edit your beacon configuration offline, before applying it to the actual physical devices.

Figure 84: Beacons Screen

Item	Description
	Edit the beacon options. Select one Beacon at a time and click the edit icon to change the Beacon options.
	Use the Enable Selected Devices button and the Disable Selected Devices button to quickly enable or disable the beacon functionality independently from the my PERSONIFY interface function.
Room Name	This is a descriptive label of the room or location where the device is located. The value of this field is the same as the one entered in the **Room Name** field of the **BLE Room Devices** screen. If you change it in the **BLE Room Devices** screen and click **Apply**, it will change automatically here too. If you change it in the **Beacons** screen, the change will be automatically applied to the **BLE Room Devices** screen.
UUID	The universally unique identifier (UUID) is a 128-bit number meant to uniquely identify your beacons' network. A company should typically have its own UUID, which should be used all over its buildings (see the example below). A UUID is composed of 32 hexadecimal digits split into 5 groups separated by hyphens. The factory default value can be modified via the Edit Beacons screen.
Major Number	This indicates the Major value, which is intended to identify a group of beacons of your EC-Multi-Sensor-BLE, e.g. all the beacons located in a given zone. Each building should typically have its own Major value (see the example below). The factory default value is based on the MAC address of your BLE device. For example, if the MAC is F3B3701CECAE55AA, the Major will be 701C (hexadecimal) / 28700 (decimal). The factory default value can be modified via the **Edit Beacons** screen.
Minor Number	This indicates the Minor value, which represents each beacon's individual identifier. The factory default value is based on the MAC address of your BLE device. For example, if the MAC is F3B3701CECAE55AA, the Minor Number will be F3B3 (hexadecimal) / 62387 (decimal). The factory default value can be modified via the **Edit Beacons** screen.
Enabled	This indicates whether the beacon has been enabled, i.e. whether the beacon function is active for the device. To enable it, use the **Enable** toggle in the **Edit Beacons** screen.
Reset	Click **Reset** to reset the devices to their default values. For the devices that are both declared in EC-*gfx*Program and physically connected to the ECLYPSE controller, the **Reset** button resets the **Room Name**, **UUID**, **Major Number**, and **Minor Number** fields. For the devices that are only declared in EC-*gfx*Program but not physically connected to the ECLYPSE controller, the **Reset** button only resets the **Room Name** field. The **Reset** button does not reset the **Enabled** field.
Export to CSV	Click **Export to CSV** to export your beacon data in a .csv file. This file includes the following details for each connected device: ☐ **Room Name**: the value entered in the Room Name field;

Item	Description
	☐ **Hardware ID**: the serial number that also appears in the Extension screen of the System tab; ☐ **UUID**: the value of the UUID field; ☐ **Major Number**: the value of the Major Number field; ☐ **Minor Number**: the value of the Minor Number field; ☐ **RSSI**: the received signal strength indicator (RSSI); ☐ **Enabled**: the position of the Enable toggle.

Table 7: Beacons Configuration

The UUID-Major-Minor triplet is meant to uniquely identify each beacon. Example:

Building 1
Beacon 1 -> UUID: 274be2bd-47e1-5995-889b-4f0316eed60a, Major: 1, Minor: 54
Beacon 2 -> UUID: 274be2bd-47e1-5995-889b-4f0316eed60a, Major: 1, Minor: 65

Building 2
Beacon 1 -> UUID: 274be2bd-47e1-5995-889b-4f0316eed60a, Major: 2, Minor: 54
Beacon 2 -> UUID: 274be2bd-47e1-5995-889b-4f0316eed60a, Major: 2, Minor: 65

Edit Beacons

The **Edit Beacons** screen allows you to edit the beacon properties of your connected EC-Multi-Sensor-BLE devices. The edition can be performed for a single device or for more than one device at a time. To edit the beacon properties:

1. Select the device(s) to edit by checking the corresponding boxes to the left. You can also select all available devices at once, by checking the header box.
2. Click the edit icon located in the top left corner of the **Beacons** screen.

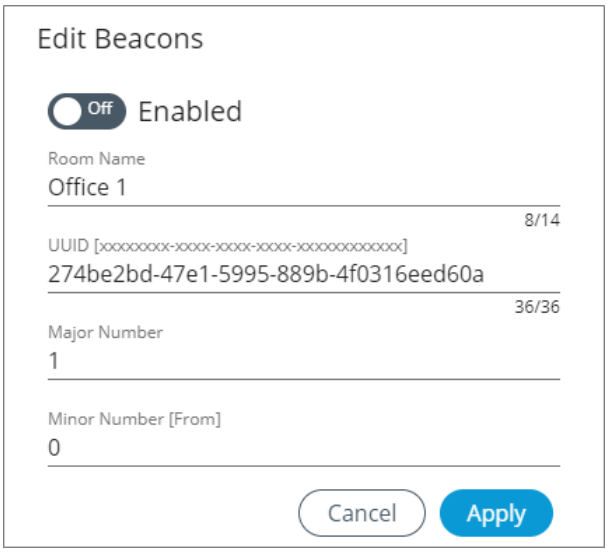


Figure 85: Edit Beacons Dialogue Box

Item	Description
Enable	Use this toggle to enable the beacon, i.e. to activate the beacon function for the device. If you have selected multiple devices, the toggle is set to Off by default.
Room Name	Enter or edit the descriptive label of the room or location where the device is located. Maximum number of characters: 14. If you have selected multiple devices, once you have edited the name, all the selected devices will have the new name, but an increment will automatically be added to the end (e.g. Name1, Name2, Name3…) to make each name unique. When the increment is added to the end, the system may trim the name to respect the 14-character size limit. If you have selected a single device, you can freely edit its name, even if the new name is the same as the name of another device. This allows you to put the same name to different devices.
UUID	The UUID of your beacons' network. If you edit this value, make sure to respect the formal constraints related to the standard UUID format: 32 hexadecimal digits grouped in 5 sets separated by hyphens. The UUID is supposed to be the same all over your sites. You can however modify it for one or more devices, but the system will ask you to confirm the edition.
Major Number	Use this field to edit the Major Number value, which is used to identify a group of beacons, e.g. all the beacons located in a given zone. It is recommended that you use one Major Number value per location (e.g. building). The allowed values range between 0 and 65535 (or 0xFFFF in hexadecimal).
Minor Number	Use this field to edit the Minor Number value, which represents each beacon's individual identifier. You must assign a unique Minor Number value to each beacon in your network (i.e. two beacons should not have the same Minor Number). If you have selected multiple devices, as soon as you enter a number in this field and click **Apply**, the Minor Number value will be automatically readjusted for all devices to ensure they all have a unique value. The allowed values range between 0 and 65535 (or 0xFFFF in hexadecimal).
Reset	Click **Reset** to reset all the fields to their factory default values.
Cancel	Click **Cancel** to cancel all the changes you have made in this screen.
Apply	Click **Apply** to apply all the changes you have made in this screen.

Table 8: Beacons Editing Screen

CHAPTER 9
Configuring the ECLYPSE Wi-Fi Adapter Wireless Networks

The ECLYPSE Wi-Fi Adapter supports a number of wireless network connection modes. This chapter describes how to configure a controller's wireless network. See also *ECLYPSE Wi-Fi Adapter Connection Modes*.

Setting up a Wi-Fi Client Wireless Network

This connects the controller as a client of a Wi-Fi access point. See *Wi-Fi Client Connection Mode* for more information.

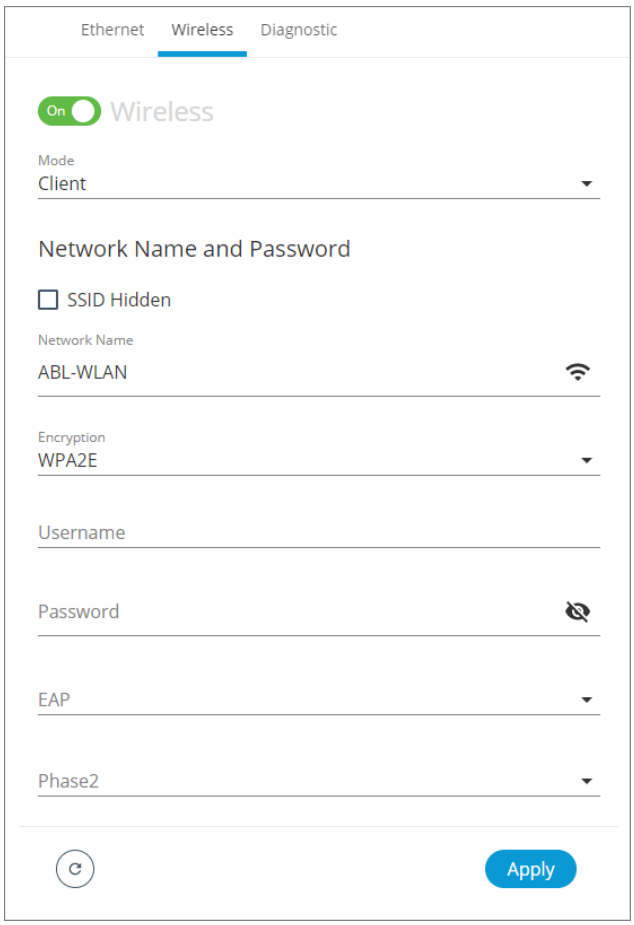


Figure 86: Client Wireless Network Settings

Configure the controller's ECLYPSE Wi-Fi adapter mode as a Wi-Fi client as follows.

1. Set **Wireless** to **On**.
2. Set the **Mode** to **Client**.
3. Choose whether the SSID should be hidden or not.

4. Click the Find Network icon to search for available access points that are within range. The access points are listed on the right.

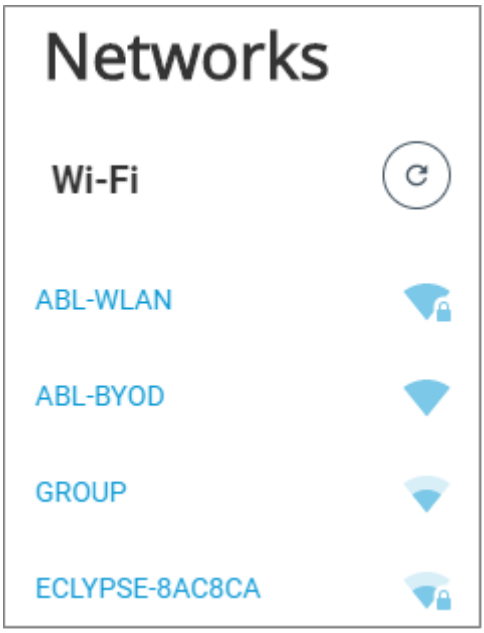


Figure 87: List of Available Access Points to Pair With

5. Set the encryption mode to be used by this access point in **Encryption**:
   - **OPEN: this option should be avoided** as it does not provide any wireless security which allows any wireless client to access the LAN.
   - **WPA2**: select the Wi-Fi Protected Access II option to secure the Wi-Fi network with a password.
   - **WPA2 Enterprise**: Use this option if you are connecting to an enterprise network that has a working RADIUS authentication server. This RADIUS server provides user authentication.
6. Enter the required **Username** and **Password**.
7. Choose the access point's **Extensible Authentication Protocol (EAP)** and **Phase2** type.
8. Click **Apply**.

Setting up a Wi-Fi Access Point Wireless Network

This turns the controller into a Wi-Fi access point that other wireless clients can use to have network access. This access point operates off of the same subnetwork and has the same IP connectivity that the controller has with its wired network connection. For example, if the controller's wired connection is to a network that has an active DHCP server, access point clients can also use this DHCP server to automatically configure their IP connection parameters. See *Wi-Fi Access Point* for more information.

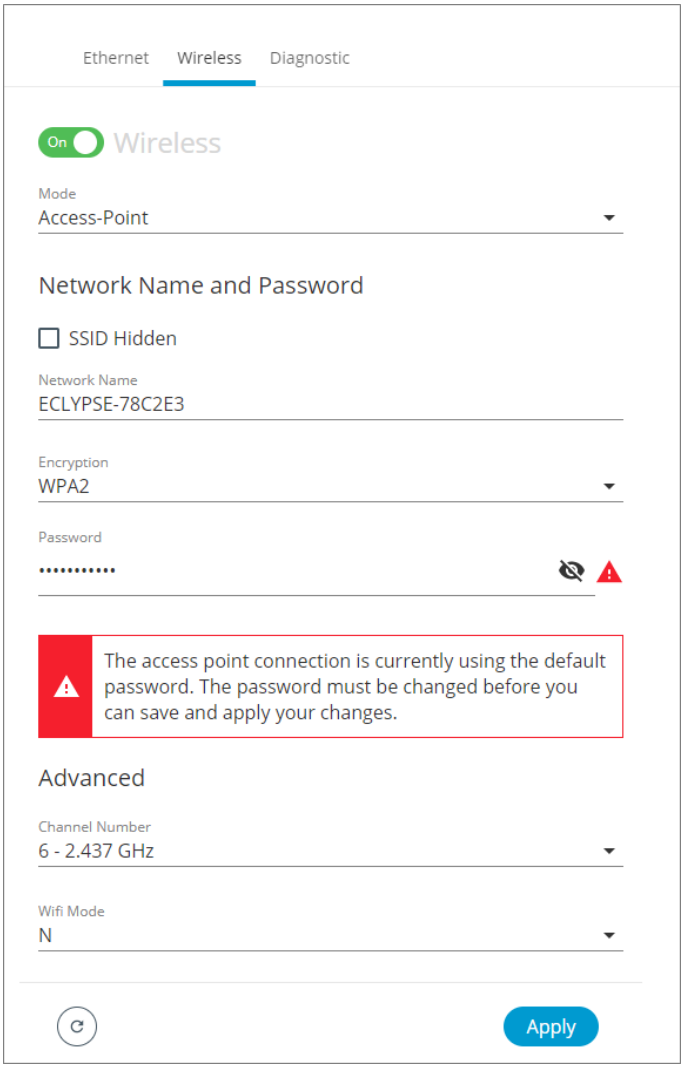


Figure 88: Access Point Wireless Network Settings

Configure the controller's ECLYPSE Wi-Fi adapter mode as a Wi-Fi access point as follows.

1. Under **Wireless Configuration**, set wireless to **On**.
2. Set the **Mode** to **Access-Point**.
3. Choose whether the **SSID** should be hidden or not.
4. Set the name for this access point by which wireless clients will identify it in **Network Name**.
5. Set the encryption mode to **WPA2**, the Wi-Fi Protected Access II option, to secure Wi-Fi network with a password.
6. Set the access point's authentication password in **Password**. This is the password wireless clients will need to know in order to connect to this access point. The default password must be changed before you can save and apply your changes to this page.
7. Under **Advanced**, set the **Channel Number** and **Wi-Fi Mode**. See *Wireless Configuration* for an explanation of these parameters.
8. Click **Apply**.

Setting up a Wi-Fi Hotspot Wireless Network

This turns the controller into a Wi-Fi hotspot with a router. This puts the hotspot into a separate sub-network with a DHCP server to provide IP addresses to any connected device. See *Wi-Fi Hotspot* for more information.

Wide area network (WAN) connectivity is through the wired connection. See *Network Address Translation / Firewall*. Though BACnet/IP uses IP protocol to communicate, this hotspot acts as an IP router; it does not forward broadcast messages which are important in BACnet to identify services that are available within the BACnet internetwork. See *BACnet/IP Broadcast Management Device Service (BBMD)*.

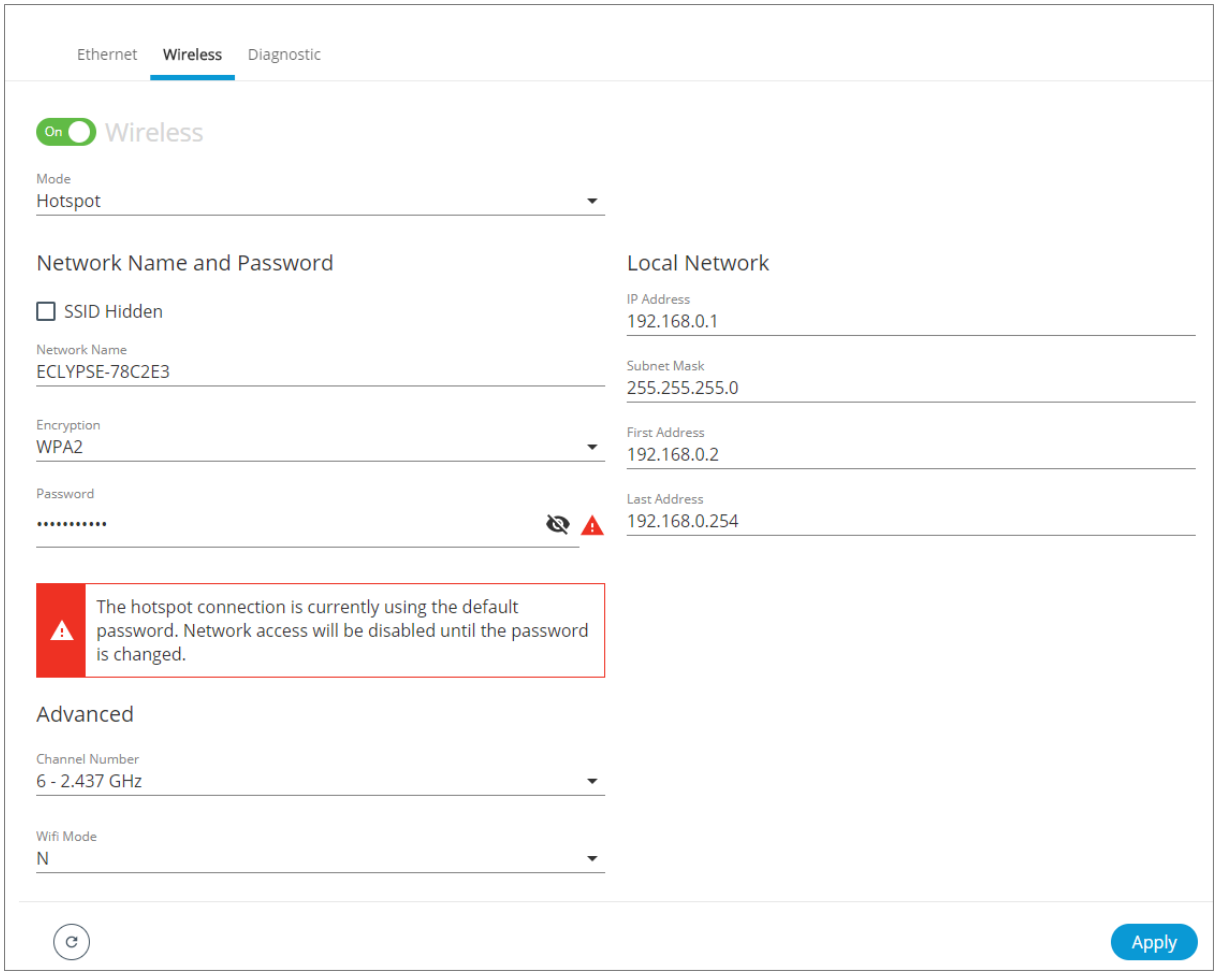


Figure 89: Hotspot Wireless Network Settings

Configure the controller's ECLYPSE Wi-Fi adapter mode as a Wi-Fi hotspot as follows.

1. Under **Wireless Configuration**, set wireless to **On**.
2. Set the **Mode** to **Hotspot**.
3. Choose whether the **SSID** should be hidden or not.
4. Set the name for this access point by which wireless clients will identify it in **Network Name**.
5. Set the encryption mode to **WPA2**, the Wi-Fi Protected Access II option, to secure Wi-Fi network with a password.
6. Set the hotspot's authentication password in **Password**. This is the password wireless clients will need to know in order to connect to this hotspot. Network access will be disabled until the default password is changed.

7. Set the hotspot's IP address that wireless clients will connect to in **Ip Address**. Ensure that this address is:
   - Not in the range of IP address set by **First Address** and **Last Address**.
   - Not the same as the **IP address** set under IP Configuration for the wired network.
8. Set the hotspot's subnet mask in **Subnet Mask**. See *About the Subnetwork Mask*.
9. Set the hotspot's addressing range in **First Address** and **Last Address**. This defines the range of IP addresses to be made available for hotspot clients to use. The narrower the range, the fewer hotspot clients will be able to connect due to the lack of available IP addresses. For example, a range where First Address = 192.168.0.22 and Last Address = 192.168.0.26 will allow a maximum of 5 clients to connect to the hotspot on a first-to-connect basis.
10. Under **Advanced**, set the **Channel Number**, and **Wi-Fi Mode**. See *Wireless Configuration* for an explanation of these parameters.
11. Click **Apply**.

CHAPTER 10
Securing an ECLYPSE Controller

This section describes how to secure an ECLYPSE controller from unauthorized access and use.

Introduction

This chapter describes how to implement best security practices for ECLYPSE controllers. Security is built up layer upon layer to make the system more resistant to attacks. This involves taking simple but effective steps to implement built-in security features.

Passwords

A username / password combination (or credentials) authenticates a user's access rights to a controller. If an attacker gains access to a user's password, the attacker has access to carry out any action on the controller that is allowed by that user's permissions.

Change the Default Platform Credentials

At the first connection to an ECLYPSE you will be forced to change the password to a strong password for the admin account to protect access to the controller.

It is important to create new user accounts with strong passwords to protect the controller from unauthorized access. The username / password can be changed in *User Management* and see also *Supported RADIUS Server Architectures*.

Use Strong Passwords

Passwords should be hard to guess. Avoid birth dates and common keyboard key sequences. A password should be composed of a random combination of 8 or more uppercase and lowercase letters, numbers, and special characters.

Do not allow a browser to remember a user's login credentials

When logging into a controller with certain browsers, the browser asks to remember a user's login credentials. When this option is set, the next time the user logs in, the credentials will automatically be filled in. While this is convenient, anyone with access to the computer can login using those credentials. Do not set this option for administrator accounts or when accessing an account from an unsecure computer.

Account Management and Permissions

User accounts must be properly managed to make it harder for an attacker to compromise security, and to make it easier to detect that an attack has occurred. To set user account parameters, see *User Management*.

Use a Different Account for Each User

Each user account should represent an individual user. Multiple users or user groups should not share an account.

Suspending an account shuts-off a single user's access to the controller – it does not disrupt many users.

Permissions can be tailored to the needs of each user. A shared account may have more permissions than all users should have.

A shared account has a shared password which is more likely to be leaked.

It is harder to implement password expiration requirements.

Use Unique Service Type Accounts for Each Project

System integrators should use different credentials for each job they do. Should an attacker gain access to one system, they cannot readily access all systems installed by the same system integrator.

Disable Known Accounts When Possible

Create a new user admin account with new credentials. It is easier to attack the default admin account when an attacker only has to guess the password.

Assign the Minimum Required Permissions

When creating a new user account, give that account only the minimum rights to access or modify the system needed for that user.

Use Minimum Possible Number of Admin Users

A compromised admin account can be disastrous as it allows complete access to everything. Only give a user admin privileges only when absolutely necessary.

HTTPS Certificates

HTTPS is a protocol which encrypts HTTP requests and their responses. This ensures that if someone were able to compromise the network, they would not be able to listen in or tamper with the communications.

Make sure that HTTPS is enabled. For more information on how to enable HTTPS, see *Web Server Access*.

Certificates

Generate and install a trusted SSL certificate. Refer to *Web Server Access* for information on how to import a custom certificate.

Additional Measures

Update the Controller's Firmware to the Latest Release

Always keep the ECLYPSE controller's firmware up-to-date. The most recent firmware has the latest bug fixes, security updates, and stability enhancements.

External Factors

Install Controllers in a Secure Location

Ensure that the ECLYPSE controller is installed in a physically secure location, under lock and key. Through physical access, an attacker can take over the controller to do with it what they please.

Make Sure that Controllers are Behind a VPN

For off-site connections, ensure that users access the controllers through a Virtual Private Network (VPN). This helps to prevent an attack through eavesdropping on the communications channel to steal user credentials.

CHAPTER 11
BACnet MS/TP Communication Data Bus Fundamentals

This chapter describes the BACnet MS/TP Communications Data Bus operating principles.

BACnet MS/TP Data Transmission Essentials

Certain ECLYPSE controller models support BACnet MS/TP to BACnet/IP routing according to the controller model purchased. See the Controller's datasheet for more information. To enable BACnet MS/TP to BACnet/IP routing, see *Routing*.

The BACnet MS/TP or Modbus RTU network option is selected in the controller's web interface. BACnet MS/TP and Modbus RTU communications are made by connecting directly to separate RS-485 ports. The Connected System Controller integrates up to three RS-485 ports when equipped with one ECY-RS485 extension module allowing the controller to support more than one trunk or communication protocol at a time. When the ECY Series Controller is configured for BACnet MS/TP, values from the connected BACnet MS/TP controllers can be used in ENVYSION graphics hosted on the ECY Series Controller. Furthermore, the ECY Series Controller acts as a BACnet/IP to BACnet MS/TP bridge that allows BACnet objects to be shared among BACnet intra-networks through BBMD. See *BACnet/IP Broadcast Management Device Service (BBMD)*.

The BACnet MS/TP data bus protocol is part of the BACnet® ANSI/ASHRAE™ Standard 135-2008 that uses the EIA-485 (RS-485) physical layer standard for data transmission (herein called the data bus). Multiple data buses can be logically tied together as each BACnet MS/TP data bus is assigned a unique Network Instance that distinguishes it from other data buses in the BACnet MS/TP Local Area Network (LAN). An example of an interconnected BACnet MS/TP data bus is shown in *Adopting a Numbering System for MAC Addresses, Device Instance Numbers, and Network Numbers*.

EIA-485 is a standard that defines the electrical characteristics of the receivers and drivers to be used to transmit data in a differential (balanced) multipoint data bus that provides high noise immunity with relatively long cable lengths which makes it ideal for use in industrial environments. The transmission medium is inexpensive and readily-available twisted pair shielded cable.

While there are many possible LAN topologies for an EIA-485 data bus, only devices that are daisy-chained together are allowed with BACnet MS/TP (see *Only a Daisy-Chained Data Bus Topology is Acceptable*). A spur is only permitted when it is connected to the data bus through a repeater (see *Using Repeaters to Extend the Data Bus*).

End-of-line (EOL) terminations are critical to error-free EIA-485 data bus operation. The impedance of the cable used for the data bus should be equal to the value of the EOL termination resistors (typically 120 ohms). Cable impedance is usually specified by the cable manufacturer.

BACnet MS/TP Data Bus is Polarity Sensitive

The polarity of all devices that are connected to the two-wire BACnet MS/TP data bus must be respected. The markings to identify the polarity can vary by manufacturer. The following table summarizes the most common identification labels for BACnet MS/TP data bus polarity.

Product	Typical Data Bus Connection Terminals		
	Inverting	Non-inverting	Reference
Distech ECB Series Controllers	NET –	NET +	24V COM
ECB-PTU Series Line-Powered Controllers	NET –	NET +	COM
ECLYPSE Series Controllers	NET –	NET +	S
Thermostat	–	+	Ref
Repeater	Data– Data1–	Data+ Data1+	N/A
BACnet/IP to MS/TP Adapter	RT–	RT+	COM
BACnet/IP to MS/TP Router	–	+	SC

Table 9: Common Identification Labels for BACnet MS/TP Data Bus Polarity for Distech Controls' Products

Except for a Distech ECB-PTU Line-Powered Controllers and ECY Series Controllers, never connect the shield of the BACnet MS/TP data bus to the Reference terminal. See *Data Bus Shield Grounding Requirements*.

Device Manufacturer	Typical Data Bus Connection Terminals		
	Inverting	Non-inverting	Reference
Common identification labels for BACnet MS/TP data bus polarity by other Manufacturers	B	A	SC
	–	+	G
	TxD–/RxD–	TxD+/RxD+	GND
	U–	U+	COM
	RT–	RT+	REF
	Sig–	Sig+	S
	Data–	Data+	

Table 10: Common Identification Labels for BACnet MS/TP Data Bus Polarity for other Manufacturers

When interfacing with BACnet MS/TP devices from other manufacturers, refer to the documentation provided with the device to correctly wire the device.

Maximum Number of BACnet MS/TP Devices on a Data Bus Segment and Baud Rate

The following technical parameters limit the number of devices on a BACnet MS/TP Data Bus Segment.

- The BACnet MS/TP Data Bus Segment has a hard limit on the number of devices that can communicate due to the device addressing scheme (the MAC Address Range for BACnet MS/TP Devices). See *Data Bus Segment MAC Address Range for BACnet MS/TP Devices*.
- Each device presents an electrical load on the BACnet MS/TP Data Bus Segment. This is called device loading. The number of devices that can be connected to a BACnet MS/TP Data Bus Segment is limited by the loading of each device. See *Device Loading*.
- Choosing a low baud rate can cause BACnet MS/TP Data Bus congestion that can limit the amount of data that can be efficiently exchanged between devices connected to the BACnet MS/TP Data Bus. For example, at 9600 baud, the maximum number of devices is reduced to 25 due to the increased time it takes for token passing between devices. The recommended baud rate is 38 400. See *Baud Rate*.
- Distech Controls recommends that you connect no more than 50 of our ⅛ or ½-load devices on a single BACnet MS/TP Data Bus Segment when a baud rate of 19 200 or higher is used (preferably 38 400 baud). This is to ensure that the BACnet MS/TP Data Bus has enough bandwidth to efficiently communicate network variables between controllers.

These parameters are described in greater detail below.

Data Bus Segment MAC Address Range for BACnet MS/TP Devices

The BACnet MS/TP data bus supports up 255 devices:

- Up to 128 devices (with device MAC addresses in the range of 0 to 127) that are BACnet MS/TP Masters (that can initiate communication).
- Up to 128 devices (with device MAC addresses in the range of 128 to 255) that are BACnet MS/TP Slaves (cannot initiate communication).

However, it is recommended that any given data bus segment have no more than 50 devices, when a baud rate of 19 200 or higher is used for the BACnet MS/TP Data Bus. A repeater counts as a device on each data bus segment to which it is connected.

All Distech Controls' devices are categorized as BACnet MS/TP Masters, that is, their device MAC address can be set in the range of 0 to 127 only.

Device Loading

Each device presents an electrical load on the BACnet MS/TP Data Bus Segment. This is called device loading. The use of full load devices limits the number of devices connected to a BACnet MS/TP Data Bus Segment to 32 devices. Distech Controls' BACnet MS/TP devices are ⅛-load devices and ½-load devices, which allows more devices to be connected to the BACnet MS/TP Data Bus Segment, as compared to full load devices.

Manufacturer	Device load on the attached BACnet MS/TP Data Bus
Distech Controls' ECB and ECLYPSE Series controllers Distech Controls' ECB-PTU Series Line-Powered Controllers	⅛-load devices
Distech Controls' BACnet MS/TP Thermostats	½-load devices
Other manufacturers	Refer to their documentation

Table 11: Device Loading

However, if a data bus segment is interoperating with devices that are full-load, ½-load, ¼-load, or ⅛-load, then the device that supports the fewest devices on the same data bus is the one that sets the limit for the maximum total number of devices for that data bus segment. For example, you plan to put on one data bus the following devices:

Manufacturer	Quantity of devices (example)	Equivalent full-load devices	Maximum devices supported by the manufacturer
Distech Controls' devices (⅛-load devices)	8	1	128[1] Maximum 50 recommended
Distech Controls' BACnet MS/TP Thermostats (½-load devices)	14	7	64 Maximum 50 recommended
Manufacturer Y (full load devices)	26	26	32
Total Full-Load Devices		34	There are too many devices on the data bus. It is limited to a maximum of 32 devices by Manufacturer's Y devices.

Table 12: Device Loading Example

1. This is limited by the maximum number of master devices allowed on a BACnet MS/TP Data Bus.

The solution for the above example is to create two data bus segments connected together by a repeater and then split up the devices between the data bus segments, ensuring again that the maximum number of devices on each separate data bus is not exceeded. See *Using Repeaters to Extend the Data Bus*.

Baud Rate

Most devices will have a range of baud rate settings and possibly an AUTO setting that detects the baud rate of other devices transmitting on the data bus and adjusts the baud rate of the device accordingly. Typical baud rates are 9600, 19 200, 38 400, and 76 800. The baud rate setting determines the rate at which data is sent on the BACnet MS/TP data bus.

At 9600 baud, the maximum number of devices is reduced to 25 due to the increased time it takes for token passing between devices.

All devices on the data bus must be set to the same baud rate. Therefore, the chosen baud rate must be supported by all devices connected to the data bus.

The recommended baud rate for Distech Controls' devices is 38 400.

We recommend that you:

- Set the baud rate of two controllers on a BACnet MS/TP Data Bus Segment to the same baud rate to provide failover protection.
- For example, set the baud rate of the ECY Series Controller (if equipped) and one other controller to 38 400 baud. If the ECY Series Controller becomes unavailable and there is a power cycle, the ECB controller will set the baud rate for the BACnet MS/TP Data Bus.
- Set all other devices to automatically detect the baud rate, if this option is available.

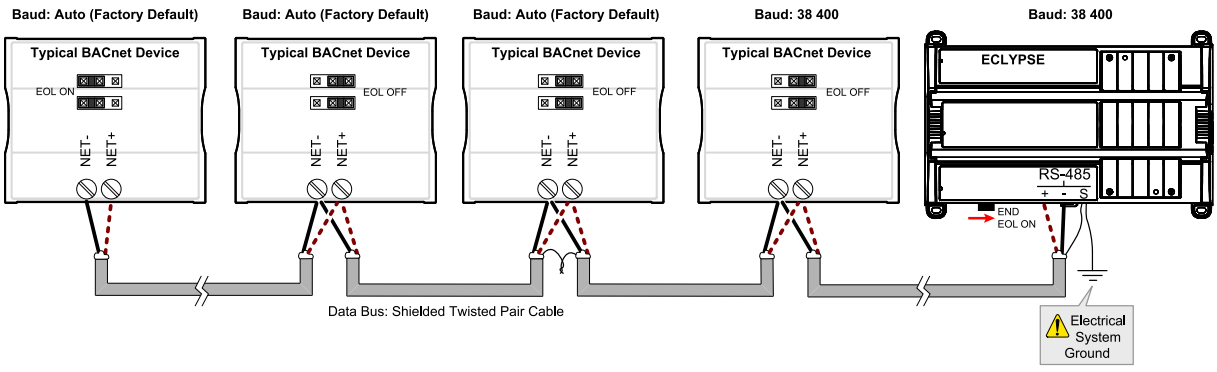


Figure 90: Setting the Baud rate on two Controllers on a BACnet MS/TP Data Bus Segment for Failover Protection

To set the baud rate for:

- ECLYPSE Series Controllers, see *Network MS/TP Ports*.
- ECB Series controllers, see the controller's hardware installation guide or the Network Guide.

Data Bus Physical Specifications and Cable Requirements

Cables composed of stranded conductors are preferred over solid conductors as stranded conductor cable better resist breakage during pulling operations. Distech Controls strongly recommends that the following data bus segment cable specifications be respected.

Parameter	Details
Media	Twisted pair, 24 AWG
Shielding	Foil or braided shield
Shield grounding	The shield on each segment is connected to the electrical system ground at one point only; see *Data Bus Shield Grounding Requirements*.
Characteristic impedance	100-130 Ohms. The ideal is 100-120 Ohms.
Distributed capacitance between conductors	Less than 100 pF per meter (30 pF per foot). The ideal is less than 60 pF per meter (18 pF per foot).
Distributed capacitance between conductors and shield	Less than 200 pF per meter (60 pF per foot).
Maximum length per segment	1220 meters (4000 feet)
Data Rate	9600, 19 200, 38 400, and 76 800 baud
Polarity	Polarity sensitive
Multi-drop	Daisy-chain (no T-connections)
EOL terminations	120 ohms at each end of each segment
Data bus bias resistors	When VCC=5V: 510 ohms per wire (max. of two sets per segment) When VCC=3.3V (The APEX is 3.3V internal): 330 ohms per wire

Table 13: BACnet MS/TP Data Bus Segment Physical Specifications and Cable Requirements

Shielded cable offers better overall electrical noise immunity than non-shielded cable. Unshielded cable or cable of a different gauge may provide acceptable performance for shorter data bus segments in environments with low ambient noise.

Cable Type	Part Number	O.D. (Ø)
300 meters (1000 feet), 24 AWG Stranded, Twisted Pair Shielded Cable – FT6, Rated for Plenum Applications	CB-BACN6BL1000	3.75mm (0.148 in.)

Table 14: Distech Controls Recommended Cable Types for BACnet MS/TP Data Buses

Distech Controls BACnet cable offers the best performance over the full range of baud rates, cable lengths, and number of connected devices. This is primarily due to lower conductor-to-conductor capacitance of this cable.

Data Bus Topology and EOL Terminations

Function of EOL Terminations

The first and last device on the data bus must have End-of-Line (EOL) termination resistors connected across the two data lines/wires of the twisted pair. These resistors serve the following purposes:

- EOL terminations dampen reflections on the data bus that result from fast-switching (high-speed rising and falling data edges) that otherwise would cause multiple data edges to be seen on the data bus with the ensuing data corruption that may result. The higher the baud rate a data bus is operating at, the more important that EOL terminations be properly implemented. Electrically, EOL terminations dampen reflections by matching the impedance to that of a typical twisted pair cable.

- EIA-485 data bus transmitters are tri-state devices. That is they can electrically transmit 1, 0, and an idle state. When the transmitter is in the idle state, it is effectively off-line or disconnected from the data bus. EOL terminations serve to bias (pull-down and pull-up) each data line/wire when the lines are not being driven by any device. When an un-driven data bus is properly biased by the EOL terminations to known voltages, this provides increased noise immunity on the data bus by reducing the likelihood that induced electrical noise on the data bus is interpreted as actual data.

When to Use EOL Terminations

EOL terminations should only be enabled / installed on the two devices located at either end of the data bus. All other devices must not have the EOL terminations enabled/installed.

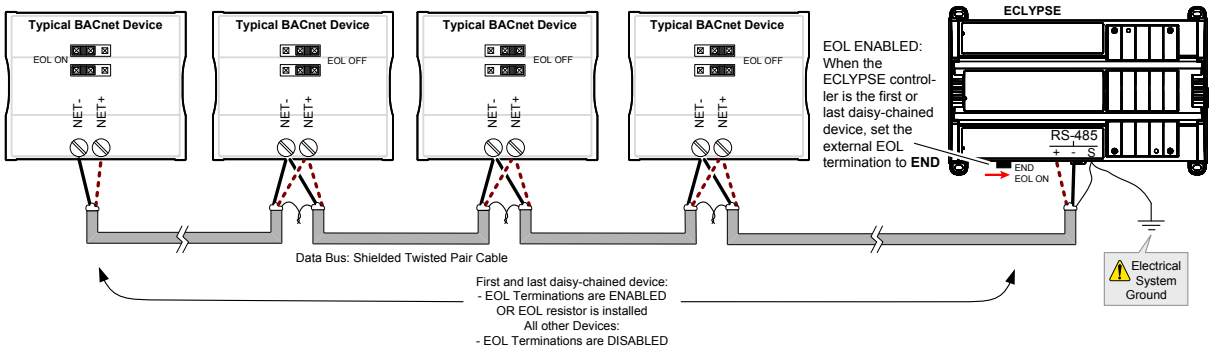


Figure 91: EOL Terminations Must be Enabled at Both the First and Last Device on the Data Bus

Devices with built-in EOL terminations are factory-set with the EOL termination disabled by default.

The BACnet/IP to MS/TP Adapter does not have EOL Termination (and BACnet MS/TP Data Bus biasing) capabilities to be used at the end of a BACnet MS/TP data bus. Instead, use the BACnet/IP to MS/TP Router for this application.

When to use EOL Terminations with BACnet MS/TP Thermostats

BACnet MS/TP thermostats support external EOL termination resistors only. When a BACnet MS/TP thermostat is the first or last daisy-chained device, add a 120 Ohm resistor across the – and + BACnet MS/TP data bus connections.

The BACnet MS/TP data bus must be biased. This bias can only be provided by built-in EOL termination resistors (ones set with jumpers or DIP switches – refer to the controller's Hardware Installation Guide for how to identify and set a controller's built-in EOL terminations). If a BACnet MS/TP data bus has a BACnet MS/TP thermostat at one end of the BACnet MS/TP data bus and an ECY Series Controller at the other end, you must set the built-in EOL termination in the controller so that proper biasing is provided to the BACnet MS/TP data bus.

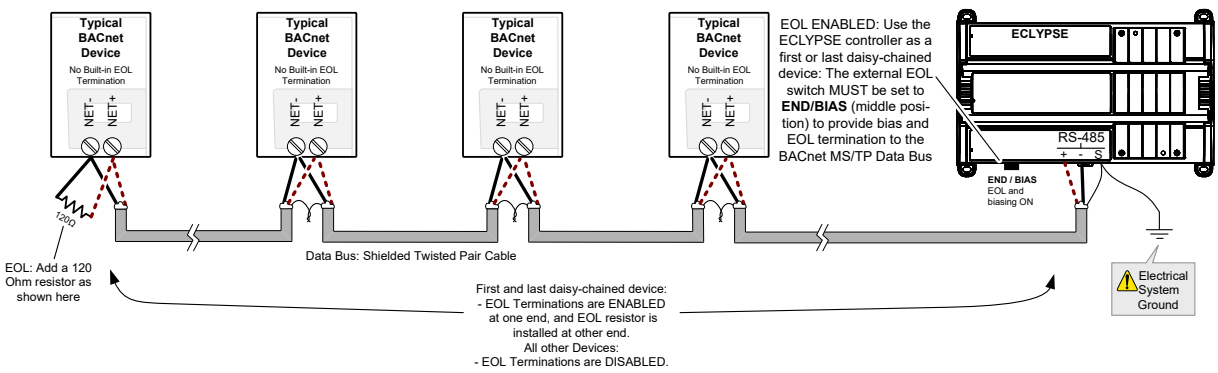


Figure 92: Typical EOL Terminations with BACnet MSTP Thermostats with Biasing Provided by the Controller's Built-in EOL Termination set to ON

About Setting Built-in EOL Terminations

The APEX has built-in EOL terminations and biasing. It uses a switch located on the bottom of the controller to enable the EOL termination and/or bias based on where it is located on a data bus (usually at the end).

- If the APEX is located at the end of a data bus, set the switch to position to “END”.
- If the APEX is located at the end of a data bus and the data bus requires biasing, set the switch position to “END / BIAS”. There should be a minimum of one device (maximum of two) with biasing on the data bus.
- If the APEX is located at the middle of a data bus, set the switch position to “MID”. The controllers located at the ends of the data bus must have their EOL terminations installed or enabled.

If a controller at the end of the data bus does not have a built-in EOL termination, then add a 120 Ohm resistor across the device’s terminals as shown at the left side of the previous figure.

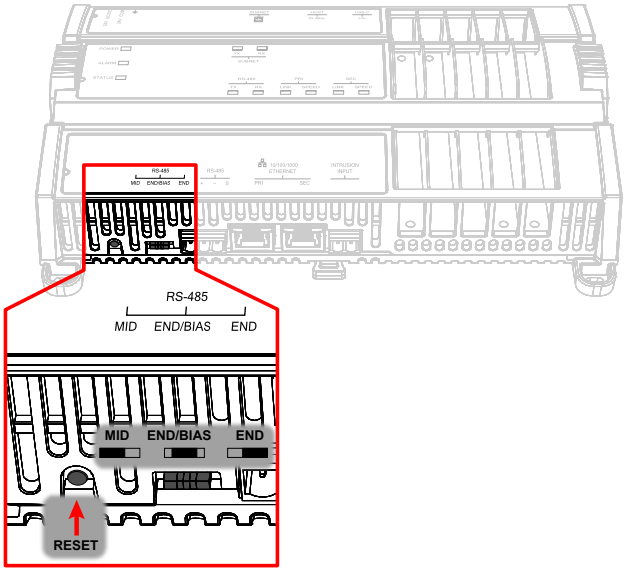


Figure 93: APEX EOL switch and reset button

ECB-PTU Series Line-Powered Controllers use DIP switches (found alongside those DIP switches used to set the MAC address) to enable the build-in EOL resistors and biasing circuitry.

ECB Series 24V-Powered Controllers have built-in EOL terminations. These Controllers use jumpers to enable the EOL resistors and biasing circuitry.

Refer to the controller’s Installation Guide for how to identify and set a controller’s built-in EOL terminations.

Only a Daisy-Chained Data Bus Topology is Acceptable

Use a daisy-chained BACnet MS/TP data bus topology only. No other data bus topology is allowed.

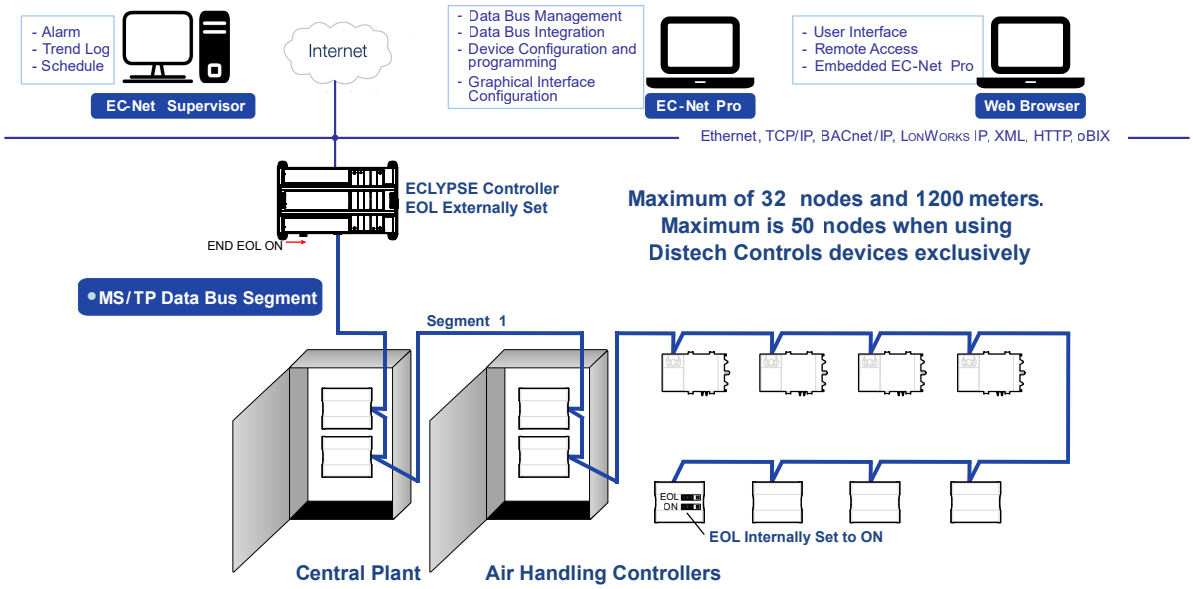


Figure 94: Typical BACnet MS/TP LAN Topology Showing How Devices are Daisy-Chained Together to Form One Data Bus Segment

Only linear, daisy-chained devices provide predictable data bus impedances required for reliable data bus operation.

Only a daisy-chained data bus topology should be specified during the planning stages of a project and implemented in the installation phase of the project.

A spur is only permitted when it is connected to the data bus through a repeater (see *Using Repeaters to Extend the Data Bus*).

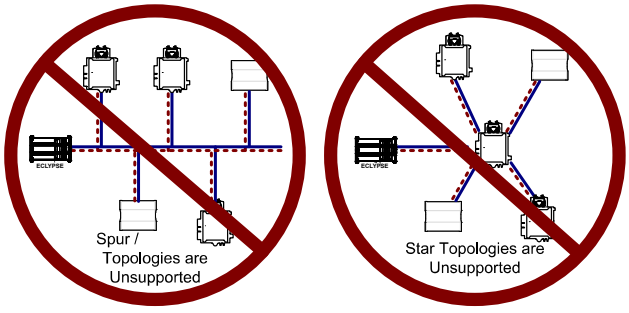


Figure 95: Unsupported BACnet MS/TP LAN Topologies

Data Bus Shield Grounding Requirements

The EIA-485 data bus standard requires that the data bus must be shielded against interference. A BACnet MS/TP data bus must also be properly grounded.

For ECB Series 24V-Powered Controllers:

The data bus' cable shields must be twisted together and isolated with electrical tape at each device. Note that for ECB 24V-Powered Controllers, the power supply transformer's secondary that is connected to the 24V COM terminal is grounded. This provides the ground reference for the data bus (see *BACnet MS/TP is a Three-Wire Data Bus*). If the controller is at the end of the BACnet MS/TP data bus, simply isolate the data bus shield with electrical tape.

For ECB-PTU Series Line-Powered Controllers:

The data bus' cable shields must be twisted together and connected to the **COM** terminal at each ECB-PTU Line-Powered Controller. Keep the cable shield connections short and take steps at each device to isolate the cable shield from touching any metal surface by wrapping them with electrical tape, for example. Note that for ECB-PTU Line-Powered Controllers, the data bus' cable shield provides the ground reference for the data bus (see *BACnet MS/TP is a Three-Wire Data Bus*). If the controller is at the end of the BACnet MS/TP data bus, simply connect the data bus shield to the **COM** terminal.

ECLYPSE Series Controller:

The data bus' cable shields must be twisted together and connected to the **S** terminal at each ECLYPSE Series Controller. Keep the cable shield connections short and take steps at each device to isolate the cable shield from touching any metal surface by wrapping them with electrical tape, for example. Note that for ECLYPSE Series Controllers, the data bus' cable shield provides the ground reference for the data bus (see *BACnet MS/TP is a Three-Wire Data Bus*). If the controller is at the end of the BACnet MS/TP data bus, simply connect the data bus shield to the **S** terminal.

The APEX controller has a GND terminal that must be connected to 24V COM (2-wire) or directly to ground (3-wire) to ensure a functional RS485 data bus (see *Power Wiring with APEX*)

Grounding the shield of a data bus segment in more than one place will more than likely reduce shielding effectiveness.

ECB 24V-Powered Controller Data Bus Shield Grounding Requirements

The shield on each data bus segment must be connected to the electrical system ground at one point only, for example, at the ECLYPSE Series Controller, as shown in the figures below.

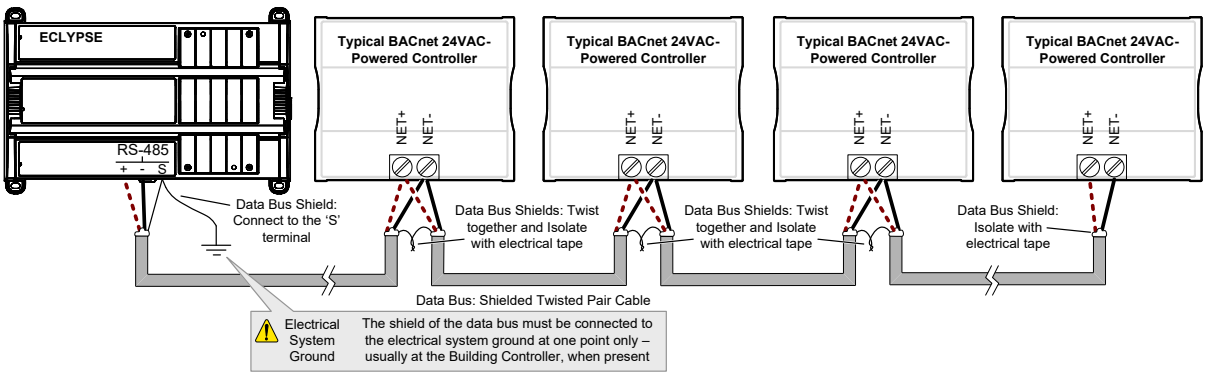


Figure 96: Typical Cable-Shield Grounding Requirements for a BACnet MS/TP Data Bus Segment with an ECY Series Controller located at the End of the Data Bus

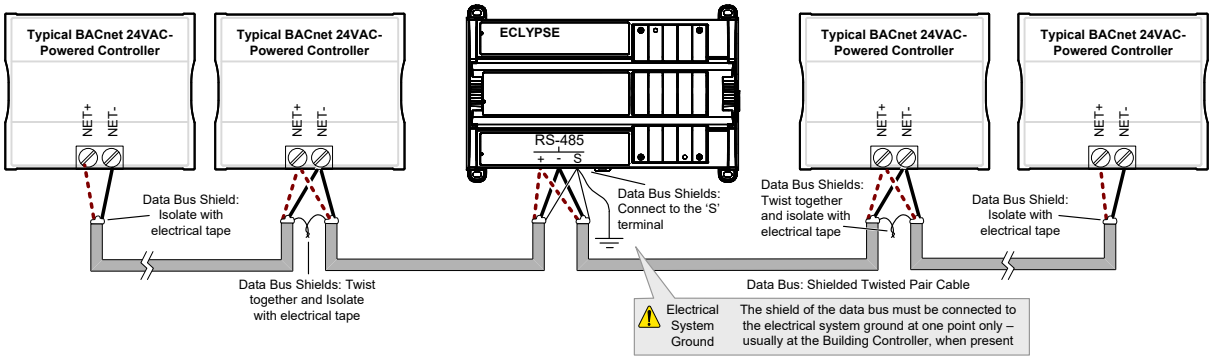


Figure 97: Typical Cable-Shield Grounding Requirements for a BACnet MS/TP Data Bus Segment with an ECY Series Controller located in the Middle of the Data Bus

ECB-PTU Line-Powered Data Bus Controller Shield Grounding Requirements

The shield on each data bus segment must be connected to the electrical system ground at one point only, for example, at the ECY Series controller, as shown in the figures below.

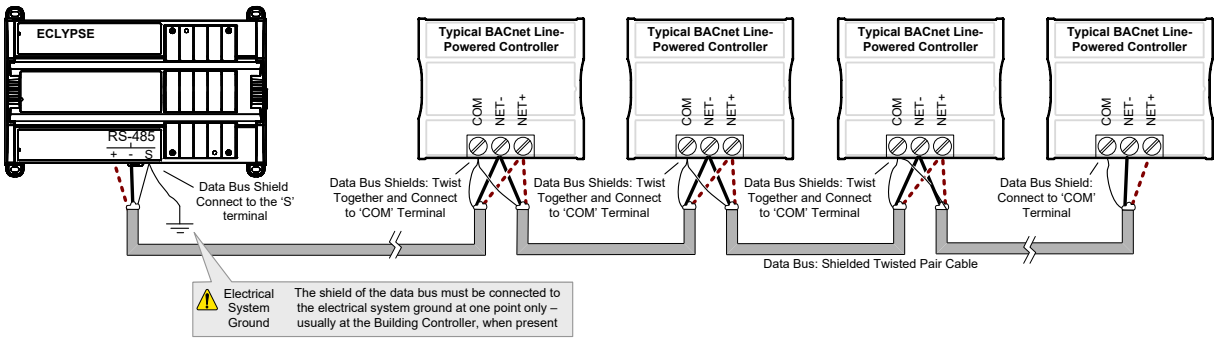


Figure 98: Typical Cable-Shield Grounding Requirements for a BACnet MS/TP Data Bus Segment with an ECY Series Controller located in the End of the Data Bus

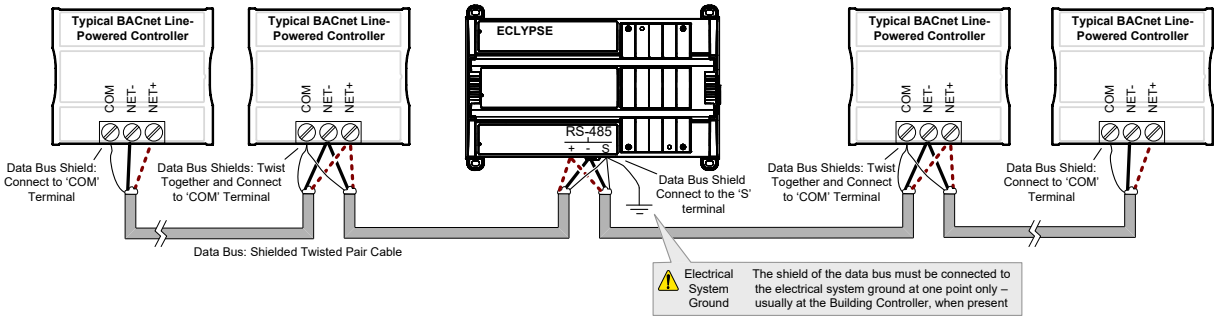


Figure 99: Typical Cable-Shield Grounding Requirements for a BACnet MS/TP Data Bus Segment with an ECY Series Controller located in the Middle of the Data Bus

Data Bus Shield Grounding Requirements When Mixing Both ECB 24V-Powered Controllers and ECB-PTU Line-Powered Controllers

The shield on each data bus segment must be connected to the electrical system ground at one point only, for example, at the ECY Series controller, as shown in the figures below.

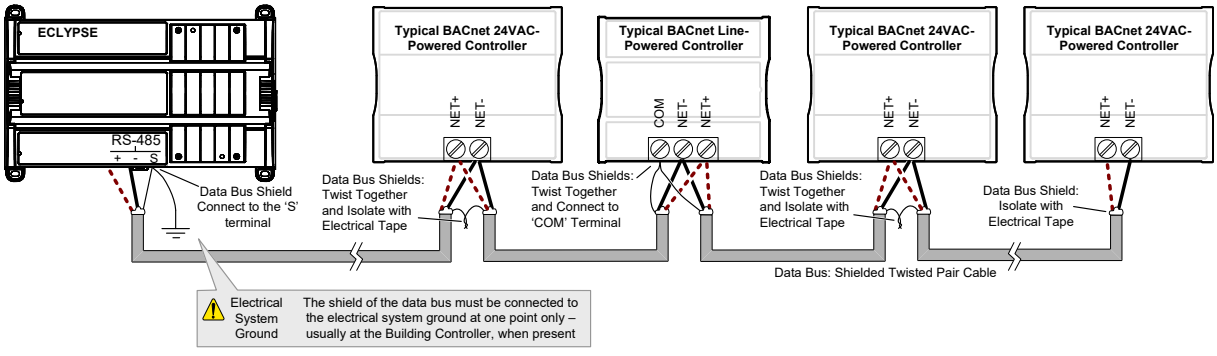


Figure 100: Typical Cable-Shield Grounding Requirements for a BACnet MS/TP Data Bus Segment with an ECY Series Controller located in the End of the Data Bus

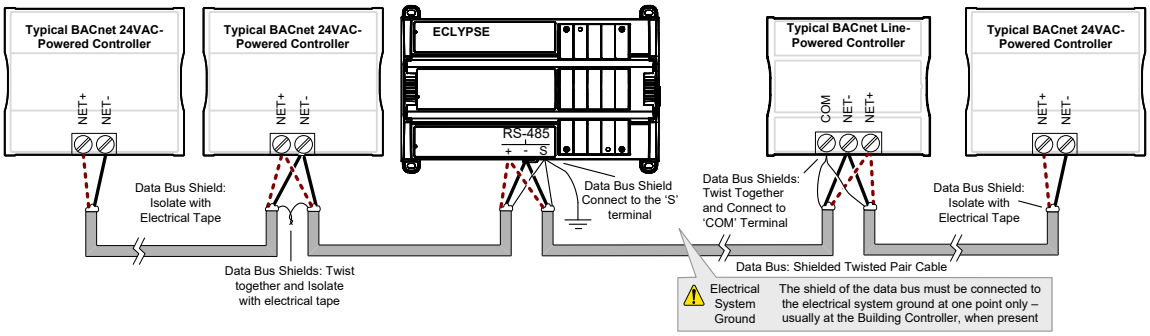


Figure 101: Typical Cable-Shield Grounding Requirements for a BACnet MS/TP Data Bus Segment with an ECY Series Controller located in the Middle of the Data Bus

Using Repeaters to Extend the Data Bus

A BACnet MS/TP data bus segment can be up to 1220 meters (4000 feet) long with up to a maximum of 50 devices. When a greater length is required, a solution is to use a repeater. A repeater increases the maximum length of the data bus.

Using a Repeater to Extend the Length of the BACnet MS/TP Data Bus

Repeaters can be used to extend a BACnet MS/TP data bus up to 3660 meters maximum total length. Do not use more than two repeaters on a BACnet MS/TP LAN.

A BACnet MS/TP repeater is a bi-directional device that regenerates and strengthens the electrical signals that pass through it. It creates two electrically-isolated BACnet MS/TP data bus segments that transparently enable devices on one side of the repeater to communicate with any device on the other side. The two BACnet MS/TP data bus segments have the same requirements of an ordinary BACnet MS/TP data bus segment; that is, each BACnet MS/TP data bus segment:

- Can be up to 1220 meters (4000 feet) long.
- The first and last device on the data bus must have End-of-Line (EOL) termination resistors connected across the two data lines/wires of the twisted pair.
- Must respect the maximum limit for *Device Loading*.
- Will have the same network number as they remain part of the same network or LAN.

It is recommended that you connect no more than 50 of our ⅛ or ½-load devices on all BACnet MS/TP Data Bus repeater segments when a baud rate of 19 200 or higher is used (preferably 38 400 baud). This is to ensure that the BACnet MS/TP Data Bus has enough bandwidth to efficiently communicate network variables between controllers.

Do not use more than two repeaters on a BACnet MS/TP data bus.

A repeater can only connect two BACnet MS/TP data bus segments even if it has ports to support more than two BACnet MS/TP data bus segments.

A repeater can be added anywhere to a data bus segment including the end of the segment as shown below.

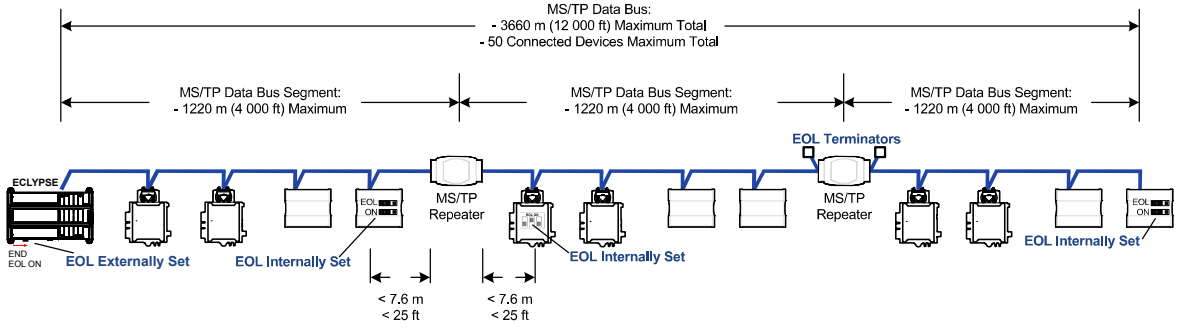


Figure 102: Using a Repeater to Extend the Range of the LAN

A repeater can be used to create a spur as shown below.

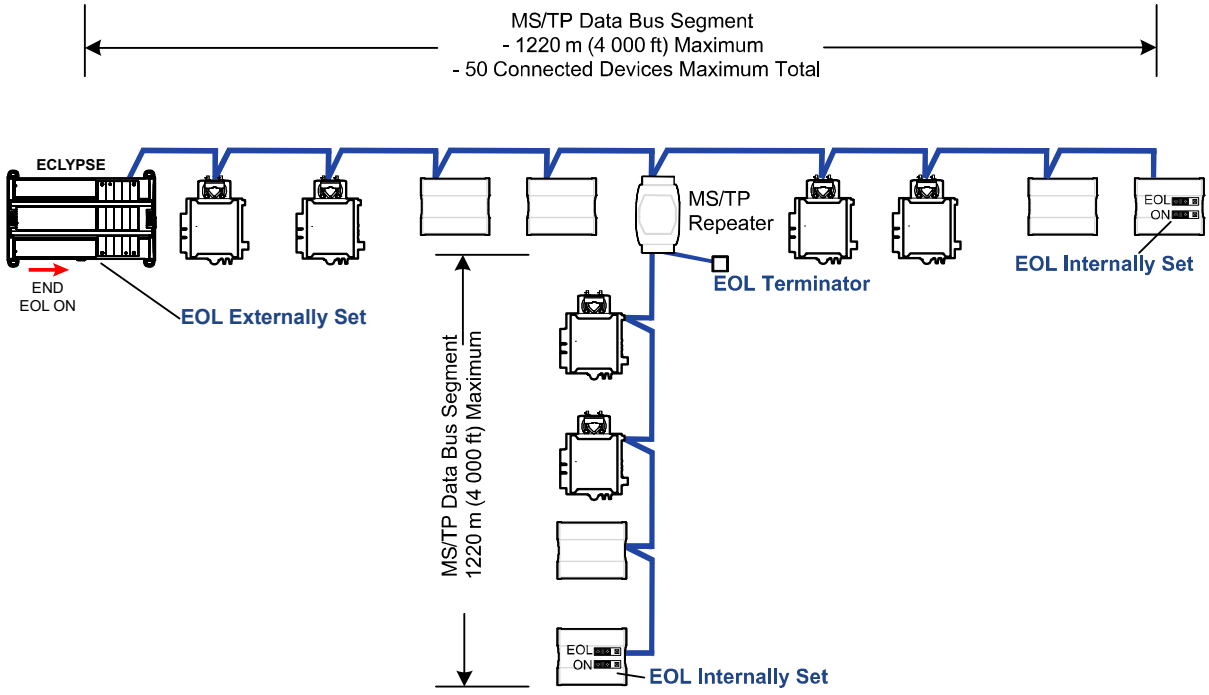


Figure 103: Adding a Spur by Using a Repeater

A repeater is counted as a device on each data bus to which it is connected.

When third party devices are connected to a data bus segment, the number of devices that can be connected to that data bus segment may be reduced. See *Device Loading*.

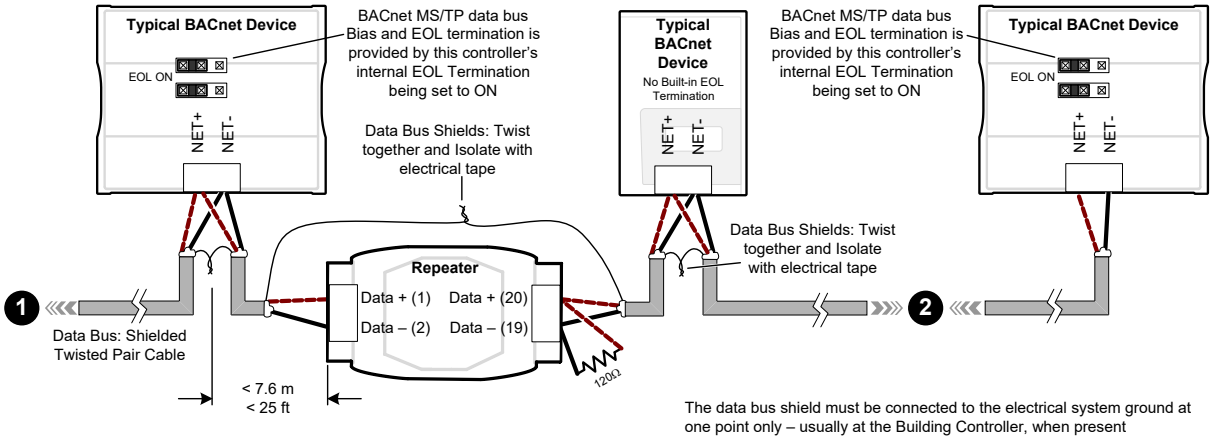


Figure 104: Repeater Connections when it is the First or Last Device on its Respective Data Bus Segment

The BACnet MS/TP Data Bus must be biased. This bias can only be provided by built-in EOL termination resistors (ones set with a jumper or DIP switch). When a repeater is the first or last device on its respective data bus segment, use the following methods to provide MS/TP Data Bus biasing and EOL termination as applicable to your situation:

1. On the BACnet MS/TP data bus segment □ shown in the above figure, bias and EOL termination is provided by a controller's built-in EOL termination being set to ON. In this case the connection to the repeater cannot be more than 7.6 meters (25 feet) from this controller.
2. On the BACnet MS/TP data bus segment □ shown in the above figure, a 120Ω EOL Termination resistor is added to the repeater's terminals. Biasing for this BACnet MS/TP data bus segment is provided by the built-in EOL termination being set to ON at the last controller at the other end of this data bus.

See *When to Use EOL Terminations* for more information. The shield of one data bus must be grounded at one point as specified in *Data Bus Shield Grounding Requirements*. The shields of the two data buses must be connected together and isolated with electrical tape as shown in the above figure. Refer to the controller's Hardware Installation Guide for how to identify and set a controller's built-in EOL terminations.

Device Addressing

Device addressing allows the coordinated transfer of messages between the intended devices on the BACnet MS/TP data bus and with devices connected to the internetwork. For this, each device connected to the BACnet MS/TP data bus is identified by a MAC address, a Device Instance number, and a Network Number:

- The MAC Address uniquely identifies a device on a Network (identified by a Network Number). Devices on another Network can have the same MAC Address as messages are not passed at the internetwork level using the MAC Address. The MAC Address also defines the devices on the data bus that are Masters and Slaves, among other categories (see *About the MAC Address*). The MAC Address is also used to share data bus bandwidth between devices through token passing between Master devices.
- The Device Instance uniquely identifies a device across the BACnet internetwork. The Device Instance is any number between 0 and 4 194 303. It is with the Device Instance that messages are exchanged between BACnet devices. The Device Instance is also used by routers to forward messages to devices located elsewhere in the internetwork. Unlike a MAC Address, a Device Instance cannot be reused elsewhere in the BACnet internetwork (it must be unique for the entire network).
- The Network Number is any number between 1 and 65 534. A network number identifies a LAN for routing purposes.

Both the MAC Address and the Device Instance must be set for each device and are essential for proper BACnet LAN operation.

For an example of how MAC address, Device Instance number, and Network Number apply to a typical BACnet network, see *Adopting a Numbering System for MAC Addresses, Device Instance Numbers, and Network Numbers*.

About the MAC Address

The MAC Address is a number from 0 to 255; however, we recommend reserving some MAC Addresses for common commissioning and maintenance tasks. For example, when a portable adapter is set to use one of these reserved MAC Addresses, it can be temporarily connected with certainty to any BACnet MS/TP data bus of any site without conflicting with other devices already connected to the BACnet MS/TP data bus. We strongly recommend that the MAC address of ECY Series Controller's MS/TP port be always set to 0.

MAC Addresses should be used as shown in the following table.

MAC Address Value / Range	Usage	Devices
0	Data Bus Master (ECY Series Controller)	This address is invalid for Distech Controls' ECB series devices
1	Temporary commissioning connection	This address is invalid for Distech Controls' ECB series devices
2	Reserved	Other
3-127	Master Range	Master devices: All Distech Controls' devices are master devices and should be in this MAC Address range
128-254	Slave Range	Slave devices and network sensors
255	Broadcast	Do not apply address 255 to any device

Table 15: Recommended BACnet MS/TP Bus MAC Address Values / Ranges for BACnet MS/TP Data Bus Devices

BACnet MS/TP Data Bus Token-Passing Overview

The BACnet MS/TP data bus protocol is a peer-to-peer, multiple-master protocol that shares data bus bandwidth by passing a token between Master devices on the data bus that authorizes the device that is holding the token to initiate communications on the data bus. Once the device has completed its request(s), it closes the communications channel, passes the token to the next Master device (making it the current Master), and liberates the data bus.

The token is passed through a short message from device to device on the BACnet MS/TP data bus in consecutive order starting from the lowest MAC address (MAC Address = 0) to the next MAC Address.

Gaps or pockets of unassigned device MAC Addresses should be avoided as this reduces data bus performance. Once a master has finished making its requests, it must poll for the next master that may exist on the Data Bus. It is the timeout for each unassigned MAC Address that slows down the data bus.

The way MAC Addresses are assigned is not a physical requirement: Devices can be daisy-chained on the data bus in any physical order regardless of their MAC Address sequence. The goal is to avoid gaps in the device MAC Address range.

Slave devices cannot accept the token, and therefore can never initiate communications. A Slave can only communicate on the data bus to respond to a data request addressed to it from a Master device. Gaps in slave device MAC Addressing have no impact on BACnet MS/TP data bus performance.

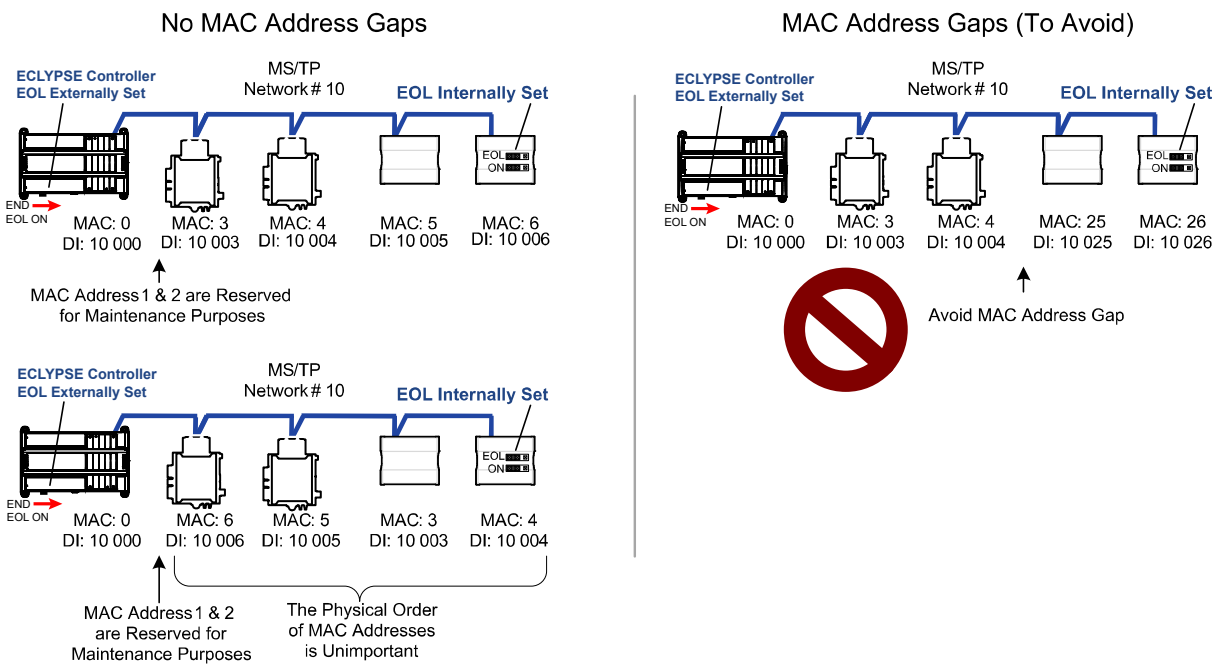


Figure 105: Setting the Max Master on the ECY Series Controller to the Highest MAC Address Used on the BACnet MS/TP Data Bus

About Tuning the Max Info Frames Parameter

Once a device has the token, it can make a number of information requests to other devices on the BACnet intranetwork. The maximum number of requests is limited by the **Max Info Frames** parameter. Once the device has made the maximum number of requests it is permitted to make according to the **Max Info Frames** parameter, the device passes the token to the following device with the next higher MAC address. This makes the BACnet MS/TP Data Bus more reactive for all devices by preventing a device from hanging on to the token for too long. Ordinary BACnet MS/TP devices should have the **Max Info Frames** parameter set to between 2 and 4. The Data Bus Master (ECY Series Controller) should have the **Max Info Frames** parameter set to 20.

About Tuning the Max Master Parameter

To prevent the passing of the token to unused MAC Addresses situated after the final Master device, the Max Master parameter must be set. By default, the Max Master for an ECY Series Controller or a Supervisor is set to 127 which allows for the theoretical maximum of 127 devices besides the Data Bus Master to be connected to the data bus.

In practice, the actual number of devices connected to a data bus is far less, resulting in a gap between the highest MAC Address of any device connected to the data bus and the value set for Max Master. This gap unnecessarily slows-down the data bus with Poll for Master requests.

When commissioning a BACnet MS/TP Data Bus, it is useful to start with the Max Master set to 127 so as to be able to discover all devices connected to the data bus. Then, once all devices have been discovered and the MAC Addressing is finalized by eliminating any gaps in the address range, set the **Max Master** (maximum MAC Address) in the ECY Series Controller and in the Supervisor to the highest Master device's MAC Address number to optimize the efficiency of the data bus.

Setting the Max Master and Max Info Frames

The **Max Master** and **Max Info Frames** are parameters used to optimize a BACnet MS/TP Data Bus. This is set in the ECY Series Controller and separately with the Supervisor for each connected BACnet MS/TP device.

For the ECY Series Controller, set the **Max Info Frames** to 20 in the screen shown in BACnet Settings of the *Network MS/TP Ports* as this is a device that will make more requests for service from other devices on the network. In general, according to the way a device is programmed, the **Max Info Frames** may have to be set to a higher value than for other devices. For example, when Roof Top Unit Controllers are used with VAV controllers that use *gfx*Applications code, they should also have their Max Info Frames set to a higher value such as 5, as Roof Top Unit Controllers will poll many VAV controllers for information.

To set the **Max Master** and **Max Info Frames** for BACnet MS/TP devices (for example, an ECB series controller), use a Supervisor to do so. See the Network User Guide for more information.

Default Device Instance Number Numbering System for Distech Controls' Controllers

By default, controllers from Distech Controls automatically self-assign a Device Instance number generated from the unique MAC Address assigned to the controller during installation. The Device Instance number is calculated as follows:

Device Instance number = 364 X 1000 + MAC Address

Where 364 is Distech Controls unique BACnet Manufacturer ID.

This Numbering system is sufficient for a BACnet network that has only one ECY Series Controller. For larger BACnet networks that have more than one controller (to form a BACnet intranetwork), set the MAC Addresses, Device Instance Numbers and Network Numbers according to the numbering scheme below.

Adopting a Numbering System for MAC Addresses, Device Instance Numbers, and Network Numbers

Good network planning requires a well-thought-out numbering scheme for device MAC Addresses, Device Instance Numbers (DI), and Network Numbers. We recommend the following scheme, as it reuses the MAC Address and Network Number in the Device Instance number to make it easier for a network administrator to know where a device is located in the network. This is shown below.

Description	Range	Example
BACnet/IP Network Number	0 to 65 534	1
ECLYPSE Controller BACnet/IP Device Instance Numbers: Multiples of 10 000	10 000 to 4 190 000	10 000 20 000
BACnet MS/TP Network Number: ECY Series Controller BACnet/IP Device Instance Number/1000 + 0,1,2,3,4 (for each LAN)	10 to 4190	10 20 30
BACnet MS/TP Device Instance Number =	10 000 to 4 190 256	10 006 where MAC = 6

Table 16: Recommended Numbering Scheme for MAC Addresses, Instance Numbers, and Network Numbers

An example of this numbering system is shown below.

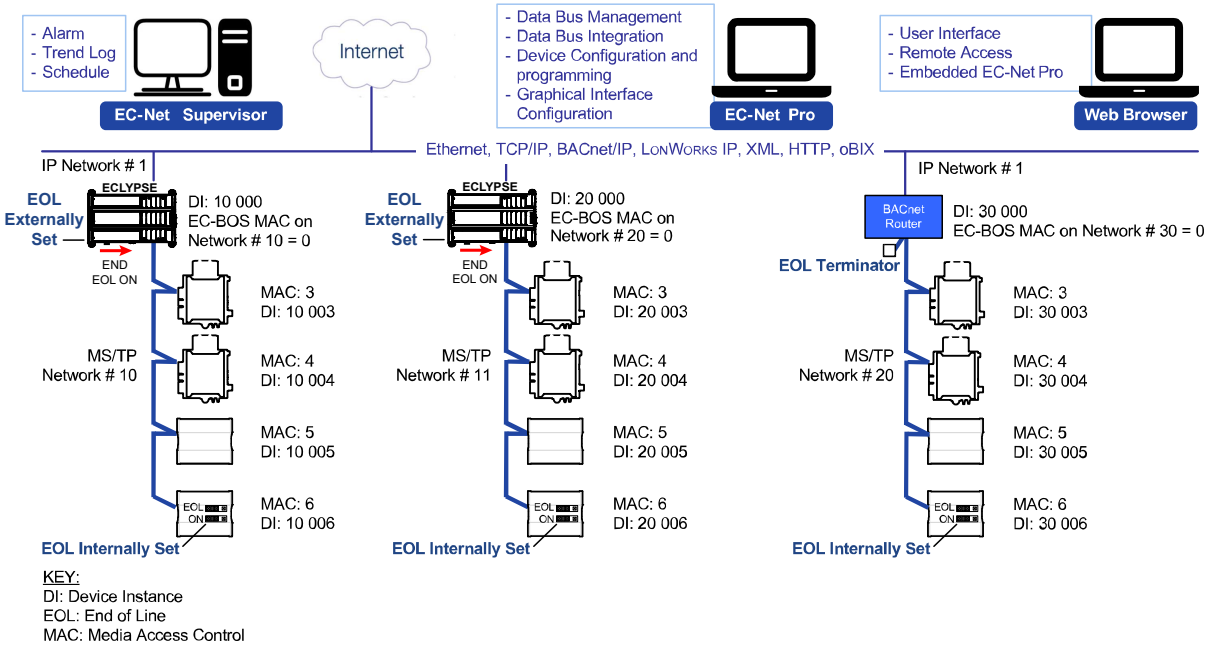


Figure 106: BACnet MS/TP Numbering System for MAC Addresses, Device Instance Numbers, and Network Numbers

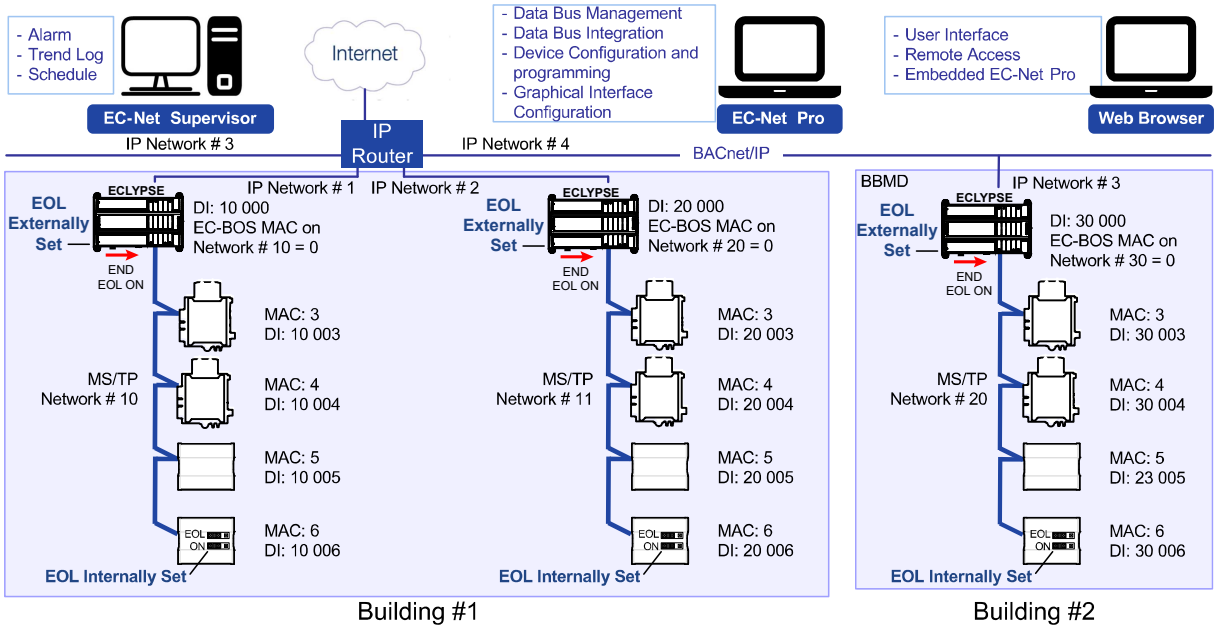
When discovering devices with EC-Net which has the routing option configured, it will discover all BACnet devices connected to all ECY Series Controllers when routing is enabled (see *Routing*). Make sure to add only the devices connected to the MS/TP port of the specific ECY Series Controller being configured. Using this numbering system will greatly help to identify those devices that should be added to a given ECY Series Controller.

Setting the Controller's MAC Address

The ECY Series Controller's MAC address can be set in BACnet Settings of the *ECLYPSE Web Interface*.

Inter-Building BACnet Connection

BACnet network connections between buildings must be made using BACnet/IP as shown below.



KEY:
DI: Device Instance
EOL: End of Line
MAC: Media Access Control

Figure 107: Typical Inter-Building Connection Using BACnet/IP or FOX

BACnet/IP Broadcast Management Device Service (BBMD)

Though BACnet/IP uses IP protocol to communicate, a standard IP router does not forward broadcast messages which are important in BACnet to identify services that are available within the BACnet internetwork.

When two ECY Series Controllers communicate to each other over a standard IP connection that is separated by an IP router, both controllers need the BACnet/IP Broadcast Management Device (BBMD) service to be configured and operational.

The BBMD service identifies BACnet messages on the BACnet MS/TP network that are intended for a device located on another BACnet network. The BBMD service encapsulates these messages into an IP message to the appropriate BBMD service of the other BACnet MS/TP network(s). The BBMD service on these networks strips out the encapsulation and sends the BACnet message on to the appropriate devices.

When sending BACnet messages across a standard IP connection that has an IP router, there must be one BBMD service running on each BACnet MS/TP network.

Power Supply Requirements for 24VAC-Powered Controllers

BACnet MS/TP is a Three-Wire Data Bus

Even though data is transmitted over a 2-wire twisted pair, all EIA-485 transceivers interpret the voltage levels of the transmitted differential signals with respect to a third voltage reference common to all devices connected to the data bus (signal reference). In practice, this common signal reference is provided by the building's electrical system grounding wires that are required by electrical safety codes worldwide. Without this signal reference, transceivers may interpret the voltage levels of the differential data signals incorrectly, and this may result in data transmission errors.

ECY-PS100-240 Power Supply is a double-insulated device and therefore is not grounded. The reference for the BACnet MS/TP data bus is made by connecting the shield of the BACnet MS/TP data bus to the ECLYPSE Controller's S terminal to provide a signal reference. This shield is grounded at one point only – see *Data Bus Shield Grounding Requirements*.

Avoid Ground Lift

24V Power wiring runs should not be too long, nor have too many devices connected to it. Wiring used to supply power to devices has a resistance that is proportional to the length of the wiring run (See the table below).

AWG	Diameter		Area		Copper wire resistance	
	Range	(mm)	(kcmil)	(mm²)	(Ω/km)	(Ω/1000 ft.)
14	0.0641	1.628	4.11	2.08	8.286	2.525
16	0.0508	1.291	2.58	1.31	13.17	4.016
18	0.0403	1.024	1.62	0.823	20.95	6.385

Table 17: Resistance of Common Copper Wire Sizes

If the power run from the power supply is relatively long and it supplies power to many devices, a voltage will develop over the length of wire. For example, a 1000 ft. of 18 AWG copper wire has a resistance of 6.4 Ohms. If this wire is supplying 1 Ampere of current to connected devices (See the figure below), the voltage developed across it will be 6.4 volts. This effect is called ground lift.

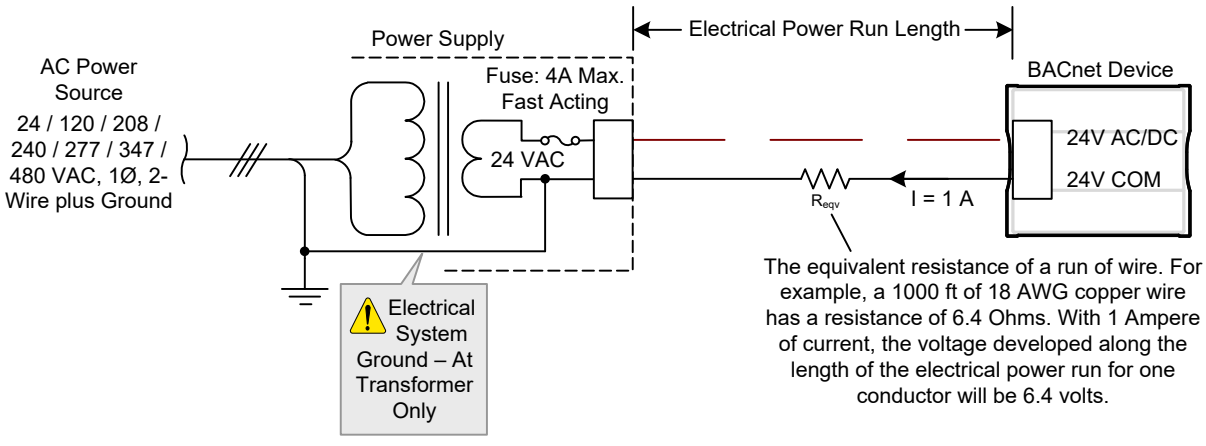


Figure 108: Ground Lift from a Long Power Run with a 24VAC Device

Because the 24V COM terminal on ECB series controllers is the signal reference point for the data bus, ground lift offsets the data bus voltage reference that is used to interpret valid data levels sent on the data bus. If the ground lift is more than 7 volts peak, there is a risk of data corruption and offline events due to the device being incapable of correctly reading data signals from the data bus. **Thus, it is important to keep the power supply (transformer) as close to the controller as possible or use a power connection of 3 wire when possible.**

Techniques to Reduce Ground Lift

Reduce the impact of ground lift as follows:

- Use a heavier gauge wire.
- Add more wire runs. Connect these wire runs to the power supply in a star pattern.
- For controllers that accept DC power (that is, models without triac outputs): Specify a 24VDC power supply. The continuous and even voltage of a DC power supply makes more efficient use of the power handling capabilities of a power run. A 24VDC power supply eliminates the 2.5 multiplication factor associated with the peak AC current being 2.5 times the average RMS AC current. See below.
- The functional ground terminal available on some controller is intended to eliminate the ground lift (when using the 3 wires connection)

About External Loads

When calculating a controller's power consumption to size the 24VAC transformer, you must also add the external loads the controller is going to supply, including the power consumption of any connected subnet module (for example, for Allure series communicating sensors). Refer to the respective module's datasheet for related power consumption information.

A controller can support a maximum of two Allure series sensor models equipped with a CO_2 sensor. See *Subnetwork Module Compatibility and Supported Quantity Charts* for how many Allure series communicating sensors are supported by a given controller model. The remaining connected Allure series sensor models must be without a CO_2 sensor.

Transformer Selection and Determining the Maximum Power Run Length

To determine the power requirements and supported quantities of connected subnet modules for the ECY Series controllers, see the Product Selection Tool available in Builder: https://builder.distech-controls.com.

Please refer to the corresponding controller's Installation Guide for specific information on power wiring.

Recommended 24V Power Cable

The table below lists Distech Controls' recommended power cable.

Cable Type	Non-Plenum Applications(FT4)		Plenum Applications (FT6)	
AWG - Number of Conductors	Part Number	O.D. (Ø)	Part Number	O.D. (Ø)
18-2	CB-W181P-1002	5.0mm / 0.20in.	CB-W181P-2051	5.0mm / 0.20in.
16-2	CB-W161P-1031	4.8mm / 0.19in.	CB-W161P-2062	4.8mm / 0.19in.
14-2	CB-W141P-1081	7.2mm / 0.29in.	CB-W141P-2013	7.2mm / 0.29in.

Table 18: Distech Controls Recommended 24V Power Cable

24VAC Power Supply Connection

Use an external fuse on the 24VAC side (secondary side) of the transformer, as shown in *the figure below*, to protect all controllers against power line spikes.

The ECLYPSE Controller uses the S terminal as the signal reference point for the data bus (see *Common Identification Labels for BACnet MS/TP Data Bus Polarity for Distech Controls' Products*).

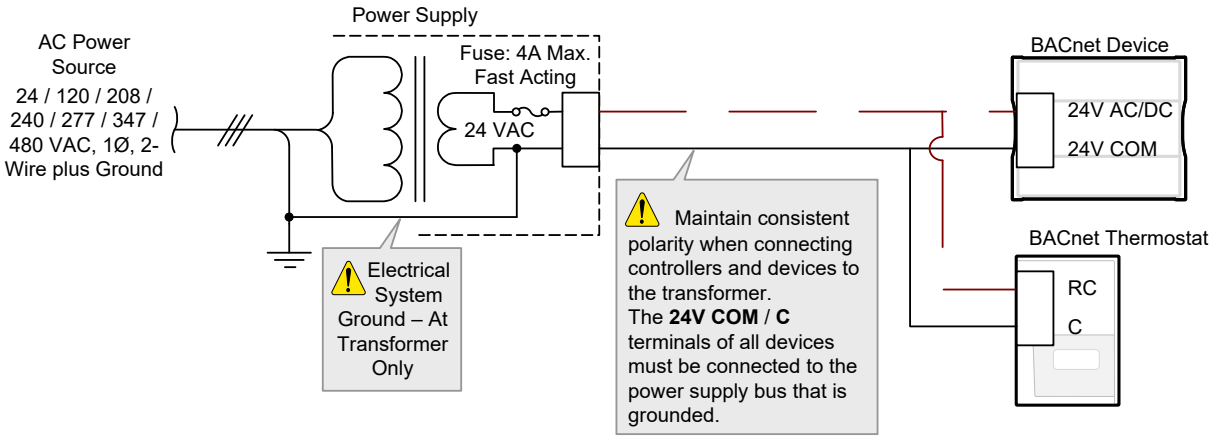


Figure 109: The 24V COM / C Terminal of all Devices must be Connected to the Grounded Power Supply Bus

Power Wiring with APEX

Voltage: 24VAC/DC; ± 15%, Class 2

This is a Class 2 Product. Use a Class 2 transformer only (rated 100VA at 24VAC) for each power supply.

A separate transformer rated at 100 VA must be used for each ECLYPSE APEX power supply in order for it to operate correctly. Choose a transformer that can supply both the needs of the APEX power supply (75VA) and any other 24VAC loads such as connected sensors and actuators: add up the maximum power consumption of all 24VAC loads and multiply this sum by 1.3. If the resulting total (75VA plus 1.3 × 24VAC loads) is higher than 100VA, use multiple transformers.

There is a penalty if operating at low input voltage. If, for example, the controller is operating at 20.4VAC (24VAC -15%), the available power is 85VA. The user should keep 15VA of buffer to compensate for voltage variation. This leaves 10VA for other loads on the same transformer.

Use an external fuse on the 24VAC side (secondary side) of the transformer, as shown in the figure below, to protect all modules against power line spikes and mis-wiring.

Each APEX power supply can supply a maximum of 18.8W@18.8V to loads connected to the right of it, up to the next connected power supply, with current limit of 27.3W including the subnet. See the ECLYPSE Selection Tool to calculate the number of Input/Output Extension Modules that can operate with each power supply, the number of power supplies required, and their location. The total power consumption of all modules including external 18VDC loads (such as 0 to 20mA current loop inputs) must be 18W@18V or less.

Maintain consistent polarity when connecting controllers and devices to the transformer. One terminal on the secondary side of the transformer must be connected to the building's ground. Ensure that the 24V COM terminals of all power supplies are connected to the grounded transformer secondary connection.

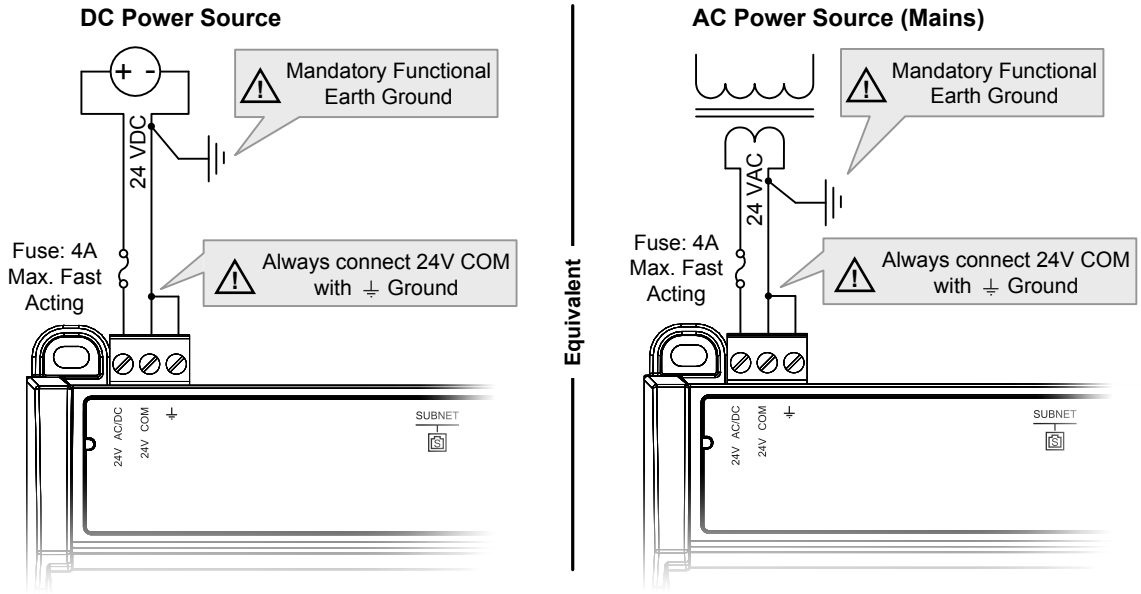


Figure 110: APEX Power wiring 2-wire

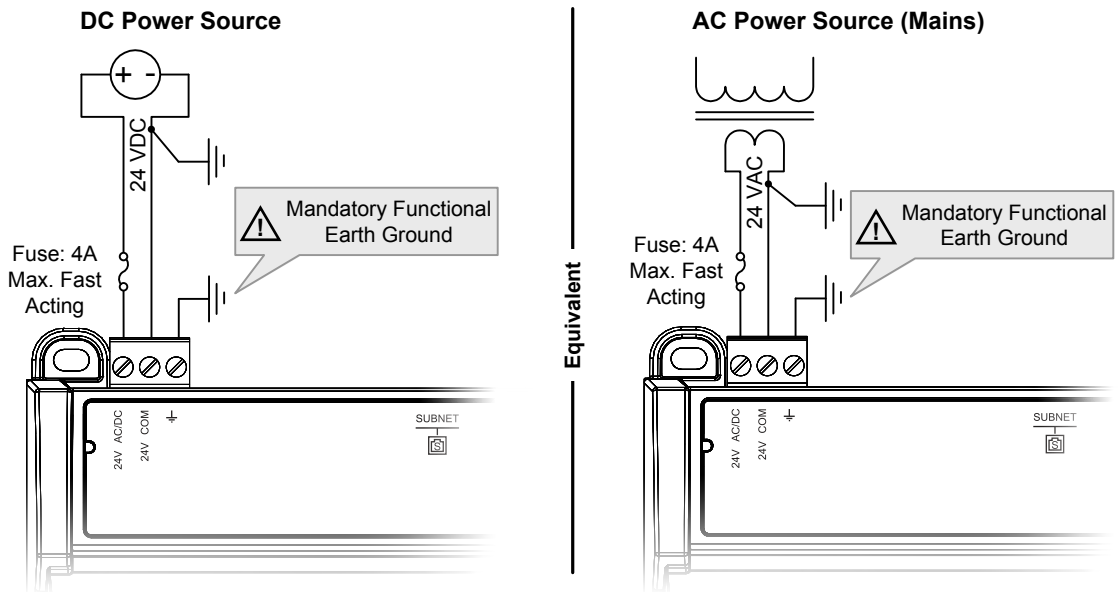


Figure 111: APEX Power wiring 3-wire

CHAPTER 12
Subnetwork Installation Guidelines

This chapter describes the subnetwork installation guidelines. This subnetwork supports a range of expansion / extension modules.

About the Subnetwork Data Bus

ECY Series Distech Controls' controllers use the subnetwork data bus to support various optional modules that add extra inputs, outputs, sensor inputs (temperature, humidity, CO_2, motion, receive wireless commands from a remote control), and interactive screen menus for user control. The subnetwork data bus uses the EIA-485 (Electronic Industries Alliance) standard for data transmission.

Subnetwork Connection Method

Connection to the subnetwork data bus is made through the RJ-45 **SUBNET** port to quickly connect expansion modules and sensors in a daisy-chained fashion to the subnetwork using a Cat 5e cable (standard straight Ethernet patch cable). Any device that connects to a controller's **SUBNET** port is collectively referred to as room devices.

This is summarized in the table below.

Subnetwork Room Device or Extension Module	Type	Connection Method
Allure UNITOUCH™	Room Device: Sensors	Cat 5e cable with RJ-45 connectors – See *Cat 5e Cable Subnetwork Data Bus*.
Allure EC-Smart-Vue series		
Allure EC-Smart-Comfort series		
Allure EC-Smart-Air series		
EC-Multi-Sensor series		
EC-Multi-Sensor-BLE		
ECx-Light-4 / ECx-Light-4D / ECx-Light-4DALI	Room Device: Application specific expansion modules	
ECx-Blind-4 / ECx-Blind-4LV		
ECx-Display	Color LCD display	

Table 19: Subnetwork Connection Method

Subnetwork Module Compatibility and Supported Quantity Charts

Not all subnetwork modules work with all controller models: The subnetwork module compatibility for an individual controller is shown in the table below along with the maximum supported quantity of standard and Bluetooth low energy room devices and extension modules. The Subnet ID address of all subnet devices must be set to be within the shown addressing range.

Adding devices to the subnetwork decreases system responsiveness which may cause delays executing commands needing a fast response such as lighting and shades/sunblind commands.

Controller Model	Subnetwork Data Bus Device	Permitted Subnet ID Addressing Range	Maximum Quantity Allowed
ECY-APEX	Allure EC-Smart-Vue series	1 to 12	12[2]
	Allure EC-Smart-Comfort series	1 to 6	
	Allure EC-Smart-Air series		
	EC-Multi-Sensor series	1 to 4	4
	Allure UNITOUCH	1 to 6	6[4]
	EC-Multi-Sensor-BLE		
	ECx-Light-4 / ECx-Light-4D / ECx-Light-4DALI	1 to 4	4
	ECx-Blind-4 / ECx-Blind-4LV / ECx-Blind-4SMI		
	ECx-Display	Not applicable	1

Table 20: Subnetwork Module Compatibility and Maximum Supported Quantity Chart

1. A controller can support a maximum of two (2) Allure series sensor models equipped with a CO_2 sensor. Any remaining connected Allure series sensor models must be without a CO_2 sensor.
2. A controller can support a maximum of 2 Allure UNITOUCH devices, regardless of the sensor model, and a maximum of 4 EC-Multi-Sensor-BLE devices.

The indicated addressing ranges group together the permitted addressing ranges for those devices:

The following devices use different Subnet address ranges so that the same Subnet ID of one device will not conflict with that of another device that is on a different Subnet address range:

- Address Ranges:
  - 1 address range for Allure EC-Smart-Vue sensors
  - 1 address range for Allure EC-Smart-Comfort and Allure EC-Smart-Air sensors
  - 1 address range for EC-Multi-Sensors
  - 1 address range for ECx-Light/Blind expansion modules
  - 1 address range for ECx-Display
  - 1 address range for Allure UNITOUCH and EC-Multi-Sensor-BLE

For example, an Allure EC-Smart-Vue sensor and an Allure EC-Smart-Air sensor can have the same Subnet ID, but an Allure EC-Smart-Air sensor and an Allure EC-Smart-Comfort sensor must have a different Subnet ID. Consequently, you cannot set both an ECx-Light-4 and an ECx-Blind-4 to have a Subnet ID as 1.

Subnetwork Module Connection

The following sections will provide further information needed to connect and configure the subnetwork devices such as cable type, cable length, wiring, data bus termination, device addressing, and more.

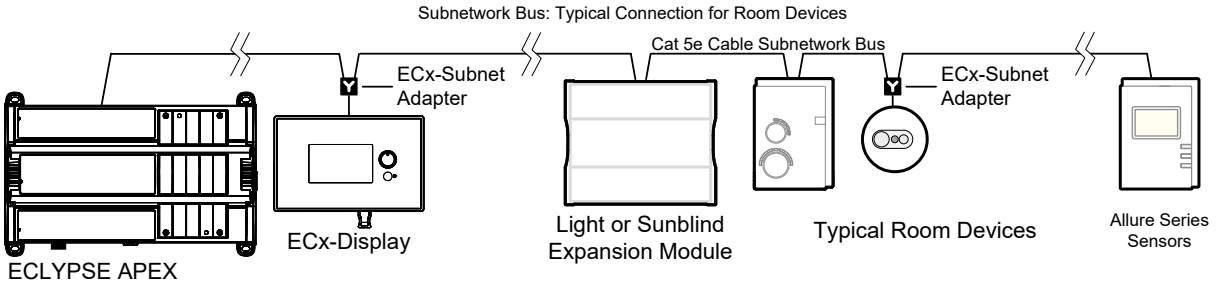


Figure 112: Subnetwork Module Connection to the APEX Controller Example

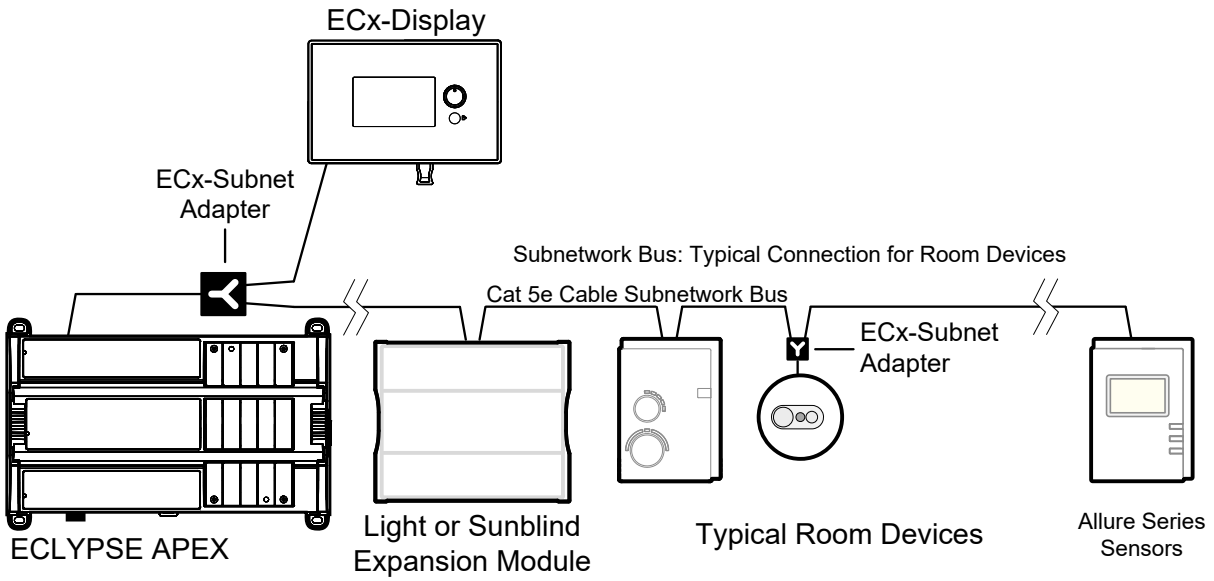


Figure 113: Subnetwork Module Connection to the APEX Controller with an ECx-Display Connected as a Stub Example

Subnetwork Data Bus Length

The maximum total length of the Cat 5e cable subnetwork data bus is 600 ft. (180 m) when using traditional Allure sensors, and 328 ft (100 m) when using BLE enabled Distech Controls devices.

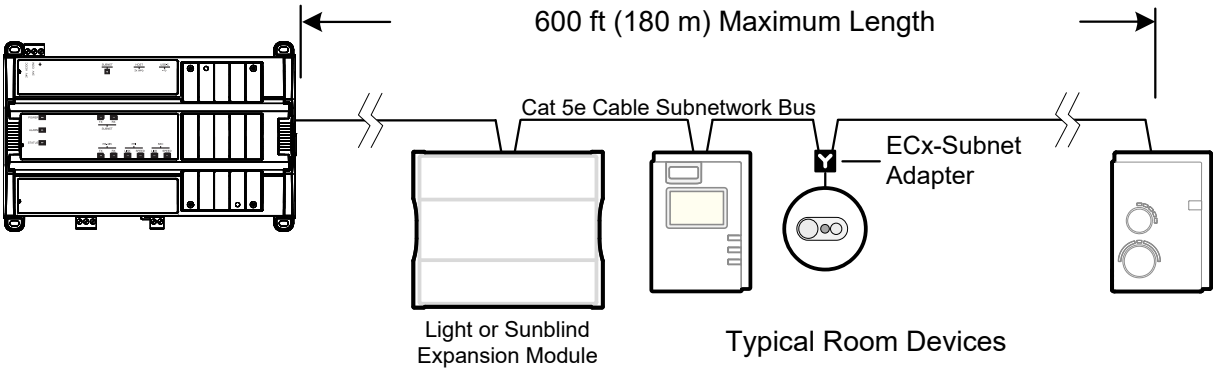


Figure 114: Maximum Length of the Cat 5e Cable Subnetwork Data Bus with traditional Allure sensors

For traditional Allure Communicating Sensor models:

A controller can support a maximum of two (2) Allure series sensor models equipped with a CO_2 sensor; the remaining connected models must be without a CO_2 sensor.

For instance, if the subnetwork for the controller model supports a subnetwork with 12 Allure series communicating sensors in total, then 10 Allure series sensor models must be without a CO_2 sensor and the remaining two (2) Allure series sensor models can be equipped with a CO_2 sensor. To ensure proper operation, it is recommended to distribute the sensors throughout the length of the subnetwork.

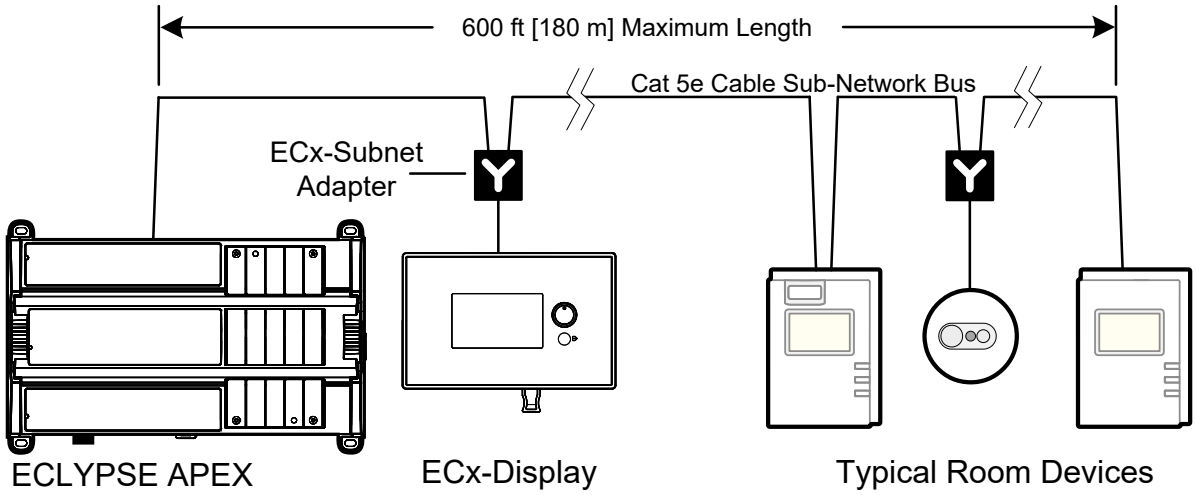


Figure 115: Subnetwork Module Connection Example

The maximum length of the Cat 5e cable subnetwork data bus used to connect an ECLYPSE controller to an ECx-display as a stub is 6.5 ft. (2m). The maximum total length of the Cat 5e cable subnetwork data bus remains 600 ft. (180 m). When other Cat 5e subnetwork devices are used, use an ECx-Subnet Adapter to connect to those devices.

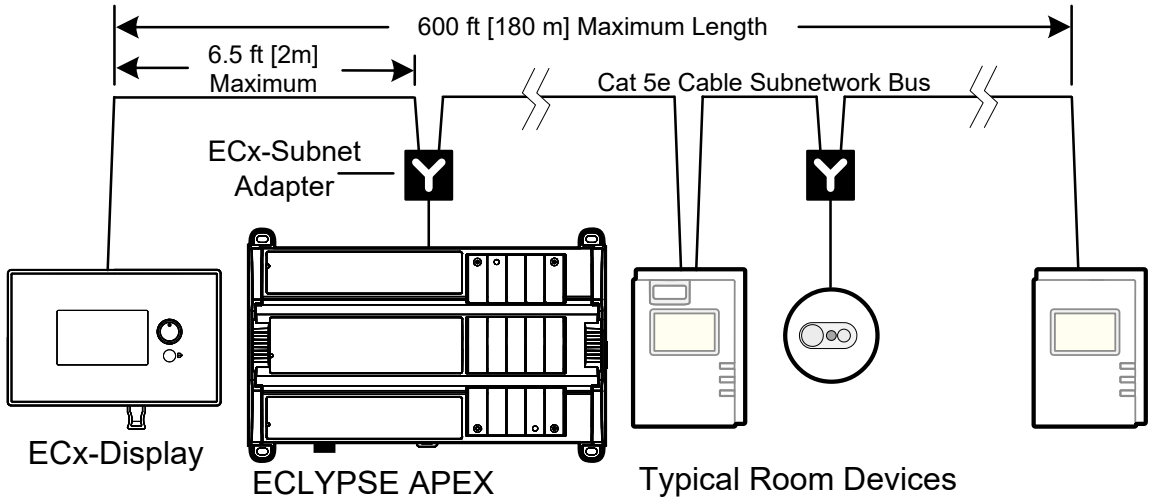


Figure 116: Subnetwork Module Connection with an ECx-Display Connected as a Stub Example

For BLE enabled Distech Controls devices:

Bluetooth low energy enabled devices such as the Allure UNITOUCH and the EC-Multi-Sensor-BLE are only compatible with Distech Controls ECLYPSE Series Controllers.

A controller can support a maximum of two (2) Allure UNITOUCH sensors, and a maximum of four (4) EC-Multi-Sensor-BLE devices.

The maximum total length of the Cat 5e cable subnetwork data bus remains 328 ft. (100 m). When other Cat 5e subnetwork devices are used, an ECx-Subnet Adapter may be required to connect to those devices.

See *Subnetwork Module Compatibility and Supported Quantity Charts* for the quantity of room devices supported by each controller model.

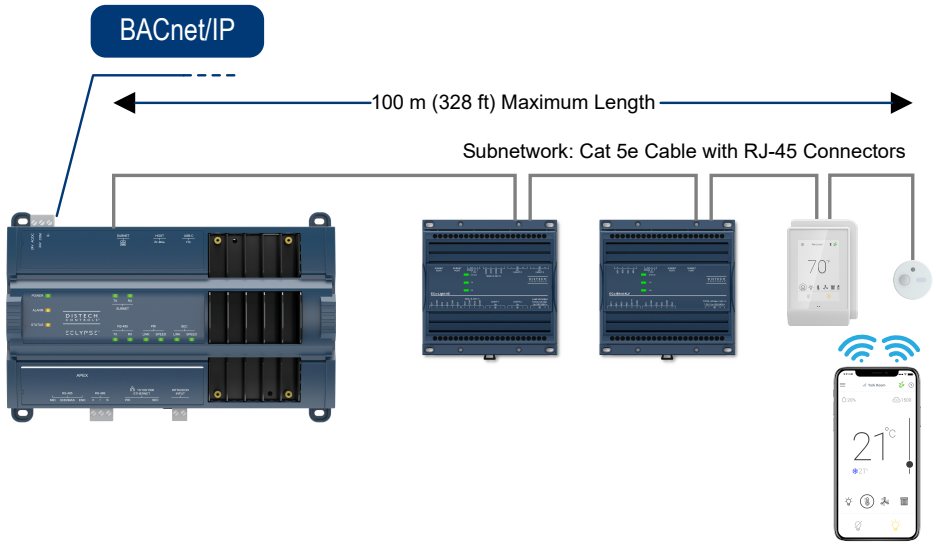


Figure 117: Subnetwork Module Connection with BLE enabled Room Devices

A mixed architecture with standard room devices and Bluetooth low energy enabled devices is not recommended.

Cat 5e Cable Subnetwork Data Bus

The Cat 5e Cable subnetwork data bus is used to connect compatible room devices (*Subnetwork Connection Method*) to any Distech Controls ECLYPSE series controller. See *Subnetwork Module Compatibility and Supported Quantity Charts* or a list of compatible extension / expansion modules.

Never connect an IP (Ethernet) network to the SUBNET PORT connector of a controller or RJ-45 connector of a room device. Equipment damage may result.

Cat 5e Cable Subnetwork Data Bus Cable Requirements

The Cat 5e Cable subnetwork data bus uses commonly available Cat 5e structural cabling fitted with RJ-45 connectors. If you make your own patch cable, use Category 5e cable and crimp the RJ-45 connectors at both ends of the cable either as T568A or T568B.

Parameter	Details
Maximum number of room devices	See *Subnetwork Module Compatibility and Supported Quantity Charts*. See also the Controller's Datasheet.
Subnet ID Addressing Configuration	See *Setting the Subnet ID Addressing for Room Devices*.
Media	Cat 5e Patch Cable with RJ-45 Connectors (standard straight patch cable)
RJ-45 Pin Configuration	Four (4) pairs required. Straight-through wiring. Crimp connectors as per T568A or T568B (both cable ends must be crimped the same way).
Characteristic impedance	100-130 Ohms
Distributed capacitance	Less than 100 pF per meter (30 pF per foot)
Maximum total length of the Cat 5e Cable subnetwork data bus plus the 2-Wire subnetwork data bus	300 m (1 000 ft.) Maximum – See *Subnetwork Data Bus Length*.
Maximum length of the Cat 5e Cable subnetwork data bus for standard room devices	180 m (600 ft.) Maximum – See *Subnetwork Data Bus Length*.
Maximum length of the Cat 5e Cable subnetwork data bus for BLE room devices	100 m (328 ft.) Maximum – See *Subnetwork Data Bus Length*.
Polarity	Polarity sensitive
Multi-drop	Daisy-chain (no T-connections) Most room devices have two RJ-45 female pass-through connectors to facilitate the daisy-chain connection of room devices. For the EC-Multi-Sensor and EC-Multi-Sensor-BLE: An optional ECx-Subnet Adapter (Y-splitter) is available to facilitate the daisy-chain connection of room devices. The ECx-Subnet Adapter must be connected directly to the EC-Multi-Sensor and its length cannot be extended.
EOL terminations	Must be set / enabled on the last room device only. This does not apply to the ECx-Display.
Shield grounding	Not applicable

Table 21: Cat 5e Cable Subnetwork Data Bus Physical Specifications and Cable Requirements

Distech Controls recommends the Cat 5e cables shown below. Cables fitted with connectors are crimped as T568B.

Cable Type	Non-Plenum Applications (Use in Conduit - FT4)		Plenum Applications (FT6)	
	Part Number	O.D. (Ø)[1]	Part Number	O.D. (Ø)[1]
0.3m (1 ft.), Cat 5e Cable fitted with RJ-45 Connectors	CB-CAT5PC4WH0001	4.6mm (0.18in.)	CB-CAT5PC6WH0001	4.6mm (0.18in.)
4.6m (15 ft.), Cat 5e Cable fitted with RJ-45 Connectors	CB-CAT5PC4WH0015	4.6mm (0.18in.)	CB-CAT5PC6WH0015	4.6mm (0.18in.)
9m (30 ft.), Cat 5e Cable fitted with RJ-45 Connectors	CB-CAT5PC4WH0030	4.6mm (0.18in.)	CB-CAT5PC6WH0030	4.6mm (0.18in.)
15m (50 ft.), Cat 5e Cable fitted with RJ-45 Connectors	CB-CAT5PC4WH0050	4.6mm (0.18in.)	CB-CAT5PC6WH0050	4.6mm (0.18in.)
22m (75 ft.), Cat 5e Cable fitted with RJ-45 Connectors	CB-CAT5PC4WH0075	4.6mm (0.18in.)	CB-CAT5PC6WH0075	4.6mm (0.18in.)
30m (100 ft.), Cat 5e Cable fitted with RJ-45 Connectors	CB-CAT5PC4WH0100	4.6mm (0.18in.)	CB-CAT5PC6WH0100	4.6mm (0.18in.)
300 m (1000 feet), Cat 5e Cable – Without Connectors	CB-W244P-1446WHTB	4.6mm (0.18in.)	CB-W244P-2176WHTB	4.6mm (0.18in.)
100 Crimp RJ-45 Connectors	CB-W5506E	N/A	CB-W5506E	N/A

Table 22: Distech Controls Recommended Cable Types to use for the Cat 5e Cable Subnetwork Data Bus

1. Outer cable diameter – This does not take into account the RJ-45 connector.

Cat 5e Cable Subnetwork Bus Topology and End-of-Line Terminations

The EOL termination settings for the Cat 5e Cable subnetwork data bus will vary depending on the type of controller the room device or extension module is connected to. By default, all room devices and ECx-4XX Series I/O Extension Module EOL terminations are factory set to OFF (except for the EC-Multi-Sensor and EC-Multi-Sensor-BLE).

For the Cat 5e Cable subnetwork data bus, only a daisy-chain topology is acceptable, and T-connections are not allowed. For the EC-Multi-Sensor, EC-Multi-Sensor-BLE, and ECx-Display, an optional ECx-Subnet Adapter (Y-splitter) is available to facilitate the daisy-chain connection of these devices. The male-end of the ECx-Subnet Adapter must be connected directly to the device and its length cannot be extended.

ECx-Subnet Adapter (Y-Splitter)

The ECx-Subnet Adapter is also used with a controller to connect to an ECx-Display and to one or more room devices. See *Subnetwork Data Bus Length*. In this scenario, the male-end of the ECx-Subnet Adapter must be connected directly to the controller's Subnet Port and its length cannot be extended.

EOL Terminations

When one or more room devices are connected to an ECLYPSE controller's **Subnet Port**, only the EOL terminations of the last room device is set to ON. All other room devices on the subnetwork data bus must have their EOL terminations set to OFF. The controller must be the first device on the Cat 5e Cable Subnetwork data bus as its internal EOL termination is permanently enabled. The ECx-Display does not have any EOL terminations to be set and as such should not be installed as the last device on the subnetwork bus. See *Subnetwork Data Bus Length*.

Please refer to the devices Installation Guide for EOL jumper or dip switch locations.

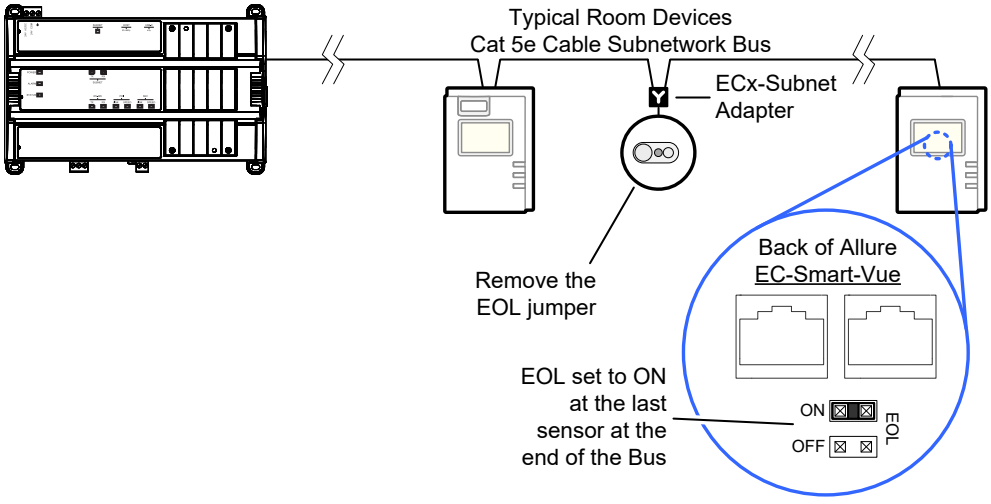


Figure 118: Setting the EOL Terminations on the Cat 5e Cable Subnetwork Data Bus for the ECLYPSE APEX (with an Allure EC-Smart-Vue)

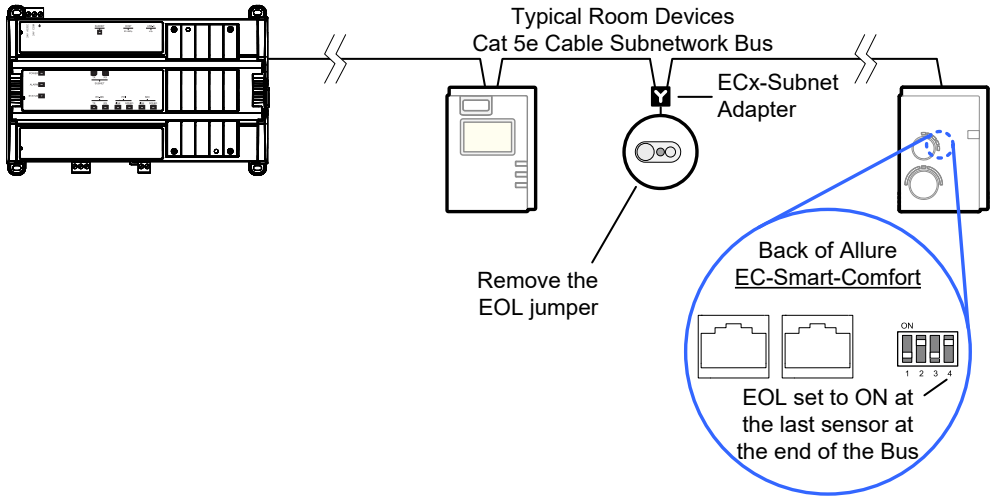


Figure 119: Setting the EOL Terminations on the Cat 5e Cable Subnetwork Data Bus for the ECLYPSE APeX (with Allure EC-Smart-Comfort)

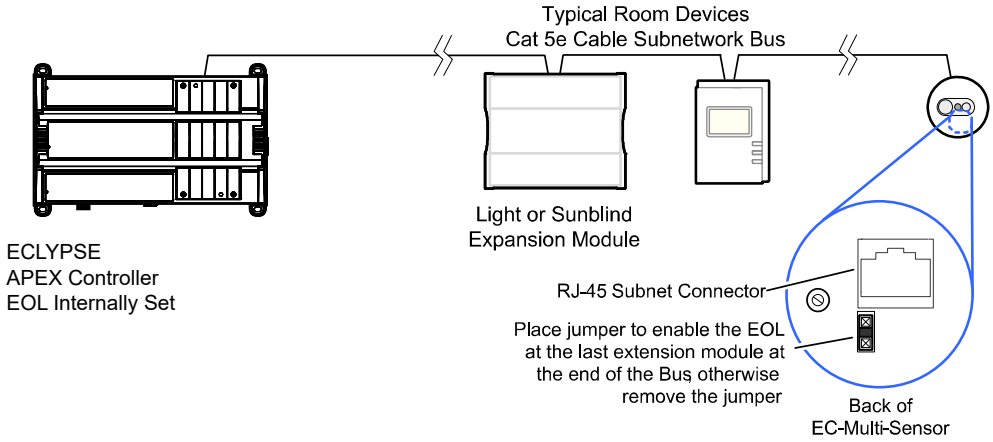


Figure 120: Setting the EOL Terminations on the Cat 5e Cable Subnetwork Data Bus for the ECLYPSE APEX (with an EC-Multi-Sensor)

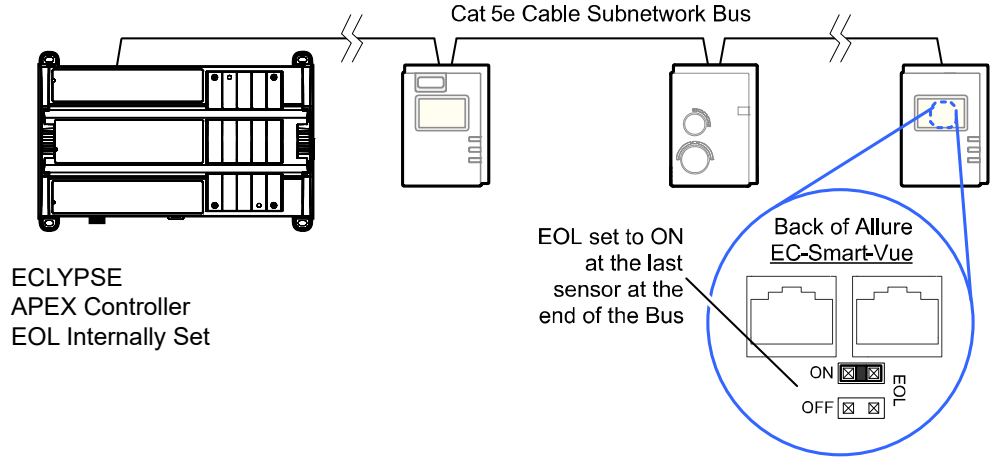


Figure 121: Setting the EOL Terminations on the Cat 5e Cable Subnetwork Data Bus for the ECLYPSE APEX (with an Allure EC-Smart-Vue)

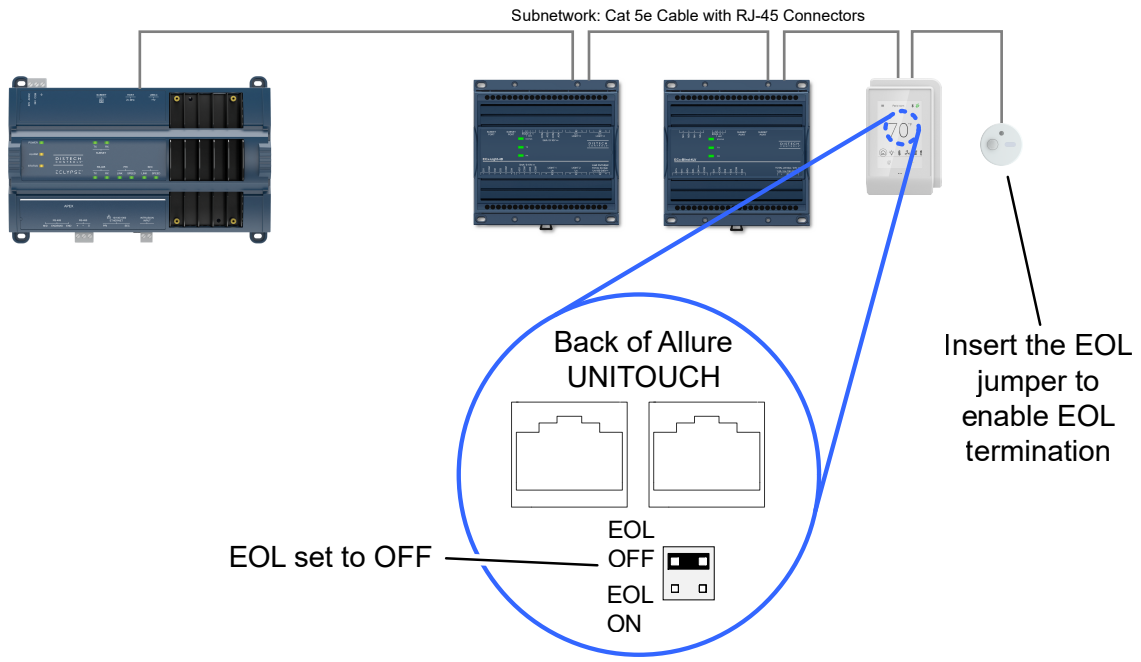


Figure 122: Setting the EOL Terminations on the Cat 5e Cable Subnetwork Data Bus for the ECLYPSE APEX with an Allure UNITOUCH and an EC-Multi-Sensor-BLE

Depending on the type of expansion module, the subnetwork data bus EOL may be set by configuring jumpers or DIP switches. Refer to the expansion module's hardware installation guide for how to identify and set a room devices' built-in EOL terminations.

Setting the Subnet ID Addressing for Room Devices

Each type of room device connected to a controller's Subnet Port must be set to a unique subnet ID address. The permitted subnet ID addressing range according to controller model can be found at *Subnetwork Module Compatibility and Supported Quantity Charts*. The method to use to set a room device's subnet ID address is shown in the table below.

Room Device Type	Configuration Method	See
Allure EC-Smart-Vue series	Configured in an on-screen menu.	*Setting the Allure EC-Smart-Vue Sensor's Subnet ID Address*
Allure UNITOUCH		*Setting the Allure UNITOUCH Sensor Subnet ID Address*
Allure EC-Smart-Comfort sensors	Dip Switch located next to the RJ-45 subnet connectors	*Setting the Allure EC-Smart-Air and EC-Smart-Comfort Communicating Sensor Series' Subnet ID Address*
Allure EC-Smart-Air series		
EC-Multi-Sensor series	Rotary selector located next to the RJ-45 subnet connector	*Setting the EC-Multi-Sensor Series' Subnet ID Address*
EC-Multi-Sensor-BLE		*Setting the EC-Multi-Sensor-BLE Subnet ID Address*
ECx-Light-4 / ECx Light-4D / ECx Light 4DALI ECx-Blind-4 / ECx Blind-4LV	DIP switch located next to Subnet Port connectors	*Setting the ECx-Light and ECx-Blind Series' Subnet ID Address*

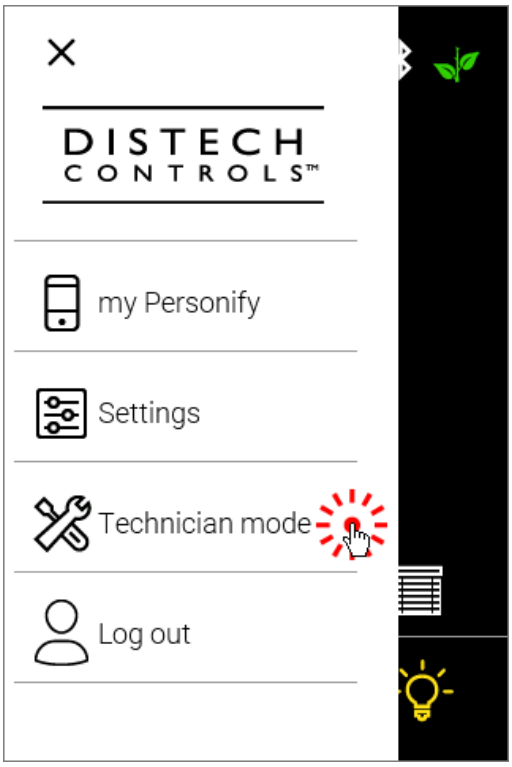
Table 23: Subnetwork Module Compatibility and Maximum Supported Quantity Chart

Setting the Allure UNITOUCH Sensor Subnet ID Address

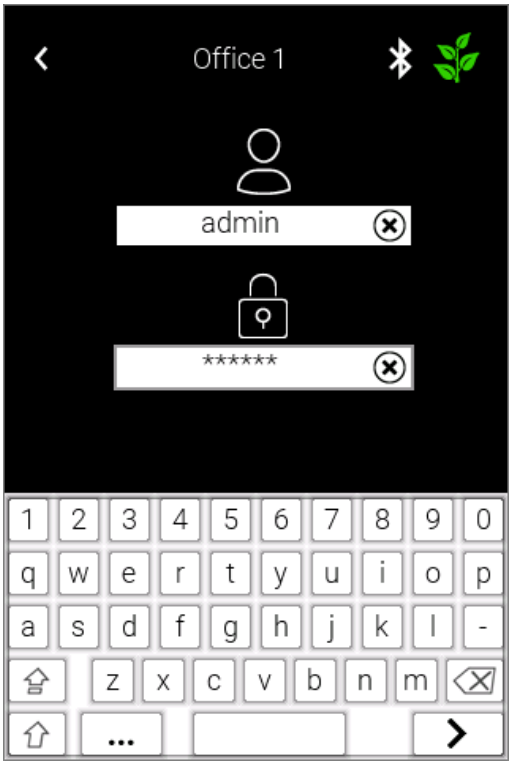
Each device on the subnet requires a unique subnet ID. If a connected device's subnet ID does not match its programmed ID in EC-*gfx*Program, or if two or more devices have the same subnet ID, there will be a communication error. A communication error screen will be displayed, and you will be prompted to enter the default password (9995) to access the subnet ID settings.

To change the subnet ID:

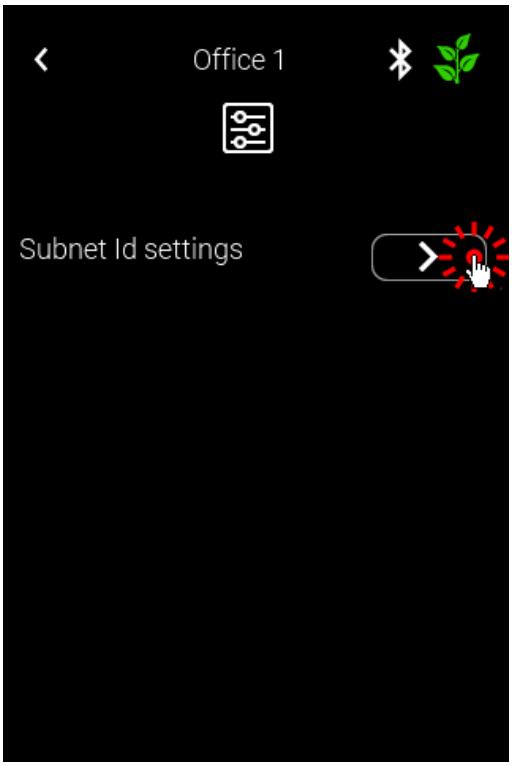
1. Tap the menu button in the top left hand corner of your Allure UNITOUCH to access the menu.
2. Once the menu has appeared, tap the **Technician Mode** tab.



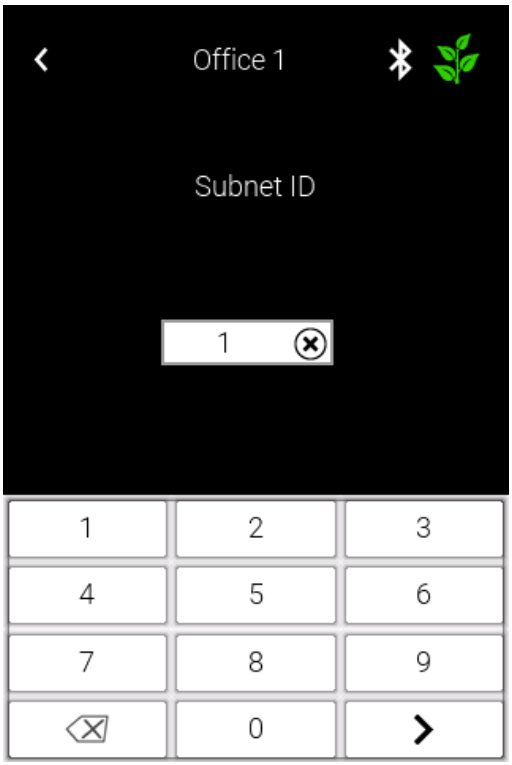
3. You will then be prompted to input a user name and password. This username and password must have Admin rights to access **Technician Mode**.



4. Once the correct user name and password has been input, the **Subnet ID settings** tab will appear. Tap the arrow to access the menu.



5. Tap the input box in the middle of the screen to access the number pad. Now choose the correct Subnet ID. Tap the [>] button to enter your new Subnet ID.



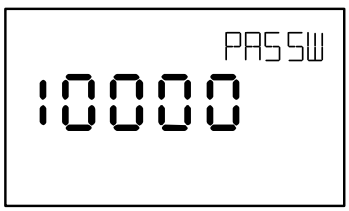
Setting the Allure EC-Smart-Vue Sensor's Subnet ID Address

An Allure EC-Smart-Vue sensor's Subnet ID corresponds to the ComSensor block instance programmed in the controller with EC-*gfx*Program. The Allure EC-Smart-Vue sensor's Subnet ID can be set in the procedure below.

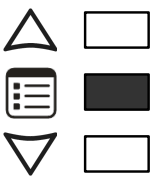
ECLYPSE Connected VAV Controllers can be commissioned with an Allure EC-Smart-Vue sensor. The default Subnet ID for an Allure EC-Smart-Vue sensor is 1. To commission an ECLYPSE Connected VAV Controller, the Allure EC-Smart-Vue sensor's Subnet ID must be set to 1. If the Allure EC-Smart-Vue sensor's Subnet ID has been set to another value (for example, the display flashes error code 1 with the Bell icon when the Allure EC-Smart-Vue sensor is connected to a controller for commissioning), change the Subnet ID to 1 as follows:

1) Connect an Allure EC-Smart-Vue sensor to the controller with a Cat 5e patch cable. Wait for the Bell icon and the number 1 to flash on the display.

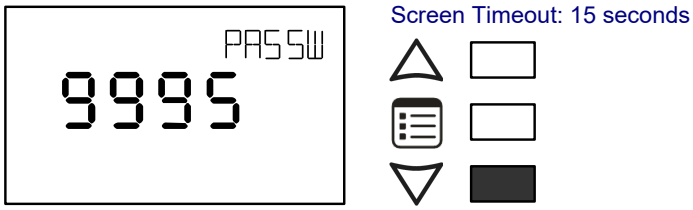
2) Press and hold the Menu button for 5 seconds to enter the password menu. 10000 is shown on the display.



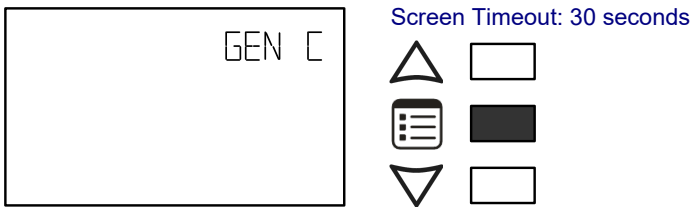
Screen Timeout: 15 seconds



1) Press the down button to set the number to 9995 (this is the default password).

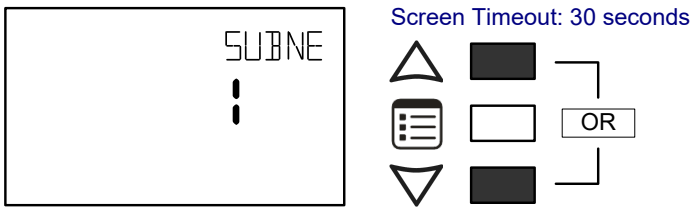


1) Press the Menu button to submit the password. Upon submitting the password, the **GEN CFG** menu appears on the display.



1) Press the down button once to enter the **GEN CFG** submenu.

2) Press the Menu button several times until SUBNET ID appears on the display. The current controller's Subnet ID is shown.



1) Use the up and down buttons to set the controller's Subnet ID to **1**. *Tip*: Hold down either the up or down button to fast-advance the display value.

2) Press the Menu button once.

3) Press and hold the Menu button for 5 seconds to exit the configuration menu.

The Allure EC-Smart-Vue sensor can now be used to go from one ECLYPSE Connected VAV Controller to the next for commissioning purposes.

When the controller has been programmed, each connected Allure EC-Smart-Vue's Sensor must be assigned a unique Subnet ID.

Setting the Allure EC-Smart-Air and EC-Smart-Comfort Communicating Sensor Series' Subnet ID Address

Each Allure EC-Smart-Air or EC-Smart-Comfort communicating sensor connected to a controller's Subnet Port must be set to a unique subnet ID address. This address should correspond to the block number of the associated Subnet Extension block in EC-*gfx*Program. The address is set through a DIP switch located inside the sensor near the RJ-45 connectors.

Allure EC-Smart-Comfort and EC-Smart-Air communicating sensor series share the same Subnet ID range: the same address cannot be assigned concurrently to an Allure EC-Smart-Comfort communicating sensor series and to an Allure EC-Smart-Air communicating sensor series.

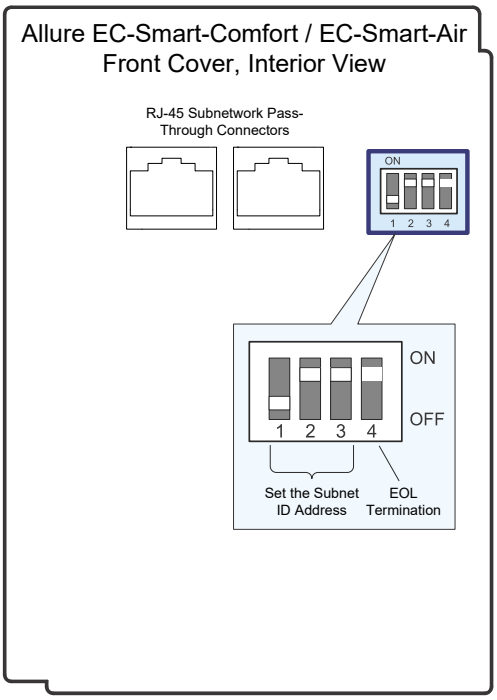


Figure 123: Setting the Allure EC-Smart-Air or EC-Smart-Comfort communicating sensor's Subnet ID Address

The above figure shows an example of how to set the Allure EC-Smart-Air or EC-Smart-Comfort communicating sensor's Subnet ID address DIP switch to 6 and how to set the EOL termination to ON.

Switch Position				Allure EC-Smart-Air or EC-Smart-Comfort communicating sensor's Subnet ID Address
1	2	3	4	
OFF	OFF	OFF	OFF: EOL disabled ON: EOL enabled	1
ON	OFF	OFF		1
OFF	ON	OFF		2
ON	ON	OFF		3
OFF	OFF	ON		4
ON	OFF	ON		5
OFF	ON	ON		6

Table 24: Allure EC-Smart-Air or EC-Smart-Comfort communicating sensor's Subnet ID Address DIP Switch Settings

Setting the EC-Multi-Sensor Series' Subnet ID Address

Each EC-Multi-Sensor connected to a controller's Subnet Port must be set to a unique subnet ID address. This address should correspond to the block number of the associated Multi Sensor block in EC-*gfx*Program. The address is set through the rotary selector located next to the Subnet Port connector.

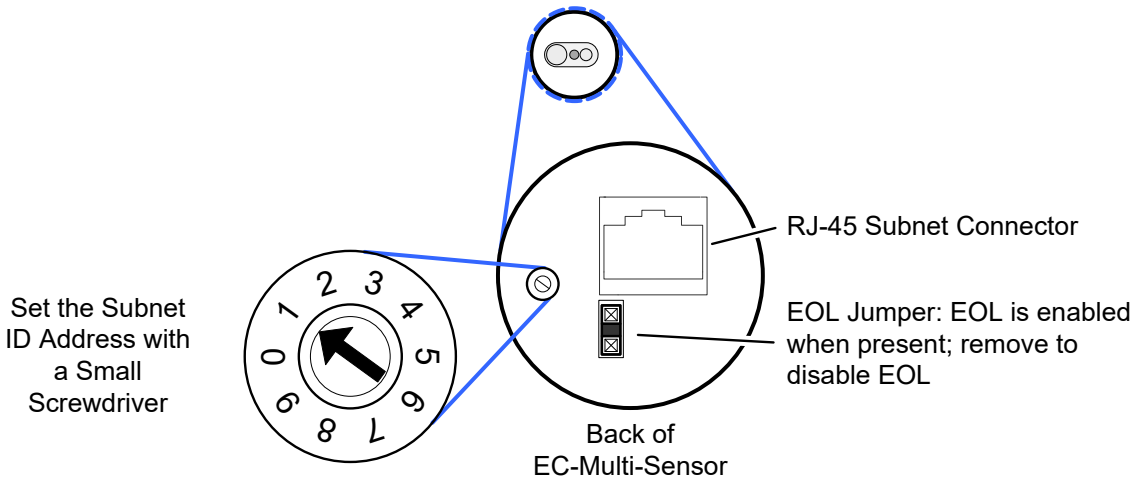


Figure 124: Setting the EC-Multi-Sensor Series' Subnet ID Address

Use a small screwdriver (for example, a precision or jeweler's screwdriver) to set the selector. The figure above shows an example of how to set the EC-Multi-Sensor Series' Subnet ID address DIP switch to 1 and the EOL termination is ON.

Once an EC-Multi-Sensor is installed, the following tip can be used during system commissioning to verify if the EC-Multi-Sensor is set to the correct subnet ID address for the zone in which it is physically located.

Run EC-*gfx*Program in debug mode for the controller with 4 Multi Sensor block instances, 1 to 4. Set a remote control to zone ID 0, then aim it at the EC-Multi-Sensor and press a command (fan speed button for example). In EC-*gfx*Program, see which block instance shows an output (RemoteFanSpeed).

Usually it is easier to reassign Multi Sensor block numbers in EC-*gfx*Program code than it is to change the Subnet ID Address of an installed EC-Multi-Sensor.

Setting the EC-Multi-Sensor-BLE Subnet ID Address

Each EC-Multi-Sensor-BLE on the ECx Subnetwork must be set to a unique subnet ID address. The address is set with the rotary switch located at the rear of the sensor using a small screwdriver (≤ 2.5 mm - 0.1'').

The Subnet ID address must be set before installing the sensor, as the rotary switch might not be accessible once the rear spring is installed.

5 different Subnet ID codifications are used on the ECx Subnetwork :

- 1 for Allure UNITOUCH™ sensors and EC-Multi-Sensor-BLE sensors
- 1 for Allure EC-Smart-Vue sensors
- 1 for Allure EC-Smart-Comfort and Allure EC-Smart-Air sensors
- 1 for EC-Multi-Sensors
- 1 for ECx-Light/Blind expansion modules

Consequently, for example, the same Subnet ID can be assigned to an ECx-Light/Blind module, to an EC-Multi-Sensor and to an Allure EC-Smart-Vue sensor without any addressing issue.

The Subnet IDs that can be allocated to EC-Multi-Sensors are 0 (factory default), 1, 2, 3, and 4. All other addresses are not used.

Automatic addressing shall only be used if only one EC-Multi-Sensor-BLE is connected to the ECx Subnetwork.

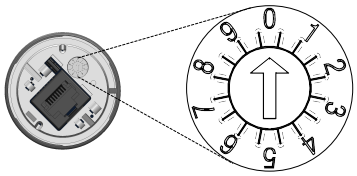


Figure 125: EC-Multi-Sensor-BLE Rotary Switch

Set the desired Subnet ID by pointing the matching number with the rotary switch arrow.

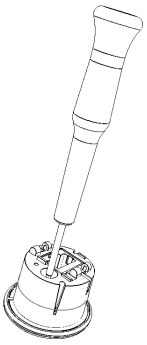


Figure 126: Setting the EC-Multi-Sensor-BLE Subnet ID Address

Setting the ECx-Light and ECx-Blind Series' Subnet ID Address

Each ECx-Light and ECx-Blind Series' connected to a controller's **Subnet Port** must be set to a unique subnet ID address. The address is set through the DIP switch located next to the **Subnet Port** connectors.

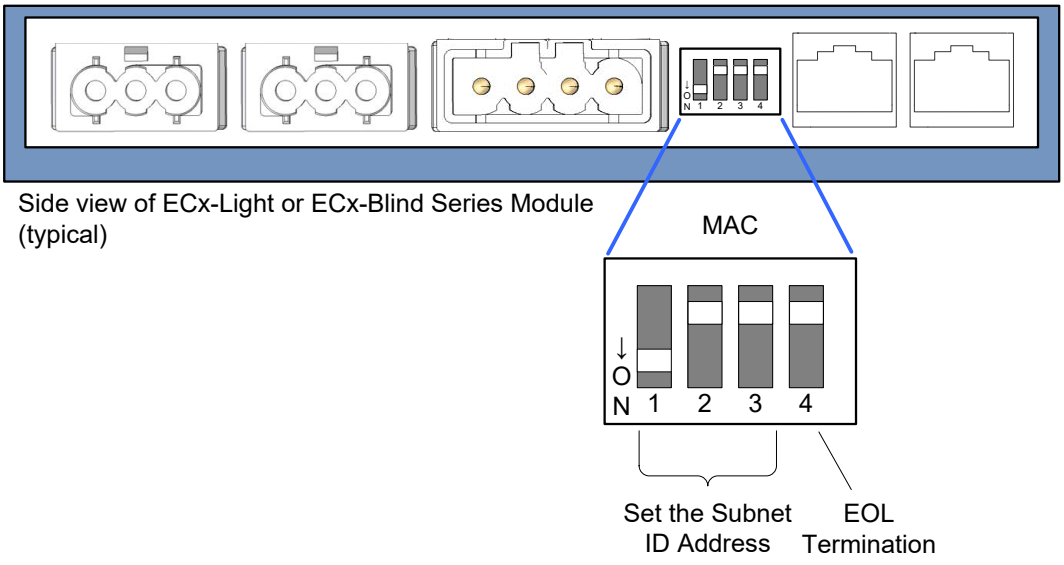


Figure 127: Setting the ECx-Light and ECx-Blind Series' Subnet ID Address (Typical)

Switch Position				Expansion Module's Subnet ID (MAC) Address
1	2	3	4	
OFF	OFF	OFF	OFF	Auto-assigned Subnet ID Address for Light and Blind Expansion Modules
ON	OFF	OFF	OFF	1
OFF	ON	OFF	OFF	2
ON	ON	OFF	OFF	3
OFF	OFF	ON	OFF	4

Table 25: ECx-Light and ECx-Blind Series' Subnet ID Address DIP Switch Settings

The above figure (*Figure 94*) shows an example of how to set the ECx-Light and ECx-Blind series' Subnet ID address DIP switch to 1 and how to set the EOL termination to OFF.

Auto-assigned Subnet ID Address for Light and Blind Expansion Modules

Often only one type of expansion module is connected to the controller; for example, one ECx-Light-4 and one ECx-Blind-4 model. By leaving the Subnet ID address DIP switch at 0 (factory default position) for these two expansion modules, the ECx-Light and ECx-Blind room device sets its own Subnet ID Address according to its model type, so no configuration is necessary.

Expansion Module Model Type	Auto-assigned Subnet ID Address when the expansion modules' MAC DIP Switch is set to 0 (factory default position)			
	1	2	3	4
ECx-Light-4 (4 lights 230V)	x			
ECx-Light-4DALI (4 DALI buses)	x			
ECx-Light-4D (4 dimming lights)		x		
ECx-Blind-4 (4 blinds/shades 230V)			x	
ECx-Blind-4LV (4 blinds/shades 24V)				x

Table 26: ECx-Light and ECx-Blind Series' Automatic Subnet ID Address when the DIP Switch is set to 0

If you connect a second expansion module of the same type to the controller's subnetwork data bus, you must set at least one of the two expansion modules' MAC DIP switches to a unique (that is, unused) subnet ID (MAC) address and then set the same value in Default address in EC-*gfx*Program. See "Manage Light and Sunblind Module Instances" in the EC-*gfx*Program User Guide.

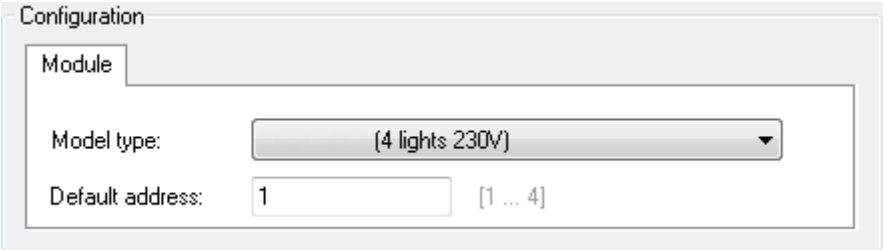


Figure 128: In EC-gfxProgram: Default Address: Setting an Expansion Modules' Subnet ID (MAC) Address for this Expansion Module Instance

Auto Learn Light and Blind/Shade Expansion Modules in EC-gfxProgram

In EC-*gfx*Program, when the connection status for the controller is **Connected**, this scans the controller's subnetwork data bus for connected expansion modules, when each expansion module has a unique subnet ID (MAC) address on the controller's subnetwork data bus. Using this feature will delete any previously configured expansion modules. See "Manage Light and Sunblind Module Instances" in the EC-*gfx*Program User Guide.

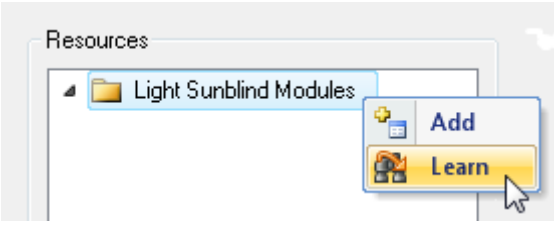


Figure 129: Light and Blind/Shade Modules Tree Options

Learn is only available after 2 minutes of the controller having been powered up. This information is no longer available after 30 minutes. Reboot the controller if **Learn** is unable to find the connected modules (in Project Synchronization, select **Download to device** and **Reboot controller** only).

Commissioning a Connected VAV Controller with an Allure EC-Smart-Vue Sensor

Commissioning a Connected VAV Controller with an Allure EC-Smart-Vue sensor involves the following tasks:

- Set the Allure EC-Smart-Vue sensor's Subnet ID. See *Setting the Allure EC-Smart-Vue Sensor's Subnet ID Address*.
- For controllers that support preloaded applications: Select the controller's preloaded application to use. See the ECY-VAV Preloaded Application User Guide for more Information.

CHAPTER 13
Modbus TCP Configuration

This chapter describes the Modbus TCP Configuration.

Controller Modbus Support

Certain ECLYPSE controller models support communication with Modbus devices. Refer to the controller's datasheet for more information.

Modbus TCP Device Connection

Modbus TCP devices are connected to the same subnet that the controller is connected to:

- Connect the Modbus TCP device to the same network switch/router to which the controller is connected.
- Connect the Modbus TCP device to either one of the controller's Ethernet ports.

Device Addressing

Device addressing allows the coordinated transfer of messages between the master (the ECY Series Controller) and the slave Modbus TCP device. For this, each Modbus TCP device is identified by its address.

About Device Addressing

Each slave device must have its own unique address number in the range from 1 to 254.

Refer to the device's hardware installation guide for information about how to set its address number.

Set the Modbus device parameters with EC-*gfx*Program in the Resources Configuration window, Modbus Device block.

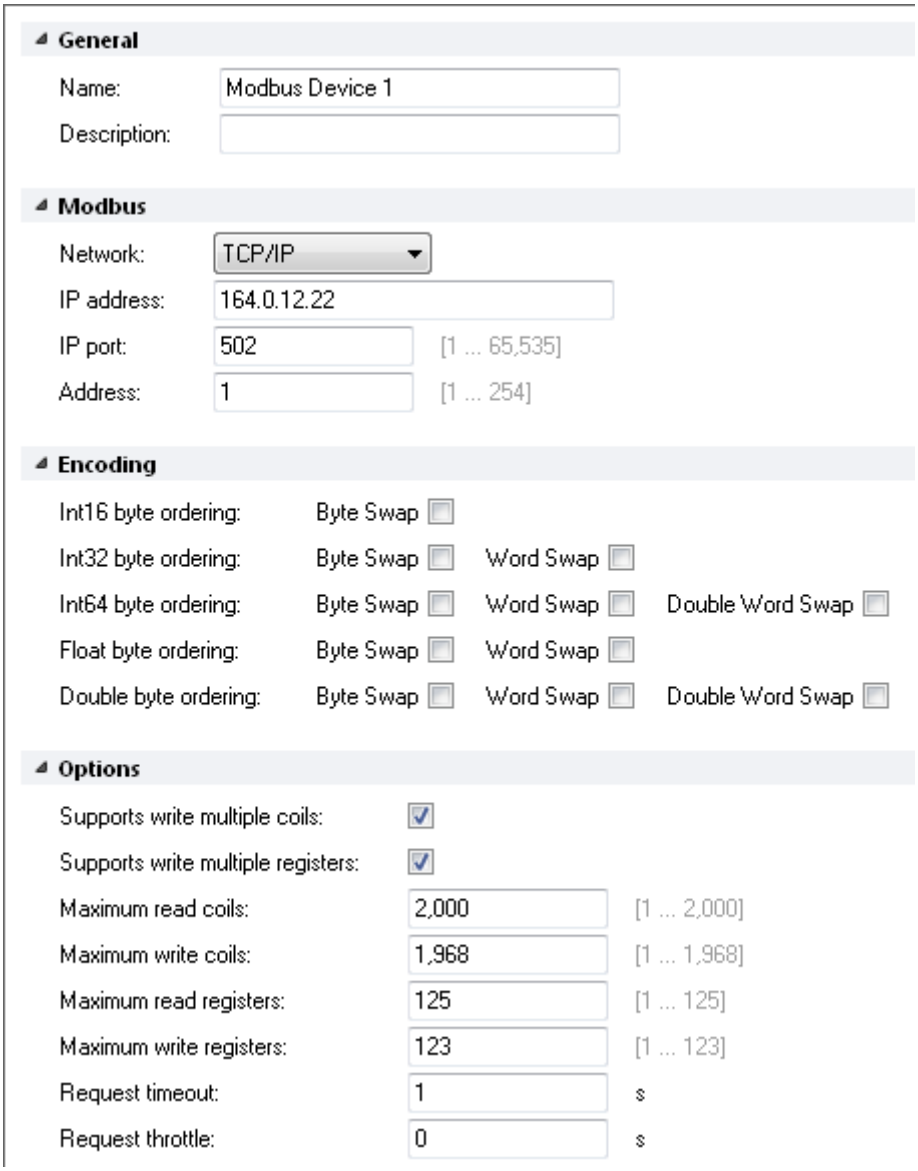


Figure 130: Setting the Modbus Device Parameters in EC-gfxProgram's Resources Configuration Window

See the EC-*gfx*Program User Guide for more information.

CHAPTER 14
Modbus RTU Communication Data Bus Fundamentals

This chapter describes the Modbus RTU Communications Data Bus operating principles.

Controller Modbus Support

Certain ECLYPSE controller models support communication with Modbus devices. Refer to the controller's datasheet for more information.

For controllers that support either BACnet MS/TP or Modbus RTU network options, this option is selected in the controller's web interface. For these controllers, BACnet MS/TP and Modbus RTU communications are made by connecting directly to separate RS-485 ports. For example, the Connected System Controller integrates up to three RS-485 ports when equipped with one ECY-RS485 extension module allowing the controller to support more than one trunk or communication protocol at a time.

Modbus RTU Data Transmission Essentials

When the ECY Series Controller is configured for Modbus RTU, it acts as the Modbus master that initiates requests to any slave device connected to this data bus. All slave devices must support Modbus RTU communications protocol. The ECY Series Controller does not work with Modbus ASCII devices.

The Modbus network communication parameters and the Modbus device parameters are configured with EC-*gfx*Program in the Resources Configuration window, Modbus Device block.

The Modbus RTU data bus protocol uses the EIA-485 (RS-485) 3-wire physical layer standard for data transmission. EIA-485 is a standard that defines the electrical characteristics of the ECLYPSE Wi-Fi Adapters and drivers to be used to transmit data in a differential (balanced) multipoint data bus that provides high noise immunity with relatively long cable lengths which makes it ideal for use in industrial environments. The transmission medium is inexpensive and readily-available twisted pair shielded cable.

While there are many possible LAN topologies for an EIA-485 data bus, only devices that are daisy-chained together are allowed with Modbus RTU (see *Figure 96*).

End-of-line (EOL) terminations are critical to error-free EIA-485 data bus operation. The impedance of the cable used for the data bus should be equal to the value of the EOL termination resistors (typically 120 ohms). Cable impedance is usually specified by the cable manufacturer.

Modbus RTU Data Bus is Polatiry Sensitive

The polarity of all devices that are connected to the Modbus RTU data bus must be respected. The markings to identify the polarity can vary by manufacturer. The following table summarizes the most common identification labels for Modbus RTU data bus polarity.

Controller	Typical Data Bus Connection Terminals		
	Inverting	Non-inverting	Reference
ECB Series Controllers	NET –	NET +	S

Table 27: Common Identification Labels for Modbus RTU Data Bus Polarity for Distech Controls' Products

Controller	Typical Data Bus Connection Terminals		
	Inverting	Non-inverting	Reference
Common identification labels for Modbus RTU data bus polarity by other Manufacturers	D0	D1	SC, C, or C
	A or A’	B or B’	Common
	Data –	Data +	Data 0V

Table 28: Common Identification Labels for Modbus RTU Data Bus Polarity for other Manufacturers

When interfacing with Modbus RTU devices from other manufacturers, refer to the documentation provided with the device to correctly wire the device.

Maximum Number of Modbus RTU Devices on a Data Bus Segment and Baud Rate

The number of Modbus devices supported by an ECY Series Controller is software limited according to the controller model purchased. See the controller’s datasheet for more information. For ECY Series Controller models that are not software limited, the controller can support a combined maximum of 32 Modbus RTU and Modbus TCP devices.

Data Bus Segment Addressing Range for Modbus RTU Devices

The Modbus RTU device address range is 1 to 254. Address 0 is used to broadcast messages to all slave devices and write only. When address 0 is used to broadcast a message, there is no confirmation that the message was properly received by any slave device.

However, it is recommended that any given data bus segment have no more than 50 devices, when a baud rate of 19 200 or higher is used for the Modbus RTU Data Bus. A repeater counts as a device on each data bus segment to which it is connected.

Baud Rate

Most devices will have a range of baud rate settings and possibly an AUTO setting that detects the baud rate of other devices transmitting on the data bus and adjusts the baud rate of the device accordingly. Typical baud rates are 9600, 19 200, 38 400, and 76 800. The baud rate setting determines the rate at which data is sent on the Modbus RTU data bus.

All devices on the data bus must be set to the same baud rate. Therefore, the chosen baud rate must be supported by all devices connected to the data bus.

The recommended baud rate is 38 400.

We recommend that you:

- Set the baud rate of two controllers on a Modbus RTU Data Bus Segment to the same baud rate to provide failover protection.

  For example, set the baud rate of the ECY Series Controller (if equipped) and one other controller to 38 400 baud. If the ECY Series Controller becomes unavailable and there is a power cycle, the controller will set the baud rate for the Modbus RTU Data Bus.

- Set all other devices to automatically detect the baud rate, if this option is available.

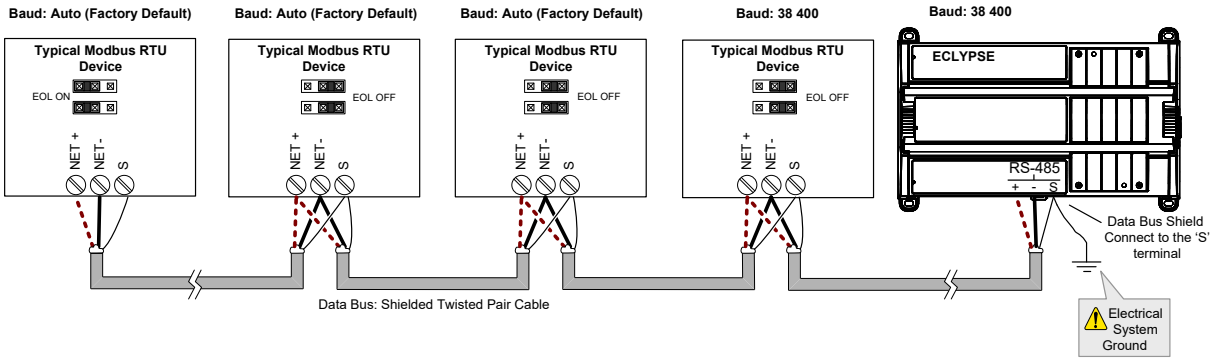


Figure 131: Setting the Baud rate on two Controllers on a Modbus RTU Data Bus Segment for Failover Protection

Set the Modbus network communication parameters with EC-*gfx*Program in the Resources Configuration window, Modbus Device block.

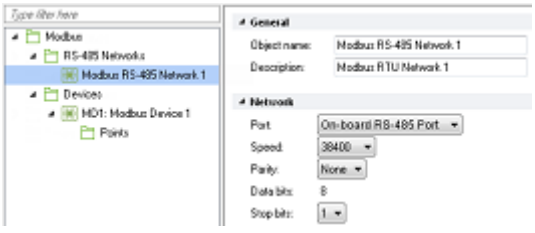


Figure 132: Setting the Modbus Network Communication Parameters in EC-gfxProgram's Resources Configuration Window

See the EC-*gfx*Program User Guide for more information.

Data Bus Physical Specifications and Cable Requirements

Cables composed of stranded conductors are preferred over solid conductors as stranded conductor cable better resist breakage during pulling operations. Distech Controls strongly recommends that the following data bus segment cable specifications be respected.

Parameter	Details
Media	Twisted pair, 24 AWG.
Shielding	Foil or braided shield
Shield grounding	The shield on each segment is connected to the electrical system ground at one point only; see *Data Bus Shield Grounding Requirements*.
Characteristic impedance	100-130 Ohms. The ideal is 100-120 Ohms
Distributed capacitance between conductors	Less than 100 pF per meter (30 pF per foot). The ideal is less than 60 pF per meter (18pF per foot)
Distributed capacitance between conductors and shield	Less than 200 pF per meter (60 pF per foot)
Maximum length per segment	1220 meters (4000 feet)
Data Rate	9600, 19 200, 38 400, and 76 800 baud
Polarity	Polarity sensitive
Multi-drop	Daisy-chain (no T-connections)
EOL terminations	120 ohms at each end of each segment
Data bus bias resistors	When VCC=5V: 510 ohms per wire (max. of two sets per segment) When VCC=3.3V (The APEX is 3.3V internal): 330 ohms per wire

Table 29: Modbus RTU Data Bus Segment Physical Specifications and Cable Requirements

Shielded cable offers better overall electrical noise immunity than non-shielded cable. Unshielded cable or cable of a different gauge may provide acceptable performance for shorter data bus segments in environments with low ambient noise.

Cable Type	Part Number	O.D. (Ø)
300 meters (1000 feet), 24 AWG Stranded, Twisted Pair Shielded Cable – FT6, Rated for Plenum Applications	CB-BACN6BL1000	3.75mm (0.148 in.)

Table 30: Distech Controls Recommended Cable Types for Modbus RTU Data Buses

Distech Controls Modbus RTU cable offers the best performance over the full range of baud rates, cable lengths, and number of connected devices. This is primarily due to lower conductor-to-conductor capacitance of this cable.

Data Bus Topology and EOL Terminations

Function of EOL Terminations

The first and last device on the data bus must have End-of-Line (EOL) termination resistors connected across the two data lines/wires of the twisted pair. These resistors serve the following purposes:

- EOL terminations dampen reflections on the data bus that result from fast-switching (high-speed rising and falling data edges) that otherwise would cause multiple data edges to be seen on the data bus with the ensuing data corruption that may result. The higher the baud rate a data bus is operating at, the more important that EOL terminations be properly implemented. Electrically, EOL terminations dampen reflections by matching the impedance to that of a typical twisted pair cable.
- EIA-485 data bus transmitters are tri-state devices. Meaning, they can electrically transmit 1, 0, and an idle state. When the transmitter is in the idle state, it is effectively offline or disconnected from the data bus. EOL terminations serve to bias (pull-down and pull-up) each data line/wire when the lines are not being driven by any device. When an un-driven data bus is properly biased by the EOL terminations to known voltages, this provides increased noise immunity on the data bus by reducing the likelihood that induced electrical noise on the data bus is interpreted as actual data.

When to Use EOL Terminations

EOL terminations should only be enabled / installed on the two devices located at either end of the data bus. All other devices must have the EOL terminations disabled / uninstalled. If a Modbus RTU device at the end of the data bus does not have a built-in EOL termination, then add a 120 Ohm resistor across the device's terminals.

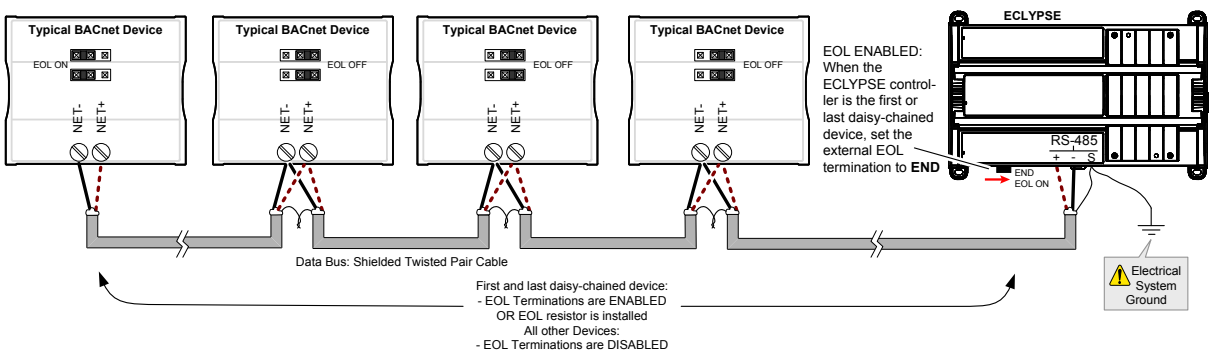


Figure 133: EOL Terminations Must be Enabled at Both the First and Last Device on the Data Bus

Devices with built-in EOL terminations are factory-set with the EOL termination disabled by default.

The *BACnet/IP to MS/TP Adapter* does not have EOL Termination (and Modbus RTU Data Bus biasing) capabilities to be used at the end of a Modbus RTU data bus. Instead, use the *BACnet/IP to MS/TP Router* for this application.

About Setting Built-in EOL Terminations

The APEX has built-in EOL terminations and biasing. It uses a switch located on the bottom of the controller to enable the EOL termination and/or bias based on where it is located on a data bus (usually at the end).

- If the APEX is located at the end of a data bus, set the switch to position to “END”.
- If the APEX is located at the end of a data bus and the data bus requires biasing, set the switch position to “END / BIAS”. There should be a minimum of one device (maximum of two) with biasing on the data bus.
- If the APEX is located at the middle of a data bus, set the switch position to “MID”. The controllers located at the ends of the data bus must have their EOL terminations installed or enabled.

If a controller at the end of the data bus does not have a built-in EOL termination, then add a 120 Ohm resistor across the device’s terminals.

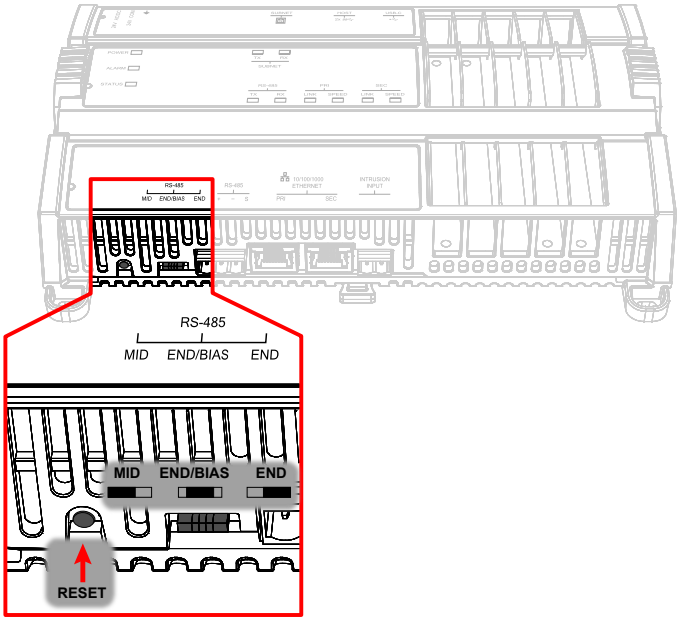


Figure 134: APEX EOL switch and reset button

ECB-PTU Series Line-Powered Controllers use DIP switches (found alongside those DIP switches used to set the MAC address) to enable the build-in EOL resistors and biasing circuitry.

ECB Series 24V-Powered Controllers have built-in EOL terminations. These Controllers use jumpers to enable the EOL resistors and biasing circuitry.

Refer to the device’s Installation Guide for how to identify and set a controller’s built-in EOL terminations.

Only a Daisy-Chained Data Bus Topology is Acceptable

Use a daisy-chained Modbus RTU data bus topology only. No other data bus topology is allowed.

Only linear, daisy-chained devices provide predictable data bus impedances required for reliable data bus operation.

Only a daisy-chained data bus topology should be specified during the planning stages of a project and implemented in the installation phase of the project.

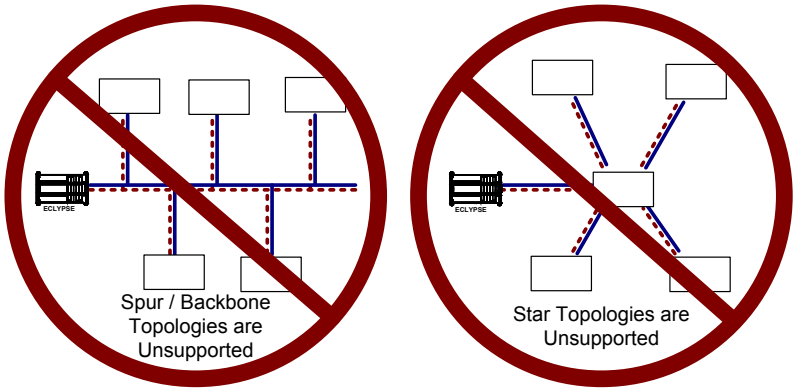


Figure 135: Unsupported Modbus RTU Data Bus Topologies

Data Bus Shield Grounding Requirements

The EIA-485 data bus standard requires that the data bus must be shielded against interference. A Modbus RTU data bus must also be properly grounded.

The data bus' cable shields must be twisted together and connected to the S or shield terminal at each ECY Series Controller. Keep the cable shield connections short and take steps at each device to isolate the cable shield from touching any metal surface by wrapping them with electrical tape, for example. Note that for ECY Series Controllers, the data bus' cable shield provides the ground reference for the data bus. If the controller is at the end of the BACnet MS/TP data bus, simply connect the data bus shield to the S terminal.

Grounding the shield of a data bus segment in more than one place will more than likely reduce shielding effectiveness.

Modbus RTU Data Bus Shield Grounding Requirements

The shield on each data bus segment must be connected to the electrical system ground at one point only, for example, at the ECLYPSE Controller, as shown below.

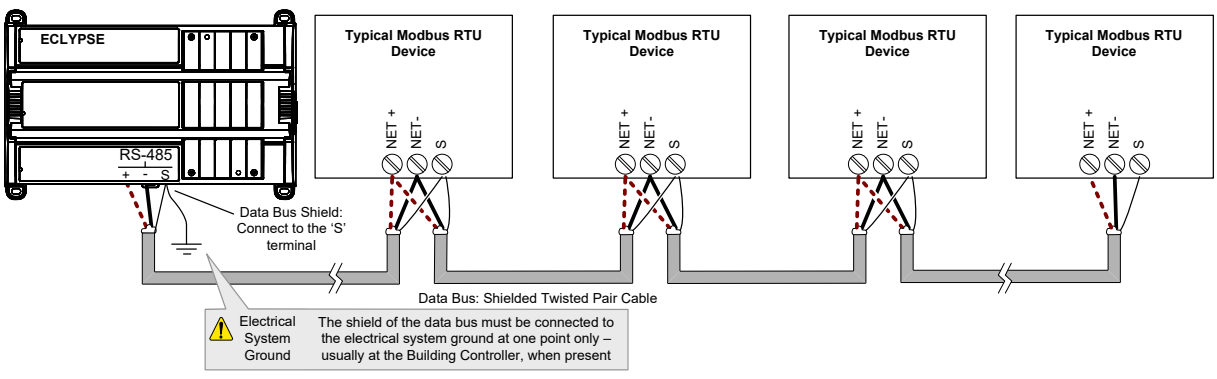


Figure 136: Typical Cable-Shield Grounding Requirements for a Modbus RTU Data Bus Segment with an ECLYPSE Controller located at the End of the Data Bus

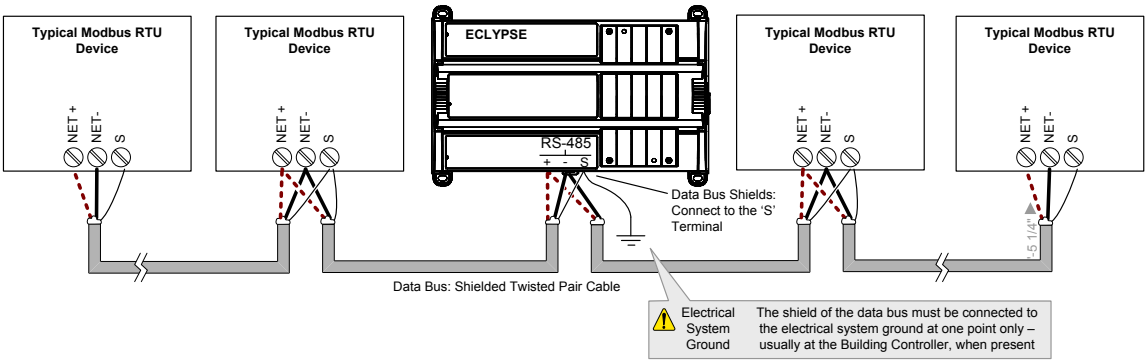


Figure 137: Typical Cable-Shield Grounding Requirements for a Modbus RTU Data Bus Segment with an ECLYPSE Controller located in the Middle of the Data Bus

Device Addressing

Device addressing allows the coordinated transfer of messages between the master (the ECY Series Controller) and the slave Modbus RTU device. For this, each device connected to the Modbus RTU data bus is identified by its address.

About the Device Address

Each slave device must have its own unique address number in the range from 1 to 247.

Refer to the device's hardware installation guide for information about how to set its address number.

Set the Modbus device parameters with EC-*gfx*Program in the **Resources Configuration** window, **Modbus Device** block.

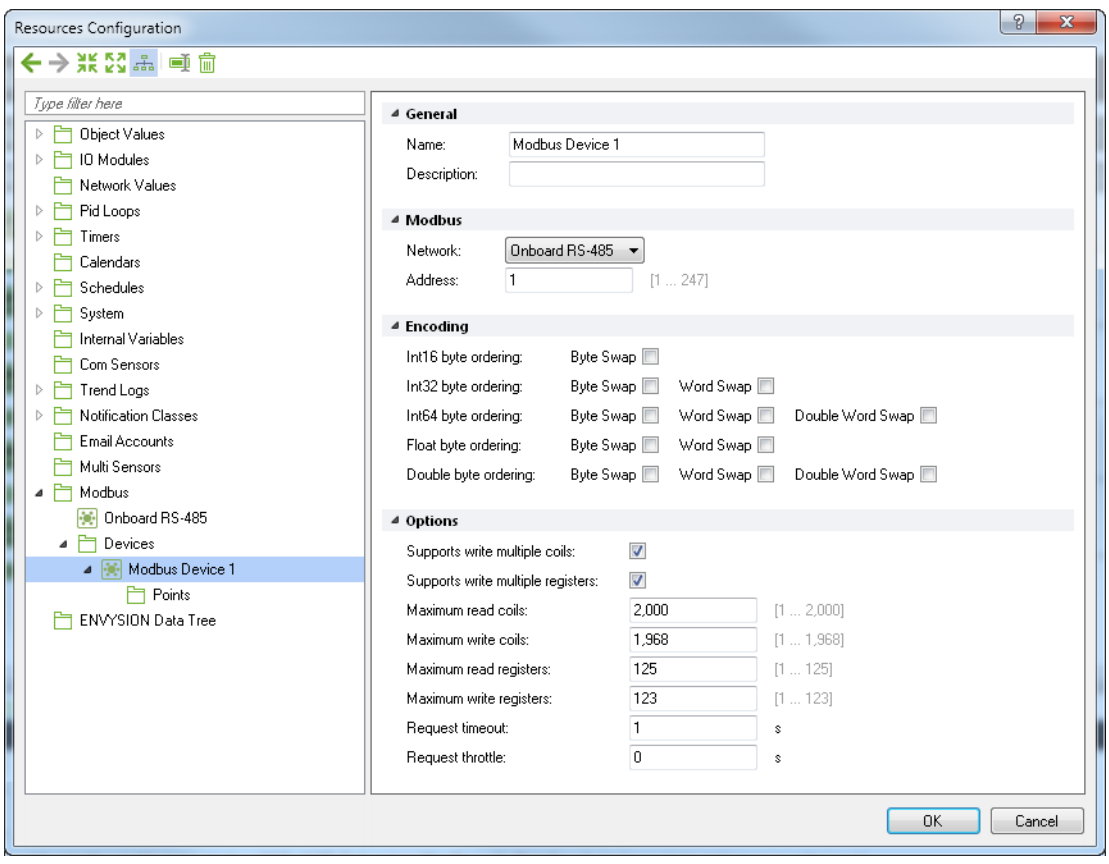


Figure 138: Setting the Modbus Device Parameters in EC-gfxProgram's Resources Configuration Window

See the EC-*gfx*Program User Guide for more information.

CHAPTER 15
Resetting or Rebooting the Controller

This chapter describes how to recover control over the controller by resetting it to the factory default settings.

Resetting or Rebooting the Controller

The reset button is a blue button located on the bottom of the ECLYPSE controller on the far left. Depending on the amount of time the reset button is held down, different actions are taken by the controller. When pressing and holding the reset button, the status LED will blink once at 5 seconds, once at 10 seconds, and once at 20 seconds.

Hold reset for	To
5 seconds	Restart / reboot the controller.
10 seconds	Reset both Ethernet and Wi-Fi IP addresses back to factory default settings.
20 seconds	Reset the controller to its factory default settings. User accounts (user names and passwords) will also be reset to the factory default settings and the controller's license and HTTPS security certificates will be cleared. When the reset process begins, the power light on the controller will go out momentarily, and the status light will flash intermittently until the controller has fully rebooted.

Always backup the controller's license through the controller's Web interface before you hold the controller's reset button for 20 seconds. Once the controller reboots, you will have to install the license through the controller's Web interface.

To backup and install the license, see *System Settings*. Click **Export To PC** to backup the controller's license to your PC. Click **Import From PC** to restore the controller's license file from your PC.

After you hold the controller's reset button for 20 seconds, the controller's HTTPS security certificates will be regenerated. If you use HTTPS to connect to the controller, you will no longer be able to connect to the controller from any PC that was used in the past to connect to the controller unless you delete the old HTTPS security certificate from these PCs. See *Removing a Certificate*.

CHAPTER 16
ECY Controller Troubleshooting

You can use this Troubleshooting Guide to help detect and correct issues with the ECLYPSE Series controllers.

Symptom	Possible Cause	Solution
Controller is powered but does not turn on	Fuse has blown (for 24V controllers)	Disconnect the power. Check the fuse integrity. Reconnect the power.
	Power supply polarity	Verify that consistent polarity is maintained between all controllers and the transformer. Ensure that the COM terminal of each controller is connected to the same terminal on the secondary side of the transformer. *See DHCP Versus Manual Network Settings*.
	The device does not have power / poor-quality power (for 24V controllers)	Verify that the transformer used is powerful enough to supply all controllers. See *Transformer Selection and Determining the Maximum Power Run Length*.
Device does not communicate on the BACnet MS/TP network	Absent or incorrect supply voltage (for 24V controllers)	1. Check power supply voltage between 24VAC/DC and 24V COM pins and ensure that it is within acceptable limits (±15% for 24V controllers). 2. Check for tripped fuse or circuit breaker.
	Overloaded power transformer (for 24V controllers)	Verify that the transformer used is powerful enough to supply all controllers. See *Transformer Selection and Determining the Maximum Power Run Length*.
	Network not wired properly	Double check that the wire connections are correct.
	Absent or incorrect network termination	Check the network termination(s).
	Max Master parameter	Configure the **Max Master** to the highest MAC Address of any device on the MS/TP data bus. See *Setting the Max Master and Max Info Frames*.
	There is another controller with the same MAC Address on the BACnet MS/TP data bus	Each controller on a BACnet MS/TP data bus must have a unique MAC Address. Look at the MAC Address DIP switch on the faceplate of each controller. If it is set to 0 (all off), use an Allure EC-Smart-Vue sensor to check the MAC Address.
	There is another controller with the same Device ID on the BACnet intranetwork	Each controller on a BACnet intranetwork (the entire BACnet BAS network) must have a unique Device ID. Use an Allure series communicating sensor to check the Device ID of each controller. See *Adopting a Numbering System for MAC Addresses, Device Instance Numbers, and Network Numbers*.
	BACnet data bus polarity is reversed.	Ensure the polarity of the BACnet data bus is always the same on all devices. See *BACnet MS/TP Data Bus is Polarity Sensitive*.
	Cut or broken wire.	Isolate the location of the break and pull a new cable.
	The BACnet data bus has one or more devices with the same MAC Address.	See *Adopting a Numbering System for MAC Addresses, Device Instance Numbers, and Network Numbers*.
	The baud rate for all devices are set to AUTO	At least one device must be set to a baud rate, usually the data bus master. See *Baud Rate*.
	The device is set to a MAC Address in the range of 128 to 255.	See if the STATUS LED on the device is showing a fault condition. See *LED Fault Condition Interpretation for ECB Devices* for a list of fault codes. This range is for slave devices that cannot initiate communication. All Distech Controls' devices are master devices and must their MAC Address set accordingly. See *Device Addressing*.
	The maximum number of devices on a data bus segment has been exceeded.	Use a repeater to extend the BACnet data bus. See *Maximum Number of BACnet MS/TP Devices on a Data Bus Segment and Baud Rate*.

Symptom	Possible Cause	Solution
The STATUS LED is blinking	The device has auto-diagnosed a fault condition	See *LED Fault Condition Interpretation for ECB Devices* for a list of fault codes.
Controller communicates well over a short network BACnet MS/TP network, but does not communicate on large network	Network length	Check that the total wire length does not exceed the specifications of the Network Guide. See *Data Bus Physical Specifications and Cable Requirements*.
	Wire type	Check that the wire type agrees with the specification of the Network Guide: See *Data Bus Physical Specifications and Cable Requirements*.
	Network wiring problem	Double check that the wire connections are correct.
	Absent or incorrect network termination	Check the network termination(s). Incorrect or broken termination(s) will make the communication integrity dependent upon a controller's position on the network.
	Number of controllers on network segment exceeded	The number of controllers on a channel should never exceed 50. Use a router or a repeater: See *Data Bus Segment MAC Address Range for BACnet MS/TP Devices*.
	Max Master parameter	Configure the maximum number of master device on the MS/TP network in all devices to the controller's highest MAC address used on the MS/TP trunk. See *BACnet MS/TP Data Bus Token-Passing Overview*.
Hardware input is not reading the correct value	Input wiring problem	Check that the wiring is correct according to the module's hardware installation manual and according to the peripheral device's manufacturer recommendations.
	Open circuit or short circuit	Using a voltmeter, check the voltage on the input terminal. For example, for a digital input, a short circuit shows approximately 0V and an open circuit shows approximately 5V. Correct wiring if at fault.
	Configuration problem	Using the controller configuration wizard, check the configuration of the input. Refer to the controller's user guide for more information.
	Over-voltage or over-current at an input	An over-voltage or over-current at one input can affect the reading of other inputs. Respect the allowed voltage / current range limits of all inputs. Consult the appropriate datasheet for controller input range limits.
Hardware output is not operating correctly	Fuse has blown (Auto reset fuse, for 24V controllers)	Disconnect the power and outputs terminals. Then wait a few seconds to allow the auto-reset fuse to cool down. Check the power supply and the output wiring. Reconnect the power.
	Output wiring problem	Check that the wiring is correct according to the module's hardware installation manual and according to the peripheral device's manufacturer.
	Configuration problem	With EC-*gfx*Program, check the configuration of the output; for example, is it enabled? Refer to the EC-*gfx*Program User Guide for more information.
	0-10V output, 24VAC powered actuator is not moving	Check the polarity of the 24VAC power supply connected to the actuator while connected to the controller. Reverse the 24VAC wire if necessary.

Table 31: Troubleshooting Controller Symptoms

ECB Device LED Interpretation	Description	Solution
RX LED not blinking	Data is not being received from the BACnet MS/TP data bus.	If there is no communication, see *Troubleshooting Controller Symptoms*.
TX LED not blinking	Data is not being transmitted onto the BACnet MS/TP data bus.	
POWER constant on	Power is available at the device. However, this does not mean that the quality of supplied power is good. See Power Supply Requirements for 24VAC-Powered Controllers on page 163.	If not lit, see *Power Supply Requirements for 24VAC-Powered Controllers* for the power requirements.
STATUS blinking	See following table.	-

Table 32: LED Fault Condition Interpretation for ECB Devices

Device STATUS LED blink patterns	Status	Description
One fast blink	Initialization	The device is starting up.
The STATUS LED is always OFF (Not applicable to ECB-PTU Series)	No anomaly	Normal operation.

Table 33: STATUS LED Interpretation for Normal Operation with ECB Devices

Action	Recommendation
Properly terminate the BACnet MS/TP data bus	EOL terminations must be enabled / installed at either end of the data bus only. See *When to Use EOL Terminations*.
Avoid duplicate MAC Addresses	Verify that no device has a duplicate MAC Address by checking the MAC Address DIP switch settings on all devices on the data bus, including segments connected by a repeater. If necessary, isolate devices from the data bus to narrow-down the number of devices that may be at fault.
All devices must be set to the same baud rate	When all devices are set to AUTO baud rate, at least one device must be set to a baud rate, usually the data bus master. See *Maximum Number of BACnet MS/TP Devices on a Data Bus Segment and Baud Rate*.
The data bus is polarity sensitive	Ensure that the polarity of all data bus wiring is consistent throughout the network. See *BACnet MS/TP Data Bus is Polarity Sensitive*.
Do not overload the data bus with Change of Value (COV) reporting	COV reports create the most traffic on the BACnet MS/TP data bus. Set the COV report rate to the largest value that provides acceptable performance. Only map COV reports for values that are necessary. For mapped analog points that are continuously changing, try increasing the COV increment on these points or set the COV minimum send time flag to true to send the value at a regular frequency.
Do not leave address holes in the device's MAC Address range	Assign MAC Address to device starting at 3, up to 127. Do not skip addresses. Set the maximum MAC Address in the Controller to the final MAC Address number actually installed. **NOTE:** The physical sequence of the MAC Address of the devices on the data bus is unimportant: For example, the MAC Address of devices on the data bus can be 5, 7, 3, 4, 6, and 8.
Only daisy-chained devices are acceptable	Eliminate T-taps and star configurations. Use a router to connect a data bus spur.
Connect no more than five devices to a power supply transformer (for 24V controllers)	BACnet MS/TP devices require good power quality. See *Power Supply Requirements for 24VAC-Powered Controllers*.

Table 34: Verify that the Following Recommendations have been Carried Out Before Calling Technical Support

CHAPTER 17
Allure EC-Smart-Vue Communicating Sensor Troubleshooting

Symptom	Status	Description
When the Allure EC-Smart-Vue sensor is connected to a Controller, the LCD display on the sensor is blank with the backlight ON for about 30 to 45 seconds	Firmware upgrade in progress	Wait for the upgrade to complete. Do not disconnect the Allure EC-Smart-Vue sensor from the controller as the upgrade will only restart once it is reconnected.

Table 35: Allure EC-Smart-Vue Sensor Normal Operation

Symptom	Possible Cause	Solution
Allure EC-Smart-Vue sensor screen is blank & back light is off	Is the Allure EC-Smart-Vue sensor connected to the controller?	Verify that the Allure EC-Smart-Vue sensor is connected to the controller and that the patch cables are plugged-in to the connectors. See *Cat 5e Cable Subnetwork Data Bus* for more information.
	Is power being supplied to the controller?	There may be no power being supplied from the controller. Check if the controller has power or if the controller's internal fuses have blown or tripped.
	Is the cable connected to the controller and Allure EC-Smart-Vue sensor?	Verify wiring.
	Was the patch cable made onsite?	Verify that the RJ-45 crimp connectors were installed on the cable correctly. See *Cat 5e Cable Subnetwork Data Bus* for more information.
Device is not communicating with controller	Is the address correctly set to a unique address?	Each Allure EC-Smart-Vue sensor must be set to a unique address for each controller. See *Commissioning a Connected VAV Controller with an Allure EC-Smart-Vue Sensor*.
	Is the device too far from controller?	Verify the distance between the device and the controller. See *Subnetwork Data Bus Length*.
	Is there a configuration problem?	With EC-*gfx*Program, check the configuration of the sensor, for example, is it enabled? Refer to the EC-*gfx*Program User Guide for more information.
	Have the subnetwork EOL settings been correctly set?	Only the last module on the subnetwork data bus must have its EOL termination set to ON. See the figures in section *EOL Terminations*.
Allure EC-Smart-Vue sensor motion detector window indicator is always ON	Does the connected controller have Allure EC-Smart-Vue sensor firmware that supports the motion and CO_2 sensor?	When the Allure EC-Smart-Vue sensor is connected to a controller, its firmware is loaded from the controller. In this case, the controller has an earlier version of Allure EC-Smart-Vue sensor firmware that does not support the motion or CO_2 sensor. To upgrade to the latest Allure EC-Smart-Vue sensor firmware, download the firmware from the Software Center and refer to the firmware upgrade procedure in the EC-*gfx*Program User Guide.
The Motion or CO_2 output of the associated ComSensor block always reads NULL in EC-*gfx*Program		
The CO2 sensor readings are too high, too low, or inconsistent between sensors	Immediately after installing the Allure EC-Smart-Vue sensor with CO_2 sensors, are the CO_2 sensor readings incoherent?	If the CO_2 sensor readings seem unusual or show inconsistencies between sensors in the same building right after installation, the following reasons should be taken into consideration: -Concentration levels in each space may be different -The installer may have unintentionally blown into the sensor while installing it.

Symptom	Possible Cause	Solution
		-The sensor may have been dropped or mishandled during shipment causing a minor shift in the original factory calibration. Allow up to 14 days of operation (without power interruptions) for the sensor to calibrate itself according to its new environment.

Table 36: Troubleshooting Allure EC-Smart-Vue Sensor Symptoms

Symptom	Possible Cause	Solution
Clock icon flashing for 15 seconds	Cannot communicate with controller.	Wait for the communication link to the controller to be established. Verify wiring. Verify that all Allure EC-Smart-Vue sensor's Subnet IDs are unique for this controller. See *Setting the Allure EC-Smart-Vue Sensor's Subnet ID Address*.
After 15 seconds: Error code 1 with Bell icon		
Error code 2 with Bell icon	Invalid configuration.	In EC-*gfx*Program, resynchronize the code with the controller. Contact Distech Controls Technical Support.
Error code 3 with Bell icon	Allure EC-Smart-Vue sensor is not properly configured in the controller	With EC-*gfx*Program, check the configuration of the sensor, for example, is the ComSensor block enabled? Refer to the EC-*gfx*Program User Guide for more information.

Table 37: Error code Interpretation for Allure EC-Smart-Vue Sensor Symptoms

CHAPTER 18
Wi-Fi Network Troubleshooting Guide

Any wireless system consists of two or more Wi-Fi transceivers and a radio propagation path (Radio Path). Problems encountered can be any of the following.

Symptom	Possible Cause	Solution
Wi-Fi communications are inexistent or intermittent	Presence of a low power jammer	If the low power jammer is close to the transceiver antenna, move low power jammer (PC, telephone, etc.) at least 6.5 feet (2 m) away from transceiver antenna.
		Change the Wi-Fi channel on the router. Use a Wi-Fi surveying or Wi-Fi stumbling tool on a laptop computer to identify unused Wi-Fi channels that may provide a better interference-free radio path.
		Move the Wi-Fi Adapter's position where it has a clear line of sight to the router.
		Move the wireless router's position. Try moving the router to the center of the room where it has a clear line of site to each wireless device.
	Presence of a high-power jammer	Remove high power jammer if possible. If not, you will have to accept strong range reduction or add another wireless router closer to the controller(s).
		Use a wired Ethernet connection to the controller.
	Defective Wi-Fi Adapter	Exchange the wireless dongle with another Wi-Fi Adapter. If the dongle is found to be defective, replace the dongle.
	The maximum wireless operating range has been exceeded	Add another wireless router closer to the controller(s).
	The controller has a known technical issue	Upgrade the controller's firmware. See *User Management*.
The Wi-Fi Adapter has been tested functional and there is no jammer in the field to interfere with the signal.	Radio signal path might be obstructed	If a new screening or metal separation wall has been installed since the network was set up, try moving the receiver to see if the issue is corrected.
	Router may have a known technical issue	Upgrade the router's firmware. See the manufacturer's Website.

Table 38: Troubleshooting Wi-Fi Network Symptoms

CHAPTER 19
Single Sign On (SSO) Troubleshooting

You can use this Troubleshooting Guide to help detect and correct issues with the SSO functionality. Even though the following table provides a work around to the issues, in general, we highly recommend that you always find the solution to any problem you may encounter.

Symptom	Possible Cause	Work Arounds	Solution
Recovery password is requested in the Web browser.	SSO Server is down or a networking or connection issue has occured.	Enter your recovery password.	Verify the server status and server connections. Verify the network connectivity. Reconfigure the SSO parameters. See *Setting Up the SSO Functionality*
When launching EC-*gfx*Program from your desktop and after entering your login credentials, connection fails.	SSO Server is down or a networking or connection issue has occurred.	Login using the SSO recovery username **ssorecovery** and then enter your recovery password. This username can only be used in recovery mode.	Verify the server status and server connections. Verify the network connectivity. Reconfigure the SSO parameters. See *Setting Up the SSO Functionality*
In xpress*Network* Utility, authentication fails	SSO Server is down or a networking or connection issue has occurred.	Login using the SSO recovery username: **ssorecovery**, and then enter your recovery password. This username can only be used in recovery mode.	Verify the server status and server connections. Verify the network connectivity. Reconfigure the SSO parameters. See *Setting Up the SSO Functionality*
When launching EC-*gfx*Program through the EC-Net launch wizard, authentication fails. The and this is requested, the device connection status led is off (device is offline).	SSO Server is down or a networking or connection issue has occurred.	Launch EC-*gfx*Program from your desktop and login using the SSO recovery username: **ssorecovery** and then enter your recovery password This username can only be used in recovery mode.	Verify the server status and server connections. Verify the network connectivity. Reconfigure the SSO parameters. See *Setting Up the SSO Functionality*

DISTECH CONTROLS™