

Honeywell

ADVANCED PLANT CONTROLLER

Niagara



Installation Instruction and Commissioning Guide

TABLE OF CONTENT

General Safety Information	7
Safety Information as per EN61010-1 (EN60730-1 certification is under process)	7
Regulations	8
FCC Regulation	8
Canadian Regulatory Statement	8
RESTRICTIONS IN THE 5 GHZ BAND	8
RESTRICTIONS DANS LA BANDE DE 5 GHZ	8
Professional Installation Warning	8
DISPOSAL AND RECYCLING	9
Technical Information.....	10
Trademark	10
Product Description	10
Software tool	10
Technical Details	10
Default IP Address	11
Installation	11
Niagara License	12
Get the Advanced Controller Niagara License and Certificate	12
Install the Niagara license	12
Automatic Licensing	12
Manual Licensing	12
Niagara help documents	13
To access the Niagara Help system:	13
To access the Niagara Help documents	14
Power supply	15
Transformers	15
Honeywell Transformers	15
Switch Power Supply	15
Advanced Plant Controller Installation Instruction and Commissioning Guide	2

Fusing	15
Power Supply of Field Devices	15
Example 1: Power Supply via Controller Using Panel Module	16
Example 2: Power Supply via Separate Transformer	16
Wiring and Set-up	17
General Safety Considerations	17
Wiring Terminals	17
Connecting Power Supply	18
Earth Grounding	18
Cable Specifications	19
Power Supply Cable Specifications	19
Field Device Power Supply Cable Specifications	19
Communication Bus Cable Specifications	19
RS485 Bus Cable Specifications	19
Earth Grounding	20
Advanced Plant Controller and SELV	20
Niagara Advanced Plant Controller System and EN60204-1	20
General Information about EN60204-1	20
When is EN60204-1 Applicable to Niagara Plant Controller System?	20
Functional EMC Grounding	21
Interfaces	22
HMI LED	22
Wi-Fi and Bluetooth LED	23
Ring LED	24
General Information on the RS485 Standard	25
RS485 LEDs	25
Panel Bus	25
BACnet MS/TP	26
Modbus	28
Mbus	29
Communication Baud Rates	31
Connection to Buses	32
Terminator Switch	33
Ethernet Interfaces and LEDs	33
Service Button/Service Alarm LED	34
Terminal Assignment	37
Controller Terminal	38
Flow chart of Commissioning and Setup Work flow	39

Work Flow 1	39
Work Flow 2	41
Connect the Niagara-Installed PC.....	44
Option 1: USB 2.0 Device	44
Option 2: Standard Ethernet Interface	44
Front USB/Ethernet interface	45
RNDIS Driver	45
General architecture of the RNDIS Protocol	45
How to Enable RNDIS driver in the Advanced Plant Controller	46
To connect to the Niagara-installed PC using Ethernet port:	49
Getting Started	51
Connecting Advanced Plant Controller	51
Open a Platform	51
Open a New Platform	52
Open an Existing Platform	56
Commissioning the Advanced Plant Controller	58
Procedure for commissioning the Plant Controller	58
Set up a Station	67
Create a New Station	67
Copy a Station using Station Copier	69
Open the Station	72
Configure TCP/IP Settings	73
Import Licenses into License Manager	75
Change Date and Time	76
Install Additional Drivers	77
Setup and Configuring Advanced Plant Controller	78
Enable HonPlantControllerService	78
Enable LED Behavior	83
Email setup	86
Setting up email components	86
Configuring the EmailRecipient	88
Securing email	89
RSTP Configuration	90
Switch Port Configuration	94
HMI Device Configuration	104
BACnet Network	105
BACnet Rounting	105
Create a Station	105

Add BACnet network	105
Enable Routing	106
Add MS/TP Devices in the Advanced Plant Controller	109
Tuning the BACnet properties	111
Tuning Network Property	111
Tuning Local Device Property	112
BACnet/SC (Secure Connect)	113
IEEE 802.1X Configuration	113
Configuring Ports to Enable Web server Function	114
WiFi Configuration	116
Introduction	116
WiFi Specifications	116
Enable WiFi	116
Prerequisites:	116
Configuring WiFi Access Point mode	119
Configure Access Point IP Adapter	119
Configure Access Point Dhcp Server Settings	120
Configure Access Point Config	121
WiFi Access Point for local tool connections	124
Firmware Update using Distribution File Installer	125
CleanDist file Installation	131
Enable/Disable USB Backup and Restore	135
USB Backup and Restore using shell command	136
Procedure for USB backup and restore	136
Creating a USB backup	139
Restoring from a USB backup	140
Automatic Resetting Fuse	142
Connection Examples	143
Connection to Panel Bus I/O Modules Powered by a Separate Transformer	143
Connection to Panel Bus I/O Modules Powered by the Same Transformer as the Advanced Plant Controller	145
Connection to BACnet MSTP Buses with Shielding as Return path	147
Recommended connection for BACnet MSTP Buses with Separate Conductor as Return path	148
Connection for BACnet MSTP Buses with Shielding as Return path (non-isolated)	149
Connection for BACnet MSTP Buses with Separate Conductor as Return path (non-isolated)	150
Connection to Modbus Modules with Shielding as Return path	151
Connection to Modbus devices with Separate Conductor as Return path	152
Connection to Modbus devices with Shielding as Return path (non-isolated)	153
Connection to Modbus devices with Separate Conductor as Return path (non-isolated)	154

Connection to a I/O Module Powered by the Separate Transformer	155
Connection to a I/O Module Powered by a Same Transformer	156
Connection to M-Bus via Level Converter	157
Connection to HMI	158
Migrating an existing station to Advanced controller	159
Troubleshooting	161
Troubleshooting with LEDs of RS485 Interfaces 1, 2, 3	161
Troubleshooting with the Ethernet Interface LEDs	161
Troubleshooting with Controller configuration	162
Technical Literature	163

GENERAL SAFETY INFORMATION

- When performing any work (installation, mounting, start-up), all manufacturer instructions and in particular the Installation and Commissioning Instructions (31-00584-02) are to be observed.
- The Niagara Advanced Plant Controllers (including the N-ADV-133-H-B-W/N-ADV-133-H-B/N-ADV-133-H/N-ADV-134-H/N-ADV-112-H controller, Panel Bus I/O Module module, manual disconnect modules, and the auxiliary terminal packages) may be installed and mounted only by authorized and trained personnel.
- Rules should be followed for electrostatic discharge.
- If the Advanced Plant Controllers is modified, except by the manufacturer, all warranties concerning operation and safety are invalidated.
- Use only accessory equipment which comes from or has been approved by Honeywell.
- It is recommended that devices be kept at room temperature for at least 24 hours before applying power. This allows any condensation resulting from low shipping/storage temperatures to evaporate.
- The Advanced Plant Controllers must be installed in a manner (e.g., in a lockable cabinet), ensuring that uncertified persons have no access to the terminals.
- Investigated according to United States Standard UL-60730-1, UL-916, and UL60730-2-9 (Certifications are under process. EN61010-1 applies to the initial field trail units only).
- Investigated according to Canadian National Standard(s) C22.2, No. 205-M1983 (CNL-listed).
- Do not open the Advanced Plant Controller, as it contains no user-serviceable parts inside!
- According to LVD Directive 2014/35/EU and EMC Directive 2014/30/EU, CE declarations.
- Product standards are EN 60730-1 and EN 60730-2-9 (Certifications are under process. EN61010-1 applies to the initial field trail units only).

Safety Information as per EN61010-1 (EN60730-1 certification is under process)

The Advanced Plant Controllers is intended for integration and control within Smart Building Automation systems.

The Advanced Plant Controllers is an independently mounted electronic control system with fixed wiring.

The Advanced Plant Controllers is suitable for mounting in fuse boxes conforming with standard DIN43880 and having a slot height of max. 45 mm.

It is suitable for the Advanced - DIN35 mm, type A standard panel rail (both horizontal and vertical rail mounting possible).

The Advanced Plant Controller is used to build HVAC control and is suitable only for non-safety controls for installation on or in appliances.



NOTE:

The initial field trial units, are certified with EN61010-1. The released products are planned to be certified with EN60730-1.

Table 1. Safety Information as per EN61010-1 (EN60730-1 certification under process)

Electric Shock Protection	SELV
Pollution Degree	Pollution Degree 2, suitable for use in industrial environments.
Installation	Class 3
Over voltage Category	24 V-powered controls: Category I
Rated Impulse Voltage	330 VAC for Category I (SELV).
Automatic Action	Type 1.C (micro interruption for the relay outputs).
Software Class	Class A
Enclosure	IP20
Ball-pressure Test Temperature	>75 °C for all housing and plastic parts. >125 °C in the case of devices applied with voltage-carrying parts, connectors, and terminals.
Electromagnetic Interference	Tested at 230 VAC, with the modules in normal condition.
System Transformer	Europe: safety isolating transformers according to IEC61558-2-6 U.S.A. and Canada: NEC Class-2 transformers.



IMPORTANT:

The below SKU's and there configurations are not part of this release. The information and configurations are in development stage and kept as a reference to upcoming releases.

1. N-ADV-133-H-B-W
2. N-ADV-133-H-B

REGULATIONS

FCC Regulation

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.



NOTE:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

However, there is no guarantee that interference will not occur in a particular installation.

Suppose this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on. In that case, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

Canadian Regulatory Statement

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. l'appareil ne doit pas produire de brouillage, et
2. l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

CE Statement: The WLAN function for this device is restricted to indoor use only when operating in the 5150 to 5350 MHz frequency range.

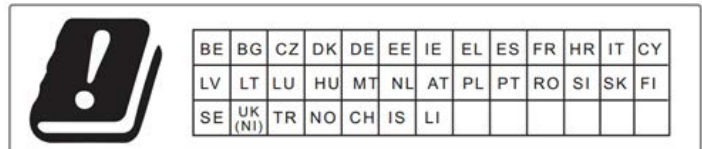


Figure 1. CE Statement

EMF Statement: To comply with the RF exposure requirement, a separation distance of 20 cm between the device and the human should be maintained.

Déclaration d'exposition Attention: Cet émetteur doit être installé pour fournir une distance de séparation d'au moins 20 cm de toute personne.

RESTRICTIONS IN THE 5 GHZ BAND

Within the 5.15 to 5.25 GHz band, UNII devices will be restricted to indoor operations to reduce any potential for harmful interference to co-channel Mobile Satellite System (MSS) operations.

RESTRICTIONS DANS LA BANDE DE 5 GHZ

Dans la bande de 5,15 à 5,25 GHz, les appareils UNII seront restreints aux opérations intérieures pour réduire toute possibilité d'interférence pouvant nuire aux opérations du Système satellite mobile dans le même canal(MSS).

Professional Installation Warning

- This device must be professionally installed, this should be noted on grantee.
- To maintain compliance, only the antenna types that have been tested shall be used.

- This device requires significant technology engineering expertise to understand the tools and relevant technology unavailable to the average consumer. Only a person professionally trained in the technology is competent.
- This device is not directly marketed or sold to general public.
- This radio transmitter IC:1609A-ADVBLEWIFI has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

DISPOSAL AND RECYCLING



WEEE DIRECTIVE

WEEE Directive 2012/2019/EC Waste Electrical and Electronic Equipment directive. This symbol on the product shows a crossed-out “wheelie-bin” as required by law regarding the Waste of Electrical and Electronic Equipment (WEEE) disposal. This indicates your responsibility to contribute in saving the environment by proper disposal of this Waste i.e. Do not dispose of this product with your other wastes. To know the right disposal mechanism please check the applicable law.

TECHNICAL INFORMATION

Trademark

- Spyder™ is a trademark of Honeywell International Inc.
- BACnet® is a registered trademark of ASHRAE Inc.
- Sylk™ is a trademark of Honeywell International Inc.

Product Description

N-ADV-133-H-B-W, N-ADV-133-H-B, N-ADV-133-H, N-ADV-134-H, and N-ADV-112-H Advanced Plant controller are designed for a wide variety of complex applications. These devices feature RS485 channels for MSTP, PanelBus, Modbus, M-Bus, and I/O module devices, Ethernet ports for BACnet™ IP devices, and RJ11 interface for HMI devices. These controllers also have touchflakes RS485-R to connect with multiple IOs in series and USB Type-C interfaces to connect with PC/laptop for serial communication. These controllers can be mounted on either a DIN rail or Wall mounted horizontally or vertically.

Software tool

Use Niagara workbench version 4.10 or higher to access the controller.

Technical Details

Please see “Advanced Plant Controller Datasheet” for below details. Document number: 31-00583 and Optimizer Advanced Datasheet: 31-00631.

- Ordering Information
- Accessories Parts
- Specification Data
- Electrical Data
- Power Consumption
- Current Consumption
- Operational Environment
- Standards
- Dimensions
- Software Licenses And Upgrades

Default IP Address

Table 2. Default IP Address

IP Address	Ethernet port 1  1 = 192.168.0.200 Ethernet port 2  2 = 192.168.2.200
Subnet Mask	255.255.255.0
RNDIS	USB1  1 = 192.168.255.241
Subnet Mask	255.255.255.0
Reserved IP address for WIFI	192.168.56.1
Subnet Mask	255.255.255.0



NOTE:

Based on Ethernet port selection the IP address will change. See [“Advanced Plant Controller Interface” on page 22](#). For RNDIS IP address, See [“RNDIS Driver” on page 45](#). The WIFI IP address and subnet is reserved but not used.

INSTALLATION

To install the Advanced Plant Controller refer the Mounting Instructions document (31-00553).

NIAGARA LICENSE

Advanced Controller should have the Niagara license before use. The license determines the number of points the controller can monitor and the duration of a software update agreement.

Get the Advanced Controller Niagara License and Certificate

The license files are created at the purchase time and stored on a central server. To license the Advanced Plant Controller, license and certificate files must be downloaded and installed on the controller. For license information See [“To install the Advanced Plant Controller refer the Mounting Instructions document \(31-00553\).” on page 11.](#)

Install the Niagara license

The Niagara license is emailed to you as a ZIP file containing a number of license and certificate files that need to be installed on the PC which will be used to commission the Advanced Plant Controller.

There are two ways to install the license and certificate

- [Automatic Licensing](#)
- [Manual Licensing](#)

Automatic Licensing

The easiest way to license the Advanced controller is to temporarily connect it to the Niagara installed PC/Laptop which is connected to Internet and install the license files from the server. See [“Connect the Niagara-Installed PC” on page 44.](#)

To automatically install the license files:

1. Once the platform is open double click License Manager. The License Manager is displayed.
2. Click **Import**.
3. Select **Import licenses** from the licensing server.
4. Once the process is complete a dialogue box is displayed, click **OK**.
5. Proceed to Connect to the Niagara-installed PC.

Manual Licensing

To manually get the Niagara workbench licensed:

1. Copy the ZIP file to the PC hard disk.
2. Extract all the files from the ZIP to an empty folder.



NOTE:

You will need to access unzipped files when running the Commissioning Wizard, and they will be installed as part of the commissioning process. – See [“Commissioning the Advanced Plant Controller” on page 58.](#)

3. Proceed to Connect to the Niagara-installed PC.

NIAGARA HELP DOCUMENTS

Niagara installed PC will have a library of Niagara documentation as a part of installation. User can access these documents in two ways.

- To access the Niagara Help system
- To access the Niagara Help documents

To access the Niagara Help system:

1. Open Niagara workbench and Click **Help** on the menu bar.

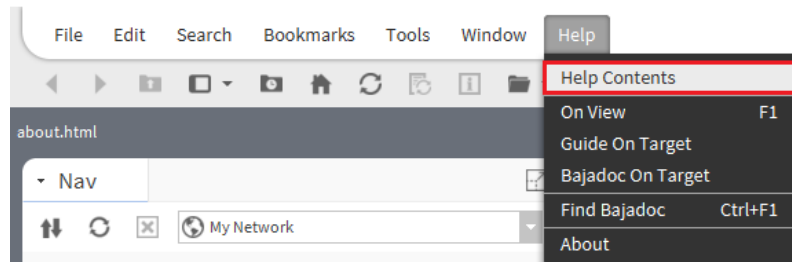


Figure 2. Niagara Help Contents

2. Select Help Contents. The Niagara Help window is displayed:

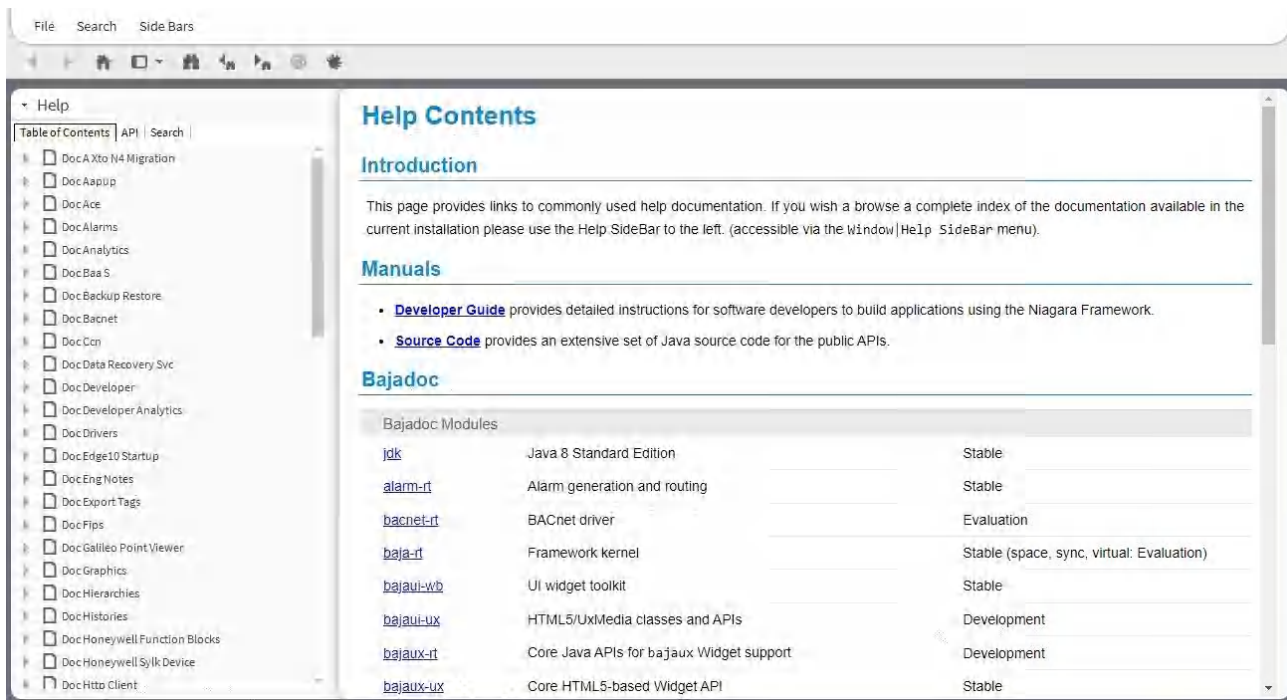


Figure 3. Niagara Help page

3. In the Help side bar search for required document with related key words and click the **search icon** or select **Table of Contents**.
4. Double-click on a topic to open it.

To access the Niagara Help documents

Niagara documents are stored in the “C drive” while installing the Niagara software. You can check the document by navigating to below drive folder.



Figure 4. Niagara Help document folder



NOTE:

The folder name may change based on the Niagara installer you use [“To access the Niagara Help system:” on page 13.](#)

POWER SUPPLY

Transformers

Honeywell Transformers

A transformer can power the Advanced Plant Controller. When determining total current consumption and selecting the appropriate transformer, consider the number of connected modules, accessories, and field devices.


NOTE:

In Europe, system transformer(s) must be safety isolating transformers according to IEC61558-2-6.

Table 3. Honeywell CRT Series Transformers (Europe)

Part No.	Primary Side	Secondary Side
CRT 2	220/230 VAC	24 VAC, 50 VA, 2 A
CRT 6	220/230 VAC	24 VAC, 150 VA, 6 A
CRT 12	220/230 VAC	24 VAC, 300 VA, 12 A


NOTE:

Controller is not intended to power up through USB.


NOTE:

In the U.S.A and Canada, NEC Class-2 transformers must be used.

Table 4. Honeywell 1450 Series Transformers (N. America)

Part No. 1450728 7	Primary Side	Secondary Side
-001	120 VAC	24 VAC, 50 VA
-002	120 VAC	2 x 24 VAC, 40 VA; 100 VA from separate transformer
-003	120 VAC	24 VAC, 100 VA; 24 VDC; 600 mA
-004	240/220 VAC	24 VAC, 50 VA

Table 4. Honeywell 1450 Series Transformers (N. America) (Continued)

Part No. 1450728 7	Primary Side	Secondary Side
-005	240/220 VAC	2 x 24 VAC, 40 VA; 100 VA from separate transformer
-006	240/220 VAC	24 VAC, 100 VA; 24 VDC, 600 mA


NOTE:

Standard commercially available transformers can also power the Advanced Plant Controller.

Switch Power Supply

The Advanced Plant Controller can be powered by a switch-mode DC power supply (rather than by a transformer) to reduce overall current consumption.

Fusing

The choice of appropriate fusing is dependent upon the given connection scenario (i.e., cable lengths and the use of a primary and/or secondary transformer) and the type of connected bus.

Table 5. Fusing

Designation	Description
F1	4 A, time-lag fuse (slow-blow), e.g., Littlefuse type 218.004.
F2	Depends upon field devices.
F3 (Field Bus, only)	8 A, time-lag fuse.
F4 (I/O Module Bus, only)	8 A, time-lag fuse or 12.5 A, time lag fuse (see “Connection to a I/O Module Powered by the Separate Transformer” on page 155).

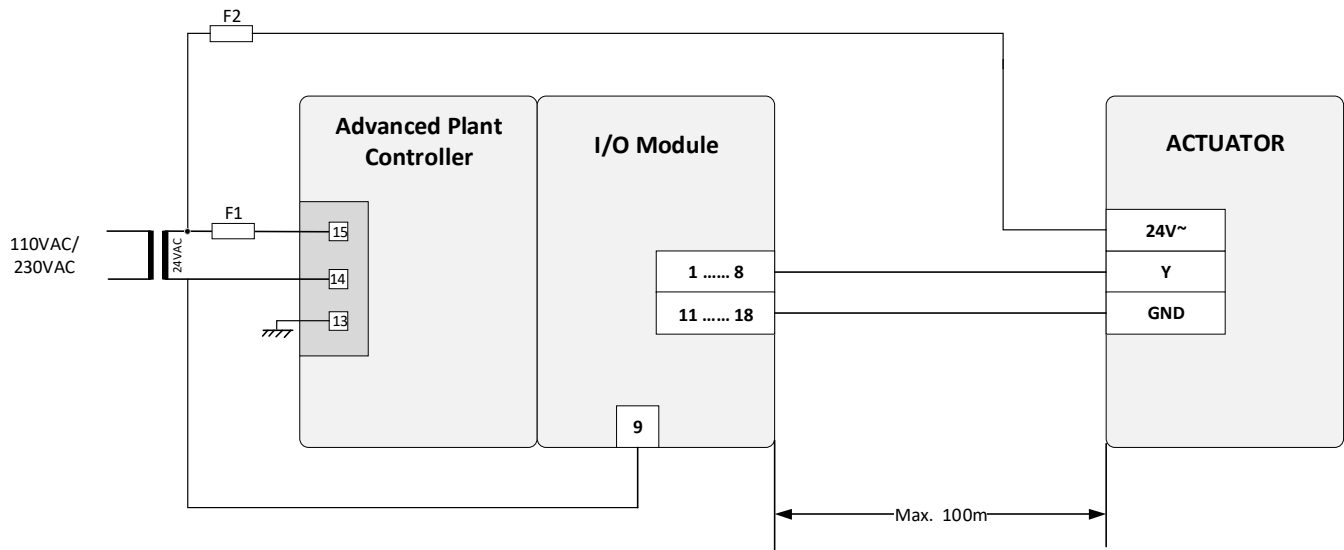
Power Supply of Field Devices

Field devices can be powered via the Advanced Plant Controller.

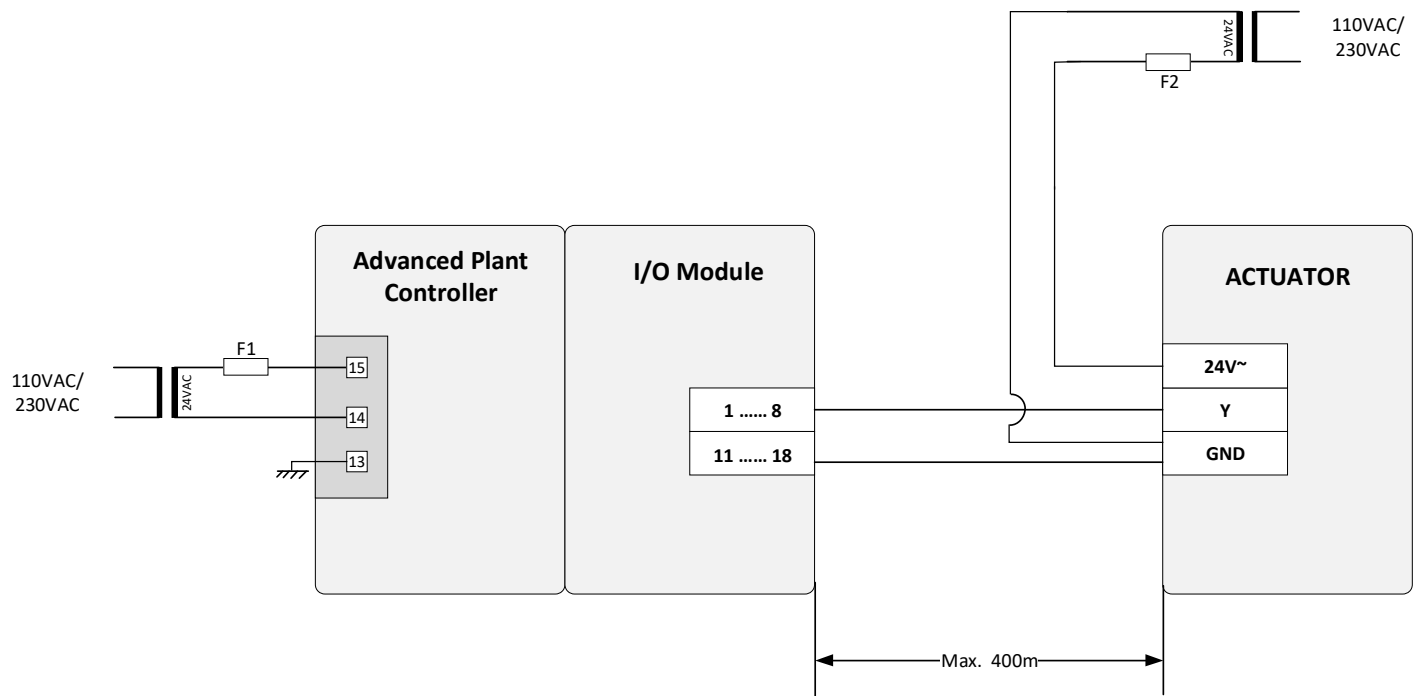
When determining the total current consumption and selecting the appropriate transformer, consider the number of connected modules, accessories, and field devices. Employing an additional transformer may be necessary. The fusing (F2) of active field devices depends on loads in use. Single-sided (secondary-sided) earth connection of the transformer is also possible. For more information, see [“Technical Literature” on page 163](#).

Example 1: Power Supply via Controller Using Panel Module

- 24 V actuator connected to an analog output module.
- Actuator less than 100 m away from the controller.

**Figure 5. Power supply of field devices via Panel Bus I/O module****Example 2: Power Supply via Separate Transformer**

- 24 V actuator connected to an analog output module.
- Actuator less than 400 m away from the controller.

**Figure 6. Power supply of field devices via a separate transformer**

WIRING AND SET-UP

General Safety Considerations

- When connecting the Advanced Plant Controller, VDE, National Electric Code (NEC) or equivalent, and any local regulations concerning grounding must be observed.
- Only qualified electricians may carry out electrical work.
- The electrical connections must be made at the terminals of the Advanced Plant Controller.



NOTE:

For Europe, only: To comply with CE requirements, devices with a voltage in the range of 50 to 1000 VAC or 75 to 1500 VDC and which are not provided with a supply cord and plug or with other means for disconnection from the supply having a contact separation of at least 3 mm in all poles must have the means for disconnection incorporated in the fixed wiring.

- Only copper conductors should be used for electrical connections.
- Only electrical cables/wires with an operating temperature at least 75° C should be used for electrical connection.



WARNING

Risk of electric shock or equipment damage!

- Do not touch any live parts in the cabinet.
- Disconnect the power supply before connecting or removing connections from controller terminals.
- Do not use spare terminals as wiring support points.
- Do not reconnect the power supply until you have completed the installation and proper connection.



CAUTION

Observe the precautions for handling electrostatic devices.

Wiring Terminals

The Advanced controllers are supplied with Screw terminals and can also be retrofitted with Push fit terminals if required. See [“Ordering Information” on page 2](#).



NOTE:

In some regions I/O modules can be ordered directly with either screw or push fit terminals.

Table 6. RS485 Interfaces 1,2, and 3 Wiring Terminals Specifications

Terminal Type	Stripping Length	Torque Value	Max. Plug Gauge
Screw (Type P1)	6-7 mm	4.425 lb-in (0.5 N-m)	26 to 12 AWG (0.1281-3.332 mm ²)
Push-in (Type P1)	9 mm	N/A	14 to 24 AWG Sol/Str (UL), 14-26 AWG Sol (UL), 0.2-2.5 mm ² Sol/Str (IEC)

Table 7. RS485 Interface 4 Wiring Terminals Specifications

Terminal Type	Stripping Length	Torque Value	Max. Plug Gauge
Screw (Type J4)	6-7 mm	4.425 lb-in (0.5 N-m)	26 to 12 AWG (0.1281-3.332 mm ²)
Push-in (Type J4)	9 mm	N/A	14 to 24 AWG Sol/Str (UL), 14-26 AWG Sol (UL), 0.2-2.5 mm ² Sol/Str (IEC)

Table 8. Power Supply Wiring Terminals Specifications

Terminal Type	Stripping Length	Torque Value	Max. Plug Gauge
Screw (Type P2)	6-7 mm	4.425 lb-in (0.5 N-m)	26 to 12 AWG (0.1281-3.332 mm ²)
Push-in (Type P2)	9 mm	N/A	14 to 24 AWG Sol/Str (UL), 14-26 AWG Sol (UL), 0.2-2.5 mm ² Sol/Str (IEC)

Terminals support both flexible and solid cables. Wires can be equipped additionally with ferrules.

Connect the power supply to the power supply terminals of the Advanced Plant Controller. See *“Power supply” on page 15*.

The factory default controller must be powered ON for a minimum of 10 hours for the first time to make the RTC function as intended.

The Advanced Plant Controller complies with SELV, so protective earth grounding is not required. However, a functional earth grounding for EMC is mandatory. For information, [See “Earth Grounding” on page 20.](#)



Cable Specifications

Power Supply Cable Specifications

The length of the power supply cable includes the length of the cables to connected modules.


NOTE:

The supply voltage must, in any case, be at least 19.2 VAC (24 VAC -20%).

Table 9. Power Supply Cable Specifications

Device	Cable Length	Cable cross-section
Niagara Advanced Plant Controller	Max. 3 m	Min. 1.5 mm ²
Panel Bus I/O	Max. 3 m	Min. 1.5 mm ²
DIO	Max. 1200 m	Min. 1.5 mm ²
M-Bus	> 3 m	Depends on Plug Gauge. See “Wiring Terminals” on page 17

Field Device Power Supply Cable Specifications

Table 10. Field Device Power Supply (24 VAC) Cable Specifications

Cable Length	Cable Cross-section
≤ 100 m (300 ft.), single transformer (See “Example 1: Power Supply via Controller Using Panel Module” on page 16.)	min. 1.5 mm ² (16 AWG)
≤ 400 m (1300 ft.), separate transformers (See “Example 2: Power Supply via Separate Transformer” on page 16.)	min. 1.5 mm ² (16 AWG)

Communication Bus Cable Specifications

Table 11. Communication Cable Specifications

Interface (Buses)	Cable Type
RS485 interfaces 1, 2, and 3 (Panel Bus, BACnet Bus, Modbus, M-Bus)	One or two pairs (depending on the application) of twisted pair complying with EIA485 standard (level IV, 22 AWG, solid core, non-shielded), e.g., J-Y-Y 2 x 2 x 0.8, or shielded wire.
RS485 interface R (Panel Bus, I/O Module Bus)	
Ethernet 1, 2 (Ethernet Bus)	Niagara Advanced Plant Controller can be used with CAT5, CAT6, and CAT47 cabling. Standard Ethernet cross-over cable, Cat-5, min. 10/100 MBaud, max. length of 100 m

RS485 Bus Cable Specifications

- An MSTP EIA-485 network shall use shielded, twisted-pair cable with a characteristic impedance between 100 and 130 ohms.
- Distributed capacitance between conductors shall be less than 100 pF per meter (30 pF per foot).
- Distributed capacitance between conductors and shield shall be less than 200 pF per meter.

EARTH GROUNDING

Advanced Plant Controller and SELV

To avoid the distribution of noise or earth ground potential differences over networks or other connections, the Advanced Plant Controller is designed to comply with SELV.

Furthermore, SELV offers the greatest possible safety against electrical impact.

To support SELV, all Honeywell external (CRT series) or internal transformers comply with standard EN60742. Earth grounding is therefore not recommended.

Niagara Advanced Plant Controller System and EN60204-1

However, if compliance with the standard EN60204-1 is required, note the following:

General Information about EN60204-1

EN60204-1 defines electrical safety for a complete application/machine, including controllers, sensors, actuators and any connected/controlled electrical device.

EN60204-1 requires controllers to be powered by SELV and earth grounding of the secondary side of the used transformers or earth grounding of the system ground.

Earth grounding is prescribed to prevent the unexpected start-up of connected rotating/moving machines due to an insulation fault and double earth grounding somewhere in the plant.

Using an earth leakage monitor is also possible to fulfill SELV if earth grounding is prohibited.

When is EN60204-1 Applicable to Niagara Plant Controller System?

SAFETY AGAINST ELECTRICAL IMPACT

EN60204-1 is not mandatory because the use of SELV and transformers provides electrical safety according to standard EN60742.

SAFETY AGAINST UNEXPECTED START-UP OF ROTATING/MOVING MACHINES

If the application/plant does not contain machines that harm the operator due to an unexpected start-up, the standard EN60204-1 is not applicable. If such machines are encountered, then EN60204-1 must be followed. Grounding is required.

Functional EMC Grounding

- Use a cable as short as possible for grounding: min 1.5 mm² (16 AWG).
- For connection details, refer to the following example.

EXAMPLE

Connecting a single transformer with multiple Advanced Plant Controller (N-ADV-133-H-B-W/N-ADV-133-H-B/N-ADV-133/N-ADV-134/N-ADV-112 etc) earth-grounded as per EN60204-1.

- Connect earth ground to FGND of the controller Plant Controllers.

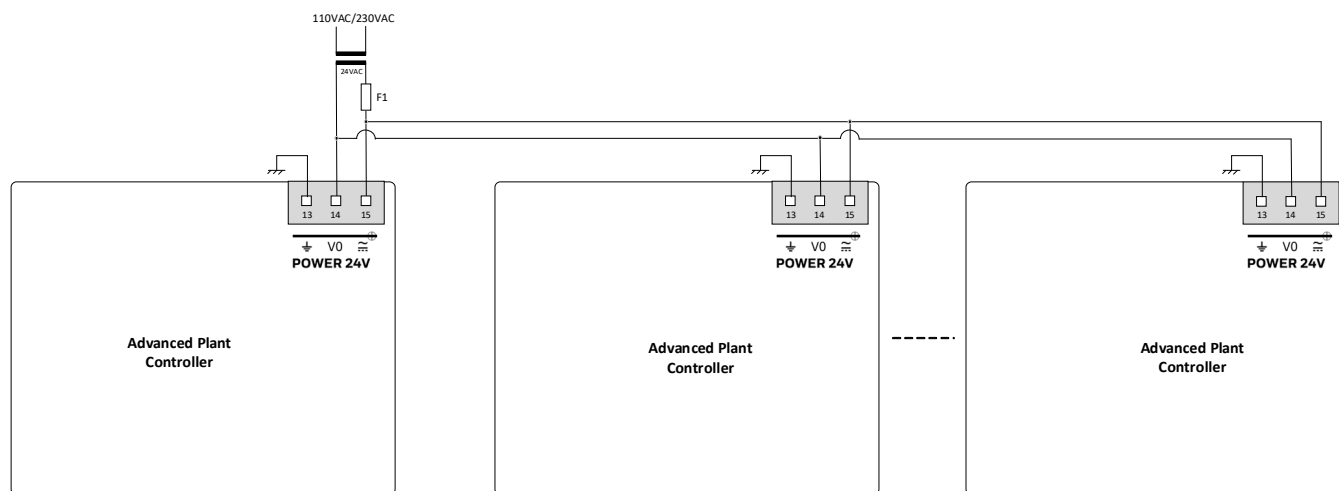


Figure 8. Connecting and earth grounding multiple controller Plant Controllers (single transformer)



NOTE:

- Use a noise-free earth ground inside the cabinet.
- Use one star-point to split power for controllers and field devices.
- If the transformer is used for several controllers, each controller ground must be wired separately to the start point.
- If a field device that prohibits earth grounding is connected to the system ground, an isolation monitoring device must be used instead of earth grounding.
- If the field device transformer is physically far away from the controller, earth grounding must still be performed for the controller.

INTERFACES

The Advanced Plant Controller can communicate with a wide range of devices and systems with its interfaces and is configurable for a variety of protocols.

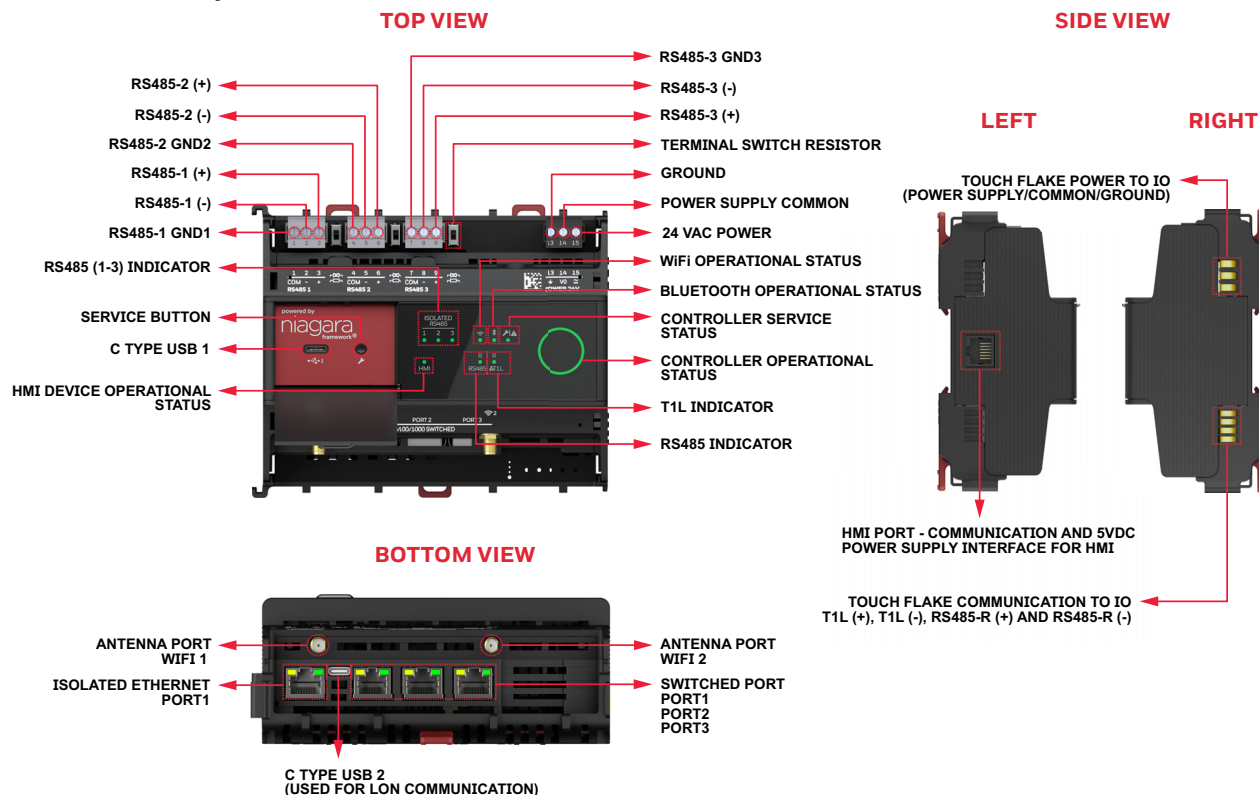


Figure 9. Advanced Plant Controller Interface

HMI LED

HMI LED indicates the connection status between HMI and Advanced Plant Controller.

Default mode: User has not added the **ledplatformService** to the platform or has added the **ledplatformService** but has not added any devices to the associated network database.

Enhanced mode: The user has added **ledplatformService** and added the devices to the database under the given network.

Table 12. Behavior and meaning of HMI LED

Mode	Color	Status	Description
Default mode	NO	OFF	Port Configured
			Port Configured and Commissioned
	Green	Blinking every 100ms	Port Configured and device is OK in database
			HMI device is down or disconnected from Controller
			After Station Restart
			After Controller Reboot

Table 12. Behavior and meaning of HMI LED (Continued)

Mode	Color	Status	Description
Default mode	Green	Blinking every 100ms	After Controller Power Cycle
Enhanced mode	No color	OFF	Port Configured
	Green	Solid	Port Configured and Commissioned
	Green	Solid	Port Configured and device is OK in database
	Red	Solid	HMI device is down or disconnected from Controller
	Green	Solid	After Station Restart
	Green	Solid	After Controller Reboot
	Green	Solid	After Controller Power Cycle

Wi-Fi LED

LEDs indicate the transmission and reception of Wi-Fi.

Applicable only for the controller N-ADV-133-H-B-W and N-ADV-133-H-B.

Table 13. Behavior and meaning of Wi-Fi LED

Mode	Color	Status	Description
Default mode and Enhanced mode	NO	OFF	WiFi Disabled
	Green	Solid	WiFi Enabled
	No color	OFF	Any changes in WiFi settings (After Saving the changes)
	Green	Blink for 2-3 Secs	After Station Restart
	Yellow	Solid	After Controller Reboot
	Red	Solid	After Controller Power Cycle

RING LED

The Advanced Plant Controller is built with a Ring LED to indicate the operational status of the controller.

When a controller restarts successfully, the Ring LED operates in the following pattern:

- Two blinks with a reduced delay between the blinks and subsequently stop glowing for a few milliseconds.

Table 14. Ring LED and Controller status

Light Status	Green (Normal) No Action Required	Yellow (Minor fault) Need Action From User	Red (Major fault) Urgently Need Action from User
			
Solid			
	Power On, Working properly, receiving data from the controller and connection is good. Station is running normally.	Platform is running, station is not up or station in IDLE or error.	Platform is not running.
Blink		N/A	N/A
	Controller under dist file update.	N/A	N/A



NOTE:

- LED will not glow in case OFF, Power OFF, Power Failure.
- LED status does not change when HMI firmware is downloaded from the Online tool to the controller.
- M-Bus and Modbus communication failures do not impact ring LED behavior.

GENERAL INFORMATION ON THE RS485 STANDARD

RS485 LEDs

These LEDs indicate the transmission and reception of data by the three RS485 interfaces.

Default mode: User has not added the **ledplatformService** to the platform or has added the **ledplatformService** but has not added any devices to the associated network database.

Enhanced mode: The user has added **ledplatformService** and added the devices to the database under the given network.

For Led configurations refer to the [“Enable LED Behavior” on page 83](#).

Panel Bus

Table 15. Behavior and meaning of RS485 LEDs for Panel Bus protocol

Mode	Color (All RS485)	Status	Description
Default mode	NO	OFF	Port Configured
	Green	Blinking at 100ms Frequency until the device discovery time and after that Led turns OFF	Port Configured and Discovery
	Green	Continuous blink at 100ms rate based on Ping Frequency	Port Configured and all devices are OK in the database
	Green	Continuous blink at 100ms rate based on Ping Frequency	Some devices are down in Database
	Green	Continuous blink at 100ms Frequency	All devices are down in Database
	Green	Led Blinks 100ms based on Poll Scheduler, will go OFF for few seconds (when some devices are offline/down) and again start's blinking as per the Ping Frequency	At least 1 device added in Database and some IO points to Point database in Fast Ping Frequency
	Green	Led Blinks 100ms based on Poll Scheduler, will go OFF for Few seconds (when some devices are offline/down) and again start's blinking as per the Ping Frequency	At least 1 device added in Database and some IO points to Point database in Normal Ping Frequency
	Green	Led Green Blinks 100ms based on Poll Scheduler, will go OFF Long time (when all devices are offline/down) and again start's blinking for 3 sec as per the Ping Frequency	At least 1 device added in Database and some IO points to Point database in Slow Ping Frequency
	Green	Continuous blink at 100ms rate based on Ping Frequency	After Station Restart
	Green	Continuous blink at 100ms rate based on Ping Frequency	After Controller Reboot
Enhanced mode	Green	Continuous blink at 100ms rate based on Ping Frequency	After Controller Power Cycle
	NO	OFF	Port Configured
	Green	Blinking at 100ms Frequency until the device discovery time and after that Led turns OFF	Port Configured and Discovery
	Green	Solid	Port Configured and all devices are OK in the database

Table 15. Behavior and meaning of RS485 LEDs for Panel Bus protocol (Continued)

Mode	Color (All RS485)	Status	Description
Enhanced mode	Yellow	Solid	Some devices are down in Database
	Red	Solid	All devices are down in Database
	Green	Solid	At least 1 device added in Database and some IO points to Point database in Fast Ping Frequency
	Green	Solid	At least 1 device added in Database and some IO points to Point database in Normal Ping Frequency
	Green	Solid	At least 1 device added in Database and some IO points to Point database in Slow Ping Frequency
	Green	Solid	After Station Restart
	Green	Solid	After Controller Reboot
	Green	Solid	After Controller Power Cycle

BACnet MS/TP**Table 16. Behavior and meaning of RS485 LEDs for BACnet protocol**

Mode	Color (All RS485)	Status	Description
Default mode	Green	Blinks at 100 ms frequency	Port Configured
	Green	Blinks at 100 ms frequency	Port Configured and Discovery
	Green	Blinks at 100 ms frequency	Port Configured and all devices are OK in the database
	Green	Blinks at 100 ms frequency	Some devices are down in Database
	Green	Blinks at 100 ms frequency	All devices are down in Database
	Green	Blinks at 100 ms frequency	At least 1 device added in Database and some IO points to Point database in Fast Ping Frequency
	Green	Blinks at 100 ms frequency	At least 1 device added in Database and some IO points to Point database in Normal Ping Frequency
	Green	Blinks at 100 ms frequency	At least 1 device added in Database and some IO points to Point database in Slow Ping Frequency
	Green	Blinks at 100 ms frequency	After Station Restart

Table 16. Behavior and meaning of RS485 LEDs for BACnet protocol (Continued)

Mode	Color (All RS485)	Status	Description
Default mode	Green	Blinks at 100 ms frequency	After Controller Reboot
	Green	Blinks at 100 ms frequency	After Controller Power Cycle
Enhanced mode	Green	Blinks at 100 ms frequency	Port Configured
	Green	Blinks at 100 ms frequency	Port Configured and Discovery
	Green	Solid	Port Configured and all devices are OK in the database
	Yellow	Solid	Some devices are down in Database
	Red	Solid	All devices are down in Database
	Green	Solid	At least 1 device added in Database and some IO points to Point database in Fast Ping Frequency
	Green	Solid	At least 1 device added in Database and some IO points to Point database in Normal Ping Frequency
	Green	Solid	At least 1 device added in Database and some IO points to Point database in Slow Ping Frequency
	Green	Solid	After Station Restart
	Green	Solid	After Controller Reboot
	Green	Solid	After Controller Power Cycle

Modbus

Table 17. Behavior and meaning of RS485 LEDs for Modbus protocol

Mode	Color (All RS485)	Status	Description
Default mode	NO	OFF	Port Configured
	NA	NA	Port Configured and Discovery
	Green	Continuous blink at 100ms rate based on Ping Frequency	Port Configured and all devices are OK in the database
	Green	Continuous blink at 100ms rate based on Ping Frequency	Some devices are down in Database
	Green	Continuous blink at 100ms Frequency	All devices are down in Database
	Green	Led Blinks 100ms based on Poll Scheduler, will go OFF for few seconds (when some devices are offline/down) and again start's blinking as per the Ping Frequency	At least 1 device added in Database and some IO points to Point database in Fast Ping Frequency
	Green	Led Blinks 100ms based on Poll Scheduler, will go OFF for Few seconds (when some devices are offline/down) and again start's blinking as per the Ping Frequency	At least 1 device added in Database and some IO points to Point database in Normal Ping Frequency
	Green	Led Green Blinks 100ms based on Poll Scheduler, will go OFF Long time (when all devices are offline/down) and again start's blinking for 3 sec as per the Ping Frequency	At least 1 device added in Database and some IO points to Point database in Slow Ping Frequency
	Green	Continuous blink at 100ms rate based on Ping Frequency	After Station Restart
	Green	Continuous blink at 100ms rate based on Ping Frequency	After Controller Reboot
	Green	Continuous blink at 100ms rate based on Ping Frequency	After Controller Power Cycle
Enhanced mode	NO	OFF	Port Configured
	Green	Blinking at 100ms Frequency until the device discovery time and after that Led turns OFF	Port Configured and Discovery
	Green	Solid	Port Configured and all devices are OK in the database
	Yellow	Solid	Some devices are down in Database
	Red	Solid	All devices are down in Database
	Green	Solid	At least 1 device added in Database and some IO points to Point database in Fast Ping Frequency
	Green	Solid	At least 1 device added in Database and some IO points to Point database in Normal Ping Frequency

Table 17. Behavior and meaning of RS485 LEDs for Modbus protocol (Continued)

Mode	Color (All RS485)	Status	Description
Enhanced mode	Green	Solid	At least 1 device added in Database and some IO points to Point database in Slow Ping Frequency
	Green	Solid	After Station Restart
	Green	Solid	After Controller Reboot
	Green	Solid	After Controller Power Cycle

Mbus

Mode	Color (All RS485)	Status	Description
Default mode	NO	OFF	Port Configured
	Green	Blinking at 100ms Frequency until the device discovery time and after that Led turns OFF	Port Configured and Discovery
	Green	Continuous blink at 100ms rate based on Ping Frequency	Port Configured and all devices are OK in the database
	Green	Continuous blink at 100ms rate based on Ping Frequency	Some devices are down in Database
	Green	Continuous blink at 100ms rate based on Ping Frequency	All devices are down in Database
	Green	Led Blinks 100ms based on Poll Scheduler, will go OFF for few seconds (when some devices are offline/down) and again start's blinking as per the Ping Frequency	At least 1 device added in Database and some IO points to Point database in Fast Ping Frequency
	Green	Led Blinks 100ms based on Poll Scheduler, will go OFF for Few seconds (when some devices are offline/down) and again start's blinking as per the Ping Frequency	At least 1 device added in Database and some IO points to Point database in Normal Ping Frequency
	Green	Led Green Blinks 100ms based on Poll Scheduler, will go OFF Long time (when all devices are offline/down) and again start's blinking for 3 sec as per the Ping Frequency	At least 1 device added in Database and some IO points to Point database in Slow Ping Frequency
	Green	Continuous blink at 100ms rate based on Ping Frequency	After Station Restart
	Green	Continuous blink at 100ms rate based on Ping Frequency	After Controller Reboot
	Green	Continuous blink at 100ms rate based on Ping Frequency	After Controller Power Cycle

Mode	Color (All RS485)	Status	Description
Enhanced mode	NO	OFF	Port Configured
	NO	OFF	Port Configured and Discovery
	Green	Continuous blink at 100ms rate based on Ping Frequency	Port Configured and all devices are OK in the database
Enhanced mode	Green	Continuous blink at 100ms rate based on Ping Frequency	Some devices are down in Database
	Green	Continuous blink at 100ms rate based on Ping Frequency	All devices are down in Database
	Green	Led Blinks 100ms based on Poll Scheduler, will go OFF for few seconds (when some devices are offline/down) and again start's blinking as per the Ping Frequency	At least 1 device added in Database and some IO points to Point database in Fast Ping Frequency
	Green	Led Blinks 100ms based on Poll Scheduler, will go OFF for Few seconds (when some devices are offline/down) and again start's blinking as per the Ping Frequency	At least 1 device added in Database and some IO points to Point database in Normal Ping Frequency
	Green	Led Green Blinks 100ms based on Poll Scheduler, will go OFF Long time (when all devices are offline/down) and again start's blinking for 3 sec as per the Ping Frequency	At least 1 device added in Database and some IO points to Point database in Slow Ping Frequency
	Green	Continuous blink at 100ms rate based on Ping Frequency	After Station Restart
	Green	Continuous blink at 100ms rate based on Ping Frequency	After Controller Reboot
	Green	Continuous blink at 100ms rate based on Ping Frequency	After Controller Power Cycle

According to the RS485 standard (TIA/EIA-485: "Electrical Characteristics of Generators and Receivers for Use in Balanced Digital Multipoint Systems"), only one driver communicating via an RS485 interface may transmit data at a time. Further, according to U.L. requirements, which may load each RS485 interface with 32 unit loads.

BACnet MSTP connections to the RS485 interfaces must comply with the aforementioned RS485 standard. Thus, it is recommended that each end of every communication bus be equipped with one termination resistor having a resistance equal to the cable impedance (90 – 120 Ohm/ 0.25 – 0.5 W).

RS485 systems frequently lack a separate signal reference wire. However, the recommended wiring is to provide a solid signal ground (signal reference) connection to ensure error-free communication between drivers and receivers – unless all devices are electrically isolated and no earth grounding exists. Under ideal conditions, the RS485 connection can have a max-length of 1200 meters—however, the longer the cable, the lower the transmission rate. As a rule of thumb, the transmission rate (in bps) multiplied by the cable length (in meters) should not exceed 100 million. For example, a system with a cable 1000 meters long should not be required to transmit data at rates exceeding 100 Kbps.

The following table provides a few examples.

Table 18. Baud rate vs. max. cable length for RS485

Baud Rate	Max. Cable Length (L)
9.6 kbps	1200 m
19.2 kbps	1200 m

Table 18. Baud rate vs. max. cable length for RS485 (Continued)

Baud Rate	Max. Cable Length (L)
38.4 kbps	1200 m
**56 kbps	1200 m
76.8 kbps	1200 m
*115.2 kbps	800 m
* In the case of configuration of RS485 interfaces 1, 2, 3, and 4 of the Advanced Plant Controller for Panel Bus, the communication rate will be automatically set to 115.2 Kbps. ** In case of configuring the Advanced Plant Controller's RS485 interface 4 for IO Bus, the communication rate will be automatically set to 56 Kbps.	

For information on wire gauge, max. Permissible cable length, possible shielding and grounding requirements, and the maximum number of devices connected to a bus refer to standard EIA-485.

Communication Baud Rates

Table 19. Communication Baud Rates

Ethernet	10/100/1000 Mbit/s, RJ45
BACnet MSTP	9.6, 19.2, 38.4, 76.8, 115.2 Kbps
Modbus	0.3 to 115.2 Kbps
Panel Bus	115.2 Kbps
M-Bus	0.3 to 19.2 Kbps
HMI Port	5Vdc power output and RS485



NOTE:

In case of configuring the baud rate of controller, first disable the port, select the baud rate, enable the port, and restart the controller.

Connection to Buses

Table 20. Connection to Buses

Protocols	Max. No. of Devices per Channel	RS485-1	RS485-2	RS485-3	RS485-4	#RS485-R
Panel Bus	64	Yes	Yes	Yes	Yes	Yes
MSTP	64	Yes	Yes	Yes	Yes	Yes
Modbus	32	Yes	Yes	Yes	Yes	Yes
M-Bus*	60	Yes*	Yes*	Yes*	Yes*	Yes



NOTE:

- The communication rate across each communication interface depends on the given communication protocol.
- RS485-4 is only applicable to N-ADV-134-H controller.
- * The N-ADV-133-H series and N-ADV-134-H series controller can function as an M-Bus Master. It uses a standard level converter to connect to the M-Bus devices.
- # A wiring adapter is required to establish communication and power supply over RS485-R (default channel). If the default channel is not used, it must be closed by an end cap. For protective covers, Refer Mounting the wiring adapter on the din rail in Mounting Instruction - 31-00553.
- Up to 64 modules on bus(16 I/O module per type), but typically not more than 16 I/O modules.



WARNING

Risk of electric shock or equipment damage!

- Do not connect more than one Advanced Plant Controllers to the same transformer.
- Do not connect an Advanced Plant Controller and a PW M-Bus Adapter device to the same transformer.

TERMINATOR SWITCH

Terminators: The RS-485 bus must be terminated at each end with a resistor matched to the cable characteristic impedance (i.e. $\pm 1\%$, $\frac{1}{4}$ Watt, range 100 to 130 ohms). If the RS485 of Advanced Plant Controller is at one end of a 120 ohm cable, switch in its built-in terminator, otherwise switch it out and fit a resistor at that end of the cable; the other end must be terminated with a matching resistor.

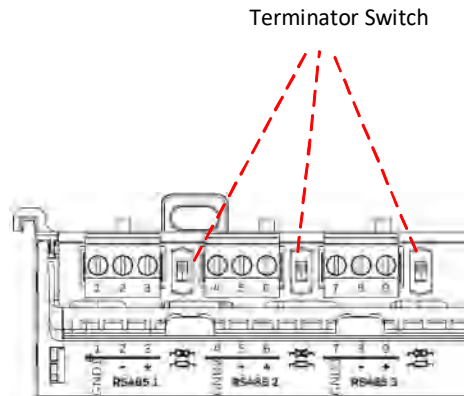


Figure 10. Terminator Switch

Ethernet Interfaces and LEDs

The Ethernet 1 connected to a single Ethernet switch. Assigned to different IP subnet and isolated from other Ethernet ports. On Ethernet 2, three ports are connected to the same network via an internal switch.

Ethernet 1 can connect the controller with the computer using an Ethernet crossover cable. The user can upload, download, and debug the controller application using the Engineering tool from the computer. This connection also establishes Internet connectivity.

They are RJ45 female interfaces, each with a yellow activity status LED (located to the left) and a green activity LED (located to the right). The possible behaviors and corresponding meanings of these LEDs are explained in the following table.

Table 21. Behavior and meaning of Ethernet 1 and 2

Left LED	Right LED	Description	Corrective action
OFF	OFF	Link is Down	Check the cable between the controller and the switch is connected.
Green ON/Blinking	OFF	Maximum speed (1000 Mbps). Link Up Blinking - Data Activity ON - No Data Activity	If the communication problem exists, then check the Ethernet parameter configuration, IP address, MAC address, or firmware.
OFF	Green ON/Blinking	Maximum speed (100 Mbps). Link Up Blinking - Data Activity ON - No Data Activity	
OFF	Yellow ON/Blinking	Maximum speed (10 Mbps). Link Up Blinking - Data Activity ON - No Data Activity	



NOTE:

The above table represent the LED's present at the Ethernet switches



Service Button/Service Alarm LED

The Advanced Plant Controller has a physical service button  to reset the device to factory default.

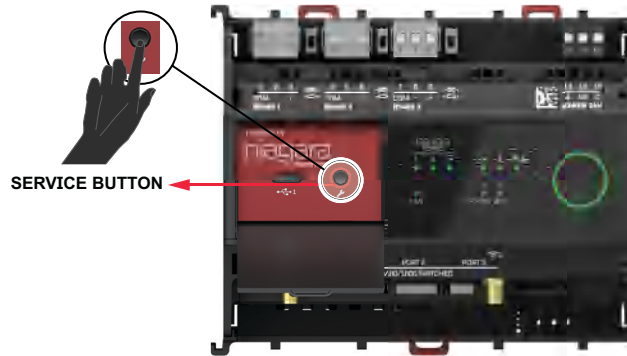


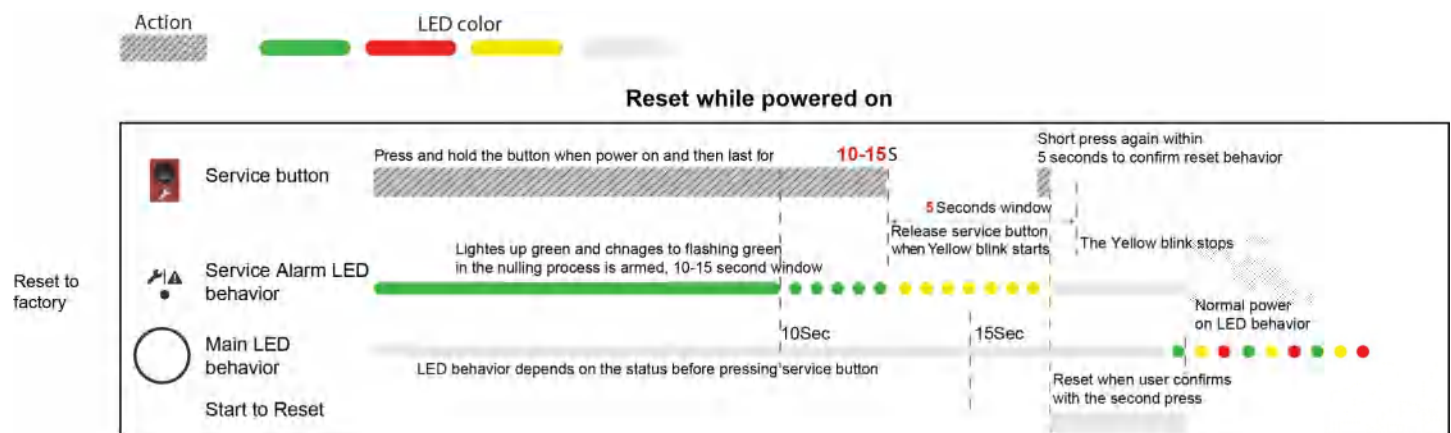
Figure 11. Service Button

In most cases, a factory reset can be achieved while keeping power on to the Advanced Plant Controller. This is the recommended method as it is easier to perform the reset.

In some side cases (i.e. - application locked up), the only way that a device will reset is if power is interrupted to the Advanced Plant Controller first. If the controller did not reset with the recommended method, only then try resetting using the alternative method.

With Power On (Recommended method):

Action	Result	Service Alarm LED Behavior
Press and hold the service button for 10-15 seconds.	For up to 10 seconds the service alarm LED will be solid green.	
Between 10-15 seconds hold.	the service alarm LED will start to blink green.	
Release the service button when the service alarm LED starts blinking Yellow.	Service alarm LED will blinking Yellow	
Short press the service button within 5 seconds of Yellow blinking to confirm the reset to factory default.	The service alarm LED will stop flashing yellow and the normal power-on LED behavior will begin after 5-8 minutes.	

**Figure 12. Factory reset in Power On****NOTE:**

If the service button is short-pressed to confirm the reset and a power failure occurs, the factory reset is successful and the controller reverts to the factory firmware version.

If the service button is not short-pressed to confirm the reset and a power failure occurs after the yellow blink, the factory reset will not be performed and the reset will be unsuccessful.

The reset performs the following operation:

- Reset the local controller configuration
- Erases historical data
- Reset firmware version from the controller
- The controller will go back to factory default firmware version

Abort/Fail Factory reset:

There are two cases when the factory reset will get abort/fail.

Case 1:

The factory reset will fail/abort when the **Service button** is pressed more than 15 seconds (Service button is not released).

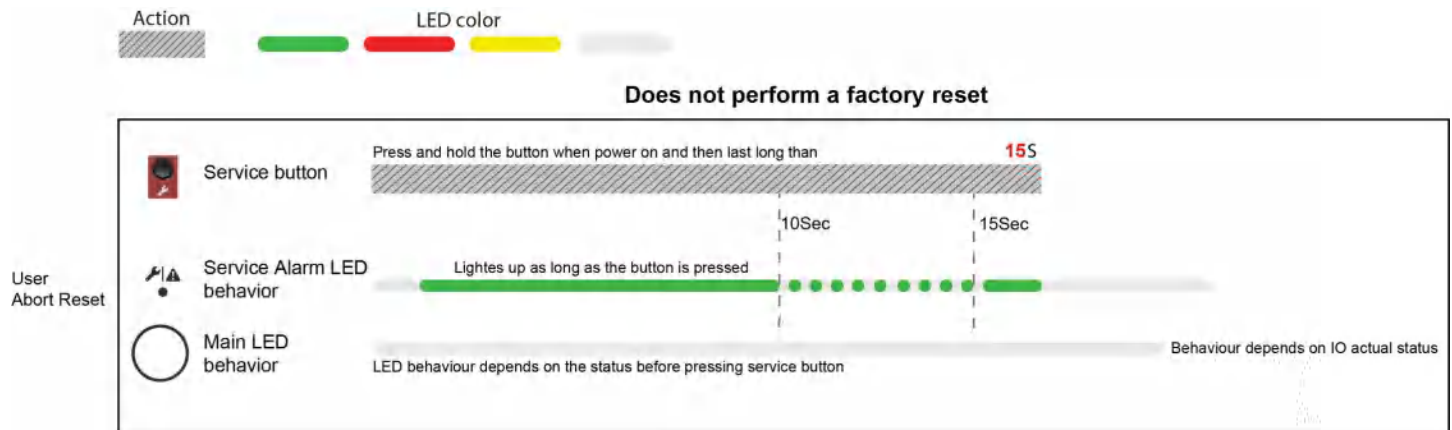


Figure 13. Abort/Fail Factory Reset

or

Case 2:

The factory reset will abort/fail when the user does not confirm the reset to factory with a short press (Within 5 seconds of yellow blink).

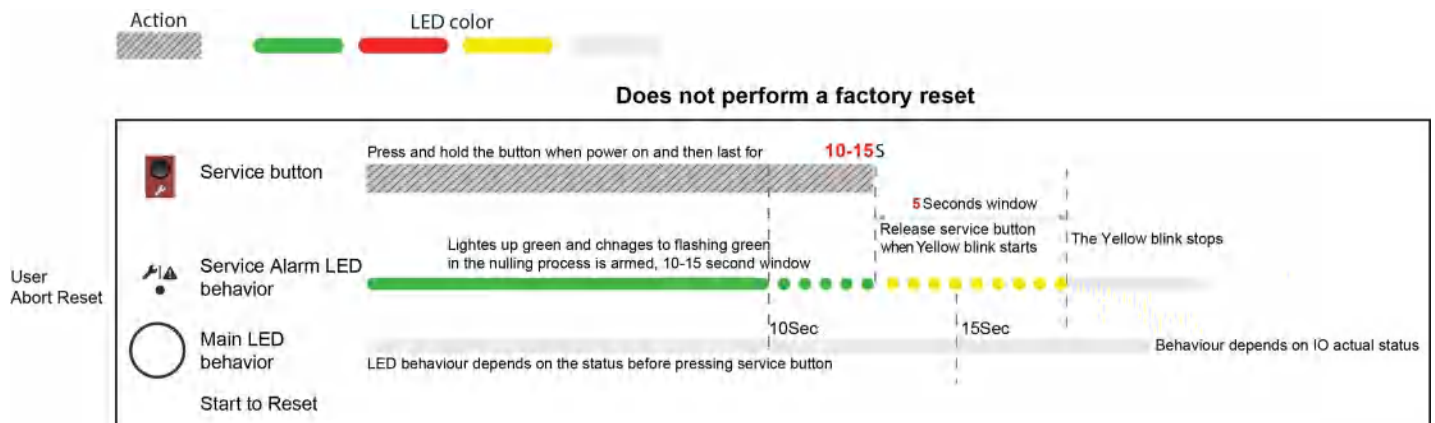


Figure 14. Abort/Fail Factory

TERMINAL ASSIGNMENT

Table 22. Terminal assignment

Type	Terminal	Signal	Description	N-ADV-134-H	N-ADV-133-H-B-W	N-ADV-133-H-B-W	N-ADV-133-H	N-ADV-112-H
RS485-1	1	GND1	GND for RS485 interface 1					
	2	RS485-1(-)	(-) for RS485 interface 1					
	3	RS485-1(+)	(+) for RS485 interface 1					
RS485-2	4	GND2	GND for RS485 interface 2					
	5	RS485-2(-)	(-) for RS485 interface 2					
	6	RS485-2(+)	(+) for RS485 interface 2					
RS485-3	7	GND3	GND for RS485 interface 3					X
	8	RS485-3(-)	(-) for RS485 interface 3					X
	9	RS485-3(+)	(+) for RS485 interface 3					X
RS485-4	18	RS485-4(+)	(+) for RS485 interface 4		X	X	X	X
	19	RS485-4(-)	(-) for RS485 interface 4		X	X	X	X
	20	GND4	GND for RS485 interface 4		X	X	X	X
Input Power 24V	13		Connect to earth ground in the field					
	14	V0	Power supply common					
	15		Power supply (24 Vac/dc)					
Power Supply (RS485-R)	Touchflake	24V~	Power supply (24 Vac/dc) for I/O Module					
		24V0	Power supply common for I/O Module					
		GND	Connection to earth ground in the field for I/O Module					
Antenna Port	Wi-Fi	Antenna Port 1	Connector for Wi-Fi antenna 1	X		X	X	X
		Antenna Port 2	Connector for Wi-Fi antenna 2	X		X	X	X
Ethernet	RJ45 (Ethernet 1)	 1	Port 1 (10/100/1000 base-T/TX)					
Switch Ports	RJ45 (Ethernet 2)	 2	Port 1 (10/100/1000 base-T/TX)					
			Port 2 (10/100/1000 base-T/TX)					X
			Port 3 (10/100/1000 base-T/TX)					X
Connectivity Ports	USB	 1	USB Type C (Device)					
	USB	 2	USB Type C (Device & Host)					

Table 22. Terminal assignment (Continued)

Type	Terminal	Signal	Description	N-ADV-134-H	N-ADV-133-H-B-W	N-ADV-133-H-B-W	N-ADV-133-H	N-ADV-112-H
Power & Com Port	RJ11	RS485_H	Communication and power supply (5Vdc) Interface for HMI					

CONTROLLER TERMINAL

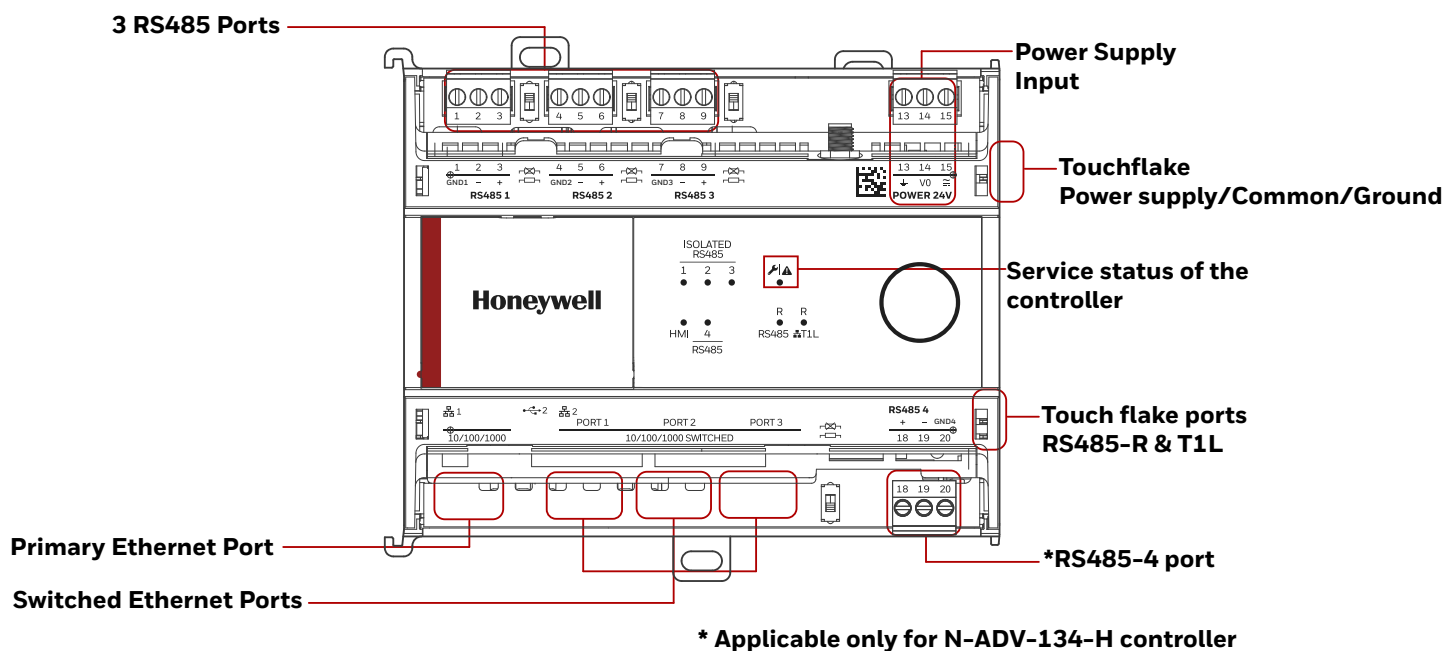


Figure 15. Controller Terminals

FLOW CHART OF COMMISSIONING AND SETUP WORK FLOW

To commission the controller, follow any one of the work flow explained in the two work flow.

- Work Flow 1
- Work Flow 2

Work Flow 1

Follow the below mandate process for commissioning the Advanced Plant Controller. Refer the table for Optional process and follow the recommended step.



NOTE:

In the flow chart the mentioned steps are topics or headings not a process. So for detailed information, go to the respective links from the below table See [“Links of Flow chart for Work Flow 1” on page 40.](#) Check the Flow chart step and click the link from the below table See [“Links of Flow chart for Work Flow 1” on page 40.](#)

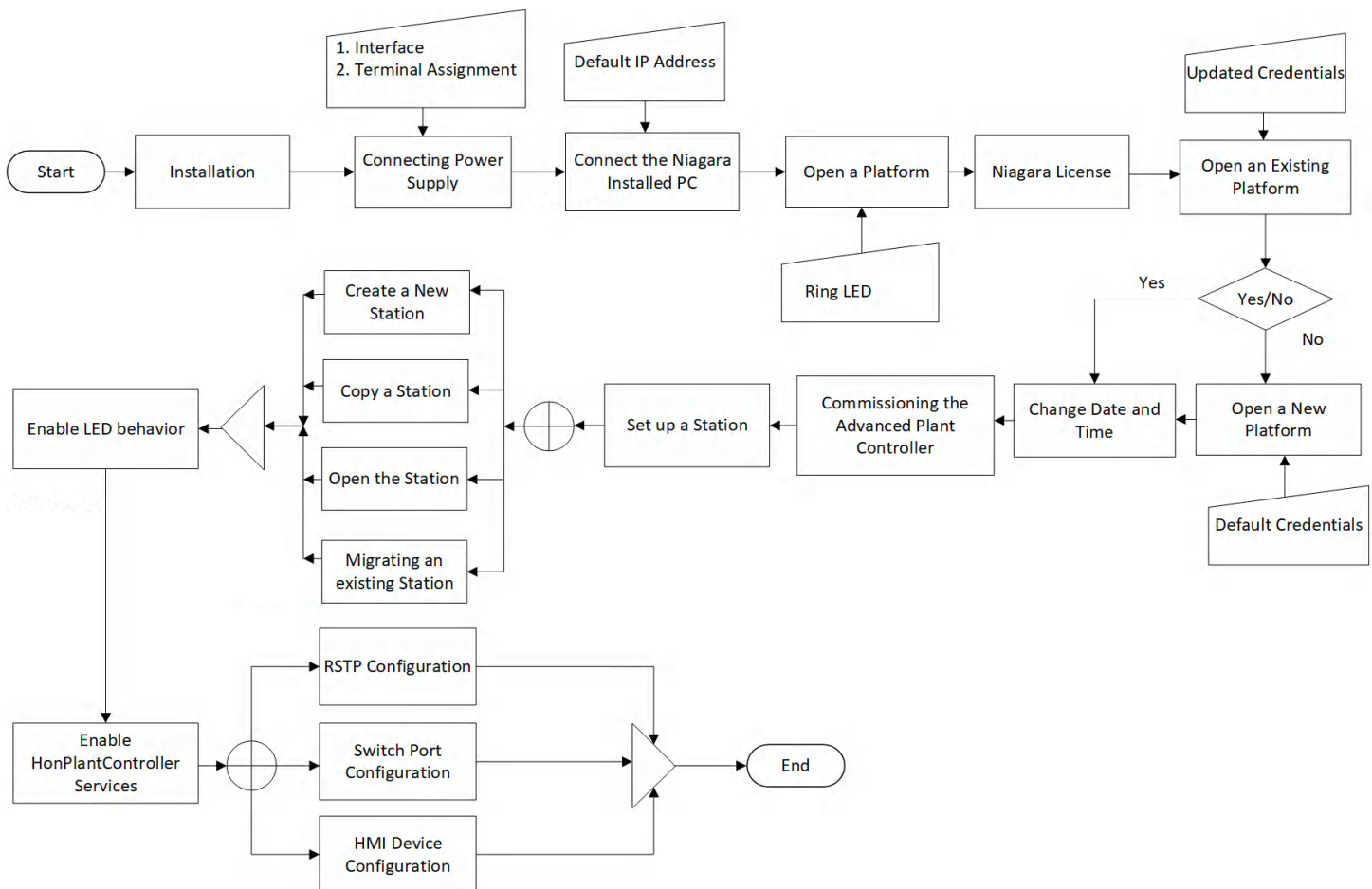


Figure 16. Flow Chart for Work Flow 1

Table 23. Links of Flow chart for Work Flow 1

Mandatory Steps	Optional Steps
“Installation” on page 11.	Refer Mounting Instructions - 31-00553
“Connecting Power Supply” on page 18.	• “Power supply” on page 15. • “Wiring and Set-up” on page 17. • “Power Supply Cable Specifications” on page 19. • “Interfaces” on page 22. • “Terminal Assignment” on page 37.
“Connect the Niagara-Installed PC” on page 44.	• “Default IP Address” on page 11. • “Technical Details” on page 10. • “Ethernet Interfaces and LEDs” on page 33. • “Connection Examples” on page 143.
“Open a Platform” on page 51.	• “Ring LED” on page 24.
“Niagara License” on page 12.	-
“Open an Existing Platform” on page 56.	-
“Open a New Platform” on page 52.	-
“Change Date and Time” on page 76.	-
“Commissioning the Advanced Plant Controller” on page 58.	-
“Set up a Station” on page 67.	• “Create a New Station” on page 67. • “Copy a Station using Station Copier” on page 69. • “Open the Station” on page 72.
“Enable LED Behavior” on page 83.	-
“Enable HonPlantControllerService” on page 78.	-
-	Port Configuration • “Configure TCP/IP Settings” on page 73. • “RSTP Configuration” on page 90. • “Switch Port Configuration” on page 94.
-	“BACnet Network” on page 105.
-	Firmware and Factory reset • “Firmware Update using Distribution File Installer” on page 125. • “CleanDist file Installation” on page 131.
-	Backup and Restore • “Enable/Disable USB Backup and Restore” on page 135. • “USB Backup and Restore using shell command” on page 136.

Work Flow 2

Follow the below mandate process for commissioning the Advanced Plant Controller. Refer the table for Optional process and follow the recommended step.



NOTE:

In the flow chart the mentioned steps are topics or headings not a process. So for detailed information, go to the respective links from the below table See [“Links of Flow chart for Work Flow 1” on page 40.](#) Check the Flow chart step and click the link from the below table See [“Links of Flow chart for Work Flow 1” on page 40.](#)

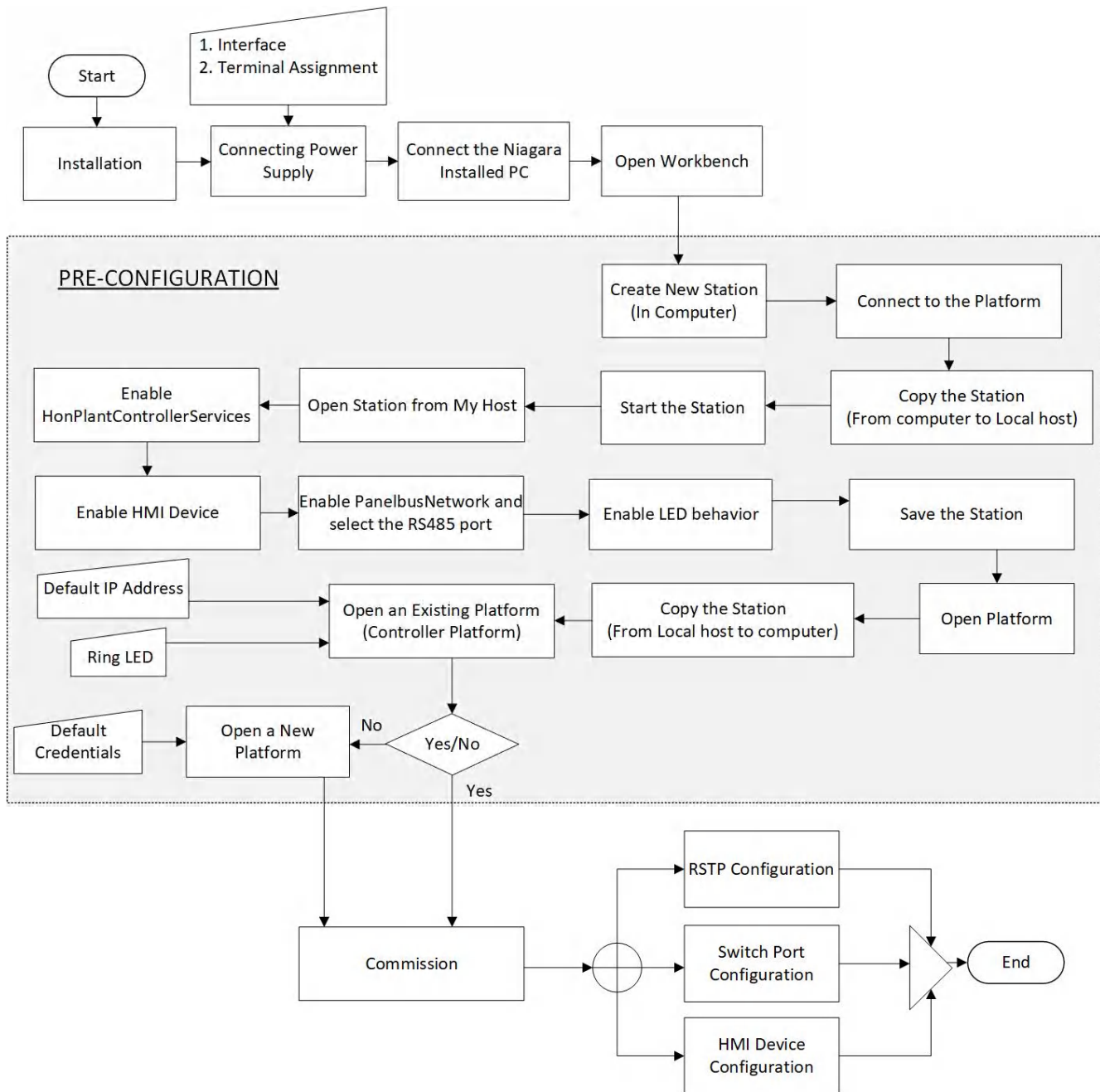


Figure 17. Flow Chart for Work Flow 2

Table 24. Links of Flow chart for Work Flow 2

Mandatory Steps	Description and Optional Steps
“Installation” on page 11.	Refer Mounting Instructions - 31-00553
“Connecting Power Supply” on page 18.	Refer below topics for more details. • See “Power supply” on page 15. • See “Wiring and Set-up” on page 17. • See “Power Supply Cable Specifications” on page 19. • See “Interfaces” on page 22. • See “Terminal Assignment” on page 37.
“Connect the Niagara-Installed PC” on page 44.	Refer below topics for more details. • See “Technical Details” on page 10. • See “Ethernet Interfaces and LEDs” on page 33. • See “Connection Examples” on page 143.
Open Workbench	Open Niagara workbench to configure the controller. See “Software tool” on page 10.
Create New Station (In Computer)	See “Create a New Station” on page 67.
Connect to the Platform	Connect to the Platform which is present in the My Host/Computer See “Open an Existing Platform” on page 56.
Copy the Station (Form computer to Local host)	Copy the station which is created in computer to Local host (De-select Auto-Start in the Station Transfer Wizard) See “Copy a Station using Station Copier” on page 69.
Start the Station	After copying the station, click Start from the Application Director. Follow the step 13 in the Copy a station using Station Copier .
Open Station from My Host	Right click on My Host and select Open Station or See “Open the Station” on page 72.
Enable HonPlantControllerServices	See “Enable HonPlantControllerService” on page 78.
Enable HMI Device	See “HMI Device Configuration” on page 104.
Enable PanelbusNetwork and select the RS485 port	Refer Create Panelbus Network topic in the document Panelbus Driver guide - 31-00591 to Enable and Port selection. or Open Station, Navigate to Config > Drivers > Double click PanelbusNetwork . Select AX Property sheet view, Enable the PanelbusNetwork and select the Panelbus Port from Panelbus Port Config.
Enable LED behavior	See “Enable LED Behavior” on page 83.
Save the Station	Right click on Station and select Save Station
Open Platform	Open the Platform which is present in the My Host/Computer
Copy the Station (From Local host to computer)	Copy the station which is pre-configured in Local host to computer. See “Copy a Station using Station Copier” on page 69.

Table 24. Links of Flow chart for Work Flow 2

Mandatory Steps	Description and Optional Steps
Open an Existing Platform (Controller Platform)	Open the Controller platform with the controller IP address. See “Open an Existing Platform” on page 56.
Open a New Platform	See “Open a New Platform” on page 52.
Commission	See “Commissioning the Advanced Plant Controller” on page 58. or Open the controller Nav tree, Right click on Platform , and select Commissioning Wizard .
RSTP Configuration	See “RSTP Configuration” on page 90.
Switch Port Configuration	See “Switch Port Configuration” on page 94.
HMI Device Configuration	See “HMI Device Configuration” on page 104.

CONNECT THE NIAGARA-INSTALLED PC

In order to access (with a laptop or computer) the controller via Ethernet/IP for the first time, the default passwords are used. For IP connections, you may employ any one of the following two options:

Option 1: USB 2.0 Device

This USB 2.0 Device interface is the recommended interface for downloading applications and firmware via Niagara workbench. An "C-type to C-type" or "C-type to A-Male" USB cable is required.

For access via USB, the Advanced Plant Controller has a permanent default IP address 192.168.255.241. Your computer IP address must match the controller's default IP address subnet (255.255.255.0). See ["How to Enable RNDIS driver in the Advanced Plant Controller" on page 46](#).

Option 2: Standard Ethernet Interface

The default IP address of Ethernet interface 1  1: 192.168.0.200

The default IP address of Ethernet interface 2  2: 192.168.2.200

In any case, your computer IP address must match the Advanced Plant controller's default IP address subnet (255.255.255.0). See ["To connect to the Niagara-installed PC using Ethernet port:" on page 49](#).

Front USB/Ethernet interface

All models of the Advanced Plant controller are equipped with a USB 2.0 Device interface at the front, which is an Ethernet over the USB connection. After connecting the controller and computer with USB 2.0, give the IP address to enable the RNDIS driver and controller begins to communicate with computer.



NOTE:

When the IP address of the controller is unknown, connect the front USB of controller to computer. The RNDIS driver will be identified in the computer, using that IP address you can connect the station and configure the controller from Niagara workbench. See [“How to Enable RNDIS driver in the Advanced Plant Controller” on page 46.](#) and See [“Getting Started” on page 51.](#)

RNDIS Driver

The Remote Network Driver Interface Specification (RNDIS) is a Microsoft proprietary protocol used mostly on top of USB and provides IP connectivity over USB. It provides a virtual Ethernet link to the operating systems. Remote NDIS (RNDIS) eliminates the need for hardware vendors to write an NDIS miniport device driver for a network device attached to the USB bus.



NOTE:

The IP connection is static. The permanent IP address of this USB interface is 192.168.255.241 (Controller).

General architecture of the RNDIS Protocol

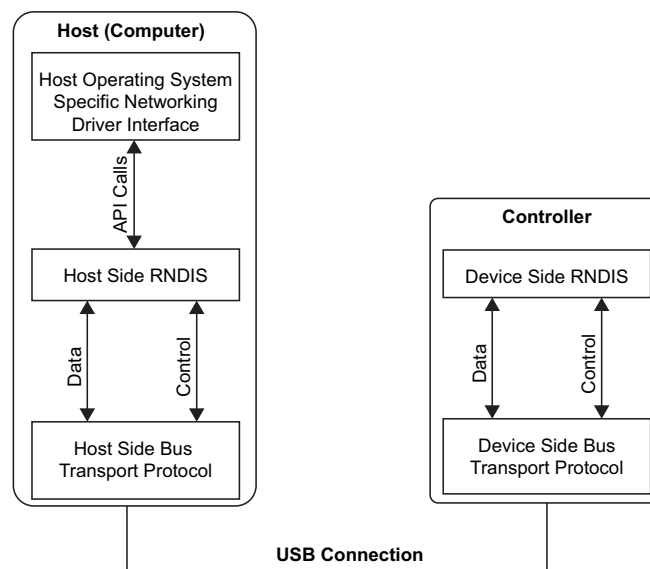


Figure 18. RNDIS Protocol Architecture

How to Enable RNDIS driver in the Advanced Plant Controller

The permanent IP address of this USB interface is 192.168.255.241 (Controller).

Procedure:

1. Power up the Controller. Connect the Advanced Plant Controller to computer with the USB cable.

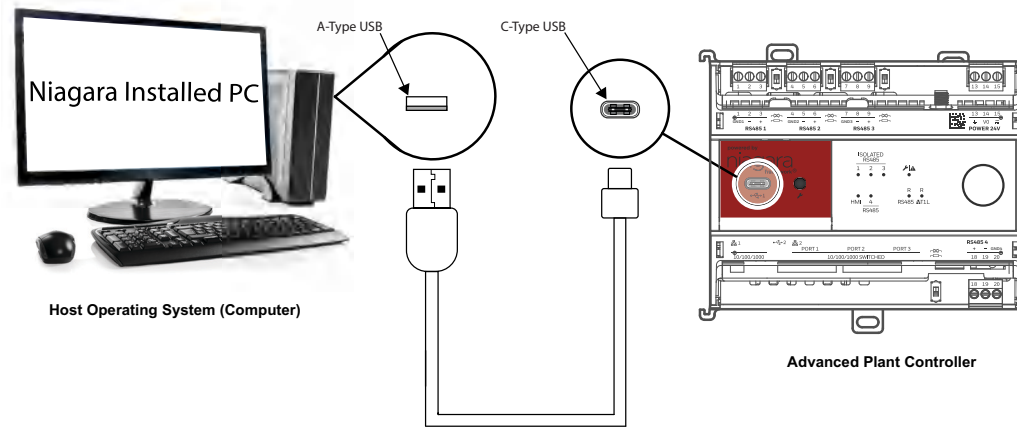


Figure 19. USB Connection from Computer to Controller

2. The RNDIS driver will be detected in the computer.
To check the RNDIS, Go to **Control Panel > Network and Internet > Network Connections**.

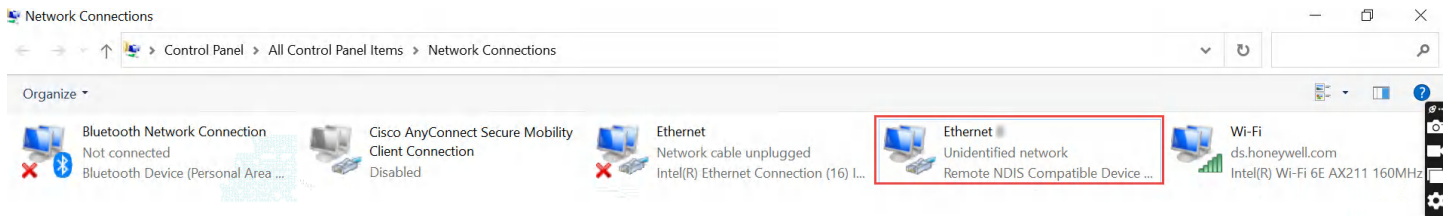


Figure 20. Network Connections Window

ADVANCED PLANT CONTROLLER INSTALLATION INSTRUCTION AND COMMISSIONING GUIDE

3. Double click on **Remote NDIS Compatible Device** (Ethernet X is an example, can be changed based on your Ethernet port number)
Ethernet X Status dialogue box appears. Click **Properties**.

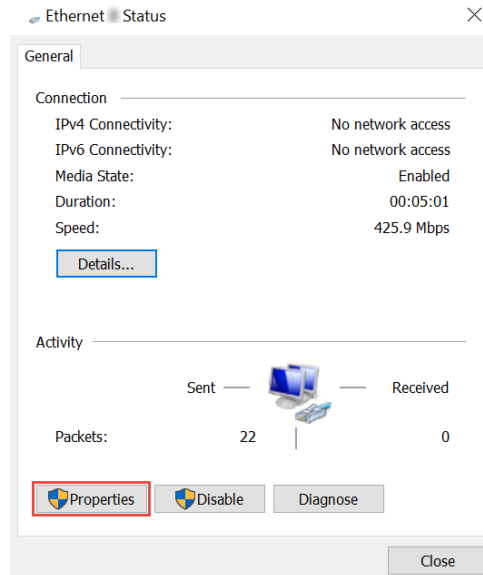


Figure 21. Ethernet Status Dialogue Box

4. Ethernet X Properties dialogue box appears.
 Double click on the **Internet Protocol Version 4 (TCP/IPv4)**.

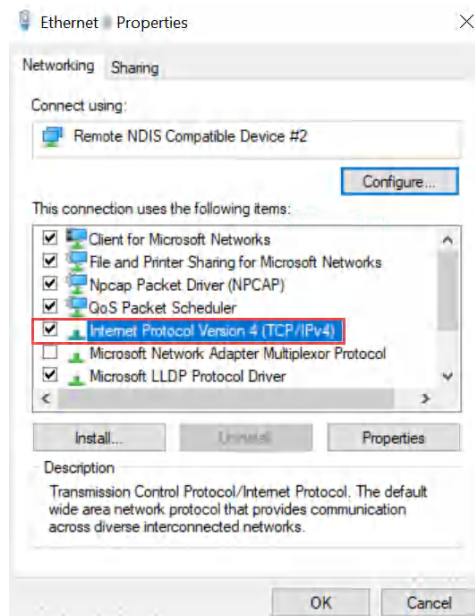


Figure 22. Ethernet Properties Dialogue Box

5. **Internet Protocol Version 4 (TCP/IPv4)** dialogue box appears. Select **Use the following IP address**. Configure the IP address of your computer. Type the IP address in the **IP address** section example, 192.168.255.XX. Replace the XX with the desired number except 192.168.255.241.

**NOTE:**

The RNDIS fails to initialize in the Network connection, if you select **Obtain an IP address automatically** and click **OK** directly. User must configure the Internet Protocol Version 4 (TCP/IPv4) properties to get Initialized.

Table 25. Internet Protocol Version 4 (TCP/IPv4) properties

IP address	192.168.255.XX - Except 192.168.255.241
Subnet mask	255.255.255.0
Default gateway	192.168.255.1

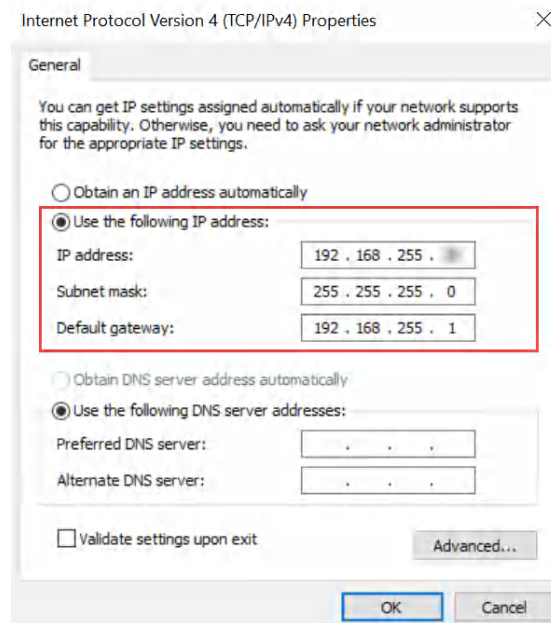


Figure 23. Internet Protocol Version 4 (TCP/IPv4) Properties Dialogue Box

6. Click **OK**.
7. The Network Status will change to Identified state after successful network connection.
8. To check the connection between the Advanced Plant Controller and the Computer, ping the controller with the 192.168.255.241 IP address from the command prompt.
If the connection is **successful**, the communication message will appear with the **IP address**.
If the connection is **unsuccessful**, than **Request time out** message will appear in the command prompt.

**NOTE:**

After Successful RNDIS driver connection, use the 192.168.255.241 IP address while creating a Station/Platform in the Advanced Plant controller and configure the controller from the Niagara workbench. See [“Getting Started” on page 51](#).

To connect to the Niagara-installed PC using Ethernet port:

1. Ensure that the Advanced Plant Controller is powered OFF. See [“Power supply” on page 15](#).
2. Connect the PC (Niagara Installed) to the Advanced Plant Controller using only the Ethernet port.



NOTE:

The number of Ethernet ports varies depending on the controller models. For ports and SKUs, Refer Ordering information table from Advanced Plant Controller Datasheet - 31-00583 and Optimizer Advanced Datasheet -31-00631.

The connection can be made via an Ethernet hub or switch:

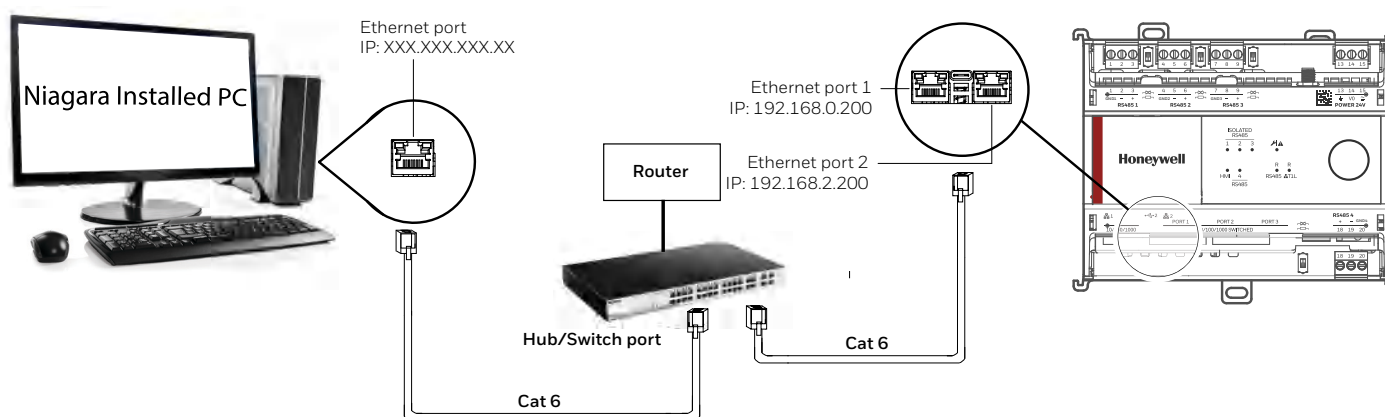


Figure 24. Ethernet Hub or Switch connection

or

Directly using a standard Cat 6 patch cable:

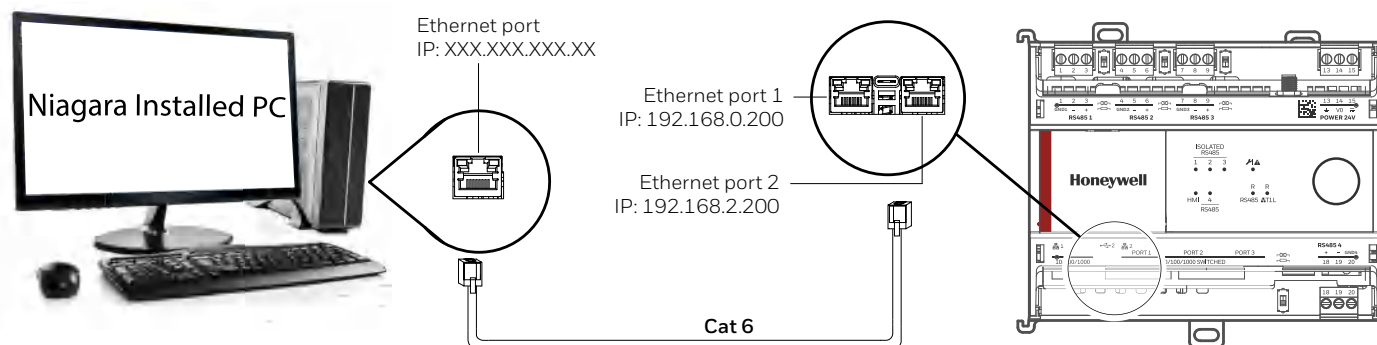


Figure 25. Direct connection

3. Power up the Advanced Plant Controller. See [“Power supply” on page 15.](#)

**NOTE:**

After powering up the Advanced Controller to check the communication, ping the controller with the [Default IP Address](#) from the PC. Go to the command prompt and type "ping 192.168.X.200" Replace "X" based on your Ethernet port (1 or 2) connection. See [“Ethernet Hub or Switch connection” on page 49.](#) and See [“Direct connection” on page 49.](#)

Check the PC's current IP settings, and change its IP settings in case the controller is not communicating.

IP address for port 1  1: Any value in the range of 192.168.0.1 to 192.168.0.254, but not 192.168.0.200

IP address for port 2  2: Any value in the range of 192.168.2.1 to 192.168.2.254, but not 192.168.2.200

Subnet mask: 255.255.255.0

See [“Terminal Assignment” on page 37.](#) for ports.

4. Wait for 30 seconds for the Ring LED indicator to commence a regular flash. See [“Ethernet Interfaces and LEDs” on page 33.](#) for Ethernet communication.
5. Launch Niagara workbench on the PC.
6. [Open a Platform](#) and proceed.

GETTING STARTED

Configuring the Advanced Plant Controller is a mandatory step to avail of the feature and use the plant controller. Before configuring the Advanced Plant Controller, connect the plant controller to BACnet and connect your supervisor's workstation (Laptop or PC) to the same network.

PRE-REQUISITES:

- [Niagara License](#)
- [Default IP Address](#)
- [Connect the Niagara-Installed PC](#)

Connecting Advanced Plant Controller

To configure the Advanced Plant Controller, Supervisor workbench is needed. Niagara Engineering tool is connected with the Advanced Controller to configure the Advanced Plant Controller, See [“To connect to the Niagara-installed PC using Ethernet port:” on page 49](#). Login with Controller [Default IP Address](#) to access the Advanced Plant Controller in Niagara workbench and proceed with [Open a Platform](#).

Open a Platform

1. Launch Niagara workbench.
2. To **Log in**, Go to **File**, click **Open**, and click **Open Platform**.

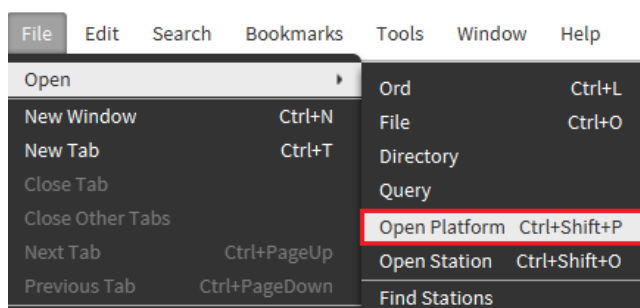


Figure 26. Open Platform

There are two ways to connect to a platform.

- [Open a New Platform](#)
- [Open an Existing Platform](#)

Open a New Platform

To open and connect to a platform of controller follow below procedure or user can open and connect to local platform in the computer and then copy the station to the controller later See [“Copy a Station using Station Copier” on page 69](#).

1. Navigate to the Nav tree and right-click My Host<host_id> and click Open Platform.
The **Open Platform** window is displayed.

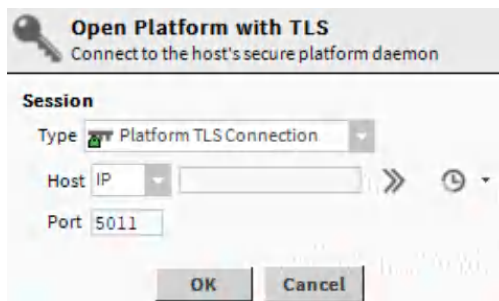


Figure 27. Open Platform with TLS Dialogue Box

2. Select the session type either **Platform TLS Connection** (secured) or **PlatformConnection** (unsecured / standard) in the Type drop-down menu.
3. Select the Host as IP in the Host drop-down menu. By default, the application takes the host Id of your system. If you select the secured platform type, the default port number is 5011.



NOTE:

The (History) icon next to the host Id displays the list of host Ids used before. You can also select the host Id from the History drop-down menu.

Honeywell recommends use of TLS type connection for secure connection.

4. Enter the IP address of Advanced Plant Controller and click **OK**.



NOTE:

The IP setting in Advanced Plant Controller is fixed and the Default IP Address to be selected. Use “192.168.0.200” for EN1 and “192.168.2.200” for Vlan 2 . For Ethernet details See [“Advanced Plant Controller Interface” on page 22](#). and See [“Terminal Assignment” on page 37](#).

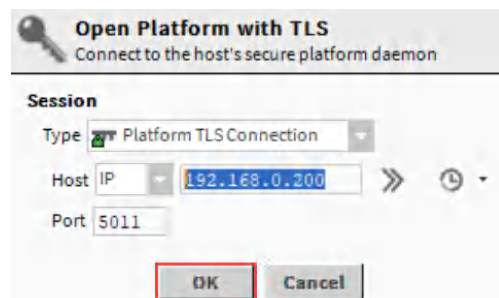


Figure 28. Open Platform Dialogue Box

5. Click **OK**. The Niagara Identity Verification dialogue box is displayed for the TLS connection.

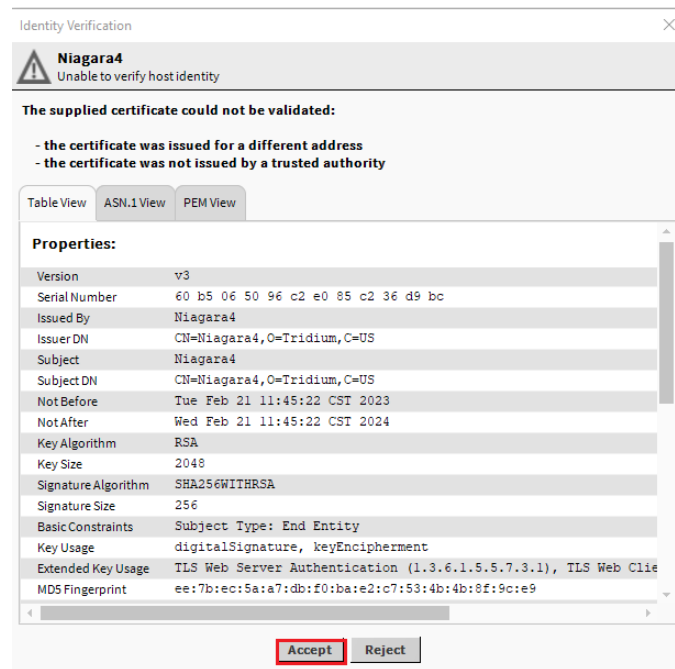


Figure 29. Identity Verification Dialogue Box

6. Click **Accept** and the **Authentication** dialogue box is displayed.

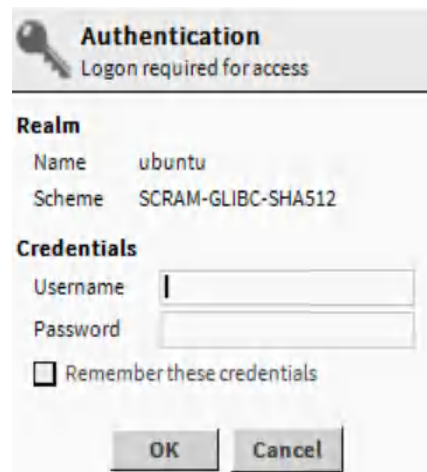


Figure 30. Authentication Dialogue Box

7. Enter the credentials, select Remember these credentials, and click **OK**. You must login with your platform credentials.



NOTE:

Enter default credentials:

Username: tridium

Password: niagara

Select the **Remember these credentials**, if you want to save the credentials.

8. **Change Platform Default Wizard** will be displayed. Click **Next** to change the default username and password.

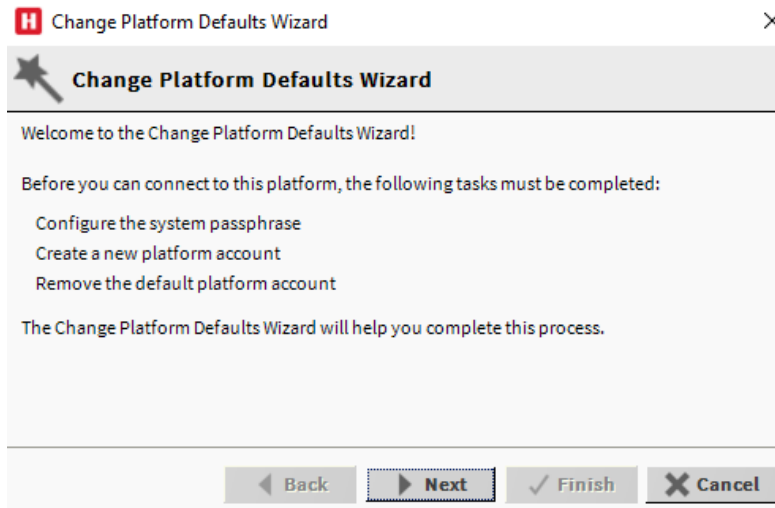


Figure 31. Change Platform Default Wizard Dialogue Box

9. **Change Platform Default Wizard** to configure the System Passphrase will be displayed. Type the new passphrase in **New Passphrase** box, Retype the new passphrase in the **Confirm New Passphrase** box and click **Next**.

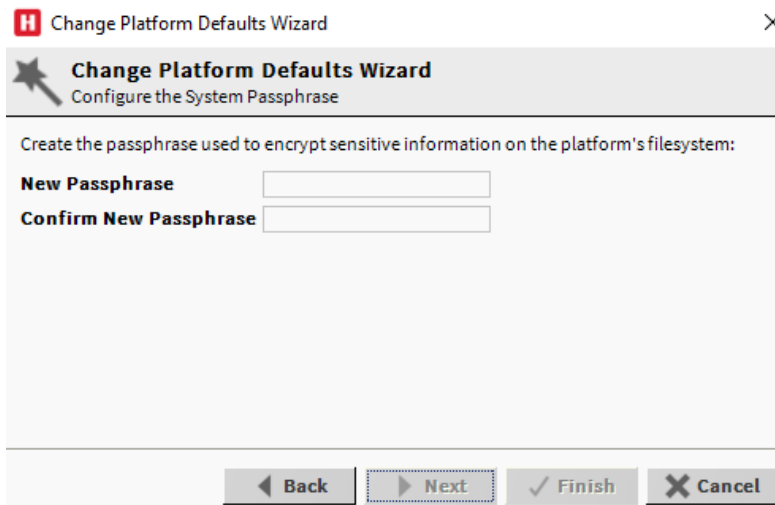


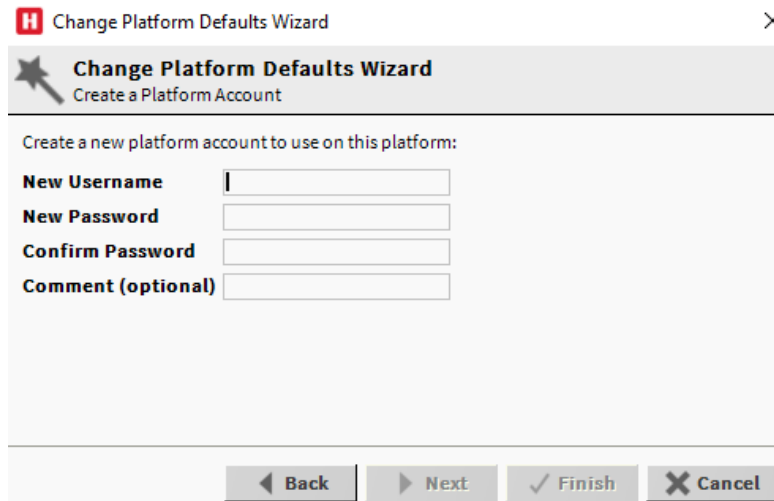
Figure 32. Change Platform Default Wizard Dialogue Box



NOTE:

The password must have a minimum of 10 characters and include at least one capital letter, one lowercase letter and one numeral (digit). Remember the new passphrase.

10. **Change Platform Default Wizard** to **Create a Platform Account** will be displayed. Type suitable name in **New Username** box, suitable password in **New Password** box, Retype password in **Confirm Password** box (Comment is optional) and click **Next**.



The screenshot shows a dialog box titled "Change Platform Defaults Wizard" with a close button (X) in the top right corner. Below the title bar, there is a star icon and the text "Change Platform Defaults Wizard" and "Create a Platform Account". The main area contains the instruction "Create a new platform account to use on this platform:". Below this, there are four input fields: "New Username", "New Password", "Confirm Password", and "Comment (optional)". At the bottom, there are four buttons: "Back", "Next", "Finish", and "Cancel".

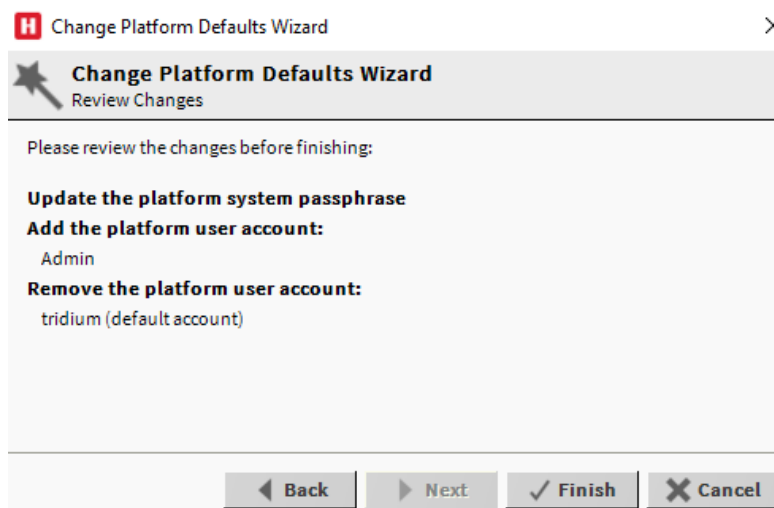
Figure 33. Change Platform Default Wizard Dialogue Box



NOTE:

The password must have a minimum of 10 characters and include at least one capital letter, one lowercase letter and one numeral (digit).
 -In the (optional) Comment field, you can enter an alphanumeric descriptor for this platform admin user. This text will be displayed in the 'Users table' and may be helpful if there is more than one platform user.

11. **Change Platform Default Wizard** to **Review Changes** will be displayed. Review the changes and click **Finish**.



The screenshot shows a dialog box titled "Change Platform Defaults Wizard" with a close button (X) in the top right corner. Below the title bar, there is a star icon and the text "Change Platform Defaults Wizard" and "Review Changes". The main area contains the instruction "Please review the changes before finishing:". Below this, there are three sections: "Update the platform system passphrase", "Add the platform user account:" with "Admin" listed below it, and "Remove the platform user account:" with "tridium (default account)" listed below it. At the bottom, there are four buttons: "Back", "Next", "Finish", and "Cancel".

Figure 34. Change Platform Default Wizard Dialogue Box



NOTE:

Default Platform credentials will be removed. Use the new username and password credentials to open the same platform.

12. Platform created and below window will be displayed.

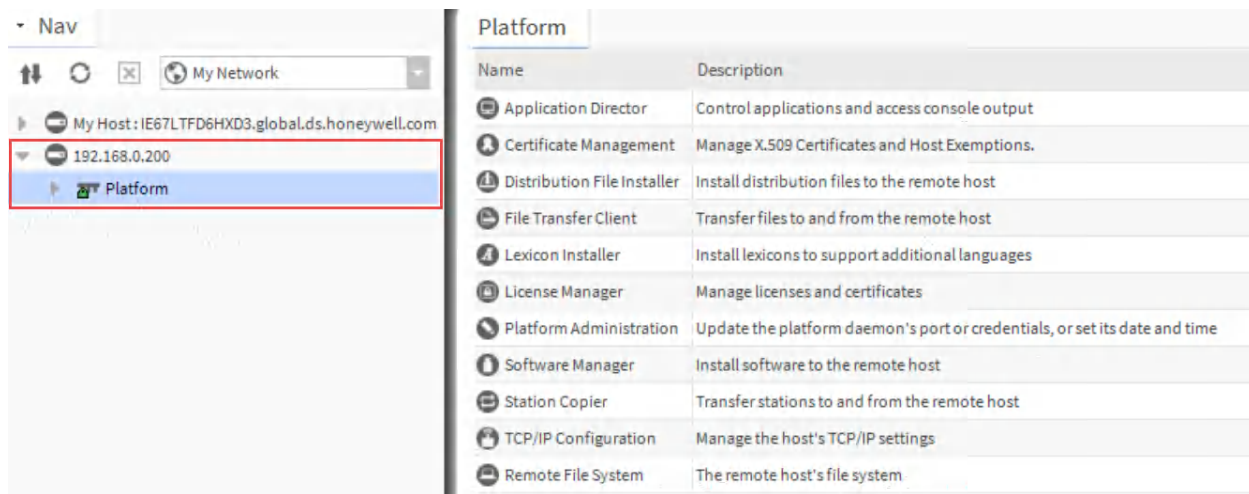


Figure 35. Host and Platform Window

Host ID (IP address) with Platform is created.

13. Proceed with [Commissioning the Advanced Plant Controller](#).

Open an Existing Platform

Use the following procedure to connect to an existing Advanced Plant Controller platform. If you have not opened a platform previously for the Advanced Plant Controller follow the procedure [Open a New Platform](#) instead.

To open an existing platform:

1. Connect to Advanced Plant Controller and run Niagara workbench. See [“Connect the Niagara-Installed PC” on page 44](#).
2. In the Nav tree, right-click the Advanced Plant Controller (IP address) entry and select **Open Platform**. The Connect dialogue box is displayed:
or
Navigate to the Nav tree and right-click My Host<host_id> and click Open Platform. The Connect window is displayed.

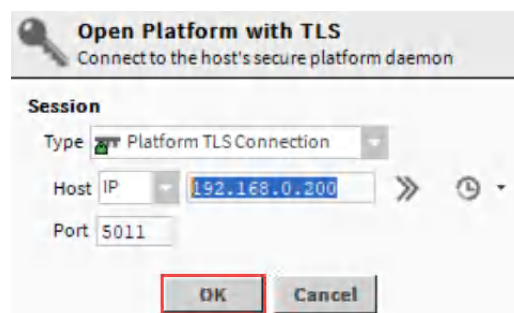


Figure 36. Open Platform Dialogue Box



NOTE:

For offline platform (Local Host), use the second method to open the platform.

- Click **OK**. The **Authentication** dialogue is displayed:

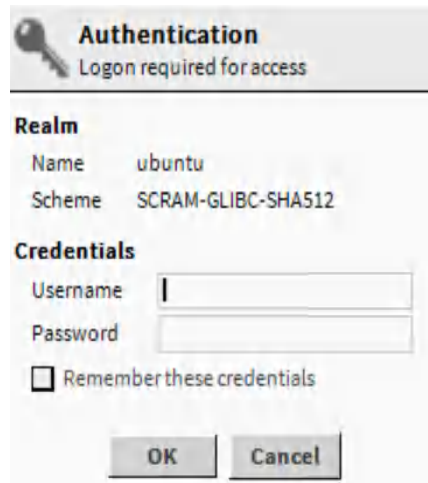
The image shows a standard Windows-style authentication dialog box. At the top, there is a title bar with a key icon and the text "Authentication" and "Logon required for access". Below this, the "Realm" section contains two labels: "Name" with the value "ubuntu" and "Scheme" with the value "SCRAM-GLIBC-SHA512". The "Credentials" section has two text input fields, one for "Username" and one for "Password". Below these fields is a checkbox labeled "Remember these credentials". At the bottom of the dialog are two buttons: "OK" and "Cancel".

Figure 37. Authentication Dialogue Box

- Enter the credentials Username and Password for the Advanced Plant Controller.



NOTE:

Use your Platform credentials which are given while creating the Platform. See [“Open an Existing Platform” on page 56.](#)

- Click **OK**. A connection to the Advanced Plant Controller will now be established and the Platform view is displayed. Proceed with [Commissioning the Advanced Plant Controller](#).

Commissioning the Advanced Plant Controller

The commissioning process is a necessary step for the new controller or existing controller after completing the changes in the Niagara workbench. The first time Advanced Plant Controller is powered up it is necessary to perform an initial set up using the Commissioning Wizard in the Niagara workbench which steps through several specific configuration tasks to simplify the initial set up. Niagara workbench is used to deploy the changes and to update the firmware based on new modules.

The Commissioning Wizard gives the option to upload an existing station to the Advanced Plant Controller. Therefore, you may wish to create a station first – See [“Create a New Station” on page 67](#). Alternatively, you can create a station and upload it after running the wizard.

IMPORTANT:

If the user has a controller with firmware version: 4.10.5.14.0.7.6
 Before upgrading to any higher firmware version, the user must upgrade the controller from firmware version 4.10.5.14.0.7.6 to 4.10.5.14.0.11. Refer to the [“Troubleshooting” on 162](#).
 Get the firmware version modules from location:
US: <Need Location URL>
EU: <Need Location URL>

Procedure for commissioning the Plant Controller

1. To start the commissioning process, Go to **Platform**, double click on **Platform Administration**, and click **Commissioning**.

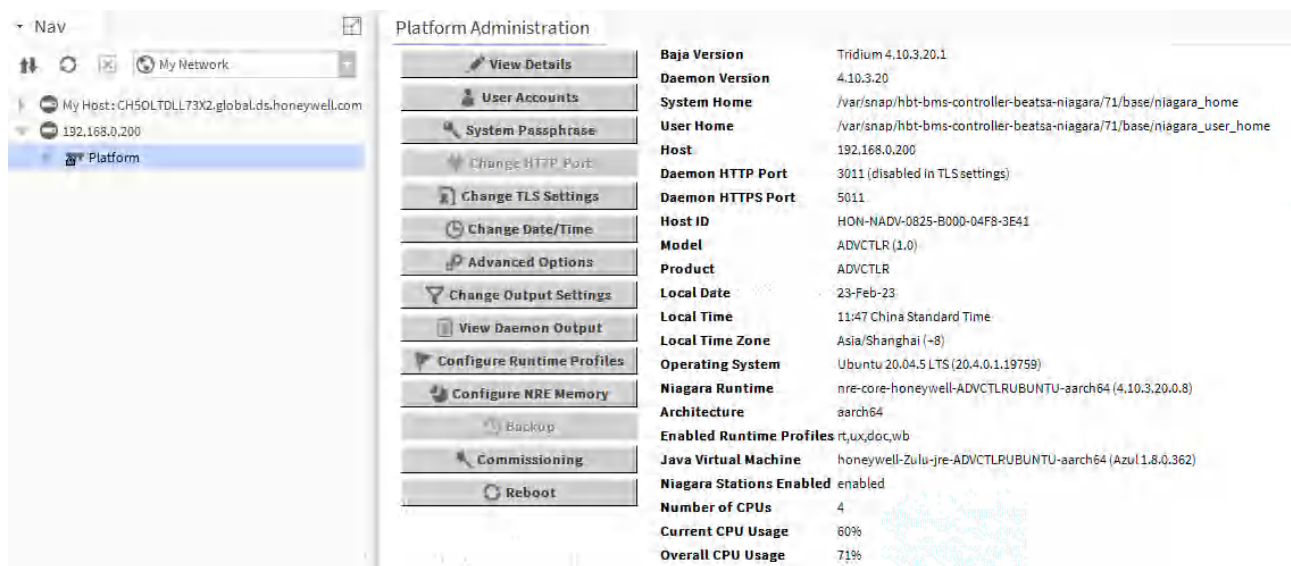
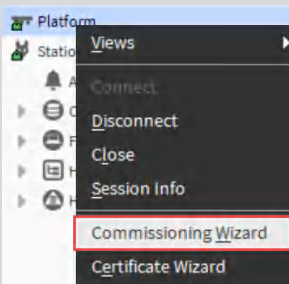


Figure 38. Platform Administration Window

NOTE:

Commissioning can also done from any page. Another method to commission the controller is, Right click on controller **Platform** and click **Commissioning Wizard**.



2. Commissioning dialogue box displayed. Select the options based on the commissioning requirement and click **Next**.
For new controller select only set enabled runtime profile and Sync with my local system date and time

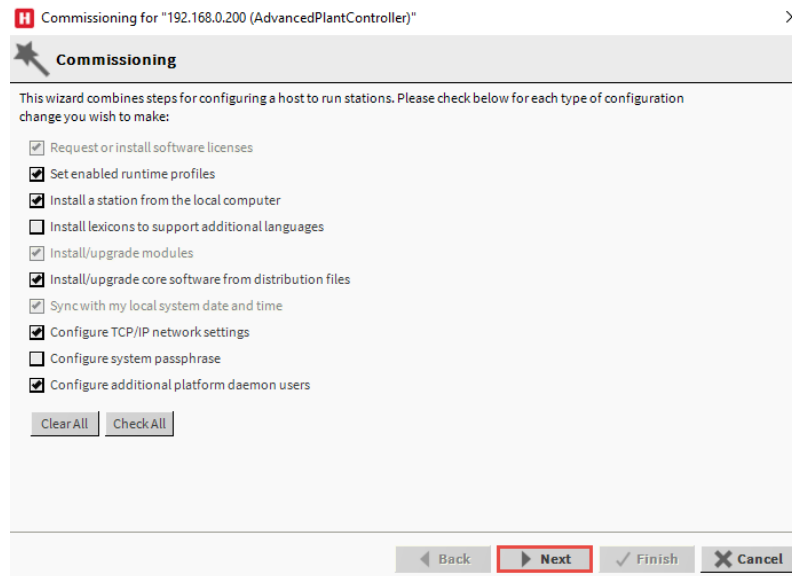


Figure 39. Commissioning Dialogue Box



NOTE:

On a first install most options are selected and cannot be deselected. For those options that can be changed, it is recommended that you keep their default settings. The following procedure assumes that the default settings have been selected. Most of the options may change while Commissioning again.

3. Commissioning dialogue box for licenses displayed. Select license and click **Next**.
If the Advanced Plant Controller has automatically installed a license it will be listed, and you can skip to step 8. Otherwise the wizard will ask for license to add:

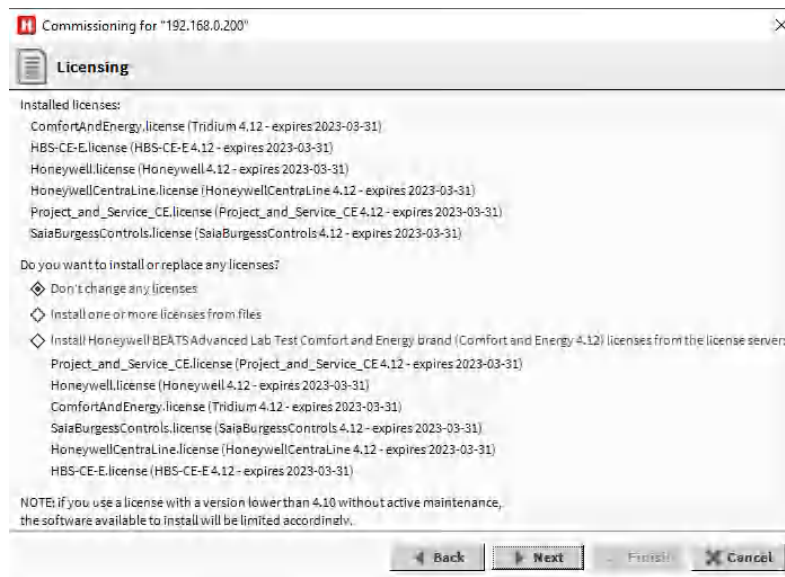


Figure 40. Commissioning Dialogue Box for License

4. Click **Next**. Licensing dialogue box is displayed.

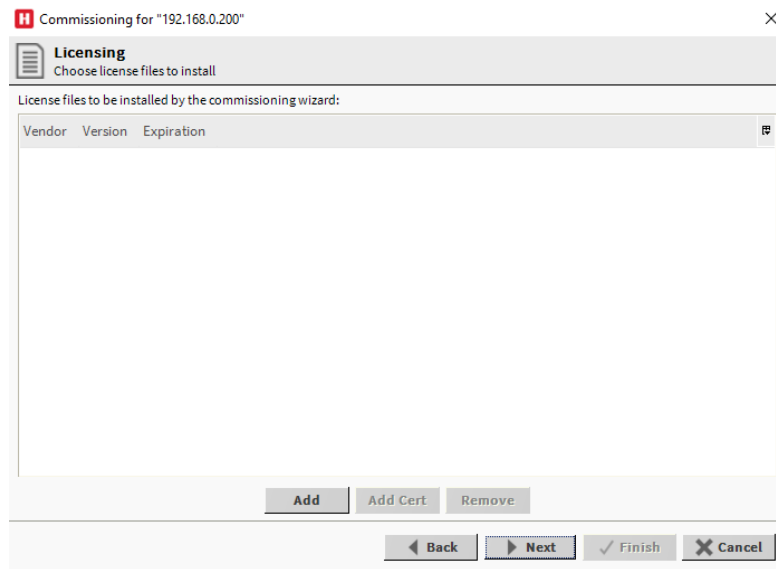


Figure 41. Commissioning Dialogue Box for License

5. Click **Add** to select a license. See [“Niagara License” on page 12](#).

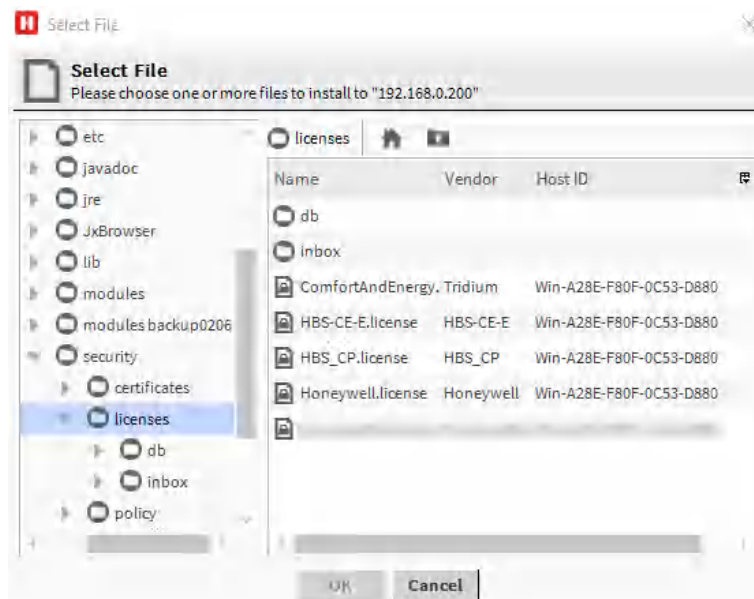


Figure 42. Select File Dialogue Box

6. Navigate to the location of the required license file. Click on the file name.

7. Click **OK**.

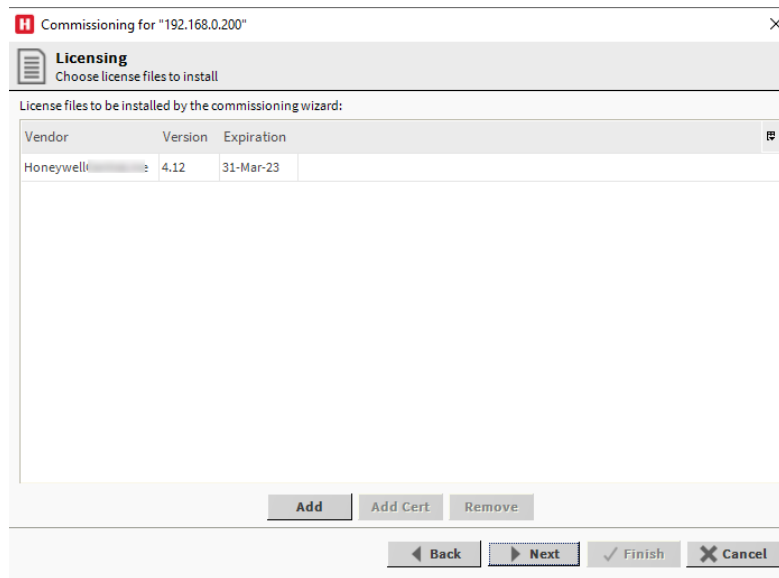


Figure 43. Licensing Dialogue Box

8. Commissioning dialogue box for **Enable Runtime Profiles** is displayed.

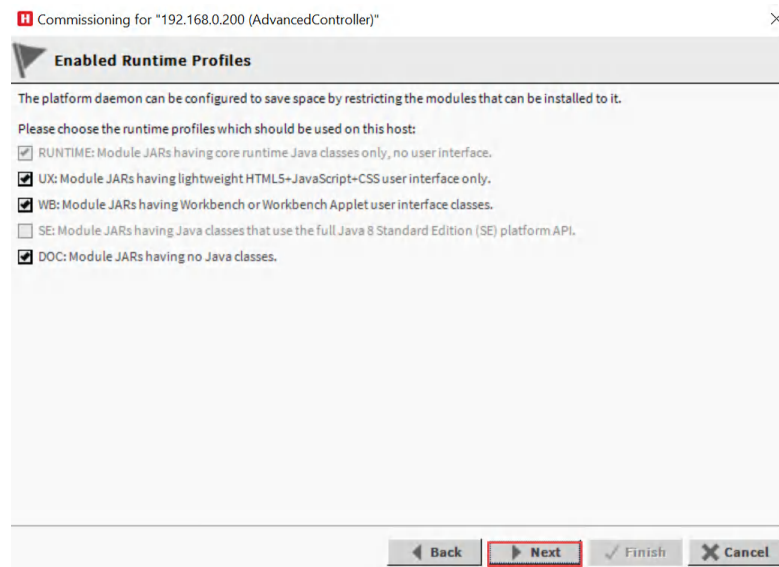


Figure 44. Enable Runtime Profiles Dialogue Box



NOTE:

Based on the commissioning wizard selected options (Step 2), the commissioning window will appear. For example: If the Configure system passphrase is selected in commissioning dialogue box (Step 2), the commissioning window to configure the system passphrase will appear while commissioning. Refer Niagara User Guide for commissioning the controller.

9. Click **Next**. The **Software Installation** dialogue box is displayed.

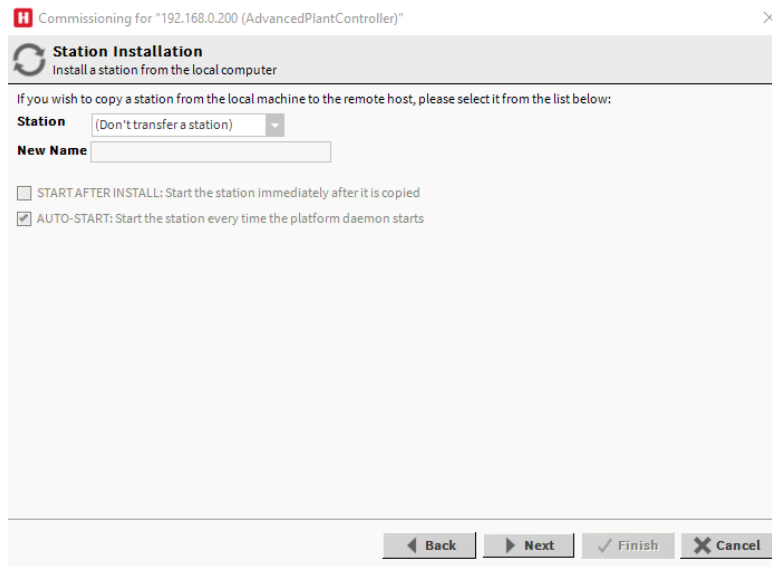


Figure 45. Software Installation Dialogue Box

10. If you do not have a pre-configured station available, or don't want to copy one to the Advanced Plant Controller at this point, leave Station set to Don't transfer a station and go to step 13. Otherwise, use the Station drop down box to select an existing station to copy to the Advanced Plant Controller.
11. Type the desired name (different from existing stations name) in the **New Name** box.
12. Set the **START AFTER INSTALL** and **AUTO-START** options as required. By default, these will both be selected.



NOTE:

START AFTER INSTALL: Select this option if you want to start the station as soon as it has copied (recommended).

AUTO-START: Select this option if you want the station to be started when the Advanced Plant Controller is restarted (recommended).

13. Click Next. After displaying a “Analyzing” messages the wizard will show a list of software that will be installed:

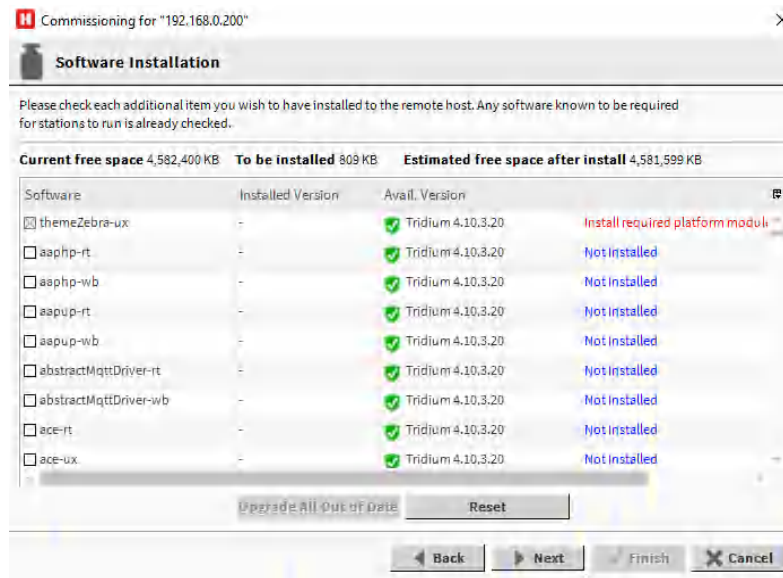


Figure 46. Software Installation Dialogue Box



NOTE:

If required, you can review the list of software items that will be installed on the Advanced Plant Controller. Items that must be installed or out of date have a red text - Select the items and Click on **Select Upgrade All Out of Date**. Installed items will appear in blue text descriptor. Out of Date and items to be installed are at the top of the list and cannot be deselected. Other items can be selected or deselected to suit specific applications. To reset the selection of modules to the original collection, click Reset. To Install Additional Drivers - See [“Install Additional Drivers” on page 77](#).

14. Click **Next**. The **Distribution File Installation** dialogue box is displayed.

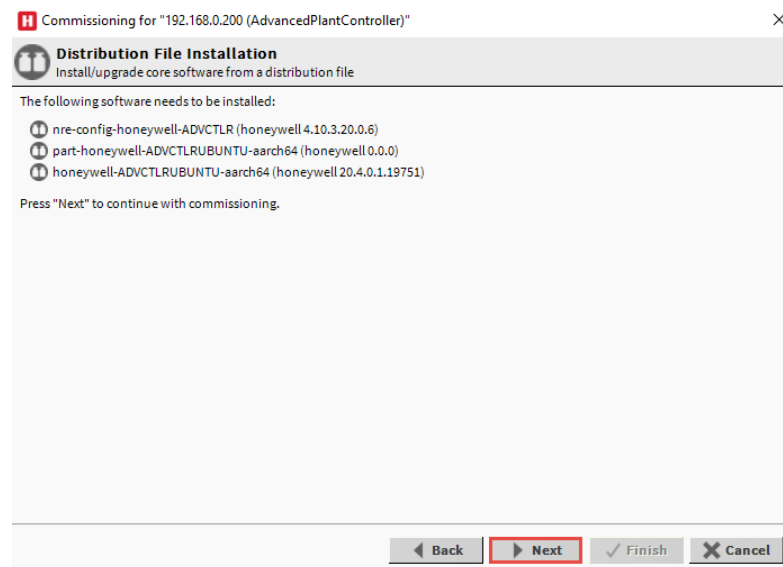


Figure 47. Distribution File Installation Dialogue Box

15. Click **Next**. The TCP/IP configuration step is displayed:

Figure 48. TCP/IP Configuration Dialogue Box



NOTE:

This step gives you the option to set up the IP settings for the two Ethernet ports. You can either do this now or after completing the wizard - See [“Configure TCP/IP Settings” on page 73](#). Configure only one Interface port with DHCP Dynamic and one Interface port with DHCP Static form Interface 1/Interface 2 port.

Example: Configure scenario as below

- Interface 1 = DHCP Dynamic, Interface 2 = DHCP Static
- Interface 1 = DHCP Static, Interface 2 = DHCP Static

Both the Interface port cannot be configured with DHCP Dynamic.

16. Click **Next**. The **System Passphrase** step is displayed:

Figure 49. System Passphrase Dialogue Box

17. Type the default passphrase (*niagara*) in the **Current Passphrase** box.

18. Type a new passphrase in the **New Passphrase** box.

**NOTE:**

The password must have a minimum of 10 characters and include at least one capital letter, one lowercase letter and one numeral (digit).

19. Retype the new passphrase in the **Confirm Passphrase** box.

**IMPORTANT:**

Remember the new passphrase.

20. Click **Next**. The **Platform Daemon Authentication** step is displayed:

Figure 50. Platform Daemon Authentication Dialogue Box

**NOTE:**

The **Platform Daemon Authentication** wizard will display users, If there are existing users in the Advanced Plant Controller or else it will ask “Please create a new platform user account” with **User Name** and **Password** to create a platform user account. Follow step 21 to step 24 for New user or continue with step 25

21. Type a suitable name for a platform admin user in the **User Name** box.
 22. Type a suitable password for the platform admin user in the **Password** box.

**NOTE:**

The password must have a minimum of 10 characters and include at least one capital letter, one lowercase letter and one numeral (digit).

23. Retype the password in the **Confirm Password** box.

**NOTE:**

In the (optional) Comment field, you can enter an alphanumeric descriptor for this platform admin user. This text will be displayed in the 'Users table' and may be helpful if there is more than one platform user.

ADVANCED PLANT CONTROLLER INSTALLATION INSTRUCTION AND COMMISSIONING GUIDE

24. If required, you can add further users at this point by clicking New User. Users can also be added, changed or removed later. See [“Niagara help documents” on page 13.](#) and search How to add new users in platform or refer Niagara User guide.
25. Click **Next**. A summary of the changes that will be implemented is displayed:

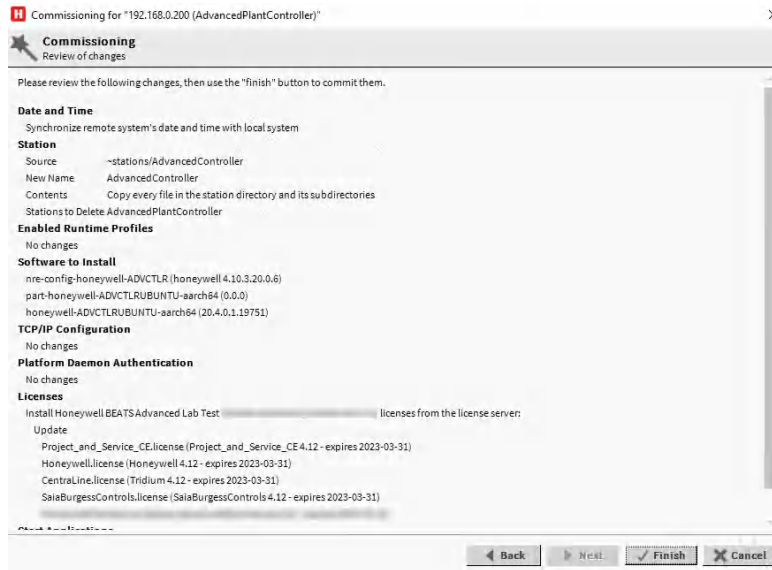


Figure 51. Commissioning Window for Review of Changes

**NOTE:**

Review the list of changes. You can use the **Back** button to go back to modify any settings.

26. Complete Commissioning window is displayed where the commissioning success message will get. Click **Close Window**.

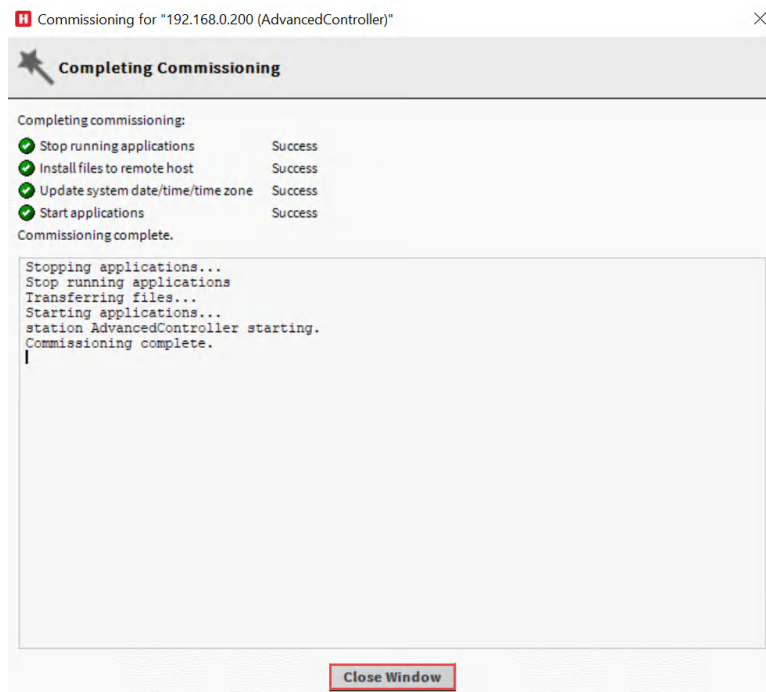


Figure 52. Completing Commissioning Window

27. Commissioning the Advanced Plant Controller Finished!

**IMPORTANT:**

The Advanced Plant Controller will go through reboot cycles three times during the commissioning process. Do not turn Off Power to the controller during this time – Doing So May cause errors in the jar file. Restart the configuration process again.

28. Observe the Ring LED indicator on the front of the Advanced Plant Controller unit – when this has solid yellow or solid green LED ON for at least 10 seconds, the setup process is finished and is ready for use. If commissioning has distribution file installed, it takes 15 minutes to fully load the distribution file before it is finished.
29. If you changed the primary Ethernet port settings on Advanced Plant Controller, remember that you may now need to:
 - Change the IP settings on the configuration PC to restore communications between the PC and Advanced Plant Controller.
 - Open a new platform in the Niagara Nav tree – See [“Open a New Platform” on page 52.](#)
 - If you copied an existing station to Advanced Plant Controller using the Commissioning Wizard, you can now proceed to [Open the Station](#). Otherwise, continue with [Set up a Station](#).

Set up a Station

The Station defines the network(s) that Advanced Plant Controller will interface to. If you did not copy an existing station to the Advanced Plant Controller using the Commissioning Wizard, you will need to create a Station and copy it to the Advanced Plant Controller.

Create a New Station

To create a station:

1. Connect to the Advanced Plant Controller and run Niagara workbench – See [“Connect the Niagara-Installed PC” on page 44.](#)
2. Navigate to **Tools** drop-down menu and click **New Station**. The New Station Wizard is displayed.

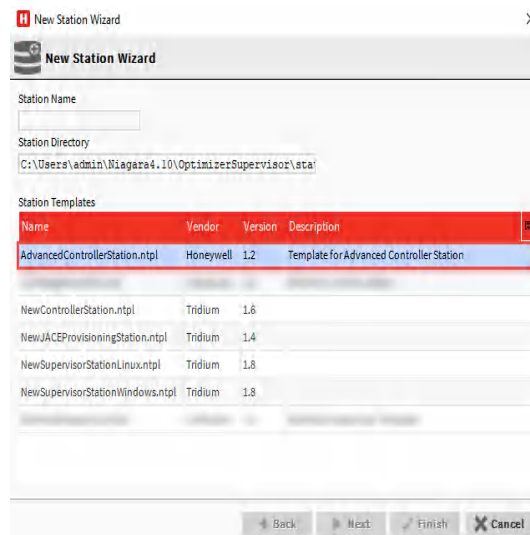


Figure 53. New Station Wizard

3. Enter the name of the station. The Station Directory field, which is non-editable field, displays the location of the station.

4. Select the **NewOptimizerAdvancedControllerStation.ntpl** template from the Station Templates and click **Next**. The next screen of the wizard is displayed.

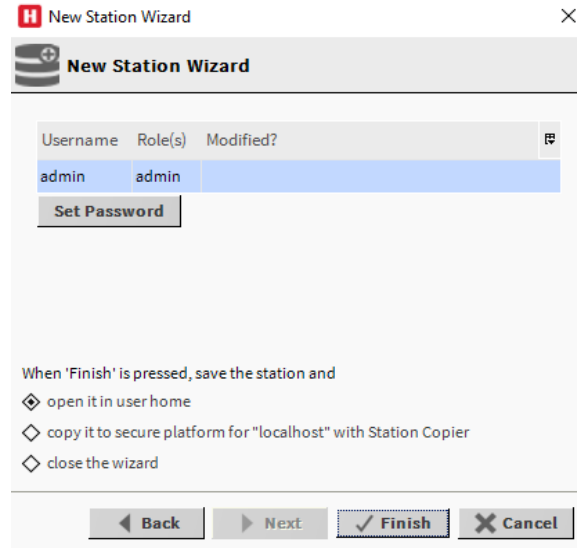


Figure 54. New Station Wizard

5. Click **Set Password** and Set Password window is displayed.

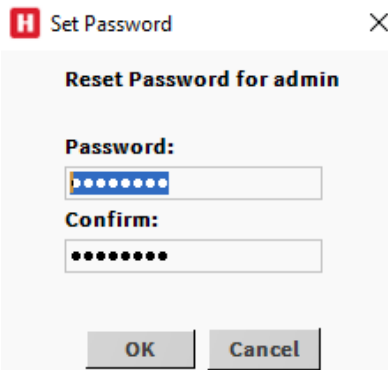


Figure 55. Set Password Dialogue Box

6. Enter the password and confirm it by re-entering the same password in the Confirm field.



NOTE:

This password is for the default 'admin' user for the station. This user must be reserved for engineers. The password must have a minimum of 10 characters and include at least one capital letter, one lowercase letter and one numeral (digit).

7. Click **OK**.
8. Click **Finish**. The station will be created:

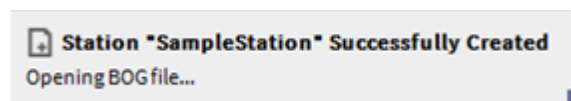


Figure 56. Station Notification After Creating Station

9. Proceed to [Open the Station](#).

Copy a Station using Station Copier

Once you have created a station it must be copied to the Advanced Plant Controller using the following procedure.

To copy a station:

1. Make a platform connection to the Advanced Plant Controller – See [“Open an Existing Platform” on page 56.](#)
2. In the Nav tree right click the Advanced Plant Controller platform and select **Views > Station Copier**.
The Station Copier is displayed:

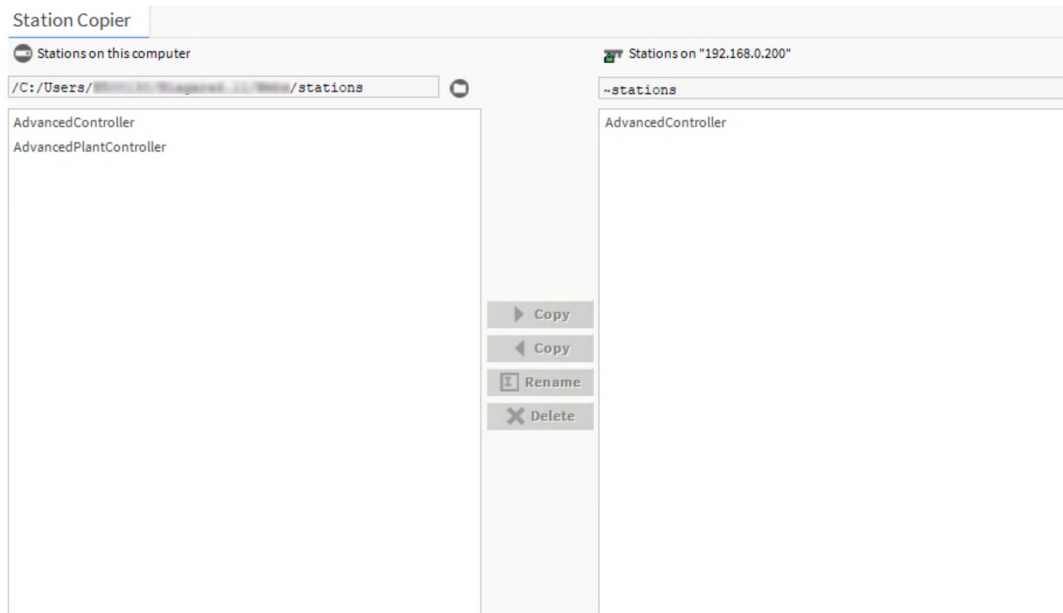


Figure 57. Station Copier Screen



NOTE:

If the user wants to copy the station from controller to computer or from computer to controller, use the same procedure to copy the station. Do the mandatory setup and configuration in the station available in computer and copy that station to the controller – This process is followed in the work flow scenario 2.

3. Click **Copy**. The Station Transfer Wizard is displayed:

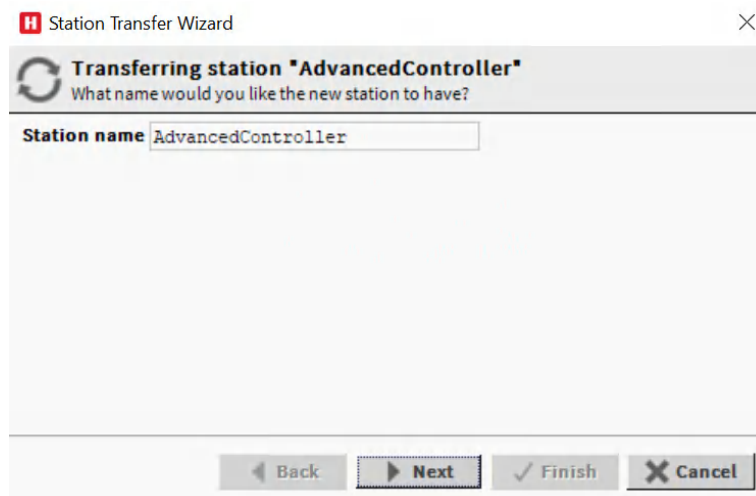


Figure 58. Station Transfer Wizard

ADVANCED PLANT CONTROLLER INSTALLATION INSTRUCTION AND COMMISSIONING GUIDE

4. If required, rename the station in the **Station name** box, then click **Next**. The wizard changes: Select the options—**START AFTER INSTALL** and **AUTO-START** as required and click **Next**.

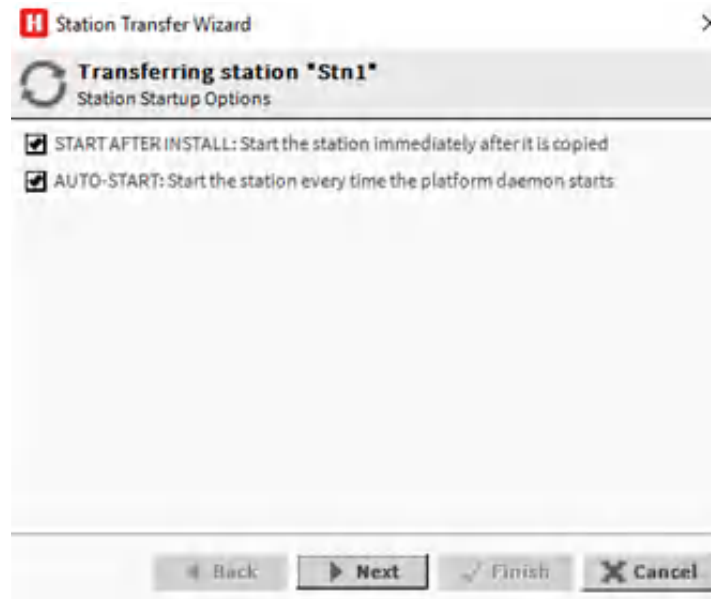


Figure 59. Station Transfer Wizard

5. Select the required start-up options.

**NOTE:**

START AFTER INSTALL: Select this option if you want to start the station as soon as it has copied (recommended).

AUTO-START: Select this option if you want the station to be started when the Advanced Plant Controller is restarted (recommended).

6. Click **Next**. Review the changes from **Station Transfer Wizard** and click **Finish**. The transfer process will commence, and progress is shown in the Transferring station dialogue box:

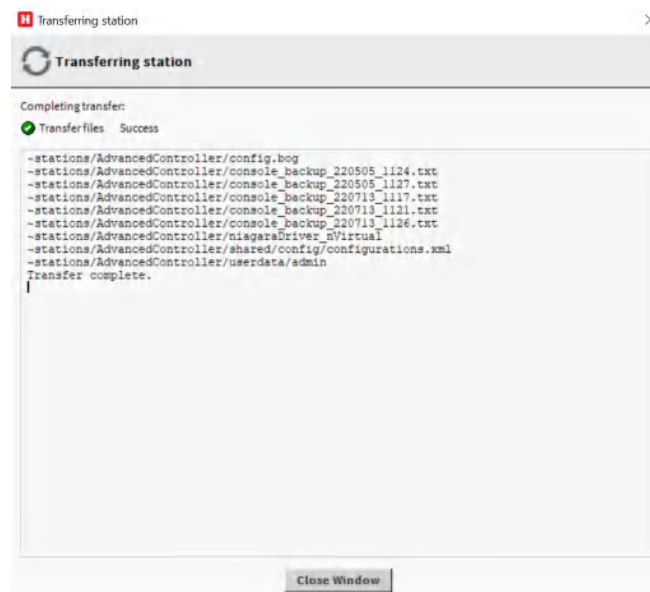


Figure 60. Transferring Station Dialogue box

7. Wait until the message 'Transfer complete' appears.
8. Click **Close Window**. The **Open Application Director** dialogue box is displayed:

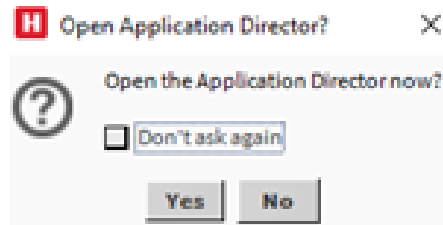


Figure 61. Open Application Director Dialogue Box

9. Click **Yes** and the application director is displayed with the station that you created in the list of stations along with station details like name, type, status, and so on.

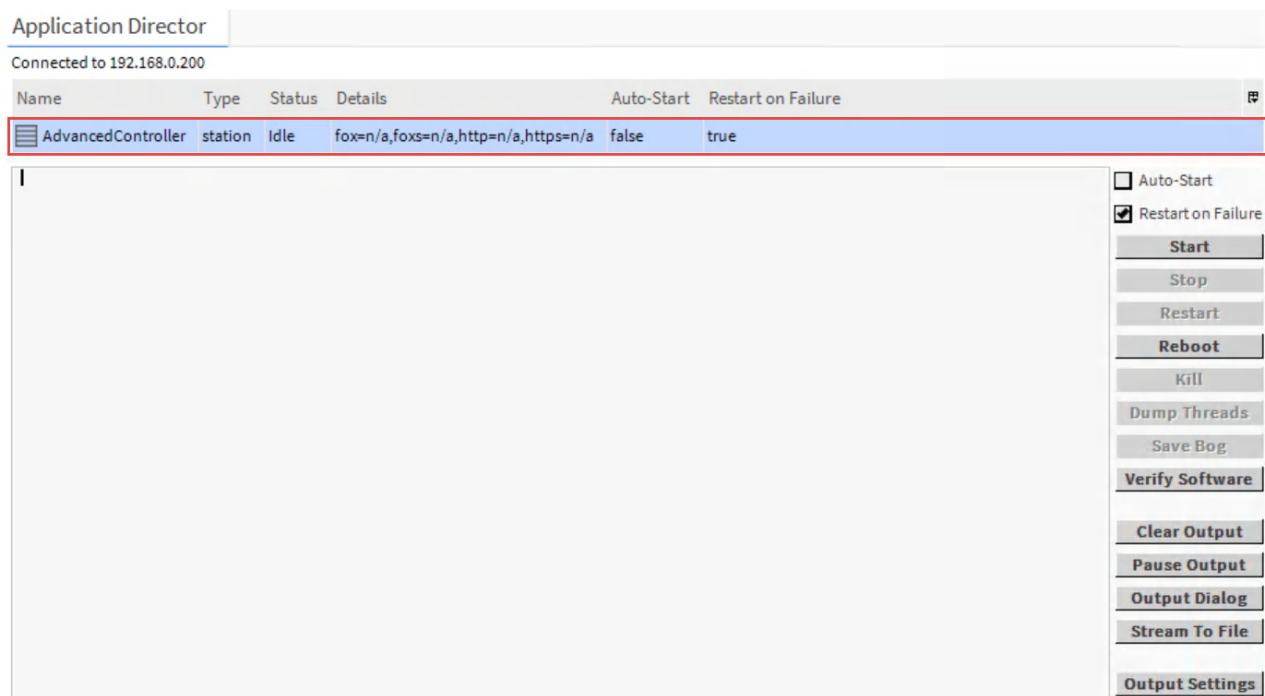


Figure 62. Application Director

10. Wait for the station to start up - this make take up to a minute. Check that a 'Station Started' message is shown. In addition, Status at the top of the window will change from 'Starting' to 'Running'.
- or
11. Select the station to start.
12. Clear or select the **Auto-Start** and **Restart on Failure** check boxes as required.
13. Click **Start** to start the station.
14. Proceed to [Open the Station](#)

Open the Station

To login in to and set up a station:

1. Navigate to the Nav tree and right-click <**IP address of Advanced Controller**> or <**My Host**> and click **Open Station**. The Connect window is displayed. Below figure is shown as an example.

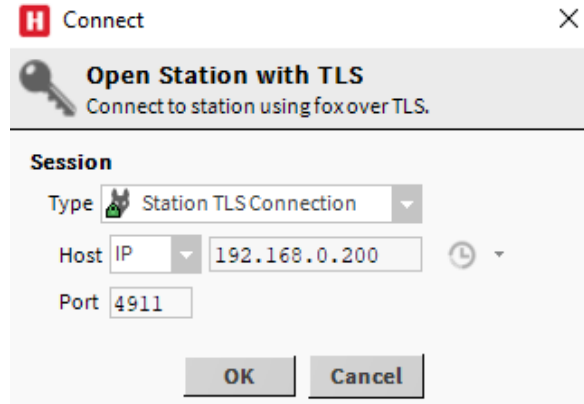


Figure 63. Connect Dialogue Box

2. Select the station type as **Station TLS Connection** (secured) or **Station Connection** (unsecured / standard) in the Type drop-down menu.
3. Select the host as **IP or Host ID** in the Host drop-down menu.
4. Enter the host Id in the input field next to Host. By default, the application takes the host Id of your system. If you select the secured platform type the default port number is 4911 and if you select the unsecured, the port is 1911.



NOTE:

The  (History) icon next to the host Id displays the list of host Ids used before. You can also select the host Id from the History drop-down menu.

5. Click **OK**. The Authentication window is displayed.

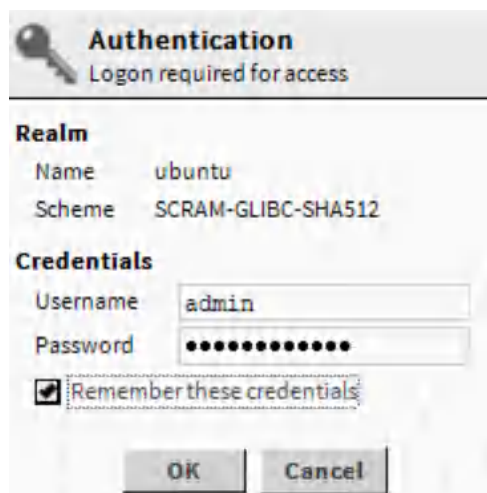


Figure 64. Authentication Dialogue Box

6. Enter the credentials and click **OK**. You must login with station credentials.

Configure TCP/IP Settings

The initial configuration of the Advanced Plant Controller Ethernet ports can be performed as part of the commissioning wizard - See [“Commissioning the Advanced Plant Controller” on page 58](#). If this step was skipped, or if the settings need to be changed at some point, follow the procedure below.

Configure TCP/IP settings:

1. Make a platform connection to the Advanced Plant Controller - See [“Open an Existing Platform” on page 56](#).
2. Double-click on **TCP/IP Configuration**. The **TCP/IP Configuration** view is displayed:

Figure 65. TCP/IP Configuration Dialogue Box

3. In the **IPv4 Gateway** box enter the IP address of the default router on the network. Default is 192.168.0.200/24 or 192.168.0.200/24 - See [“Default IP Address” on page 11](#).

IMPORTANT:
An IP address must be specified even if there is no router on the system. In this case, you must enter IP address that is valid for the network.

4. Click Interface 1. The display expands to show the settings for the primary (LAN1) Ethernet port.

Figure 66. TCP/IP Configuration window

5. In the **IPv4 Address** box enter the Advanced Plant Controller's IP address.
6. In the **IPv4 Subnet Mask** box enter required subnet mask.
7. If required, click **Interface 2** to change the settings for the secondary (LAN2) Ethernet port.

**NOTE:**

Configure only one Interface port with DHCP (Dynamic) and one Interface port with Static form Interface 1/Interface 2 port.

Example: Configure scenario as below

- Interface 1 = DHCP, Interface 2 = Static
- Interface 1 = Static, Interface 2 = DHCP
- Interface 1 = Static, Interface 2 = Static

Both the Interface port cannot be configured with DHCP at the same time. Only one interface can support a Default router/Gateway setting.

8. Click **Save**. If any changes require the Advanced Plant Controller to be rebooted, the following prompt will be displayed:

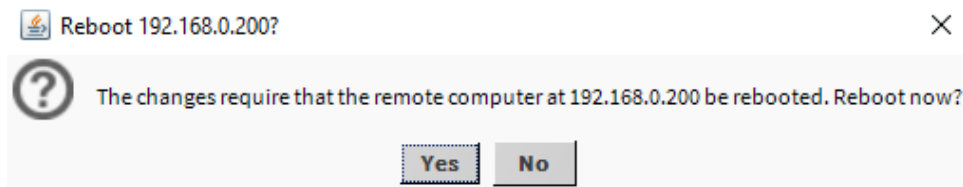


Figure 67. Reboot Dialogue Box

Figure 68.

9. Click **Yes** to reboot now. Click **OK** from The Rebooting dialogue box is displayed.
10. Observe the Ring LED indicator on the front of the Advanced Plant Controller unit - when this has solid green LED ON for at least 10 seconds, the setup process is finished and ready for use.
11. Click **OK**.
12. If you changed the primary Ethernet port settings on Advanced Plant Controller remember that you may now need to:
 - Change the IP settings on the configuration PC to restore communications between the PC and Advanced Plant Controller.
 - Open a new platform in the Niagara workbench Nav tree - See [“Open a New Platform” on page 52.](#)

Import Licenses into License Manager

The License Manager lets you install (import) licenses and certificates to a remote platform, sourced either from your Workbench PC or the Niagara licensing server. You can also view the contents of licenses and certificates, and if desired, delete them from a remote platform. Import Licenses to host and platform.

1. Go to **Platform**, click **License Manager** to open Licenses and Certificates.

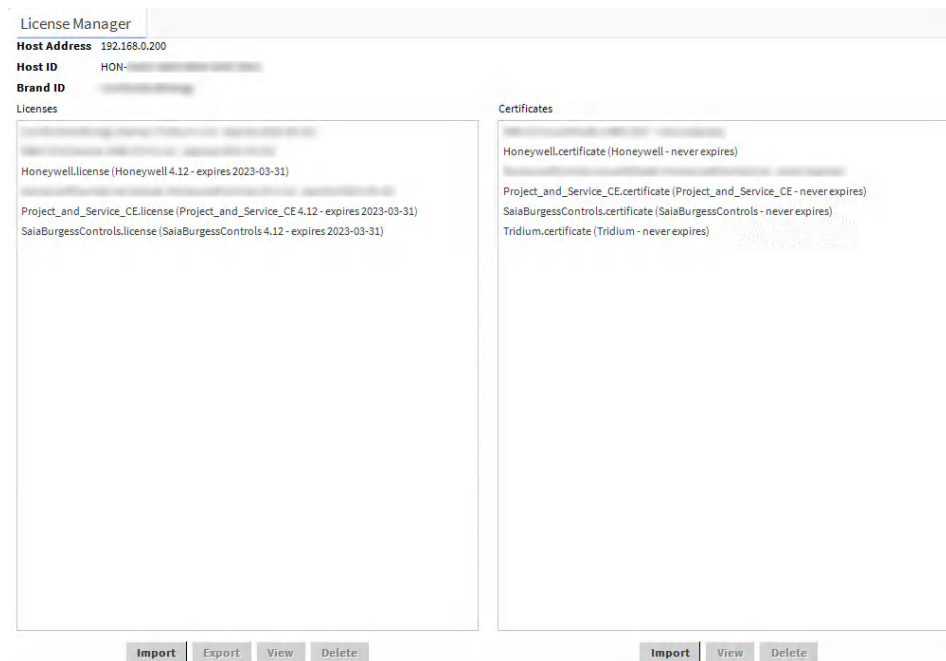


Figure 69. License Manager

2. Click **Import** button to import licenses and select **Import Honeywell BEATS Advanced Lab test Comfort and Energy brand (Comfort and Energy 4.12) licenses from the licensing server.**

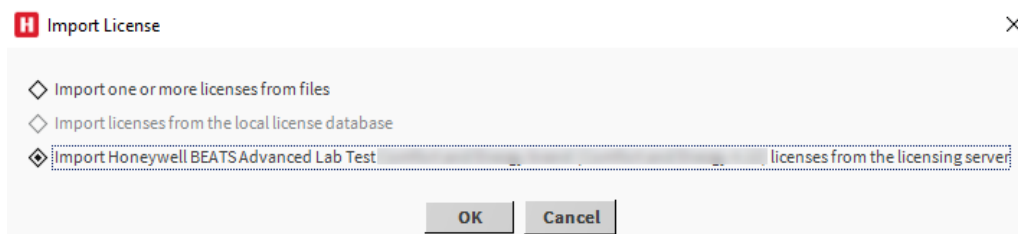


Figure 70. Import License Dialogue Box

3. Click **OK**. Licensing complete dialog box and imported licenses is displayed.

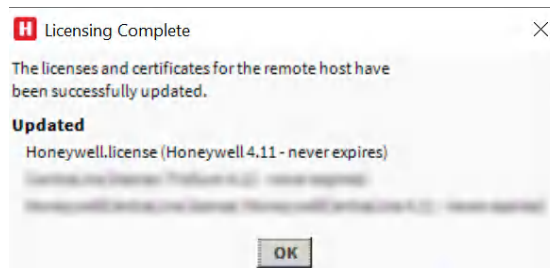


Figure 71. Licensing Complete Dialogue Box

4. Click **OK**.

Change Date and Time

Platform Administration for a Windows-based platform is different from the same for a controller. Change Date/Time from the Platform Administration to sync with system time.

1. Go to **Platform** and click **Platform Administration**.

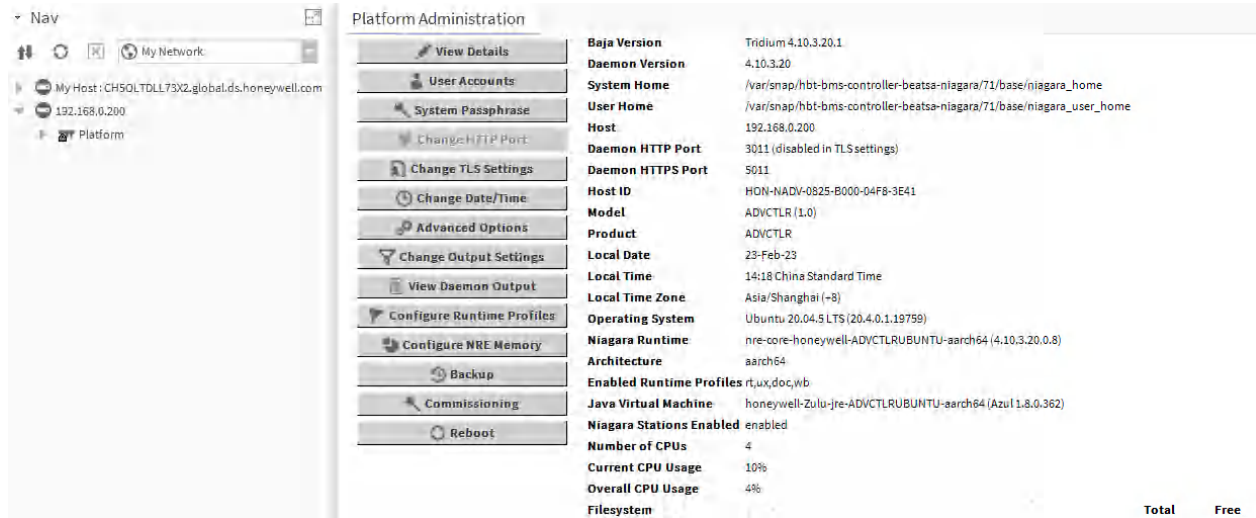


Figure 72. Platform Administration Window

2. Click **Change Date/Time** to change the date and time.

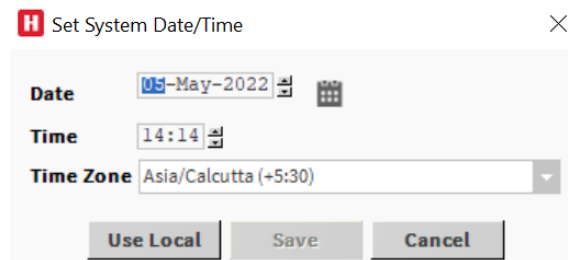


Figure 73. Set System Date/Time

3. Click on **Use Local** and **Save**.

INSTALL ADDITIONAL DRIVERS

If you have purchased additional 3rd party drivers that you did not install when the Commissioning was done, they must be installed before they can be used. If the driver is an additional purchase not included in your original license it will also necessary to update the Advanced Plant Controller's license See [“To install the Advanced Plant Controller refer the Mounting Instructions document \(31-00553\).” on page 11.](#)

The new drivers will be supplied in an email.

To install additional drivers:

1. Close Niagara workbench.
2. Save the driver files from the email to the C:\Niagara\Niagara-4.X\modules folder.
3. Restart Niagara workbench.
4. Make a platform connection to the Advanced Plant Controller - See [“Open an Existing Platform” on page 56.](#)
5. Double-click **Software Manager**. There will be a short delay while the list of software is compiled, after which the **Software Manager** is displayed:

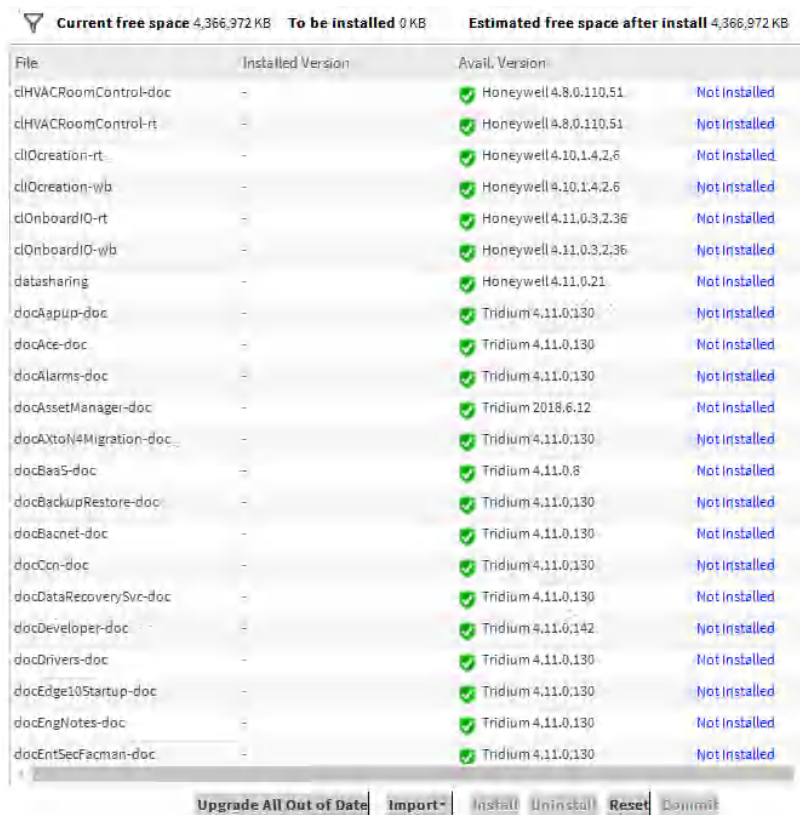


Figure 74. Software Manager window

6. Click the driver that is to be installed to highlight it.
7. Click **Install**. The selected driver and any dependencies will be selected. If necessary, click **OK** in any dialogue boxes that are displayed.
8. Click **Commit**. The driver is installed.

SETUP AND CONFIGURING ADVANCED PLANT CONTROLLER

To configure the Advanced Plant Controller or update the controller, services need to be enabled.

Enable HonPlantControllerService

IMPORTANT: Follow step 1 to step 5 if the **HonPlantControllerService** is not available in the services and if you are using the migrated station. Services will not be available if the user wants to use another controller station other than the advanced controller.

IMPORTANT: Skip step 1 to step 5 and proceed from step 6 if the **HonPlantControllerService** is available in the station services.

1. Navigate to **Window, Side Bars, Palette** to open the palette pane. The palette pane is displayed at the lower left side of the screen.

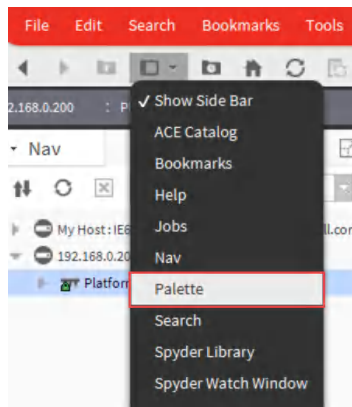


Figure 75. Palette

2. Click  (Open Palette). The Open Palette window is displayed.

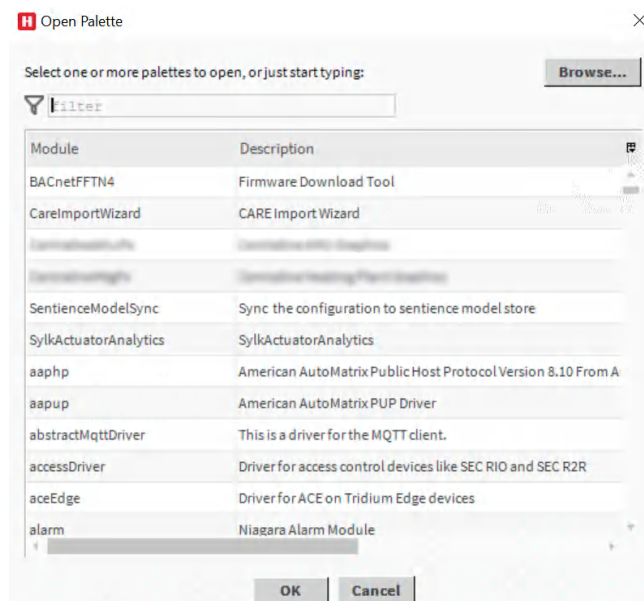


Figure 76. Open Palette Dialogue Box

3. Select the module **honPlantController** from the list or type the module name in the input field to open the palette, and then click **OK**. To select multiple modules, hold the Ctrl key on the keyboard and select the required modules. This adds the selected module to the palette drop-down menu and the palette pane displays the selected palette. The **honPlantController** palette is displayed in palette.

You can also use the Browse button on the Open Palette window to select the path of the module file from the device if you know the module location.

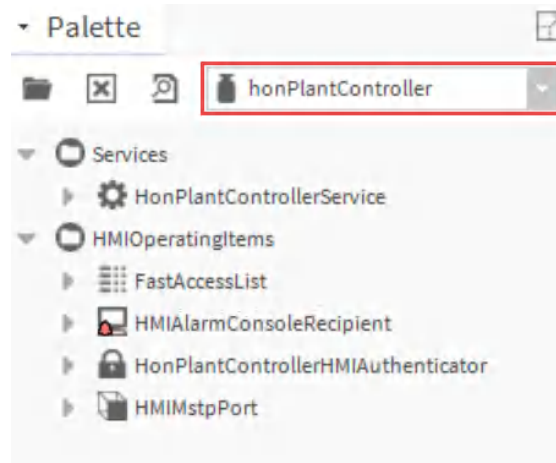


Figure 77. Palette Window



NOTE:

To open another palette, click the palette drop-down menu and select the required palette if present, or open it by clicking the Open Palette icon.

To close the opened palette, click (Close Palette).

To view the preview of an item inside the object in the palette, select the item, and then click (Preview). The preview of the selected item is displayed at the lower side of the palette pane.

4. From the **Nav** tree, expand **Station > Config > Services**. From Palette, select honPlantController and expand Services. Drag and drop the **HonPlantControllerService** from the palette to **Services** folder.

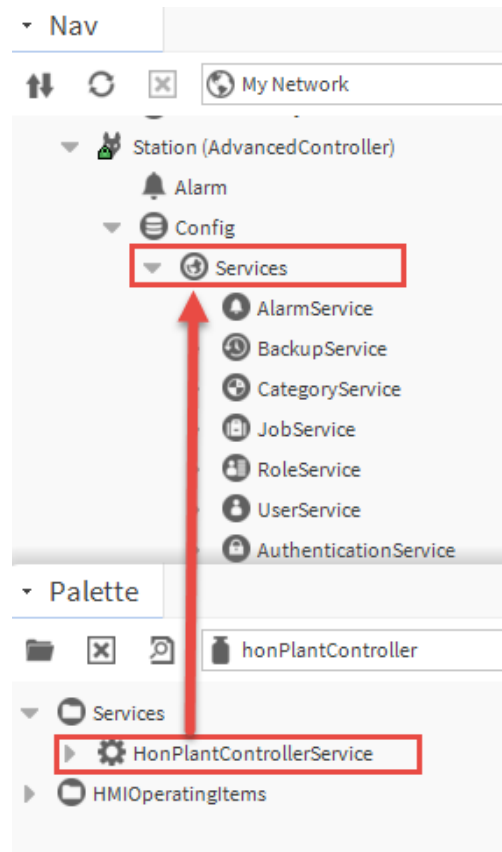


Figure 78. Drag and Drop HonPlantControllerService

NOTE:

Errors with dialogue box will appear while Drag and Drop HonPlantControllerService, which indicates the service “jar” file is not installed properly. Install the “jar” file in Software Manager and commit the Installation. See [“Install Additional Drivers” on page 77..](#)
For installing files in Software Manager, Refer: [module://docPlatform/doc/aSoftwareManager.html](#)

5. A Name dialogue box is displayed. Change the name if desired, and click **OK**.

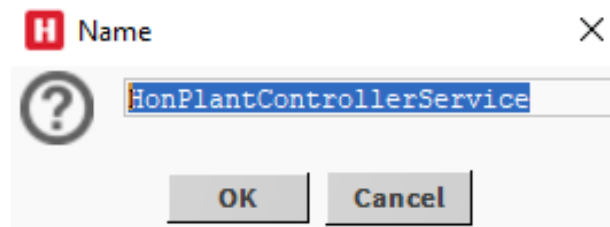


Figure 79. Name Dialogue box

The HonPlantControllerService is added to the Services folder now enable the service.

6. To enable the **HonPlantControllerService** in controller, **Open Platform** - See [“Open a Platform” on page 51..](#)

7. Open a Station - See [“Open the Station” on page 72.](#), if the station is already created or create a station See [“Set up a Station” on page 67.](#)

**NOTE:**

After opening the station Commission the controller - See [“Commissioning the Advanced Plant Controller” on page 58.](#) if the commissioning is not done.

8. From **Nav** tree, expand **Station > Config > Services** and select the **HonPlantControllerService**.

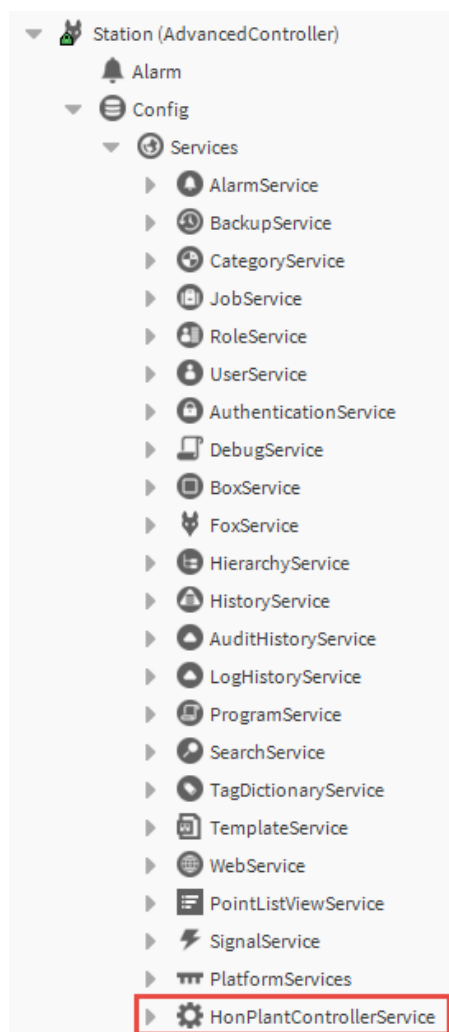
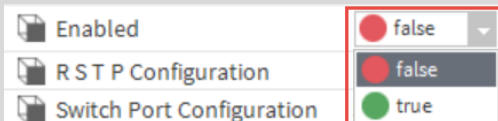


Figure 80. HonPlantControllerService

9. Click **HonPlantControllerService** to display the **Property Sheet** on the right. Navigate to Enable, make **Enable** to **true** to enable the HonPlantControllerService and click **Save**.

**NOTE:**

To enable the service, make the service true. As a Default, the HonPlantControllerService is false.



true to Enable and **false** to disable service.

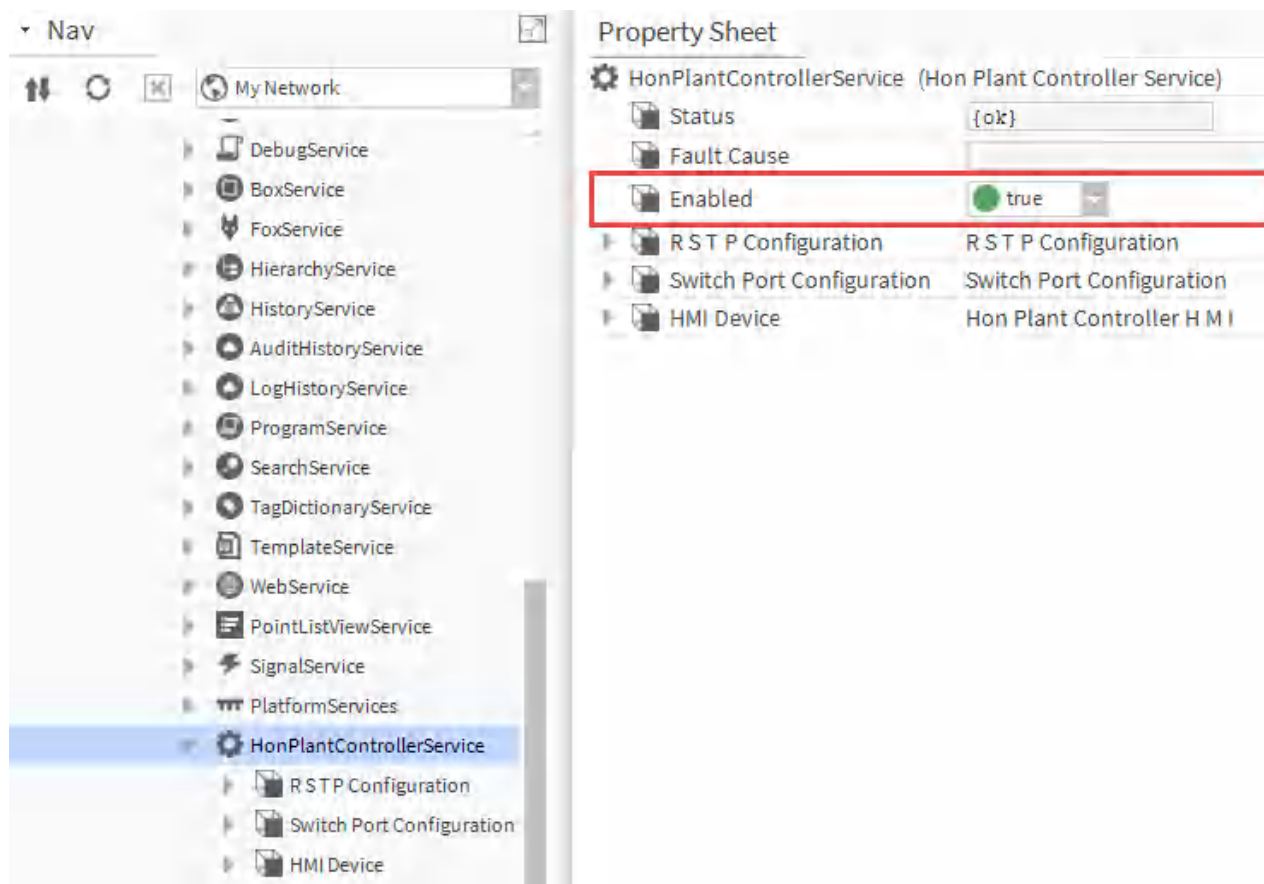


Figure 81. Property Sheet Window

The HonPlantControllerService is enabled.

Setup HMI PIN. Refer HMI Driver Guide - 31-00590.

Enable LED Behavior

The status of the Advanced Plant Controller and its feature status are shown with the different color indication. To identify the status visually, user should enable the LED behavior. To enable the LED behavior in the Advanced Plant Controller the “ledMonitor” jar file should be installed and services has to be added. To install the “ledMonitor-rt” jar file See [“Install Additional Drivers” on page 77](#).

1. Save the driver files “ledMonitor-rt” jar file to the C:\Niagara\Niagara-4.X\modules folder.
2. Follow the procedure [Install Additional Drivers](#) to install the **ledMonitor** jar file and commit.



NOTE:

Installed items will appear in blue text descriptor. Out of Date and items to be installed are at the top of the list and cannot be deselected. Other items can be selected or deselected to suit specific applications.

3. Navigate to **Window, Side Bars, Palette** to open the palette pane. The palette pane is displayed at the lower left side of the screen.

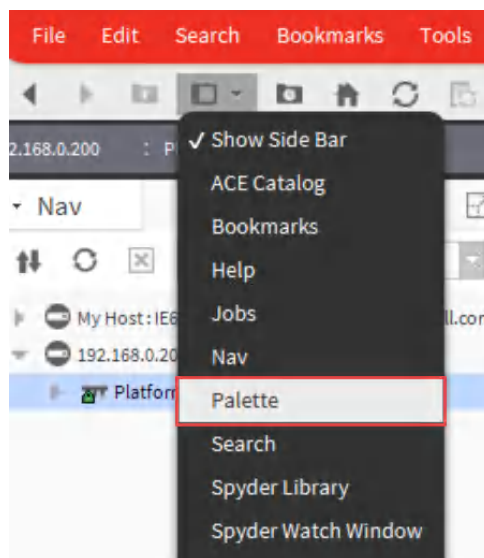


Figure 82. Open Palette

4. Click  (Open Palette). The Open Palette window is displayed.

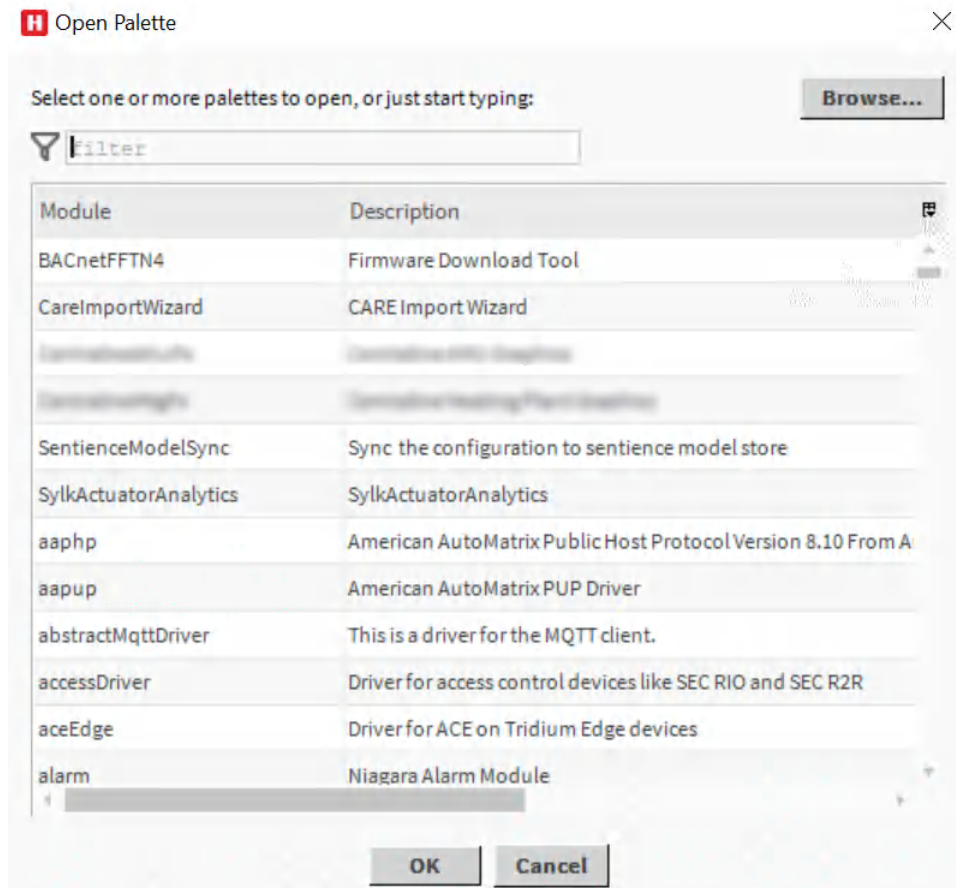


Figure 83. Open Palette Dialogue Box

5. Select the module **ledMonitor** from the list or type the module name in the **filter** input field to open the palette, and then click **OK**.

You can also use the Browse button on the Open Palette window to select the path of the module file from the device if you know the module location.



NOTE:

To open another palette, click the palette drop-down menu and select the required palette if present, or open it by clicking the Open Palette icon.

To close the opened palette, click  (Close Palette).

To view the preview of an item inside the object in the palette, select the item, and then click  (Preview). The preview of the selected item is displayed at the lower side of the palette pane.

6. Drag & Drop the **Ledplatformservices** to **PlatformServices**.

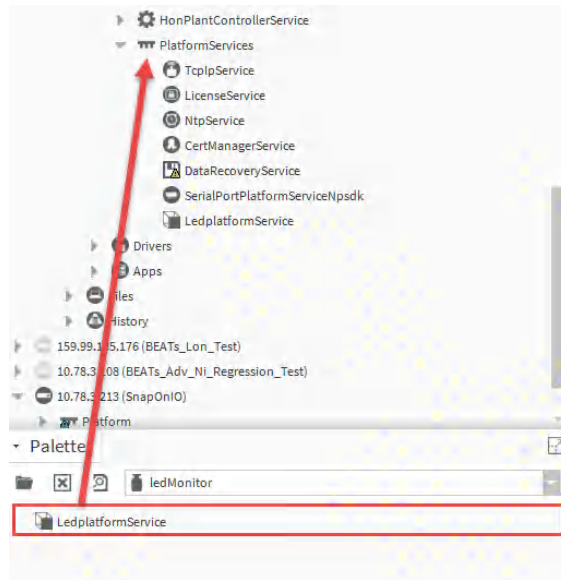


Figure 84. Drag and Drop Services

Led behavior enabled! Repeating the Commissioning is not required.

Email setup

Configuring a system to send and receive email involves adding the email-related components to the Services container and configuring EmailRecipient components. Email components are available in the email and report palettes.

Setting up email components

Two palettes contain email components: the **email** palette and the **report** palette. Change the name of config properties if desired.

Prerequisites: Your station is licensed to use the email feature.

1. For email messaging, open the **email** palette and drag the **EmailService** component to the **Config > Services** container.

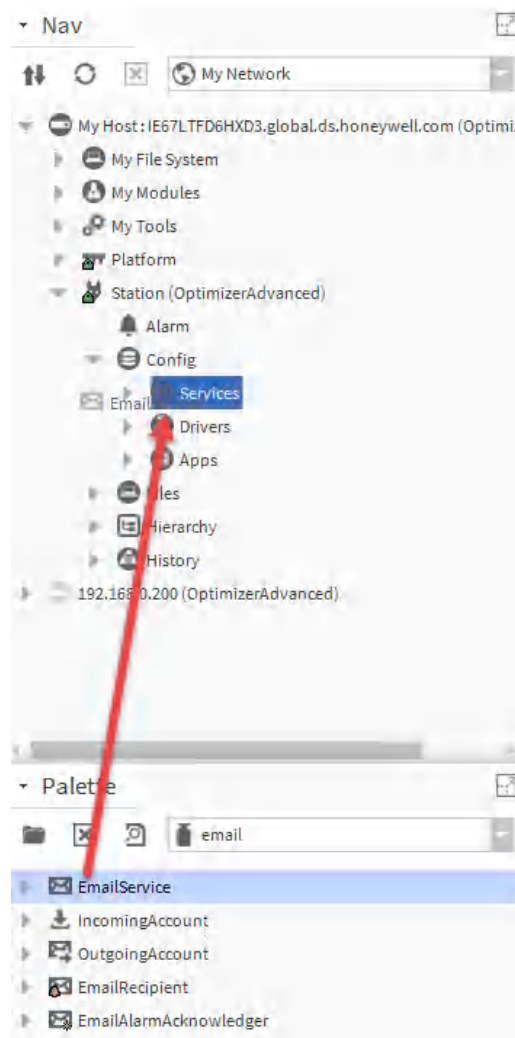


Figure 85. Nav Tree and Palette View

2. From the **email** palette, drag the **IncomingAccount** and **OutgoingAccount** components to the **EmailService**.

You may have multiple incoming and outgoing accounts, which allow you to set up connections to servers that support secure communication and others that may not.

3. Double-click the incoming and outgoing account services and configure properties.

By default, the system deletes all emails from the mail server when it checks the account to retrieve new email, even if the emails are already marked as read by another email client. To permanently retain emails:

- Change the Delivery Policy setting from Delete to Mark as Read or Mark as Unread, or
 - Configure a second service account to which the mail server forwards email, and configure the station's incoming account to check the second service account.
4. To prepare to send alarms via email, drag the **EmailRecipient** from the **email** palette to the **EmailService** node in the Nav tree.
 5. To prepare to acknowledge alarms via email, drag the **EmailAlarmAcknowledger** from the **email** palette to the **EmailService** node in the Nav tree.
 6. For report messaging, open the **report** palette and drag the **ReportService** component to the **Config>Services** container.

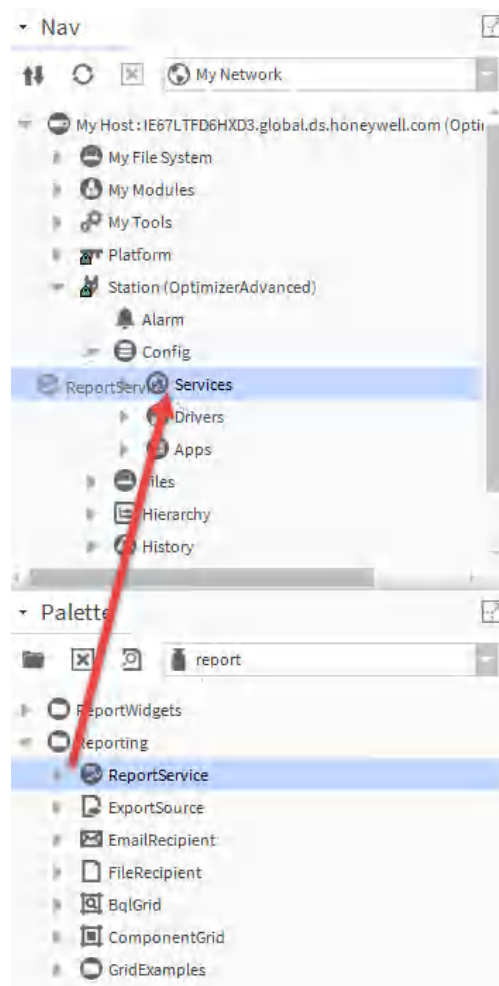


Figure 86. Nav Tree and Palette View

7. To set up email reporting from the station, drag the **EmailRecipient** from the **report** palette to the **ReportService** node in the Nav tree.



NOTE:

Both the **email** and **report** palettes have an **EmailRecipient**. Although these components have the same name, they are not the same component.

Configuring the EmailRecipient

Two **EmailRecipient** components send email from the system. One is in the **email** palette. This component manages alarms that are configured to be sent via email. The second is in the report palette. It manages the sending of reports to one or more specific email addresses.

Prerequisites: The **EmailService** and **ReportService** are available in the station's **Config** and click **Services** container.

1. Right-click the **EmailRecipient** under **ReportServices** or **EmailServices** nodes and click **Views > Property Sheet**.
2. Enter the name and email address of recipient(s) and click Save.

For EmailRecipient of EmailServices. Configure below properties.

Property Sheet

EmailRecipient (Email Recipient)

Time Range: 12:00 AM - 12:00 AM

Days Of Week: ☒ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat

Transitions: ☒ toOffnormal ☒ toFault ☒ toNormal ☒ toAlert

Route Acks: ☒ true

To: Name: Address: + X

Cc: Name: Address: + X

Bcc: Name: Address: + X

Language:

Email Account:

Subject: Niagara Alarm From %alarmData.sourceName% ?

Body: Source: %alarmData.sourceName% ?
Timestamp: %timestamp%
State: %sourceState% / %ackState%
Priority: %priority%
Alarm Class: %alarmClass%
Text: %alarmData.msgText%

Figure 87. EmailRecipient Property Sheet

For EmailRecipient of ReportServices. Configure below properties.

Property Sheet

EmailRecipient (Email Recipient)

To: Name: Address: + X

Cc: Name: Address: + X

Bcc: Name: Address: + X

Language:

Email Account:

Subject: %reportName% from %sys().station.station% ?

Body: Attached is the %reportName% report from %sys().station.station% ?

Figure 88. EmailRecipient Property Sheet

3. Do the same for the alarm **EmailRecipients**.

Securing email

Niagara supports secure outgoing and incoming email using TLS (Transport Layer Security).

Prerequisites: The **EmailService** is in your **Services** container with both **IncomingAccount** and **OutgoingAccount** components. If not, add the **EmailService** component from the email palette before you begin. You may have multiple incoming and outgoing accounts, which allow you to set up connections to servers that support secure communication and others that may not.

Follow this procedure for both your incoming and outgoing accounts.

1. In the station's Nav tree, right-click the **IncomingAccount** or **OutgoingAccount** node under the **EmailService** container and click **Views > Property Sheet**.

The account Property Sheet opens.

 Use Ssl	☐ false
 Use Start Tls	☐ false
 Transport	Smtpt

The system provides two secure communication options:

- The default, Use Ssl, encrypts the connection before it is ever opened. To do the encryption, it automatically uses either SSL v3 or TLS (depending on email server requirements). This provides the most secure data transmission since the connection is encrypted from the start.
- Use Start Tls makes it possible to connect to an unprotected email server. The handshake occurs without encryption, then switches to encrypt the message itself.

Use Ssl and **Use Start Tls** are mutually exclusive. Both may be **false**.

2. To provide secure email, set one property to **true**, and the other **false**. The example shows the configuration when Transport is set to **Smtpt**.

Incoming and outgoing messages use different ports for secure communication as follows:

Table 26. Incoming and Outgoing messages

	Outgoing (SMTP)	Outgoing (IMAP)	Incoming (POP3)
Not encrypted	25	143	110
Use Start Tls	587	143	110
Use Ssl	465	993	995

 **NOTE:**
Not all servers follow these rules. You may need to check with your ISP (Internet Service Provider). Do not enable or disable the Use Ssl or Use Start Tls properties without configuring the Port.

3. Change the Port to the appropriate port number (defaults are: 25 for outgoing and 110 for incoming email). The system also provides server identity verification. For most email servers, the root certificate is already in the **System Trust Store**.
4. If no root CA certificate for the email server is in the station's **System Trust Store** (third-party signed certificate) or in the User Trust Store (your own certificate if you provide your own secure email server), either:
 - Import your own or a third-party signed root CA certificate into the station's **User Trust Store**.
 - Or, if you do not have a signed certificate yet, accept the system-generated, self-signed certificate when challenged. This creates an exemption in the **Allowed Hosts** list. Later, import the root CA certificate and delete this temporary exemption.

RSTP Configuration

The Rapid Spanning Tree Protocol (RSTP) configures the Port State of each Bridge Port in the Bridge Local Area Network.

RSTP is faster than STP in terms of convergence when topology changes occur. The loop-free topology ensures that there are no broadcast storms and duplicate frame transmission.

Table 27. Spanning Tree Algorithm Timer Values

Parameter	Recommended or Default values	Fixed value	Range
Bridge Hello Time	2.0	-	1.0-10.0
Bridge Max Age	20.0	-	6.0-40.0
Bridge Forward Delay	15.0	-	4.0-30.0
Hold Time	-	1.0	-



NOTE:

It is always recommended for a user to keep

Bridge Hello Time default value 2 seconds. Change the default value cause performance issue.

- **Bridge Max Age** recommendation

If user has less than 20 RSTP devices connected, keep the **Bridge Max Age** to default value 20 seconds.

If user has more than 20 RSTP devices connected, keep the **Bridge Max Age** to be the same as the devices number that has RSTP enabled.

Example: If 30 RSTP devices are connected in the environment, set the Bridge Max Age to 30 seconds. The max value is 40s.

- **Bridge Forward Delay** should be changed accordingly when Bridge Max Age change.

Rule: $2 \times (\text{Bridge_Forward_Delay} - 1.0 \text{ seconds}) \geq \text{Bridge_Max_Age}$



NOTE:

You can configure the RSTP from the station settings without connecting to the station each time.

Property Sheet

R S T P Configuration (R S T P Configuration)

Status {ok}

Fault Cause Configuration Loaded from the File Succe

Enabled ☒ false

Override Platform Config On Startup Never

Note

Changes will be written to platform only after performing "Apply RSTP Settings" action on R S T P Configuration (Services->HonPlantControllerService->R

Reboot After Save ☒ false

Bridge Priority 49152

Port1 Priority 128

Port2 Priority 128

Port3 Priority 128

Hello Time 2 s[1-10]

Forward Delay Time 15 s[4-30]

Maximum Aging Time 20 s[6-40]

Rstp Port Role And Status R S T P Port Role And Status Component

Figure 89. RSTP Configuration Properties

Table 28. RSTP Parameters

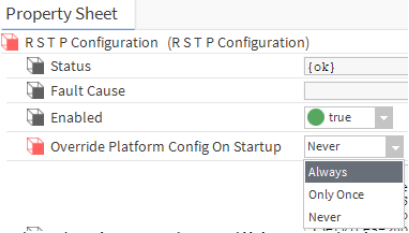
Property	Description
Override Platform Config On Startup	Allows the user to control how and when the RSTP configuration should be copied to the platform.  Always: The RSTP configuration in the station will be copied to the platform each time the station is started. Only Once: The RSTP configuration in the station will be copied to the platform the first time the station is started, or the /RSTP service is enabled. Never: The RSTP configuration in the platform will be copied to the station each time the station is started, or the /RSTP service is enabled.
Status	Read-only. Displays the status of the RSTP configuration (ok/fault).
Fault Cause	Read only. Displays the fault, that caused the RSTP configuration to go into the fault state.

Table 28. RSTP Parameters

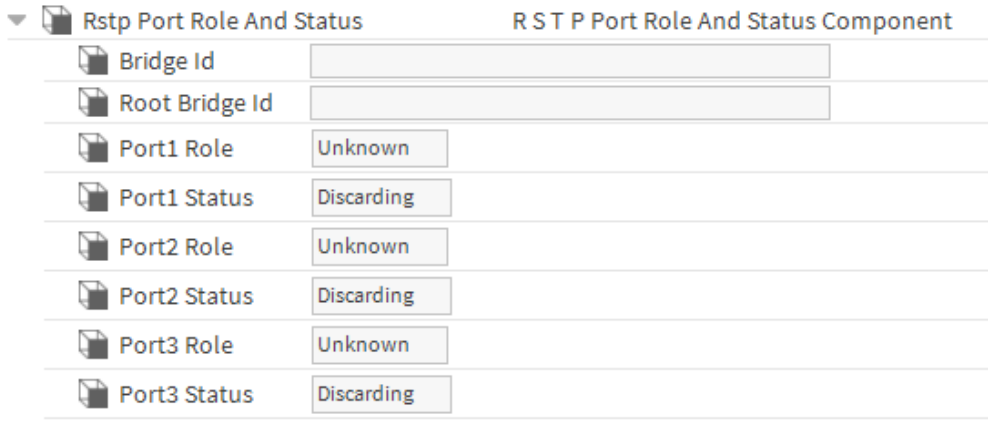
Property	Description																		
Note	Read only. Displays the information, “changes will be written to the platform after performing Apply RSTP Settings on the RSTP configuration components.																		
Enabled	Enables/Disables the spanning tree protocol.																		
Reboot After Save	Specifies if a controller will reboot after the configuration is saved. True - A reboot is required after saving the RSTP configuration change. False - No reboot is required after saving the RSTP configuration change.																		
Bridge Priority	The bridge priority for forwarding the packets. Range = 0 to 61440, 0 is highest priority.																		
Port Priority	Port Priority1 - The port priority for port 1. Range = 0 to 240, 0 is highest priority. Port Priority2 - The port priority for port 2. Range = 0 to 240, 0 is highest priority. Port Priority3 - The port priority for port 3. Range = 0 to 240, 0 is highest priority.																		
Hello Time	The Hello Time interval between transmissions of configuration messages by the root device. Range = 0 to 10 seconds, default = 2 seconds.																		
Forward Delay Time	The maximum amount of time for which the root device waits before changing the states. Range = 4 to 30 seconds, default = 15 seconds.																		
Maximum Aging Time	The maximum length of time old messages remains on the network. This will ensure that old messages do not circulate endlessly on the network. Range = 6 to 40 seconds, default = 20 seconds.																		
Rstp Port Role And Status	Read only. Displays the role and status of each port, that is connected and configured with the device.  The screenshot shows a web interface for the 'Rstp Port Role And Status' component. It features a table with two columns: 'R S T P Port Role And Status Component' and a data column. The table lists the following data: <table border="1"> <thead> <tr> <th>R S T P Port Role And Status Component</th> <th>Data</th> </tr> </thead> <tbody> <tr> <td>Bridge Id</td> <td></td> </tr> <tr> <td>Root Bridge Id</td> <td></td> </tr> <tr> <td>Port1 Role</td> <td>Unknown</td> </tr> <tr> <td>Port1 Status</td> <td>Discarding</td> </tr> <tr> <td>Port2 Role</td> <td>Unknown</td> </tr> <tr> <td>Port2 Status</td> <td>Discarding</td> </tr> <tr> <td>Port3 Role</td> <td>Unknown</td> </tr> <tr> <td>Port3 Status</td> <td>Discarding</td> </tr> </tbody> </table> RSTP adds new bridge port roles to speed convergence following a link failure. The number of states a port can be in, has been reduced to three instead of STP's original five.	R S T P Port Role And Status Component	Data	Bridge Id		Root Bridge Id		Port1 Role	Unknown	Port1 Status	Discarding	Port2 Role	Unknown	Port2 Status	Discarding	Port3 Role	Unknown	Port3 Status	Discarding
R S T P Port Role And Status Component	Data																		
Bridge Id																			
Root Bridge Id																			
Port1 Role	Unknown																		
Port1 Status	Discarding																		
Port2 Role	Unknown																		
Port2 Status	Discarding																		
Port3 Role	Unknown																		
Port3 Status	Discarding																		

Table 28. RSTP Parameters

Property	Description
	RSTP standard Port Roles: • Root - A forward port that is the best port from non-root bridge to root bridge. • Designation - A forwarding port for every LAN segment. • Alternate - An alternate path to the root bridge. This path is different from using the root port • Backup - A backup/redundant path to a segment where another bridge port already connects • Disabled - Not strictly part of STP a network administrator can manually disable a port. RSTP switch port States: • Discarding - No user data is sent over the port • Learning - The port is not forwarding frames yet, but is populating its MAC-address-table • Forwarding - The port is fully operational

After changing the RSTP properties, it is necessary to set **Reboot After Save** to **True** and then **Apply RSTP Settings**, to save the changes in the Advanced Plant Controller.

PROCEDURE

1. Select **RSTP Configuration** and right click **Actions** and select **Apply RSTP Settings**.

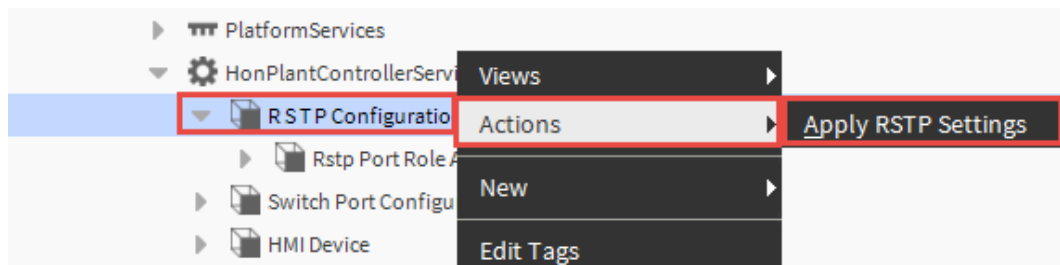


Figure 90. RSTP Configuration



NOTE:

If the user reboots the station without performing the Apply RSTP settings action, any RSTP property changes will not be saved in the Advanced Plant Controller.

Switch Port Configuration

The Advanced Plant Controller (N-ADV-133 series & N-ADV-134-H) has a 3-port Ethernet IP switch. The Switch Port Configuration property sheet allows the user to configure the ports. The Switch port location on the Advanced Plant Controller is shown below.

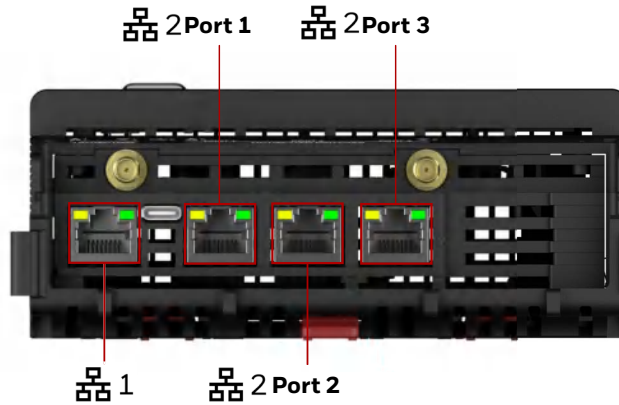


Figure 91. Switch Port

Switch Port Configuration allows the user to configure the Advanced Plant Controller's port using BACnet programming tool. For terminal assignment of ports See [“Terminal Assignment” on page 37](#).

Switch Port Configuration has the following features:

- Enable/ disable ports
- Restrict access to each port to specified MAC addresses
- Allows user to configure Allowed MAC Addresses

TO CONFIGURE A SWITCH PORT:

1. Double click on Switch Port Configuration

Property Sheet

Switch Port Configuration (Switch Port Configuration)

Status {ok}

Fault Cause

Enabled ☒ true

Override Platform Config On Startup Never

Switch Port 1 (Left) Switch Port Config Details

Switch Port 2 Switch Port Config Details

Switch Port 3 (Right) Switch Port Config Details

Figure 92. Property Sheet for Switch Port

2. In the Override Platform Config box specify whether the Ethernet port configuration in the station overwrites the Ethernet port configuration in the platform.
- **Always** - The Ethernet port configuration from the station will be copied to the platform each time an Switch port is enabled in Advanced Controller, each time an enabled Switch port is added to Advanced controller, or each time Advanced Plant Controller station is started with an enabled Switch port.
 - **Only Once** - The Ethernet port configuration from the station will be copied to the platform the first time an Switch port is enabled in Advanced controller, the first time an enabled Switch port is added to Advanced controller, or the first time Advanced Plant Controller station is started with an enabled Switch port.
 - **Never** - The Ethernet port configuration from the platform will be copied to the station each time an Switch port is enabled in Advanced controller, each time an enabled Switch port is added to Advanced controller, or each time Advanced Plant Controller station is started with an enabled Switch port.

**NOTE:**

The Ethernet ports are controlled by the platform's Ethernet configuration therefore copying the configuration from the **station to the platform** (Always and Only Once) will mean the configuration defined in the station is used. Similarly copying the configuration from the **platform to the station** (Never) will set the station's Ethernet port configuration to be the same as the platform's Ethernet port configuration meaning the platform's Ethernet port configuration will be used.

When **Override Platform Config** is set to Always or Only Once, if there is an error in the port configuration an enabled Switch port is added to Advanced controller, or the Advanced Controller station is started with an enabled Switch port., the switch configuration will not be written to the platform.

When Override Platform Config is set to Never, controller station starts, or the Switch port is enabled the switch configuration will be read from the platform and will override the switch port configuration on the station.

Property Sheet

Switch Port 1 (Left)	Switch Port Config Details
Enabled	☒ true
Speed (Mbps)	Disconnected
Status	{down}
Fault Cause	
Config Status	{fault}
Config Fault Cause	Failed to write Switch port configuration to firmware. Please run action "Write Configuration To Platform" on SwitchPortConfiguration (Localdevice->SwitchPortConfiguration) component.
Last Ok Time	null
Last Fail Time	null
Last Fault Cause	
Mode	Disconnected
Connected Device MAC Addresses	
MAC Address Filter	Disabled
Allowed MAC Addresses	
Cable Diagnostics	Cable Diagnostics
Switch Port 2	Switch Port Config Details
Switch Port 3 (Right)	Switch Port Config Details

Refresh Save

Figure 93. Switch Port Configuration Properties

Table 29. Switch Port Configuration Property

Property	Description
Enable	Switch Port 1(left) is read only and always enabled, this prevents the port from being disabled, ensure that it is not possible to be locked out of the controller.

Table 29. (Continued)Switch Port Configuration Property

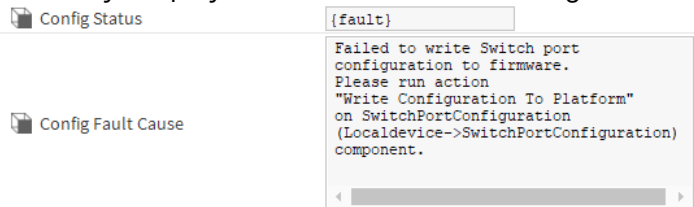
Property	Description
	 NOTE: Switch Port 2, Switch Port 3, and Switch Port 4(Right) are configurable and can be individually enabled/disabled.  Changes to this parameter will take effect immediately after saving. Ensure that the right users get access to enable or disable the switch ports.
Speed (Mbps)	Read only. Displays the connectivity speed of the connected device (10/100/1000/Disconnected).
Status	Read only. Displays the physical status of the port (OK/Down).
Fault Cause	Read only. Displays the reason port is in Down/Fault state.
Config Status	Read only. Displays the configured status • OK - There are no configuration errors on the port • Fault - The port configuration is invalid
Config Fault Cause	Read only. Displays the details of invalid configuration. 
Last Ok Time	Read only. Displays last time when the port is in the OK state.
Last Fail Time	Read only. Displays last time when the port in Down or Fault state
Last Fault Cause	Read only. Displays the details of the last reported invalid configuration reported, which caused controller to go into the Down or Fault state: • Link Down - A device is connected to Advanced Plant Controller port, but the controller does not detect a device connected to the port. • Cable - There is issue with device cable connection.  NOTE: Advanced Plant Controller has auto sensing feature, which allows to detect the ethernet cable connection.
Mode	Read only. Displays the device communication mode (Full/ Half/Disconnected).
Connected Device MAC Addresses	Read only. Displays the MAC address(s) of devices connected to the port.

Table 29. (Continued)Switch Port Configuration Property

Property	Description
MAC Address Filter	Enables/Disables MAC addresses filtering. • Enabled - Only devices whose MAC address listed in the Allowed MAC Address property will be able to communicate with the controller. • Disabled(default) - All the devices connected to the port can communicate with the controller.  NOTE: Enabling or Disabling the MAC address filter will have immediate effect, no restart is required.
Allowed MAC Addresses	The MAC address of devices that user wants to allow to communicate with the Advanced Plant Controller • Only the following formats allowed > FF:FF:FF:FF:FF:FF > FF-FF-FF-FF-FF-FF > FFFF.FFFF.FFFF • Maximum of 16 MAC address • Each MAC address must be on a separate line • Duplicate MAC addresses are not allowed.  NOTE: Changes in the Allowed MAC Addresses property will have immediate effect, no restart is required.

Table 29. (Continued)Switch Port Configuration Property

Property	Description																
Cable Diagnostics	Read only. Displays the cable diagnostics status for all the four cable pairs. • Pair Status - The status of the cable pair (Normal/Open/Short/TestFailed) • Pair Result - The length of the cable, which is basically the location of the issue in the cable, that caused the port to be in the Down state. If any of the pairs display Open/Short/TestFailed status, then the port status is Down. If all of the pair display Normal status, then the port status is OK and port result is 0.00.  Cable Diagnostics Cable Diagnostics <table> <tr><td> Pair A Status</td><td>Good</td></tr> <tr><td> Pair A Result (meters)</td><td>0.00</td></tr> <tr><td> Pair B Status</td><td>Good</td></tr> <tr><td> Pair B Result (meters)</td><td>0.00</td></tr> <tr><td> Pair C Status</td><td>Good</td></tr> <tr><td> Pair C Result (meters)</td><td>0.00</td></tr> <tr><td> Pair D Status</td><td>Good</td></tr> <tr><td> Pair D Result (meters)</td><td>0.00</td></tr> </table>  Note Pair result is cable length represented in meters unit	 Pair A Status	Good	 Pair A Result (meters)	0.00	 Pair B Status	Good	 Pair B Result (meters)	0.00	 Pair C Status	Good	 Pair C Result (meters)	0.00	 Pair D Status	Good	 Pair D Result (meters)	0.00
 Pair A Status	Good																
 Pair A Result (meters)	0.00																
 Pair B Status	Good																
 Pair B Result (meters)	0.00																
 Pair C Status	Good																
 Pair C Result (meters)	0.00																
 Pair D Status	Good																
 Pair D Result (meters)	0.00																
	 NOTE: When a port is connected to a device port with a speed of 100Mbps, the Switch Port configuration may display inaccurate Cable Diagnostics. Sometimes it may display inaccurate cable data length for pairs A, C, and D or display link failure status. When the pair status is reported as normal, the corresponding pair result might report inaccurate data, which can be ignored as the links will be working correctly, if the status is normal.																

Once the changes to the Switch Port Configuration are saved in the property sheet, the switch configuration will be saved in controller platform.

Write Configuration To Platform – Writes the switch port configuration from the station to platform.

Procedure

3. Right click on **Switch Port Configuration**, select **Action**, and click **Write Configuration To Platform**. There are errors in the switch port configuration, the switch port configuration status will be in the Fault state. The changes will not be written in the controller platform until the switch port configuration errors are fixed.

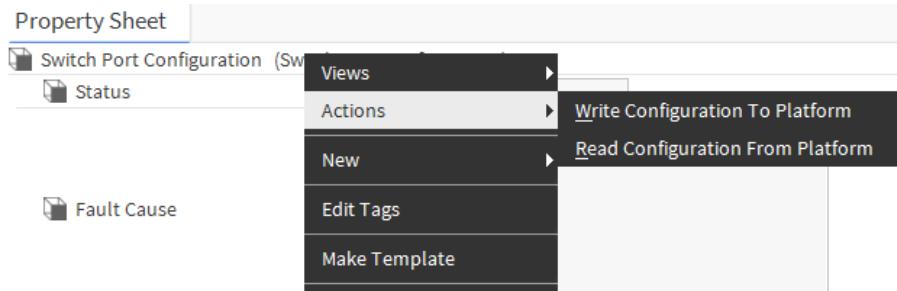


Figure 94. Switch Port Configuration Options

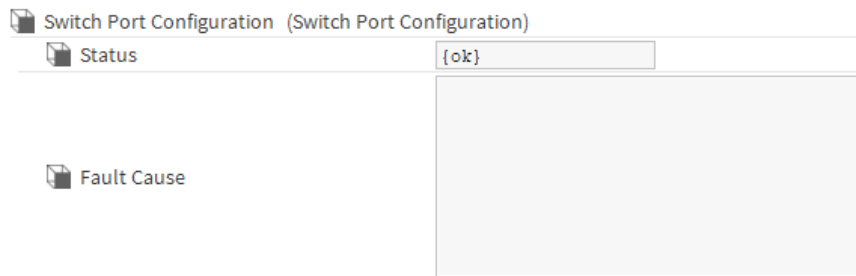


Figure 95. Switch Port Configuration Property Sheet

- **Status** Read only. Displays the outcome of configuration for all the ports.
 - **Ok** - All the ports have a valid configuration.
 - **Fault** - At least one port has an invalid configuration
- **Fault Cause** - Read only. Displays the details of the fault state.

Config Status and **Config Fault Cause** of each port will have details which will help fix the invalid configuration of the switch port.

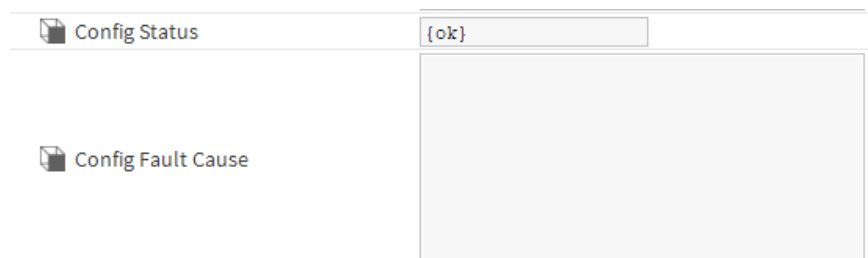


Figure 96. Switch Port Configuration Property Sheet

**NOTE:**

If the Config Status of switch port configuration enters the fault state because of changes made by user, the changes will not be written to the platform.

Once the Config Status returns to OK state i.e. configuration errors are corrected, all the changes made after the switch port configuration entered the fault state will be written to the platform.

Example: In a station, while adding a new MAC address of a device in the 4th switch port, you enter an invalid MAC address. After saving the Switch Port configuration status goes to fault state.

Without fixing the error in the Switch Port configuration, you modified the 1st and 3rd switch port configuration. When you click save, these changes will not be written to controller platform, as the switch port configuration is in the fault state.

To fix the error, you need to check the **Config Status** and **Config Fault Cause** of each port to identify the issue and correct it.

Once the error is fixed and Switch port configuration returns to the OK state the properties that were changed in the 1st and 3rd port 's configuration, while the Switch Port configuration was in the fault state will be written to the controller platform.

Read Configuration From Platform - This action will read switch configuration from platform and overrides switch port configuration in station.

Procedure

1. Right click on Switch Port Configuration, select Action, and click Read Configuration From Platform.

**NOTE:**

If the user has enabled "MAC Address Filter" on all four ports and not configured "laptop/supervisor/programming computer" in any one of the port, then the platform will allow connections only from the MAC addresses that are configured in "Allowed MAC Addresses".

If the user forgets the MAC address of the configured laptop/supervisor/programming computer. Use Serial connection through USB, to reset the switch configuration to default factory settings and can get access to the controller.

Steps to reset switch configuration.

1. Connect the Advanced Plant Controller with the serial console using the terminal emulators tool. Refer to Serial Shell option available in Advanced Plant Controller. See ["USB Backup and Restore using shell command" on page 136](#).
2. In the IPC System Shell, choose "8 Reset switch config" and type Yes <Y> or No<N> to double confirm.

**NOTE:**

After resting the switch configuration, reboot the controller.

CONNECTED DEVICE KNOWN BEHAVIOR

The Connected Device MAC address property displays all learned MAC address on the port, irrespective whether the address is allowed or not.

Example: In the example below, the port receives the packets from the devices with these MAC address, so the source address is learned and displayed.

Whether these devices can communicate successfully with the Advanced Plant Controller depends on the configuration of MAC Address Filter and allowed MAC Addresses.

When the MAC Address Filter set to Enable, only MAC Address listed in the Allowed MAC Addresses property (F0:54:94:00:03:B8) can communicate with the Advanced Plant Controller.

Similarly, when the MAC Address Filter is set to Enable, only the MAC address listed in the allowed MAC addresses property can communicate with the Advanced Plant Controller.

Figure 97. Switch Port Configuration Property Sheet

If a device connected to multiple other devices using a daisy chain connection is connected to the controllers port, then the Connected Device MAC address property displays all the MAC address of all the devices in the daisy chain when all these devices are communicating with the Advanced controller.

Because the MAC address is the list has aging time (default is 300s), if a device stops communication with the Advanced Plant Controller, its MAC address will disappear from the Connected Device MAC Address box after the aging time i.e. 300s ~ 360s.

Example: In the image below, the device F0:54:94:00:03:B8 is connected to multiple other devices using the daisy chain connection type. The Connected Device MAC Address displays, all the connected devices in the daisy chain connection type till they are communicating.

Figure 98. Switch Port Configuration Property Sheet

After the aging time (300s ~ 360s), if there is no communication between the devices and the Advanced Plant Controller. The devices MAC address in the daisy chain connection will disappear from the Connected Device MAC Address list.

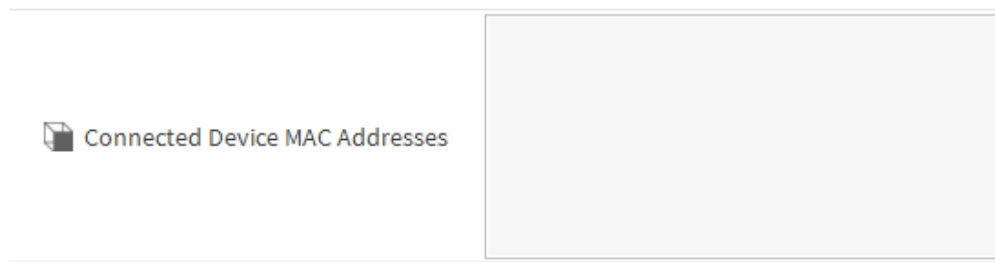


Figure 99. Switch Port Configuration Property Sheet

When a device connected to the controller's port using a daisy chain connection type, the following behavior is expected

- If the RSTP property is Enabled, the expected MAC address is not displayed in the **Connected MAC Address** box for a few seconds.
- If the RSTP property is Disabled, the MAC address is displayed in **Connected MAC Address** box as expected.

HMI Device Configuration

Advanced Plant Controller supplies power to HMI device. HMI device is connected to the Advanced Plant Controller with an RJ11 cable and configured by enabling the HMI device service in the Niagara workbench.

To configure the HMI device in the Niagara workbench, refer document [HMI Driver Guide - 31-00590](#)

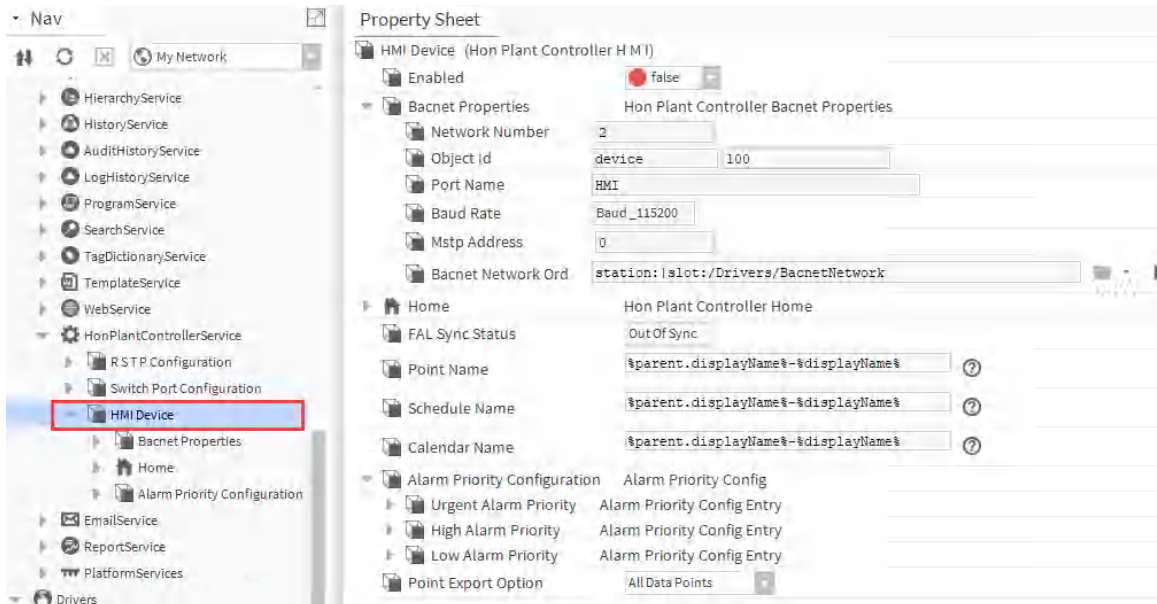


Figure 100. Property Sheet



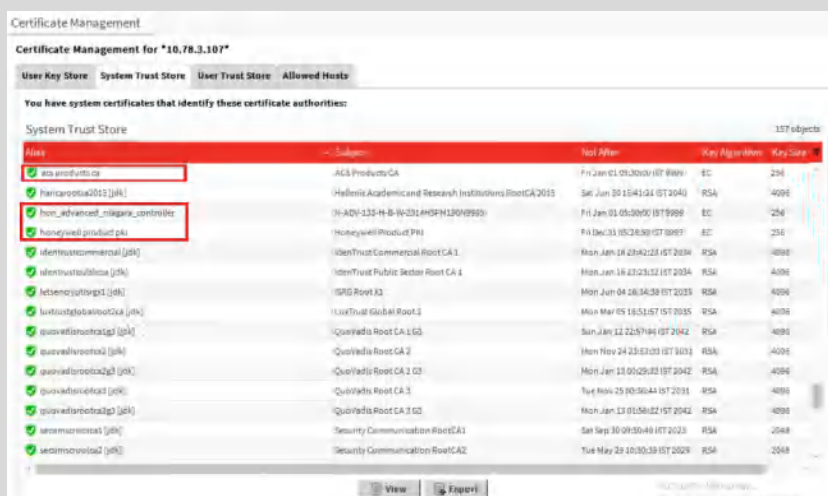
NOTE:

As a pre-requisite please check the System Trust store for below HMI certificates:

- acs products ca
- hon_advanced_niagara_controller
- honeywell_product pki

Procedure:

Open **Platform**, Navigate and open **Certificate Management**. Click on **System Trust Store** tab.



BACNET NETWORK

BACnet (Building Automation Control network) is a data communication protocol developed by ASHRAE (American Society of Heating, Refrigerating, and Air Conditioning Engineers) for managing building automation devices. The BACnet driver uses the standard Niagara Framework® network architecture.

Refer the Niagara BACnet Driver guide for Network setup and for more details:

- Adding a BACnet network in a Supervisor station
- Adding a BACnet network in a controller station
- Configuring a network with an Ethernet port
- Configuring a network with an MS/TP port
- Setting up a controller under the Supervisor's network in the Supervisor station

BACnet Rounting

The Advance Plant Controller can be used in a Router mode to increase the performance and to reduce the load. The BACnet configuration parameters like Apdu Timeout, Number of retries, Max Info frames and other necessary settings needs to be tuned based on the Complex Program / Application Size.



NOTE:

In default settings the Advanced Plant Controller will face the reported issue.
- Devices per MS/TP port = 40 Max (Recommendation). 64 Devices can be connected Max.

If the router function is enabled in the controller, the physical devices will be added to the workbench and the MS/TP ports in controller will acts as router. To enable and check the routing follow below workaround:

Create a Station

Create a station in the local workbench and in the Advanced Plant Controller.

Refer See [“Set up a Station” on page 67.](#)

Add BACnet network

Add the BACnet network IP in the Niagara workbench (Local Host) and in the Advanced Plant Controller.

1. Open **Palette** - click **Window > Sidebars > Palette** and type BACnet.
2. click OK.
3. Expand the station's **Config** container and drag the network component “BACnet” from its palette to the station's **Drivers** container.
The **Name** window opens.

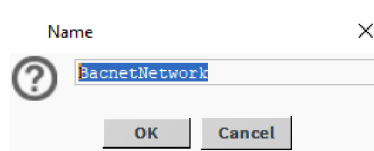


Figure 1. Name Dialogue Box

4. Rename the network, or use the default name, and click **OK**.
The added BACnet network is available under your **Drivers** container.
5. Save the Station.

Enable Routing

Enable the routing in both workbench and controller.



NOTE:

Routing can be possible from Controller to Controller or Workbench to Controller.

Enable Routing in the Advanced Plant Controller:

1. Add the BACnet network
2. Navigate to Station's **Config** > **Drivers** > **BacnetNetwork** > **Bacnet Comm** > Double click on **Network** (Set the view to AX Property Sheet).

Property Sheet	
Network (Bacnet Network Layer)	
Router Table	Bacnet Router Table
Ip Port	NetworkPort: id=1 net=555 enabled max...
Network Number	555
Link	B/IP (10.78.3.176:0xBAC0) Standard
Status	{ok}
Fault Cause	
Poll Service	BacnetMultiPoll
Max Devices	max
Enabled	false
Port Id	1
Port Info	Annex J IP
Routing Enabled	true
Maintain Routing Enabled	false
Minimum Router Update Time	500 ms
Router Discovery Timeout	5000 ms
Termination Time Value	120 s
HMI Port	NetworkPort: id=2 net=2 enabled max=2...
MstpPort	NetworkPort: id=3 net=7722 enabled ma...

Figure 2. Network Property Sheet

- Make the drop down of **IP Port**, **Routing Enabled**, and **Maintain Routing Enabled** to **true**.
IP Port - Provides the connection through the BACnet IP network.

Figure 3. Network Property Sheet

- Click **Save**.
- Enable **MstpPort** (From **Palette** > search **bacnet** > expand **NetworkPorts** > Drag and drop the **MstpPort** to > **Network** under **BacnetNetwork**. If the MstpPort is not available in the BacnetNetwork.)
Change Enabled to **true**.

Figure 4. Network Property Sheet



NOTE:

While configuring/changing the Advanced Plant Controller's MS/TP port with a baud rate, follow the below steps:

- Disable the MS/TP port (Make **Enabled** = false)
- Select the baud rate in the **Link**.
- Enable the MS/TP port (Make **Enabled** = true)
- Restart the Advanced Plant Controller.

- Click **Save**.

Enable Routing in the Workbench:

1. Add the BACnet network
2. Navigate to Station's **Config > Drivers > BacnetNetwork > Bacnet Comm** > Double click on **Network** (Set the view to AX Property Sheet).

Property Sheet

Network (Bacnet Network Layer)

Router Table Bacnet Router Table

Ip Port NetworkPort: id=1 net=1 enabled max=2...

Network Number 1

Link B/IP (10.78.3.218:0xBAC0) Standard

Status {ok}

Fault Cause

Poll Service BacnetMultiPoll

Max Devices max

Enabled false

Port Id 1

Port Info Annex J IP

Routing Enabled true

Maintain Routing Enabled false

Minimum Router Update Time 500 ms

Router Discovery Timeout 5000 ms

Termination Time Value 120 s

Figure 5. Network Property Sheet

3. Make the drop down of **IP Port**, **Routing Enabled**, and **Maintain Routing Enabled** to **true**.

Property Sheet

Network (Bacnet Network Layer)

Router Table Bacnet Router Table

Ip Port NetworkPort: id=1 net=1 enabled max=2...

Network Number 1

Link B/IP (159.99.185.118:0xBAC0) Standard

Status {ok}

Fault Cause

Poll Service BacnetMultiPoll

Max Devices max

Enabled true

Port Id 1

Port Info Annex J IP

Routing Enabled true

Maintain Routing Enabled true

Minimum Router Update Time 500 ms

Router Discovery Timeout 5000 ms

Termination Time Value 120 s

Figure 6. Network Property Sheet

4. Click **Save**.

Add MS/TP Devices in the Advanced Plant Controller

1. Add the MS/TP devices to the Advanced Plant controller to one of the RS485 (RS485-1, RS485-2, RS485-3, RS485-4 or RS485-R).
See See [“Connection to BACnet MSTP Buses with Shielding as Return path” on page 147.](#)
2. Go to Workbench station.
Expand the Station's **Config > Drivers** and double click on **BacnetNetwork** (Set the view to **Hon Bacnet Device Manager**).
3. Discover the devices.
Click **Discover**.

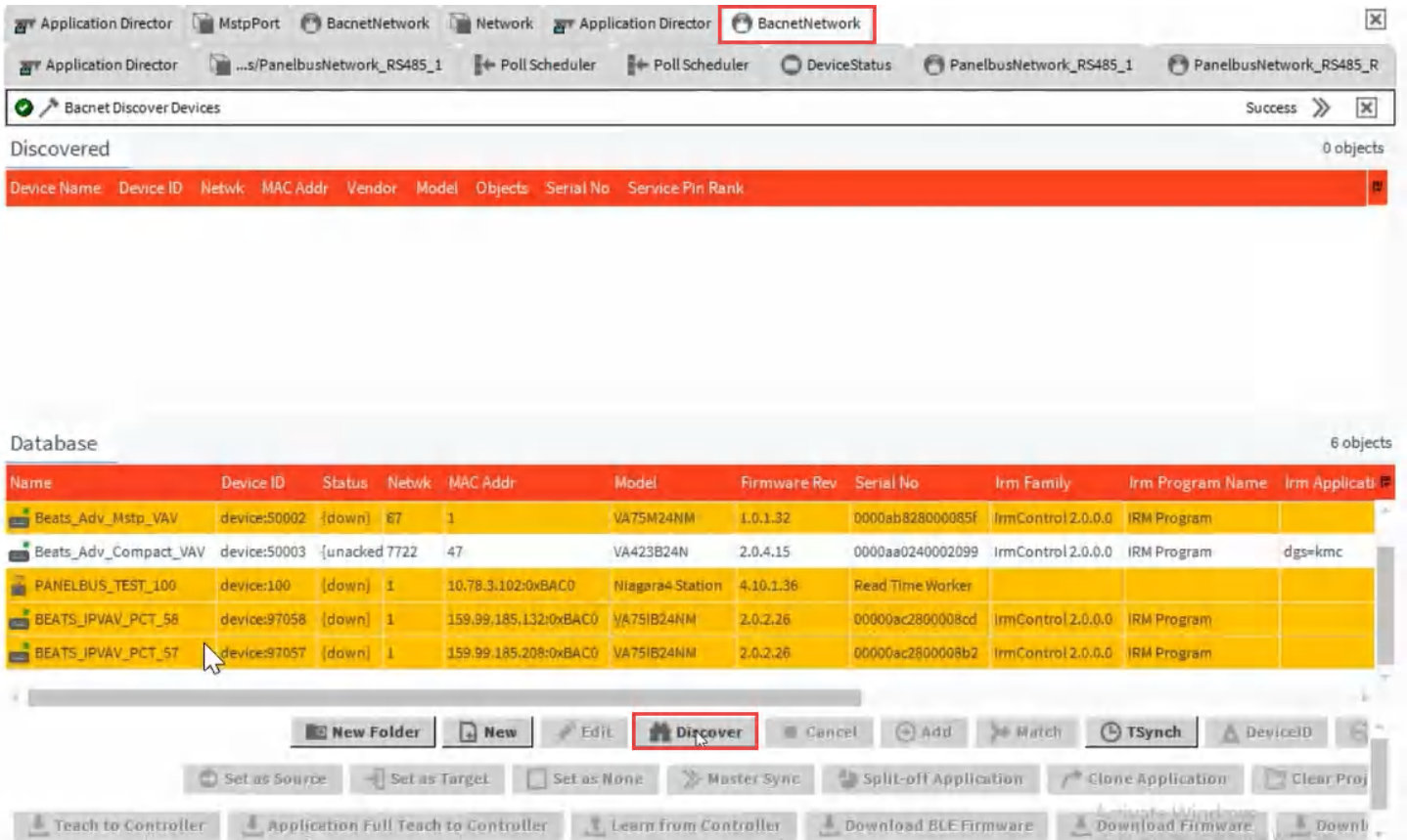


Figure 7. BacnetNetwork Banet Device Manager view

4. A Configure Device Discovery dialogue box will appear.
Optional - Clear all and select the network number from the **Networks** and click **OK**.

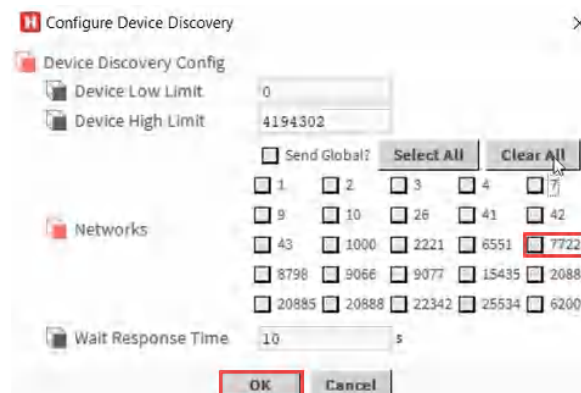


Figure 8. Configure Driver Discovery Dialogue Box

ADVANCED PLANT CONTROLLER INSTALLATION INSTRUCTION AND COMMISSIONING GUIDE

5. The devices will appear in the Discovery section.

The screenshot shows the 'Bacnet Discover Devices' window with a 'Success' status. Below the title bar, there are tabs for 'Application Director', 'MstpPort', 'BacnetNetwork', 'Network', 'Poll Scheduler', 'DeviceStatus', and 'PanelbusNetwork_RS485_1'. The 'Discovered' section shows 3 objects:

Device Name	Device ID	Netwk	MAC Addr	Vendor	Model	Objects
MSTP_VAV	device:60002	7722	9	Honeywell International Inc.	VA75M24NM	168
BEATS_MSTP_FCU	device:60004	7722	13	Honeywell International Inc.	RL1644MSB24NM	24
CPO-RSSN_IRM_FCU	device:60001	7722	15	Honeywell International Inc.	RS5N	151

The 'Database' section shows 6 objects:

Name	Exts	Device ID	Status	Netwk	MAC Addr	Vendor	Model	Firmware Rev	App SW Version
Beats_Adv_CPO_RSSN	[Icons]	device:50001	[down]	68	33	Honeywell International Inc.	RS5N	2.0.3.08	FCU.16777216.0.0_0_0_0
Beats_Adv_Mstp_VAV	[Icons]	device:50002	[down]	67	1	Honeywell International Inc.	VA75M24NM	1.0.1.32	VAV.16777216.16777216.2_30_0
Beats_Adv_Compact_VAV	[Icons]	device:50003	[ok]	1	0A 4F 74 91 BA C0	Honeywell International Inc.	RL1644ESB24NM	2.0.3.31	FCU.0.0.20_0_28_2
PANELBUS_TEST_100	[Icons]	device:100	[down]	1	10.78.3.102:0xBAC0	Honeywell	Niagara4 Station	4.10.1.36	Tridium 4.10.1.36
BEATS_IPVAV_PCT_56	[Icons]	device:97058	[down]	1	159.39.185.132:0xBAC0	Honeywell International Inc.	VA75IB24NM	2.0.2.26	VAV.33554432.117440512.13_0
BEATS_IPVAV_PCT_57	[Icons]	device:97057	[down]	1	159.39.185.208:0xBAC0	Honeywell International Inc.	VA75IB24NM	2.0.2.26	VAV.33554432.117440512.13_0

Figure 9. BacnetNetwork Banet Device Manager view

6. Drag and drop the devices to the **Database**.



NOTE:

The Network number (Example: 7722 in the figure) should match with the Advanced Plant Controller Bacnet-network for routing and communication. See HMI Network Number and HMI Instance Number from the HMI Driver Guide - 31-00590.

Tuning the BACnet properties

When the BACnet network is added in the Advanced Plant Controller, the controller BACnet properties will be default state. Tune the properties helps to increase the performance and reduce the load in controller. Before tuning some BACnet properties, make the controller as router.

Properties to Tune:

- **Max Info Frames** from the Network Property Sheet
- **Apdu Timeout** from the Local Device Property Sheet
- **Number Of Apdu Retries** from the Local Device Property Sheet

Tuning Network Property

Configure the Max Info Frames based on the application size and number of devices connected to the network.

1. Open the Advanced Plant Controller's Station.
2. Navigate to Station's **Config > Drivers > BacnetNetwork > Bacnet Comm > Double click on Network** (Set the view to AX Property Sheet).
Change the Max Info Frames based on the application requirements and number of devices connected to the Advanced Plant Controller.

Figure 10. Network Property Sheet



NOTE:

Max Info Frames Range:

- Default = 20
- Tune Range = [1-100]

3. Click **Save**. (Continue with Tuning Local Device property See [“Tuning Local Device Property” on page 112.](#))

Tuning Local Device Property

Configure the **Apdu Timeout** and **Number Of Apdu Retries** based on the application size and number of devices connected to the network to enhance the performance of the controller.

1. Open the Advanced Plant Controller's Station.
2. Navigate to Station's **Config > Drivers > BacnetNetwork** > Double click on **Local Device** (Set the view to AX Property Sheet).
Change the **Apdu Timeout** and **Number Of Apdu Retries** based on the application requirements and number of devices connected to the Advanced Plant Controller.

Property Sheet	
Firmware Revision	4.10.5.14
Application Software Version	Tridium 4.10.5.14
Location	unknown
Description	Local BACnet Device object
Protocol Version	1
Protocol Revision	14
Protocol Services Supported	1111111111110111110100000111110111110110
Protocol Object Types Supported	111111011101111010110000000010000000000100001101000000
Max A P D U Length Accepted	1476
Segmentation Supported	Segmented Both
Max Segments Accepted	255
Apdu Segment Timeout	2000 ms [0 - max]
Apdu Timeout	3000 ms [0 - max]
Number Of Apdu Retries	3
Database Revision	480
Last Restore Time	XXXX-XX-XX XX:XX:XX.XX
Backup Failure Timeout	00000h 03m 00s [0 ms - +inf]
Backup Preparation Time	00000h 01m 00.000s
Restore Preparation Time	00000h 01m 00.000s
Restore Completion Time	00000h 03m 00.000s
Backup And Restore State	Idle
Character Set	iso10646_U CS2

Figure 11. Local Device Property Sheet



NOTE:

Default Ranges:

Apdu Timeout: - 3000 ms
Number Of Apdu Retries - 3

Recommended Ranges:

Apdu Timeout: - Not More than 20000 ms (Communication gap may occur)
Number Of Apdu Retries - 1 (Decrease the limit based on the Apdu Timeout)

3. Click **Save**.

BACNET/SC (SECURE CONNECT)

The Advanced controller is supported and secure with BACnet/SC. BACnet/SC, added in Niagara, provides a link layer for securing the messages communicated among the Secure Connect nodes of a BACnet network. BACnet Secure Connect (BACnet/SC) uses TLS (Transport Layer Security) version 1.3 to provide strong data encryption and device authentication. With the increased likelihood of cyber attacks on critical infrastructure, including buildings, it is important to secure automation networks. BACnet/SC secures communication on TCP/IP networks using standard IT technologies that are used in critical applications, such as online banking.

TLS is the widely-available protocol that uses PKI (Public Key Infrastructure) keys to encrypt and decrypt data transmissions, and certificates to ensure that only authorized devices can communicate with each other.

With TLS protecting a BACnet network, companies can use a service, such as Qualys, which is a web application and cloud-based service used to detect data breaches and critical misconfiguration across a company's global hybrid environment. E-banking and other critical applications use such services to identify vulnerabilities including cross-site scripting (XSS) and SQL injection.

Refer to the Chapter 8 for BACnet/SC (secure connect) in Niagara BACnet Driver guide for below details:

- BACnet/SC and BACnet/IP
- Message handling
- Node certificates
- Setting up a secure hub
- Creating a direct node connection
- Setting up a secure port
- FAQ

IEEE 802.1X CONFIGURATION

IEEE 802.1X is an IEEE Standard for port-based network access control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

In Niagara 4.12.u2 and later, there is added support for the IEEE 802.1X Wired Authentication standard on the Advanced Plant Controller. On the primary adapter of a the Advanced Plant Controller you have the option to enable 802.1X security on the device.

IEEE 802.1X is a wired authentication protocol that protects a closed network from unauthenticated access. In 802.1X terminology, the remote device or “client” is referred to as the “supplicant”. The Advanced Plant Controller supplicant device requests network access via a port on the secure network. Once successfully authenticated to the port, the supplicant device can access the network.

Refer to the Niagara IEEE 802.1X Configuration Guide for below details:

- Preparation and installation
 - Requirements
 - Installing software
 - Setting up security
- Configuring adapter settings
 - Configuration examples
 - platIEEE8021X-IEEE8021XDaemonSessionPlugin
- Troubleshooting
 - Runtime behavior
 - Additional details in system shell
 - Uninstall
- About IEEE 802.1X Wired Authentication
 - How it works
 - IEEE 802.1X and Niagara
 - About Wired Authentication and SSL connectivity

CONFIGURING PORTS TO ENABLE WEB SERVER FUNCTION

The Advanced Controller provides webserver functionality, e.g., for using the Niagara Supervisor. In order to use webserver functions, the http and https standard port settings can be changed between:

- http standard port: 2 - 65535
- https standard port: 2 - 65535



NOTE:

port is https is a secure port. (Recommended)
 The default port http and https are:
 http: 80
 https: 443

Default port settings are recommended port as standard. If user wants to change the port settings, please follow the below procedure. After the changes are done, the controller is reachable via both pairs of ports, i.e., via the old standard ports and via the newly set ports.

PROCEDURE

1. In the Engineering Tool Nav tree, expand the **Config**, **Services** folder, and then double-click WebService. The Property sheet will appear to the right

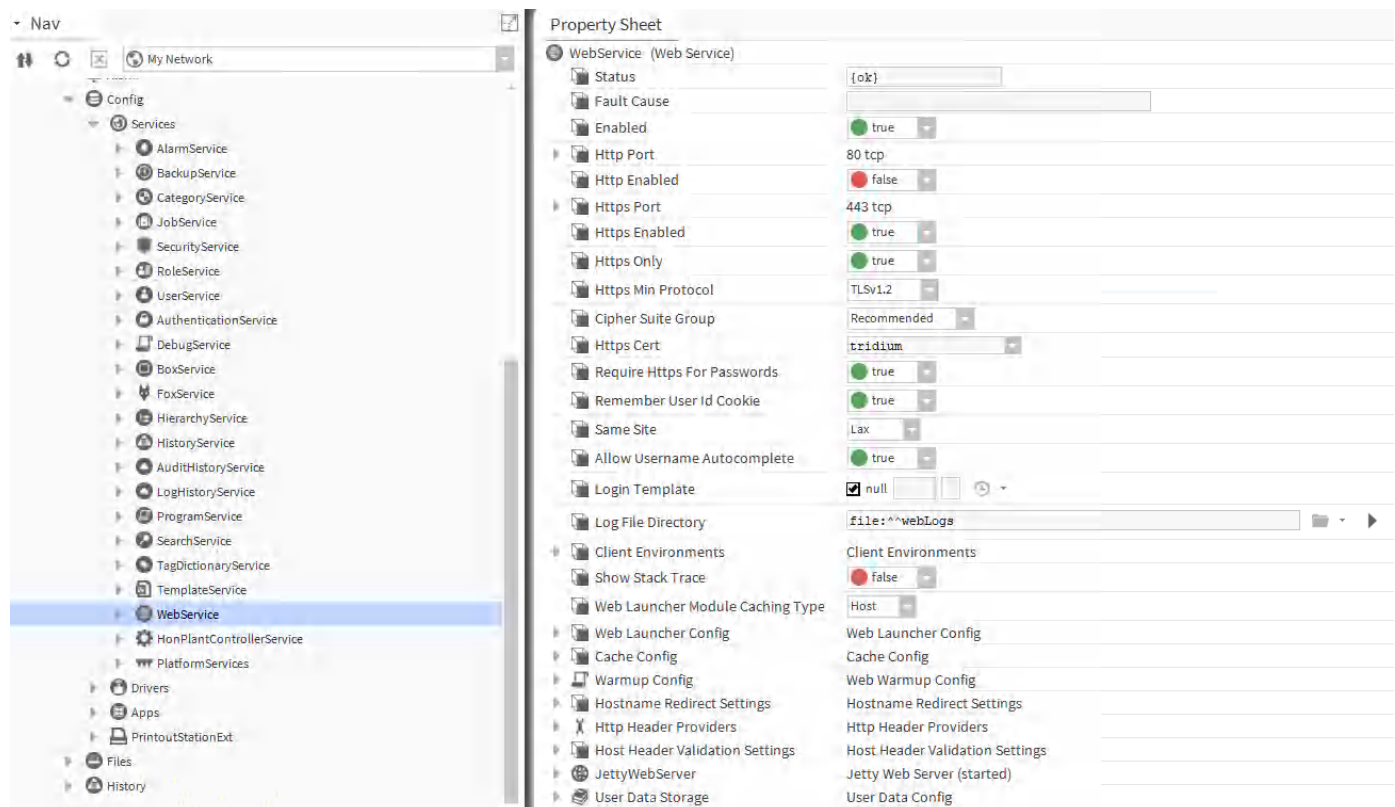
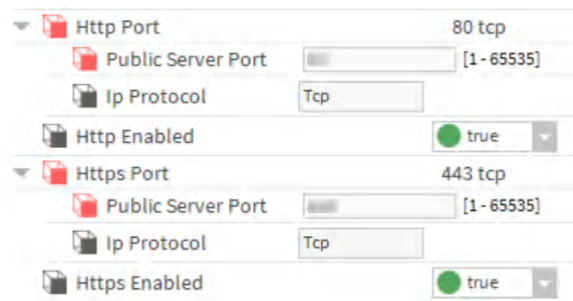


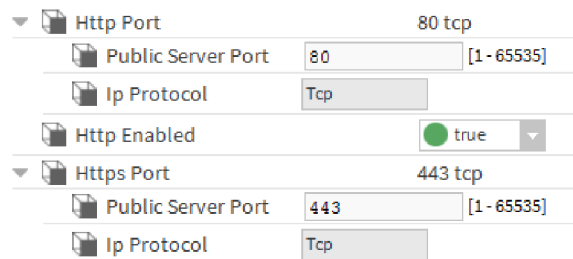
Figure 101. Property Sheet Window

- Expand the Http port, Https Port options, and Enable “**true**” the options.



The screenshot shows a configuration interface with two main sections: 'Http Port' and 'Https Port'. Each section is expanded, revealing its settings. For 'Http Port', the 'Public Server Port' is set to 80, 'Ip Protocol' is set to 'Tcp', and 'Http Enabled' is set to 'true'. For 'Https Port', the 'Public Server Port' is set to 443, 'Ip Protocol' is set to 'Tcp', and 'Https Enabled' is set to 'true'. Each 'Enabled' option has a green circle icon next to it, indicating it is active.

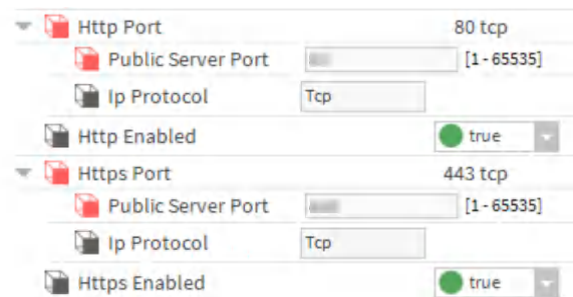
Figure 102. Enable Http and Https Options



This screenshot is similar to Figure 102, but the port numbers have been changed. In the 'Http Port' section, the 'Public Server Port' is now 444. In the 'Https Port' section, the 'Public Server Port' is now 81. The 'Http Enabled' and 'Https Enabled' options remain set to 'true' with green circle icons.

Figure 103. Http Port and Https Port Options

- Change Http Port to 444 and the Https Port to 81 (The values are provided as an example).



This screenshot is identical to Figure 103, showing the 'Http Port' and 'Https Port' sections with 'Public Server Port' values of 444 and 81 respectively, and both 'Enabled' options set to 'true'.

Figure 104. Page to Change Http and Https Option

- Click the **Save** button at bottom to Save the settings.

WIFI CONFIGURATION

Introduction

The Advanced Plant Controller platform feature an integrated IEEE 802.11 module for enabling wireless Ethernet communications to or from the platform. Refer to the [“Ordering Information” on page 2](#). Access Point mode are supported.

By default, these devices ship with the WiFi feature turned OFF. You can enable WiFi using the Niagara workbench, and configure the device for the country of operation. The process of enabling WiFi varies slightly depending on the country the device is shipped to. The initial WiFi setup requires Workbench or serial connectivity. When enabled, you can configure the device as a client to an already established IEEE 802.11 access point and network, or as an access point to establish a new network.



NOTE:

Upgrade the controller firmware with 4.10.5.14.0.16 version before configuring the controller. Refer to the [“Firmware Update using Distribution File Installer” on page 125](#). For Antenna connection, refer to the Optimizer Advanced Controller Mounting Instructions - 31-00553-02

WiFi Specifications

Disabled by default, the WiFi option (on factory configured WLAN-enabled models) can be enabled and configured as an Access Point (ACC) to establish a new network.

- Supports IEEE 802.11a/b/g/n networks
- Configurable radio (AC)
- Supports WPA-PSK, WPA2-PSK security protocols
- Supports 2.4 or 5.8 GHz frequencies
 - 2.4 GHz channels: 2400 MHz - 2483.5 MHz
 - 5.8 GHz channels: 5150 MHz- 5250 MHz, 5250 MHz- 5350 MHz, 5470 MHz- 5725 MHz, 5725 MHz- 5850 MHz
- Single dual band 2.4/5.8 GHz antenna. The antenna may be remotely located using an extension cable.

Enable WiFi

This procedure describes the steps to enable WiFi of the controller from the Niagara workbench.

Prerequisites:

- Controller is licensed and commissioned
- Ensure that the WiFi jar modules honAdvWirelessCfg-rt and honAdvWirelessCfg-wb are available in the Software manager
- Platform connection to the Controller



CAUTION

When enabling more than one Ethernet port (applies to Ethernet port 1, Ethernet port 2, WiFi) the IP address for each must be configured on different subnets, otherwise the ports will not function correctly.

Follow the steps below to enable the WiFi:

1. Go to **Platform Administration**.

- Click **Honeywell Controller Wireless Configuration** from the drop down list.

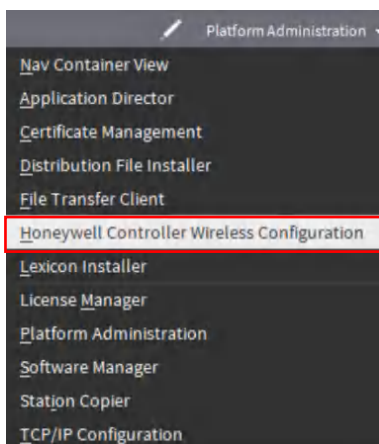


Figure 105. Platform Administration Options

- Select **wifi** from the **Honeywell Wireless Configuration** window.

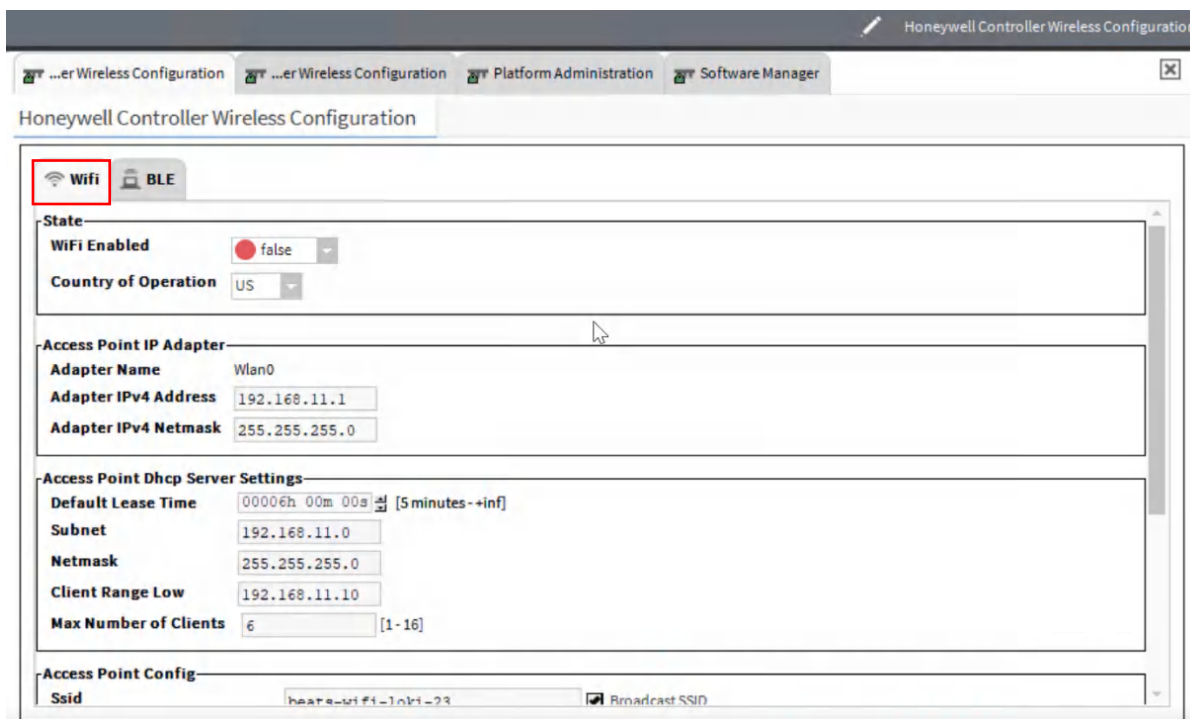


Figure 106. Honeywell Wireless Configuration Window

- Expand the **WiFi Enabled** and enable “**true**” the option.

The screenshot shows the 'Honeywell Controller Wireless Configuration' window. The 'Wifi' tab is selected. Under the 'State' section, 'WiFi Enabled' is set to 'true' (indicated by a green circle and a red box). 'Country of Operation' is set to 'US'. Below this, the 'Access Point IP Adapter' section shows 'Adapter Name' as 'Wlan0', 'Adapter IPv4 Address' as '192.168.11.1', and 'Adapter IPv4 Netmask' as '255.255.255.0'. The 'Access Point Dhcp Server Settings' section includes 'Default Lease Time' (00006h 00m 00s), 'Subnet' (192.168.11.0), 'Netmask' (255.255.255.0), 'Client Range Low' (192.168.11.10), and 'Max Number of Clients' (6). The 'Access Point Config' section shows 'Ssid' as 'hars-wifi-1nki-23' and 'Broadcast SSID' checked.

Figure 107. Honeywell Wireless Configuration Window

- Expand the Country of Operation and select your region.

This screenshot shows the same configuration window as Figure 107, but the 'Country of Operation' dropdown menu is expanded. The options 'US', 'DE', and 'US' are visible, with 'US' at the top highlighted by a red box. The 'Access Point IP Adapter' and 'Access Point Dhcp Server Settings' sections remain unchanged.

Figure 108. Honeywell Wireless Configuration Window

WiFi of the controller is enabled and continue with the [“Configuring WiFi Access Point mode” on page 119](#).

Configuring WiFi Access Point mode

This procedure describes the steps to configure the controller WiFi subsystem to run in Access Point mode. This configuration can be used either as a network for WiFi enabled field bus devices, or to provide browser or Workbench access to local tools.

Configure Access Point IP Adapter

In the Honeywell Controller Wireless Configuration window change the Access Point IP Adapter parameters.

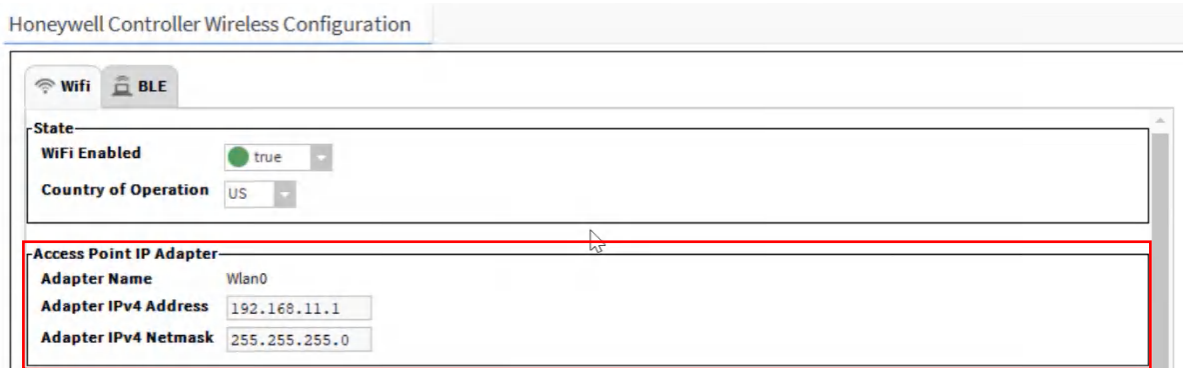


Figure 109. Honeywell Wireless Configuration Window

Table 30. Access Point IP Adapter fields

Property	Value	Description
Adapter Name	Wlan0 (default)	Read only value.
Adapter IPv4 Address	IP address	This sets the IP address of the WiFi adapter. A client uses this to make an IP connection over WiFi while the unit is functioning as an Access Point.
Adapter IPv4 Netmask	IP address	This sets the netmask of the WiFi adapter.

Follow the below procedure to configure the Access Point IP Adapter:

1. Click the Wifi tab and if desired, modify the Adapter IPv4 Address and/or Adapter IPv4 Netmask values. This sets the address that a client uses to make an IP connection to this unit over WiFi while the unit is functioning as an access point.

NOTE:
The IP address and subnet must not conflict with IP addresses used for wired Ethernet connections.

Configure Access Point Dhcp Server Settings

From the Honeywell Controller Wireless Configuration window change the **Access Point Dhcp Server Setting** parameters.

The screenshot shows the 'Honeywell Controller Wireless Configuration' window. It has tabs for 'Wifi' and 'BLE'. Under the 'Wifi' tab, there is a 'State' section with 'WiFi Enabled' set to 'true' and 'Country of Operation' set to 'US'. Below this is the 'Access Point IP Adapter' section with 'Adapter Name' as 'Wlan0', 'Adapter IPv4 Address' as '192.168.11.1', and 'Adapter IPv4 Netmask' as '255.255.255.0'. The 'Access Point Dhcp Server Settings' section is highlighted with a red box and contains the following fields: 'Default Lease Time' (00006h 00m 00s, [5 minutes--inf]), 'Subnet' (192.168.11.0), 'Netmask' (255.255.255.0), 'Client Range Low' (192.168.11.10), and 'Max Number of Clients' (6, [1-16]).

Figure 110. Honeywell Wireless Configuration Window

Table 31. Access Point Dhcp Server Settings fields

Property	Value	Description
Default Lease Time	Time 6 hours (default)	Fixed duration (in hours, minutes, and seconds) for a DHCP IP address lease, before it expires the lease must be renewed.
Max Lease Time	12 hours (default)	Maximum duration (in hours, minutes, and seconds) for a DHCP IP address lease.
Subnet	address	The subnet of IP addresses assigned by the DHCP server. CAUTION Configure this to assign addresses on a different subnet than that used in either of the controller's other LAN configurations, otherwise the ports will not function correctly.
Netmask	number	The Netmask of IP addresses assigned by the DHCP Server.
Client Range Low	address	Lowest IP address for the range. The order of assigning IPs from the Access Point DHCP is indeterminate. NOTE: The adapter IP should be in the same subnet, but not in the range of addresses defined here.
Max Number of Clients	11 (default)	Maximum number of WiFi clients that can attach at a giventime (maximum limit is 16).

Follow the below procedure to configure the **Access Point Dhcp Server Settings**:

1. In the DHCP Server Settings pane, in the **Client Range Low** field, enter the lowest IP address for the range.



NOTE:

The adapter IP should be in the same subnet, but not in the range of addresses defined here.

2. In the **Max Number of Clients** allowed field, enter the maximum number of WiFi clients that can attach at a given time (maximum limit is 16).
3. The WiFi adapter supports a maximum of 6 user interface devices such as, a laptop, PC, or WiFi phone, at a given time. However, this limit is not enforced.
4. Click **Save**.



NOTE:

The saved configuration changes take effect the next time WiFi is started.

Configure Access Point Config

From the Honeywell Controller Wireless Configuration window change the **Access Point Config** parameters.

Figure 111. Honeywell Wireless Configuration Window

Table 32. Configure Access Point Config fields

Property	Value	Description
Ssid	beats-wifi (default)	Service Set Identifier is a unique alphanumeric identifier. Sets the name for this access point. Replace default name with a unique, meaningful network name. NOTE: It is important to change the default value to a unique name to avoid having multiple units with the same SSID in a particular area.
Broadcast SSID	enabled (default), disabled	If enabled, periodically broadcasts WiFi signal so that devices can detect and connect. If disabled, the SSID is "hidden" and not discoverable, and a client must be manually configured with the correct SSID which matches the controller Ssid field above.

Table 32. Configure Access Point Config fields (Continued)

Property	Value	Description
Passkey	text	Sets a password that a client must enter to connect to this network. Strong password required  NOTE: Default Passkey is 12345678
Wpa Mode	WPA WPA2 WPA WPA2 (default)	WiFi security protocols and security certification programs. WPA WPA2 will accommodate most devices. Devices with older network cards may only work with WPA security.
Key Management Algorithms	WPA-PSK (default) WPA-EAP WPA-PSK WPAEAP	Methods of authentication key distribution and the encryption protocols that protect passwords via encryption using either a pre-shared key and/or an authentication server.
Pairwise Cipher Suites	TKIP CCMP TKIP CCMP (default)	Encryption protocol options. TKIP CCMP will accommodate most devices.
Whitelist	list	Allows you to configure the access point with a range of device MAC addresses that can connect.
Enable Whitelist	disable (default), enable	If enabled, only an address in the configured whitelist can connect. If disabled, connection to the access point is not limited to a specific range of devices.
Mode and Channel	Country code: two digit code Radio mode: 802.11a/g/n Bandwidth: HT20, HT40, HT20 HT40 Channel number: (number of channel options depends on selected radio mode)	Once it is configured, County Code is a read only value. The Config Channel button invokes the Configure Mode and Channel dialog, which you can use to modify radio mode, bandwidth, and channel selections.

Follow the below procedure to configure the **Access Point Config**:

1. In the **Access Point Config** area, in the SSID field enter a name for this access point. Best practice is to replace the default name with a unique, meaningful network name.

Click the Broadcast SSID checkbox only if configuring the Access Point for field bus devices so that the devices can detect the access point signal and connect as needed. Otherwise, for security purposes do not click the checkbox.

2. Enter a Passkey for the unit.
This sets a password that a client must enter to connect to this network.

**NOTE:**

Default Passkey is 12345678

3. Click the **Wpa Mode** dropdown list and select the preferred mode. WPA WPA2 (default) will accommodate most devices.
4. Click the **Key Management Algorithms** dropdown list and select an encryption algorithm appropriate for the devices connecting to this network.

5. Click the **Pairwise Cipher Suites** dropdown list and select an encryption suite appropriate for the devices connecting to this network.
6. To configure a **Whitelist**, click the Enable Whitelist checkbox and then click the Whitelist button to enter MAC addresses that will be permitted to join the network (up to 16 addresses).

A “whitelist” is an inventory of known MAC addresses that are permitted (or denied) access to the WiFi access point, functioning as an added layer of protection for the WiFi network. The format is six HEX addresses separated by a colon, for example: d8:f2:ca:87:85:07

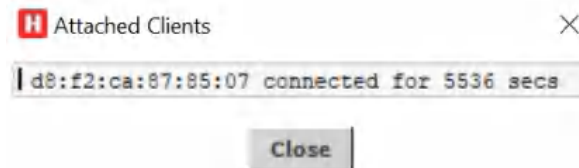


Figure 112. Attached Clients Window

7. To configure Mode and Channel properties, click the Config Channel button and select from the following:

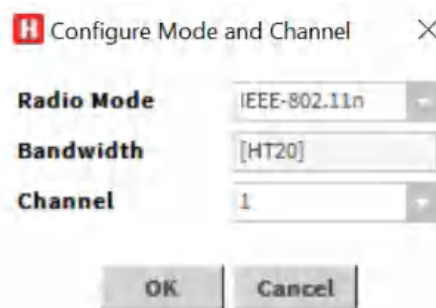


Figure 113. Configure Mode and Channel Window



NOTE:

For WW models, if the country code is not pre-configured then you must set it. For US models, the country code is pre-configured at the factory and cannot be changed.

- a. Click the **County Code** dropdown list and select the appropriate two-digit country code.
 - b. Click the **Radio Mode** dropdown list and select an appropriate 802.11 type for the devices connecting to the network.
 - c. Click the **Bandwidth** dropdown list and select the preferred frequency band. The HT20 HT40 (default) option accommodates most devices.
 - d. Click the **Channel** dropdown list and select the least congested channel number for your network.
 - e. Click **OK**.
8. Click **Save**.

WiFi Access Point for local tool connections

In this configuration, the controller Access Point feature is turned on temporarily to provide a browser or Workbench with access to the platform and/or station running on the unit. The Access Point may support 6 or more simultaneous tool connections.

When configured for Access Point mode, tools such as laptops and mobile devices can connect to the WiFi adapter and access all features available over a wired Ethernet connection. For example, a tablet device can view web pages, or a laptop running Workbench can upgrade software.

FIRMWARE UPDATE USING DISTRIBUTION FILE INSTALLER

1. Check the firmware version installed in your Advanced Controller as follows:
Open Engineering Tool, go to the Platform - See [“Open a Platform” on page 51](#). Double click on **Platform Administration**, and check the version of the **Niagara Runtime** installed in the Advanced Controller.

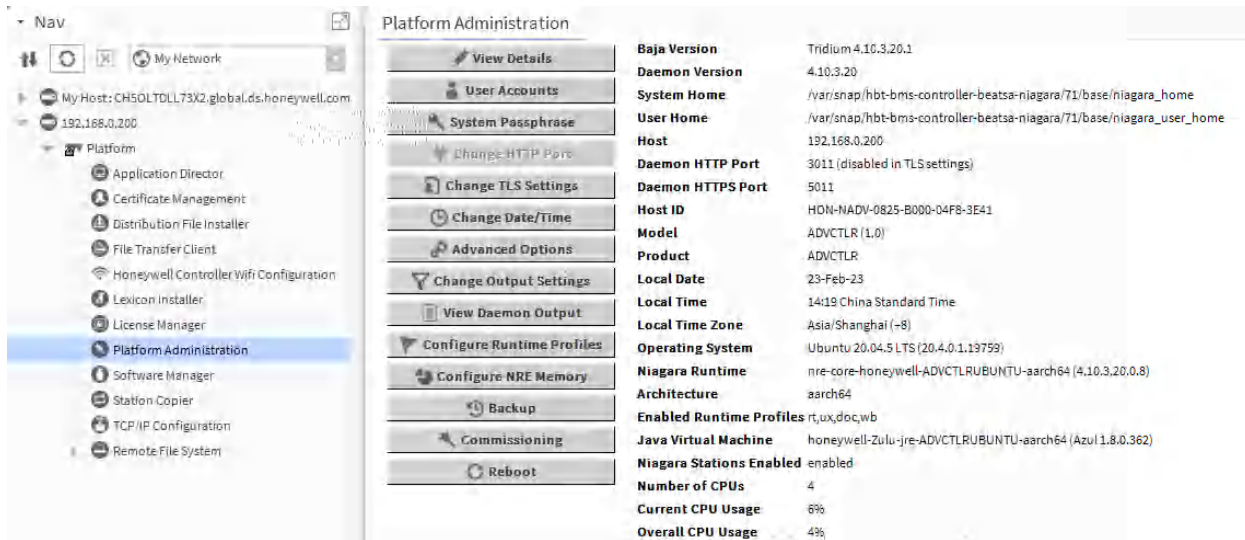


Figure 114. Platform Window



IMPORTANT:

If the user has a controller with firmware version: 4.10.5.14.0.7.6
Before upgrading to any higher firmware version, the user must upgrade the controller from firmware version 4.10.5.14.0.7.6 to 4.10.5.14.0.11. Refer to the [“Troubleshooting” on 162](#).

2. Double click on **Distribution File Installer** to open the distribution file installer.

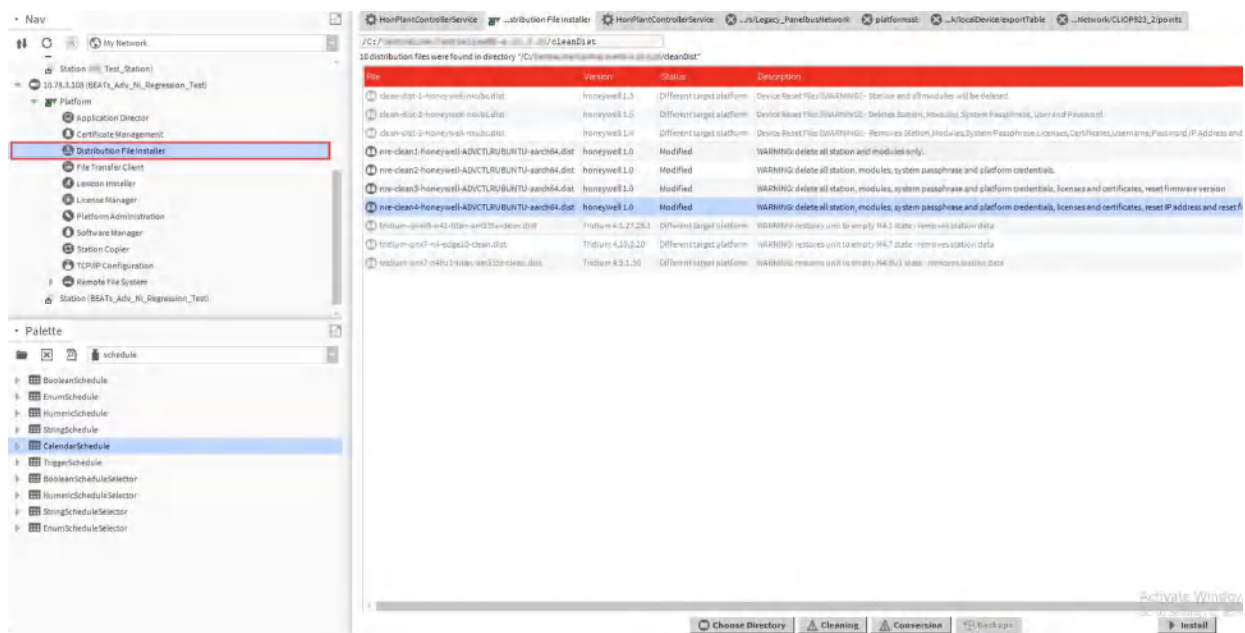


Figure 115. Distribution File Installer Window

ADVANCED PLANT CONTROLLER INSTALLATION INSTRUCTION AND COMMISSIONING GUIDE

3. Click **Choose Directory** from below options.

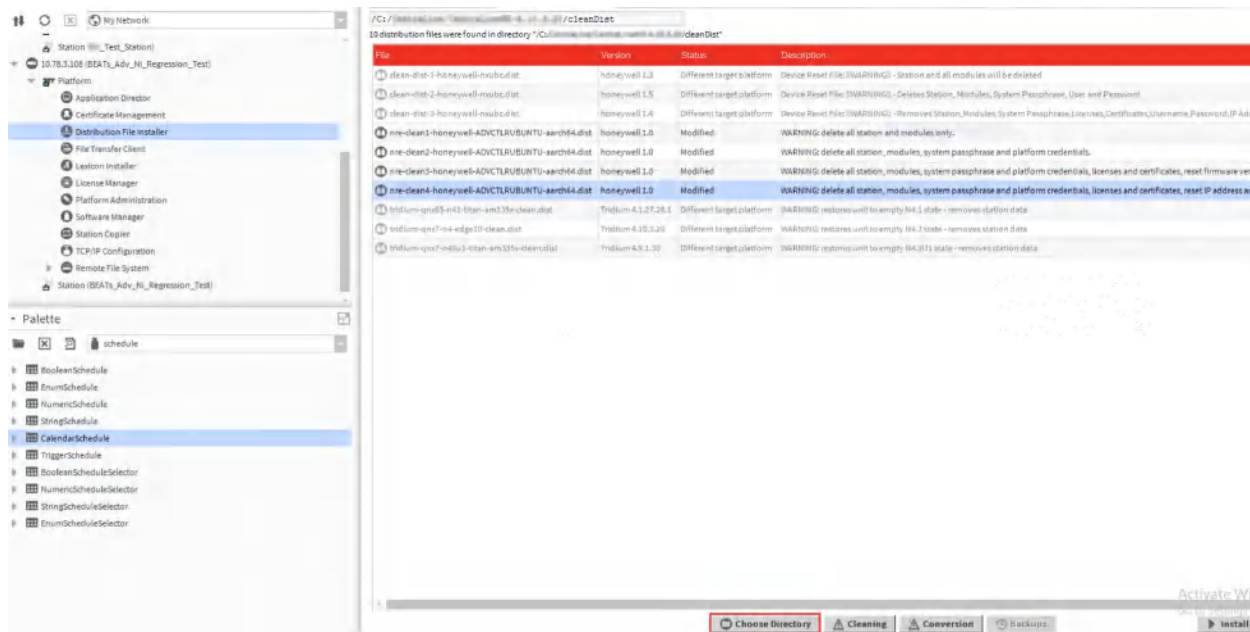


Figure 116. Distribution File Installer Window

4. **Change Directory** dialog box will display.

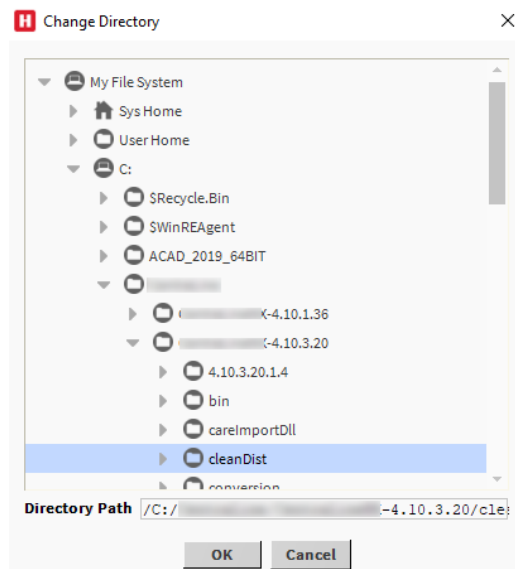


Figure 117. Change Directory Dialogue Box

- Expand Supervisor version > **sw** as show in below figure.

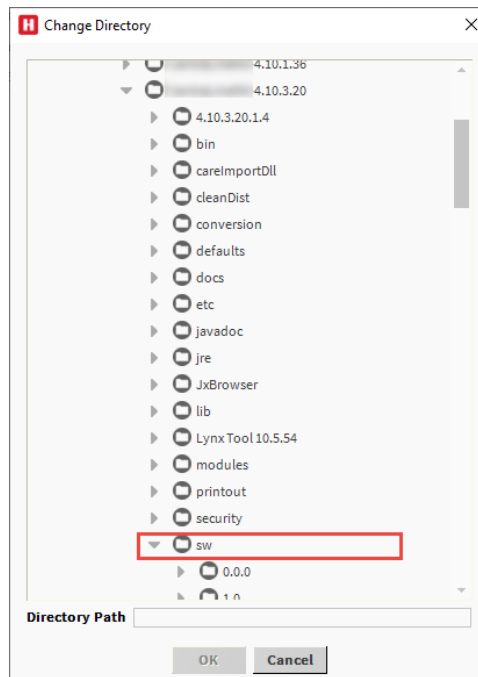


Figure 118. Change Directory Dialogue Box



NOTE:

Supervisor version may change based on your workbench version and brand. Expand current Supervisor workbench version which is open.

- Double click on version to select the updated firmware version and click **OK**.



Figure 119. Change Directory Dialogue Box



NOTE:

The version which is selected in the above figure is an example. The version can change time to time.

ADVANCED PLANT CONTROLLER INSTALLATION INSTRUCTION AND COMMISSIONING GUIDE

7. The selected version will be displayed on the **Distribution File Installer** window. Select the version file **Example:** honeywell 4.XX.X.XX.XX and click **Install**.

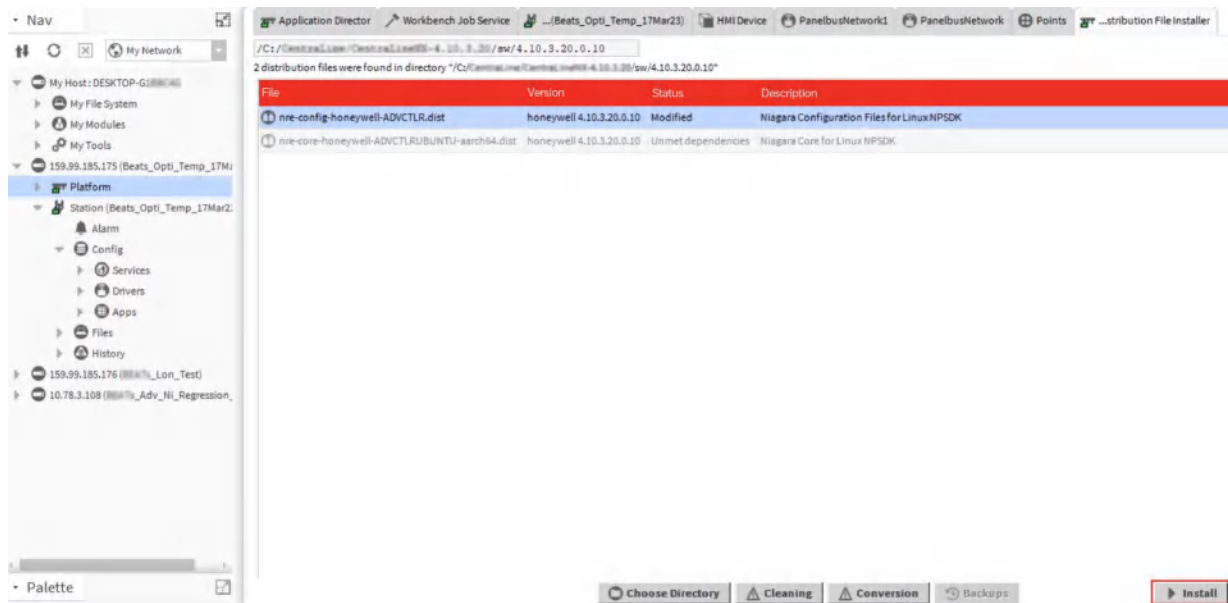


Figure 120. Distribution File Installer Window

8. **Distribution File Installer** dialog box will be displayed. Click **Next**.

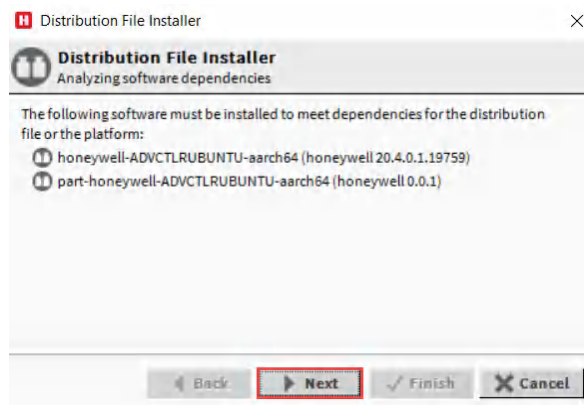


Figure 121. Distribution File Installer Dialogue Box

9. **Distribution File Installer** dialog box will be displayed. Click **Finish**.

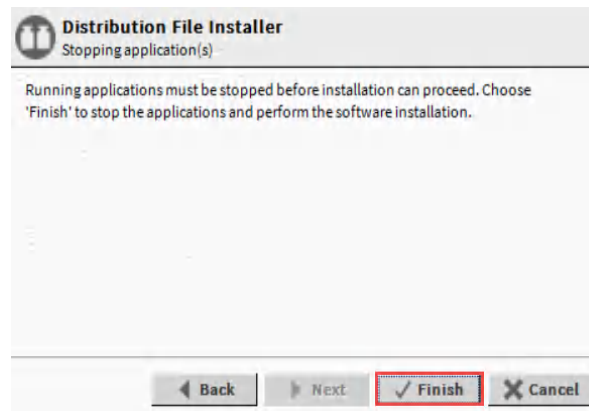
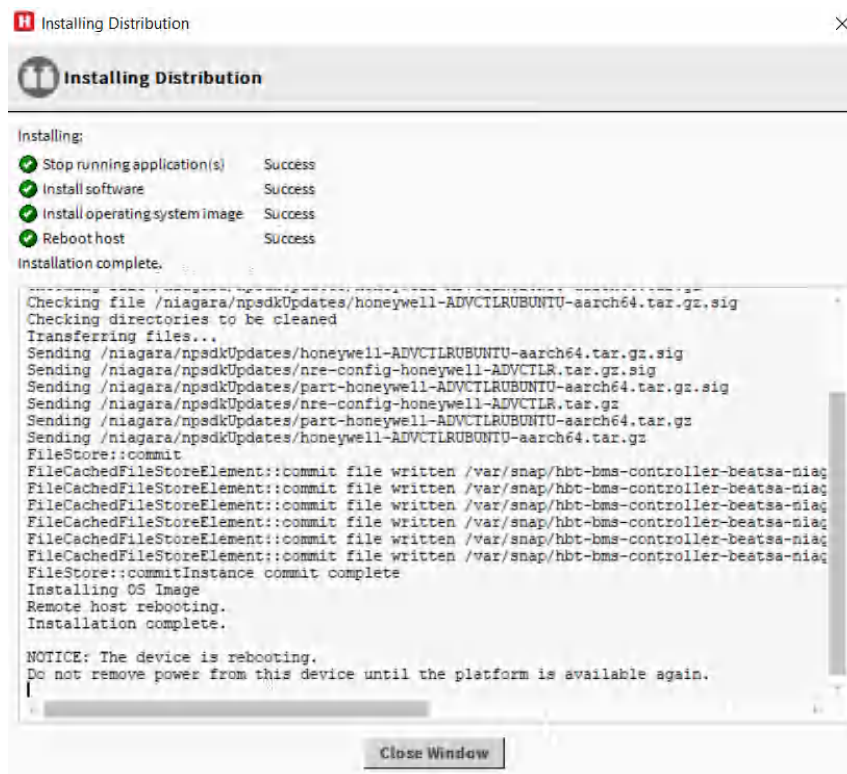


Figure 122. Distribution File Installer Dialogue Box

10. **Installing Distribution** dialogue box will be displayed. The software will be installed and the device will reboot.



CAUTION

Do not remove power or click Close Window while the Distribution file is installing.

11. Click **Close Window** after completing the installation process.
12. Reboot the device and open platform - See [“Open a Platform” on page 51](#). Check the version from platform administration - follow Step 1.

ADVANCED PLANT CONTROLLER INSTALLATION INSTRUCTION AND COMMISSIONING GUIDE

13. After a successful update, the Platform Administration should show the new firmware version in the Niagara Runtime field:

The screenshot displays the Platform Administration web interface. On the left is a navigation pane with a tree view containing items like 'Application Director', 'Certificate Management', 'Distribution File Installer', 'File Transfer Client', 'Honeywell Controller Wifi Configuration', 'Lexicon Installer', 'License Manager', 'Platform Administration' (highlighted), 'Software Manager', 'Station Copier', 'TCP/IP Configuration', and 'Remote File System'. The main area is titled 'Platform Administration' and features a vertical list of configuration buttons on the left, including 'View Details', 'User Accounts', 'System Passphrase', 'Change HTTP Port', 'Change TLS Settings', 'Change Date/Time', 'Advanced Options', 'Change Output Settings', 'View Daemon Output', 'Configure Runtime Profiles', 'Configure NRE Memory', 'Backup', 'Commissioning', and 'Reboot'. To the right of these buttons is a table of system information.

Baja Version	Tridium 4.10.3.20.1
Daemon Version	4.10.3.20
System Home	/var/snap/hbt-bms-controller-beatsa-niagara/71/base/niagara_home
User Home	/var/snap/hbt-bms-controller-beatsa-niagara/71/base/niagara_user_home
Host	192.168.0.200
Daemon HTTP Port	3011 (disabled in TLS settings)
Daemon HTTPS Port	5011
Host ID	HON-NADV-0825-B000-04F8-3E41
Model	ADVCTLR (1.0)
Product	ADVCTLR
Local Date	23-Feb-23
Local Time	14:24 China Standard Time
Local Time Zone	Asia/Shanghai (+8)
Operating System	Ubuntu 20.04.5 LTS (20.4.0.1.19759)
Niagara Runtime	nre-core-honeywell-ADVCTLRUBUNTU-aarch64 (4.10.3.20.0.8)
Architecture	aarch64
Enabled Runtime Profiles	rt,ux,doc,wb
Java Virtual Machine	honeywell-Zulu-jre-ADVCTLRUBUNTU-aarch64 (Azul 1.8.0.362)
Niagara Stations Enabled	enabled
Number of CPUs	4
Current CPU Usage	6%
Overall CPU Usage	4%

Figure 123. Update Successful

The number of Advanced controller CleanDist files has been enhanced to now four CleanDist files. These CleanDist files allow each user to individually clean up the respective controller according to the individual requirements. Follow below procedure for CleanDist file Installation.

- Nav

My Network

My Host: CH50LTDLL73X2.global.ds.honeywell.com

192.168.0.200

Platform

Application Director

Certificate Management

Distribution File Installer

File Transfer Client

Honeywell Controller Wifi Configuration

Lexicom Installer

License Manager

Platform Administration

Software Manager

Station Copier

TCP/IP Configuration

Remote File System

Platform Administration

View Details

User Accounts

System Passphrase

Change HTTP Port

Change TLS Settings

Change Date/Time

Advanced Options

Change Output Settings

View Daemon Output

Configure Runtime Profiles

Configure NRE Memory

Backup

Commissioning

Reboot

Baja Version

Tridium 4.10.3.20.1

Daemon Version

4.10.3.20

System Home

/var/snap/hbt-bms-controller-beatsa-niagara/71/base/niagara_home

User Home

/var/snap/hbt-bms-controller-beatsa-niagara/71/base/niagara_user_home

Host

192.168.0.200

Daemon HTTP Port

3011 (disabled in TLS settings)

Daemon HTTPS Port

5011

Host ID

H0N-NADV-0825-B000-04F8-3E41

Model

ADVCTLR (1.0)

Product

ADVCTLR

Local Date

23-Feb-23

Local Time

14:19 China Standard Time

Local Time Zone

Asia/Shanghai (+8)

Operating System

Ubuntu 20.04.5 LTS (20.4.0.1.19759)

Niagara Runtime

nre-core-honeywell-ADVCTLRUBUNTU-aarch64 (4.10.3.20.0.8)

Architecture

aarch64

Enabled Runtime Profiles

rt,ux,doc,wb

Java Virtual Machine

honeywell-Zulu-jre-ADVCTLRUBUNTU-aarch64 (Azul 1.8.0.362)

Niagara Stations Enabled

enabled

Number of CPUs

4

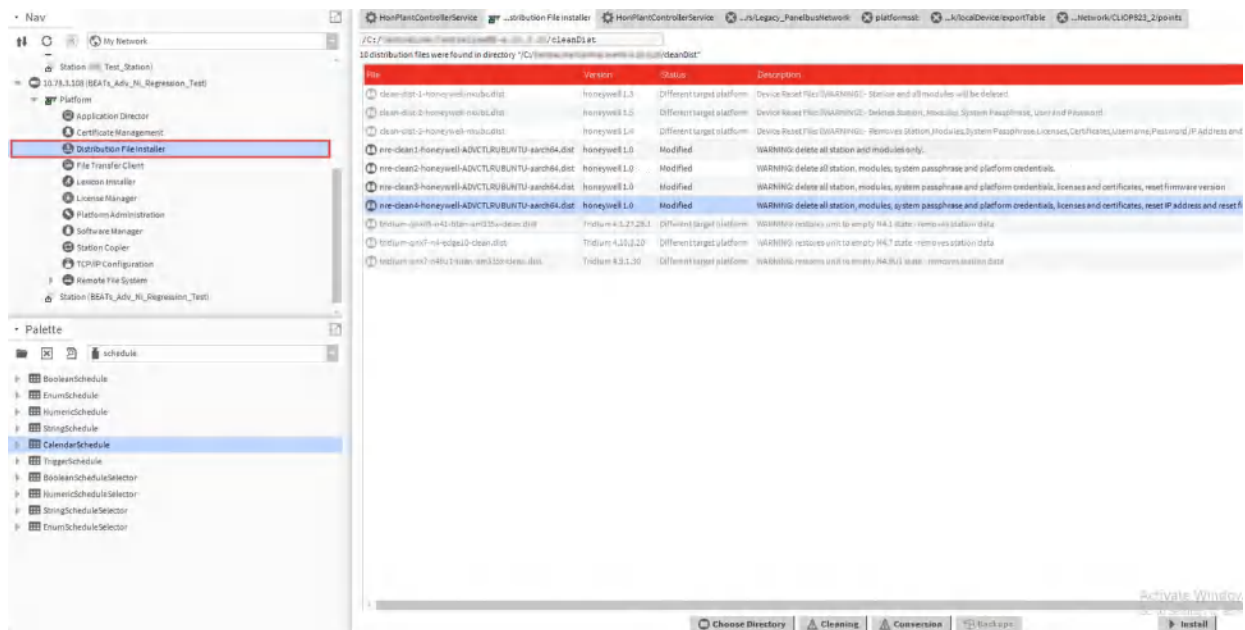
Current CPU Usage

6%

Overall CPU Usage

43%

2. Double click on **Distribution File Installer** to open the distribution file installer.



31-00584-02

ADVANCED PLANT CONTROLLER INSTALLATION INSTRUCTION AND COMMISSIONING GUIDE

3. Click **Choose Directory** from below options.

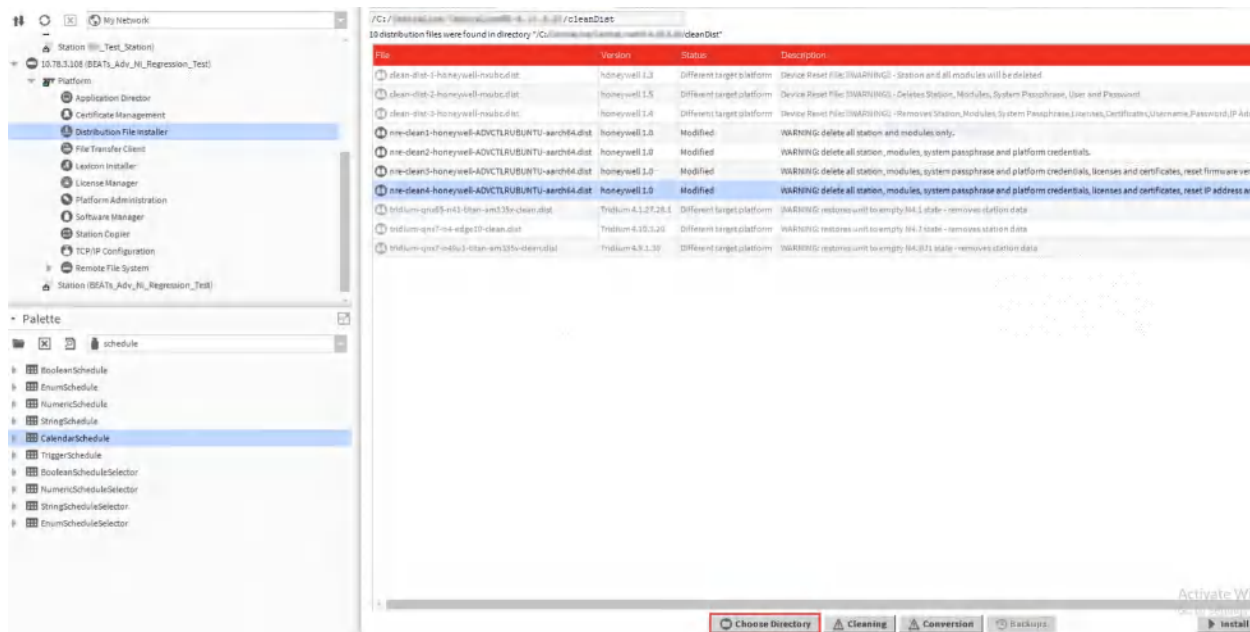


Figure 126. Distribution File Installer Window

4. **Change Directory** dialog box will display. Select **cleanDist**.

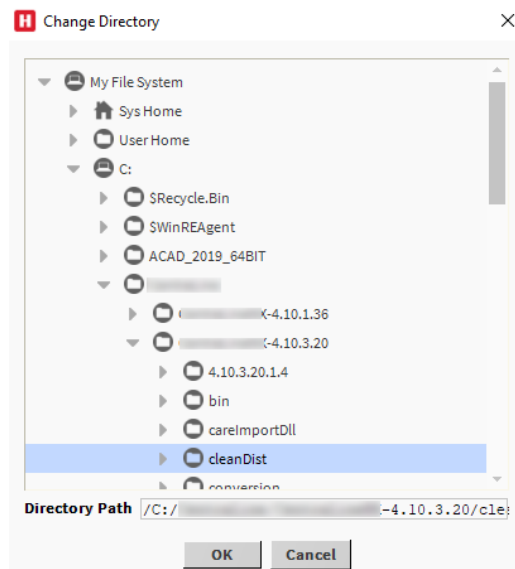


Figure 127. Change Directory Dialogue Box

5. CleanDist files will appear on the **Distribution file Installer** window as shown in below figure. Select one file (clean1/clean2/clean3/clean4) as per the requirement and click **Install**.

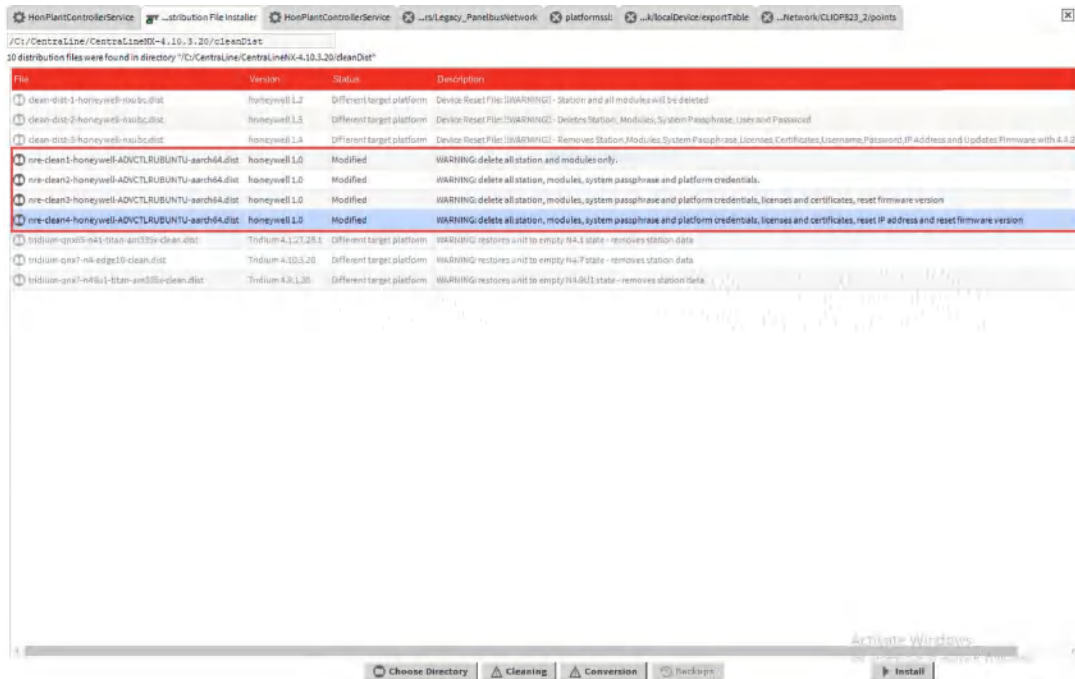


Figure 128. Distribution File Installer Window



NOTE:

Each file has a different purpose and function to reset the controller. Selecting one of the files will result below:

- **Clean1:** Delete all stations and modules from the controller.
- **Clean2:** Delete all stations, modules, system passphrase, and platform credentials from the controller.
- **Clean3:** Delete all stations, modules, system passphrase, platform credentials, licenses and certificated, and reset firmware version.
- **Clean4:** Delete all stations, modules, system passphrase, platform credentials, licenses and certificated, reset IP address and reset firmware version from the controller.

If the “Clean4” is installed than, the controller will go back to factory default settings. Refer CleanDist options table.

Table 33. CleanDist options

Elements which gets deleted from controller	CleanDist1	CleanDist2	CleanDist3	CleanDist4
Station	X	X	X	X
Module	X	X	X	X
System passphrase	-	X	X	X
Platform credentials	-	X	X	X
Licenses and certificates	-	-	X	X
Reset Firmware version	-	-	X	X
Reset IP address	-	-	-	X
				Factory default

6. **Distribution File Installer** dialog box will be displayed. Click **Finish**.

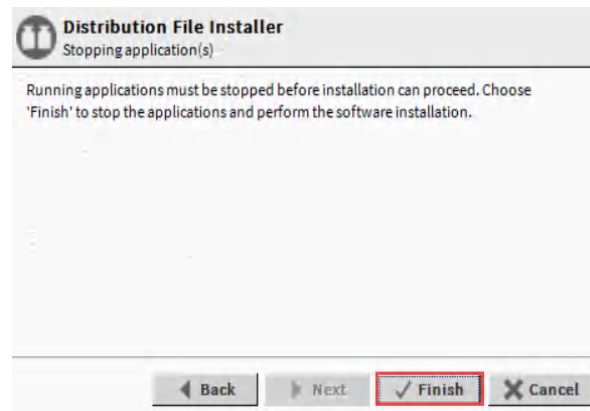


Figure 129. Distribution File Installer Dialogue Box

7. **Installing Distribution** dialogue box will be displayed. The Dist file will be installed and the device will reboot.

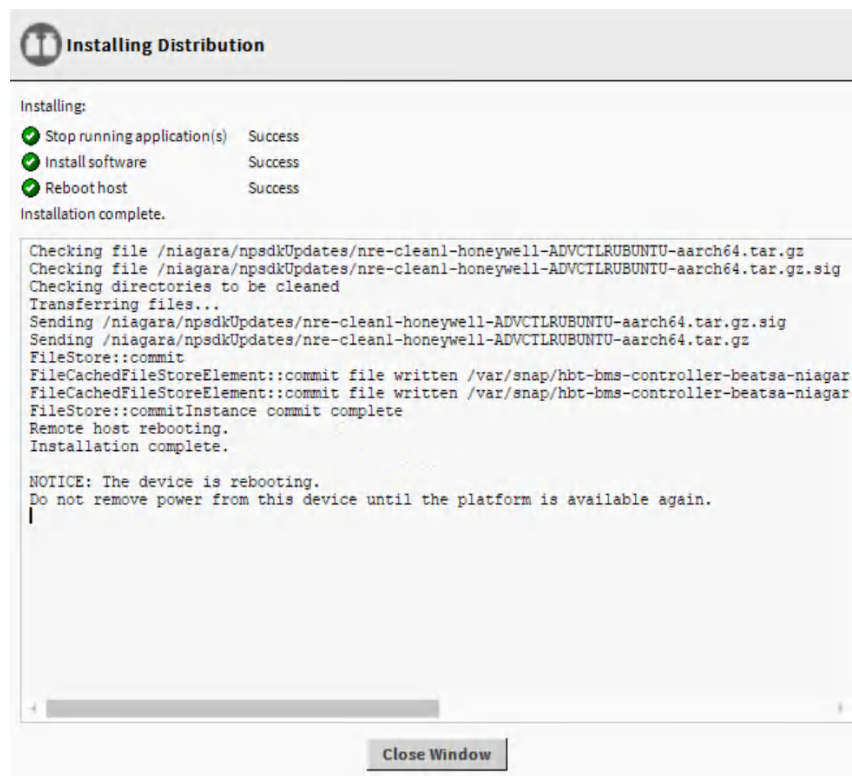


Figure 130. Installing Distribution Dialogue Box

CAUTION

Do not remove power or click Close Window while the Distribution file is installing. Based on the cleanDist file selection the file name will appear on Installing Distribution window.

8. Click **Close Window** after completing the installation process.
9. Reboot the device and open platform - See [“Open a Platform” on page 51](#). Check the version from platform administration - follow Step 1.

ENABLE/DISABLE USB BACKUP AND RESTORE

The USB backup and restore function is enabled by default. If this function is required or not required, it must be disabled or enabled.

To enable/disable USB backup & restore:

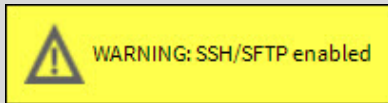
1. Make a platform connection to the Advanced Plant Controller. See [“Open a Platform” on page 51.](#)
2. Double-click **Platform Administration**.



NOTE:

If the USB Backup and Restore is enabled, A warning message will appear in yellow in Platform Administration main page.

Warning:



3. Click **Advanced Options**. The **Advanced Platform Options** dialogue box is displayed:

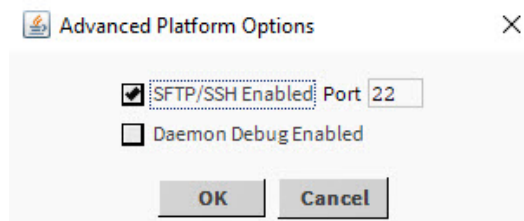


Figure 131. Advanced Platform Options

4. To enable, ensure USB Backup Enabled is selected; to disable, ensure USB Backup Enabled is deselected.
5. Click **OK**.

USB BACKUP AND RESTORE USING SHELL COMMAND

Prerequisites:

- USB backup and restore support only FAT32 and FAT32X file systems. NTFS is not supported.
- Need a USB flash drive with enough memory (Currently, the remaining space is at least 300Mb).
- The USB backup and restore procedure does not require access to Workbench.
- Use a terminal emulator (system shell program), like the PuTTY program to access the controller's system shell menu, which lists the restore options.

CAUTION

Only flash drives are recommended for backup/restore operations. USB bus-powered external hard drives often have higher power requirements. They may not function as expected, possibly resulting in permanent damage to the flash drive or to the Advanced controller. Plugging in an external hard drive may cause the controller to become unresponsive, requiring a reboot.



NOTE:

The USB Backup and Restore feature is not intended to upgrade or downgrade the firmware version. The User can only backup and restore the Station data and configurations on controllers running at the same Niagara version.

Procedure for USB backup and restore

1. Connect the controller to PC and Power ON the controller. See [“Connect the Niagara-Installed PC” on page 44.](#)
2. Insert a USB flash drive into the USB port.

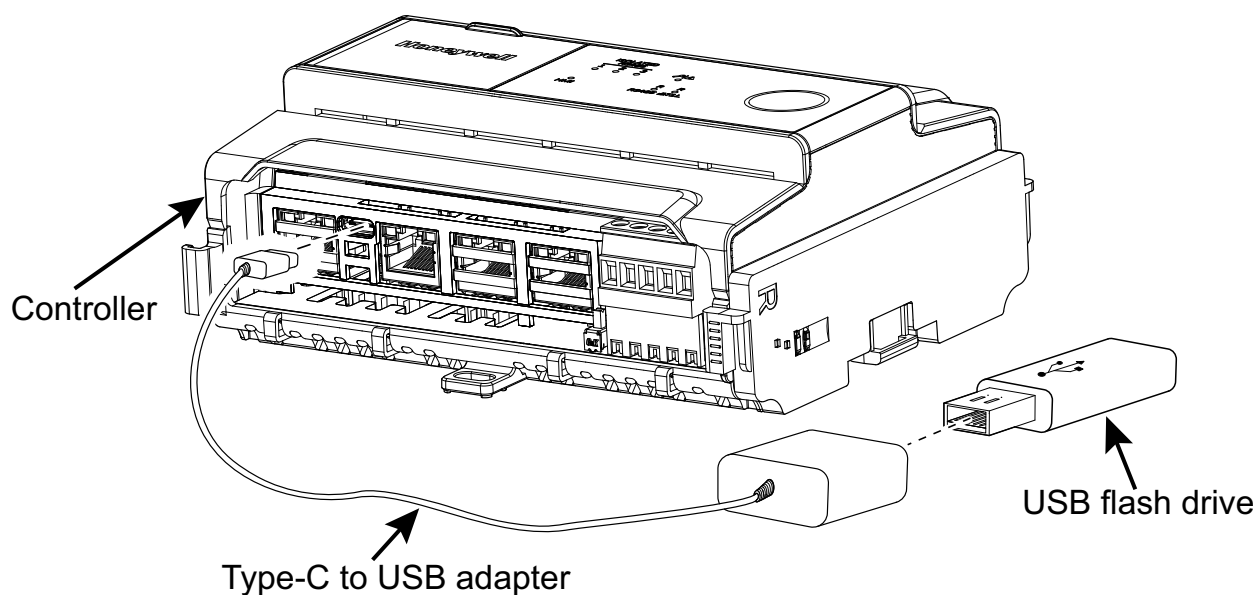


Figure 132. USB port to USB Flash Drive connection



NOTE:

The USB port is a Type-C interface, so a Type-C to USB adapter is required.

- Open the shell command view from the Serial Port or Network Port use PuTTY.

**NOTE:**

Serial line: Check Device Manager from PC/Laptop for communication port (USB port).
Speed: 115200

- Enter the platform User name and password to open the system start-menu.

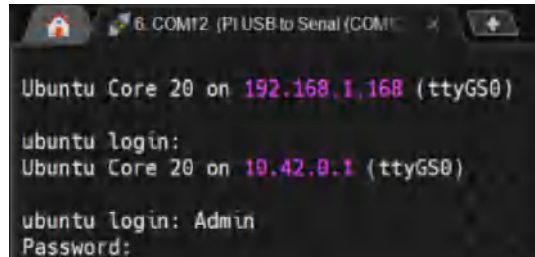


Figure 133. System Shell Login window

- Start Menu will display.
From Start Menu select and Type the number of “USB Backup and Restore” (here it is 6) in **Enter choice:**

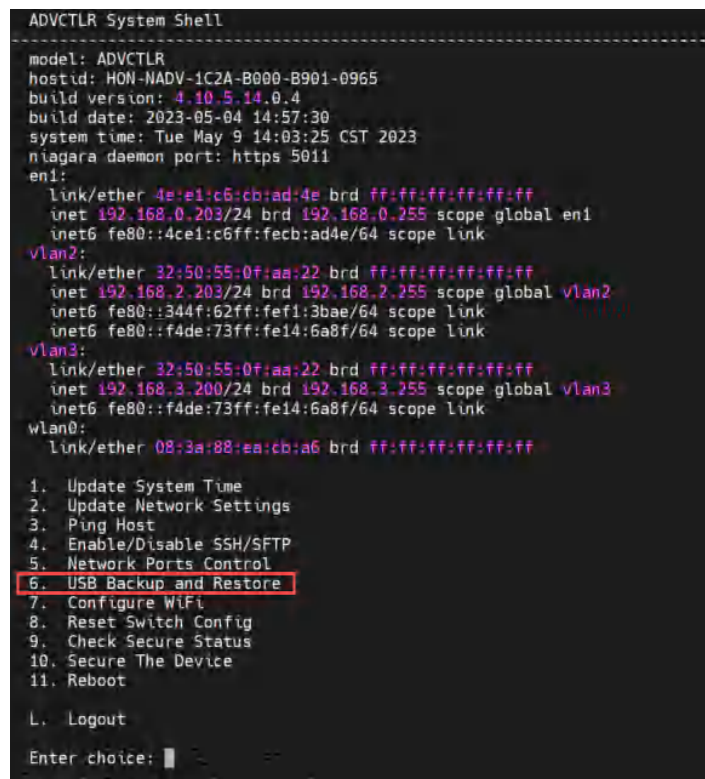


Figure 134. Start Menu

6. List of options will display. Type the number in “Enter choice:” based on your choice and click **Enter**.

```

ADVCTRL System Shell
-----
model: ADVCTRL
hostid: HON-NADV-1C2A-B000-B901-0965
build version: 4.10.5.14.0.4
build date: 2023-05-04 14:57:30
system time: Wed May 10 10:05:53 CST 2023
niagara daemon port: https 5011
en1:
  link/ether 4e:e1:c6:cb:ad:4e brd ff:ff:ff:ff:ff:ff
  inet 192.168.0.203/24 brd 192.168.0.255 scope global en1
  inet6 fe80::4ce1:c6ff:feeb:ad4e/64 scope link
vlan2:
  link/ether 32:50:55:0f:aa:22 brd ff:ff:ff:ff:ff:ff
  inet 192.168.2.203/24 brd 192.168.2.255 scope global vlan2
  inet6 fe80::344f:62ff:fe11:3bae/64 scope link
  inet6 fe80::f4de:73ff:fe14:6a8f/64 scope link
vlan3:
  link/ether 32:50:55:0f:aa:22 brd ff:ff:ff:ff:ff:ff
  inet 192.168.3.200/24 brd 192.168.3.255 scope global vlan3
  inet6 fe80::f4de:73ff:fe14:6a8f/64 scope link
wlan0:
  link/ether 08:3a:88:ea:cb:a6 brd ff:ff:ff:ff:ff:ff

1. Start USB Backup
2. Start USB Restore
3. Exit

Enter choice: 

```

Figure 135. System Shell window



NOTE:

Below actions will trigger based on the choice:

Start USB Backup: Begin to do the backup.

Start USB Restore: Begin to do the restore

Exit: Exit the USB Backup and Restore and back to the main menu

Creating a USB backup

To create a USB backup follow above process first See [“Enable/Disable USB Backup and Restore” on page 135.](#) and See [“USB Backup and Restore using shell command” on page 136.](#)

1. Select and type '1'(Start USB Backup) to auto begin USB Backup. This may take several minutes until completion prompts success or failure.

```
Start USB Backup...

Scan USB Device:
/dev/sda

-----> Start to mount USB device: /dev/sda
/dev/sda mount succeed.
usbInfoArray = /dev/sda vfat 7847936 50844 7797092 1% /mnt/backup
usbAvailable = 7797092, usbAvailableCheck = 7797092
Begin to Stop niagarad .....
CMD is still doing.
CMD is still doing.
CMD is Done.

-----Creating clone Image-----
hostid=HONX-0000-0000-0031-04C7, model=nxubc(2.0)
cmls = common/base common/chunkfs common/geom common/logs
xnlS = x15/base x15/sysinfo x15/wifi

Cloning filesystem. This can take several minutes.....
CMD is still doing.
CMD is still doing.
CMD is still doing.
CMD is still doing.
CMD is still doing.
CMD is still doing.
CMD is Done.
cloneName = HONX-0000-0000-0031-04C7_20220630042056
CMD is Done.
Clone HONX-0000-0000-0031-04C7_20220630042056 created in 10 sec, calculating cksum....

-----Backup Complete.-----

Begin to Restart niagarad .....
CMD is still doing.
CMD is Done.
-----niagarad is restart now.
Check mount point status to umount the mount point...
fileType = tmpfs
remove /mnt/backup
delete file : /tmp/clone-info-v2.txt
delete file : /tmp/niagaraSnapshot

Exit USB Backup...

Press ENTER to continue
```

Figure 136. System Shell window

2. Press **Enter** to finish the USB Backup.

When the backup Complete, remove the USB flash drive and store it in a safe place.

The name of the backup resulting image file follows this convention: hostid (unique host ID of the Controller), underscore (_) timestamps.

Example: HONX-0000-0000-0031-04C7_20220630042056



NOTE:

If no USB flash drive is detected, the following message is displayed:

```
Start USB Backup...

No USB flash drive is detected. Insert the USB flash drive and back up data.

Press ENTER to continue
```

If the backup is unable to complete successfully, check the error log in shell view. Or simply unplug the USB thumb drive, then insert the thumb drive and try the backup procedure again. If problems persist, possible causes could be:

- Insufficient disk space on the thumb drive.
- Write protect enabled on the thumb driver.

Restoring from a USB backup

Restoring from a USB backup returns the controller to the state it was in when the system made the backup. You may restore to a controller other than the one on which the backup was made, provided that the target controller is the same model. To create a USB backup follow above process first See [“Enable/Disable USB Backup and Restore” on page 135](#). and See [“USB Backup and Restore using shell command” on page 136](#).

1. Select and type **2** (Start USB Backup) to begin USB Restore.

```
Start USB Restore...

*****
Restore from a USB Backup
*****

Existing Niagara and platform installation will be completely removed!
This includes:
  Licenses
  TCP/IP Configuration
  Platform credentials
  TLS certificates

If restoring a backup from another unit, you will need to
install a new license.

TCP/IP configuration and platform credentials will be set to values
in the backup.

Niagara daemon and station will be killed if they are currently running
check the passphrase file.
Enter the system passphrase for this system to proceed, or return to exit : █
```

Figure 137. System Shell window

2. System passphrase prompt window will display. Enter the current system passphrase for the controller and click **Enter**. The two scenario will appear based on given system passphrase.
 - a. If the entered passphrase does not match the system passphrase for this controller more than three times, then it will exit the USB restore. Follow the procedure again and type the valid system passphrase.

```
check the passphrase file.
Enter the system passphrase for this system to proceed, or return to exit :
Invalid system passphrase, Input the passphrase again:
Enter the system passphrase for this system to proceed, or return to exit :
Invalid system passphrase, Input the passphrase again:
Enter the system passphrase for this system to proceed, or return to exit :
Invalid system passphrase, Input the passphrase again:
Enter the system passphrase for this system to proceed, or return to exit :
Invalid system passphrase, will exit the restore.

Press ENTER to continue █
```

- b. If the entered passphrase and the passphrase stored on the controller match, the system will display USB drive mounts backup. The options are as shown in below figure.

```
check the passphrase file.
Enter the system passphrase for this system to proceed, or return to exit :
Are you sure you want to exit? (Y/n) : n
Enter the system passphrase for this system to proceed, or return to exit :
Scan USB Device:
/dev/sda

-----> Start to mount USB device: /dev/sda
/dev/sda mount succeed.
usbInfoArray = /dev/sda
usbAvailable = 7797468, usbAvailableCheck = 7797468
hostId=HONX-0000-0000-0031-04C7
This platform is HONX-0000-0000-0031-04C7
Please make your selection below
1) Abort Recovery/Restore mode          4) HONX-0000-0000-0031-04C7_20220613080547
2) Show backups for other host IDs       5) HONX-0000-0000-0031-04C7_20220613063549
3) HONX-0000-0000-0031-04C7_20220613080114 6) HONX-0000-0000-0031-04C7_202206130942056
#? █
```

3. If the scenario **b** persists: Type the number for a listed backup file name (for example: 6) or other option and press **Enter**.



NOTE:

The backup file name is the name of the backup file stored on the USB flash drive.

4. From the prompt asking if the backup files passphrase is the same as the system passphrase for the controller, type Y (yes) or N (no).

**NOTE:**

- If Yes, then the system passphrase entered in the earlier step is used to decode the backup.
- If No, you must enter the passphrase for the backup file to decode the backup.

```
This platform is HONX-0000-0000-0031-04C7
Please make your selection below
1) Abort Recovery/Restore mode          4) HONX-0000-0000-0031-04C7_20220613080547
2) Show backups for other host IDs      5) HONX-0000-0000-0031-04C7_20220630035549
3) HONX-0000-0000-0031-04C7_20220613080114  6) HONX-0000-0000-0031-04C7_20220630042056
#? 6
Check the backup package password.
Is the backup passphrase the same as the system passphrase? (Y/n) : n
Enter the passphrase used to encrypt the backup:
█
```

5. If you entered **N** in the previous step, type the backup file passphrase for the backup file at the prompt, and click **Enter**.
If you entered **Y** the restore begins. This can take a few minutes.

```
Restoring Clone Image HONX-0000-0000-0031-04C7_20220630042056

-----Extracting metadata files. This can take several minutes-----
Load properties...
-----loadProperties = 0
Verifying backup matches platform
Verify Backup matches platform OK.
    cksumUSB = 12305310
    cksumB = 12305310
Begin to Stop niagarad .....
CMD is still doing.
CMD is still doing.
CMD is Done.
Preparing Filesystem for restore
DO The restore clean
Restoring files...
Import snapshot = tmp/niagaraSnapshot
CMD is still doing.
CMD is Done.
CMD is still doing.
CMD is still doing.
CMD is Done.
CMD is Done.

Begin to Restart niagarad .....
CMD is still doing.
CMD is Done.
-----niagarad is restart now.
0
Check mount point status to umount the mount point...
/dev/sda      vfat  7847936 50468  7797468  1% /mnt/backup
Current mountPoint=/mnt/backup has been mounted, and will umount it. and remove the mount point
fileType = tmpfs
remove /mnt/backup
delete file : /tmp/clone-info-v2.txt
delete file : /tmp/niagaraSnapshot

Exit USB Restore...

Restore Succeeded!
Please poweroff and Reboot this device.

Press ENTER to continue█
```

Figure 138. System Shell window**CAUTION**

Once a restore begins, do not interrupt the process by removing the USB flash drive or disconnecting the power.

6. When the restore successfully completes, press Enter to exit the USB restore. Then turn the controller's power off and restart it again.

AUTOMATIC RESETTING FUSE

The 24V~ and 24V0 terminals at RS485-R Interface have an automatic resetting fuse protection. The table below provides a maximum quantity of each IO module type that can be powered from the 24V~ and 24V0 terminals at RS485-R Interface. If a mixture of IO modules is to be installed, use the table as a guide to determine if the IO modules can be powered from the 24V~ and 24V0 terminals at RS485-R Interface or if a separate power source needs to be used.

Table 34. Automatic Resetting Fuse Protection at RS485-R Interface - Maximum Number of IO Modules

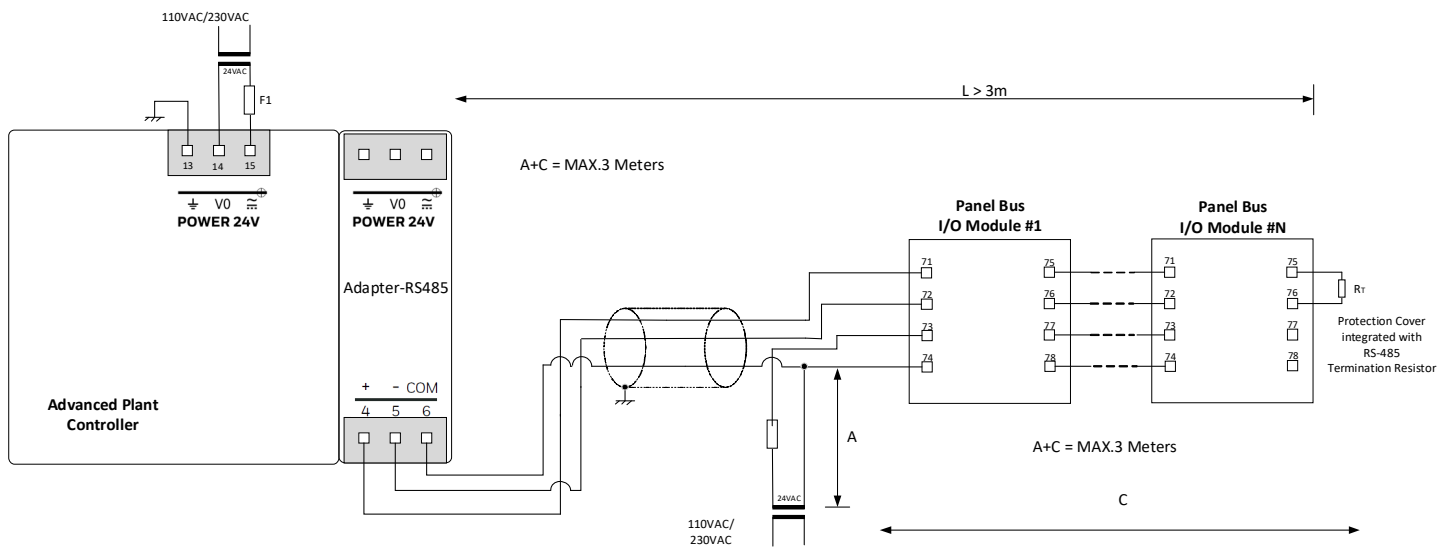
IO Module Type*	** IO Module Current Ratings (AC)	Controller Ratings 24V~/24V0 at RS485-R		
		3 A @ 20 C (68 F) Ambient	2.4 A @ 40 C (104 F) Ambient	2.1 A @ 50 C (122 F) Ambient
I/O Module	0.625 A	4	3	3



NOTE:

- The fuse will reset one minute after removing the current from the circuit.
- ** The Rating assumes all inputs and outputs are used on the IO modules.

31-00584-02

CONNECTION VIA RS485 INTERFACE R**Figure 140. Connection ($L > 3 m$) of RS485 interface R to a Panel Bus****NOTE:**

- * The 24V~ and 24V0 terminals at the RS485-R Interface have an automatic resetting fuse protection. For more information, [See “Automatic Resetting Fuse” on page 142.](#)
- $N = \text{max. 16 modules}$ (Total max. no. of Panel Bus I/O modules:64).
- For communication cable lengths, transmission speeds, and termination [See “General Safety Information” on page 7.](#) For fusing, [See “Example 1: Power Supply via Controller Using Panel Module” on page 16.](#)

Connection to Panel Bus I/O Modules Powered by the Same Transformer as the Advanced Plant Controller

This configuration is suitable for connecting Panel Bus I/O modules located in the same wiring cabinet as the Advanced Plant Controller.

CONNECTION VIA RS485 INTERFACES 1, 2, OR 3

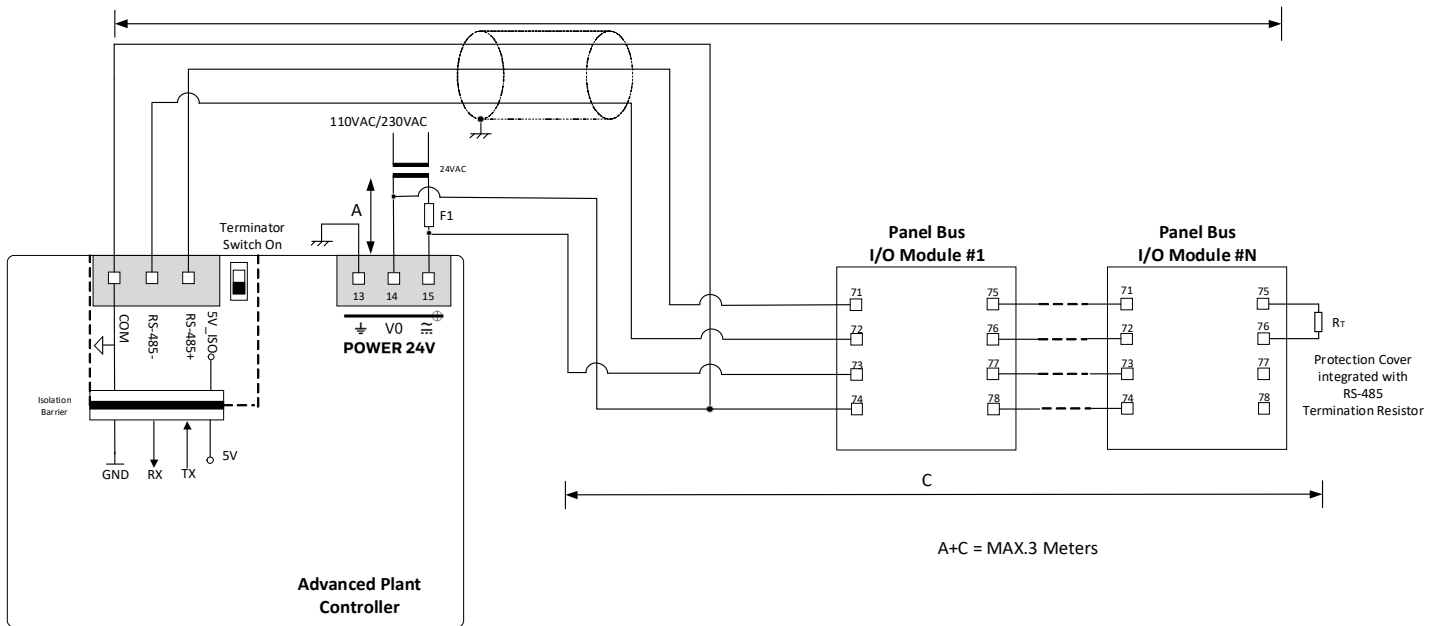
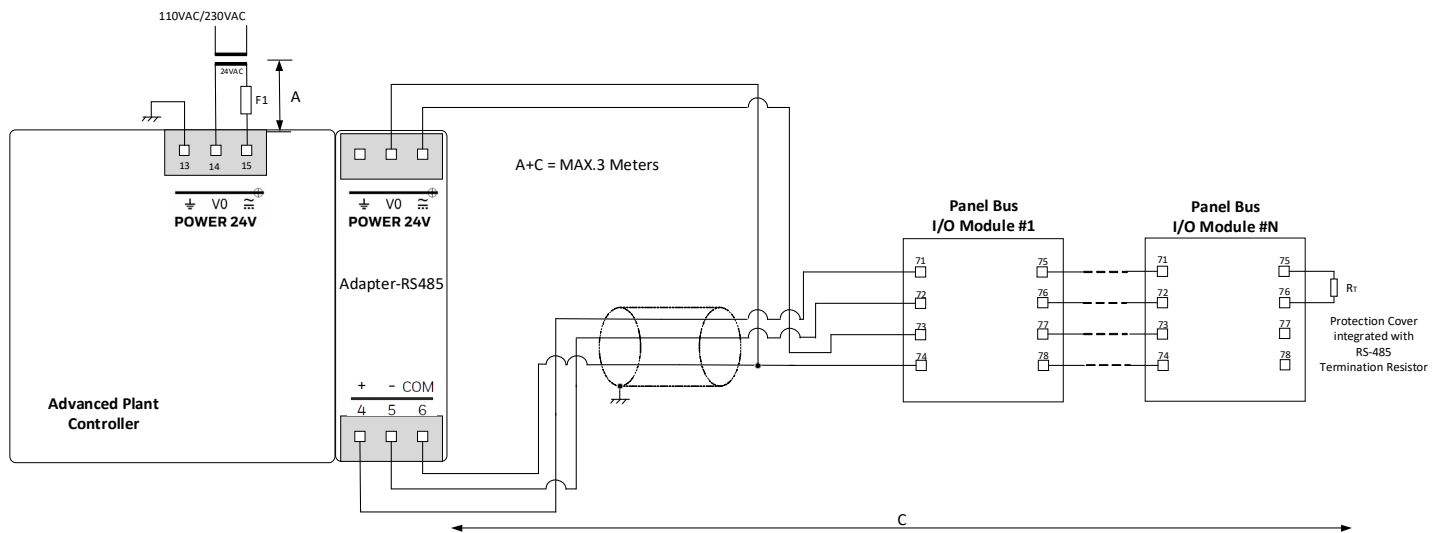


Figure 141. Connection (L < 3 m) of RS485 interfaces 1, 2, or 3 (RS485 interface 1 shown) to a Panel Bus



NOTE:

- N = max. 16 modules (Total max. no. of Panel Bus I/O modules:64).
- For communication cable lengths, transmission speeds, and termination, [See “General Safety Information” on page 7](#). For fusing, [See “Example 1: Power Supply via Controller Using Panel Module” on page 16](#).

CONNECTION VIA RS485 INTERFACE R**Figure 142. Connection ($A + C < 3 \text{ m}$) of RS485 interface R to a Panel Bus****NOTE:**

- * The 24V~ and 24V0 terminals at RS485-R Interface have an automatic resetting fuse protection. For more information, [See “Automatic Resetting Fuse” on page 142.](#)
- N = max. 16 modules (Total max. no. of Panel Bus I/O modules:64).
- For communication cable lengths, transmission speeds, and termination, [See “General Safety Information” on page 7.](#) For fusing, [See “Example 1: Power Supply via Controller Using Panel Module” on page 16.](#)

Connection to BACnet MSTP Buses with Shielding as Return path

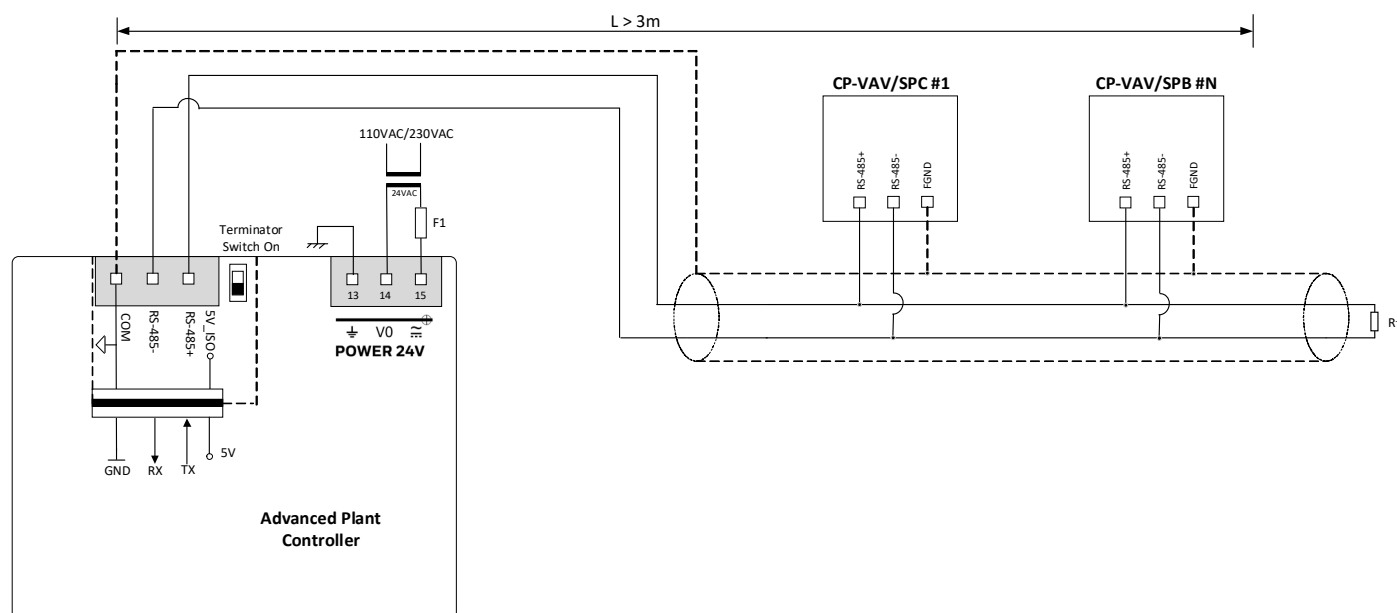
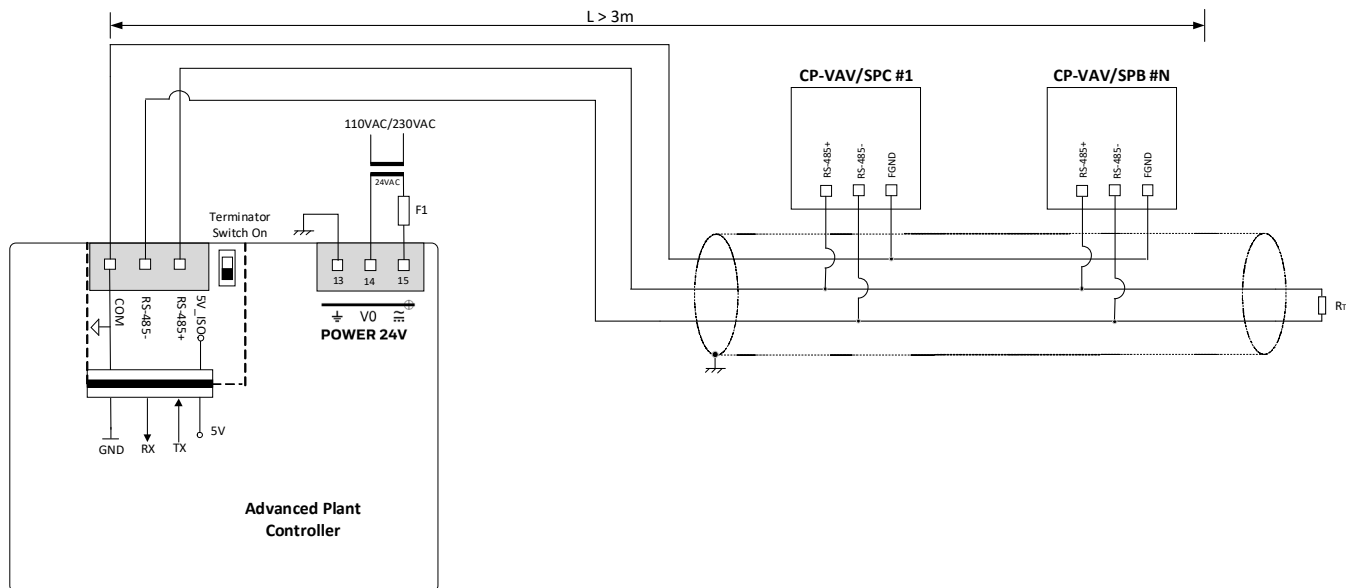


Figure 143. Connection ($L > 3$ m) of RS485 interfaces 1, 2, or 3 (RS485 interface 1 shown) to a BACnet Bus



NOTE:

- Always power the Advanced Plant Controller with a transformer separate to the connected BACnet MSTP modules.
- $N = \text{max. } 64$ modules.
- Signal ground (signal reference) connection is recommended if not all devices are electrically isolated. For more information, [See “General Safety Information” on page 7.](#)
- Connection via RS485 1, 2 or 3 where shielding works as RS485 return path.
- For communication cable lengths, transmission speeds, and termination, [See “General Safety Information” on page 7.](#) For fusing, [See “Example 1: Power Supply via Controller Using Panel Module” on page 16.](#)
- Termination resistors must be inserted directly into the terminals of the individual BACnet MSTP modules. In the above figure, the controller is shown operating as the Master BACnet controller.

Recommended connection for BACnet MSTP Buses with Separate Conductor as Return path**Figure 144. Connection ($L > 3\text{ m}$) of RS485 interfaces 1, 2, or 3 (RS485 interface 1 shown) to a BACnet Bus****NOTE:**

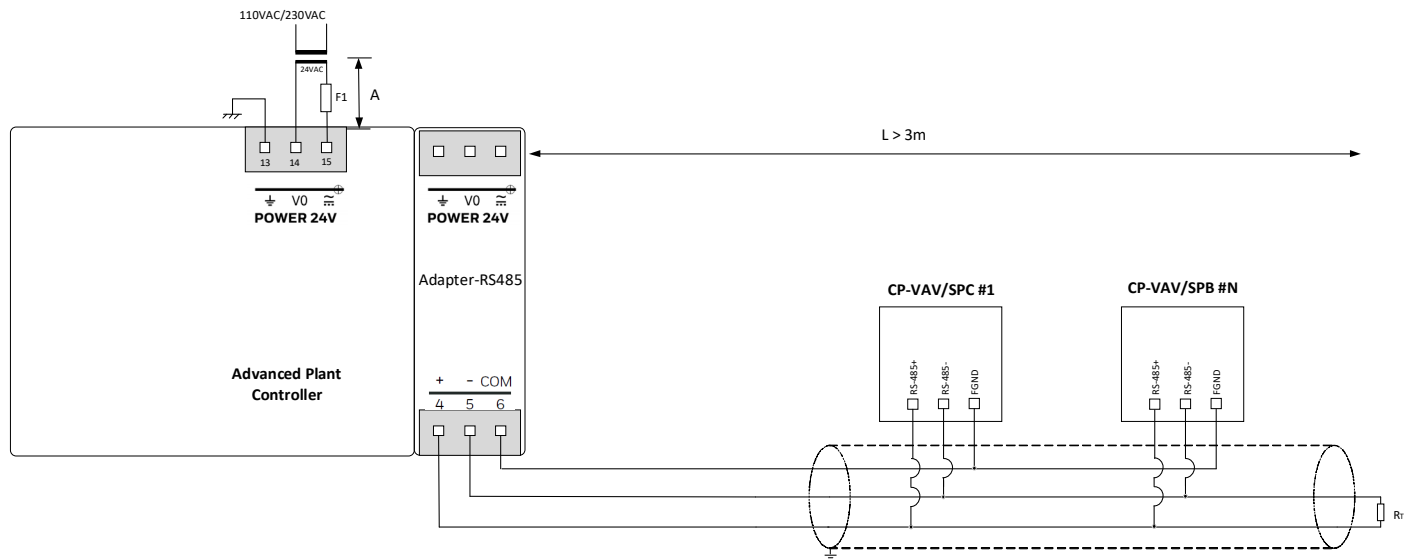
- Always power the controller with a transformer separate to the connected BACnet MSTP modules.
- $N = \text{max. } 64$ modules.
- Signal ground (signal reference) connection is recommended if not all devices are electrically isolated. For more information, [See “General Safety Information” on page 7.](#)

The diagram illustrates the experimental setup for the CP-VAV/SPC and CP-VAV/SPB systems. It includes the following components and connections:

- Power Supply:** A 110VAC/230VAC source is connected to a 24VAC source, which is then connected to a fuse (F1) and a terminal block (13, 14, 15). The terminal block is connected to the **POWER 24V** input of the **Advanced Plant Controller** and the **Adapter-RS485**.
- Advanced Plant Controller:** A large rectangular block on the left, connected to the power supply and the Adapter-RS485.
- Adapter-RS485:** A central block that interfaces between the Advanced Plant Controller and the CP-VAV/SPC and CP-VAV/SPB units. It has a **POWER 24V** input and an **RS-485** output.
- CP-VAV/SPC #1 and #2:** Two identical units, each with an **RS-485+** input, an **RS-485-** input, and a **GND** input. They are connected to the Adapter-RS485 via RS-485 lines.
- CP-VAV/SPB:** A single unit with an **RS-485+** input, an **RS-485-** input, and a **GND** input. It is connected to the Adapter-RS485 via RS-485 lines.
- RS-485 Lines:** Solid lines represent the RS-485+ and RS-485- signals. Dashed lines represent the common ground (GND) and the return line (Rt).
- Distance:** The distance between the CP-VAV/SPC and CP-VAV/SPB units is indicated as $L > 3m$.

NOTE:

- Always power the controller with a transformer separate to the connected BACnet MSTP modules.
- N = max. 64 modules.

Connection for BACnet MSTP Buses with Separate Conductor as Return path (non-isolated)**Figure 146. Connection ($L > 3\text{ m}$) of RS485-R to a BACnet Bus**

- NOTE:**
- Always power the controller with a transformer separate to the connected BACnet MSTP modules.
 - N = max. 64 modules.

Connection to Modbus Modules with Shielding as Return path

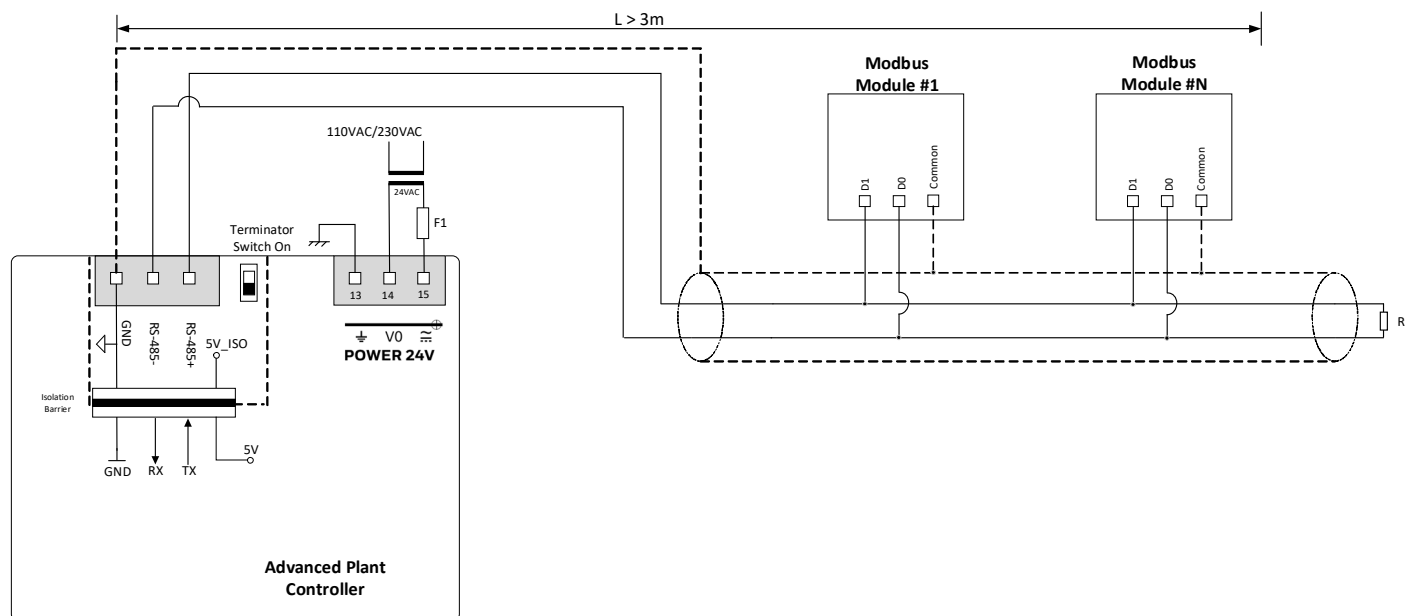


Figure 147. Connection ($L > 3\text{ m}$) of RS485 interfaces 1, 2, or 3 (RS485 interface 1 shown) to a Modbus



NOTE:

- $N = \text{max. } 32$ unit loads. Always power the Advanced Plant Controller and connected Modbus modules with separate transformers. Termination resistors must be inserted directly into the terminals of the individual Modbus modules.
- Signal ground (signal reference) connection is recommended. For more information, See [“General Safety Considerations” on page 17.](#)
- If the connected controllers do not have isolated RS485 interfaces and if they share a common ground between the power supply and Earth ground, See [“Connection to Modbus devices with Separate Conductor as Return path \(non-isolated\)” on page 154.](#) provided in Connection to Modbus devices with non-isolated RS485 interfaces. This provides the best electrical noise rejection.
- For communication cable lengths, transmission speeds, and termination, See [“RS485 Bus Cable Specifications” on page 19.](#)

Connection to Modbus devices with Separate Conductor as Return path

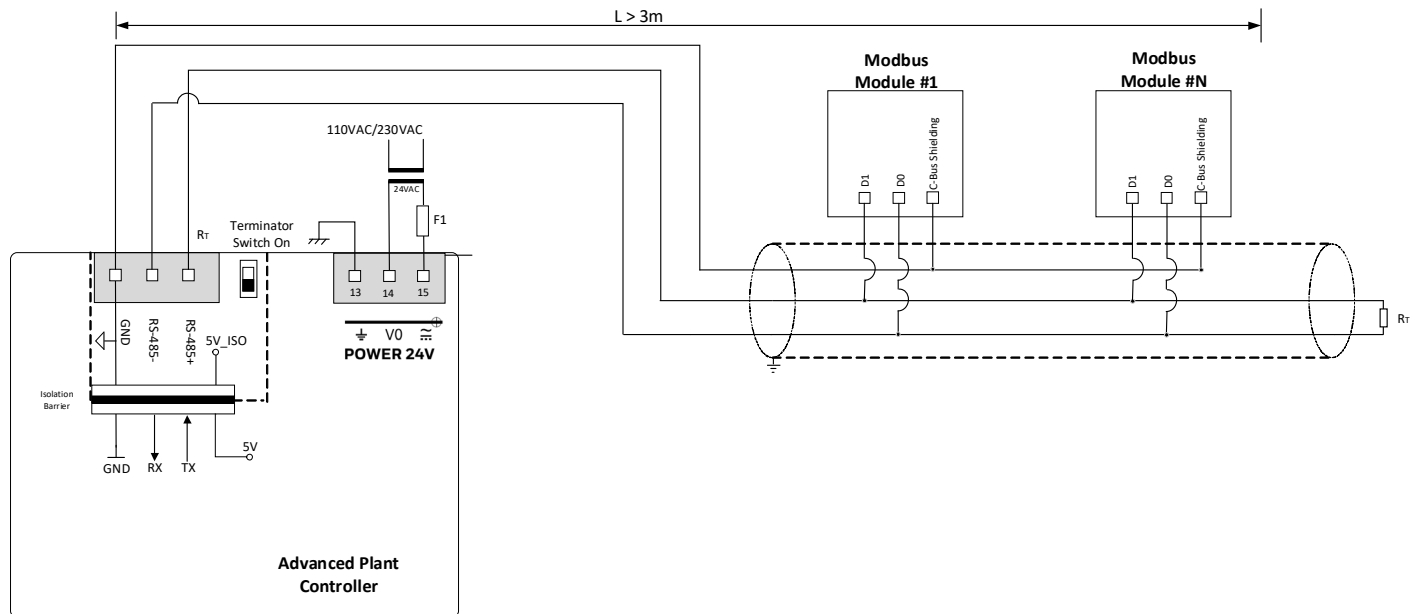


Figure 148. Connection ($L > 3$ m) of RS485 interfaces 1, 2, or 3 (RS485 interface 1 shown) to a Modbus



NOTE:

- $N = \text{max. } 32$ unit loads. Always power the Advanced Plant Controller and connect Modbus modules with separate transformers. Termination resistors must be inserted directly into the terminals of the individual Modbus modules.
- Signal ground (signal reference) connection is recommended. For more information, See [“General Safety Considerations” on page 17](#).
- For communication cable lengths, transmission speeds, and termination, See [“RS485 Bus Cable Specifications” on page 19](#). For fusing, See [“Example 1: Power Supply via Controller Using Panel Module” on page 16](#).

Connection to Modbus devices with Shielding as Return path (non-isolated)

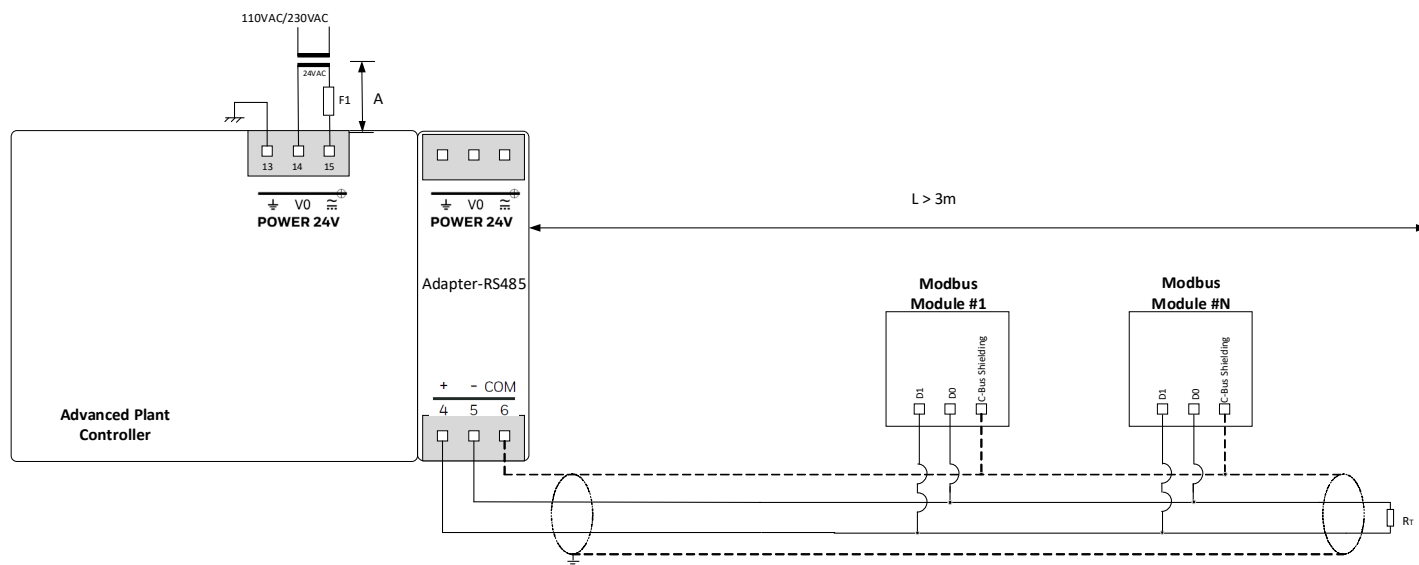


Figure 149. Connection ($L > 3\text{ m}$) of RS485-R to a Modbus



NOTE:

- $N = \text{max. } 32$ unit loads. Always power the Advanced Plant Controller and connect Modbus modules with separate transformers. Termination resistors must be inserted directly into the terminals of the individual Modbus modules.
- Signal ground (signal reference) connection is recommended. For more information, See [“General Safety Considerations” on page 17.](#)

Connection to Modbus devices with Separate Conductor as Return path (non-isolated)

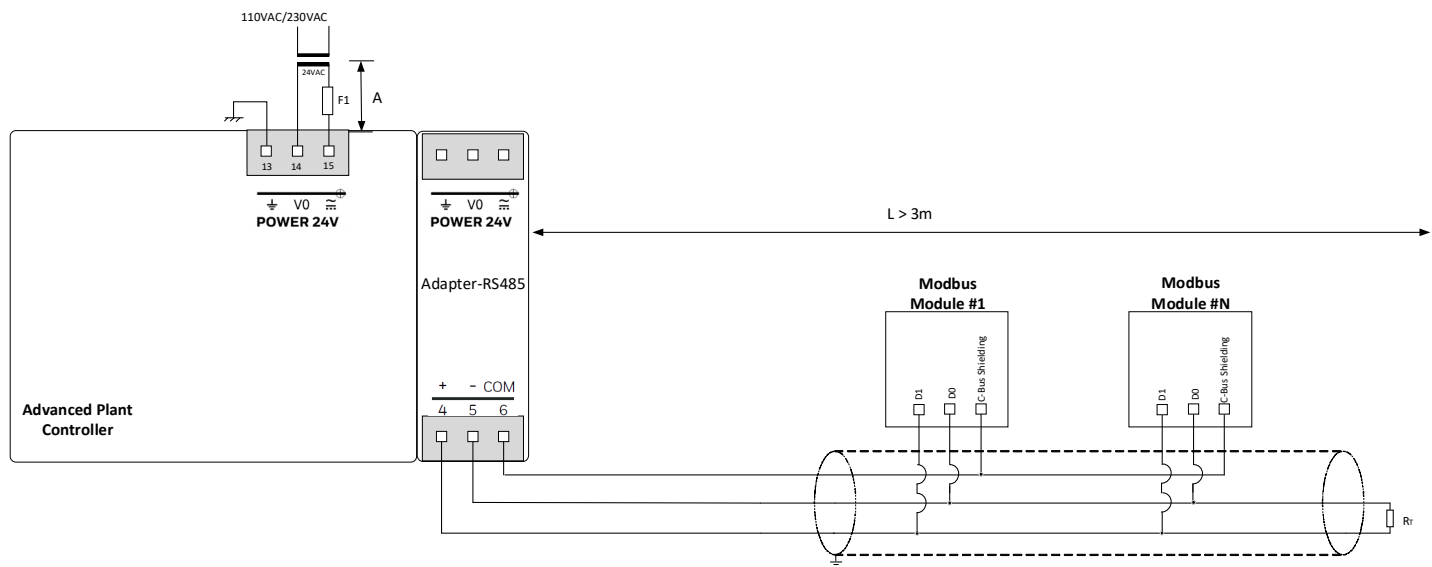


Figure 150. Connection ($L > 3\text{ m}$) of RS485-R to a Modbus



NOTE:

- $N = \text{max. } 32$ unit loads. Always power the Advanced Plant Controller and connect Modbus modules with separate transformers. Termination resistors must be inserted directly into the terminals of the individual Modbus modules.
- Signal ground (signal reference) connection is recommended. For more information, See [“General Safety Considerations” on page 17.](#)

Connection to a I/O Module Powered by the Separate Transformer

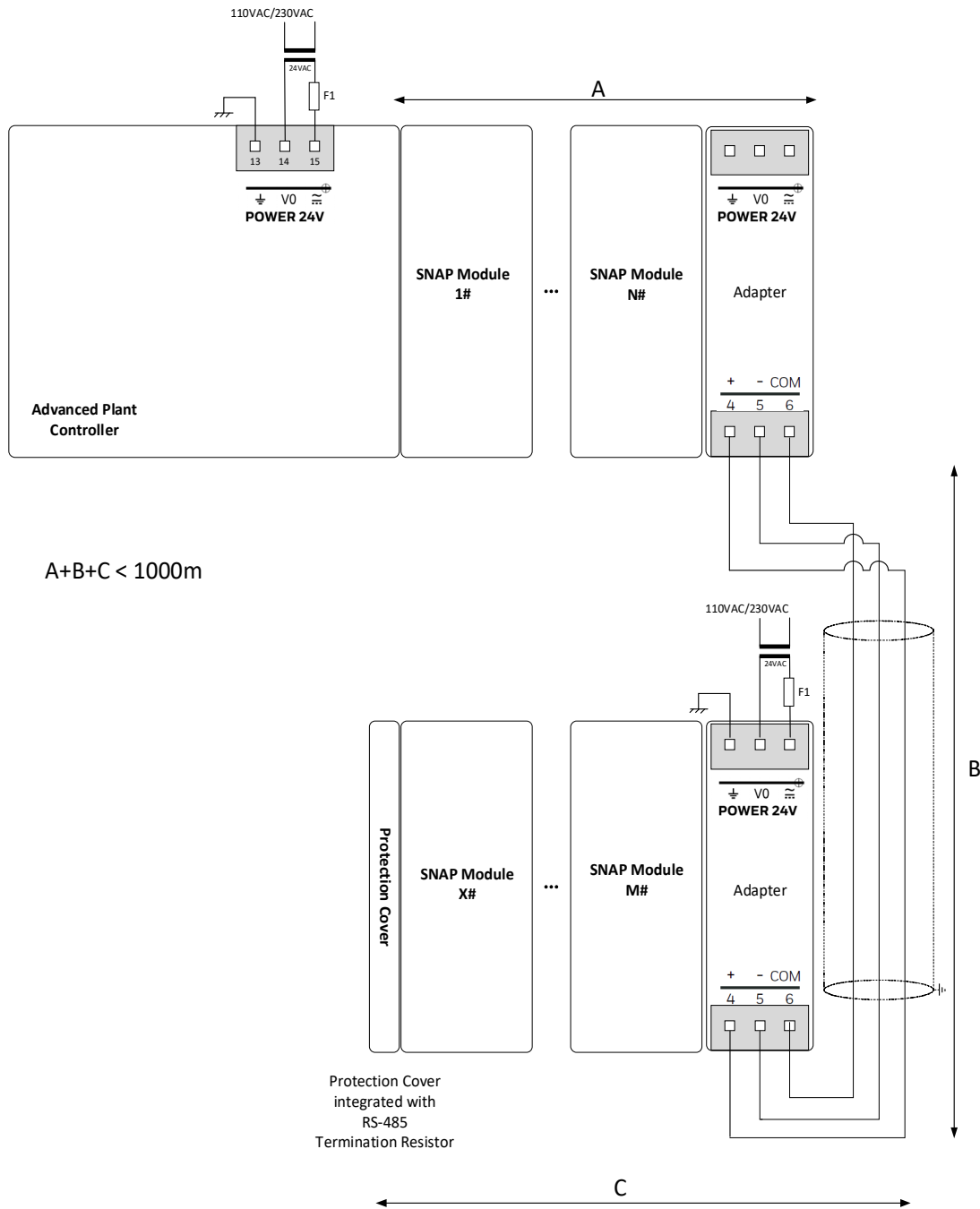


Figure 151. Connection (L > 3 m) of RS485-R to a I/O Module-IO Bus



NOTE:

— For communication cable lengths, transmission speeds, and termination, See [“General Safety Information” on page 7](#). For capacity restrictions, See [“Connection to a I/O Module Powered by the Separate Transformer” on page 155](#). For fusing, See [“Example 1: Power Supply via Controller Using Panel Module” on page 16](#).

Connection to a I/O Module Powered by a Same Transformer

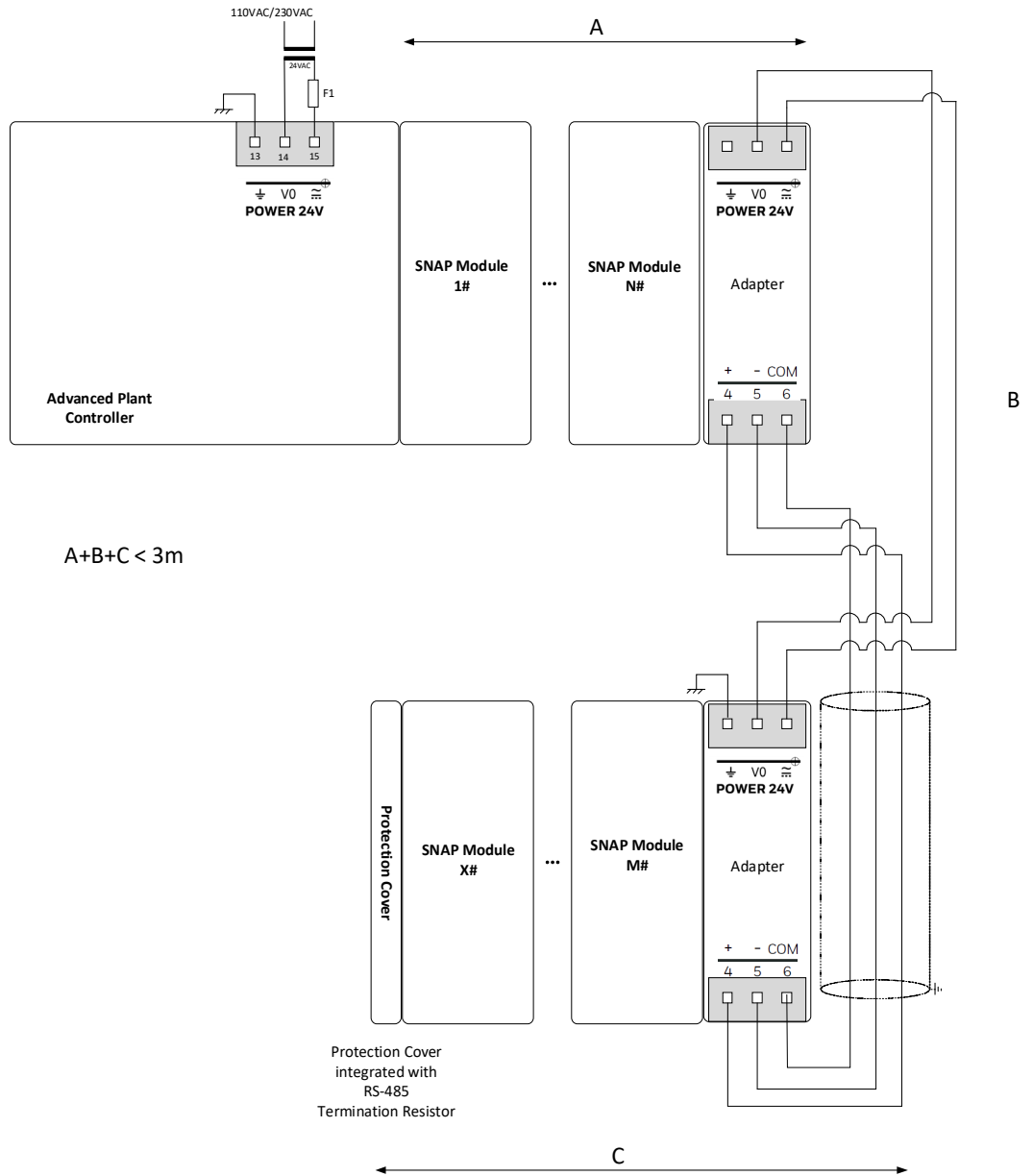


Figure 152. Connection (L < 3 m) of RS485-R to a I/O Module Bus



NOTE:

- * The 24V~ and 24V0 terminals at the RS485-4 Interface have an automatic resetting fuse protection. For more information, [See “Automatic Resetting Fuse” on page 142.](#)
- For communication cable lengths, transmission speeds, and termination, [See “General Safety Information” on page 7.](#) For capacity restrictions, see [See “Connection to a I/O Module Powered by the Separate Transformer” on page 155.](#) For fusing, [See “Example 1: Power Supply via Controller Using Panel Module” on page 16.](#)

Connection to M-Bus via Level Converter

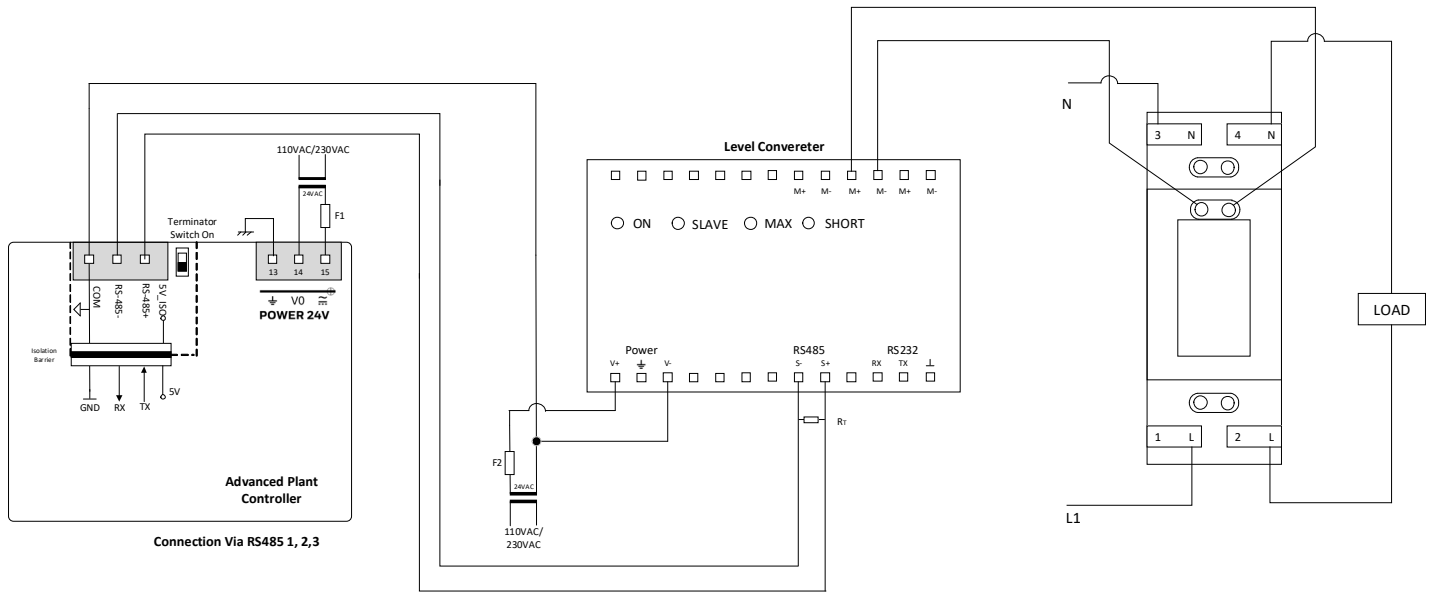


Figure 153. Connection to M-Bus via Level Converter

Connection to HMI

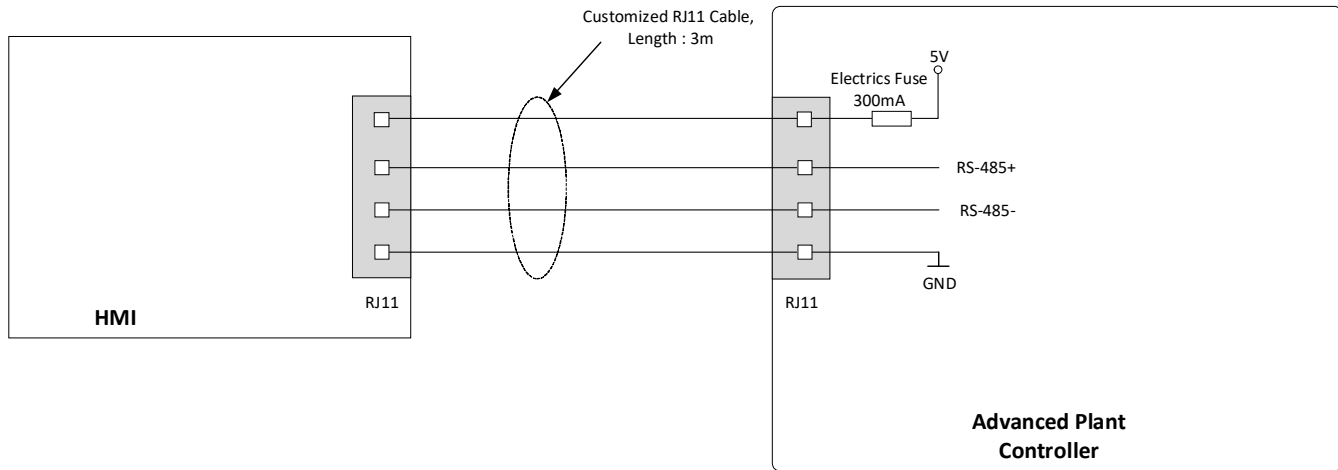


Figure 154. Connection of RJ11 interface to a HMI device



NOTE:

Maximum length of RJ11 cable is (L) 3m.

MIGRATING AN EXISTING STATION TO ADVANCED CONTROLLER

The station which is present in EagleHAWK controller can be migrated to the Advanced Plant Controller using the Niagara workbench. After migration the HMI has to be configured manually from Niagara work bench. Follow below procedure for migrating the existing station:

1. Install the following missing jars on Advanced Plant Controller: See [“Install Additional Drivers” on page 77](#). for installing the jar files.
 - honTagDisctionary-rt.jar
 - honEagleHawkHMI-rt.jar
 - honEagleHawkHMI-wb.jar
 - honEagleHawkHMI-ux.jar
2. Restart the Advanced Plant Controller. See [“Connect the Niagara-Installed PC” on page 44](#).
3. Remove the “OnboardIONetwork” (if present) from the station to migrate on the Eagle Hawk Controller. To delete the network, go to **Station** and Navigate to **Driver** > Right click on **OnboardIONetwork** and select **delete**.



NOTE:

The **OnboardIONetwork** of Eagle Hawk station will not support in the Advanced Plant Controller. So remove the OnboardIONetwork before copying the station to the Advanced Plant Controller

4. Copy the EHN4 station to the Advanced Plant Controller. See [“Copy a Station using Station Copier” on page 69](#).
5. Under the **Services** > **UserService** > Loop throw each User.
6. Delete the “**honEagleHawkHMIAuthenticator**” slot from each user. From the Nav tree, Go to Platform and login – See [“Open a Platform” on page 51](#). Expand **Station** > **Services** > **Userservices** > User name > Right click on **honEagleHawkHMIAuthenticator** and select delete.



NOTE:

The **honEagleHawkHMIAuthenticator** must be deleted from each users before enabling the **HonPlantController-Service**.

7. Add **HonPlantControllerService** under services, if the service is not available in the Station template which is copied. See [“Enable HonPlantControllerService” on page 78](#).
8. Enable “**HonPlantControllerHMIAuthenticator**” and Setup a **PIN** for HMI. Refer Setting HMI Pin from the document HMI Driver Guide - 31-00590.



NOTE:

Enable **HonPlantControllerHMIAuthenticator** and setup a PIN for each user.

9. Add a new **FAL** with the Existing FAL’s Name under **honPlantControllerService** > **HMI Device**. Refer **Filling Fast Access Lists** from the document HMI Driver Guide - 31-00590.



NOTE:

Use the same FAL name in the new copied station if the points under the existing station’s FAL are required. Points will automatically add under FAL’s after creating FAL’s with existing EagleHawk FAL’s name.

10. Delete the **honEagleHawkHmiService**, from Service.
From the Nav tree, Go to Platform and login - See [“Open a Platform” on page 51](#). Expand **Station** > **Services** > Right click on **honEagleHawkHmiService** and select delete.
11. Enable **“HonPlanControllerService”** from the Niagara workbench. See [“Enable HonPlantControllerService” on page 78](#). Commission the Advanced Plant Controller. See [“Commissioning the Advanced Plant Controller” on page 58](#).
12. Enable **HMI Device** in the **HonPlanControllerService** from the Niagara workbench. Refer **Enable HMI Device** from the document HMI Driver Guide - 31-00590.
13. Commission the HMI.
Right click on **HMI Device** > **Actions** > Click **Commission HMI**. Refer **Commissioning HMI** from the document HMI Driver Guide - 31-00590.

 **NOTE:**
Job success will appear in the **Job log** if the commissioning is successful and there are no errors.

14. Update the BACnet User Role as admin (if not exists).
15. If the Existing station already has BACnet Driver with any Local Device ID, then Local Device ID will change to 100 after-commission HMI under honPlantControllerService.

 **NOTE:**
Refer **HMI Device Configuration** from the document HMI Driver Guide - 31-00590.

16. After that Change, the Local Device ID and HMI Instance number under BACnet driver as per the Requirement, then Commission again.

 **NOTE:**
For **Local Device ID** and **HMI Instance number**, Refer the document HMI Driver Guide - 31-00590.

17. Save station.

TROUBLESHOOTING

Troubleshooting with LEDs of RS485 Interfaces 1, 2, 3

Table 35. Advanced Plant Controller Tx and Rx LEDs of RS485 Interfaces 1,2, and 3

Case	LED Behavior	Meaning	Remedy
1	Green (ON) - Solid	Bus is functioning properly.	No action is necessary.
2	Yellow (ON) - Solid	Bus is not functioning properly.	Check termination. Check the polarity of bus connections. Check for EM interference.
3	Red (ON) - Solid	No communication over given interface.	Use Niagara to check interface assignment in the application.
4	Red (ON) - Blink every 0.5 S (On/Off)	Reserved	Check the wiring.

Troubleshooting with the Ethernet Interface LEDs

Table 36. Advanced Plant Controller link and activity LEDs of Ethernet interfaces 1 and 2

Case	LED Behavior	Meaning	Remedy
1	Yellow LED is ON steadily.	Ethernet is working with connectivity below 100Mbps.	If communication problems persist, then check the green LED. See Case 3 and Case 4 given below.
2	Yellow LED is OFF	If the green LED is ON or flashing, then Ethernet is working with connectivity below 10Mbps. If green LED is OFF, then Ethernet is disconnected.	Connect the cable between the controller and the switch.
3	Green LED is flashing.	Normal operation. The controller is transmitting/receiving data to/from the switch via cable.	If communication problems persist, the Ethernet parameter configuration may be defective: Check the IP address, MAC address, and firmware.
4	Green LED is ON	Ethernet connectivity exists but no data flow.	Check the software configuration.
5	Green LED is OFF	Ethernet port link is down.	Check the cable connection between the controller and the switch. Check the switch. Use good a laptop or good cable to directly connect the controller and the switch.

Troubleshooting with Controller configuration

Table 37. Advanced Plant Controller Troubleshooting

Case	Problem	Meaning	Remedy
1	Station is not running after USB restore.	USB restore version is not compatible with the Niagara workbench version.	- Check the backup version. Station data and configurations shall be backup and restored on controllers running at the same Niagara version. Refer to the “Enable/Disable USB Backup and Restore” on page 135. - Check the USB backup procedure and perform again, if it is not proper.
2	Unable to upgrade the Controller firmware version from 4.10U5 to 4.12U2	Controllers with below firmware versions: 4.10.5.14.0.6.5 4.10.5.14.0.7.5 or older cannot be updated to higher versions: 4.10.5.14.0.7.6 4.10.5.14.0.11  NOTE: If you have a controller with firmware version: 4.10.5.14.0.7.6, Before upgrading to any higher firmware version, upgrade the controller from firmware version 4.10.5.14.0.7.6 to 4.10.5.14.0.11.	If you have or updated controller version 4.10.5.14.0.11, please follow the below steps to update the controller firmware version to 4.12.2.16.5. Procedure: - Update the Niagara workbench version 4.10.5. with the modules that you receive with the build. Get the firmware version modules from location: US: <Need Location URL> EU: <Need Location URL> - Copy the 4 firmware files of the version 4.10.5.14.0.11 into the following 4.10 U5 workbench directory. Example: "C:\Users\exxxxxx\Niagara4.10\OptimizerSupervis or\sw\inbox" - Stop the 4.10.5 Niagara workbench. - Install Platform Daemon of 4.10.5 Niagara workbench. - Restart 4.10.5 Niagara workbench. - After the workbench restart, connect to the controller's platform. - Commission the firmware 4.10.5.14.0.11 into the controller by using the commissioning wizard. Refer to the “Commissioning the Advanced Plant Controller” on page 58. - After restarting the controller, start the workbench 4.12.2.16.0.4 and connect to the controller platform. - Now commission your station into the controller. Note: Firmware update to version 4.12.2.16.0.4. To check the firmware version Go to Station's Platform Administration and see Niagara Runtime version.

TECHNICAL LITERATURE

Table 35. Technical Literature

Title	Product Literature Number
ComfortPoint Niagara Advanced Plant Controller Product Datasheet	31-00583
Optimizer Advanced Product Datasheet	31-00631
Mounting Instruction	31-00553

The material in this document is for information purposes only. The content and the product described are subject to change without notice. Honeywell makes no representations or warranties with respect to this document. In no event shall Honeywell be liable for technical or editorial omissions or mistakes in this document, nor shall it be liable for any damages, direct or incidental, arising out of or related to the use of this document. No part of this document may be reproduced in any form or by any means without prior written permission from Honeywell.

Honeywell | Building Automation

715 Peachtree Street, N.E.,
Atlanta, Georgia, 30308, United States.
<https://buildings.honeywell.com/us/en>

® U.S. Registered Trademark
©2024 Honeywell International Inc.
31-00584-02 Rev. 01-24

Honeywell