SENSIA
Rockwell Automation + SLB

QRATE HCC2

Hyperconverged Edge Controller

Software Manual

SOFTWARE VERSION 1.9.3.500
JANUARY 2026

IMPORTANT SAFETY INFORMATION

SYMBOLS AND TERMS

The following messages may be used in this document to help ensure personal safety and efficient handling of equipment.

	**CAUTION** A hazardous situation which, if not avoided, can result in minor or moderate injury, loss of property, or business risk.
Important	Non-urgent information that may impact the outcome of a process or procedure.
Note	Additional information or a tip that may help the user to work more efficiently.

CONTACT SENSIA

For technical support, please refer to https://www.sensiaglobal.com/Technical-Support.

For all other inquiries, please refer to https://www.sensiaglobal.com/Customer-Care or dial 1-866-773-6742.

RELEASE HISTORY

Release	Description of Change	Issuer	Approver	Date
1.6.2.181	Commercial Release	KM/KK	MN	Feb. 7, 2024
1.6.5.279	Added information regarding • web server certificate enrollment • cellular connectivity health check • user firewall port screen for adding new ports • use of private web browser mode (Incognito/InPrivate) when connecting with Unity Edge	KM	MN	May 31, 2024
1.7.0.343	Changes include: • Enhancements to alarm configuration screens • Enhancements to data log export screens and the data log extractor wizard • Addition of a configurable Unity Edge display mode, allowing a selection of light or dark screens • Bug fixes	KM	MN	Oct. 17, 2024
1.8.1.383	Changes include: • Sparkplug B configuration procedure • OPC UA server configuration procedure • FTOptix information	KM	MN	March 20, 2025

	• operating system support for delta updates and online container registry bundle updates for low-bandwidth connections • removal of requirement to use private web browser mode (Incognito/InPrivate) when connecting with Unity Edge • substitution of “data point” for “tag” • updates to Modbus Protocol Map Editor user interface (section 8)			
1.9.1.396	Changes include: • ENIP target driver description and configuration procedure (section 11) • DNP3 outstation driver description and configuration procedure (section 12) • availability of a custom mender instance as an alternative to the Sensia-managed instance previously supported for remote management of the HCC2 • updates to the Edge Package Manager (EPM) device management menu	KM	MN	May 31, 2025
1.9.3.500	Changes include: • OPC UA client configuration procedure • Licensing gateway description • Serial communication over Bluetooth • Updates to CIP device library, EPM functionality, ISaGRAF space monitoring • Updates to configuration deployment process and interface deployment buttons	KM	MN	Jan. 14, 2026

PUBLISHER NOTES

DISCLAIMER

While Sensia has taken every care in the preparation of this document, it cannot accept responsibility for printing errors or omissions and does not warrant that it is correct and comprehensive in every particular instance. Equipment supplied should always be operated by persons with an appropriate level of skill and training.

Sensia shall not be liable for incidental or consequential damages resulting from the furnishing, performance or use of this material.

Sensia pursues a policy of continuous improvement, and information given herein may be updated without notice. Further, this information is proprietary to Sensia, and must not be disclosed to any third party except as may be required to operate the equipment supplied in accordance with the purposes for which it was sold by the persons properly licensed to operate it.

COPYRIGHT NOTICE

TRADEMARKS & SERVICE MARKS

An asterisk (*) is used throughout this document to designate marks of Sensia. Other company, product, and service names are the properties of their respective owners.

Sensia, the Sensia logotype, and other words or symbols used to identify the products and services described herein are either trademarks, trade names or service marks of Sensia and its licensors, or the property of their respective owners. These marks may not be copied, imitated or used, in whole or in part, without the express prior written permission of Sensia. In addition, covers, page headers, custom graphics, icons, and other design elements may be service marks, trademarks, and/or trade names of Sensia and may not be copied, imitated, or used, in whole or in part, without the express prior written permission of Sensia.

WARRANTY

Product warranty is specified in Sensia Terms and Conditions at the time of purchase.

SECURITY NOTICE FOR SOFTWARE PRODUCTS

The software described herein is designed to operate with the minimum hardware and operating system specifications recommended by Sensia. The software should be operated in a secure environment whether operation is performed across a network, on a single system and/or on multiple systems.

The end user is responsible for configuring and maintaining networks and/or system(s) in a secure manner. The end user is also responsible for obtaining, installing, operating and maintaining all hardware, other equipment and third party software required for use of the software. Sensia is not responsible for data loss arising as a result of software use or interaction of the software with any third party software.

For more information about recommended security practices, please contact Sensia Technical Support via https://www.sensiaglobal.com/Technical-Support.

TABLE OF CONTENTS

Section 1: Introduction

This user guide describes the steps required to configure, monitor, and maintain your QRATE HCC2 Edge controller.

Here you will find instructions for

- establishing a PC or laptop connection with your HCC2
- launching and navigating the user interface
- updating the software and installing/removing applications
- configuring workflows for integrating data from external devices and monitoring critical operations

The HCC2 combines the functionality of an RTU, a PLC, an edge computer, and a wired/wireless gateway in a tightly integrated and configurable package.

Note	See the HCC2 device hardware manual for details about the product's functionality, hardware design, and installation.

1.1 AUDIENCE

This guide is intended for the following user groups.

User	Sample Tasks
Process automation engineers	Build and deploy an ISaGRAF app, configure digital and analog IO, add and configure subdevices, configure communication protocols, etc.
Field engineers	Deploy an edge application, connect to sub devices or drives, map data from subdevices or apps
Industrial internet of things engineers	Deploy a gateway, map data from sub devices or apps, connect to Avalon
Operators	Operate and maintain equipment
System integrators	Build systems comprising HCC2 and other equipment, integrate hardware and software, configure data paths and communication

Users should have experience and/or expertise in the following:

- control logic
- hard-wired and Ethernet connections
- software configuration
- Modbus protocol
- ISaGRAF (if you will be integrating ISaGRAF projects into the HCC2)
- basic Avalon configuration (if you will be provisioning the HCC2 Avalon Gateway)

1.2 HCC2 MODELS

Sensia offers several HCC2 controller models as shown in the table below.

RTU plus App Enablement is a license that enables you to install custom edge applications developed with the Edge Software Development Kit to expand HCC2 functionality beyond the core applications supplied out of the box. See also section 1.3.4 License(s), page 14.

Model Number	Description
50365260-2001	QRATE, HC2, Hyperconverged Edge Controller Base Model
50369741-2001	QRATE, HCC2, Hyperconverged Edge Controller with Wi-Fi and LTE
50365260-2002	QRATE, HCC2, Hyperconverged Edge Controller Base Model, RTU plus App Enablement*
50369741-2002	QRATE, HCC2, Hyperconverged Edge Controller with Wi-Fi and LTE, RTU plus App Enablement*

* The App Enablement upgrade is also sold separately (part number Edge-Ena-Lic) for user installation. Ask your Sensia sales representative for details.

1.3 HCC2 SOFTWARE OVERVIEW

This section describes the software components required to operate and maintain the HCC2 controller.

1.3.1 User System Requirements

Ensure that your Windows computer meets the following system requirements for use with Unity Edge software.

Supported Browsers	Google Chrome, Microsoft Edge
Recommended Screen Resolution	1366 x 768 or better
OS	Windows 10 or 11
CPU	4th generation Intel Core i3 or later processor AMD Ryzen or later processor
RAM	8 GB
Interface Network Connections	Choose from local USB-C, Ethernet, or wireless. See Section 2: Connecting to Unity Edge, page 17, for details.

1.3.2 Pre-installed Software

Each HCC2 controller ships with

- a pre-installed Linux-based operating system
- a set of core applications supporting RTU and Edge functionality

With this software and a USB-C cable or an Ethernet cable, you can connect to the HCC2 via Unity Edge, a web-based user interface that you can access from a Google Chrome or Microsoft Edge web browser.

Unity Edge

Unity Edge is the configuration and operations monitoring interface for the HCC2.

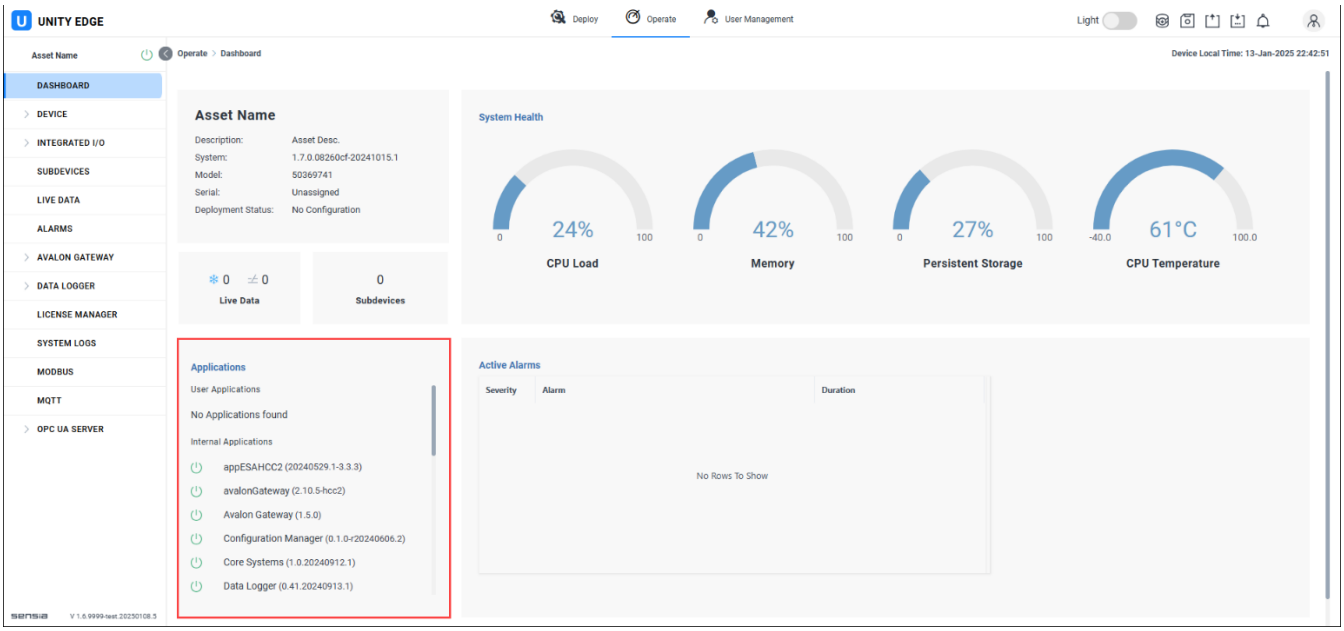


Figure 1.1—Unity Edge Interface

See Section 3: Navigating the Unity Edge Interface, page 30, for a step-by-step guide to the menu structure and navigation.

Applications

The applications installed on an HCC2 device define its functionality. The pre-installed core applications which appear on the interface dashboard (as highlighted in Figure 1.1) on all HCC2 devices manage

- alarms and events
- data logging
- Modbus server and client configuration
- integrated and external I/O
- Avalon connectivity

Optionally, you can expand and customize your operations by purchasing and installing custom Edge applications. They can be domain-specific (for example, managing submersible pump control or flow computation) or general purpose, providing harmonic analysis or additional communication protocols. Contact your Sensia sales representative for information regarding your specific needs.

1.3.3 Software Downloads

Software for HCC2 maintenance and extended functionality is available for download from Sensia's Microsoft Azure Storage Explorer repository.

For download instructions

1. Visit URL https://www.sensiaglobal.com/Technical-Support.
2. Click Customer Support Portal Access in the top right corner of the screen and search for RTU and Edge Devices Firmware and Software Download Procedure. Or use this link to navigate to the procedure: Knowledge Article KA-04676.
3. Follow the procedure to connect to the Microsoft Azure Storage Explorer repository and download any of the software files listed below.

Software	Filename	Description	For more info, see:
Release notes	Release Notes***.pdf	READ FIRST! HCC2 Operating System and CoreApps bundle release notes.	
Edge Package Manager (EPM)	EPM***.zip	A maintenance utility for updating the OS and HCC2 applications	Section 4.1
Data Log Extractor (DLE)	DataLogExtractor***.zip	A utility for extracting HCC2 data logs for analysis and viewing	Section 4.7
Operating system updates	sensia-os***.mender	HCC2 operating system (OS) update file	Section 4.2
“Delta” operating system updates (small files)	delta-***-to-***.mender	HCC2 operating system (OS) update file for low-bandwidth or high-latency connection	Section 4.4.1
Application and app bundle updates	bundle installer.mender	HCC2 core applications container bundle update file	Section 4.3
Online container registry for app/app bundle updates (small files)	online only bundle installer.mender	HCC2 core applications container registry update file for users with low-bandwidth or high-latency connection	Section 4.4.2
EtherNet/IP target driver	hcc2_eniptarget***.mender	Application to allow the exchange of HCC2 data points with Rockwell Automation control systems	Section 11
DNP3 outstation driver	hcc2_dnp3outstation***.mender	Application allowing HCC2 to gather and transmit data as an outstation to a master station using TCP communications	Section 13
HCC2 ISaGRAF Add-in	HCC2IOB-***.zip	Add-in that makes the ISaGRAF Workbench software compatible with the HCC2 Important: This add-in is for use ONLY with ISaGRAF Workbench software, a product of Rockwell Automation. See the ISaGRAF Workbench download link below.	Section 15
FactoryTalk Optix installer	hcc2OptixBundle.mender	Data visualization software for use with HCC2. Requires FactoryTalk Optix license from Rockwell Automation and FactoryTalk Optix Studio software	Section 16

Security certificate	hcc2-unity.pfx	Certificate for enabling trusted HTTPS connections to Unity Edge.	Section 2.1.3

ISaGRAF Workbench

For the ISaGRAF integration, ISaGRAF Workbench version 6 is required for use with HCC2 and is distributed by Sensia under Part No. ISA-WB6_Lic. Ask your Sensia sales representative for details.

Download ISaGRAF Workbench software from this URL:
https://compatibility.rockwellautomation.com/Pages/home.aspx

1.3.4 License(s)

Pre-installed core applications supplied with every HCC2 require no license to operate.

Edge applications may require the purchase of a Sensia License. See section 7.8 License Manager, page 89, for more information about securing, installing, and monitoring Sensia licenses in Unity Edge.

ISaGRAF Workbench

ISaGRAF Workbench software, which creates ISaGRAF applications for the HCC2, requires a paid license. Contact your Sensia sales representative for more information.

HCC2 Edge App Enablement

Edge applications are custom apps that expand HCC2 functionality beyond the core applications supplied with each device.

An Edge App Enablement license is required for installing applications other than the core bundle supplied with every HCC2. This license is a one-time purchase that enables future Edge application installations. Depending upon the HCC2 model you purchased, this license may be pre-installed at the factory or issued separately for user installation. See section 1.2 HCC2 Models, page 10, for a list of HCC2 models.

1.4 SOFTWARE SECURITY FEATURES

The HCC2 software package includes multiple security features as shown below.

Security Feature	Description
TPM 2.0	Binds licenses to the hardware and secure key storage
Secure Boot	Ensures that only trusted software runs on the device
Signing of applications, containers, and firmware	Prevents installation of malicious software on the HCC2
Firewall	Enables users to select protocols/services allowed on each port. Minimum access is allowed by default for out-of-box operation.
Access	Manages access via configurable User Access systems (based on LDAP) supported by device management and configuration tools
Protected Mode	Prevents unwanted changes to active deployments using physical DIP switch settings
ISaGRAF Workbench	Restricts access to the ISaGRAF instance or edits to the ISaGRAF applications using a password feature
Secure Update Protocols	Enables updates using secure communication

1.4.1 Protected Mode

When your HCC2 configuration is complete, you can use Protected mode to prevent unwanted or malicious changes to an active HCC2 deployment.

In Protected mode, your HCC2 maintains its normal operation functions and its alarm acknowledgment features and allows some changes to app runtime settings.

Access Restrictions

Before enabling Protected mode, you should consider the following limitations.

In Protected Mode You CANNOT	In Protected Mode You CAN
Remotely access the HCC2	Perform standard Operate menu functions
Deploy configuration updates from Unity	Acknowledge alarms
Update apps or the OS from EPM or the Mender.io site	Change some app runtime settings
Perform actions (start, stop, edit, download, etc.) on any ISaGRAF resource on the IO board	
Remotely reset or reboot either board	
Reset the device to factory default settings	
Wipe data or apps	
Change Ethernet, serial, or Wi-Fi settings	
Change the time manually	
Apply a new software license	

Enabling Protected Mode

Important Do not enable Protected mode before you configure your HCC2.

Important Protected mode restricts remote access to the HCC2 device. When Protected mode is active, you must have direct access to the HCC2 device to reconfigure it.

To enable the Protected mode

1. Remove the small round plug from the left side panel. Note the switch location shown in Figure 1.2, page 16.
2. Set the two configuration (DIP) switches to the ON (up) position.
3. Replace the plug.

See the QRATE HCC2 Hardware Manual for additional information.

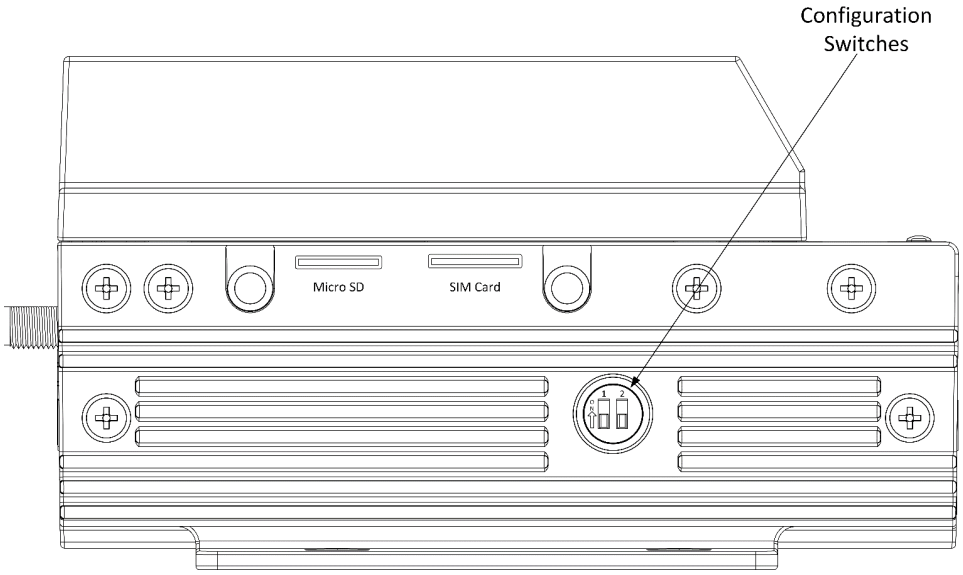


Figure 1.2—Configuration Switches for Enabling Protected Mode (Cover Removed)

Section 2: Connecting to Unity Edge

This section discusses the connectivity options available in the HCC2, provides instructions for connecting to the Unity Edge web interface, and provides an overview of the software menu structure and basic navigation of configuration and monitoring features.

For a first-time connection, Sensia recommends the USB-C port (requires a user-supplied cable) or the Ethernet 2 port.

2.1 FIRST-TIME CONNECTION TO UNITY EDGE (USB-C)

Use the USB-C maintenance port on the top panel of your HCC2 (Figure 2.1) to make the initial connection to HCC2 and to launch Unity Edge.

The port's fixed IP address is 169.254.1.1.

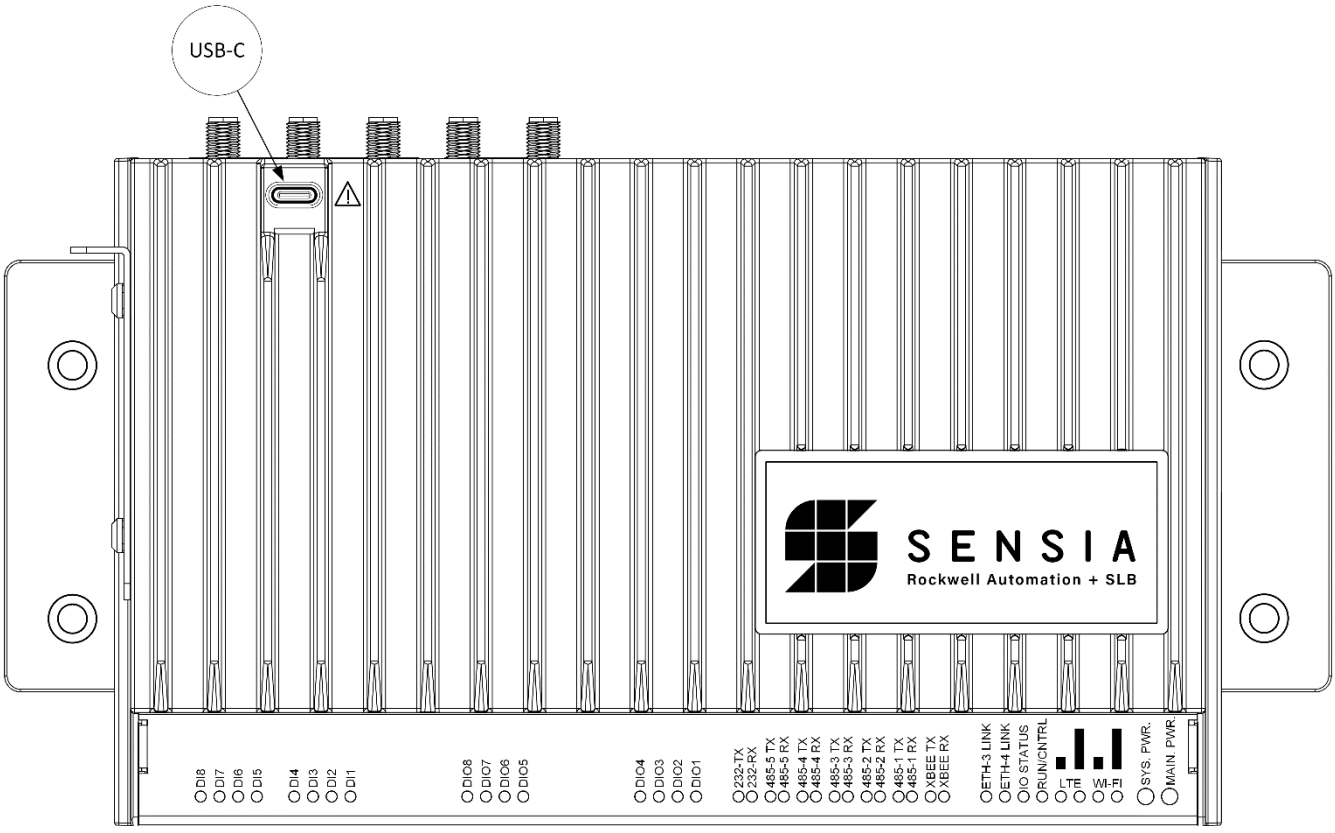


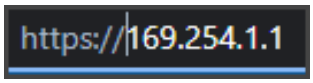
Figure 2.1—USB-C port location

Important The USB-C maintenance port IP address cannot be modified and cannot be disabled in the firewall settings. This connection method is recommended when you

- do not know the IP address of another network interface
- cannot change the IP address of the other HCC2 network interfaces
- have a new device with a default configuration

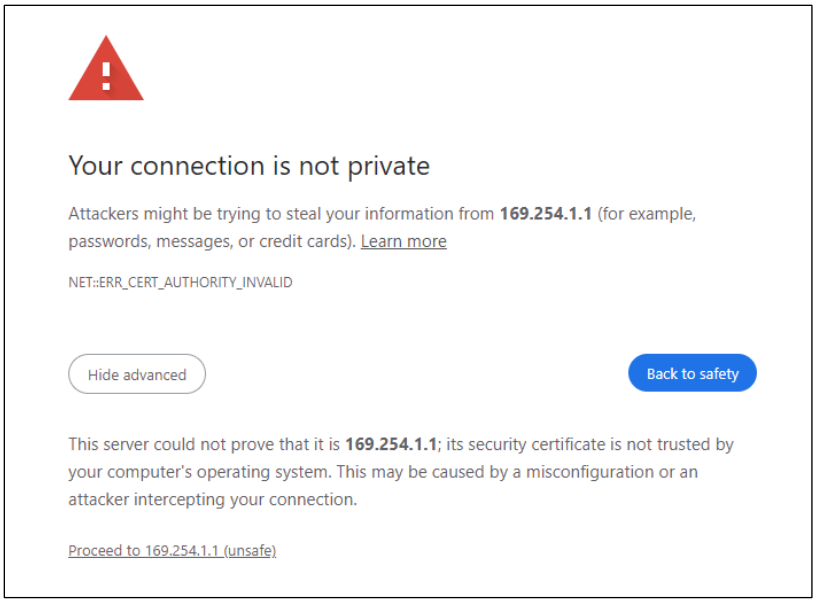
To connect:

1. Obtain a USB-A to USB-C cable or USB-C to USB-C cable. The USB-C side connects to the HCC2. The other connector must be compatible with your computer port.
2. Connect the cable connectors to the USB-C port of your HCC2 and to your PC or laptop.
3. In your Google Chrome or Microsoft Edge web browser, enter the IP address of the maintenance port in the address bar and press ENTER:

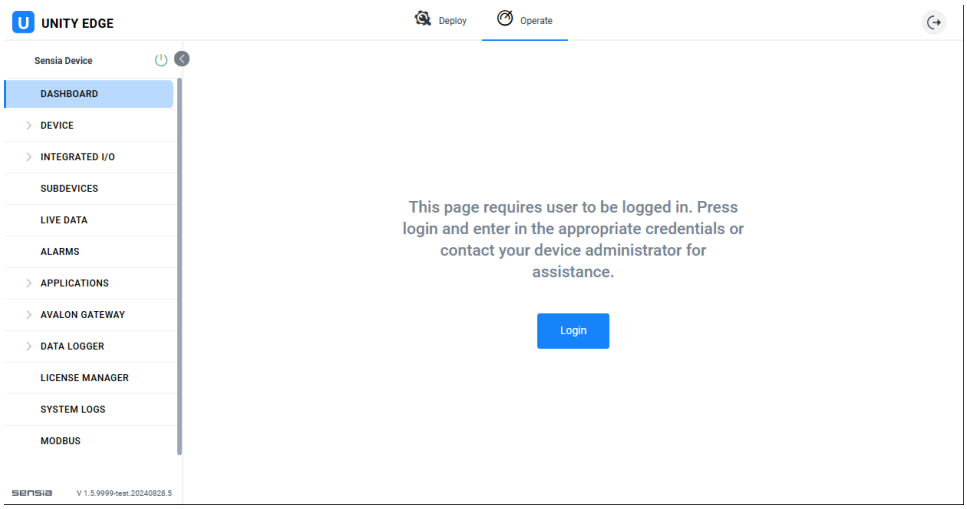
4. At the first Unity connection attempt, a warning may appear, advising you that your connection is not private. This is expected because the Unity Edge interface has a Web Server Certificate that is signed by a Private Sensia Certificate Authority.

   To safely bypass the warning, click Advanced and then click the Proceed to 169.254.1.1 (unsafe) link.

   Alternatively, you can enroll the Web Server Certificate so that your Windows operating system will recognize it as a trusted certificate. See section 2.1.3, Enroll a Web Server Certificate (Optional), page 20, for details.

5. Follow the login instructions in section 2.1.1, Manage Login and Admin Passwords, page 19.

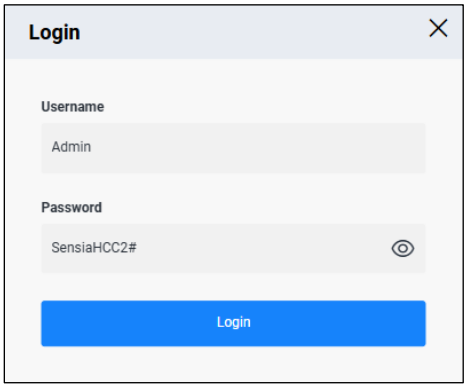


2.1.1 Manage Login and Admin Passwords

1. Click Login to open a Login dialog screen.
2. Enter your login information.

Default username (not case-sensitive)	admin
Default password (case-sensitive)	SensiaHCC2#

3. Click Login.

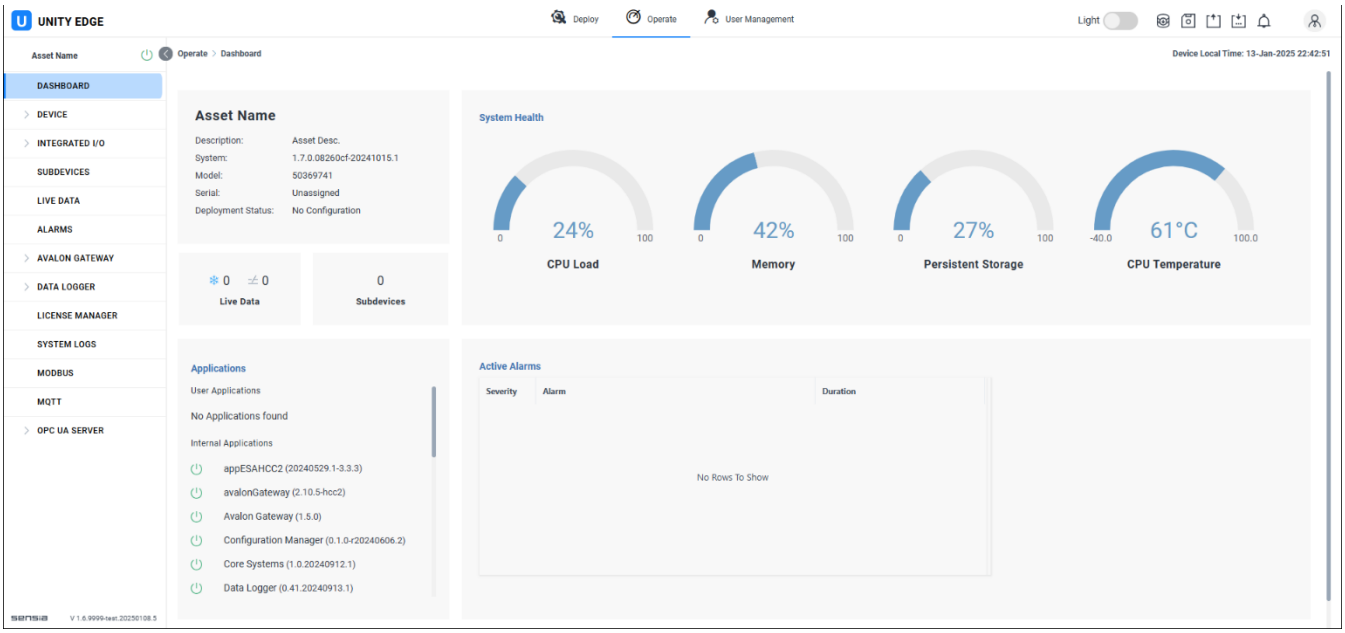


Important For security reasons, you are directed to change the default administrator password after your initial login. **Record this new password, preferably with a password manager. If you lose this password, you will be locked out of the Unity administrator account.**

This password is also used when connecting to the device using EPM.

4. Change the password as directed and log back into Unity using the new credentials.

   The Unity Edge dashboard is displayed.



See Section 5: Managing Users and Permissions, page 49, to set up new users and apply controls to user access.

2.1.2 Store your USB-C Cable

When you have completed your HCC2 configuration, disconnect the cable from your USB-C maintenance port.

CAUTION

Store your USB-C cable in a safe place when it is not installed on your HCC2. Maintenance technicians may require its use to connect with your device. If you inadvertently block your access to Unity Edge with configuration controls, the USB-C cable is the only method of restoring access to the software interface.

2.1.3 Enroll a Web Server Certificate (Optional)

The Unity Edge interface has a Web Server Certificate that is signed by a Private Sensia Certificate Authority.

Important As the Sensia Certificate Authority is not a public Certificate Authority, a web browser may not automatically validate it. If your web browser generates a warning that the Certificate can't be trusted or validated, you can bypass the message as described on page 18. Alternatively, for USB-C connections only, you can use the following procedure to enroll the Certificate so that it will be recognized and trusted by your Windows operating system.

The following instructions are for enrolling a Web Server Certificate in a Windows Desktop Operating System.

1. Download the hcc2-unity PFX file from the list of HCC2 software files provided by Sensia.
2. Use the Windows+R keyboard shortcut to open a Run command window.
3. Type mmc, click OK, and authorize the Microsoft Management Console Program to make changes to your device.
4. In the Microsoft Management Console Program
   a. Click on File > Add/Remove Snap In…
   b. Select Certificates, click Add.
   c. Select My User Account, click Finish, and click OK.

d. In the left column, navigate to Certificates - Current User > Trusted Root Certification Authorities > Certificates.

e. In the Toolbar, click on Action > All Tasks > Import…

f. Follow the Certificate Import Wizard instructions.

- At the prompt to select files to import, click “Browse…” and select “all files” in the file type field to view the .pfx file.
- No password is required.

5. When the import process is finished, close the Microsoft Management Console Program.
6. Close any open browser windows.

   The following certificates should be installed:

Serial Number	7d:5c:ef:4d:24:04:b4:bf:78:ef:ff:01:4f:29:2c:3e:d0:2f:a3:5f
Signature Algorithm	ecdsa-with-SHA384
Issuer	C=US ST=Texas L=Houston O=Sensia LLC OU=Sensia Digital Solutions CN=Sensia CA
Subject	C=US ST=Texas L=Houston O=Sensia LLC OU=Sensia Digital Solutions CN=Sensia Intermediate CA

Serial Number	2f:e7:a8:11:6b:bb:f1:24:11:9f:7e:a8:a4:eb:68:89:dd:42:3d:18
Signature Algorithm	ecdsa-with-SHA384
Issuer	C=US ST=Texas L=Houston O=Sensia LLC OU=Sensia Digital Solutions CN=Sensia CA
Subject	C=US ST=Texas L=Houston O=Sensia LLC OU=Sensia Digital Solutions CN=Sensia CA

7. Add the USB-C port IP address (169.254.1.1) and a valid Fully Qualified Domain Name (FQDN) for your HCC2 to the following System 32 hosts file:

   %SystemRoot%\System32\drivers\etc\hosts

This will allow the browser to validate the FQDN against the Server Certificate when you connect to Unity Edge via a USB-C network connection.

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#   127.0.0.1       localhost
#   ::1             localhost
169.254.1.1         hcc2-1219110790422.local
```

The only valid FQDNs for HCC2 devices are:

- hcc2-<HCC2 SERIAL NUMBER>.local
- hcc2-<HCC2 SERIAL NUMBER>.sensia.local

To connect to Unity Edge, you will now enter a valid FQDN into the web browser instead of the USB-C IP address.

2.2 FIRST-TIME CONNECTION TO UNITY EDGE (ETHERNET)

ETH-1 and ETH-2 ports are located on the front panel of the HCC2 (Figure 2.2). For a first-time connection, Sensia recommends ETH-2 because of its static IP address. By default, ETH-2 has the IP address 192.168.1.41.

Note	The ETH-2 connection will work only if your PC is on the same subnet.

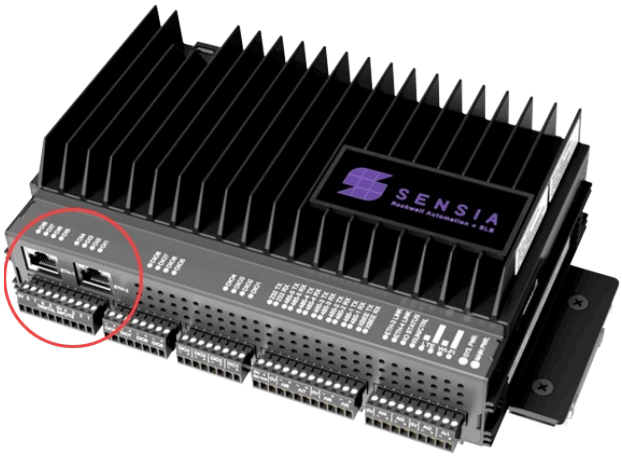
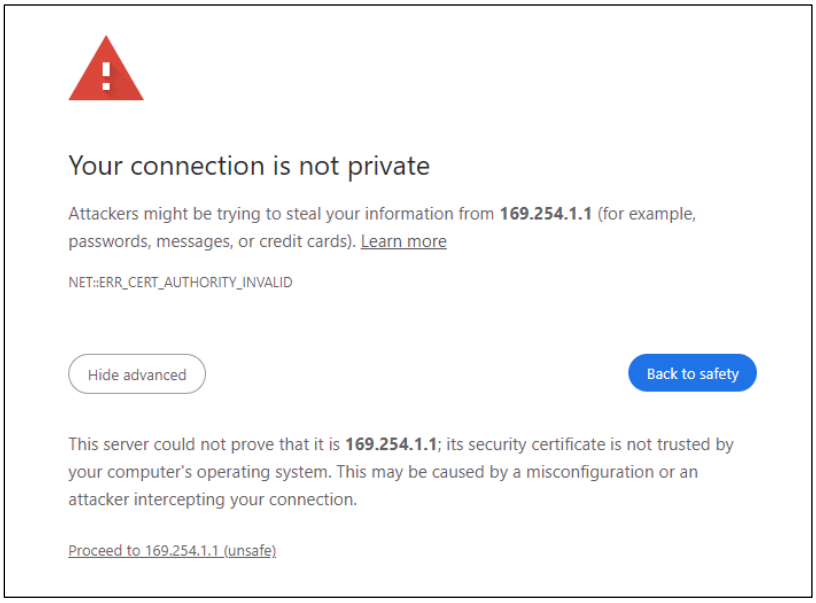


Figure 2.2—Ethernet port location

To connect to Unity Edge:

1. Connect an Ethernet cable to the ETH-2 port and to your PC or laptop.
2. In your Google Chrome or Microsoft Edge web browser, enter IP address 192.168.1.41 in the address bar and press Enter.
3. At the first Unity connection attempt, a warning may appear, advising you that your connection is not private. This is expected because the Unity Edge interface has a Web Server Certificate that is signed by a Private Sensia Certificate Authority.

   To safely bypass the warning, click Advanced and then click the Proceed to 169.254.1.1 (unsafe) link.



4. Proceed with the login instructions in section 2.1.1, Manage Login and Admin Passwords, page 19.

ETH-2 is a configurable port. For information on configuring network settings, see section 2.5 Configuring an Ethernet Connection, page 25.

See Section 5: Managing Users and Permissions, page 49, to set up new users and apply controls to user access.

2.3 OVERVIEW OF NETWORK CONNECTIONS

After making the initial connection to and launching Unity Edge, you can change the connection type to Ethernet, Cellular or Wi-Fi, if your network administrator permits.

- Unity Edge access is always enabled on USB-C.
- Unity Edge access is enabled on ETH-1 and ETH-2 by default, but you can disable it. Unity Edge access is not supported by ETH-3 or ETH-4.
- Unity Edge access is disabled by default on wireless, but you can enable it.

You can access Unity Edge from a Microsoft Edge or Google Chrome web browser over any TCP/IP network by using the IP address of the HCC2 on that interface.

All the network interfaces listed below (except ETH-3 & ETH-4) support the Unity Edge connection. You may need to update firewall configuration settings to enable access. See section 2.8 Managing Firewall Settings, page 28.

Feature	USB-C Maintenance Port	ETH-1 Ethernet	ETH-2 Ethernet	ETH-3, ETH-4 Embedded Switch	Wi-Fi IEEE 802.11	Cellular Modem
Configurable	No	Yes	Yes	Yes	Yes	Yes
Default Configuration	IP address: 169.254.1.1	Dynamic IP (DHCP)	IP address: 192.168.1.41 Subnet mask: 255.255.255.0	IP address: 192.168.1.33 Subnet mask: 255.255.255.0	Disabled	Disabled
Static IP	Yes	Yes*	Yes	Yes	No	No
Dynamic IP (DCHP)	No	Yes	Yes*	Yes*	Yes	Yes
EPM	Yes	Yes	Yes	No	Yes*	Yes**
Unity Edge	Yes	Yes	Yes	No	Yes*	Yes**
Modbus Editor	Yes	Yes	Yes	No	Yes*	Yes**
ISaGRAF Workbench	No	Yes	Yes	No	Yes*	Yes**
CIP Explicit	No	Yes	Yes	Yes	Yes*	Yes**
SSH / SFTP	Yes	Yes	Yes	No	Yes*	Yes**
NTP Client	No	Yes	Yes	No	Yes*	Yes**
Modbus TCP (502)	No	Yes	Yes	No	Yes*	Yes**
Modbus RTU over TCP (502)	No	Yes	Yes	Yes (Modbus Client only)	Yes*	Yes**
Internet Interface	No	Yes*	Yes*	No	Yes*	Yes*

* Disabled by default.

** Access via the Sensia cellular network requires secure VPN connectivity

2.4 INTERNET INTERFACE SELECTION

If you require remote internet access to the HCC2, pay special attention to the Internet Interface selection in your HCC2 configuration.

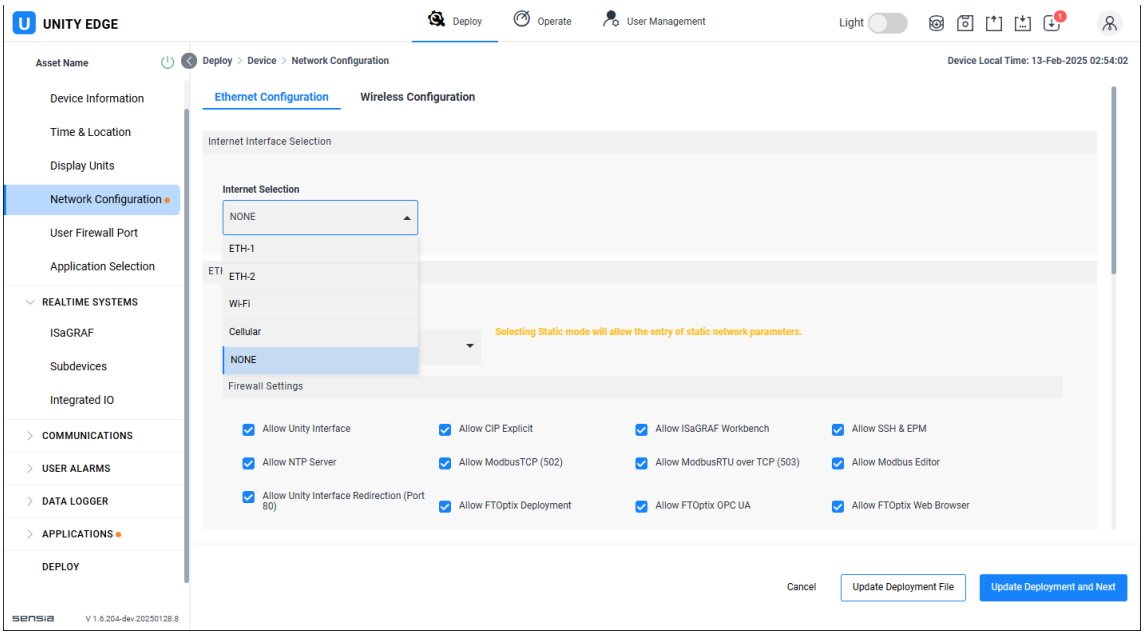
Your Internet Interface selection is the only interface by which the HCC2 can make an external internet connection. Its selection affects how you

- access the HCC2 remotely (to include updating core app files over low-bandwidth networks)
- connect to an internet-based service, such as the Avalon platform or Mender.io site

By default, the Internet Interface Selection is set to NONE.

CAUTION

Be careful when changing your Internet Interface selection. An inadvertent change to this setting could cause you to lose remote access to the HCC2. This is especially important if you are connecting to Unity Edge through the internet. If you lose remote access, you must physically connect to the HCC2 USB-C port to change the Internet Interface selection and restore remote access.

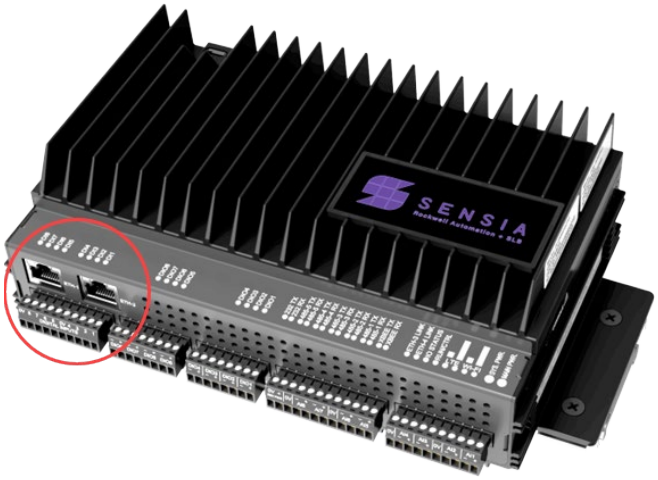


The Internet Interface selection will also affect your default gateway. On the Operate page, you will only see the default gateway for the port that you have selected as the internet interface.

2.5 CONFIGURING AN ETHERNET CONNECTION

2.5.1 Ethernet Ports 1 and 2

ETH-1 and ETH-2 ports are located on the front panel of the HCC2. By default, ETH-1 is configured as DHCP, and ETH-2 has the IP address 192.168.1.41. These are configurable ports.



Note	Consult with network administrators prior to configuring any new Ethernet device on a local or wide area network.

To configure network settings in the Unity Edge interface, perform the following steps:

1. Make the necessary Ethernet cable connections to your HCC2.
2. Select the Deploy menu and navigate to Device > Network Configuration.

3. Select your Ethernet connection properties.

   The configurable items presented in the table are: Enable, Mode, Static IP Address, Static Subnet Mask, Static Default Gateway, Static Primary DNS, and Static Secondary DNS.

   - Enable – Turn the Ethernet port on.
   - Mode – Determines whether the port is to be configured manually (static) or to be automatically configured via a retrieved configuration (dynamic) e.g., using DHCP (Dynamic Host Configuration Protocol).

   If Dynamic mode is selected, all other fields are ignored.

   If Static mode is selected, configure the following fields as needed. Consult your network administrator if you have questions.

   - Static IP Address (values between the dots must be between 0 and 255)
   - Static Subnet Mask
   - Static Default Gateway
   - Static Primary DNS
   - Static Secondary DNS

   You can control which types of communications can use each Ethernet port by selecting/deselecting the "Allow…" checkboxes. See section 2.8, Managing Firewall Settings, page 28, for details.

WARNING

Beware—deselecting the Allow Unity Interface checkbox will block all users from accessing the HCC2 with the associated Ethernet port. Make sure you have another means of connecting to your HCC2 (such as a USB-C cable) before changing this setting. The Network Validation feature in deploy will warn you if it detects a potential communications vulnerability.

4. Click Deploy in the navigation tree on the left side of the screen and use the Deploy wizard to send the network configuration change to the HCC2 device.
5. Launch a new window in your Google Chrome or Microsoft Edge web browser and enter the IP address of your configured Ethernet connection to reconnect with Unity Edge.

Important If you require remote internet access to the HCC2, pay special attention to the Internet Interface selection in your HCC2 configuration. See section 2.4, Internet Interface Selection, page 24, for details.

2.5.2 Ethernet Ports 3 and 4

ETH-3 and ETH-4 ports do not support connection to Unity Edge, but you can configure them as an embedded switch for device and instrument field networks. They share the same IP configuration settings and are DLR-capable. They too are configured from the Deploy > Device > Network Configuration screen (Ethernet Configuration tab).

The enabling of Static mode on ETH-3/ETH-4 is controlled by the state of Dip Switch 2 at power up: (OFF = Static, ON = Dynamic). See Figure 1.2, page 16, or the QRATE HCC2 Hardware User Manual for switch location.

2.6 CONFIGURING A WIRELESS CONNECTION

After you make an initial connection to Unity Edge via the USB-C port or the ETH-1/2 port, you can use the Wi-Fi adapter in the HCC2 to connect to a local Wi-Fi network. The Wi-Fi adapter is disabled by default and can be enabled by updating its configuration settings in Unity Edge.

To connect to Unity Edge via Wi-Fi, ensure that your Windows PC is connected or can route to the Wi-Fi network the HCC2 is connected to.

To configure wireless network settings in the Unity Edge interface, perform the following steps:

1. Ensure there is an available Wi-Fi network and identify its SSID and SSID Password.
2. Select the Deploy menu and navigate to Device > Network Configuration > Wireless Configuration.
3. In the Wi-Fi Client Interface section, toggle the Enable switch to enable the wireless connection.
4. Enter the Wi-Fi network's SSID and SSID Password.
5. Use the "Allow…" checkboxes (section 2.8, Managing Firewall Settings, page 28) to determine the types of communications that can use the wireless network.
6. Click Deploy in the navigation tree on the left side of the screen and use the Deploy wizard to send the network configuration change to the HCC2 device. When making a wireless connection, wait for verification that your wireless connection is complete before proceeding to the next step.
7. Disconnect the cable from your USB-C maintenance port, if applicable.

CAUTION

Store your USB-C cable in a safe place when it is not installed on your HCC2. Maintenance technicians may require its use to connect with your device. If you inadvertently block your access to Unity Edge with configuration controls, the USB-C cable is the only method of restoring access to the software interface.

8. Launch a new window in your Google Chrome or Microsoft Edge web browser and enter the IP address of your configured Wi-Fi connection to reconnect with Unity Edge.

Important If you require remote internet access to the HCC2, pay special attention to the Internet Interface selection in your HCC2 configuration. See section 2.4, Internet Interface Selection, page 24, for details.

2.7 CONFIGURING A CELLULAR MODEM CONNECTION

If you have a wireless HCC2 model, you can use the internal cellular modem for various connections, such as remotely connecting to the Avalon platform or the Mender.io service without a traditional local network infrastructure.

The cellular modem is disabled by default. You can enable it by updating HCC2 configuration settings in Unity Edge.

Before enabling the modem

1. Connect to Unity Edge.
2. Verify that a modem is installed in your device. Select the Operate menu, click the Network Status menu in the navigation tree, and select the Wireless Status tab. If the Installed checkbox under Cellular Modem Interface is checked, a cellular modem is detected.
3. Ensure that an approved LTE antenna is connected, and properly oriented, to obtain the optimum signal. If the signal strength is too low, the modem may not connect.

2.7.1 Enable a Cellular Modem

If you are using a Wireless Logic SIM from Sensia, follow these steps to configure the modem in the Wireless Configuration Deploy page:

1. Select the Deploy menu, click Device > Network Configuration in the navigation tree, and select the Wireless Configuration tab on the screen.
2. In the Cellular Modem Interface settings block, toggle the Enable button to an active status (blue).
3. Complete these network settings:
   - Access Point Name: `eapn1.net`
   - Username: Sensia (optional)
   - Password: Sensia (optional)
   - Pin (optional, not required for use with Sensia-issued SIM cards)
4. If you use cellular connectivity in an area with compromised signal or you rely on the cellular modem for connectivity, you can optimize your chances for signal restoration by enabling a periodic health check of your connection. To enable this feature, complete these settings:
   a. Health Check Site: enter any URL
   b. Heath Check Rate (s): the HCC2 will check your connection and attempt to restore an interrupted connection every 1800 seconds by default. If you desire a check more frequently or less frequently, you can edit this value.

Important If you do not enable this check, a loss of cellular connectivity may result in a permanent loss of connection until you restart the system.

The status message of the Health Check will only show a valid check if the connection has previously gone down. Otherwise it will show “Awaiting.”

5. Configure your required firewall settings by checking all appropriate checkboxes.
6. Click Deploy in the navigation tree on the left side of the screen and use the Deploy wizard to send the network configuration change to the HCC2 device. The initial connection to the cellular network may take 5 minutes or longer to complete.
7. After deployment, click the Operate menu and navigate to the Device > Network Status screen to view the IP address and signal strength for the cellular modem connection. The signal strength is a number between 0 and 100.

Important If you require remote internet access to the HCC2, pay special attention to the Internet Interface selection in your HCC2 configuration. See section 2.4, Internet Interface Selection, page 24, for details.

2.8 MANAGING FIREWALL SETTINGS

You can enable or disable services in Unity Edge for each network interface individually. Some services are available only on certain interfaces.

Firewall Name	Description
Allow Unity Interface	Allow access to the Unity Edge configuration and monitoring interface
Allow CIP Explicit	Allow CIP explicit (as needed) message connections (future)
Allow ISaGRAF Workbench	Allow downloading and online monitoring of an ISaGRAF application using the ISaGRAF Workbench connected to the network interface
Allow SSH and EPM	Allow Secure Shell (SSH) connections through the network interface. SSH connections are generally used by system administrators to connect securely to and interface with a device via command line.

Firewall Name	Description
	Note: The HCC2 Edge Package Manager (EPM) uses SSH to update and manage the HCC2 operating system and application containers. Before using the EPM, ensure that the required network interface allows SSH communications.
Allow NTP Server	Allow the NTP client to synchronize the clock with an external NTP server through the network interface
Allow Modbus TCP (502)	Allow Modbus TCP communications through port 502 of the network interface
Allow Modbus RTU over TCP (503)	Allow Modbus RTU over TCP communications through port 503 of the network interface
Allow Modbus Editor	Allow access to the Modbus Map Editor through the network interface
Allow Unity Interface Redirection (Port 80)	Allow a user to access Unity Edge without explicitly typing `https` in the navigation bar of a browser
Allow FT Optix "…" (Deployment, OPC UA, or Web Browser)	Allow FT Optix functionality for the HCC2 HMI NOTE: FT Optix requires an additional license purchase. See a Sensia representative for further details.

Section 3: Navigating the Unity Edge Interface

3.1 SOFTWARE DASHBOARD

Each time you log into Unity Edge, the Operations Dashboard displays by default. From here, you can monitor device status at a high level and navigate to other menus and tasks.

3.1.1 Navigation Aids

You will make most of your navigational selections via a Menu Bar at the top of the screen and a Navigation Tree at the left side of the page. You can access both elements from any screen in the interface.

The menu bar provides access to several key navigation aids including three main menus that serve as a starting point for accessing nearly all other software selections. See Figure 3.1 below for a summary of navigation elements.

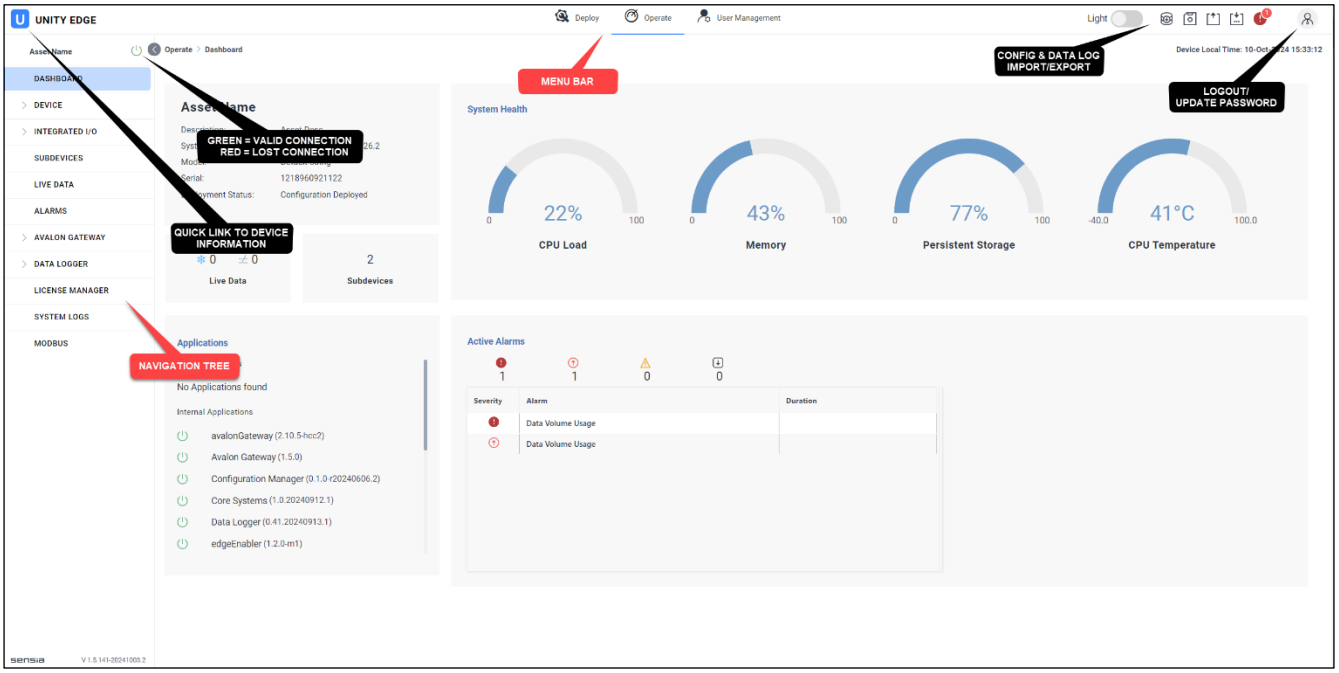


Figure 3.1—Key navigation aids

Item	Description	
Menu Bar	Three main menus—Deploy, Operate and User Management—allow you to quickly navigate to functions that are specific to your role and task.	
Navigation Tree	A secondary menu of assets associated with the main menu selection (Deploy, Operate, or User Management). Assets with nested menus are identified by an Expand icon (›); click the icon to view additional selections.	
Device Information	U	A quick link to Device Information (asset and project identification). Device information is also accessible under Device in the navigation tree.
Connection Status	⏻	A green icon indicates a valid HCC2 connection. When the connection is lost, the icon turns red, and an Information dialog box notifies you of the lost connection.
Display Mode	Light	Toggles the Unity interface between light and dark modes (defaults to system setting)

Item	Description		
Data Log Export		Links to the Data Logger screen containing tools for creating, downloading, and exporting log files to your local drive	
Configuration Import/Export		Exports configuration from device memory to your local drive in a compressed GZ format	
		Imports a saved configuration file from your local drive	
		Exports a cached configuration from your browser to your local drive in a compressed GZ format	
Alarm Status		Identifies the number of active alarms and indicates the highest severity among active alarms (the bell icon changes to denote low, medium, high, and critical severity)	
User Profile		Logged out	Displays login status and the username of the current user when someone is logged in. This profile also supports password changes and logout of Unity Edge. See section 5.1, Roles, page 49, for detailed role descriptions.
		View Only	
		Technician	
		Operator	
		Admin	
		View Only	

3.1.2 Real-time Status Display

The dashboard provides a real-time status overview of a connected HCC2 device (Figure 3.2, page 32). From here, you can

- verify the operating system version
- check system health diagnostics
- check live data status
- view active alarms by severity
- check the number of subdevices configured
- view a list of applications loaded and verify the install version of each

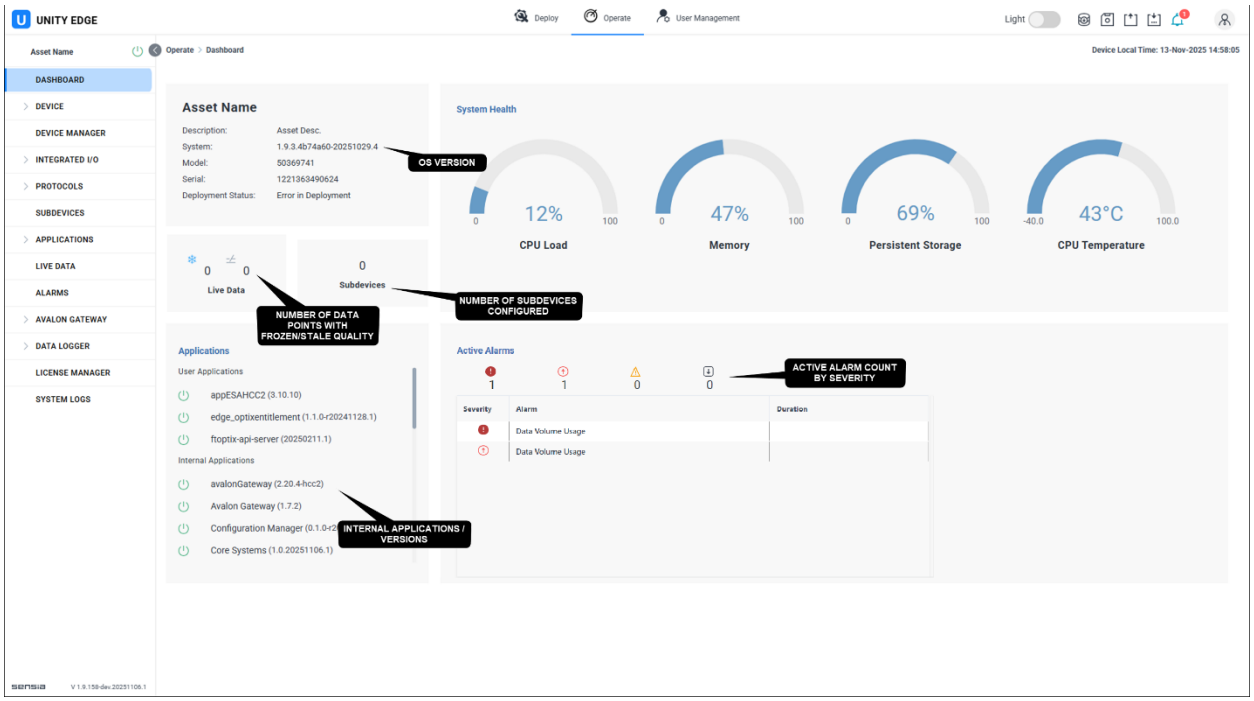


Figure 3.2—Key status information

3.2 OPERATE MENU

The Operate menu (Figure 3.3) presents the current HCC2 measurements, statuses, alarms, and statistics. The data are mostly read-only, designed to give an operator an overview of the system.

Actionable functions, such as Reset IO System in the screen below, appear as rectangular buttons.

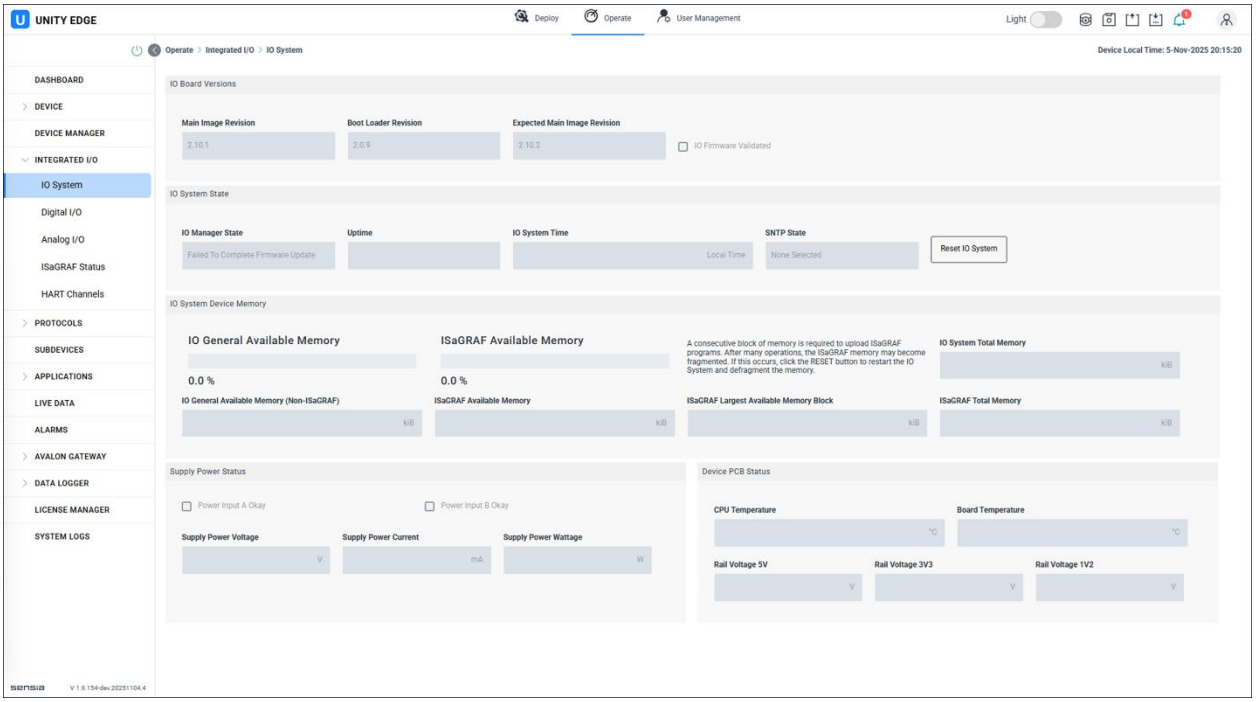


Figure 3.3—Operate Menu

Operate Menu Screen	Description	Actions Supported
Dashboard	Displays basic information about the connected HCC2 device. It includes the firmware version, model and serial numbers, live data status, subdevice count, and a list of installed applications, and active alarms. It monitors in percentages the CPU load, system memory, and persistent storage currently in use. It displays the CPU temperature.	
Device	The child nodes display OS and device hardware details; CPU core temperatures; usage statistics; time zone; latitude and longitude; ethernet and wireless status and address.	Sync to computer time
Integrated I/O	The child nodes provide an overview of the I/O board status; details about the digital and analog inputs and outputs; the status of any connected ISaGRAF resources; details about HART protocol channels.	Reset I/O system
Subdevices	Lists connected subdevices, their connection status, and statistics	
Live Data	Displays the data quality and current value of all system and custom data points. A toggle allows you to show/hide out-of-service data points.	
Alarms	Displays details about alarms and their history	Acknowledge all Clear all Export in CSV Get (history) from device
Applications	Displays data used to manage and monitor HCC2 edge applications	
Avalon Gateway	Allows you to provision the HCC2 device to the Avalon framework and monitor HCC2 status and file transfer status	Provision HCC2 to Avalon Unpair HCC2 from Avalon assets
Data Logger	Displays statistics for event/alarm, data point, and trend logs	Export and download logs
License Manager	Displays name, status, type, and expiration date of all licenses granted	Apply license Get license request (use only on request from Sensia)
System Logs	Displays log messages and errors	Check archived logs Export Refresh
Modbus	Displays assigned ports and configuration details for Modbus servers and clients	
MQTT	Displays broker connection status and statistics for MQTT communications	
OPC UA Server	Displays status and statistics for OPC UA Server.	Manage Trusted Peer Certificates for deployed OPC UA Server applications

3.3 DEPLOY MENU

Administrators and technicians use the Deploy menu functions (Figure 3.4) to configure the HCC2 OS, applications, communication channels, subdevices, alarms, and protocols.

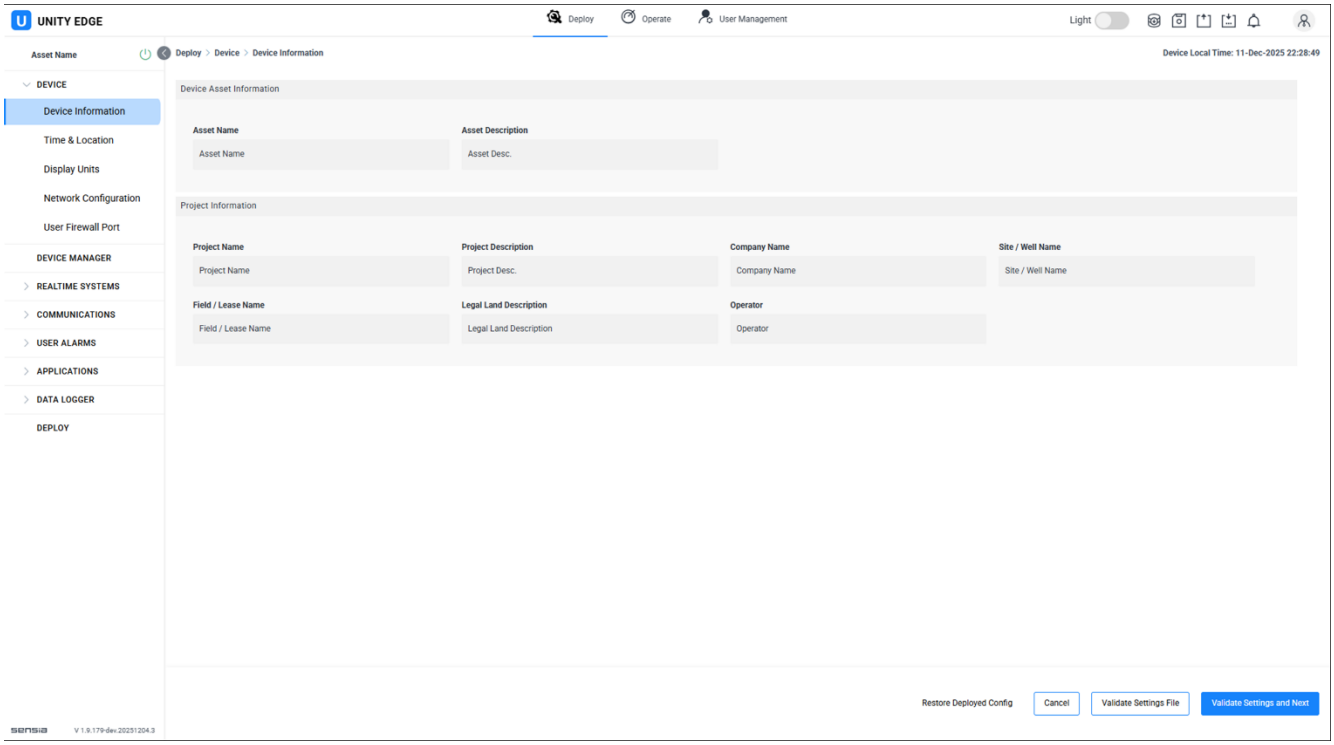


Figure 3.4—Deploy Menu

Deploy Menu Screen	Description	
Device	Device Information	Specify the details about the project your HCC2 device is monitoring. Specify the time source and geographic location; display units for different measurements; and Ethernet and wireless connections.
	Time & Location	
	Display Units	
	Network Configuration	
	User Firewall Port	
	Application Selection	Select edge applications from a dropdown list to run in the OS. Applications will not appear in this list until they are loaded onto the HCC2 using the Edge Package Management tool. When an application is enabled in this list, any associated Deploy and Operate pages are available to you.
Realtime Systems	ISaGRAF	Upload ISaGRAF resource definition files from which you can select variables to map to custom or selected data points. These definition files are created during the build process in the ISaGRAF Workbench software.

Deploy Menu Screen	Description	
	Subdevices	Select, add, and configure subdevices including select Flex IO and Powerflex Drives.
	Integrated IO	Specify values for analog and digital channels
Communications	Port Configuration	Specify values for serial and server/client TCP ports
	Protocols: Modbus	Contains the definitions of your Modbus client and server instances and displays the current in-use client and server protocol definition files. In addition to adding Modbus protocol definition files, you can also launch the Modbus Protocol Map Editor from the Protocols > Modbus screen.
	Protocols: MQTT	Set up Group ID, Edge Node ID for Sparkplug B compliance. Enable broker connections and configure broker communications. Navigate a list of available applications and choose the data points you want to transmit using MQTT communications.
	Protocols: OPC UA Server	Enable OPC UA Server protocol and configure engineering unit for address space. Configure security and authentication modes. Select functionalities and applications to expose to OPC UA address space.
User Alarms	Alarm Configuration	Define the parameters (display name, LoLo, Lo, Hi, HiHi, etc.) of user-defined alarm data points.
Data Logger	User Log Configuration	Configure user logs for historizing data point data. This menu allows you to select data points to be logged, assign a logging priority to each data point (which determines log frequency), and choose the type of value you wish to record (instantaneous, min, max, or average). Data stored in the log files created by Data Logger can be extracted and exported for analysis using a Data Logger Extractor utility that is installed separately on your PC or laptop.
	Logging Priority Configuration	Configure logging priority periods.
Applications	Custom Applications configuration	Configure applications enabled in the Application Selection menu.
Deploy	Launches the Deploy wizard used to update the browser configuration and deploy it to the HCC2 device	

Note Deploy is both the name of a main menu (a tab at the top of the interface) and the name of a wizard used to commit configuration changes to the HCC2 (displayed in the navigation tree on the left side of the interface screen).

3.3.1 Understanding Deployment of Configuration Changes

Updating the HCC2 configuration is a two-step process.

1. First, make the required change to an HCC2 setting, which is saved to a deployment file.
   - A green banner notification will appear at the top of the screen, confirming “Deployment file has been updated successfully.”
   - An orange dot will appear in the navigation tree to indicate the location of changes made.
2. Then use the Deploy wizard in the navigation tree on the left (item 2, Figure 3.5) to apply the changes to the HCC2. Until this step is complete, the HCC2 configuration will be unchanged.

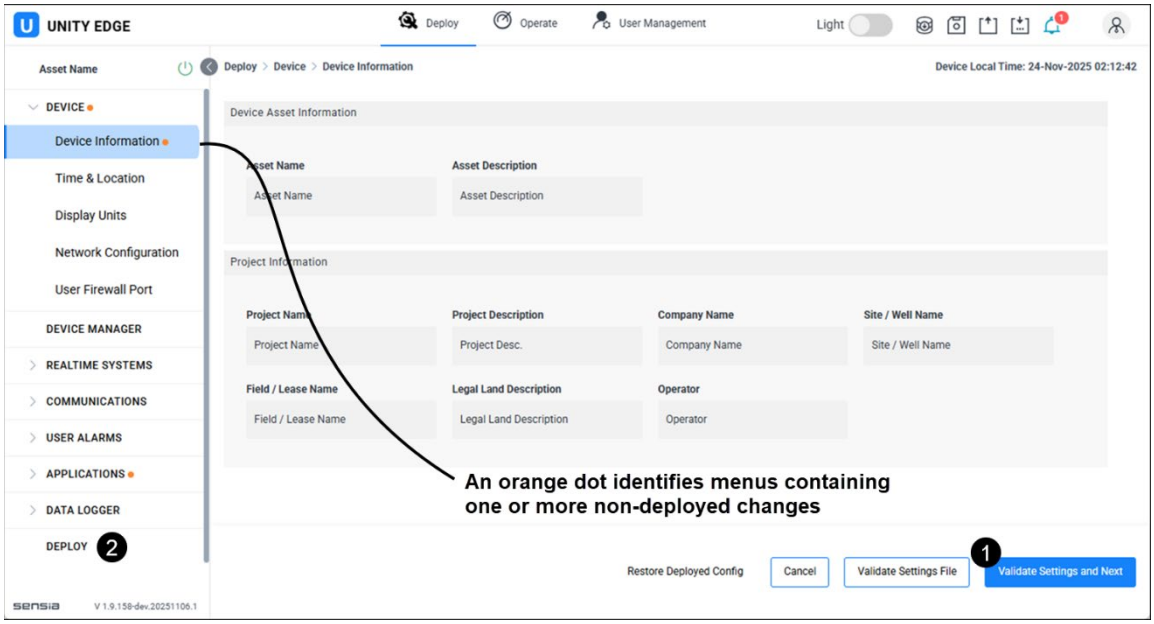


Figure 3.5—Two-step deployment process

3. When you initiate a change ***and navigate away from the screen***, the HCC2 will automatically attempt to validate your configuration settings and save them as long as they do not conflict with any validation rules.
4. However, you can perform your own integrity check before you leave the screen by clicking the Validate Settings button. This may be useful if you are changing multiple settings or values on a screen or are unsure if your change is allowed.

Note	In previous versions of Unity Edge, these buttons for initiating configuration changes were labeled Update Deployment File and Update Deployment and Next.

Validate Settings

If an attempted configuration change violates the rules established for HCC2, you will receive an error message, the source of error will be highlighted, and you will be unable to navigate to another screen until the rule violation is resolved.

To proceed,

1. Note the source of the error identified in the error message.
2. Attempt to resolve the issue.
3. Click Validate Settings File.

Click the Validate Settings and Next button to update the browser configuration with your changes and advance to the next menu screen.

CAUTION

You can overwrite changes made to the deployment file up to the point of deployment, but you cannot undo configuration changes once they are deployed. To save a copy of a configuration file for use in restoring a prior configuration, export the configuration before making changes. See section 6.15.1 Export Configuration from Device, page 76, for details.

Reverse a Setting Change

Once you make a change to a setting, you can opt out of deploying it to the HCC2 two ways.

1. Before you leave the screen, you can click Cancel at the bottom of the screen. This function works only if you act before leaving the screen. It has no effect after you navigate away from the screen where you made the change.
2. Press the Restore Deployed Config button at the bottom of the screen to delete any changes made since the last deployment.

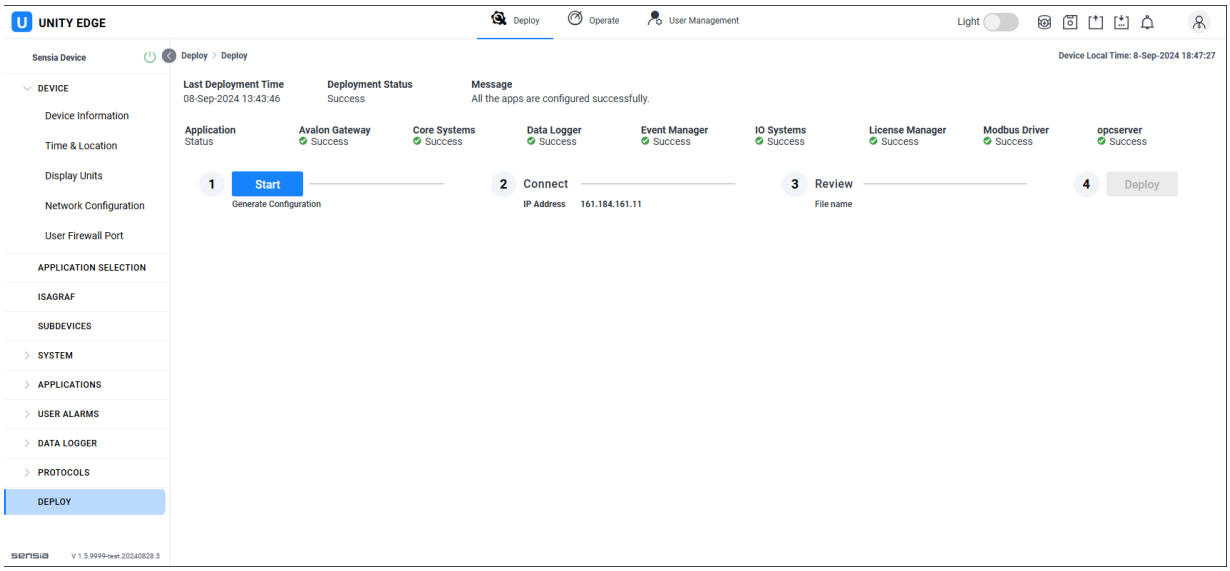
3.3.2 Deploy Your Changes

Deploying your changes is the final step in configuring your HCC2.

Important Once you deploy the configuration, your current configuration will be overwritten. Back up your configuration before deploying changes if required.

When you are satisfied with your configuration, deploy it as follows:

1. Press Deploy in the navigation tree to open a wizard as shown below.

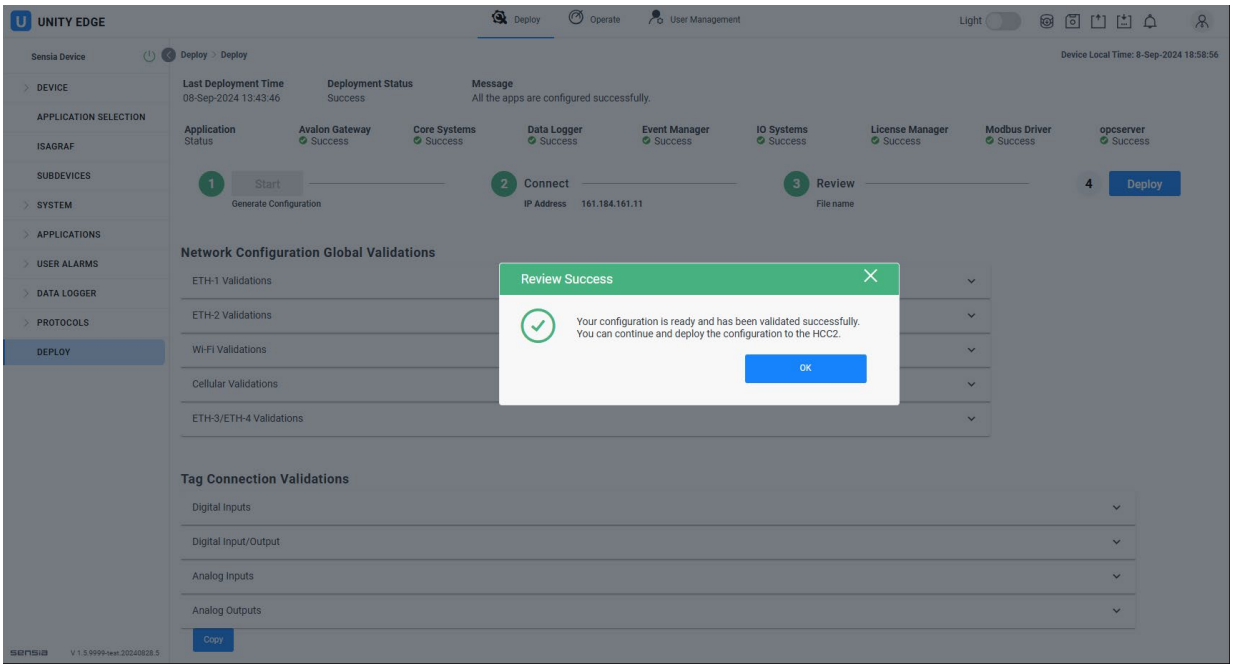


2. Press the blue Start button to generate your configuration file and initiate a validation of your network and data point connection changes.

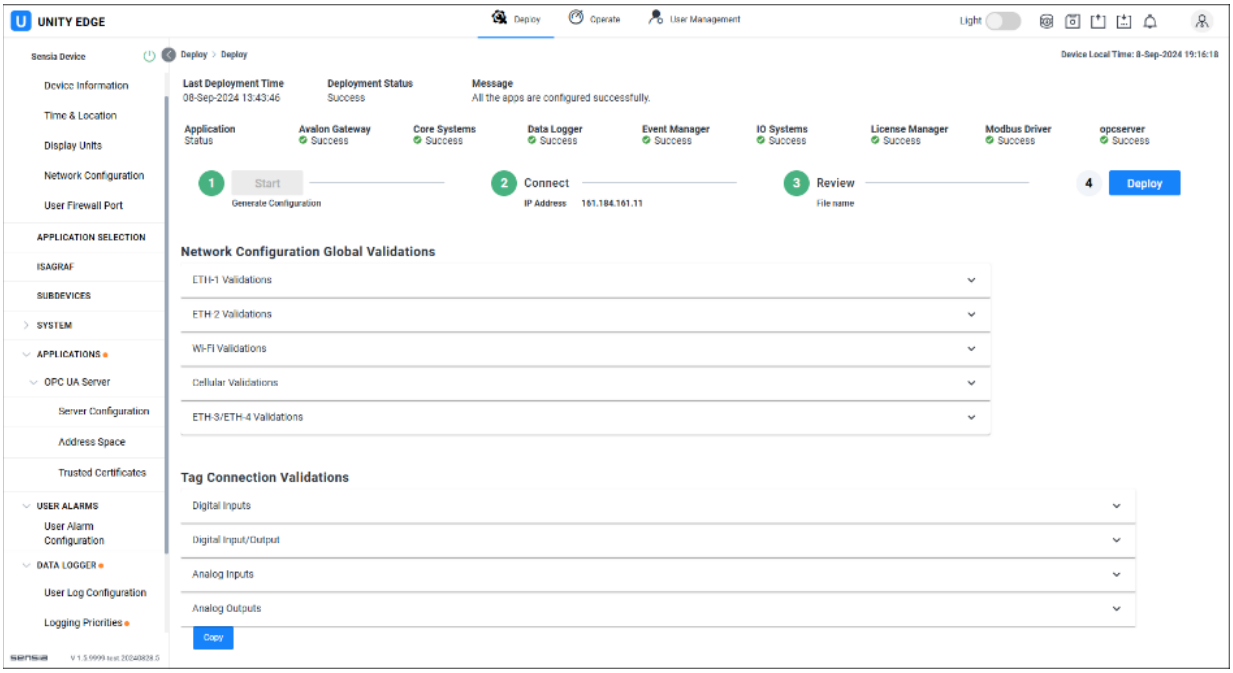
   A dialog box will identify the changes about to be processed.

3. Click OK to acknowledge the validation results in a popup window. If no warnings are present, a Review Success popup will appear.

If warnings are present, a validation report will provide details for troubleshooting. See section 3.3.3, Network Configuration Global Validations, page 38, and 3.3.4, Data Point Connection Validations, page 39.



4. Click the blue Deploy button on the right to overwrite your HCC2 configuration.



3.3.3 Network Configuration Global Validations

Since networking and maintaining connectivity both to and from the HCC2 is critical, the built-in validator (Figure 3.6) checks for changes to your network settings. It will give warnings if it detects settings that could affect your connectivity. It will also indicate warning severity to alert you to issues that could block your connectivity – for example, if you are connecting to the HCC2 remotely and you inadvertently change your Internet Interface connection setting. The validation report contains comprehensive information on the changes for your review.

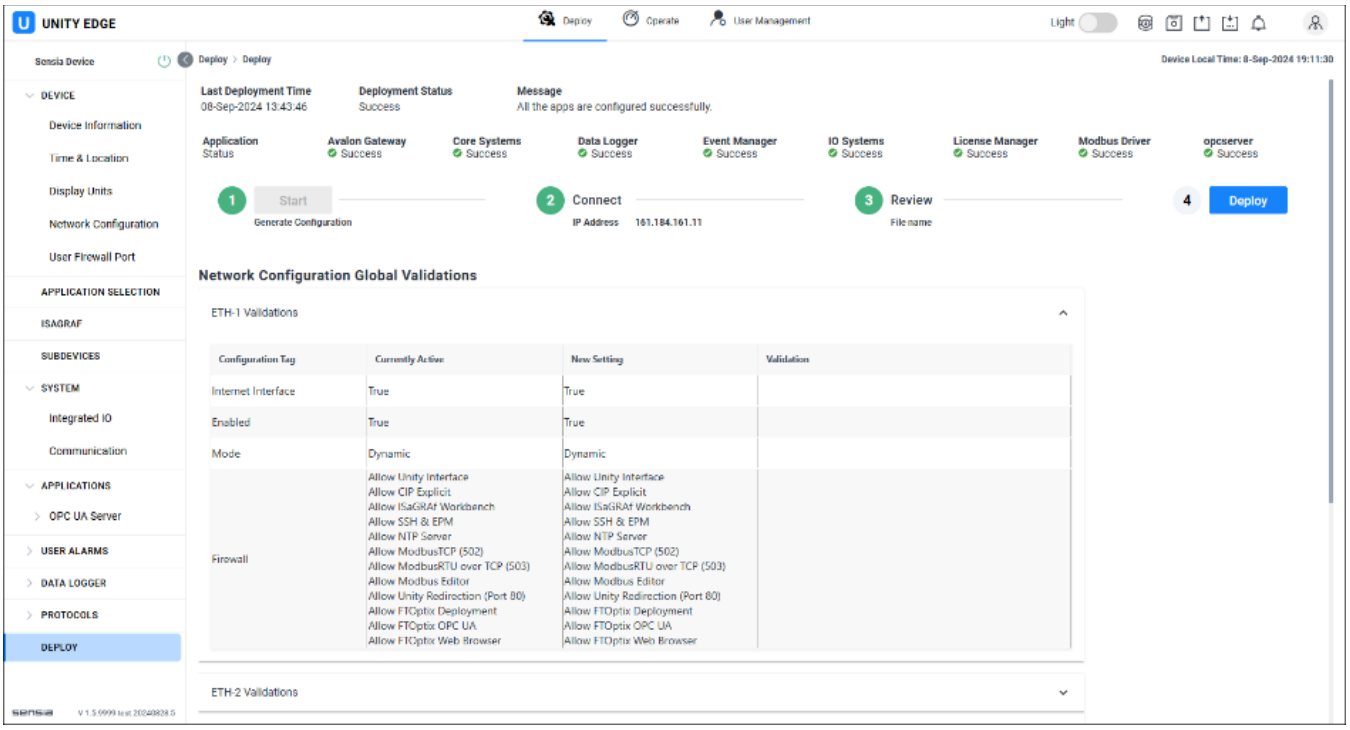


Figure 3.6—Network Configuration Global Validations report

3.3.4 Data Point Connection Validations

The data point connection validator (Figure 3.7) examines all of your data points and associated mappings (e.g., Modbus, ISaGRAF, IO, etc.) for data type compatibility, correct mapping. So, a data point that is relying on data from elsewhere in the system, but is not mapped to anything, will be flagged as a potential mapping error. Review the mapping report to make sure that all mappings are as expected.

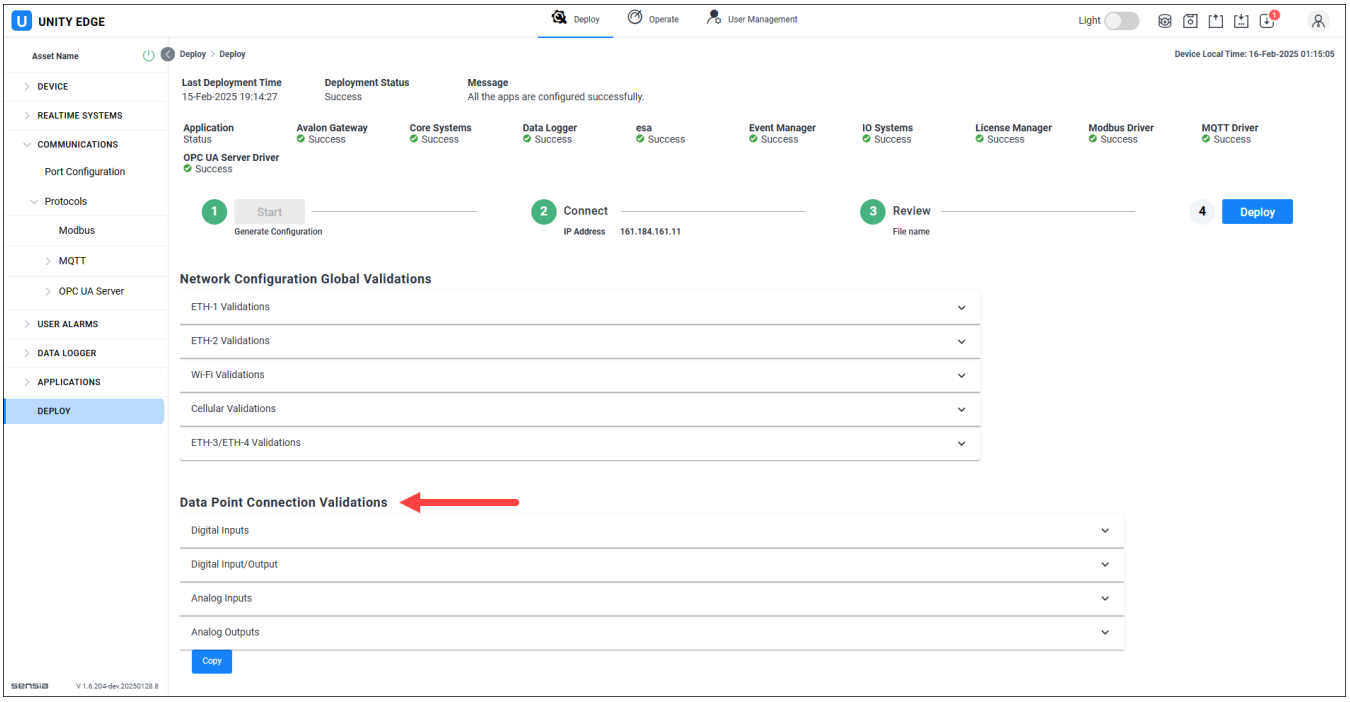


Figure 3.7—Data Point Connection Validations report

For more information, see Section 6: Configuring the HCC2 Device, page 52.

Important In the Unity Edge interface and in this manual, the term "tag" is replaced with "data point." Please note that the measurements and values referenced by these terms *have not* changed. The term was changed only to address a concern that the widespread association of "tag" with specific programming rules may cause confusion when it is used to describe values in HCC2.

In the HCC2, a “data point” (formerly “tag”) is a value originating from a physical measurement, an internal calculation, system diagnostics, an external device, or other sources, and may be simple or a more complex group of values. The state of a data point is updated within the system by sending a message to all consumers of that data point, and it can only be updated by the source creating it. For example, changing the state of a remote IO involves one data point to observe the current state of the IO and another data point to request a change of state from the value's owner.

3.4 USER MANAGEMENT MENU

The User Management menu (Figure 3.8) allows an administrator to add, modify, or delete users, specify their roles, and enter passwords.

For more information, see Section 5: Managing Users and Permissions, page 49.

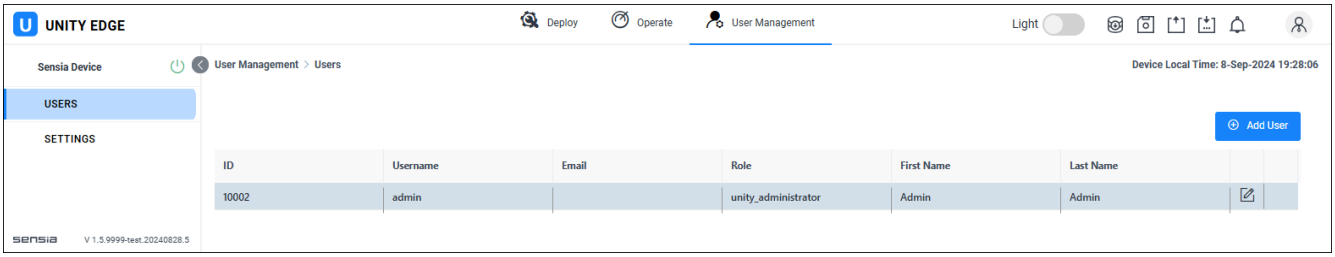


Figure 3.8—User Management Menu

Section 4: Updating and Managing HCC2 Software

This section describes the tools and processes for updating and managing your HCC2 software.

4.1 USING THE HCC2 EDGE PACKAGE MANAGER (EPM)

Install the Edge Package Manager (EPM) software utility (Figure 4.1) on your Windows PC or laptop to load operating system and application updates into the HCC2. For installation details, see section 1.3.3, Software Downloads, page 12.

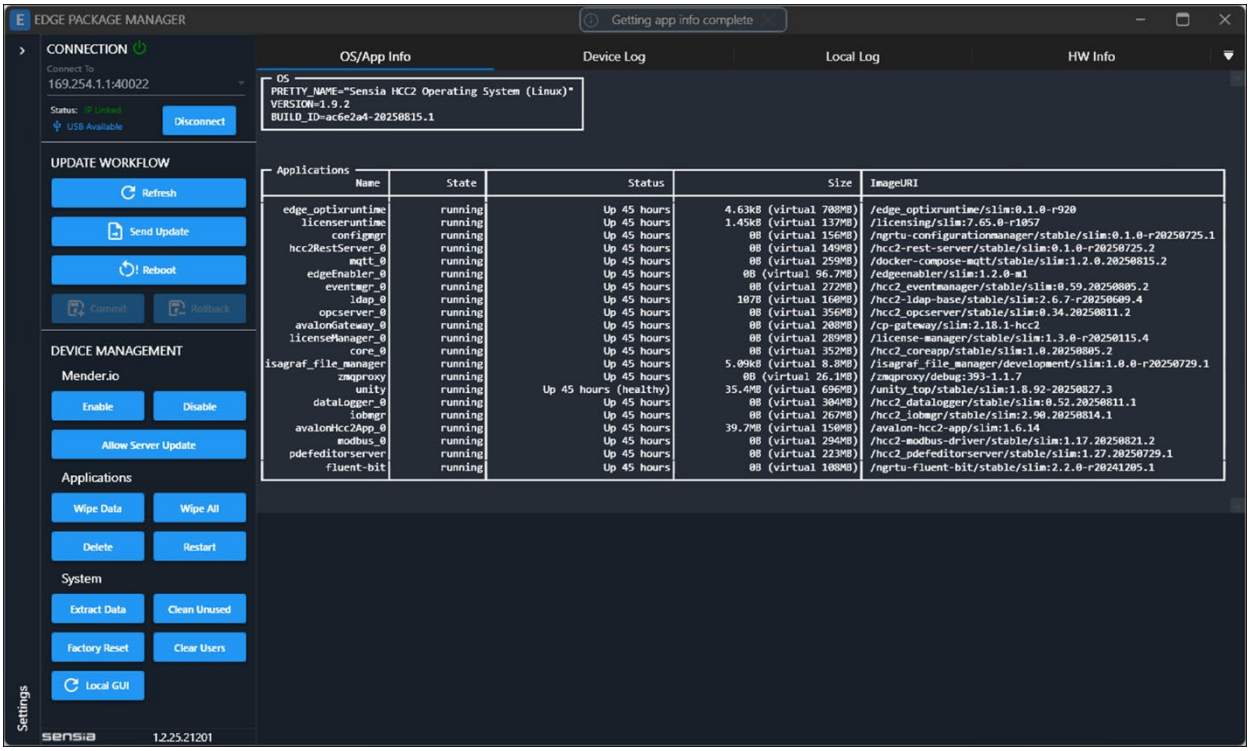


Figure 4.1—Edge Package Manager utility

From the EPM, you can

- connect to an HCC2 via Ethernet, Wi-Fi, local USB-C connection or cellular (through secure VPN)
- identify by version number the OS and applications currently loaded in the HCC2
- update the OS and/or the applications loaded to an HCC2
- install a new application on an HCC2
- remove an application from an HCC2 (with a special removal mender file)
- refresh or reboot the HCC2 connection
- roll back to the last OS loaded into an HCC2
- restart one or more user-specified applications
- extract data
- remove unused applications from the HCC2
- reset the HCC2 to factory settings
- clear users
- restart the browser that displays a local GUI
- enable and disable connection to Mender.io (see section 4.5.1 for details)

The EPM allows you to update the OS and app containers running on the device. When OS files and apps are released as a package, you should perform the uploads sequentially. You can also install OS and application updates independently as needed.

To update only portions of the OS or app container that have changed between version installations, see section 4.4 for time-saving and space-saving download options.

CAUTION

Application updates are developed for use with specific OS versions. If updating the OS and application containers separately, make sure that OS and app versions are compatible. See software release notes for details.

4.1.1 User Authentication

Use your Unity Edge login credentials (Section 5: Managing Users and Permissions, page 49) to log into the EPM.

Note As with Unity Edge user authentication, you can log into EPM initially using the default username and password. When you have updated your Unity Edge password for your default Admin account, you will then use your unique password for EPM login.

4.1.2 Network Requirements

Before you perform an OS or app upload,

1. Determine the IP address of your selected connection port.
   - ETH-1 is configured for DHCP protocol (default).
   - ETH-2: 192.168.1.41 (default)
   - USB-C: 169.254.1.1 (default)
   - Wi-Fi/Cellular will be based on your specific configuration

Important The EPM does not connect over Ethernet communication port ETH-3 or ETH-4.

2. Verify that the required network interface allows SSH communications. See section 2.8, Managing Firewall Settings, page 28.

4.2 UPDATING THE HCC2 OPERATING SYSTEM WITH EPM

To update the operating system, perform the following steps:

1. Navigate to the Sensia Azure Storage Explorer using the instructions in this knowledge article:

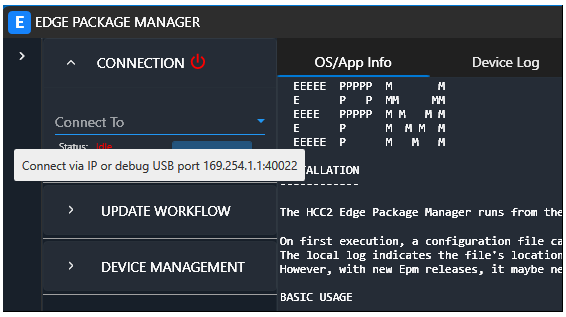
   https://sensiacustomerserviceportal.powerappsportals.com/knowledgebase/article/KA-04676/en-us

2. Download the EPM file and the OS file from the Azure Storage Explorer.

Important If your network is prone to high-latency issues or expensive-bandwidth connections, review section 4.4.1, Delta OS Update, page 44, before choosing an update method. Your choice will determine which OS install file you will download from Azure.

3. Run the EPM program and connect to the HCC2 as follows:
   - If using an IP connection, enter the HCC2 IP address in the Connect To dropdown menu at the top of the screen and click Connect.

- If using the USB-C port, the USB will appear. Select the IP address of the USB in the dropdown menu and click Connect. Hover over the Connect To field to see the USB IP address in the tooltip, as shown. You can see the status of the USB port in the Status field under Connection.



4. Click Update Workflow to expand the menu and view the grid of blue buttons.
5. When the Connection Status indicator at the top of the screen displays green, click Send Update and select the OS file (a signed.mender file) from your Downloads folder (or other location used to store the OS file after download).
6. Monitor the progress bars until the upload is complete.
7. Click Reboot to reboot the HCC2. While the reboot is in process
   - Your connection status at the top of the EPM window will change to red to indicate a disconnected status.
   - If you are connected to Unity, you will receive a momentary notification that your connection is lost during reboot.
8. Click Connect to reconnect to the HCC2.
9. If you are satisfied that the update worked correctly, click Commit to activate the new OS image. This stores it in the HCC2 as the active OS, ensuring it loads with subsequent reboots.

CAUTION

If you DO NOT click Commit, the HCC2 loads the previous OS image on the next reboot. See also OS Rollback for more details on OS restoration methods.

4.2.1 OS Rollback

The HCC2's OS management system allows you to load a new OS without interrupting the function of the device. The HCC2 stores two copies of the operating system: an *active* version and an *inactive* version. When you boot the HCC2, the *active* version loads and runs. When a new OS is loaded with the EPM, this *active* version is copied to the *inactive* space and the bootloader loads the new image on the next boot, making it the new *active* version.

If, after rebooting your device to load a new OS, you are not satisfied with the OS, you can restore the previous OS by selecting Rollback from the EPM menu.

As a security measure, if the device is completely inaccessible (you cannot select the Rollback button), you can force a rollback to a previous OS image simply by power cycling the unit without committing the new image.

4.3 UPDATING HCC2 APPLICATIONS WITH EPM

The downloadable image used to install updates to HCC2 applications may contain updates for one or many applications. A bundle of applications is typically used when a number of related applications are available for use. The user installation process is the same, regardless of whether apps are bundled or packaged individually.

CAUTION
Immediately after the new application image loads, the HCC2 restarts all applications. Be prepared for disruptions to your work.

CAUTION
An app bundle update may change the IO board manager firmware. If you have critical control applications that could be interrupted, be sure to check the release notes for iobmgr firmware details before loading a new app bundle.

Important If your network is prone to high-latency issues or expensive-bandwidth connections, review section 4.4.2 Online App Bundle (Container Registry) Update, page 45, before choosing an update method. Your choice will determine which OS install file you will download from Azure.

To load an application file or bundle:

1. Download the file or bundle from the Sensia Azure Storage Explorer using the instructions in this knowledge article:

   https://sensiacustomerserviceportal.powerappsportals.com/knowledgebase/article/KA-04676/en-us

2. Open the EPM utility and connect to the HCC2 as follows:
   - If using an IP connection, enter the HCC2 IP address in the dropdown menu at the top of the screen and click Connect.
   - If using the USB-C port, the USB will appear as a selection. Select the port's IP address in the dropdown menu and click Connect.
3. If the Update Workflow menu is closed, click the menu title to expand it and view the grid of blue buttons.
4. When the Connection Status indicator at the top of the screen displays green, click Send Update and select the application/bundle file from your local Downloads folder (or other location used to store the application file after download) to load the application file or bundle.
5. Monitor the progress bars until the upload is complete. The HCC2 will immediately restart all applications.
6. Wait at least 1 minute and then reconnect to Unity Edge.

4.4 OS AND APP BUNDLE UPDATES FOR LOW-BANDWIDTH NETWORKS

Effective with Sensia Operating System 1.8, HCC2 users with a high-latency or expensive-bandwidth connection can update their OS and/or online application container registry bundle using smaller file sizes for faster processing.

4.4.1 Delta OS Update

A delta OS update file updates only the parts of the OS that have changed since the installed version was released, which reduces the size of the upload as much as 90%.

You can find these delta files in the same Microsoft Azure Storage Explorer repository containing the full-size OS installation files (see section 1.3.3, Software Downloads, page 12). Each delta install file is labeled with a "delta" prefix and a beginning and ending version (delta-XXX to YYY.mender).

To update your OS version, select the filename that specifies your current version and the version you wish to install from the Downloads list in Azure Storage Explorer, and follow the instructions provided in section 4.3, Updating HCC2 Applications with EPM, page 43.

4.4.2 Online App Bundle (Container Registry) Update

HCC2 users who found application bundle updates to be difficult due to high latency or expensive bandwidth connections over a slow network may benefit from a new online container registry update method.

To use this update method, your HCC2 must have an active internet connection. An online mender file, only a few megabytes in size, is sent to the HCC2, providing instructions for updating the container layers that have changed since the bundle version was installed on the device. It then updates these layers through Sensia's container registry.

You can find this registry update file in the same Microsoft Azure Storage Explorer repository containing the full app bundle install files (see section 1.3.3, Software Downloads, page 12). The online bundle is identified as the "online only bundle installer."

Users with access to mender.io can use this server to remotely update the app bundles on one or more devices, provided that all devices have an active internet connection.

All other users can use EPM to upload the online bundle installer to their HCC2, using the same procedure they use to upload full app bundles. The only difference is the required active internet connection for uploading the "online only" bundle installer.

4.5 DEVICE MANAGEMENT WITH EPM

The device management features of the EPM are not part of the usual workflow, and they are generally used sparingly or in exceptional circumstances.

If the Device Management menu is closed, click the menu title to expand it and view the grid of blue buttons defined below.

4.5.1 Mender.io

Enable Mender.io and Disable Mender.io

Enable Mender.io and Disable Mender.io enables and disables HCC2 remote management via the Sensia Mender Management Server. A Mender Management server can be on-premise or cloud-based. By default, the EPM tool's "Enable Mender.io" button will try to connect to Sensia's Mender.io Cloud instance and enable Sensia to remotely manage the device. You will need the serial number of your HCC2 to identify your unit in Mender.io.

Allow Server Update

The Allow Server Update button allows you to change the Mender server from the Sensia-managed instance to a custom one of your choosing. If you are interested, contact your technical representative for instructions on how to set up your own custom Mender instance.

4.5.2 Applications

Wipe Data

Before performing a Wipe Data function, export your configuration.

Wipe Data will delete all volumes in the containers, causing most settings to be reset to defaults, and your HCC2 will need to be reconfigured. Wipe Data will not delete any critical files (licenses, logs, etc.).

This may be necessary when updating application bundles that are not compatible, to ensure that all data on deployment are valid. Check the release notes accompanying your application installation for application compatibility details.

Wipe All

Wipe All deletes data, as Wipe Data does, and removes all applications from the HCC2.

Use this button only if you want to remove both data and apps simultaneously (for example, when reconfiguring an HCC2 for a different purpose). **Not recommended during normal workflow**.

Delete

The Delete button allows the user to selectively delete applications from the HCC2.

This is useful when developing custom apps using the SDK, or to remove applications (e.g., protocols) that are no longer in use, freeing up system resources. Be careful to avoid deleting any core applications, which can create unexpected vulnerabilities and, in some cases, render the HCC2 inoperable.

Restart

The Restart button allows you to selectively restart applications on the HCC2. Click Restart to access a list of all application containers installed. Then, select the container for the application you want to restart and click Restart at the bottom of the list.

This is useful if you have an application that has crashed or not behaving as expected but you don't want to restart the HCC2.

4.5.3 System

Extract Data

Extract Data will retrieve certain data from the applications running in the HCC2. This data can be sent to Sensia support to help diagnose any issues in the HCC2.

This is useful when troubleshooting. See Appendix B, page B-1, for more information.

Clean Unused

Clean Unused will remove unused/old containers from the HCC2.

If you make frequent upgrades to your HCC2, or install many additional applications, there may be some unused containers in the HCC2 file system. This feature will remove those unused containers and free up space on the HCC2.

Clear Users

The Clear Users button removes all users from the system and resets user login to the default Admin account and password. This is useful if you lose all access to the HCC2 or there are issues with logging in.

Factory Reset

Factory Reset restores the HCC2 to factory settings. All containers are removed, along with any user-specific data.

This is recommended only for extraordinary circumstances—for example, when preparing to transfer an HCC2 to another user or repurposing it.

To perform the reset:

1. Back up any data/configuration you wish to keep.
2. From the EPM, connect to the HCC2.
3. Press Factory Reset in the EPM interface.

Local GUI

The Local GUI button restarts the web browser that runs on the HCC2 operating system to display information in an HMI (by default, FactoryTalk Optix). This is useful if the HMI crashes for any reason, or if you develop a custom HMI application that uses the same web server as FactoryTalk Optix.

4.6 OTHER EPM FUNCTIONALITY

The EPM interface contains several tabbed displays for monitoring operations as well as a Settings tab for optimizing your EPM display and exporting logs needed for troubleshooting.

4.6.1 Tabbed Window Information

Below is a summary of the information provided in four tabs along the top of the EPM interface.

Tab	Description
OS/APP Info	Displays a list of current Operating System and Applications on the HCC2 and is a useful spot check for assessing the health of your applications. Refreshing will display the up-to-date state of each container and how long it has been running.
Device Log	Shows logs from the HCC2 related to EPM functionality and is useful for troubleshooting an issue.
Local Log	Shows the log of the operations you have performed, interacting with the HCC2 using the EPM.
HW Info	Shows detailed info on HCC2 hardware that can help with debugging if the HCC2 has an issue that may be related to hardware.

4.6.2 EPM Settings

To access the Settings tab, click the thin vertical bar along the left edge of the interface (note the Settings label in the lower left corner, Figure 4.2). The window will expand to allow full view of the Settings controls.

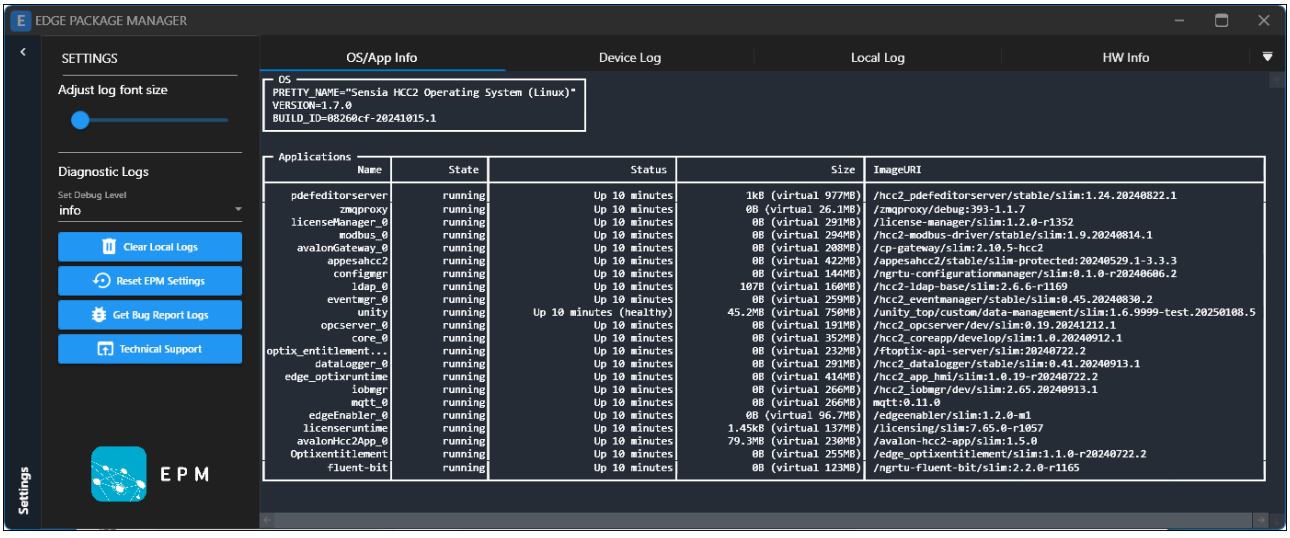


Figure 4.2—Edge Package Manager settings

From the Settings panel, you can

- adjust the font size for the EPM display using the slider bar
- set the debug level for diagnostic logs
- clear logs

- reset EPM settings (may resolve timeout issues that can occur when upgrading from a previous version of EPM)
- download a zip file with runtime information for submitting with a bug report if needed
- access Sensia Technical Support (use this link to report a bug)

4.7 USING THE DATA LOG EXTRACTOR

Install the Data Log Extractor utility on your Windows PC or laptop for use in extracting data from HCC2 log files and exporting it in CSV format for analysis and graphing.

To download the Data Log Extractor utility

1. Visit URL https://www.sensiaglobal.com/Technical-Support.
2. Click Customer Support Portal Access in the top right corner of the screen and search for RTU and Edge Devices Firmware and Software Download Procedure. Or use this link to navigate to the procedure: Knowledge Article KA-04676.
3. Follow the procedure to connect to the Microsoft Azure Storage Explorer repository and download the extractor utility installer.

The Data Log Extractor (Figure 4.3, page 48) is a setup wizard that walks you through the steps of opening a log file, defining export parameters, and exporting the data to an output file.

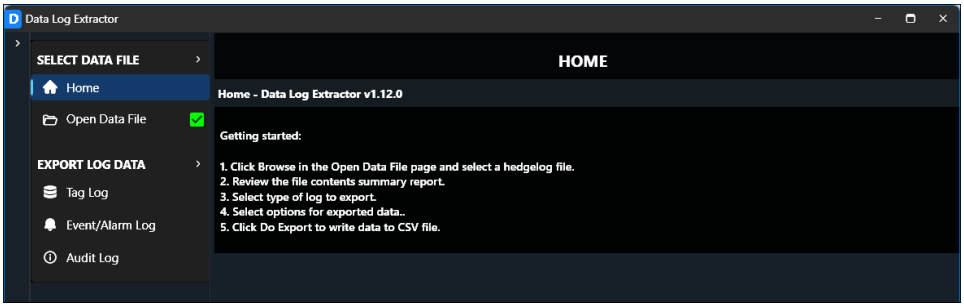


Figure 4.3—Data Log Extractor wizard

The HCC2 stores high-resolution data points in a data log file with a .hedgelog file extension. The Data Log Extractor allows you to finely customize and refine your data exports through multiple filter selections and to export your data in a synchronized time series list. This output file is a .csv file that can be edited in a text editor such as Notepad or imported into a spreadsheet for analysis and charting.

From the Data Log Extractor, you can customize your log export size and content by selecting

- start and end times for your export
- log interval period
- the applications from which you want data logs
- data groupings (columns) to include in your export (as defined by your application and reporting period selection

You can also choose export preferences such as

- the units system in which you want your logs displayed
- the header rows (data type, max size, measurement category, unit label, etc.) to include
- the location used for storing the output .csv file

Refer to section 6.13, Configuring User Logs through Data Logger, page 67, for the procedures.

Section 5: Managing Users and Permissions

This section describes the software interface settings you use to add new users and control user access levels.

For initial login information, see

- section 2.1, First-Time Connection to Unity Edge (USB-C), page 17
- section 2.1.3, Enroll a Web Server Certificate (Optional), page 20
- section 2.2, First-Time Connection to Unity Edge (Ethernet), page 22

Important At initial connection, you have full administrator access to all configurable settings. At least one user of each device must retain this administrative access for security management.

The administrator controls access levels for all other users by assigning each user to a specific role. Access to screens and configurable settings will be role-specific.

5.1 ROLES

By default, the HCC2 supports four access levels listed below in the order of highest to lowest restriction:

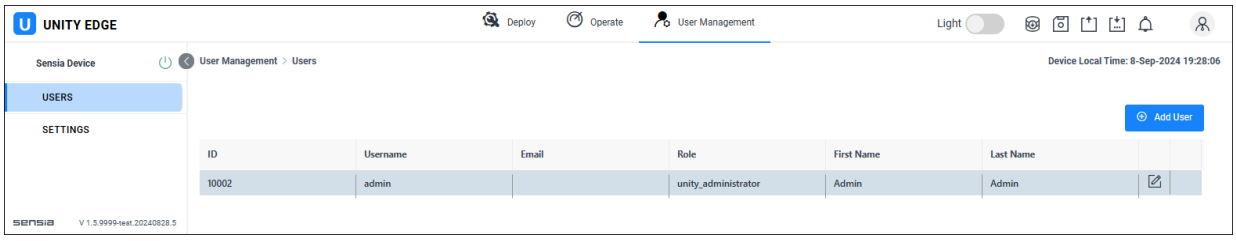
Access Level	Permissions
View Only	Read-only access to live data and diagnostics in the Operate menu tab
Operator	Read-only access to the Deploy menu tab and full access to the Operate menu tab. This is for users involved in day-to-day use of the system, who may need to view configuration settings but not modify them.
Technician	Full access to Deploy and Operate menu tabs. This is the standard level for users who are responsible for maintaining and configuring the device.
Administrator	Technician access plus access to the User Management menu tab for configuring security. Allowed to use EPM.

5.2 ADMINISTRATIVE CONTROLS

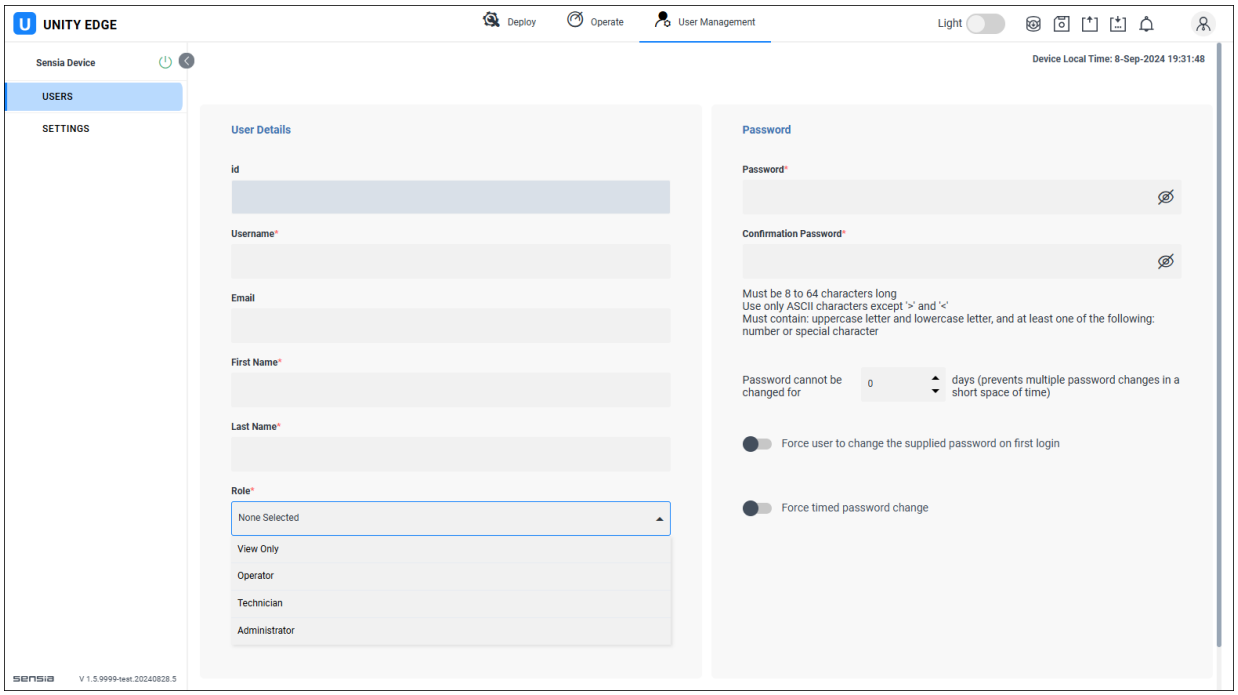
From the User Management menu, administrators can view a list of current users and access details, add users, delete users, and edit user information.

5.2.1 Add a User

1. To add a user, click Add User in the top right corner of the User Management screen.



2. Enter user details as described below.



Each user must be identified by the following:

Id	Numeric identification that is automatically assigned by the software when you save other user detail entries. This field is non-editable.
Username	A unique identification used to log into the system. Must contain at least 2 characters, start and end with a letter, and can include only letters, numbers or underscore (no spaces)
First Name	Must contain at least 2 characters
Last Name	Must contain at least 2 characters
Role	One of four access levels selectable from a dropdown menu (defined in section 5.1, page 49)

3. Enter a user password that meets these minimum requirements:

Password	Must be 8 to 32 characters long. Use only ASCII characters except '>' and '<'. Must contain an uppercase letter, a lowercase letter, and at least one number or special character

4. Enable optional password controls, if desired.

Password should be unchanged for ‘x’ Days	Sets how often a user is allowed to change his or her password. For the default ‘0’ setting, there are no restrictions. Note: This restriction does not apply for expired passwords set by the flags below.
Should change default password	Requires the user to change the password upon initial login
Temporary	Creates a password that will expire after a user-specified number of days

5.2.2 Change User Information/Password

To edit user information, click the Edit symbol  near the end of the user row. Change user details and/or password as described in section 5.2.1 Add a User, page 49.

Administrators need to change the administrative password immediately to secure access. Always record this password in a safe place or pick a password that you won't forget.

CAUTION
If the administrator password is lost, you will be unable to access the HCC2. Contact your system administrator for assistance.

5.2.3 Delete a User

To delete a user from Unity Edge, open the User Management menu tab and click the trash can icon  at the end of the user row.

Important The trash can icon does not appear upon first login when a single admin user is set up. This ensures that you cannot delete yourself as a user. The trash can icon will appear when two or more users are set up.

5.3 PASSWORD MANAGEMENT (ALL USERS)

5.3.1 Change Password

A password change may be required by your network administrator after initial login and is routinely recommended as a best practice for security maintenance.

To change your password

1. Click the user profile icon in the top right corner of the Unity Edge interface.
2. Select Update Password to open a dialog.
3. Enter your old password and create/confirm your new password.
4. Click Save.

5.3.2 Restore Forgotten Password

If you forget your password, contact your administrator for assistance.

5.3.3 Configurable Timeout

You can limit user access to Unity Edge during periods of inactivity by configuring a timeout period in the User Management > Settings screen. Use the dropdown menu to specify the number of hours of inactivity you want to allow before the system automatically logs out the current user.

Section 6: Configuring the HCC2 Device

This section describes how to configure assets selections in the Unity Edge browser interface and deploy the changes to the HCC2. Most of these tasks originate in the Deploy menu described in section 3.3, Deploy Menu, page 34.

6.1 SPECIFYING DEVICE AND PROJECT INFO

The Device Information page in Unity Edge allows you to provide device-specific information about your HCC2.

These details include:

- Asset Name: a name used to uniquely identify an HCC2
- Asset Description: information about where or how the HCC2 is being used
- Project Information: information about where your HCC2 is being used, which is especially useful in managing well sites and for custody transfer

6.2 SETTING TIME AND LOCATION

HCC2 time synchronization is very important to ensure that events are captured accurately and logged in the correct order. There are two time source types to choose from in configuring time in the HCC2: Auto and Manual.

Auto is the preferred option for accuracy. However, if your installation does not support an auto time source (specifically, a GPS antenna or NTP server), you can manually synchronize HCC2 time to your computer time with the Manual time source selection.

Time Source	Description
Auto Source (GPS)	The HCC2 has an on-board GPS module, capable of providing accurate time and location. The PPS (pulse per signal) from the GPS module is used to control the internal RTC on the CPU board. As long as the GPS module has sufficient satellite lock, the time remains synchronized.
Auto Source (NTP)	Generally, NTP will ensure that the time remains synchronized within milli-seconds of the known time. However, NTP can be prone to 'jump' forward or backward in time when attempts to poll the remote NTP server fail. This may result in event timestamps being out of order. The HCC2 uses NTP only when the GPS signal is not present or too weak to provide dependable synchronization.
Manual Source	Sensia does not recommend the manual time source because it is the least accurate time synchronization method. Unity Edge will apply the time from the host computer when the "Sync to Computer Time" button is pressed on the Operate > Device > Time & Location Status screen. A location address can be entered as text if needed.

To configure time and location with an Auto source

1. Navigate to Deploy > Device > Time & Location.
2. Select Auto or Manual from the Time Source dropdown menu. If you select a Manual time source, proceed to step 5.
3. If you select an Auto time source

- The HCC2 will search for a GPS signal. If a GPS antenna is connected with good signal strength, GPS is used as the time source.
- If GPS is not available, the time source will switch to NTP. To use NTP, ensure that your HCC2 can access the specified NTP server, whether that is on your local network or an internet time server. (If using internet routing, make sure your network is properly configured – see Network Configuration for more details).

4. Select the time zone that is appropriate for your HCC2 location.

Note	Internally, the HCC2 uses UTC for all timestamps. You can use the Time Zone setting to convert UTC timestamps to local time. The way time is shown in Unity can be configured using the Deploy > Device > Display Units page.

5. Enter a location name to uniquely identify your HCC2's location.
6. Click Update Deployment to save your configuration to the browser.
7. Deploy your time and location settings to the HCC2 using the Deploy wizard at the bottom of the navigation tree.
8. Navigate to the Operate > Device > Time & Location Status screen.
   a. If you selected an Auto time source, check the Active Time Source setting to verify which source (GPS or NTP) is controlling the time settings. If NTP is the active source, the IP address of the NTP server will be displayed.

   If GPS is the active source, your HCC2's longitude and latitude will also be displayed on the Time & Location screen.

   b. If you select a Manual time source, ensure that the time zone on your computer is correctly configured for the location of the HCC2. Click on Sync to Computer Time to manually synchronize the HCC2 time with your computer time.

6.3 SETTING DISPLAY UNITS

You can configure all values displayed within Unity Edge that have an associated unit (i.e., °C) to use a different unit. You can select a global unit system, which will default all the unit categories to either SI units or US custom units. Or you can start with one of the default categories and then change the sub-categories as needed. With each category, you can choose

- Units to use
- Rate (where applicable)
- Decimal places to display

These changes are applied immediately throughout Unity Edge upon updating the deployment file. For example, changing the temperature unit from °C to °F will cause every screen that shows a temperature to display temperature in °F. (The CPU Temperature on the Operate dashboard might change from 46 °C to 114 °F.) However, if you do not deploy these changes to the HCC2, they are lost when you close the browser.

6.4 USER FIREWALL PORT

To enable additional ports in the firewall (beyond the selections provided as a check-box configuration on the network pages), navigate to Deploy > Device > User Firewall Port in the navigation tree.

To add a port,

1. Select the 'Add Port' button. A new line will appear in the table for configurating.
2. Specify the Port Number, Interface, Port Type, and optionally a Description.
3. Click Update Deployment to save your configuration to the browser.
4. Deploy your settings to the HCC2 using the Deploy wizard at the bottom of the navigation tree.

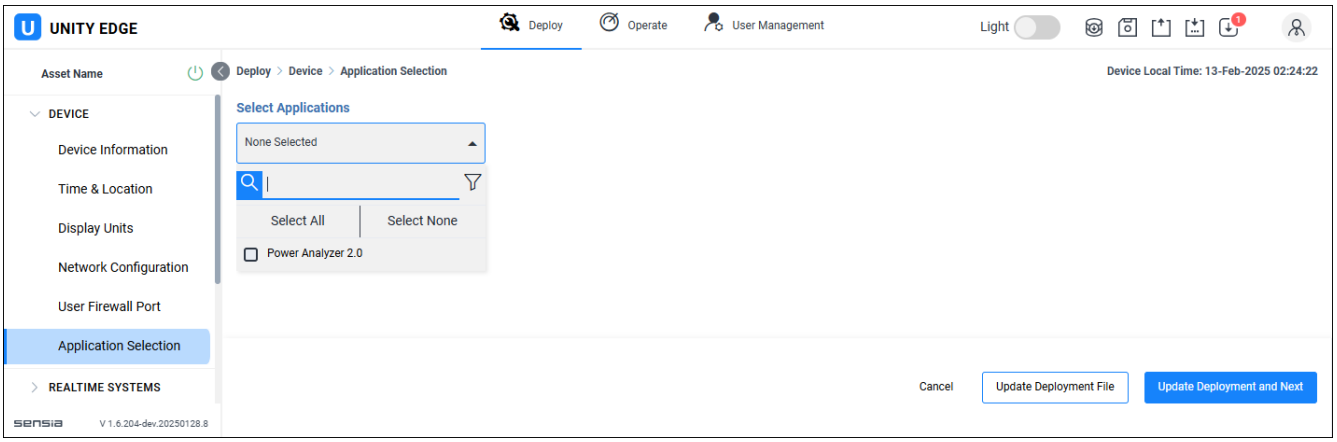
Once deployed, your new port will be open in the firewall.

6.5 SELECTING APPLICATIONS

By default, core out-of-the-box applications are enabled upon installation and do not appear in the Device > Application Selection screen.

Custom edge applications built with the HCC2 SDK will appear here if they are loaded onto the HCC2 (using EPM or Mender.io) and have Unity Deploy or Operate screens. Once you select an application from the list, the relevant screens will be populated in the Unity menu structure, and you can configure your application.

Note To run edge applications on the HCC2, you must have a valid Edge App Enablement license installed. See HCC2 Edge App Enablement, page 14, for details.



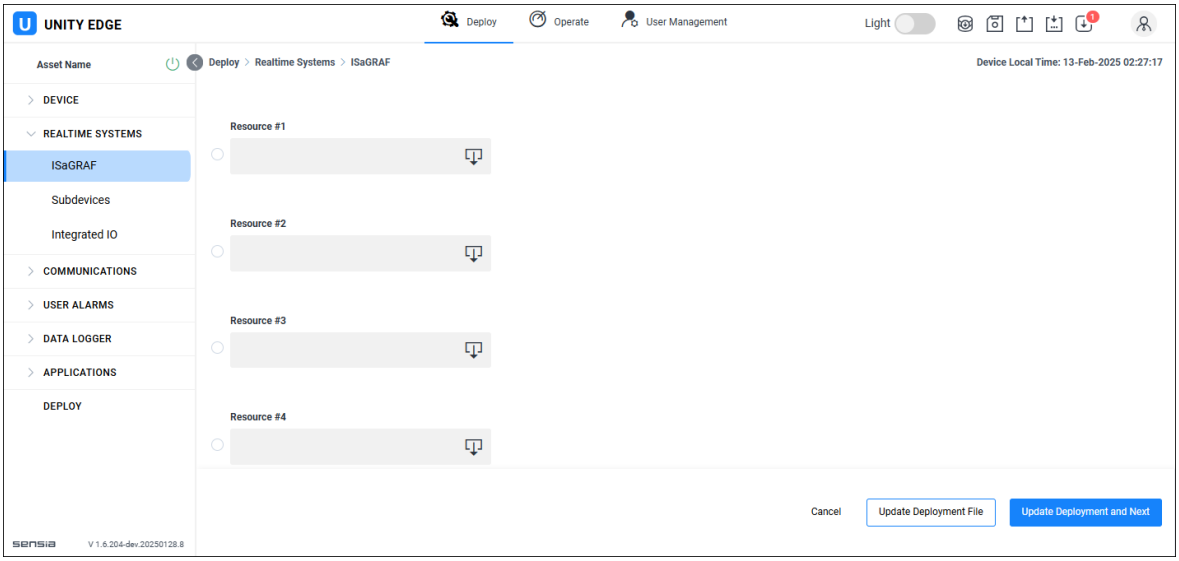
6.6 ADDING ISAGRAF RESOURCES

Adding ISaGRAF resources to Unity Edge allows you to map inputs and outputs from HCC2 applications to ISaGRAF data points, and map process data points from ISaGRAF to Unity Edge data points for use in other applications.

The HCC2 supports up to four ISaGRAF Resources running simultaneously. These resources are developed using the ISaGRAF Workbench software installed with the HCC2 ISaGRAF Add-In, as described in Section 11: Developing an ISaGRAF Application for HCC2, page 146. See section 11.2 for ISaGRAF Workbench and HCC2 ISaGRAF Add-in installation instructions.

ISaGRAF Workbench is used to download each resource to the HCC2 (see section 11.10 for details). However, these ISaGRAF resources must also be loaded to Unity Edge to enable ISaGRAF variables to be mapped to

data points outside of ISaGRAF. The Resource Numbers for the Resources running in the HCC2 must be configured consecutively from 1 to 4 using ISaGRAF Workbench (see section 11.6.1 for details).



6.6.1 Add a Resource

When you add a Resource to Unity Edge, you select variables that can be mapped to data points related to the integrated I/O, other ISaGRAF Resources, Modbus registers, CIP subdevices, alarms and events, and other applications running in the HCC2.

To enable access to these variables, you must load the corresponding symbol table file in Unity Edge.

ISaGRAF Symbol Table File

The symbol table file is created in ISaGRAF when the application is built (compiled) for the first time, and it is updated with every build operation. For information about building an application, see section 11.9 Building an ISaGRAF Application, page 184.

The symbol table file is an “IDS…” file located in the ISaGRAF project folder. For projects stored in the default location, the symbol file can be found here:

C:\Users\<UserName>\Documents\ISaGRAF 6.6\Projects\<ProjectName>\<ProjectName>\IDSnnn01

where 'nnn' is the Resource Number in hexadecimal (i.e., IDS00101 for Resource #1, IDS00201 for Resource #2, IDS00301 for Resource #3, and IDS00401 for Resource #4).

Load a Resource

To load a Resource into Unity Edge:

1. In Unity Edge, go to Deploy > Realtime Systems > ISaGRAF.
2. Click on the radio button next to the desired Resource.
3. Click on the browse button inside the selection box and browse to the symbol table file.
4. Select the symbol table file and click Open.
5. Select variables required for data point mapping in Unity Edge (see section 6.6.2, Select Variables for Data Point Mapping, page 56).
6. Click Deploy in the navigation tree and use the Deploy wizard to commit the Resource configuration to the HCC2 device.

6.6.2 Select Variables for Data Point Mapping

Selecting an ISaGRAF Resource displays its Variable Selection window. The Variable Selection window provides a list of all the variables in the Resource and allows you to select relevant variables to be made available as HCC2 data points for use outside of the ISaGRAF application.

Important For best system performance, select only the ISaGRAF variables required for mapping HCC2 data points. Selecting more variables than needed will compromise performance and make the data point mapping process more difficult.

Before you begin mapping variables to data points, consider the function they will play in your automated system:

"Produced" and "Consumed" Variable Definitions

Each variable is marked as "produced" or "consumed" with respect to the ISaGRAF runtime in the IO board. These markings appear in the attribute column of the ISaGRAF Global Variables database.

- Produced variables are those marked as "Read/Write" or "Write".
- Consumed variables are those marked as "Read".
- Produced data points can be configured to update in Unity Edge periodically or "on change."
- Consumed variables are never produced to Unity Edge. Instead, Unity Edge is constantly writing its value to ISaGRAF.
- Users cannot read data from Consumed variables.

Configuration Settings

The following configuration settings are available :

Enable Data Point Checkbox	• When checked, the ISaGRAF variable is available as an HCC2 data point for use outside the ISaGRAF application. • When unchecked, the variable is available only to the ISaGRAF application.
ISaGRAF Access	• Indicates the Attribute (read and write access) defined for the variable in the ISaGRAF application. • Variables with Read/Write and Write access are presented as ISaGRAF Produced. • Variables with Read access are presented as ISaGRAF Consumed. • This setting can only be changed from the ISaGRAF Workbench.
Data Type	• Indicates the Data Type defined for the variable in the ISaGRAF application. • Possible values are BOOL, SINT, USINT, BYTE, INT, UINT, WORD, DINT, UDINT, DWORD, LINT, ULINT, LWORD, REAL, LREAL, TIME, DATE, STRING, Array types, and instances of Function Blocks. • This setting can only be changed from the ISaGRAF Workbench.
Units	• Configurable units descriptor for the ISaGRAF variable. • For ISaGRAF Produced variables, it indicates the units in which the variable is being produced by the ISaGRAF application. • For ISaGRAF Consumed variables, it indicates the expected units that the ISaGRAF application will receive when consuming the variable. • This setting is optional. • If left as NONE, the value of ISaGRAF Consumed variables will be received in SI units.

Data Point	• When checked, the Data Point Name used for the ISaGRAF variable as an HCC2 data point can be customized by entering the required name in the Data Point Name column. • When unchecked, the Data Point Name will be the default Data Point Name presented in the Data Point Name column, derived from the ISaGRAF variable Name.
Min Publish Period (ms)	• Minimum amount of time in milliseconds before the value of an ISaGRAF variable is published to its corresponding HCC2 data point.
Data Point Publish	• For ISaGRAF Produced variables, the method used to determine when to publish its value to its corresponding HCC2 data point. • Variables configured as On Change Only will only publish their value to the HCC2 data point when the variable changes its value. • Variables configured as Periodic will publish their value once every configured Min Publish Period.

6.7 ADDING SUBDEVICES

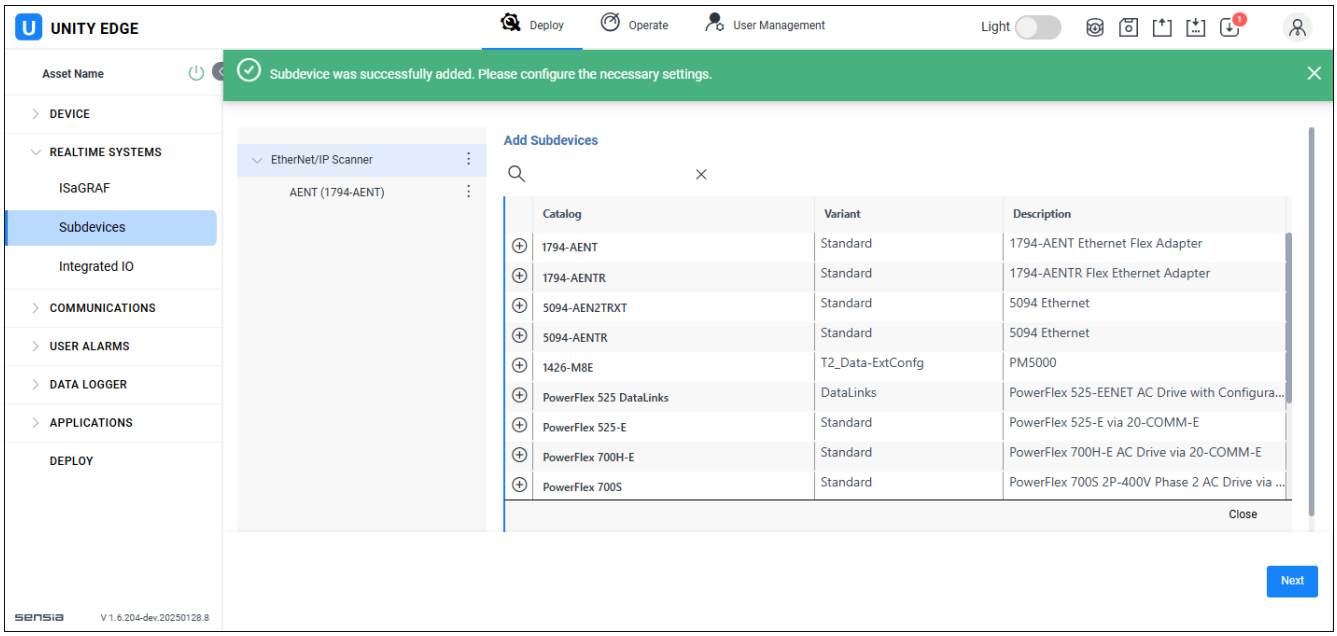
6.7.1 EtherNet/IP & CIP

The HCC2 is equipped with libraries that enable it to connect to EtherNet/IP devices including Rockwell drives and external IO devices.

Libraries in the HCC2 that allow for connection to external devices have the extension .vlb. If you have a library file for a device that is not yet in the Unity Edge catalog of devices, you can import the file for use with your HCC2. Simply select Import Device from the 3-dots menu next to EtherNet/IP Scanner and browse to the location of your .vlb file.

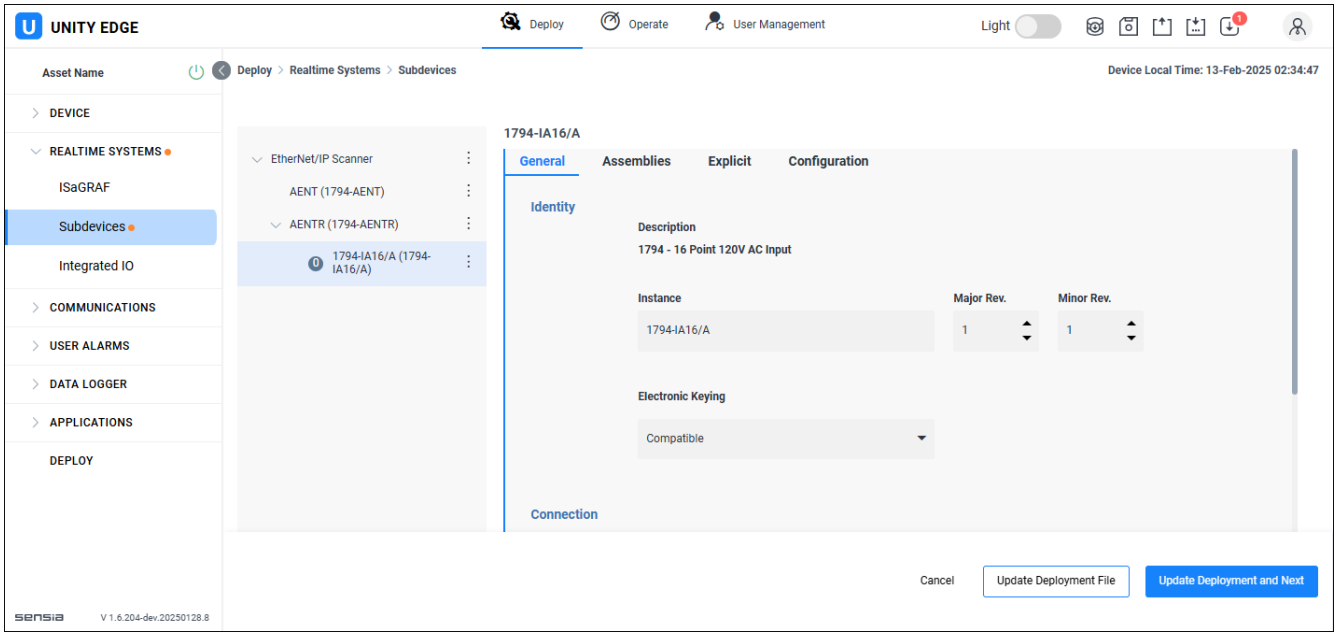
To add a subdevice to your deployment configuration

1. In Unity Edge, go to Deploy > Realtime Systems > Subdevices.
2. From the EtherNet/IP Scanner menu item in the tree, click the 3-dots icon, and click Add in the pop-up dialog. A catalog of subdevices will appear.
3. Scan the catalog and select the drive or external I/O adapter of your choice to add it to the menu tree on the left.



Note	Some subdevices have child I/O modules. Add a child I/O module only after adding an appropriate drive or I/O adapter to the menu tree.

4. To view child I/O devices, click the 3-dots icon next to a subdevice in the menu tree. If child I/O devices exist, they will appear in the catalog listing for your selection. Click on a child device to add it to the menu tree, as shown below.



5. Repeat steps 3 and 4 to select all subdevices required.
6. Click on each subdevice in the menu tree to display its default configuration settings.
7. Update configuration settings as required, referencing section 6.7.2, Configuration Tabs, page 59, as needed.

The configuration layout and options are similar to those of an add-on-profile (AOP) in Rockwell's Studio 5000 configuration software. Specifics can be found in RA user manuals and literature posted on this site:

Technical Documentation Center | Rockwell Automation

8. Once you have configured each subdevice, update your deployment file and deploy your configuration. To view the status, health, and data points associated with the subdevices, refer to the Operate menu in Unity Edge (section 3.2, Operate Menu, page 32).

The following sections focus on configuration that is specific to the HCC2 system (not the operation of the subdevice IO/VSD).

6.7.2 Configuration Tabs

General

The General tab facilitates module configuration with entries including the Instance name, IP address (if applicable), its location in the tree, and the RPI (requested packet interval). This process is similar to configuration via AOP in Studio 5000.

Assemblies

The Assemblies tab allows you to select which of the assembly data are mapped to the HCC2 data point system. You can select only the data you need from each module. The assembly data are populated from the data available in each module, and, if selected in Unity Edge, a data point is auto-created in the format InstanceName.Assembly.Description.

The assembly tab also allows you to select whether the data point is updated on change, or at the configured module RPI.

Explicit (Future)

The Explicit tab allows you to create an explicit (Class 3/unconnected) message to send to the device. The parameters to specify include the Class, Instance, and Attribute to read/write (these can be found in the respective user manual of the subdevice). These messages can then be triggered from an application.

Config

The Config tab(s) allows you to enter configuration selections for I/O modules such as analog input and output range formats, input filter settings, and fault mode criteria. The number of configuration tabs and tab names will vary depending on the I/O module type.

6.7.3 PowerFlex Drive Specific Tabs

Input

This tab is available when a drive has configurable data links (configurable Class 1 data connections). The Input tab allows you to set up your data links according to your drive configuration.

Important	This configuration must match the configuration of your drive to establish a connection.

These data links are available in the Assembly tab as Input Assemblies to map to internal HCC2 system data points, as described above.

Output

Like the input tab, the output tab allows you to configure the output data links to match that of your drive.

Important	This configuration must match the configuration of your drive to establish a connection.

These data links are available in the Assembly tab as Output Assemblies to map to internal HCC2 system data points as described above.

6.8 INTEGRATED IO DATA POINT MAPPING

All of the data integrated with Unity Edge are identified and consumed through data points and data point mapping. The data point mapping mechanism allows you to map data to

- integrated input and output channels
- ISaGRAF variables
- Modbus registers
- subdevice parameters
- other apps running in the OS containers

Data points are mapped to inputs or outputs of applications/services in the system in cases where there is a general purpose I/O. Each mapped data point is configured as an input or an output within each application. Data points are not mapped to other data points.

User alarm configuration and data logging are just two of the ways data point mapping is commonly used.

By assigning data points that reflect real world measurements, developers and end users can define system inputs and outputs consistently. Using data point mapping and consistent data point naming, you can define much of the communication between apps before you interact with the system.

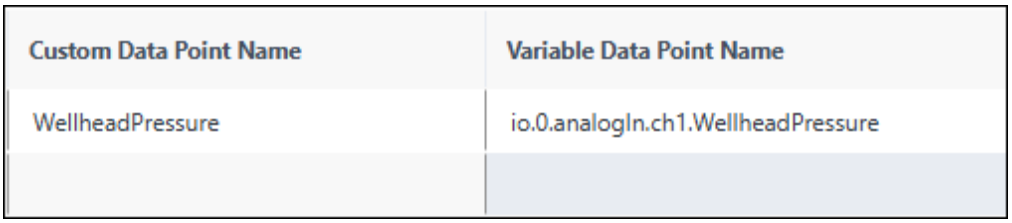
For example, an application that processes wellhead pressure via a 4-20mA analog sensor or Modbus register does not need to be modified if the source of wellhead pressure changes. A simple data point mapping update can resolve the issue.

6.8.1 Data Point Names

Unity Edge supports both pre-defined system data points and user-defined custom data points.

Each data point has two names (Figure 6.1):

- a human-readable display name reflecting the real world meaning of the measurement (such as wellhead pressure)
- a unique internal system-generated variable data point name that ensures that every data point is uniquely identifiable within a network



Custom Data Point Name	Variable Data Point Name
WellheadPressure	io.0.analogIn.ch1.WellheadPressure

Figure 6.1—Data point name formats

6.9 CONFIGURING ANALOG INPUTS AND OUTPUTS

The HCC2 allows you to configure up to eight Analog Inputs and two Analog Outputs.

6.9.1 Analog Inputs

Analog Inputs can be configured with the following parameters:

Parameter	Selections	Description
Mode	Voltage	Sets the port to measure the voltage on the terminals.
	Current	Sets the port to measure the current on the terminals.
	HART	Fixed Address. Enable a fixed address where applicable. Set to a value between 0 and 255.
		HART Address. Set to a value between 0 and 63.
		HART Rate. Set to a value between 0 and 255.
Range	Voltage	0-10 V, 0-5 V, -10-10 V
		0-100mV for channels 7 and 8 only
	Current	0-20mA or 4-20mA
	HART	0-20mA or 4-20mA
Unit		Sets the category and associated units for Analog Input values. Includes a scalar selection for rate values.
EU Low		Sets the low range value of the Analog Input in reference to the Units.
EU High		Sets the high range value of the Analog Input in reference to the Units.
Fixed Publish Interval (ms)	Default: 500 ms Configurable Range: 1 to 3,600,000 ms (1 hr)	Sets the value used when publishing values.
Map To:	Custom Data Point	Allows you to create a new data point for the input.
	Selected Data Point	Allows you to select an existing system data point for the input.
Selected Data Point Name		If mapped to Selected Data Point, select a system data point from the dropdown menu.
Custom Data Point Name		If mapped to Custom Data Point, enter a unique custom data point name.
Variable Data Point Name		When a Custom Data Point name is specified, click the Variable Data Point Name field to auto-assign a variable name. This setting is disabled when a Selected Data Point is configured.

6.9.2 Analog Outputs

Analog Outputs can be configured with the following parameters:

Parameter	Selections	Description
Mode	Voltage	Sets the port to output a voltage signal on the terminals.
	Current	Sets the port to output a current signal on the terminals.
Range	Voltage	0-10 V, 0-5 V, -10-10 V
	Current	0-20mA or 4-20mA
	HART	0-20mA or 4-20mA
Selected Data Point Name		Select the parameter data point to be output through the channel as detailed within Data Point Mapping.
Unit		Automatically populated in accordance with the units associated with the selected parameter data point. If no unit is specified for the selected parameter data point, Unit will display No Units.
EU Low (Required)		Sets the low range value of the analog output in reference to the Units.
EU High (Required)		Sets the high range value of the analog output in reference to the Units.
Default Value on Startup		The value that the channel is initialized with at startup.

6.10 CONFIGURING DIGITAL INPUTS AND OUTPUTS

The HCC2 offers eight fixed Digital Input channels and eight DIO channels for configuration as either inputs or outputs. The eight fixed inputs are no different in their application from a DIO configured as a digital input.

Digital I/O is transmitted as a discrete signal that is either energized (on) or de-energized (off).

Digital inputs are used to record the state of a normally open or normally closed external contact. The number of times the signal changes is recorded as a DI counter value.

A DIO can be configured as a standard digital input, a digital output, or a pulse width modulator

Unity Edge provides two types of data points for mapping variables to digital inputs and outputs:

- Custom data points. Digital inputs and outputs (typically, I/O that is already wired to a known device) can be configured with custom data point names. This would be appropriate for I/O that is being set up for logging or alarm configuration purposes.
- Selected data points. When the variables driving a digital input or output are established and named—for example, when an ISaGRAF operator has digital input and output variables already identified in an ISaGRAF program—it is not necessary to set up custom data points. We can simply select a data point from the ISaGRAF system and add it to our map.

When you configure a DIO as a digital input, you are reading an input on a terminal and producing data into the system to publish a data point. You can publish to your own custom data point or a selected data point.

When you configure a DIO as a digital output, the non-inverted position is normally open, and the inverted position is normally closed. Unlike a digital input, a digital output needs a value from the system to enact a physical change on something. Digital outputs are mapped only to system data points (not custom data points) since every variable available for output already has a data point in the system.

Keep in mind that when you select a system data point, you inherit the range of the data point you are choosing, and you must configure output values accordingly.

6.10.1 Digital Input (DI1 through DI8, DIO1 through DIO8)

Digital Inputs can be configured with the following parameters:

Parameter	Selections	Description
Mode	Digital Input	
Debounce (ms)	Default: 15 ms Configurable Range: 0 to 500 ms	Time allowed for filtering digital input noise which commonly occurs when a physical switch closes
Counter Rollover	Default: 10,000s	The upper limit on the state change counter before it restarts from 0.
Minimum Publish Interval (ms)	Default: 50 ms Configurable Range: 1 to 3,600,000 ms (1 hr)	The minimum interval at which the value from the input will be measured and published to the message bus.
Fixed Publish Interval (ms)		Note: This field is deactivated in Unity Edge at this time.
Map To	Custom Data Point	Allows you to create a new data point for the input.
	Selected Data Point	Allows you to select an existing system data point for the input.
Selected Data Point Name		If mapped to Selected Data Point, select a system data point from the dropdown menu.
Custom Data Point Name		If mapped to Custom Data Point, enter a unique custom data point name.
Variable Data Point Name		When a Custom Data Point name is specified, click the Variable Data Point Name field to auto-assign a variable name. This setting is disabled when a Selected Data Point is configured.

6.10.2 Digital Output (DIO1 through DIO8)

Digital Outputs can be configured with the following parameters:

Parameter	Description	
Inverted	Enable/Disable	Available only when the DIO mode is Digital Output. Reverses the configured output signal (True/False conditions) automatically.
Mode	Digital Output	Functions as a solid state relay.
	Pulse Width Modulator	Generates variable-width pulses representing the amplitude of an analog signal using a digital output.
Debounce (ms)	Default: 15 ms Configurable Range: 0 to 500 ms	Time allowed for filtering digital input noise which commonly occurs when a physical switch closes
Pulse Interval (ms)	Enabled only when DIO mode is Pulse Width Modulator.	Default: 10 ms Configurable Range: 1 to 10,000 ms
Counter Rollover	Default: 10 ms	The upper limit on the state change counter before it restarts from 0.
Minimum Publish Interval (ms)		How frequently the output will be published
Fixed Publish Interval (ms)		Note: This field is deactivated in Unity Edge at this time.

Default Value on Startup		The value that the channel is initialized with at startup.
Map To	Selected Data Point	Select an existing system data point for the output.
Selected Data Point Name		Select a system data point from the dropdown menu.
Custom Data Point Name		If mapped to Custom Data Point, enter a unique custom data point name.
Variable Data Point Name		When a Custom Data Point name is specified, the system auto-assigns a variable name. This setting is disabled when a Selected Data Point is configured.

6.11 CONFIGURING COMMUNICATION PORTS

6.11.1 Serial Ports

The Serial Port table shows the six available serial ports: 5 RS-485 serial ports and 1 RS-232 port.

Note RS485 ports 4 and 5 are located on the IO board and are software-enabled via a 120 Ω resistor. They support Modbus RTU in client mode only. See the HCC2 Hardware Manual for details.

The configurable options for a serial port connection are baud rate, parity, stop bit, terminate, Rx bus timeout, Tx bus delay, and protocol.

Label	Description
Baud rate	Determines the speed of communication over a data channel. For successful communication the baud rate selected needs to match the same speed as the connected serial device. Data transmission will still occur when there is a mismatch but the data will be unintelligible.
Parity	Parity is a method of detecting errors in data transmission. The parity bit is an optional parameter used in serial communications to determine if the data character being transmitted is correctly received by the remote device. Select the correct parity option for your connected serial device.
Stop bit	Serial links transmit data in distinct packets or frames. The stop bit is used to signal the end of each frame. The stop bits will be determined by the connected serial device.
Terminate	A termination resistor is a single resistor placed at the end of an electrical transmission line. They are used for differential pair signals, like RS-485. In the HCC2, RS-485-4 and RS-485-5 serial buses can be terminated via a software enabled 120 Ω resistor. This configuration is disabled for all other ports.
Rx Bus Timeout (ms)	Timeout interval used to wait for a response.
Tx Bus Delay (ms)	Delay of the transmission of any request, after receiving a response or timing out.
Protocol	This is the task assigned to this particular instance of the HCC2 serial bus. The specific settings for the selected protocol will be available under the left panel *Protocols* menu.

6.11.2 Server TCP Ports

You can configure the HCC2 to act as a Modbus server, client, or both. HCC2 can support up to two Modbus TCP server connections through ports 502 and 503.

For more information, see section 8.4 Setting Up TCP Server and Client Connections, page 106.

6.11.3 Client TCP Ports

HCC2 can support up to four TCP Modbus client connections.

Each HCC2 Modbus client can connect with and support multiple servers. Your system resources determine the number of servers that each client instance can support.

For more information, see section 8.4 Setting Up TCP Server and Client Connections, page 106.

6.12 CONFIGURING USER ALARMS

To configure an alarm, navigate to the Deploy > User Alarms > User Alarm Configuration page.

There, in the search and filter menu, you will find a list of data points from which you can create alarms. You can manually configure simple range-based alarms using system (i.e., IO Board) or application-specific data points.

1. Click the Add User Alarm button.
2. Click the Pencil icon and select a data point from the list provided. Filter selections and search fields allow you to quickly locate a data point based on known attributes (application/data point group, data point category, display name, data type, and unit). A definition corresponding to the data point you have selected will appear in the lower left corner.
3. Click Save to add it to your User Alarm Configuration table.
4. Make the following selections/data entries to define the alarm:
    - Display Name: Must be at least 3 characters and no more than 40 characters.
    - Latching: Enabled by default. Toggle to a disabled status if latching is not desired.
    - Auto Acknowledge: In the Default (disabled) state, a user or application must acknowledge an alarm to clear the alarm status when alarm conditions are no longer present. This setting ensures that users are notified of all current and previous alarm conditions. Toggle this setting to Enabled if you do not wish to be notified of previous alarm conditions and you want them to be automatically acknowledged as they occur.
    - Holdoff Period (ms): Optional; default is 0. A hold-off period delays alarm activation for a specified time when an alarm condition occurs and can be useful to minimize alarms when values are hovering near a setpoint.
    - Range: Range values for Low Low, Low, High, and/or High High alarms (based on pre-existing data point units); see also section 6.12.2, Change Alarm Range Units, page 67.
5. Click Deploy in the navigation tree and use the Deploy wizard to save the alarm configuration to the HCC2.

6.12.1 Latching and Automatic Alarm Acknowledgment

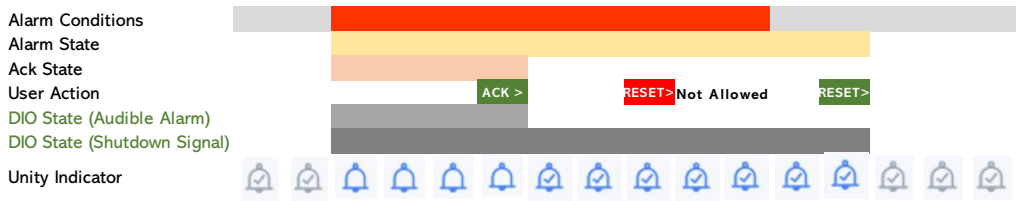
When you configure an HCC2 alarm, the selections you make for Latching and Automatic Acknowledgment will determine how alarms behave and how they are displayed in the Unity interface both during and after an alarm event. Latching and automatic acknowledgment selections may vary, depending on criticality of an alarm condition and individual user preferences for notification.

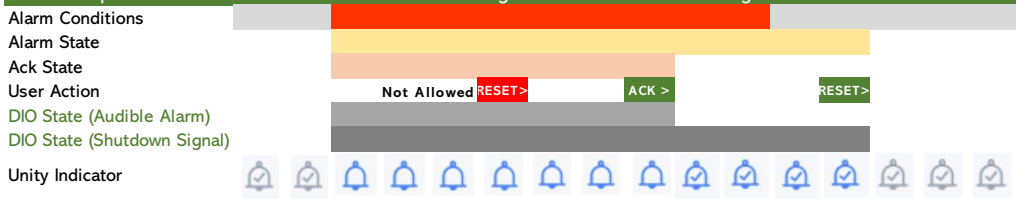
For best results, consider how various combinations of these settings will impact the data displayed in Unity. Below are a few examples of Latching and Auto Acknowledge settings to help you visualize the differences and choose the best alarm configuration for your needs:

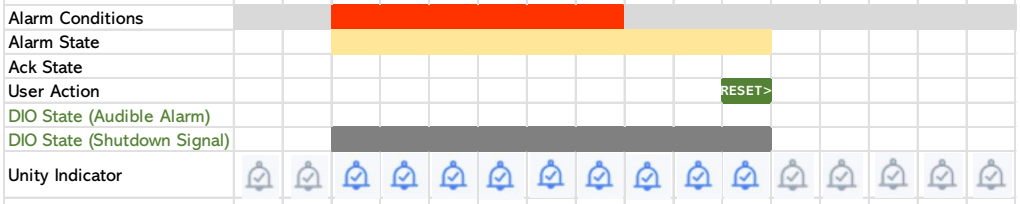
Alarm Configuration Examples

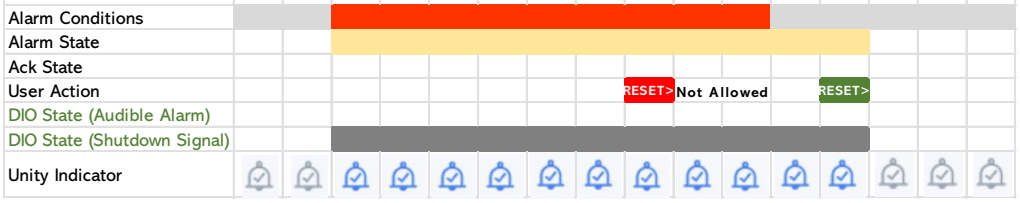
<table>
<tr><th>Latching</th><th>Auto-Ack</th><th></th></tr>
<tr><td>Enabled (default)</td><td>Disabled (default)</td><td>
Latching = Enabled Auto Acknowledge = Disabled
User acknowledges alarm and then resets event after conditions are no longer met.


User resets event and then acknowledges alarm after conditions are no longer met.

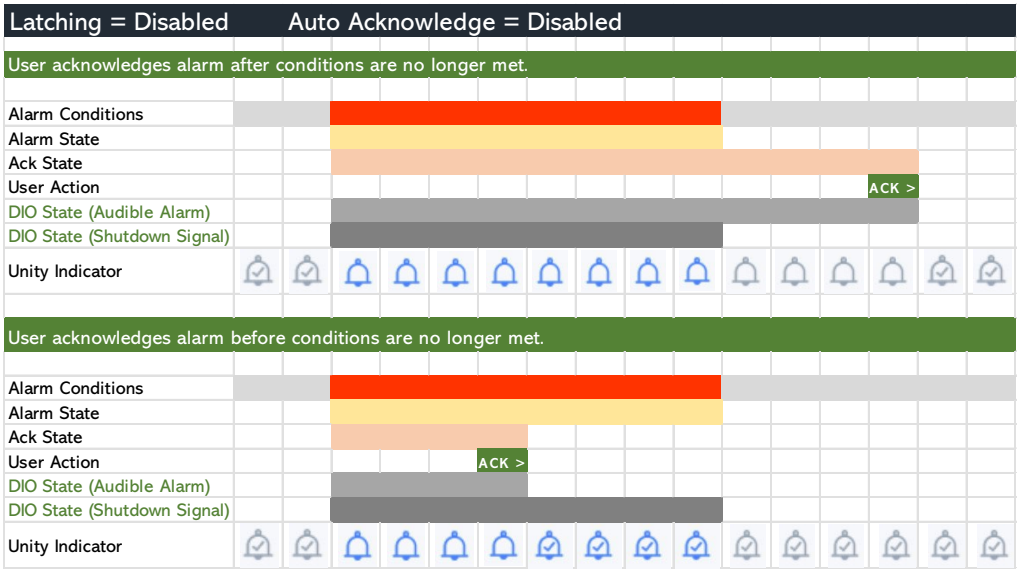
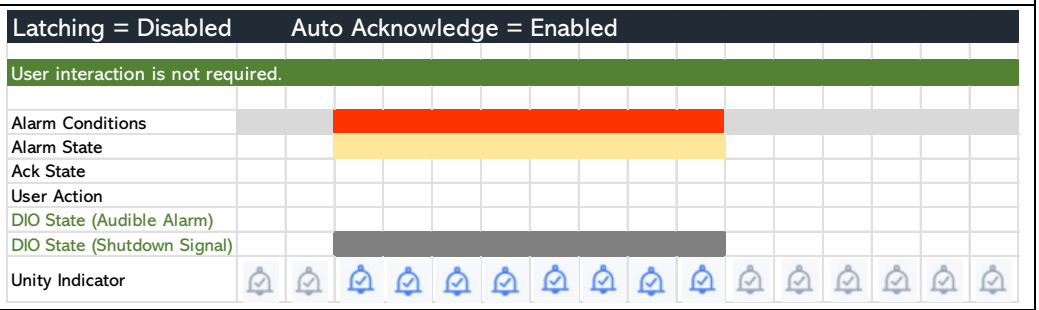

User acknowledges alarm and attempts to reset event before conditions are no longer met.


User attempts to reset event before conditions are no longer met and then acknowledges alarm.


</td></tr>
<tr><td>Enabled (default)</td><td>Enabled</td><td>
Latching = Enabled Auto Acknowledge = Enabled
User resets event after conditions are no longer met.


User attempts to reset event before conditions are no longer met.


</td></tr>
</table>

Disabled	Disabled (default)	
Disabled	Enabled	

6.12.2 Change Alarm Range Units

Range values use the units associated with the data point selected for the alarm. For example, if a temperature data point has a °C unit and you enter 100 as your “high” alarm range value, the HCC2 will alarm when the temperature exceeds 100°C.

You can change the unit associated with a data point by configuring display units on the Deploy > Device > Display Units screen. See also section 6.3 Setting Display Units, page 53.

6.12.3 Remove an Alarm

To remove a configured alarm, click the corresponding selected data point item in the search and filter menu; this will deselect the item (remove the blue checkmark) and remove it from the alarm table.

6.13 CONFIGURING USER LOGS THROUGH DATA LOGGER

Log the data points of your choosing with the HCC2 Data Logger feature. You can log any data point published within the system, including those produced by ISaGRAF, integrated IO, protocols, or an edge application installed on the HCC2.

This section describes the configuration selections you can use to customize the logging process to your specific needs.

The Data Logger feature allows you to select which data points to monitor. For each data point, you can specify

- A logging priority

  The priority determines how often the data point is logged: for example, every second, every five seconds, every minute, etc. It indicates how closely you want to monitor certain data points. For example, you might want to track pressure every second but monitor temperature every minute.

- An update algorithm

  The specified update algorithm determines the aggregate of the enumerated values captured and stored by the data point: for example, the current value only, an average of multiple values, the minimum of multiple values, etc.

6.13.1 Configure a User Log

To configure a user log, navigate to the Deploy > Data Logger > User Log Configuration page. You can add new data points to log or edit existing ones.

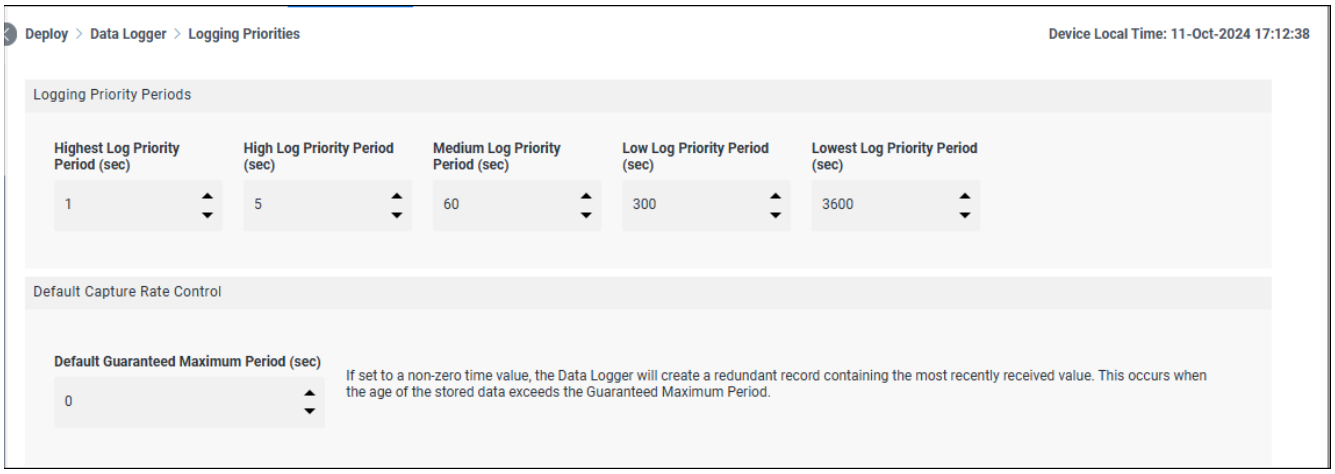
1. Under the User Log Data Point Selections, click Add Data Point to insert a new row.
2. Click the Edit icon in the Selected Data Point Name field to access a list of all available data points.
3. In the Data Points Selection List, filter your selection by application/data point group, data point category, or data type using dropdown menus, or enter a word or phrase in a search field (application, data point category, display name, data type, or unit).
4. Click Save to add your selection to the User Log Data Point Selections table.
5. Specify the values for Logging Priority and Algorithm if different from the default values.

Configuration Parameter	Description	
Logging Priority	Logging frequency; data points with the highest priority or rate are logged most frequently to the disk. Settings are configurable up to a maximum of 4 hours (14,400 seconds).	
	Real-time / Highest Log Rate (default is one log per second)	
	High log rate (default is one log per 5 seconds)	
	Medium log rate (default is one log per minute)	
	Low log rate (default is one log per 5 minutes)	
	Lowest log rate (default is one log per hour)	
Algorithm	Aggregate value to be stored:	
For the Visual, Average, Minimum, and Maximum value selections, the stored quality is the aggregate of the qualities that are received.	None	Only the latest update is stored. All other updates are discarded and unrepresented within the log.
	Visual	Value calculated by the Largest-Triangle-Three-Buckets (LTTB) algorithm. LTTB helps to filter time series data for visual representation, reducing the number of redundant data points.
	Average	All updated data point values are saved. The average of the updated values is used to create the stored value.
	Minimum	Minimum value of all captured values is the stored value. For example, if you are monitoring tank levels, you might want to know the minimum and/or maximum level over the logging rate.
	Maximum	Maximum value of all captured values is the stored value.
Trend	Displays a trend view of the selected data point on an FT Optix HMI (if available)	

6. Click Deploy in the navigation tree and use the Deploy wizard to push the user log configuration to the HCC2 device.

6.13.2 Change Logging Priority (Log Rate)

By default, logging rates are displayed in seconds. The corresponding logging priorities have default rate settings ranging from one per second (highest priority) to one per hour (lowest priority).



You can modify logging priorities in two ways:

- You can specify different default logging rates for each period, as long as the value is between one and 14,400 seconds (four hours). As indicated in the above screenshot, the periods are Highest, High, Medium, Low, and Lowest.
- You can add protection against stale data by enabling a Default Capture Rate Control feature. This feature creates a redundant log record containing the most recently received update when the specified period of time has passed since the last log record was generated.

To change the log rate

1. Navigate to the Deploy > Data Logger > Logging Priorities page.
2. For the targeted log priority period, type a value between 1 and 14,400 (seconds).
3. Click Deploy in the navigation tree and use the Deploy wizard to push the user log configuration to the HCC2 device.

Stale Data Protection

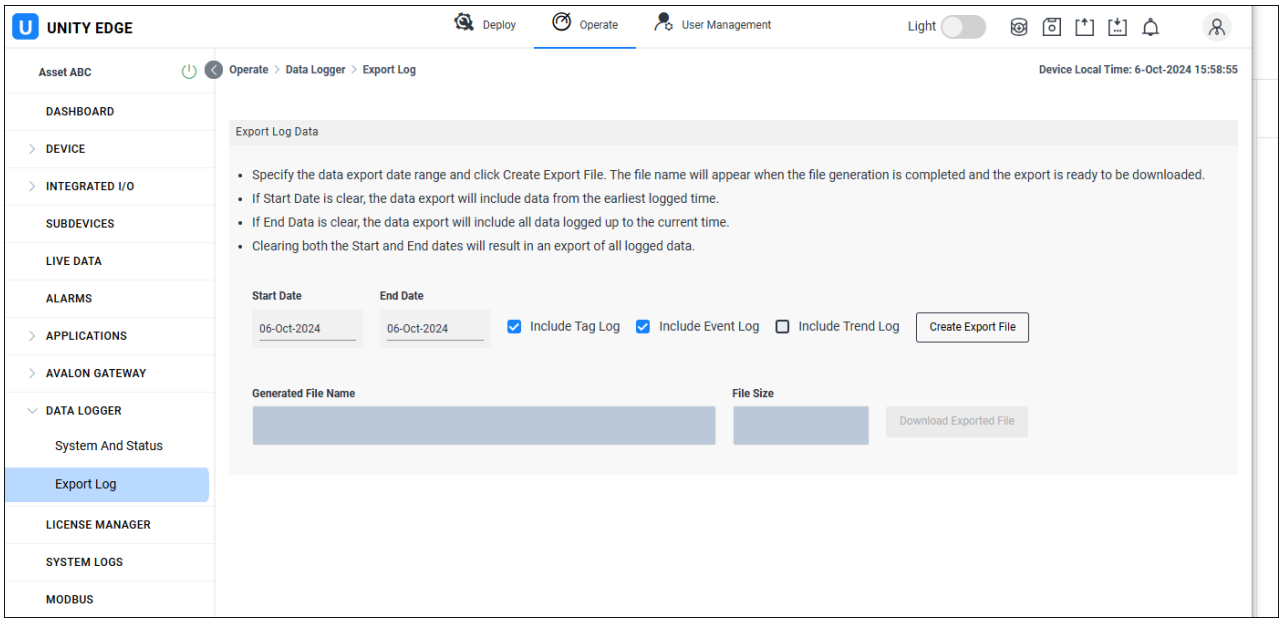
You can add protection against stale data. Under the Default Capture Rate Control heading, type a maximum wait period (in seconds, by default). When the age of your stored data exceeds this value, the Data Logger creates a redundant record containing the most recently received value for your log data points.

6.14 EXPORT DATA LOGS

To access the logged data for analysis, you will first navigate to the Operate menu to create an export file (*.hedgelog) of the log records, and download it to your PC or laptop, as described below. Then, you can extract your time series data through the Data Log Extractor utility (section 6.14.1, Exporting Logs to CSV Report, page 70).

To create and download the export file

1. Go to Operate > Data Logger > Export Log.



2. Select Start and End dates, and select the log data types you want to export.
3. Click Create Export File.

   The file name will appear in the Generated File Name field when the file generation is completed, and the export is ready to be downloaded. The generated file name includes the export time stamp, the Asset Name and the Site Well Name used to identify the HCC2.
4. File size is also displayed. See Manage Export File Size below for details on how to further optimize your export file. Click Download Exported File to open a Save As window and save the .hedgelog file to your Downloads folder.
5. Click the Downloads icon in your browser to see the available file. Proceed to section 6.14.1, Exporting Logs to CSV Report, 70, for instructions on how to open the .hedgelog file and export selected data to a .csv report.

Manage Export File Size

If you are connected to an HCC2 with limited bandwidth or a metered connection, export file size may be a consideration when making your export selections. Consider regenerating the file with more restrictive options to reduce file size.

- Specify Start and End dates that minimize the date range for log data collection.
  - If Start Date is unspecified, the data export will include data from the earliest logged time.
  - If End Date is unspecified, the data export will include data logged up to the current time.
  - If both Start and End dates are unspecified, the data export will include all logged data.
- Reduce the number of log data types you include in the export file (Data Point Log, Alarm Log, Event Log, Audit Log). Only including the Data Point Log data can greatly reduce the export file size.

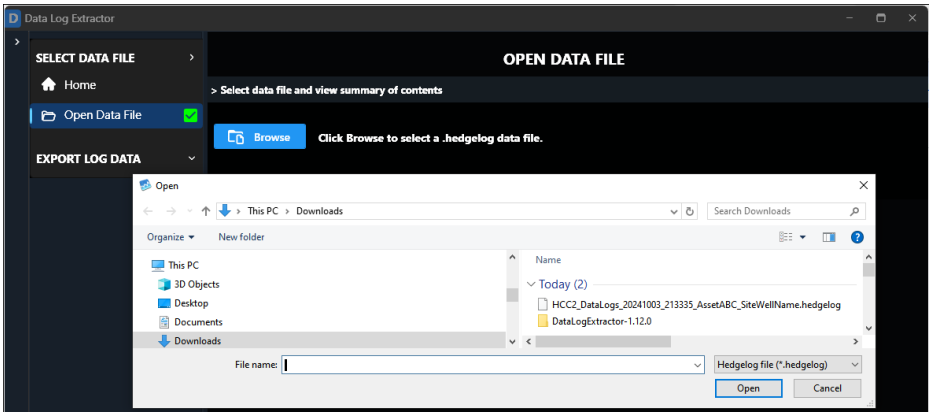
6.14.1 Exporting Logs to CSV Report

After you generate the .hedgelog export file, you can use the Data Log Extractor wizard to export selected data to a readable time series CSV output.

Important If you haven't installed the utility on your PC or laptop, see section 4.7 Using the Data Log Extractor, page 48, for installation instructions before proceeding.

To configure the export to .csv,

1. Launch the Data Log Extractor wizard.
2. With the Open Data File folder selected in the navigation tree on the left , click Browse to select the .hedgelog file containing the data you want to export to .csv format.



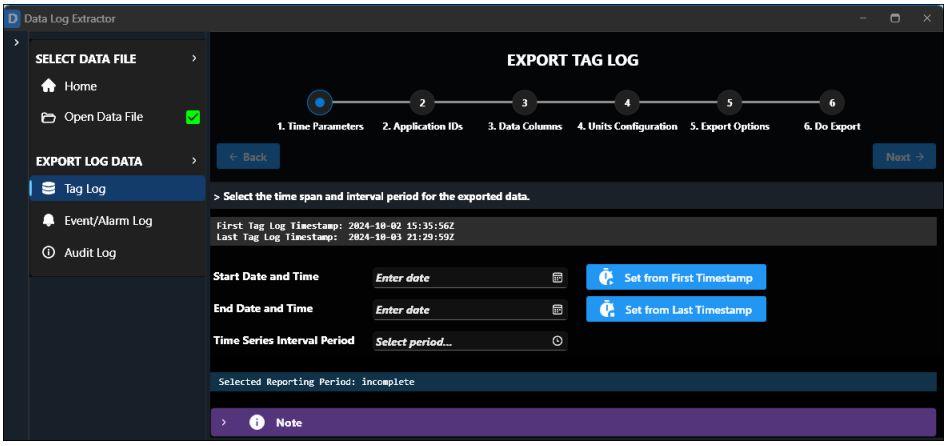
Note	The utility will scan the hedgelog file and publish a Data File Summary on screen. Depending on the size of the file, this can take more than a few seconds. The Data File Summary displays device and asset information, start and end dates of the export period, number of log data files detected, and a summary of records contained within those files (shown below).

```
Data File Content Summary
-------------------------------------------

Log Type          Records       Earliest                  Latest
-------------------------------------------------------------------------------

Tag Log           362           2024-10-02 15:35:56Z      2024-10-03 21:29:59Z
Event Log         5,646         2024-08-28 01:16:34Z      2024-10-03 20:58:39Z
Alarm Log         2,703         2024-08-28 01:16:34Z      2024-10-03 20:58:39Z
Audit Log         73            2024-08-28 01:16:33Z      2024-10-03 18:21:39Z
```

3. Click to expand the Export Log Data menu in the left panel and view additional menus for configuring data point log, event/alarm log, and audit log exports. Clicking on any one of these screens displays a screen similar to the Export Data Point Log shown below. At the top of each screen is a sequential status bar to guide your selections to the final step of exporting data to .csv. A blue indicator will follow your progress, adding a blue checkmark to each step completed, and displaying a blue circle on the step in process.



4. As you complete each set of tasks, click Next to progress to the next numbered step. You can also click Back at any time to return to the previous screen.
5. When you complete the last step (Do Export) for each log type, look for a green checkmark next to the log in the navigation tree showing which logs have been exported.

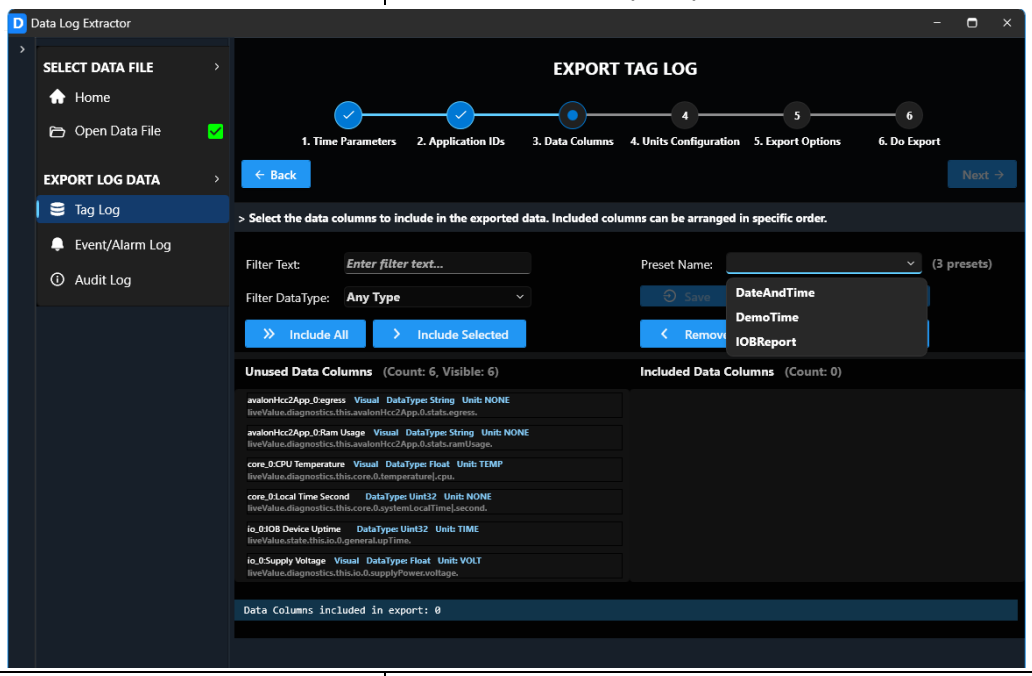
6.14.2 Configure Data Point Log Export

In this section, we will look at ways to customize data point log data presentation in the .csv report by configuring the export in the Data Log Extractor. CSV files can be edited in text editors such as Notepad++.

If your export file is very large and you intend to import the CSV data into a spreadsheet such as Excel, you may wish to manage the size of the .csv file using one of these methods:

- Use a smaller report period by adjusting Start and End dates.
- Increase the Time Series Interval Period to produce fewer rows over the same report period.
- Edit the produced .csv data in a text editor to reduce the size. Spreadsheet applications are typically limited to 1,048,576 rows.

Tabbed Screen	Functions	Task Details
Time Parameters	Select the time span for the exported data.	Select start and end dates and times using the calendar tool. Or, to apply the first or last timestamp in your log data as a start or end point, click the blue “Set from First Timestamp” or “Set from Last Timestamp” button(s) to populate this entry.
	Select the interval period for the exported data. Your exported file will contain a row for each Time Series Interval period that falls within the Start and End date and time.	The available interval selections range from one second to 24 hours (24 hours displays as 00:00:00). The interval period will be captured in the generated .csv filename.
Application IDs	Select application logs from a list of Application IDs that have produced log records within your selected report period.	
Data Columns	Select the data columns to include in the .csv export.	Filter available selections by text search or by data type selection. The Filter Text method will find text matches within all data point Display Names, Units, and Fully Qualified Data Point Names. The Filter Data Type method filters by Floating Point Type, Integer types, and any specific data type. To add a data column to your export configuration, select the item from the Unused Column list at the left of the screen and move it to the Included Data Columns list on the right using drag and drop or the blue buttons provided. (Likewise, you can remove items from the Included Data Columns list in the same way.)
	Specify the order in which data columns appear in the .csv export. Column order from top to bottom defines CSV column order from left to right.	To change the order of included columns, click and drag an item upward until a blue line appears in the location where you want the file.

Data Columns (cont'd)	Save a group of tags for reuse with other .csv exports by creating a preset configuration (optional).	To save a collection of tags as a preset: Select and order the tags in the Included Data Columns list. Type a name for the preset in the Preset Name field shown below and click Save. To recall a preset, select the preset from the Preset Name dropdown (shown below) and click Load. The contents of your preset collection will be added to the Included Data Columns in the order you specified when creating the preset. To update a preset, load the preset, make any content or order changes to Included Data Columns, click Save, and click OK at the prompt.
		
Units Configuration	Set the units of measure for exported data values.	Choose a unit system from the Units System dropdown list: HCC2 base units, SI units, or US Customary units.
Export Options	Specify the data header rows you want to include in the report.	By default, all log output files include header rows for export dates, device information, and asset information. Data Point Log output files also include TagName and ArrayIndex by default. Click the checkboxes to select any additional data header rows you want to include in the report, or click Select/Deselect All Header Rows to add all of them.
	Specify the folder where the export file will be exported.	Click the Select Folder button and browse to the location where you want the .csv report to be saved.
Do Export	Generate a data point log time series data, write it to a .csv file, and save it in the user-specified folder.	Review the export configuration details under the Export Progress heading. If no additional changes are needed, click Do Export to generate the log file, as shown below. The output filename will follow this format: `export_taglog_YYYYMMDD_HHMMSS_XXXsec.csv` `YYYYMMDD_HHMMSS` is the date and time when the file was written. `XXXsec` is the configured time series interval period. Click the **Click here** hyperlink to open the output folder where the exported report resides.

6.14.3 Configure Event/Alarm Log Export

In this section, we will look at ways to customize event/alarm log data presentation in the .csv report by configuring the export in the Data Log Extractor.

Tabbed Screen	Functions	Task Details
Time Parameters	Select the time span for the exported data.	Select start and end dates and times using the calendar tool. To apply the first or last timestamp in your log data as a start or end point, click the blue “Set from xxx TimeStamp” button(s) to populate this entry.
Data Point Sources	Select the data point sources to include in the exported data.	
Alarm Criteria	Select the alarm levels and publish reasons to include in the exported data.	Select individual checkboxes or click the Select/Deselect All… checkbox.
Units Configuration	(Same selection as described in section 6.14.2).	
Export Options	Specify whether event log records should be included in the exported data.	By default, all log output files include header rows for export dates, device information, and asset information. Check the Also export Event Log records checkbox to output a separate event log report in addition to the alarm log report.
	Specify the folder where the export file will be exported.	Click the Select Folder button and browse to the location where you want the .csv report to be saved.

Do Export	Write alarm log records to a .csv file, and save it in the user-specified folder.	Review the selected parameters under the Export Progress heading. If no additional changes are needed, click Do Export to generate the log file.
		The alarm (and event, if applicable) output filenames will follow this format:
		`export_alarmlog_YYYYMMDD_HHMMSS.csv`
		`export_eventlog_YYYYMMDD_HHMMSS.csv`
		`YYYYMMDD_HHMMSS` is the date and time when the file was written.
		Click the Click here hyperlink to open the output folder where the exported report(s) reside.

6.14.4 Configure Audit Log Export

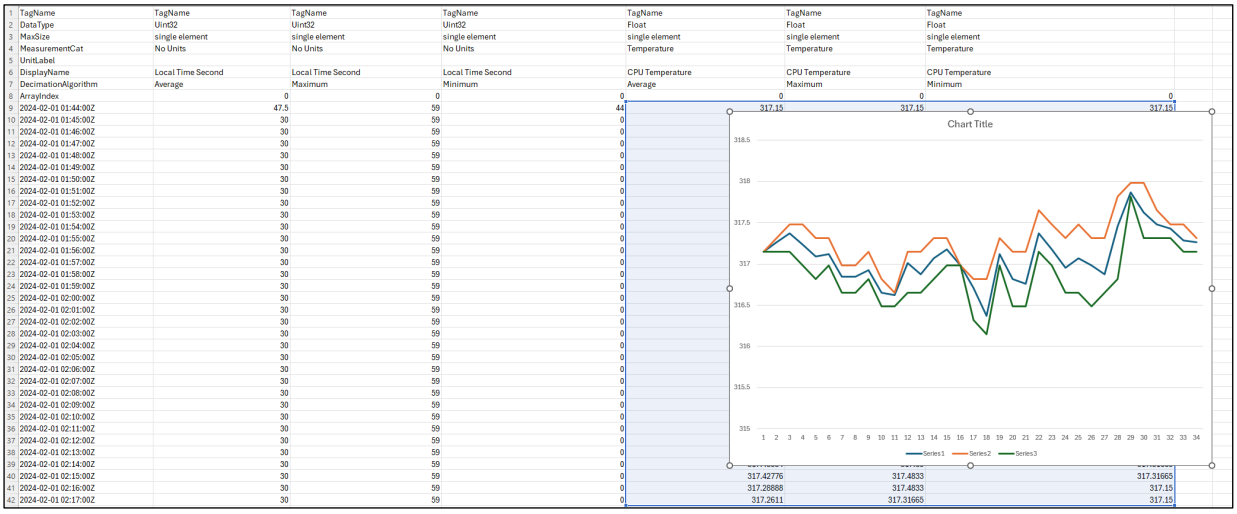
In this section, we will write the audit log data to a .csv report.

Tabbed Screen	Functions	Task Details
Export Options	Specify the folder where the export file will be exported.	By default, all log output files include header rows for export dates, device information, and asset information. Click the Select Folder button and browse to the location where you want the .csv report to be saved.
Do Export	Write Audit Log records to a .csv file.	Click Do Export to generate the log file. The audit output filename will follow this format: `export_auditlog_YYYYMMDD_HHMMSS.csv` `YYYYMMDD_HHMMSS` is the date and time when the file was written. Click the Click here hyperlink to open the output folder where the exported report resides.

6.14.5 Create a Trend Chart from CSV Report

The .csv report format makes it easy to analyze data and display it as a trend chart.

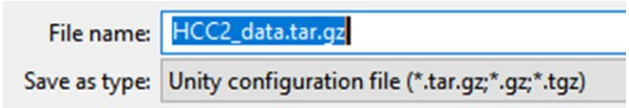
In the example image below, a user exported three data columns containing the minimum, maximum, and average values of a HCC2 data point and then produced a custom trend chart.



6.15 IMPORTING AND EXPORTING FILES

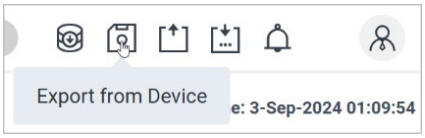
In addition to building your HCC2 configuration from the selections described in Section 6, you can use the icons in the top right corner of the Unity Edge interface to import and export configuration files and export data logs.

When you export configuration settings, they are stored in a file with a .tar.gz format. By default, the filename prompt will be config.tar.gz or HCC2_data.tar.gz, but you can assign a unique filename to meet your needs.

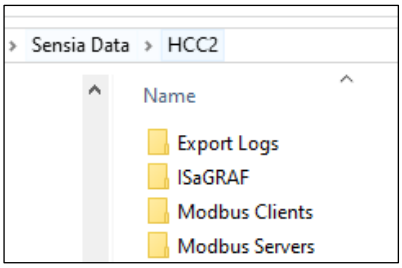


6.15.1 Export Configuration from Device

The Export Configuration from Device button allows you to export the most recently deployed configuration from the HCC2. Click the button shown below to initiate an export and enter a file name and storage location at the prompt.

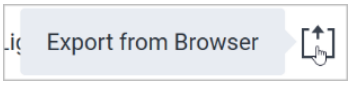


For ease in locating your HCC2 export files, consider building a folder structure on your PC similar to the one below:



6.15.2 Export Configuration from Browser

Unlike the Export from Device option, the Export from Browser selection includes any nondeployed changes that you have made in the browser. Click the button shown below to initiate an export and enter a file name and storage location at the prompt.



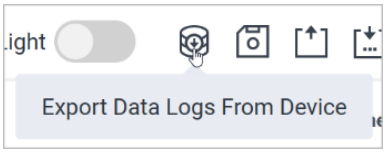
Nondeployed selections are lost when the browser is closed. This export function is especially useful for saving an incomplete configuration—at the end of a workday, for example—in a format that you can import to complete your work and deploy to the HCC2.

6.15.3 Import Configuration

Use the Import Configuration button to select a previously saved configuration file to replace the existing configuration stored within the browser. The browser will update instantaneously. However, you must deploy the new settings using the Deploy wizard to write them to the HCC2. Otherwise, the settings will be lost when the browser is closed.

6.15.4 Export Data Logs from Device

The Export Data Logs from Device button is a quick link to the Export Log screen of the Data Logger. It contains features for creating, downloading, and exporting user log files to your local drive.



Section 7: HCC2 Operations

This section describes how to monitor your configured assets in the Unity Edge browser interface. Most of these tasks originate in the Operate menu described in section 3.2, Operate Menu, page 32.

7.1 MONITORING THE DASHBOARD

The Operate Dashboard provides an overview of the HCC2 status, health and alarms using graphical tiles and tables. By default, the Unity Edge software opens to this view when a connection is made with an HCC2.

7.1.1 Device

The Device tile includes both user-configurable and static device information to allow you to quickly identify connected HCC2 devices.

Label	Description	
Asset Name	The user-defined asset name, displayed as the title of this tile. To edit, see Deploy > Device > Device Information.	
Description	The user-defined asset configuration. To edit, see Deploy > Device > Device Information.	
System	The device operating system version number (the first three digits – x.x.x – identify the OS version loaded). If you are unable to connect to Unity Edge, the same OS version information is available in the Edge Package Manager.	
Model	The device model number (non-editable)	
	50365260-2001	QRATE, HCC2, Hyperconverged Edge Controller Base Model
	50369741-2001	QRATE, HCC2, Hyperconverged Edge Controller with Wi-Fi and LTE
	50365260-2002	QRATE, HCC2, Hyperconverged Edge Controller Base Model, RTU plus App Enablement
	50369741-2002	QRATE, HCC2, Hyperconverged Edge Controller with Wi-Fi and LTE, RTU plus App Enablement
Serial	The device's unique serial number (non-editable)	
Deployment Status	Status of the last attempted deployment	

7.1.2 Live Data

The Live Data tile shows the number of data points with particular OPC quality codes, as defined below.

OPC Criteria	HCC2 Criteria	HCC2 Description & Application Usages	Glyph
Uncertain [Non-Specific]	Data Stale	The value is known to not be updated within a watched time period (Stale). CP: Stale Server Data. Modbus: Data query age has exceeded the stale alarm, but the remote server has not yet qualified as lost. Event Manager: Event contains a condition that is watching a data point that has reported this state. No higher priority quality code present in all event conditions.	
Uncertain [Non-Specific] (Constant)	Frozen	The value does not change during a watched time period. CP: Frozen	

7.1.3 Subdevices

The Subdevices tile displays the number of configured and connected subdevices.

7.1.4 System Health

The System Health tile includes real time graphical indicators of key system parameters for monitoring the operation of the HCC2 hardware.

Parameter	Range	Meaning
CPU Load	0-100%	Percentage of CPU processing power in use
Memory	0-100%	Percentage of memory in use
Persistent Storage	0-100%	Percentage of persistent storage in use
CPU Temperature	-40-100 Deg C	Temperature of the HCC2 main processor

7.1.5 Applications

The Applications tile lists the installed and running applications on the device and an icon that changes depending on the status of the application.

Icon	Meaning
Grey Question Mark	Installed with no status (may indicate the need for troubleshooting)
Green Power Button	Application is running
Red Power Button	Application is stopped

7.1.6 Active Alarms

The Active Alarms tile displays the current active alarms on the HCC2, including the severity level and duration of alarm. For more detailed alarm management options, see section 6.12, Configuring User Alarms, page 65, and section 7.6, Monitoring Alarms, page 85.

7.2 MONITORING THE HCC2 DEVICE

7.2.1 System Information

The Device > System Information page provides a summary of important software and hardware parameters described below.

System Version

Parameter	Description
OS Build Version	Version of the operating system running on the HCC2 CPU board.
OS Build ID	Reference for the particular build / compilation that was run to create the operating system image running on the HCC2 CPU board.

Hardware Information

Parameter	Description
Manufacturer	Static manufacturer name for reference, Sensia LLC.
Product Family Name	Static descriptive name of the product
Product Name	Static market name of the product
Model Number	Model number; differs based on wireless vs. non-wireless models

Parameter	Description
Assembly Version	Assembly version for internal auditing purposes
Serial Number	The unique serial number of the connected HCC2 device.
CPU Board Hardware Version	CPU board hardware version for auditing purposes
CPU Board Serial Number	CPU board serial number for auditing purposes
CPU Board Part Number	PN of CPU board for auditing purposes
Hardware Identifier	A unique identifier for the HCC2

7.2.2 System Status

The Device > System Status page provides a granular, numerical and real time display of various important system parameters described below.

Parameter	Description
CPU and CPU Core Temperatures	Overall and per-core temperature measurement of the CPU
CPU Usage	Overall and per-core usage of the CPU, in percentage
Disk Usage	Usage of various data volumes on the HCC2
Memory Usage	Shows available and used memory on your HCC2

7.2.3 Network Status

The Device > Network Status page provides a summary of the current real time network settings by interface. For a description of what these parameters mean and how to configure them, see Section 2: Connecting to Unity Edge, page 17.

In addition, the firewall port status is shown for each port, with checkboxes next to the name of the port. If the firewall allows that particular port, it will be marked with a tick.

Status is shown for all four Ethernet ports. ETH-3 and ETH-4 share the same configuration.

Ethernet Status

Parameter	Description
Enabled	A blue checkmark indicates the interface is enabled. A blank box indicates a disabled status.
Mode	Indicates whether the interface is configured with a static IP address, or a Dynamic (DHCP) IP address.
Assigned IP Address	The current IP address assigned to the interface.
Assigned Subnet Mask	The current subnet mask assigned to the interface.
Assigned Default Gateway	The current default gateway assigned to the interface.
Assigned Primary DNS	The current primary DNS server assigned to the interface.
Assigned Secondary DNS	The current secondary DNS server assigned to the interface.
Link Status/Connection State	The status of the physical and logical layer. Text in the status box will show which of the layers are functional for each interface (ETH-1 & ETH-2). For ETH-3 & ETH-4, the text will show which of the links are connected.

Wireless Status

Parameter	Description
Enabled	A blue checkmark indicates the interface is enabled. A blank box indicates a disabled status.
Installed	Indicates whether the Wi-Fi and/or Cellular modem is installed in the device
SSID (Wi-Fi Only)	Service Set Identifier, the name assigned to a Wi-Fi network when a router is set up
Access Point Name (Cellular Only)	Name of the configured access point (APN)
Access Point IP Address	The current IP address assigned to the interface
Mode (Wi-Fi Only)	Indicates whether the interface is configured in 'Infra' or 'Ad-hoc' mode
Access Point IP Address	The current IP address assigned to the interface
Signal Strength	Percentage strength of the wireless signal
Link Status	Shows whether an active link is established
IMEI (Cellular Only)	IMEI number of the SIM card in the modem
FCCID	Unique number assigned to electronic devices by the FCC
SNR (Cellular Only)	The signal-to-noise ratio of the given signal
RSRP (Cellular Only)	The average power received from a single Reference signal. Its typical range is -44dbm (good) to -140dbm (bad).
RSRQ (Cellular Only)	The quality of the received signal. Its typical range is -19.5dB (bad) to -3dB (good)
RSSI (Cellular Only)	The entire received power including the wanted power from the serving cell as well as all unwanted co-channel power and other sources of noise

See the chart below for RF condition signal strengths to ensure that your antenna is well positioned and that your Cellular signal is going to be consistent.

	RSRP (dBm)	RSRQ (dB)	SINR (dB)
Excellent	>= -80	>= -10	>=20
Good	-80 to -90	-10 to -15	13 to 20
Mid Cell	-90 to 100	-15 to -20	0 to 13
Cell Edge	<= -100	<= -20	<= 0

7.3 MONITORING IO CONNECTIONS

Screens for monitoring the HCC2's inputs and outputs can be found in the Operate > Integrated I/O menu, and are presented below by IO type, as they are listed in the Unity Edge interface.

7.3.1 IO System

The IO System page provides a summary of important IO parameters. Parameters that are not self-evident by name are described below.

IO Board Versions

Parameter	Description
Main Image Revision	Version of the currently installed firmware on the IO board. The HCC2 will verify that this is the expected version.
Boot Loader Revision	Revision level of the Boot Loader.

Parameter	Description
Expected Main Image Revision	The loaded HCC2 software bundle includes the required version of the IO board firmware. This field indicates the version number of this firmware. If required, the software will update the IO board firmware.
IO Firmware Validated	A checkmark should appear following a firmware upgrade, indicating the IO Board is functional and executing the required IO board firmware. If the checkmark does not appear, you do not have a current version of firmware. Contact technical support for assistance.

IO System State

Parameter	Description
IO Manager State	Displays the current state of the IOB Manager. If operating normally, the state will display as IO Operational.
Uptime	The number of seconds the IO system has been operational.
IO System Time	Local time.
SNTP State	The IO system synchronizes to the core HCC2 via SNTP for accurate timestamps. Ensure that this is synchronized if you are using your IO system.
Reset IO System	This button resets the IO system, causing the IO Manager State to restart and the Uptime count to restart at zero.

IO System Device Memory

Parameter	Description
IO General Available Memory (%)	Memory used for subdevices, Ethernet IP mapping, etc., not including ISaGRAF memory
ISaGRAF Available Memory (%)	Memory used by ISaGRAF code, variables, and any other overheads related to ISaGRAF.
IO General Available Memory (Non-ISaGRAF)	IO General memory available in the system for subdevices, Ethernet IP mapping; expressed in kibibytes (kiB). A kibibyte is a binary unit of memory equal to 1024 bytes, not 1000 bytes.
ISaGRAF Available Memory	Memory in the IO system available for ISaGRAF applications.
ISaGRAF Largest Available Memory Block	A consecutive block of memory required to download ISaGRAF programs. If the ISaGRAF memory becomes fragmented after many operations, click the Reset IO System button to restart the IO system and defragment the memory.
IO System Total Memory	Total IO system memory, not including ISaGRAF memory.
ISaGRAF Total Memory	Total ISaGRAF memory.

Supply Power Status

Parameter	Description
Power Input A Okay (checkbox)	Checked when Power Input A has a voltage applied to it in the acceptable operating range.
Power Input B Okay (checkbox)	Checked when Power Input B has a voltage applied to it in the acceptable operating range.
Supply Power Voltage	Measured input voltage. This will be the higher of the two voltages applied to Power Inputs A and B.
Supply Power Current	Measured electrical current drawn from Power Inputs A or B.
Supply Power Wattage	Computed power consumption from Power Inputs A and B combined.
Rail Voltage 5V	A diagnostic measurement of the internal 5V power supply.

Parameter	Description
Rail Voltage 3V3	A diagnostic measurement of the internal 3.3V power supply.
Rail Voltage 1V2	A diagnostic measurement of the internal 1.2V power supply.

Device PCB Status

Parameter	Description
CPU Usage	The current value (percentage) of IO Board system CPU usage
CPU Temperature	Temperature of the IOB CPU
Board Temperature	Temperature of the IOB circuit board system temperature monitor

7.3.2 Digital Inputs and Outputs

Digital Inputs States

Parameter	Description
DI Input State (Channels 1 through 8)	A blue checkmark in the checkbox indicates the input is energized. A gray checkbox indicates the input is de-energized.
DI Counter Value (Channels 1 through 8)	The number of times the input has changed status.

Digital Input/Output States

Parameter	Description
DIO Input State (Channels 1 through 8)	A blue checkmark in the checkbox indicates the input is energized. A gray checkbox indicates the input is de-energized.
DIO Output State (Channels 1 through 8)	A blue checkmark in the checkbox indicates the output is energized. A gray checkbox indicates the output is de-energized.
DIO Output Mode (Channels 1 through 8)	Digital Input, Digital Output, or Pulse Width Modulator
DIO Output Count (Channels 1 through 8)	The number of times the output has changed status.

7.3.3 Analog Inputs and Outputs

Analog Inputs and Outputs

Parameter	Description
AI Value Percentage (Channels 1 through 8)	—
AI Value EU (Channels 1 through 8)	—
DI Input State (Channels 1 through 8)	A blue checkmark in the checkbox indicates the input is energized. A gray checkbox indicates the input is de-energized.
DI Counter Value (Channels 1 through 8)	The number of times the input has changed status.

7.3.4 ISaGRAF Resources

ISaGRAF Resources #1 Status

Parameter	Description
Resource Name (Resources 1 through 4)	Name of the resource.
Resource 1 Number (Slave) (Resources 1 through 4)	Unique number identifying a resource within a project.
Cycle Date Stamp	Timestamp of the beginning of the cycle in milliseconds.
Programmed Cycle Time	The cycle time for the device in milliseconds. When configured to Trigger Cycles, if a cycle is completed within the cycle timing period, the system waits until this period has elapsed before starting a new cycle. The cycle consists of scanning the physical inputs of the process to drive, executing the program organization units (POUs) of the resource, then updating physical outputs.
Current Cycle Time	The cycle time of the last application cycle, in milliseconds.
Max Detected Cycle Time	The longest period of time used for a cycle since last start, in milliseconds.
Number of Detected Cycle Time Overflows	The number of cycles having exceeded the programmed cycle time.
Scan Counter	Input scan counter since last start.
Cycle Counter	Number of cycles since last start.
Resource Execution Mode	Resource execution mode. Possible modes are: -4: Stopped in stepping mode after bound check exception -3: Stopped in stepping mode after division by zero exception -2: Stopped in stepping mode after exception -1: Fatal error 0: No resource available 1: Stored resource available NOT USED (CMG) 2: Ready to run 3: Running in real time 4: Running in cycle by cycle 5: Stopped from encountering a Sequential Function Chart (SFC) breakpoint 7: Stopped while in stepping mode
Resource Warning Code	Code of the last emitted warning message. Unsigned 32 Integer.
Resource Warning Argument	Argument of the last emitted warning message. Unsigned 32 Integer.
Resource Warning Component Name	Name of the component (ex: I/O driver) that emitted the last warning.

7.3.5 HART Channels

The HCC2 supports up to four HART channels. To monitor the operation of HART variables and verify configuration for any one of the four channels, click the desired channel at the top of the HART Channels page (HART Analog In 1… HART Analog In 4). The title of the selected channel is highlighted in blue for easy recognition.

HART Process Variables (Analog Inputs 1 through 4)

Parameter	Description
PV	Primary variable
SV	Secondary variable
TV	Tertiary (third) variable

Parameter	Description
FV	Quaternary (fourth) variable
PV Units Code	HART Units code is provided by the remote HART transmitter. The code will follow HART Standard: HCF_SPEC-183, FCG TS20183, section 5.2 Table 2, Engineering Units Codes (page 68).
SV Units Code	
TV Units Code	
FV Units Code	
Analog Current	The measured analog being transmitted by the HART device.

7.4 MONITORING SUBDEVICES

The Subdevices page in the Operate menu allows you to monitor all configured and deployed subdevices attached to the HCC2.

The subdevices are displayed in a tree format on the left-hand side of the page, with an icon next to each subdevice showing their connection status. The Subdevice Instance column details the Instance Name, Catalog Number, and Slot Number (if applicable) of the device.

Clicking on the device brings up further live diagnostics for each subdevice.

- Assembly data will show the value of the Assembly data that was configured in the system.
- Connection Status provides information from the device which could be useful in identifying disconnected/unconfigured devices.
- Explicit Statistics is not yet supported by the HCC2.

To refresh the statistic counters, click the Reset Statistics button.

The Live Data page can be used to view the user-configured data points for each subdevice.

7.5 MONITORING LIVE DATA

The Live Data page is a critical tool for analyzing HCC2 operations in real time. Every data point published on the data bus is visible in this page, allowing you to check production values, configuration, diagnostics and find/review the state of all data points available in the system. It updates continuously as values update in real time. Data points are only available on this page after they have been published and/or after a state change.

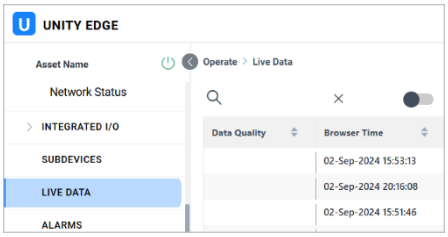
7.5.1 Live Data

Live data are arranged in a table, with each column representing information about a data point. Hover your mouse over a cell to view a tooltip for more information. The contents of the table are sorted by the timestamp with most recent values at the top.

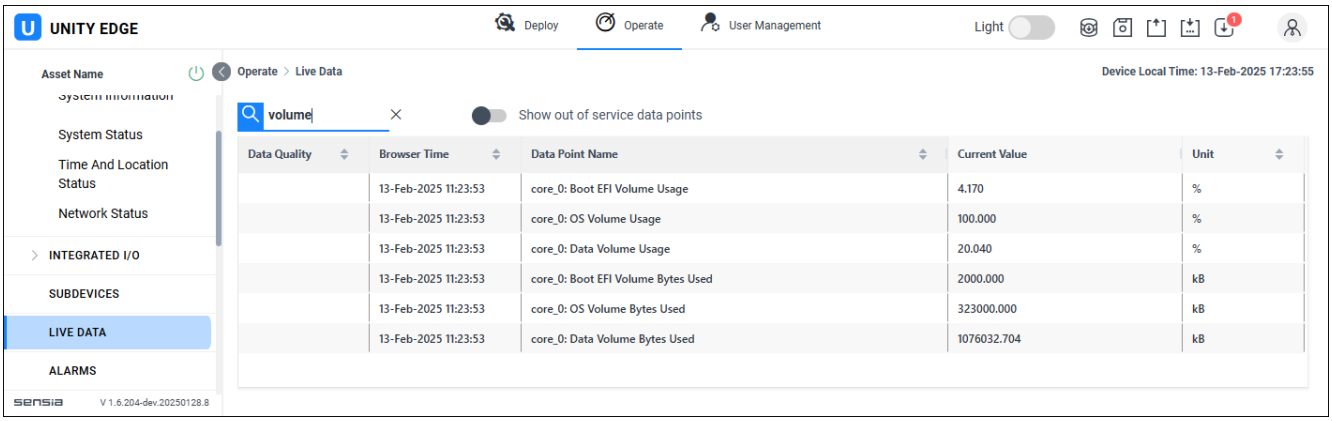
Column	Description	Tool Tip
Data Quality	An icon representing the data quality.	The OPC quality code that the icon represents.
Browser Time	The time value stored in the message, converted to your time zone and presented in a user-selected date format.	Still in the local time zone, formatted in default date format.
Data Point Name	The user-readable ‘display name’.	The underlying full data point name sent on the message bus.
Current Value	The data point value, converted to the selected unit of measure.	The entire contents of the data point value, useful for arrays, long strings, and JSON.
Unit	The selected unit of measure for the displayed value	Full data point metadata.

7.5.2 Live Data Filtering

An active system can contain hundreds, or even thousands of data points, making it difficult to find data by scrolling alone. You can vastly improve this navigation by filtering the contents of the table using the search field at the top of the Live Data page.



This field will filter the list to only data points containing the entered text.



By default, live data displays do not include named data points without any valid updates since system start. To include these out of service data points in your search, toggle the Show out of service data points button to the enabled position.

7.6 MONITORING ALARMS

Unity Edge provides easy access to current and historical alarms.

You can view active alarms ranked by severity on the Operate > Dashboard screen, but the Operate > Alarms screen is the best place to monitor all alarms. In this section, we will explore the various ways you can view and manage these alarms.

Configured alarms are presented in two tabs, Alarms and Alarm History.

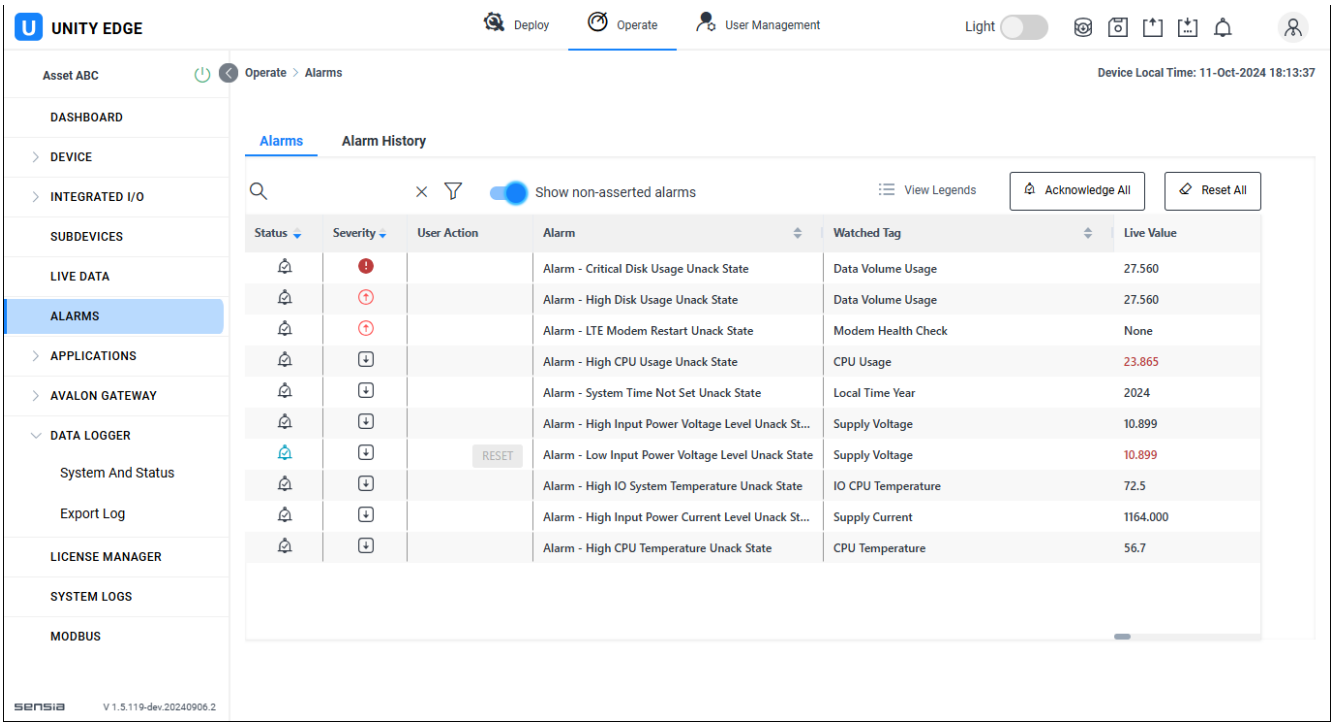
See also section 6.12, Configuring User Alarms, page 65, for details on configuring alarms.

7.6.1 Current Alarms

From the Operate > Alarms screen, you can monitor the status of configured alarms, acknowledge active alarms, and reset alarms after alarm conditions are no longer met.

By default, only alarms that are active (alarm condition is met) and/or unacknowledged are displayed. Alarms that are inactive (alarm condition is not met) are hidden.

To view all configured alarms regardless of their alarm state, toggle the Show non-asserted alarms button to the enabled position.



Note	When Show non-asserted alarms is enabled, the view will include critical system alarms that are automatically configured for all applications and cannot be deleted. To view only these alarms, select “core” from the Filter menu. This filter is applicable only when Show non-asserted alarms is enabled.

Alarms are sorted in this order by default:

- Bypassed and Unacknowledged
- Unacknowledged and Asserted
- Acknowledged and Asserted
- Bypassed and Acknowledged
- Unacknowledged and Not Asserted
- Acknowledged and Not Asserted

Customize the View

You can customize the view three ways:

- select an alarm category from the Filter icon menu at the top of the screen
- enter a descriptive word in the search box (magnifying glass icon) to filter alarm display names
- sort contents by any column with a sort indicator (Status, Severity, Alarm (name), Watched Data Point, Unit, Start Time, End Time, or Duration)

Interpret Alarms

Colored icons (Figure 7.1, page 87) identify alarm status and severity. Click the View Legends link in the top right corner of the screen to view a list of icons and their definitions.

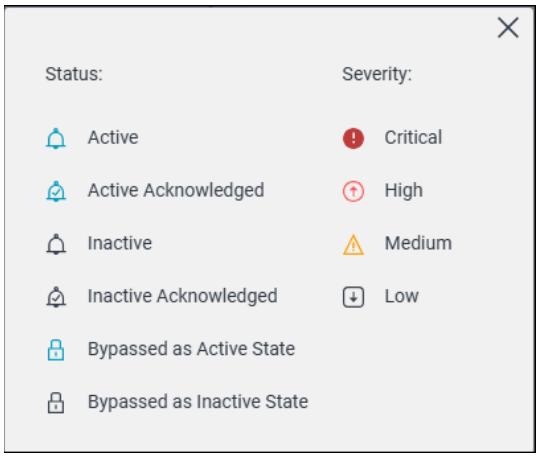


Figure 7.1—Alarm icons

You can also view an alarm definition in a tooltip by hovering your mouse over an icon in an alarm record.

Alarm properties displayed in the alarm table are defined below. When an alarm condition is met, the Live Value and Alarm Condition indication changes from black to red.

Please note that the alarm table contains hidden columns. Use the scroll bar at the bottom of the window to view all data.

Column	Description
Status	An icon indicating the status of the alarm. This is a combination of current health status (active/inactive) and a quality assessment such as good, bad input, bypassed etc. For status definitions, see the View Legends link.
Severity	An icon reflecting the severity assessed for the condition when the alarm was created. Severity indicators include, from least to greatest severity, Notification, Low, Medium, High and Critical.
User Action	If a user action is possible, it will be indicated here. Examples include resetting an underlying latch that is inhibiting a process or acknowledging an alarm that is no longer active but is configured to remain visible until explicitly cleared.
Alarm	The user-readable display name given to the alarm (based on data point).
Watched Data Point	Name of the data point that is being alarmed.
Live Value	Current value of the data point. Displays in red when alarm condition is met.
Value at Assertion	The value of the alarm when the alarm was triggered. Displayed in the user-selected unit of measurement for that data type.
Alarm Condition	The condition or threshold that was exceeded, thus causing the alarm to become active. Displays in red when alarm condition is met.
Unit	The unit of measure associated with the alarm value/condition.
Start	The time the alarm became active.
End	The time the alarm became inactive (if no longer active).
Duration	The span of active alarm time between Start and End times.
Adjust	A link to the User Alarm Configuration page.
Bypass Alarm	Optional setting for bypassing an alarm output for a user-specified period.

Acknowledge or Reset Alarms

You can acknowledge or reset an alarm by clicking ACK or RESET in the User Action column of a configured alarm. Alternatively, you can “acknowledge all” or “reset all” current alarms in one click using the Acknowledge All button or Reset All button in the top right corner of the screen.

In Unity Edge, a user acknowledges an alarm to indicate that the alarm has been observed and will be investigated.

Depending on how an alarm is configured, you may have to manually acknowledge it or it may auto-acknowledge when the condition (event) that triggered the alarm condition has passed (when you enable this feature).

A user can acknowledge an alarm at any time. It will not become unacknowledged until it is reset and then recurs.

A user resets an alarm to clear it from the system. An alarm can be reset only when alarm conditions are not met. Attempts to reset an alarm before alarm conditions have passed will be rejected. Resetting an alarm that has been acknowledged will remove it from the active Alarms list and add it to the Alarm History view.

The behavior of I/O associated with the alarm following an acknowledgement or a reset may vary, depending on the alarm’s configuration, as shown in the Alarm Configuration Examples, page 66.

7.6.2 Alarm History

Historical alarm data retrieved from the Data Logger are presented on the Alarm History tab when the Operate > Alarms menu is selected.

This display defaults to current day activity for all applications and all alarm severity levels.

To customize your selection of historical alarm data,

1. Apply a filter to specify alarms by application, if desired.
2. Apply a filter to specify alarms by severity, if desired.
3. Enter desired start and end times in the fields provided. Dates and times must be entered in this format: DD:MMM:YYYY HH:MM:SS
4. Click the Get from device button to update the Alarm History grid with historical alarms matching your filter and date/time specifications.

The data are arranged in a table, with each row presenting information about a past alarm state change. You can sort contents by any column with a sort indicator (Status, Severity, Alarm [name], Unit, or Timestamp).

The properties displayed in the alarm history table are defined below. Hover your mouse over an alarm to view a tooltip for more info.

Column	Description
Status	An icon indicating the status of the alarm when the change in state was recorded. This is a combination of if the alarm was active and its status such as good, bad input, bypassed etc. For status definitions, see the View Legends link.
Severity	An icon reflecting the severity assessed for the condition when the alarm occurred. Severity indicators include, from least to greatest severity, Notification, Low, Medium, High and Critical.
Alarm	The user-readable display name given to the alarm.
Value at Trigger	The value of the alarm when the state change occurred. Displayed in the user-selected unit of measurement for that data type.
Alarm Condition	The condition or threshold that was exceeded, thus causing the alarm to change state.

Column	Description
Unit	The unit of measure associated with the alarm value/condition.
Timestamp	The time the alarm changed state.
Record Note	A description of what triggered the state change.

Export Alarm History

From the Alarm History screen, you can export historical alarm data which can then be converted to .csv format for sharing with others.

To export historical alarm data, click the Export History button. You will be redirected to the Data Logger menu to complete your export selections. See section 6.14, Export Data Logs, page 69, for complete instructions.

7.7 MONITORING DATA LOGGER SYSTEM AND STATUS

You can monitor Data Logger activities at the global, event/alarm, data point, and trend levels. Under the Operate tab, go to Data Logger > System and Status. You can view logging details such as capacity level percentages, average number of disk writes, number of stored records, watched tags, database disk size, etc.

To assign and configure tags for the user log, refer to section 6.13 Configuring User Logs through Data Logger, page 67.

7.8 LICENSE MANAGER

Licenses are used to control applications on your HCC2 device. While you do not need a license to run “core” factory-installed applications supporting RTU functionality, all edge applications require a license.

The License Manager allows you to see the status of installed licenses as well as to add new licenses.

7.8.1 Application Enablement

To load a new custom edge application, you must first install an HCC2 Edge App Enablement license. Your HCC2 will then accept and load other Sensia-signed applications.

Note	If you ordered your HCC2 with Edge App Enablement pre-installed at the factory, the HCC2 Edge App Enablement license will appear on your License Manager screen as shown below.

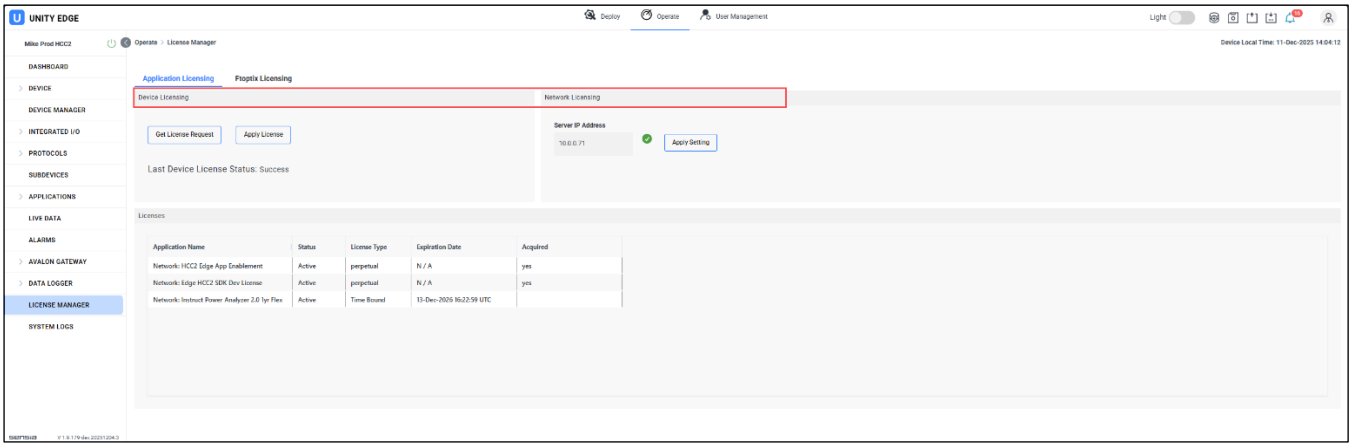


Figure 7.2—License Manager screen

You have two options for managing application licenses— device licensing and network licensing—as indicated by the panels at the top of the License Manager screen.

A device license is bound to a specific HCC2.

A network license, rather, is bound to a CmContainer on a server. With a network license enabled, many HCC2 devices can connect to a central server to acquire a license. Sensia uses WIBU CodeMeter software to set up remote network servers and manage the licenses stored on them.

7.8.2 Network Licensing

Network licensing is an ideal choice for users with multiple HCC2s who want to manage licenses from one location and would benefit from the ability to transfer licenses between devices. Unlike the device licensing process which requires a physical file exchange with Sensia to activate a license, network licensing is largely self-managed once Sensia issues the licenses purchased. You only need to maintain communication between your devices and the remote server to enable/disable licenses for any HCC2 device.

To obtain a network license for Edge App Enablement or a custom Edge application

1. Contact your Sensia sales representative or submit your request to Sensia Customer Care at this web page: https://sensiaglobal.com/Customer-Care.

2. When payment is confirmed, Sensia will attach the license to an email.

Setup of a remote network license server involves three basic steps:

1. Install the WIBU CodeMeter Runtime kit on a Windows PC.
2. Create a new remote network license server using the CodeMeter interface. See CodeMeter Network License Server - Wibu-Systems for details.
3. Download to the licensing server any licenses purchased from Sensia.

Once the server is set up, you can apply a license to a device by pointing the device to your server in the License Manager screen in Unity Edge. See Obtaining a License from a Network Server for details.

The license server allows you to centrally host activations for applications on the HCC2. From Unity Edge, you can connect to the remote license server and poll activations for the apps installed locally. The HCC2 License Manager will browse the remote server for activations valid for the device and automatically check them out.

Rehosting a License

At any time, you may have a combination of HCC2s with local licenses and HCC2s with licenses enabled from a remote network server. If you find a need to rehost a license, Sensia can help. For example, if you have an HCC2 that is out of commission and you wish to renew the license issued to it for use with a different HCC2, Sensia can rehost the license to allow you to manage it via a remote network server. To request rehost support, send an email request to licensing@sensiaglobal.com and a member of the Sensia support team will respond to confirm your specific needs.

Obtaining a License from a Network Server

When licenses are loaded into a remote network server, you can proceed with configuring an HCC2 to use a server from the License Manager menu in Unity Edge.

1. Open the Operate > License Manager screen in Unity Edge.
2. Enter your server IP address. If the IP address is confirmed as valid, a green checkmark will appear next to the IP address field.
3. Click Apply Settings.

Licenses will appear by application name in a list at the bottom of the screen. The license status, type, and expiration date (if applicable) are also displayed. Licenses for applications running on the HCC2 will be applied.

7.8.3 Device Licensing

To obtain an Edge App Enablement license or a separate custom Edge application license, perform the following steps:

1. Contact your Sensia sales representative or submit your request to Sensia Customer Care at this web page: https://sensiaglobal.com/Customer-Care.
2. When payment is confirmed, Sensia will email an order confirmation and a request for a serial number.
3. Return the email with the serial number for your HCC2 (as shown on the Operate > Device > System Information screen of Unity Edge). Sensia will match this number to a manufacturing record and generate a unique, signed Edge App Enablement license.
4. Sensia will attach the license to a second email including instructions for installing the license.

To install the license,

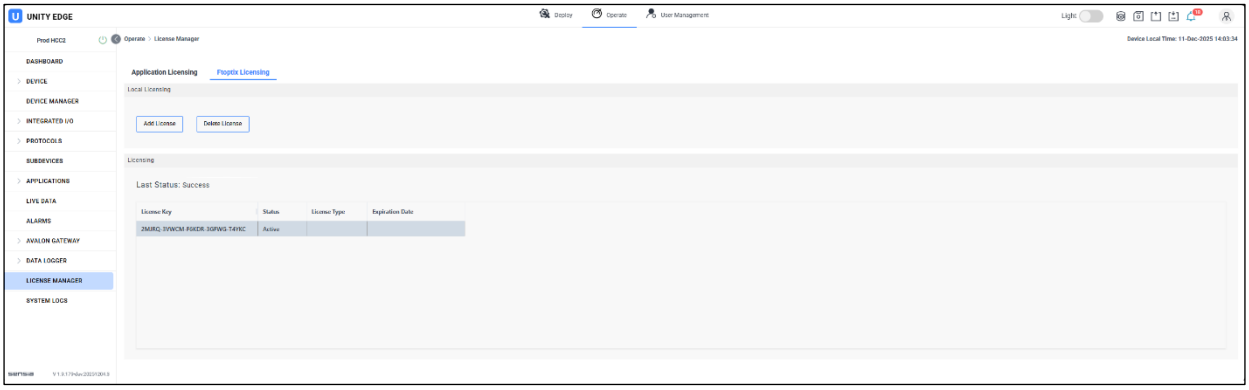
1. Save the license file with a WibuCmRaU extension to your PC.
2. Open the Operate > License Manager Status screen in Unity Edge and click Apply License.
3. At the dialog prompt, map to the saved license file and click Open.
4. When the upload completes, the license will appear in the License Manager table by Application name. The license status, type, and expiration date (if applicable) are also captured.

In the event Sensia is unable to verify your unit by the serial number you provide, Sensia may ask you to provide a license request file. You can generate this file from Unity Edge as follows:

1. From the Operate > License Manager Status screen, click Get License Request. An encrypted file with a WibuCmRaC extension (for example, HCC2-1218652330822.WibuCmRaC) will be generated instantaneously and stored in your PC's Downloads folder.
2. Email the encrypted file to Sensia.
3. Sensia will process the signed license and return it by email.

7.8.4 FactoryTalk Optix Licensing

FactoryTalk Optix, a data visualization tool supplied by Rockwell Automation, is available for use with some custom HCC2 edge applications. If a FactoryTalk Optix license is purchased, accompanying license information will appear when the FactoryTalk Optix Licensing tab is selected. FactoryTalk Optix is available only with the purchase of an edge application. For details, see Section 12: FactoryTalk Optix, page 190.



7.8.5 Other Custom Edge Licenses

Sensia will issue separate licenses for each edge application purchase.

Contact your Sensia sales representative for more information on the Edge App Enablement license or individual edge applications.

7.9 MONITORING SYSTEM LOG

The Operate > System Logs screen gives you access to the logs generated by the system or user applications running on the device. These logs are automatically loaded chronologically when the page loads. Click Refresh to refresh the load from the device.

Only logs from the past 24 hours are shown because logs are archived daily in the device. To view archived logs, click the Check archived logs button provided.

7.9.1 Filtering

To filter logs, type the text you wish to filter on in in the empty fields at the top of the Logger Name, Log Level and/or Log Messages columns and click Enter on your computer keyboard.

To clear the filter, delete the text from the filter fields and click Enter on your computer keyboard.

Alternatively, you can click the Filter icon to perform more complex filtering using and/or commands and two text strings. Click Apply to activate the filter. Click Reset to clear the filter.

7.9.2 Export

To export loaded logs in CSV format logs, click the Export button. If a filter is applied at the time of export, only filtered logs will be exported.

7.10 MONITORING MODBUS PORTS, SERVERS, AND CLIENTS

The Operate > Modbus page provides statistics for each Port, Server, and Client, each in a separate tab.

These statistics include status (enabled/disabled), error counts, throughput, and active connections. You can reset the accumulated statistics using the Reset Stats button provided in the User Action column, if desired.

7.11 PROVISIONING HCC2 AND MONITORING AVALON GATEWAY

By default, the HCC2 contains an instance of the Avalon Gateway application. Using this application, you can connect and integrate the HCC2 device with the Avalon platform. This process consists of pairing the HCC2 device with a compatible Avalon data provider and provisioning the HCC2 within the Avalon framework (Figure 7.3, page 93).

After you pair and provision the HCC2 device, you can

- monitor HCC2 status in the Avalon environment
- monitor Avalon Gateway statistics and file transfer status through the HCC2 Unity Edge interface

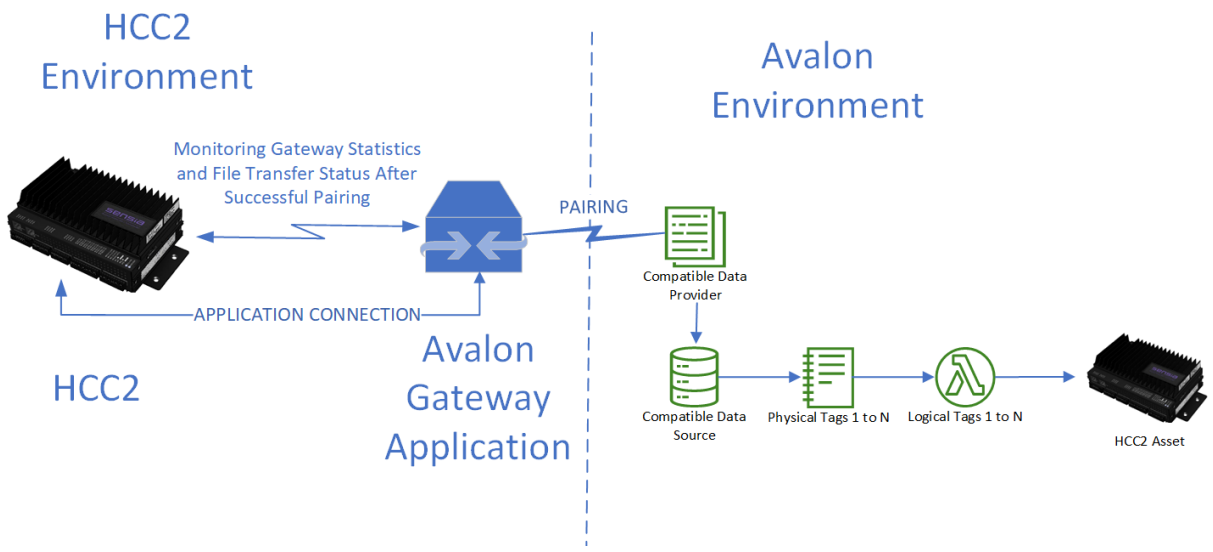


Figure 7.3—Overview of HCC2 to Avalon connection and data flow

7.11.1 Prerequisites

Important Before attempting to provision the HCC2 device, verify that your corresponding Avalon instance is configured with a compatible data provider and supporting components. Without these, your provisioning effort will fail. If in doubt, check with your Avalon administrator.

The following parameters must be defined in your Avalon instance:

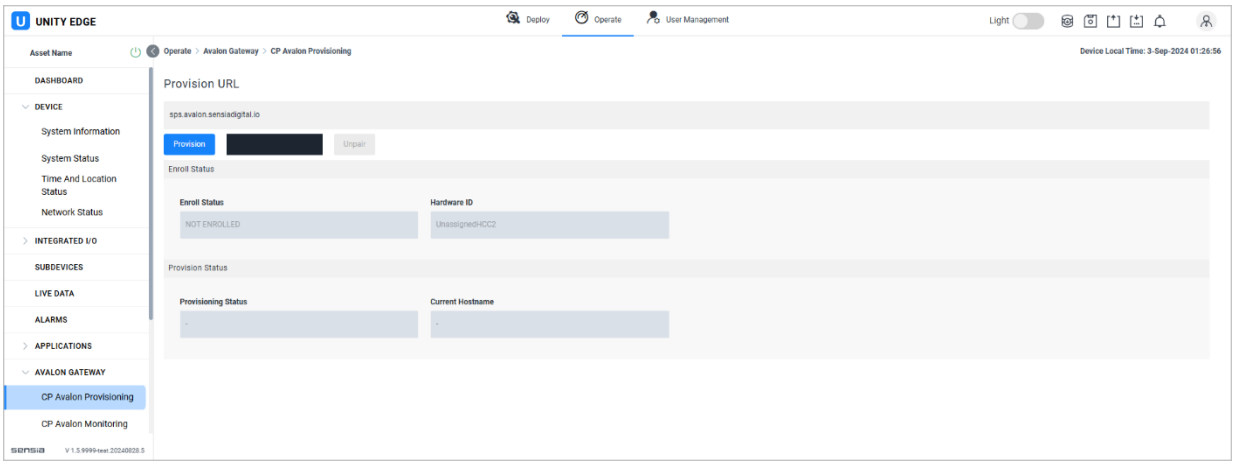
- Customer account
- Data provider that supports the Avalon Gateway
- Data source and asset templates that contain the physical and logical tags
- Compatible data source or source(s)
- HCC2 asset

7.11.2 Provision the HCC2 Device within Avalon

To provision the HCC2 device within Avalon, click Operate > Avalon Gateway > CP Avalon Provisioning.

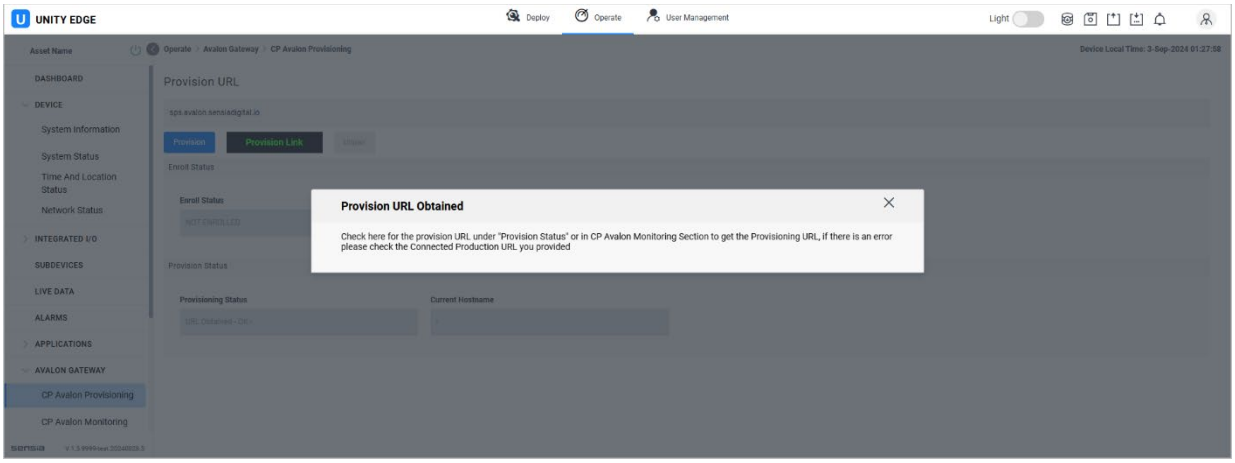
Provision the HCC2 as follows:

1. Type or paste the URL of the Avalon instance (sps.avalon.sensiadigital.io) into the Provision URL field.

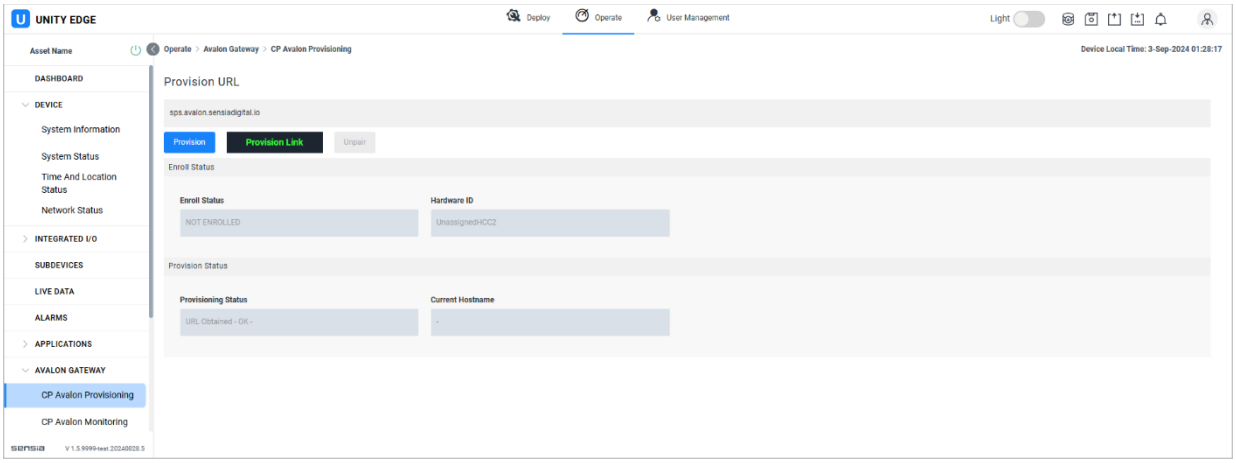


The Enroll Status indicates whether your HCC2 device is validated and/or has been provisioned. *NOT ENROLLED* indicates that the device is not currently provisioned.

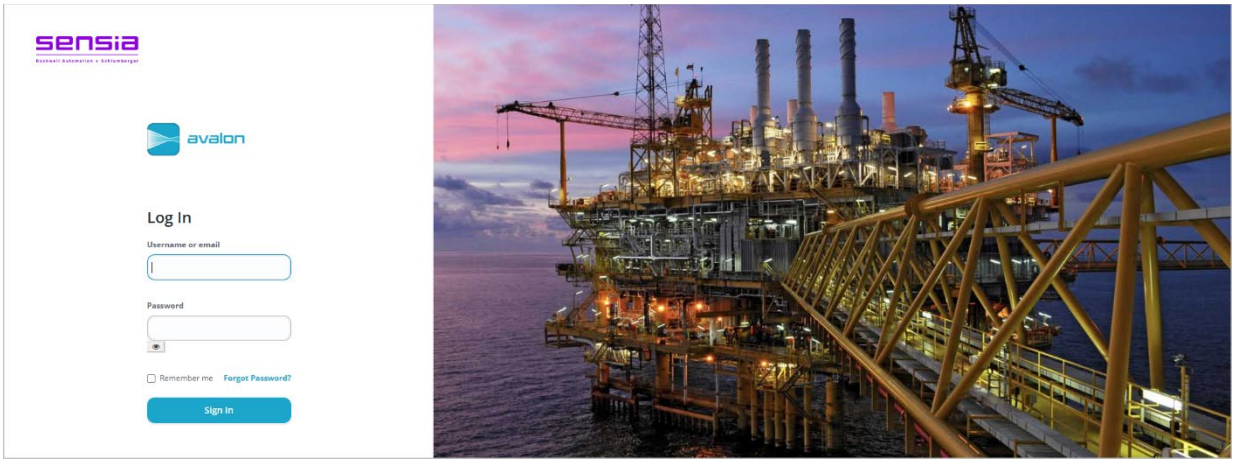
2. Click the blue Provision button.
3. A URL confirmation message will appear. Click the X in the right corner to close the message.



4. After a few seconds, the green provisioning link (Provision Link) will appear on the screen.



5. Click the Provision Link (green) to open an Avalon login dialog in the internet browser. If you are not already logged into the Avalon instance, the Avalon login page opens.

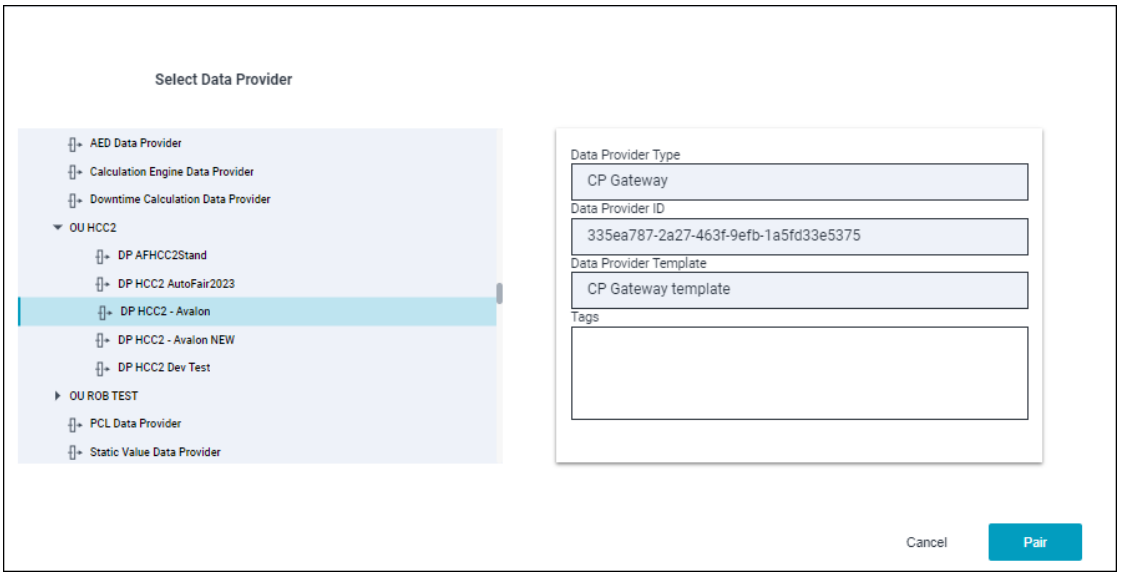


6. Enter your Avalon credentials and log into Avalon.

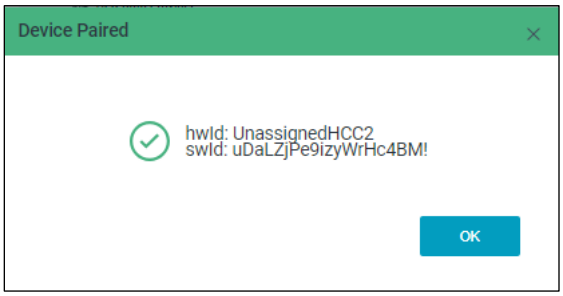
   The Pair Device with Data Provider dialog opens.

Note In the above sample screenshot, the HCC2 device is identified as UnassignedHCC2. Your device should have an assigned ID.

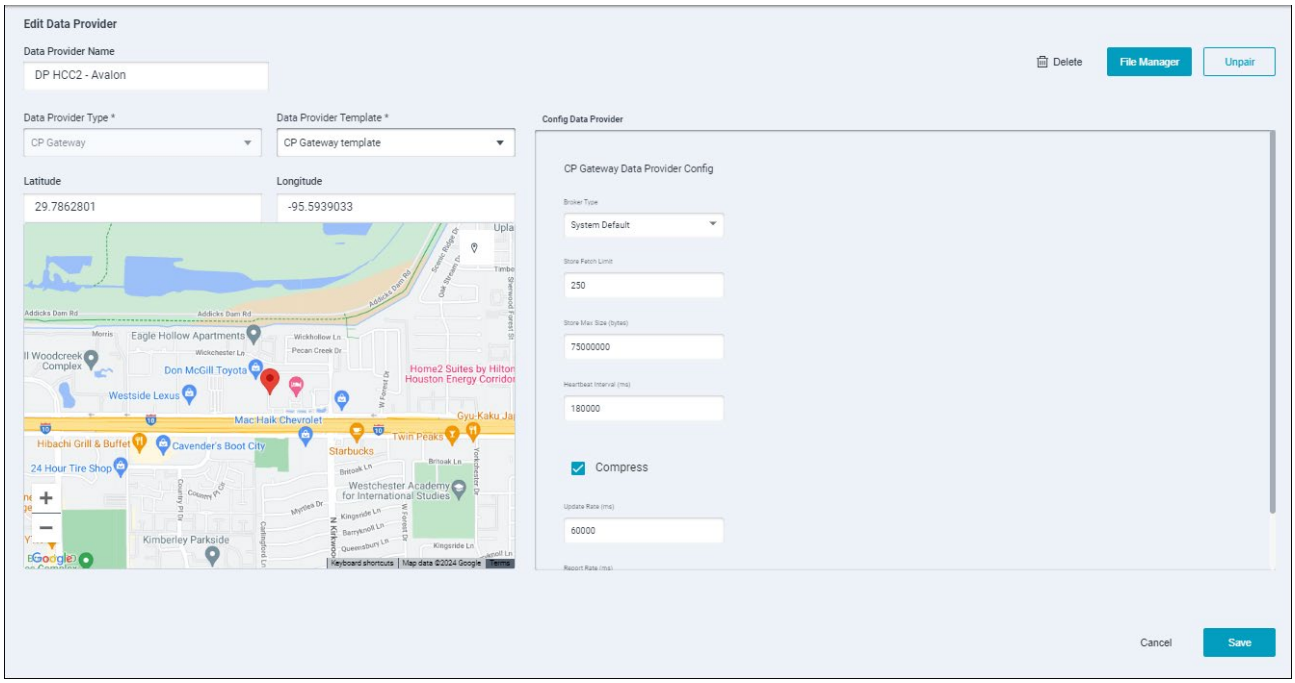
7. Scroll through the Select Data Provider list and select the compatible data provider.



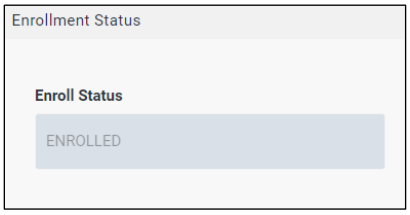
8. Click Pair in the lower right corner of the dialog.
9. When a Device Paired pop-up window appears, displaying hardware and software IDs (“hwId” and “swId”), click OK to complete the device pairing.



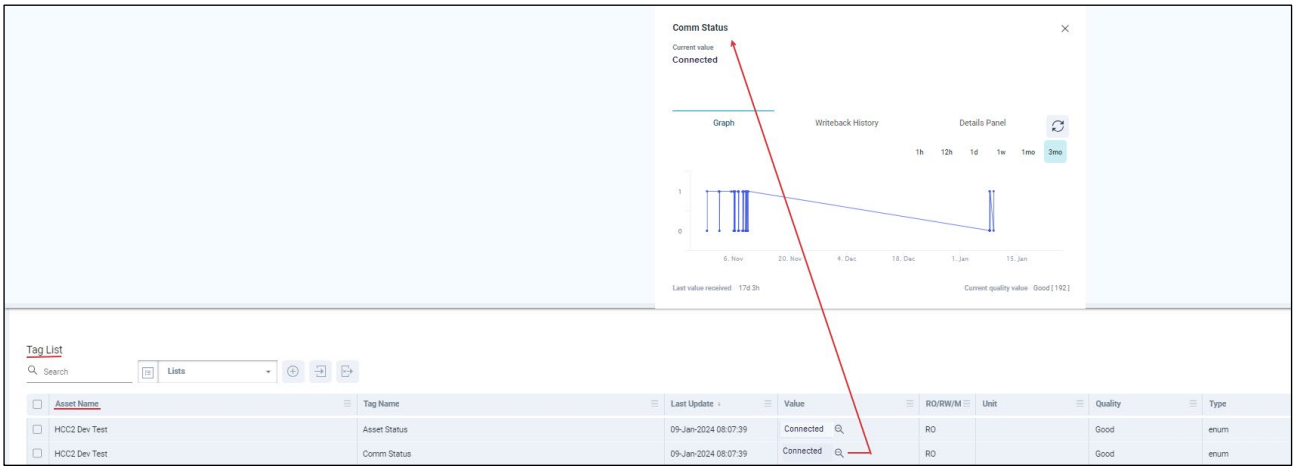
Optionally, in the Avalon interface you can check the Edit Data Provider screen to verify pairing details.



10. In Unity Edge, go to the Avalon Monitoring page, and verify that the Enrolled status displays Enrolled.



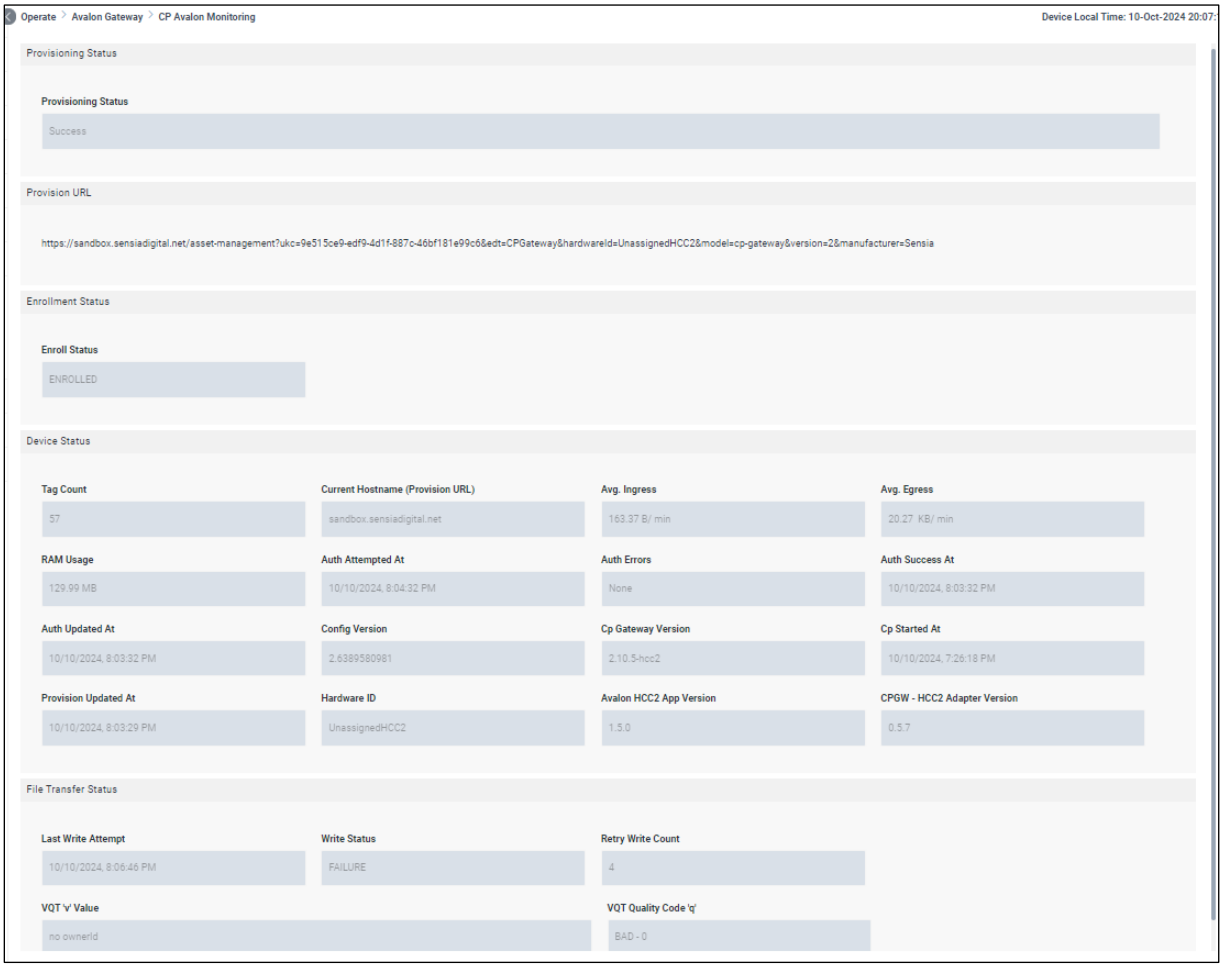
11. Once this process is completed, the HCC2 should be connected to Avalon and reporting the data configured in the Avalon template. To confirm this connection in the Avalon interface, check the status of the Comm Status data point for the selected data provider and asset as shown in the following example screenshot.



7.11.3 Monitor the Avalon Gateway Status

You can monitor communication status and statistics of your HCC2 connection with Avalon through the Avalon Gateway.

Click Operate > Avalon Gateway > CP Avalon Monitoring in the navigation tree to access the Avalon Monitoring page.



The CP Avalon Monitoring parameters are described below:

Parameter	Description
Provisioning Status	Status of provisioning. Displays “Success” or “Waiting for provisioning to complete”.
Provision URL	Avalon URL link. This link directs to the Avalon page where the pair process is done.
Enroll Status	HCC2 enrollment status. Displays “Enrolled” or “Not Enrolled”.
Last Enrollment Status	Latest HCC2 enrollment status. Displays “OK” or “None”.

Device Gateway Stats:

Parameter	Description
Data Point Count	Number of registered tags that are reporting to Avalon. The number of tags depends on the tags defined in the Avalon template.
Current Hostname (Provision URL)	Avalon hostname for a connected HCC2
Avg. Ingress	Ingress average transfer data rate in bytes per minute
Avg. Egress	Egress average transfer data rate in kilobytes per minute
Ram Usage	CP-Gateway RAM Memory Usage (MB)
Auth Attempted At	Date of authentication attempt
Auth Errors	Error while auth attempt (403 Forbidden for instance)
Auth Success At	Date of successful authentication
Auth Updated At	Date of refreshing authentication token
Config Version	Version of config of HCC2 application
Cp Gateway Version	Version of CP Gateway
Cp Started At	Start date for Avalon gateway for current device
Provision Updated At	Date of last updated provision
Hardware ID	Hardware identification of the HCC2. This number is identified by the device serial and the text "HCC2" at the end of the number. It can be found in the Live Data menu.
Avalon HCC2 App Version	Version of Avalon HCC2 application
CPGW – HCC2 Adapter Version	Version of CP Gateway adapter

File Transfer Stats

Parameter	Description
Last Write Attempt	Date of last write to Avalon attempt
Write Status	Status of last file transfer attempt
Retry Write Count	Attempts to make a write to Avalon on file transfer
VQT ‘v’ Value	Value of file transfer
VQT Quality Code ‘q’	Quality of file transfer (q value should be one of the Data Point Quality Status Values for instance: 192 – Good, 0 - Bad)

7.11.4 Unpair the HCC2 from Avalon

In the event you need to relocate a provisioned HCC2 for use with a different installation, you will need to unpair the HCC2 from existing Avalon assets.

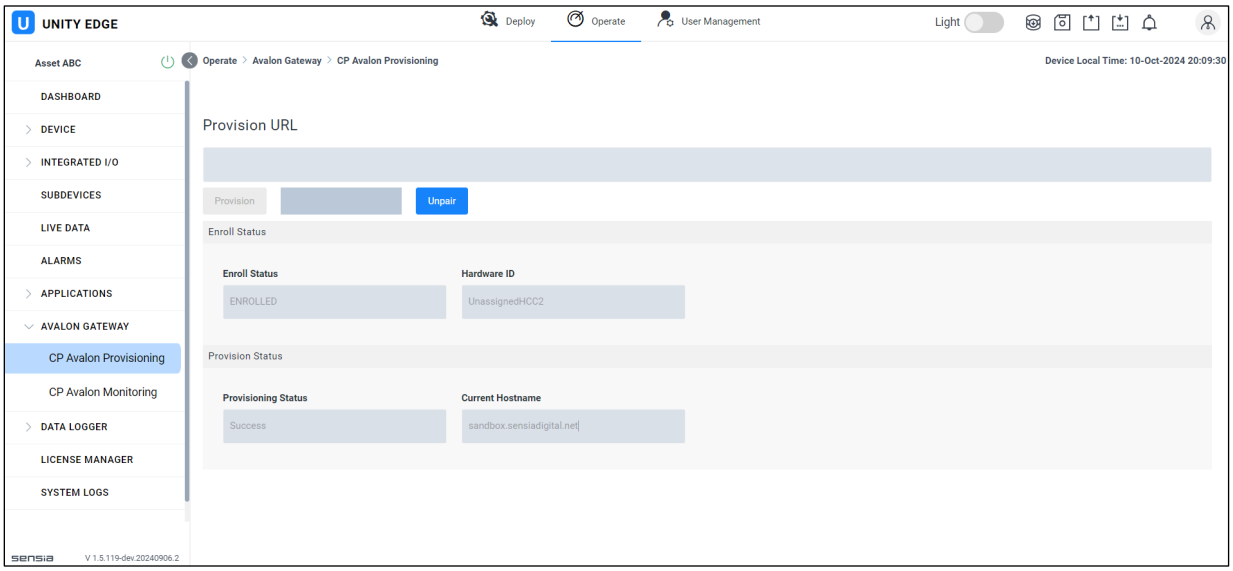
To “unpair” your HCC2 with Unity Edge software:

1. Log in to the HCC2 Unity Edge interface.
2. Click Operate in the top menu.

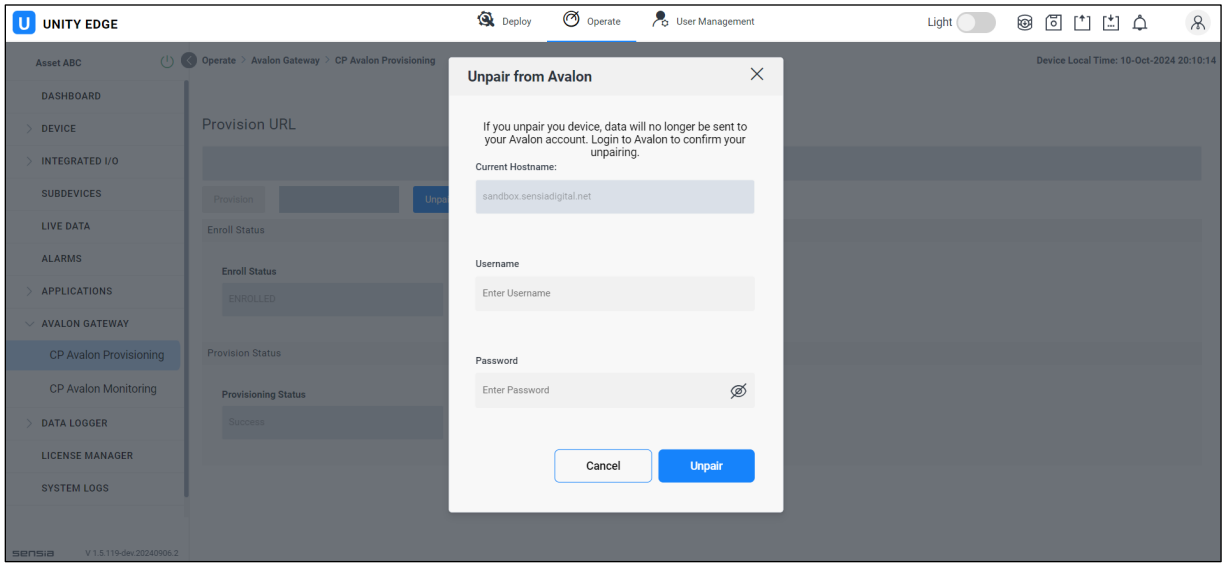
3. Click Avalon Gateway > CP Avalon Provisioning. If the HCC2 is paired with one or more Avalon assets, a blue Unpair button will be visible.

Note	If the Unpair button is grayed out, the HCC2 is not currently paired with an Avalon asset and you can disregard the rest of this procedure.

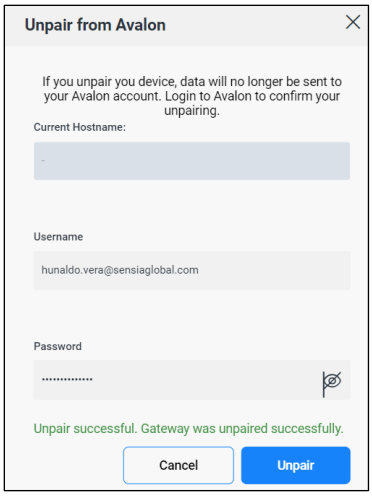
4. Click the Unpair button.



5. An Unpair from Avalon dialog will appear, prompting you for login information. Enter your login credentials and click the blue Unpair button.



6. If the unpair process is successful, a confirmation message will appear momentarily in green text at the bottom of the screen as shown below, and the dialog will then close.



Your HCC2 is now unpaired from Avalon.

Section 8: Configuring Modbus Protocol

This section describes the workflow for defining Modbus server and/or Modbus client instances on your HCC2 device. It walks you through the following configuration actions:

- specifying Modbus server and client properties using Unity Edge's Modbus Protocol Map Editor
- saving the configuration to a proprietary protocol definition (*.pdef) file
- deploying the pdef file to your HCC2 device with Unity Edge

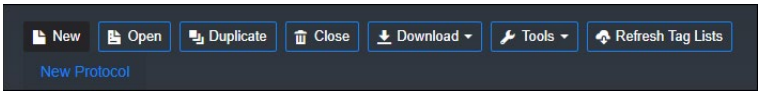
8.1 MODBUS PROTOCOL MAP EDITOR

The Modbus Protocol Map Editor is a custom tool for configuring the HCC2 to act as a Modbus server, a Modbus client, or both. It allows you to specify Modbus server and client properties and save them to a proprietary file format that you upload to an HCC2 device. The Modbus Protocol Map Editor is bundled in the HCC2 software package. After one or more HCC2 ports have been configured as a Modbus server or a Modbus client, the Modbus Protocol Map Editor can be accessed from within the Unity Edge interface (Deploy > Communications > Protocols > Modbus).

Note	You can also access the Modbus Protocol Map Editor through your HCC2's IP address using the HTTP protocol and port number 7070. Launch a window in your Google Chrome or Microsoft Edge web browser and enter your HCC2 IP address followed by a colon and the port number: http://< IPADDRESS>:7070.

8.1.1 Menu Commands

The Modbus Protocol Map Editor interface presents a row of menu commands at the top of the display, along with the name of the currently open protocol definition file.



The New, Open, Duplicate, and Close commands function in the usual way: New starts a fresh protocol definition file, Open launches an existing definition from your local system or a device library, and so forth.

The Download command gives you the option to download the following file types:

- a validation report that provides an error check on the currently open protocol definition file
- the currently open protocol definition file (pdef file extension)
- an HTML summary of the properties specified in the protocol definition file
- a comma-separated variables (.csv) file containing the tags selected for your protocol definition file

A Tools dropdown menu supports a refresh of all register and query data point selection and data point metadata from current data point lists. See the tool called Refresh TagSelection MetaData.

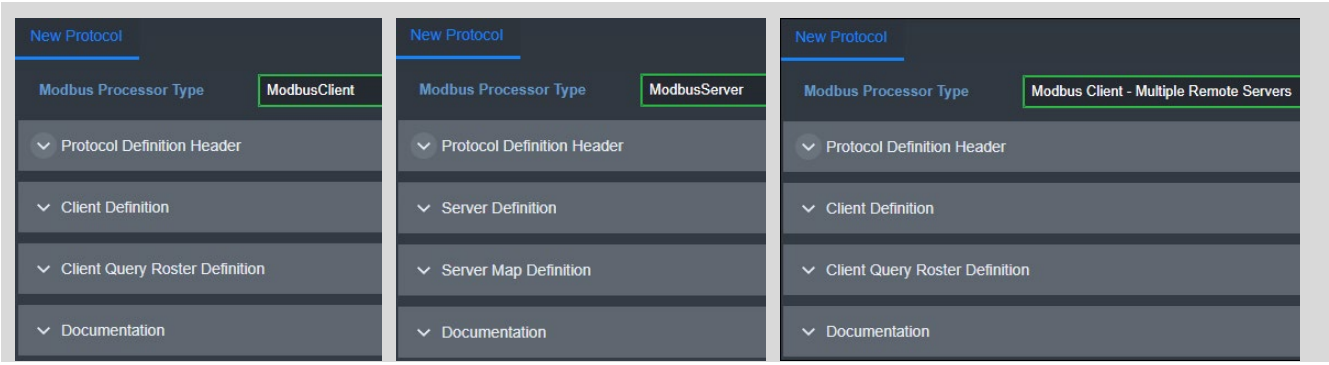
A Refresh Tag Lists button updates the tags currently assigned to the *.pdef definition file. You will need to refresh the tag list if you have made additional changes to the HCC2 configuration while creating the protocol definition file. Enacting the refresh will make any data points recently created available as selections for your Modbus maps.

8.1.2 Processor Type and Panel Overview

The Modbus Protocol Map Editor displays a standard protocol definition header for both the Modbus client and Modbus server definitions. It requires different property values for the specifics of each client and server configuration. Modbus Client files can be created in one of two selections.

The default Modbus Client form is a simplified tool that supports a single remote Modbus server target. Using this form to create your Modbus Client pdef may allow you to configure the communication parameters for that target server within the Unity Edge configuration. If there is no option on the Modbus configuration page to input the communication parameters, you can set them in the Client Definition section by overriding the Unity configuration. The Modbus Client makes it simple to create re-usable single remote server target templates. If supported, multiple copies of the pdef can be used on the same port.

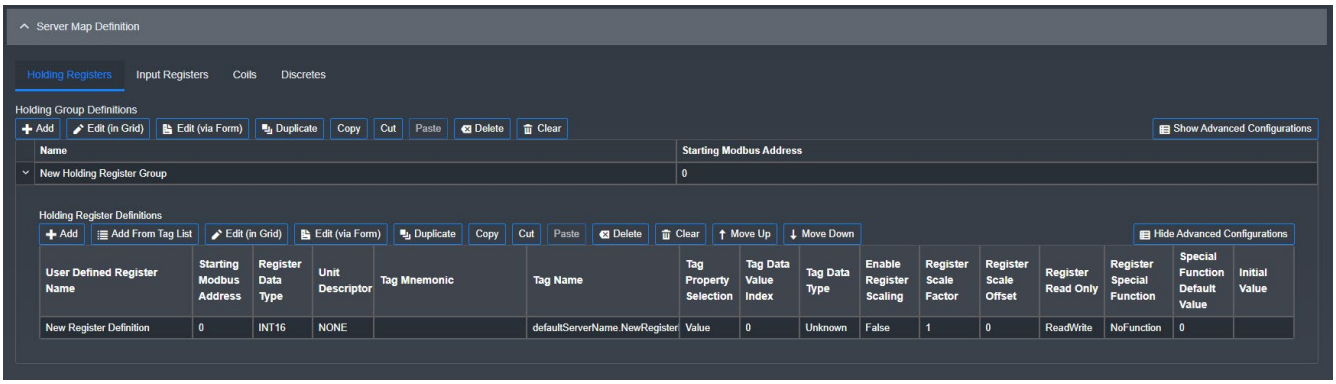
Modbus Processor Type Selections



Refer to the following table for an overview of each expandable panel.

Processor Type	Panel	Description
Modbus Client	Protocol Definition Header	Contains general header information for identifying the client instance: name, version number, text description, creation/modification dates, and notes
	Client & Remote Server Target Definition	Contains the single target server definition
	Client Query Definition	Contains the respective register queries and tags
	Documentation	Summary log of the client definition
Modbus Server	Protocol Definition Header	Contains general header information for identifying the server instance: name, version number, text description, creation/modification dates, and notes
	Server Definition	Contains the data format, exception handling, and access options for the server protocol
	Server Map Definition	Contains the register definitions and system tags that are assigned to the server
	Documentation	Summary log of the server definition
Modbus Client – Multiple Remote Servers	Protocol Definition Header	Contains general header information for identifying the client instance: name, version number, text description, creation/modification dates, and notes
	Client Definition	Displays inter packet delay.
	Client Query Roster Definition	Contains the target server definition(s) and the respective register queries and tags
	Documentation	Summary log of the client definition

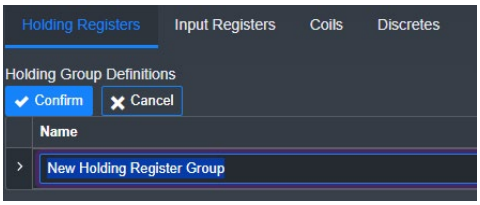
For example, under Server Map Definitions, you can expand the respective panels (Holding Registers, Input Registers, Coils, etc.) to view and edit the specific properties of the client or server configuration. The following grid, for example, shows the controls for adding and editing tags for the Modbus server's Holding Register definitions.



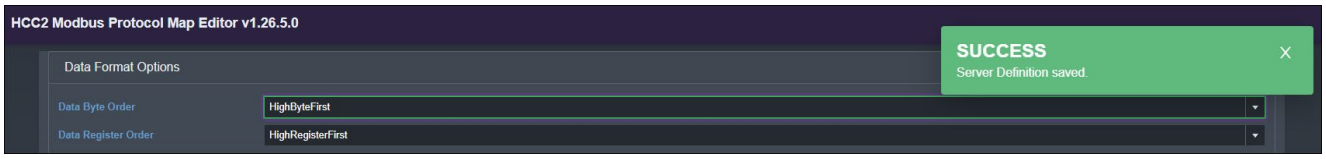
Select Edit (in Grid) to make changes directly to a selected row.

Select Edit (via Form) to make changes in a form presentation that groups properties by category.

In the Server Map Definition tables, you will be prompted to confirm or cancel your additions and changes.



In other panels such as the Server Definition panel shown below, your entries and selections are automatically saved, as indicated by the "SUCCESS" pop-up message in the top right corner of your screen.



8.2 HCC2 MODBUS CLIENT-SERVER SETUP

You can configure the HCC2 to act as a Modbus server, a Modbus client, or both a server and a client. HCC2 can support:

- up to six Modbus RTU deployments (server and/or client) through serial port connections
  - five RS-485 cable connections
  - one RS-232 connection
- up to two Modbus TCP server connections through ports 502 and 503
- up to four Modbus TCP client connections

Note	The HCC2 can support Modus RTU serial port and TCP client-server connections simultaneously.

Each HCC2 Modbus client can connect with and support multiple servers. Your system resources determine the number of servers that each client instance can support.

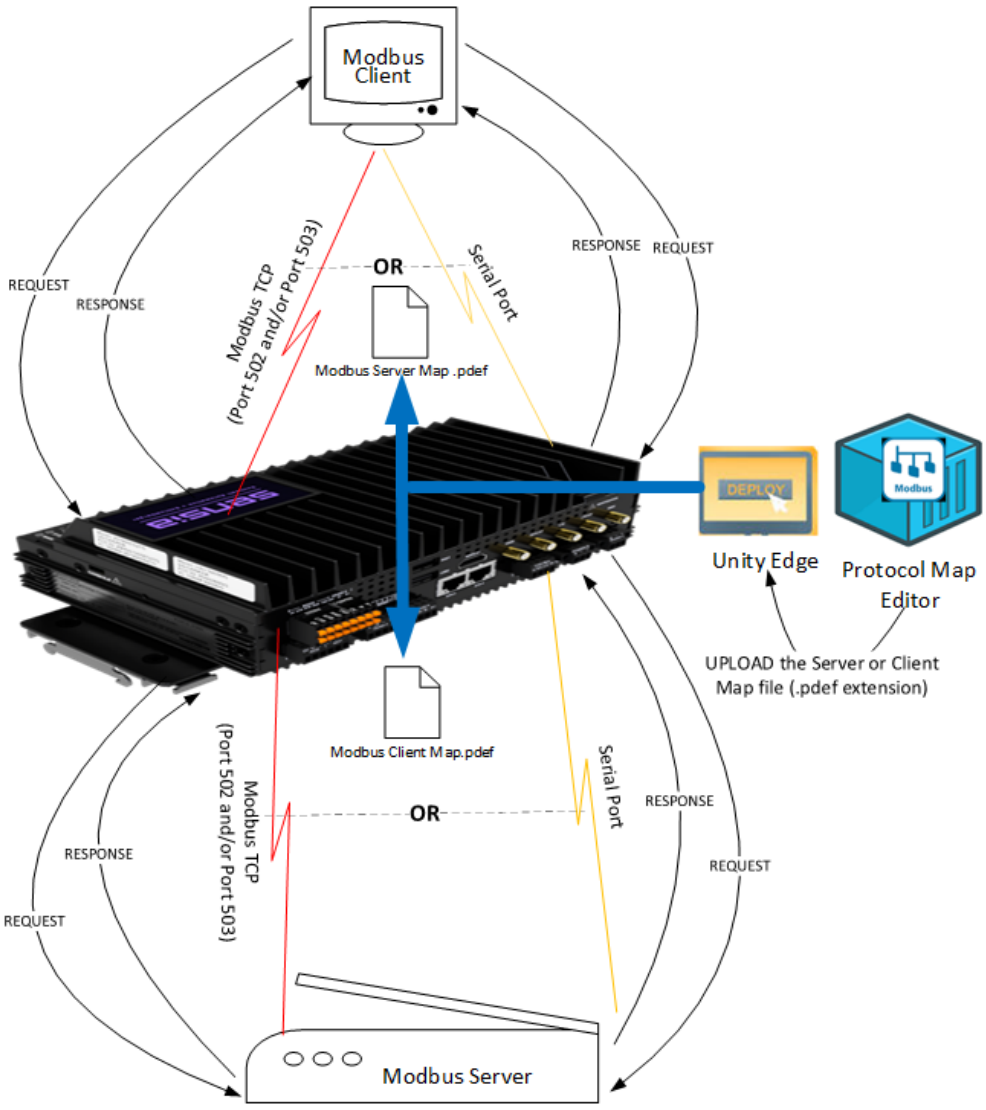


Figure 8.1—HCC2 Modbus Client/Server setup

Step	Task Description
1	Review your network setup and determine how your HCC2 device fits in the data flow. Determine if it will act as a client, a server, or both. Check the capabilities of the device or devices you are connecting to and decide which adjustments you must make to your HCC2 client or server protocol settings.
2	In Unity Edge, go to Deploy > Communications > Port Configuration and specify the serial or TCP port connection that your Modbus server or client connection will use. By default, all port connections are disabled until you assign a Modbus protocol to them.
3	Launch the Modbus Protocol Map Editor. In the Modbus Protocol Map Editor, define and deploy one protocol definition (.pdef) file for each Modbus client or server instance. For example, if you are defining two Modbus server instances and one Modbus client instance on your HCC2, you define and deploy three .pdef files.

Step	Task Description
4	From the Modbus Protocol Map Editor, download the validation report for the protocol definition file and correct any errors. Then download the .pdef file to your local PC.
5	In Unity Edge, go to Deploy > Communications > Protocols > Modbus and upload the respective .pdef file for the corresponding Modbus client or server protocol. By default, the Modbus communications will be enabled on deploy. If that is not the intended behavior, uncheck the Enabled On Deploy checkbox before you deploy the change.
6	For each protocol definition file, launch the Deploy wizard and deploy the .pdef file to your device.

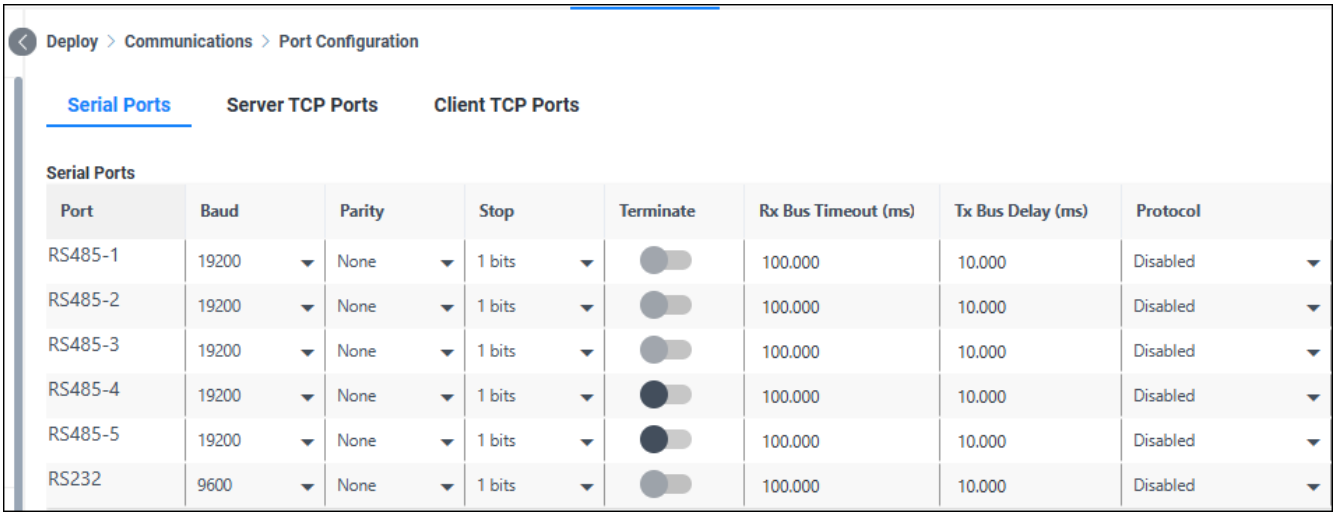
8.3 SETTING UP A SERIAL PORT CONNECTION

The HCC2 provides six serial ports: five RS-485 serial ports and one RS-232 port. You specify the serial port connection for your Modbus server and Modbus client instance(s) when, for example, you are connecting to a PLC.

Note Refer to the HCC2 Hardware User Manual for wiring guidelines.

To prepare a serial port connection, follow these guidelines:

1. Launch Unity Edge and choose the Deploy tab in the menu bar at the top of the display.
2. In the navigation tree, choose Communications > Port Configuration.
3. Choose the Serial Ports tab at the top of the panel.



4. Complete the parameters needed for your server or client connection, using the following descriptions as a reference.

Parameter	Description
Baud Rate	Determines the speed of communication over a data channel. For successful communication the selected baud rate needs to match the speed as the connected serial device. When there is a mismatch, data will transmit but it will be unintelligible.
Parity	Parity is a method of detecting errors in data transmission. The parity bit is an optional parameter used in serial communications to determine if the data character being transmitted is correctly received by the remote device. Select the correct parity option for your connected serial device.

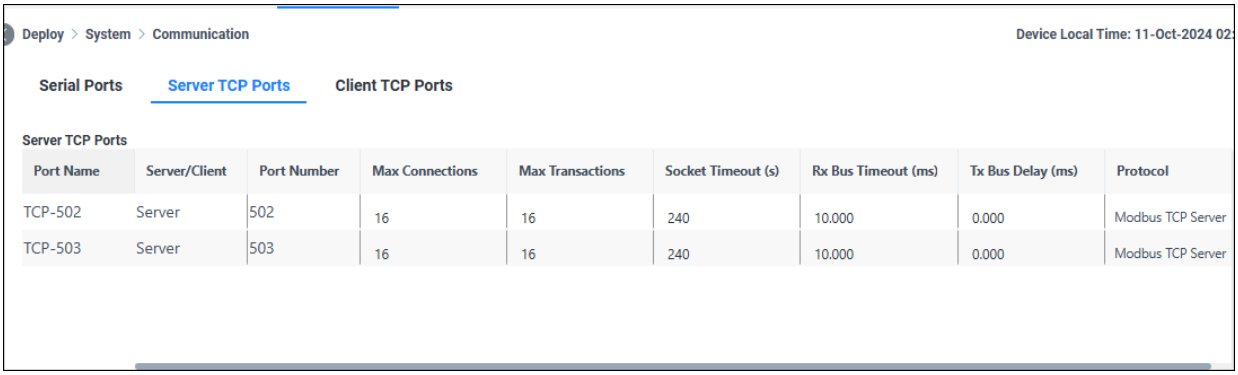
Parameter	Description
Stop bit	Serial links transmit data in distinct packets or frames. The stop bit is used to signal the end of each frame. The stop bits will be determined by the connected serial device.
Terminate	A termination resistor is a single resistor placed at the end of an electrical transmission line. The resistor is used for differential pair signals, like RS-485. In the HCC2, RS-485-4 and RS-485-5 serial buses can be terminated via a software enabled 120 Ω resistor. This configuration is disabled for all other ports.
Rx Bus Timeout (ms)	The time in milliseconds before the receive (Rx) bus times out
Tx Bus Delay (ms)	The delay in milliseconds before the transmit (Tx) bus sends the message
Protocol	Options are Disabled, Modbus RTU Server, and Modbus Client.

8.4 SETTING UP TCP SERVER AND CLIENT CONNECTIONS

You specify the TCP parameters for both Modbus server and client connections in separate display windows.

Note HCC2 Ethernet ports ETH-1 and ETH-2 can be configured for TCP connections. Refer to the HCC2 Hardware User Manual for wiring information.

1. Verify the Deploy menu is selected at the top of your screen.
2. In the navigation tree, choose Communications > Port Configuration.
3. To define the Modbus Server TCP port, do the following:
   a. Choose the Server TCP Ports tab at the top of the panel. Modbus server TCP ports 502 and 503 are displayed.



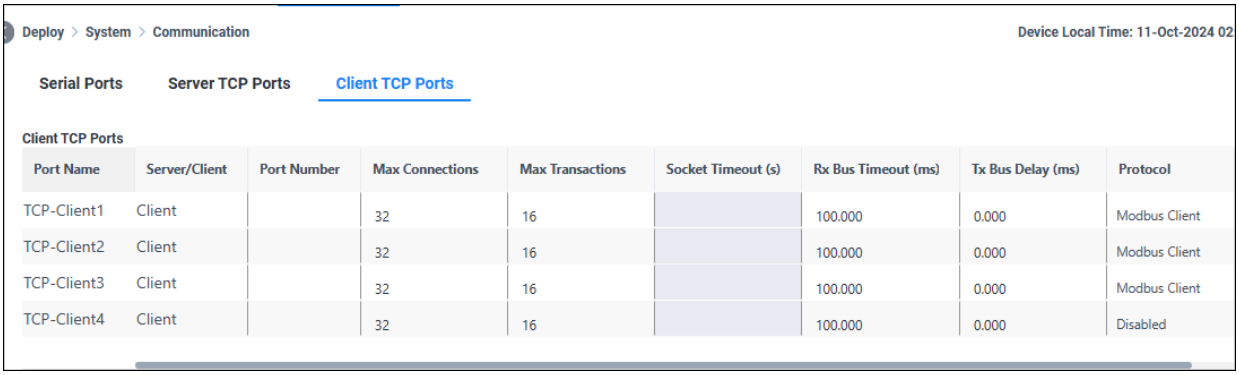
   b. Select a server TCP port and make any configuration changes. Refer to the following table for guidelines.

Parameter	Description
Port Name	Defaults to TCP-502 or TCP-503
Server/Client	Defaults to Server
Port Number	Defaults to 502 or 503
Max Connections	The maximum number of Modbus client connections allowed for the server port connection
Max Transactions	The maximum number of transactions that can be processed
Socket Timeout (s)	The time in seconds between data packets before the socket times out
Rx Bus Timeout (ms)	The time in milliseconds before the receive (Rx) bus times out

Parameter	Description
Tx Bus Delay (ms)	The delay in milliseconds before the transmit (Tx) bus sends the message
Protocol	Options are Disabled, Modbus RTU Server over TCP, and Modbus TCP Server. Note that Modbus RTU Server over TCP is normally used for legacy systems. Modbus TCP Server is the usual server protocol selection.

4. To define the Modbus Client TCP port, do the following:

   a. Choose the Client TCP Ports tab at the top of the panel. The available client TCP ports are displayed. Each HCC2 device supports up to four Modbus TCP Client connections. Each Modbus TCP Client can support multiple Modbus TCP Server connections based on system memory.



   b. Select the Client TCP port and make any configuration changes. Refer to the following table for guidelines.

Parameter	Description
Port Name	Defaults to TCP-Client1, TCP-Client2, TCP-Client3, TCP-Client4
Server/Client	Defaults to Client
Port Number	Defined on server side of connection
Max Connections	The maximum number of Modbus client connections allowed for the server port connection
Max Transactions	The maximum number of transactions that can be processed
Socket Timeout (s)	Defined on server side of connection
Rx Bus Timeout (ms)	The time in milliseconds before the receive (Rx) bus times out
Tx Bus Delay (ms)	The delay in milliseconds before the transmit (Tx) bus sends the message
Protocol	Options are Disabled and Modbus Client.

8.5 MODBUS PROTOCOL DEFINITION GUIDELINES FOR HCC2

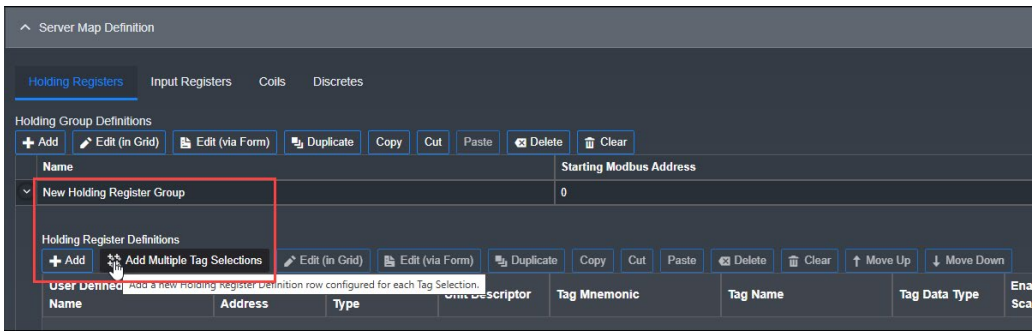
When defining your Modbus server and client, note the high-level guidelines described in this section.

8.5.1 Tag Mapping Considerations: Server and Client

For Modbus server definitions, you can select and map existing tags from Unity Edge apps to Modbus server registers through the Tag Selection List – All Tags display window.

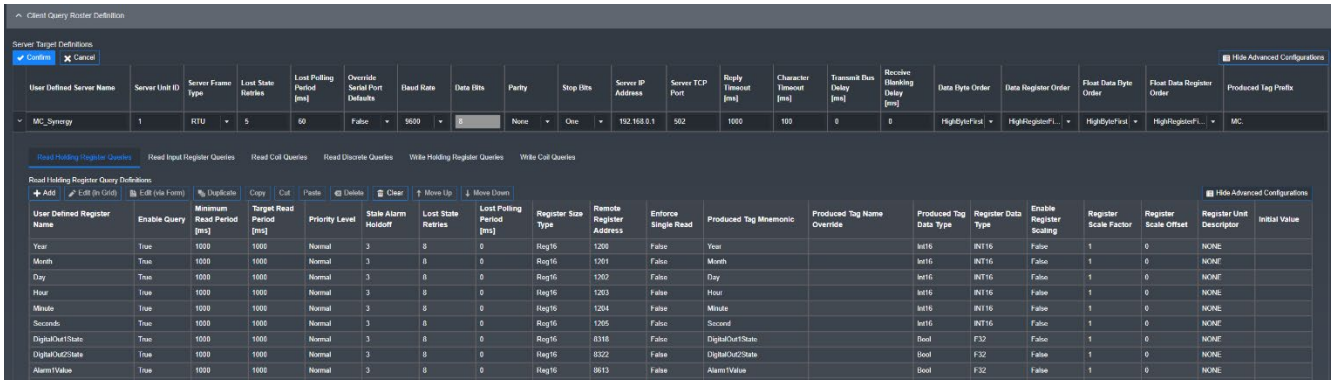
In the Server Map Definition panel

- Click +Add to add a single register definition which can be configured by one of the following methods:
  - select an existing HCC2 Data point (SelectTag)
  - construct a custom data point by building the data point from the context (ConstructFromMnemonic)
  - construct a custom data point with the full data point FQN provided (UserDevicedOverride)
- Click the Add Multiple Tag Selections icon to select and add many HCC2 data points to the register map in one action using SHIFT-Click and CTRL-Click operations.



In the Tag Selection List – All Tags window, you can sort, filter, and select tags for different HCC2 applications.

For Modbus client definitions, you can add and map custom tags to Modbus client registers through the Client Query Definition panel.



Choose either of two views by toggling the hide/show button in the top right corner. Show the Advanced view for maximum detail, or hide it for a view of commonly used parameters.

The tag names for custom tags must follow these conventions:

- Begin with a letter
- Use only alphanumeric characters
- Contain a maximum of 32 characters

Camel case is recommended but not required. Camel case is the use of a capital letter to begin the second word in a compound name or phrase, when it is not separated from the first word by a space—for example, *iPad*.

8.5.2 Modbus Server Address Range

HCC2 applies the Modbus address range 0 – 65,535 to the Modbus data types. Refer to the following table:

Modbus Data Type	Modbus Address Range	Base Address Range	Reference Prefix	Reference Address Range
Coils	0 – 65,535	1 – 65,536	0	000001-065,536
Discrete Inputs	0 – 65,535	1 – 65,536	1	100001-165,536
Input Registers	0 – 65,535	1 – 65,536	3	300001-365,536
Holding Registers	0 – 65,535	1 – 65,536	4	400001-465,536

If the device you are connecting to uses the base address range (1 – 65,536), you should define an offset on the device to accommodate the Modbus address range.

If your device uses the reference prefix for the Modbus data types, you may need to adjust the reference address range to match the Modbus address range.

8.6 CREATING A MODBUS CLIENT PROTOCOL DEFINITION FILE

Before you begin, verify that your desired serial port or Modbus TCP Ethernet connection is available and that you have technician or admin level access.

8.6.1 Set Up the Client Definition File

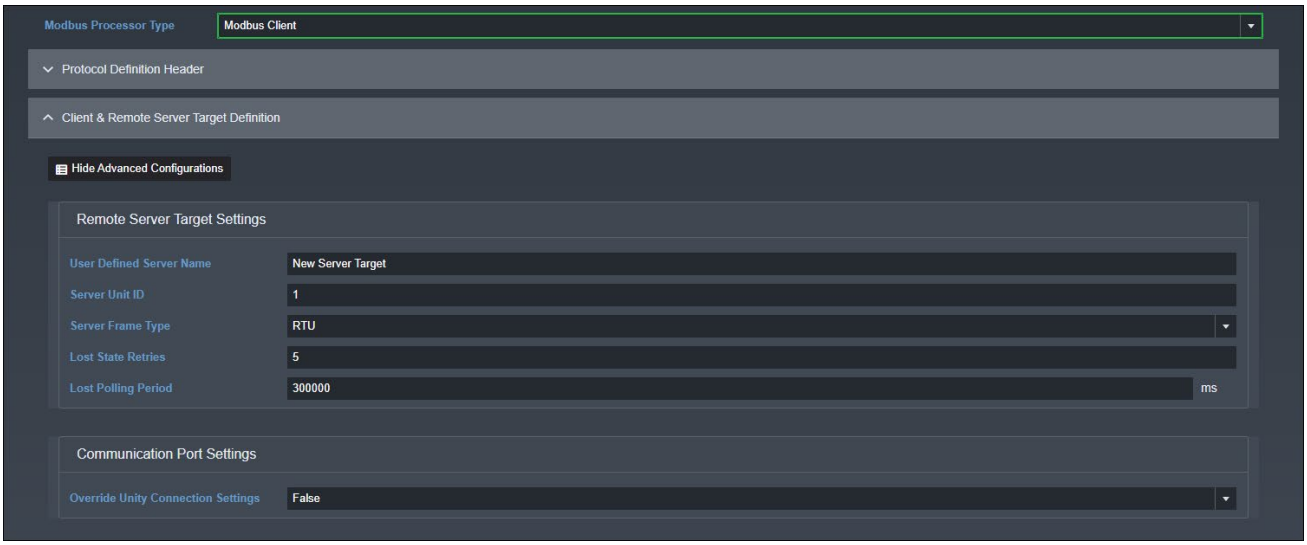
1. Access the Modbus Protocol Map Editor through the Unity Edge interface. Alternatively, you can do the following:
   a. Launch a window in your Google Chrome or Microsoft Edge web browser.
   b. Enter your HCC2 IP address followed by a colon and the port number 7070 (as described in section 8.1, Modbus Protocol Map Editor, page 101).
2. If **New Protocol** is not displayed at the top of the interface below the Map Editor's commands, click **New**.
3. In the Modbus Processor Type dropdown, choose Modbus Client or alternatively, Modbus Client – Multiple Remote Servers.
4. Under the Protocol Definition Header label, make the following entries as needed.

Parameter	Description
User Protocol Name	Assign a unique, descriptive name to the map
Protocol Map Version	Defaults to zero. Enter a numeric sequence identifier
User Description	Optional. Enter a helpful description that indicates the purpose of the map.
Author	Optional. Enter the name of the organization or person who creates the map.
Owner	Optional. Enter the name of the organization or person responsible for the map.
Creation Date	Defaults to the local time

Parameter	Description
Modified Date	Defaults to the local time
Release Notes	Optional. Add any explanatory text.

8.6.2 Define a Target for a Single Server

Proceed to the Client & Remote Server Target Definition section to define the target server and its parameters.



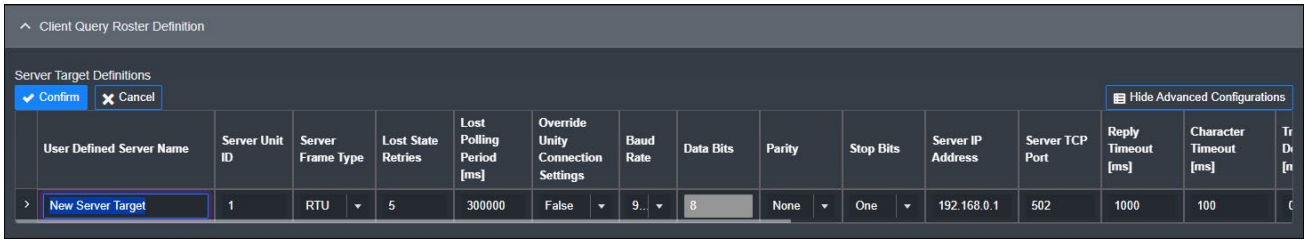
8.6.3 Define Targets for Multiple Remote Servers

If you use the Modbus Client – Multiple Remote Servers processor type, follow this procedure to configure multiple server targets.

1. Expand the Client Query Roster Definition panel.

   The Server Target Definitions grid is displayed.

2. Click Add to insert an editable row. Default parameter values populate the columns.



3. Enter the parameter values as required. Refer to the following table for guidelines. Your settings will be applied automatically, as indicated by a green “SUCCESS” pop-up notification.

Parameter	Description
User Defined Server Name	Specify a unique name for the server your HCC2 client connects to.
Server Unit ID	Numeric ID of the server. The value range is 0 through 255, inclusive. Note that 0 can be used to create a one-to-one connection between client and designated server.
Server Frame Type	Dropdown list that specifies the protocol type: RTU or TCP. The RTU requires a serial port configuration. The TCP requires an Ethernet configuration. If you select RTU, the Server IP Address and Server TCP Port properties do not apply and are disabled. If you select TCP, the following properties are disabled: • Override Serial Port Defaults • Baud Rate • Data Bits • Parity • Stop Bits
Lost State Retries	Number of failed attempts before the query is considered lost. Once the query is in the lost state, the priority of the query is lowered, and polling is done at the Polling Period Lost value. If the poll is successful, the query is no longer considered lost. Range: 1 to 32.
Lost Polling Period (ms)	Polling period used for the query when it is considered in the lost state
Override Unity Connection Settings	True/False dropdown list. If set to True, the communication settings you define here override the serial port settings defined on the Modbus client device. Note: If the installed version of Unity Edge does not support the configuration of the Client communication settings on the Deploy > Protocols > Modbus page, you must configure the settings here. Select True and proceed to configure the remote server communication parameters.
Baud Rate	For the RTU protocol type, specifies the data rates in bits per second
Data Bits	For the RTU protocol type, specifies the number of data bits. Note that only 8 bits are supported.
Parity	For the RTU protocol type, this dropdown list shows the parity bit sent with each character. The values are None, Odd, Even, Mark, or Space.
Stop Bits	For the RTU protocol type, this dropdown list shows the number of stop bits sent at the end of each character. The values are None, One, Two, and OnePointFive.
Server IP Address	For the TCP protocol type, specify the IPv4 address of the server connection.
Server TCP Port	For the TCP protocol type, specify the listener port of the remote server—typically 502 or 503.
Reply Timeout (ms)	The time in milliseconds before the client query is declared as failed if a server reply is not received. The value range is 10 to 65,535 milliseconds (one minute).
Character Timeout (ms)	Maximum time interval allowed between two successive bytes of the same response message before an incomplete response is declared. The value range is 0 to 65,535 milliseconds.
Transmit Bus Delay (ms)	The minimum time interval before a response is sent. This property is applied when the remote server does not parse large numbers of streaming packets. The value range is 0 to 65,535 milliseconds.

Parameter	Description
Receive Blanking Delay (ms)	The blanking period inserted after a transmission completion during which the character reception is ignored. Use this delay to block data before accepting a response. The value range is 0 to 65,535 milliseconds.
Data Byte Order	Dropdown list that specifies the order of bytes within a register. You can swap the order of the data. Valid values are High Byte First and Low Byte First.
Data Register Order	Dropdown list that specifies the order of registers that are part of a multi-register value. You can swap the order of the data. Valid values are High Register First and Low Register First.
Float Data Byte Order	Dropdown list that specifies the order of the bytes withing a register containing a floating point representation. You can swap the order of the data. Valid values are High Byte First and Low Byte First.
Float Data Register Order	Dropdown list that specifies the order of the registers that are part of a multi-register value containing a floating point representation. You can swap the order of the data. Valid values are High Register First and Low Register First.
Produced Tag Prefix	This prefix designates the base part of the tag name generated by each read and write query. It is concatenated with the Produced Tag Mnemonic specified in the register query definition to obtain the complete tag name of the generated HCC2 tag. The prefix format must contain alphanumeric characters and end with a dot (Scanner123.).
Inter Packet Delay (ms)	4. Under the Client Options label, specify the in milliseconds (0.001). This is the minimum time interval between queries when you are scheduling queries to transmit. This delay interval is applied when your client is connected to multiple servers that do not optimally respond with defined polling rates.

5. Proceed to 8.6.4, Configure Client Read and Write Queries.

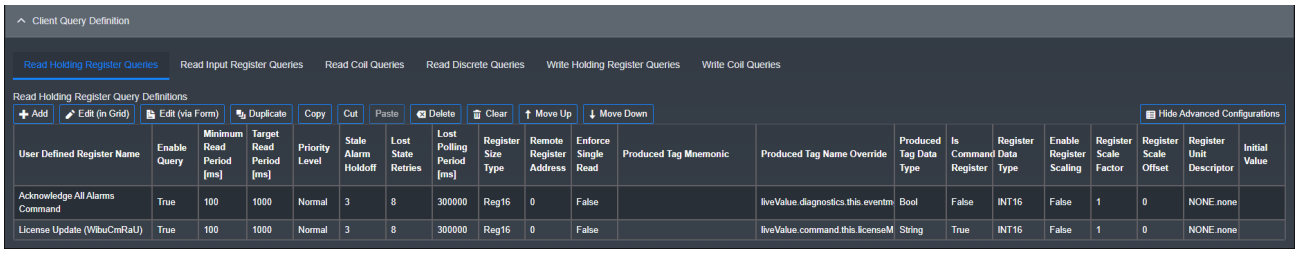
8.6.4 Configure Client Read and Write Queries

You can add and configure custom tags to convey the client read and write queries addressed to the specified target server.

Note that the Client Query Definition panel does not have the grouping feature of the Server Target Definition panel. You need to check that the starting Modbus addresses are correct.

To add the Modbus client queries, follow these steps:

1. Select the type of query you want to add. Choose from
   - Read Holding Register Queries
   - Read Input Register Queries
   - Read Coil Queries
   - Read Discrete Queries
   - Write Holding Register Queries
   - Write Coil Queries
2. Click Add to display the editable input row for the selected query definition. This example uses the query definition Read Holding Register Queries.



The different queries share common parameters but also contain unique parameters. The following table describes both common and unique parameters. Reference this table for help to complete your query definitions. Parameters highlighted in yellow are displayed only when the Advanced Configurations view is enabled (see the link in the top right corner of the screen).

Query Setting	Parameter	Description
General	User Defined Register Name	Specify a name that identifies your query.
	Enable Query	A True/False dropdown selection that lets you disable a query by setting the flag to False. By disabling the query, you do not have to delete it and can still maintain it.
Read	Minimum Read Period (ms)	Minimum period that must elapse after the previous successful query for another read query to be performed. This setting represents the fastest period the Modbus driver will be allowed to read the data and can be used to prevent values from being read too frequently, independently of the frequency at which the value is updated.
	Target Read Period (ms)	Target period for the read query to be performed. Used to define how often the data will be polled (e.g., to poll data 4 times per second, use 250 ms).
	Priority Level	Used to increase the priority of the query. Use only when a fast response time is required, as overuse of the higher priority levels can cause other queries to become unread until their priority is increased due to their stale alarm state. Choose between Normal, High, or Critical.
Lost and Stale	Stale Alarm Holdoff	Number of polling periods before the query is considered stale. Once data are considered stale, the priority of the query increases with time. Range 0 to 16.
	Lost State Retries	Number of failed attempts before the query is considered lost. Once the query is in the lost state, the priority of the query is lowered, and polling is done at the Polling Period Lost value. If the poll is successful, the query is no longer considered lost. Range: 1 to 32.
	Lost Polling Period (ms)	Polling period used for the query when it is considered in the lost state
Remote Register Definition	Register Size Type	Size of the Modbus register. Choose between 16 bits (Reg16) and 32 bits (Reg32).
	Remote Register Address	Modbus address of the Remote register in the target Modbus Server HCC2 Modbus addressing starts at zero. If the target Modbus Server addressing starts at one, consider the offset when specifying the Remote register address. For example, if the target Modbus Service addressing starts at one, then for a Remote register with address 1, enter 0 in the Remote register address.
	Enforce Single Read	If True, the query is read as a separate packet. Used to

Query Setting	Parameter	Description
		prevent including this register in a multi-register read query. If False, consecutive registers belonging to the same remote server and of the same register size type (16 bits or 32 bits) will be combined in a single packet.
Produced Tags	Produced Tag Mnemonic	Tag name to be appended to the Produced Tag Prefix when the Produced Tag Name Override is left unconfigured or is set to Construct From Mnemonic
	Produced Tag Name Override	Existing tag that will receive the value from the read query. Use the Select Tag button to open the Tag Selection window and choose a tag associated to one of the applications loaded in the HCC2. If this setting is left unconfigured or is set to Construct From Mnemonic, then a new produced tag will be created using the Produced Tag Mnemonic tag name. See section 8.6.5 for details.
	Produced Tag Data Type	Data type of a produced HCC2 tag. If an existing HCC2 tag is selected, this parameter is part of the tag properties and cannot be modified from the Modbus Protocol Map Editor. If a new HCC2 tag is created using the Construct From Mnemonic setting, the Produced Tag Data Type must be defined.
	Is Command Register	If declared a command register, the HCC2 will permit multiple sources to produce the data point during Unity deployment Data Point Mapping Validation step.
Remote Register Definition	Register Data Type	Data type of the Modbus register in the remote server
	Enable Register Scaling	If True, the register value can be scaled using the Register Scale Factor and the Register Scale Offset parameters. Register Scale Factor For read queries, the scaling is applied to the Modbus register value prior to unit conversion. For write queries, the scaling is applied to the Modbus register value after the unit conversion is complete. Scaled Value = (Value * Register Scale Factor) + Register Scale Offset
	Register Scale Factor	Multiplier used to scale the Modbus register when Enable Register Scaling is set to True
	Register Scale Offset	Value added to the Modbus register when Enable Register Scaling is set to True
	Register Unit Descriptor	Engineering units of the Modbus register in the remote server. When the Modbus register is linked to an existing HCC2 tag, the base quantity (e.g., temperature, pressure) is inherited from the tag and only the engineering units of the register (e.g., °C, °F, K, R) can be modified. When a new tag is being produced for the Modbus register using the Construct From Mnemonic, the base quantity and units of the register can be specified.
	Initial Value	Initial value given to the Modbus register before the first successful query to the remote server.

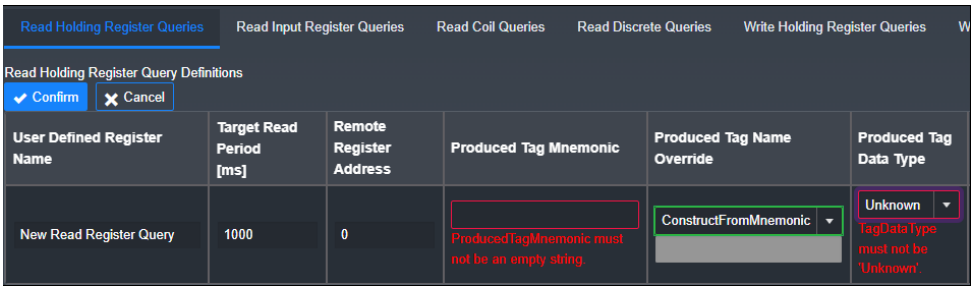
3. Click Confirm.
4. To add a new query, select the target server and repeat these steps for the specific query.

8.6.5 Construct Produced Tag Name from Mnemonic

To use the same .pdef on multiple ports, configure your query definition to override the produced tag name.

1. Select ConstructFromMnemonic in the Produced Tag Name Override field.
2. Enter a unique tag name in the Produced Tag Mnemonic field.
3. Select a tag data type from the Produced Tag Data Type list provided.

Important If the same pdef file is mounted on multiple ports, this data point construction method must be used. This method will prevent data point validation errors caused by devices connected to different ports attempting to publish to the identical data point. Data points produced with this override are uniquely identified by their port name and the string entered into the Modbus page in Unity Edge.



8.6.6 Verify the Modbus Client Protocol

Expand the Documentation panel to review the status of the Modbus client protocol.

8.6.7 Validate the Client Protocol Definition File

To check whether the client protocol definition conforms with the rules, choose Download > Validation Report from the top menu bar to download a text file.

8.6.8 Review Tag Definitions

You can view the tags that you have added to the specified registers. Click Download > .CSV Optik Register Import File. A comma-separated variables (.csv) file is downloaded to your local system in an Excel spreadsheet.

8.7 CREATING A MODBUS SERVER PROTOCOL DEFINITION FILE

Before you begin, verify that your desired serial port or Modbus TCP Ethernet connection is available and that you have technician or admin access level.

8.7.1 Set Up the Server Definition File

1. Open the Modbus Protocol Map Editor from Unity Edge.
2. If New Protocol is not displayed at the top of the interface below the Map Editor's commands, then click New.
3. In the Modbus Processor Type dropdown, choose Modbus Server.
4. Under the Protocol Definition Header label, enter a descriptive name for your ModbusServer.pdef file and additional information as needed.

Parameter	Description
User Protocol Name	Assign a unique, descriptive name to the map
Protocol Map Version	Defaults to zero. Enter a numeric sequence identifier
User Description	Optional. Enter a helpful description that indicates the purpose of the map.
Author	Optional. Enter the name of the organization or person who creates the map.
Owner	Optional. Enter the name of the organization or person who is responsible for the map.
Creation Date	Defaults to the local time
Modified Date	Defaults to the local time
Release Notes	Optional. Add any explanatory text.

5. Under the Server Definition pane, specify the following parameters as required. You make most of the selections through a dropdown menu.

   a. Under Tag Options, the Tag Prefix defaults to the server name. A customized tag prefix must end with a dot character (.): for example, **defaultServerName.**<HCC2TagName>.

   b. For the Data Format options, you may need to customize the settings to accommodate the client device you are connecting with. For example, you may need to override default settings in your client device so that the format matches the format of the Modbus server protocol definition file.

Option	Parameter	Description
Data Format	Data Byte Order	Convention used for the order of the bytes within a register. This setting allows swapping the order of the data. Choose between High Byte First or Low Byte First
	Data Register Order	Convention used for the order of the registers that are part of a multi-register value. This setting allows swapping the order of the data. Choose between High Register First or Low Register First.
	Float Data Byte Order	Convention used for the order of the bytes within a register containing a floating point representation. This setting allows swapping the order of the data. Choose between High Byte First or Low Byte First.
	Float Data Register Order	Convention used for the order of the registers that are part of a multi-register value containing a floating point representation. This setting allows swapping the order of the data. Choose between High Register First or Low Register First.

   c. For the Exception Handling options, you can instruct the Modbus server on how to handle client queries.

Option	Parameter	Description
Exception Handling	Partial Multi Register Value Query Allowed	If True, the Illegal Data Address exception response is suppressed when a query addresses only a portion of a multi-register value. If the exception response is suppressed, the operation is performed and the read response contains partial data.
	Suppress Illegal Data Value Exception	If True, the Illegal Data Value exception response is suppressed when a value in a query is not an allowable value for the server and the write operation was rejected. All other writes which were not rejected will be enacted.

Option	Parameter	Description
	Suppress Read Address Exception	If True, the Illegal Address exception is suppressed, and a response is issued when a read query contains addresses that are not present in the map. All values read that are not represented in the map return a value equivalent to zero.

d. Likewise, for the Enron Access options, you can instruct the Modbus server on how to handle client queries.

Option	Parameter	Description
Enron Access	Enable Enron Archive Retrieval	Period after the last successful query in which the query to begin registering a priority score, indicating it is pending. If the query is sent successfully, this time will be reset.
	Enable Enron Event Year Offset	If True, the query is written as a separate packet. If False, consecutive registers belonging to the same remote server and of the same register size type (16 bits or 32 bits) will be combined in a single packet.
	Enron History Record Size	Fixed archive record size required by an Enron host. If the Enron record provided is greater than the Enron History Record Size, only the first selected number of fields are used. If the Enron record provided is less than the Enron History Record Size, the response is padded with zeroes. The range is 0 to 255.
	Enable Alarms Record Creation	If True, the Modbus Server will generate alarm records for its events archive. To create an event, the Modbus Server will process each alarm message from the system. If an alarm message is regarding an HCC2 tag for which a Modbus address has been assigned, the record is created.
	Enable System Events Record Creation	If True, the Modbus Server will generate system event records for its events archive. System event records are not strictly an Enron type, but a method of recording a system event as an enumerated value that can be decoded with provided decoder documents. These records are used when an event has acquired an associated Modbus address. (e.g., device reset, system critical failure, defaults loaded, network events, RTC changes, container launch/shutdown).

e. For the Access Restriction options, you can limit access to the server. For example, you can restrict the server to read-only or allow read-write access but limit the registers the client can access.

Option	Parameter	Description
Access Restriction	Global Write Disable	Globally controls the Modbus Server access. Choose between Read/Write or Read Only access.
	Enable Holding Range Limits	If True, Holding Registers query operations are limited to a programmable address range.

Option	Parameter	Description
	Lowest Accessible Holding	If Enable Holding Register Range Limit is True, this is the lowest register address value presented to the port. The range is 0 to 65,535.
	Highest Accessible Holdings	If Enable Holding Register Range Limit is True, this is the highest register address value presented to the port. The range is 0 to 65,535.
Access Restriction	Enable Input Range Limits	If True, Input Registers query operations are limited to a programmable address range.
	Lowest Accessible Input	If Enable Input Register Range Limit is True, this is the lowest register address value presented to the port. The range is 0 to 65,535.
	Highest Accessible Input	If Enable Input Register Range Limit is True, this is the highest register address value presented to the port. The range is 0 to 65,535.
	Enable Coil Range Limits	If True, Coil query operations are limited to a programmable address range.
	Lowest Accessible Coil	If Enable Coil Range Limit is True, this is the lowest register address value presented to the port. The range is 0 to 65,535.
	Highest Accessible Coil	If Enable Coil Range Limit is True, this is the highest register address value presented to the port. The range is 0 to 65,535.
	Enable Discrete Range Limits	If True, Discrete Input query operations are limited to a programmable address range.
	Lowest Accessible Discrete	If Enable Discrete Range Limit is True, this is the lowest register address value presented to the port. The range is 0 to 65,535.
	Highest Accessible Discrete	If Enable Discrete Range Limit is True, this is the highest register address value presented to the port. The range is 0 to 65,535.

8.7.2 Define the Server Map

After defining the Modbus server, you can add one or more registers to the server map using the Server Map Definition dropdown option in the Modbus Protocol Map Editor. In addition, you can create multiple groups for each register, each with a different starting Modbus address. For example, if you are adding a holding register, you can create separate groups for temperature, pressure, and offsets with starting Modbus addresses of 6002, 6016, and 7002, respectively.

1. Select one of four register types:
   - Holding Registers
   - Input Registers
   - Coils
   - Discretes
2. Click Add to insert an editable row where you specify the group name, starting Modbus address, and register size type if applicable to the register type.
3. Click Confirm.
4. Repeat steps 2 and 3 to include additional groups.
5. Click the Expand icon ( ) next to the Group name to display the accompanying register definition grid.

You can reference the following parameter descriptions to help you plan your group definition as you add tags to the group in the next procedure.

For holding and input registers, refer to the following table.

Type of Register	Parameter	Description
Holding and Input Registers	User Defined Register Name	The reporting register you would use instead of a name derived from a tag
	Starting Modbus Address	Starting Modbus address that the register is mapped to. This value is automatically assigned from the Starting Modbus Address of the group and accounts for the Register Size Type of the group and the Register Data Type of the register.
	Register Data Type	Data type of the Modbus register that the HCC2 tag is mapped to
	Unit Descriptor	Engineering units of the Modbus register. The base quantity (e.g., temperature, pressure) is inherited from the Tag Data Type and only the engineering units of the register (e.g., °C, °F, K, R) can be modified.
	Tag Mnemonic	An HCC2 tag name that you append to the tag prefix to form a fully qualified tag name that you map to the Modbus register. The tag mnemonic does not apply if the register is assigned a special function.
	Tag Name	Existing HCC2 tag that will be mapped to the Modbus register. Use the Select Tag button to open the Tag Selection window and choose a tag associated to one of the applications loaded in the HCC2. This parameter is not used if the register is assigned a Register Special Function.
	Tag Property Selection	Indicates the property of the HCC2 tag to be mapped to the Modbus register. Choose from Value (or Indexed Value), Timestamp Date, Timestamp Time, or Quality.
	Tag Data Value Index	For HCC2 tags that contain an array of indexed values, it indicates the data index to be mapped to the Modbus register. This setting is only used when the Tag Property Selection is set to Value.
	Tag Data Type	Data type of the HCC2 tag. This parameter is part of the tag properties and cannot be modified from the Modbus Protocol Map Editor.
	Is Command Register	If declared a command register, the HCC2 will permit multiple sources to produce the data point during the Unity deployment Data Point mapping Validation step.
	Enable Register Scaling	If True, the register value can be scaled using the Register Scale Factor and the Register Scale Offset parameters. For read queries, the scaling is applied to the Modbus register value prior to unit conversion. For write queries, the scaling is applied to the Modbus register value after the unit conversion is complete. Scaled Value = (Value * Register Scale Factor) + Register Scale Offset
	Register Scale Factor	Multiplier used to scale the Modbus register when Enable Register Scaling is set to True

Type of Register	Parameter	Description
	Register Scale Offset	Value added to the Modbus register when Enable Register Scaling is set to True
	Register Read Only	For Holding Registers only. Controls the write access of the register, providing an extra configuration layer for read-only registers in addition to the overall Modbus Server Access Restriction Options. If ReadWrite, values written to this register are accepted. If ReadOnly, values written to this register are ignored and no exceptions are generated.
	Register Special Function	Special function assigned to the register. When a Special Function is assigned, the Tag Name selection is ignored, and the values are provided by the selected function.
	Special Function Default Value	A default value may be specified when a register has been assigned a Special Function of Indirect Address 1.64 or Indirect Register 1.64. This allows for pre-configuration of the indirect addressing system.
	Initial Value	The initial value to register as a string

For coils and discretes, refer to the following table.

Type of Register	Parameter	Description
Coils and Discretes	User Defined Register Name	The reporting register you would use instead of a name derived from a tag
	Modbus Address	The Modbus address that the register is mapped to
	Tag Mnemonic	An HCC2 tag name that you append to the tag prefix to form a fully qualified tag name that you map to the Modbus register.
	Tag Name	Existing HCC2 tag that will be mapped to the Modbus register. Use the Select Tag button to open the Tag Selection window and choose a tag associated to one of the applications loaded in the HCC2. This parameter is not used if the register is assigned a Register Special Function.
	Tag Data Value Index	For HCC2 tags that contain an array of indexed values, it indicates the data index to be mapped to the Modbus register. This setting is only used when the Tag Property Selection is set to Value.
	Tag Data Type	Data type of the HCC2 tag. This parameter is part of the tag properties and cannot be modified from the Modbus Protocol Map Editor.
	Is Command Register	If declared a command register, the HCC2 will permit multiple sources to produce the data point during the Unity deployment Data Point Mapping Validation step.
	Register Read Only	For Coils only. Controls the write access of the register, providing an extra configuration layer for read-only registers in addition to the overall Modbus Server Access Restriction Options. If ReadWrite, values written to this register are accepted. If ReadOnly, values written to this register are ignored and no exceptions are generated.

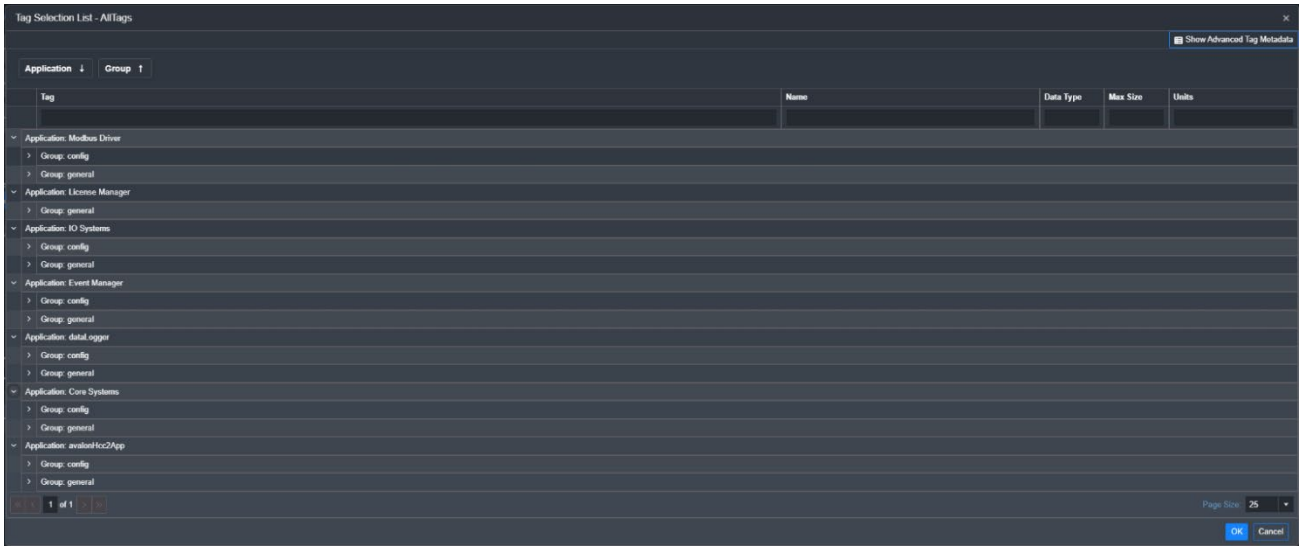
Type of Register	Parameter	Description
	Register Special Function	Special function assigned to the register. When a Special Function is assigned, the Tag Name selection is ignored, and the values are provided by the selected function.
	Special Function Default Value	A default value may be specified when a register has been assigned a Special Function of Indirect Address 1.64 or Indirect Register 1.64. This allows for pre-configuration of the indirect addressing system.
	Initial Value	The initial value to register as a string

8.7.3 Map Tags to the Server Register

After you selected the group definition for your server, you can select tags to map to your server register.

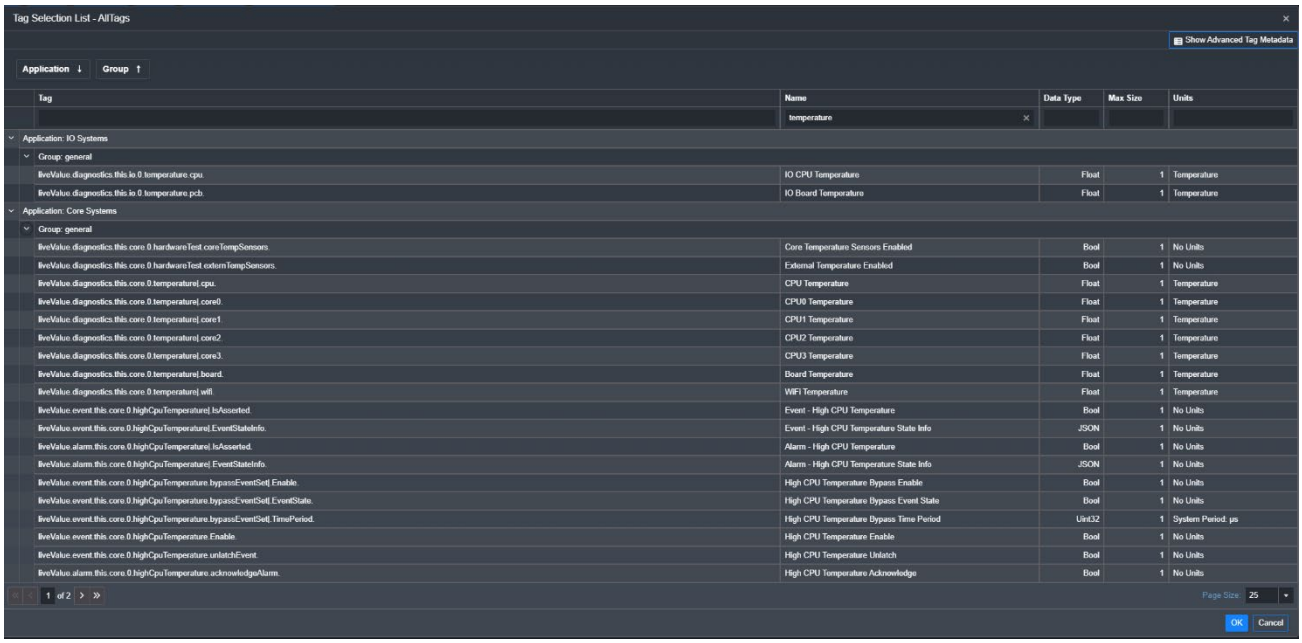
1. To select tags, click Add Multiple Tag Selections in the Register Definition grid inside a register group. The Tag Selection List – All Tags window opens.

   In this window, you can filter and choose tags from the available applications. Each application contains tag groups (general and config) that you can open by clicking the Expand icon ( ).



2. To search for specific tags, enter your filter criteria in the corresponding field—Tag, Name, Date Type, etc.—and press **ENTER** on your keyboard. The matching selections are returned.

   In this example, *temperature* is entered in the Name field.



3. Click and highlight the row(s) in the display to select your desired tags. To make multiple selections in the display, use **CTRL + Click**.
4. Click **OK** to add the tags to the register.
5. Repeat steps 1 through 4 to select additional tags.

8.7.4 Verify the Modbus Server Protocol

Expand the Documentation panel to review the details of the Modbus server protocol definition.

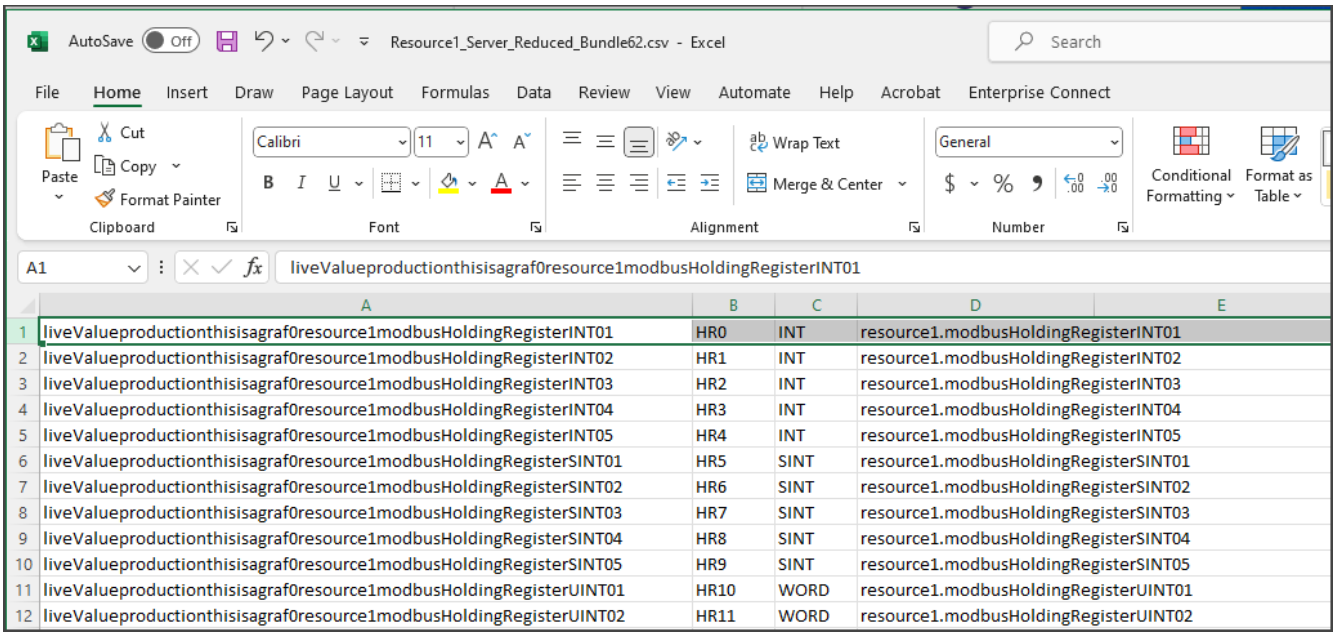
8.7.5 Validate and Download the Server Protocol Definition (.PDEF) File

To check whether the server protocol definition conforms with the rules, choose Download > Validation Report from the top menu bar to download a text file that contains any errors in your configuration.

Correct any errors. If there are no errors, you can download the server Protocol Definition file to your local system by clicking Download > .PDEF Protocol Definition.

8.7.6 Review Tag Definitions

You can view the tags that you have added to or selected for the specified registers. Click Download > .CSV Protocol Import File. A comma-separated variables (.csv) file is downloaded to your local system. You can open it in an Excel spreadsheet, as shown in the following example:

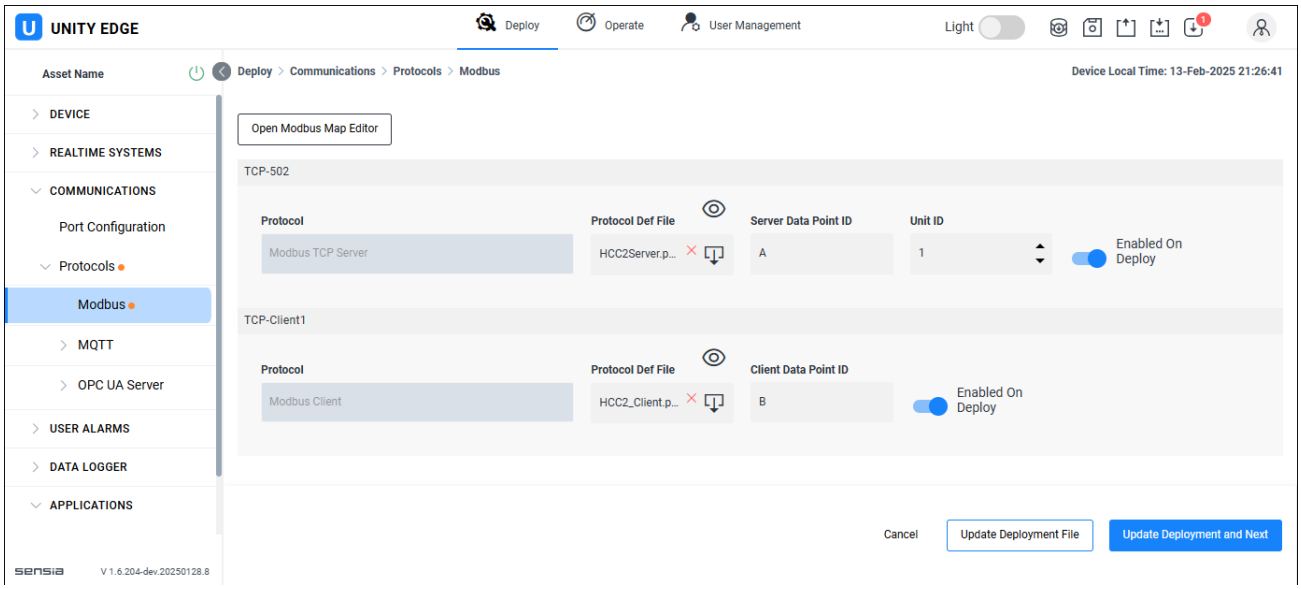


	A	B	C	D	E
1	liveValueproductionthisisagraf0resource1modbusHoldingRegisterINT01	HR0	INT	resource1.modbusHoldingRegisterINT01	
2	liveValueproductionthisisagraf0resource1modbusHoldingRegisterINT02	HR1	INT	resource1.modbusHoldingRegisterINT02	
3	liveValueproductionthisisagraf0resource1modbusHoldingRegisterINT03	HR2	INT	resource1.modbusHoldingRegisterINT03	
4	liveValueproductionthisisagraf0resource1modbusHoldingRegisterINT04	HR3	INT	resource1.modbusHoldingRegisterINT04	
5	liveValueproductionthisisagraf0resource1modbusHoldingRegisterINT05	HR4	INT	resource1.modbusHoldingRegisterINT05	
6	liveValueproductionthisisagraf0resource1modbusHoldingRegisterSINT01	HR5	SINT	resource1.modbusHoldingRegisterSINT01	
7	liveValueproductionthisisagraf0resource1modbusHoldingRegisterSINT02	HR6	SINT	resource1.modbusHoldingRegisterSINT02	
8	liveValueproductionthisisagraf0resource1modbusHoldingRegisterSINT03	HR7	SINT	resource1.modbusHoldingRegisterSINT03	
9	liveValueproductionthisisagraf0resource1modbusHoldingRegisterSINT04	HR8	SINT	resource1.modbusHoldingRegisterSINT04	
10	liveValueproductionthisisagraf0resource1modbusHoldingRegisterSINT05	HR9	SINT	resource1.modbusHoldingRegisterSINT05	
11	liveValueproductionthisisagraf0resource1modbusHoldingRegisterUINT01	HR10	WORD	resource1.modbusHoldingRegisterUINT01	
12	liveValueproductionthisisagraf0resource1modbusHoldingRegisterUINT02	HR11	WORD	resource1.modbusHoldingRegisterUINT02	

8.8 DEPLOYING THE PROTOCOL DEFINITION (.PDEF) FILE

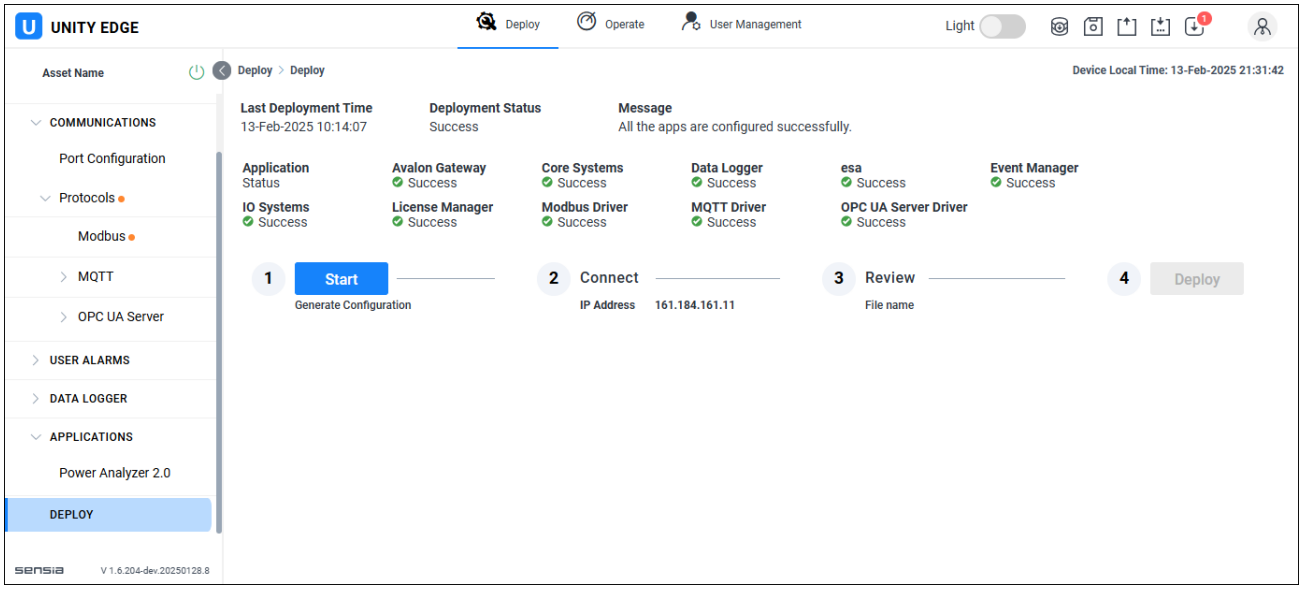
Verify that you have created appropriate serial or TCP port connections for your Modbus implementation. Refer to sections 8.3 and 8.4 for details.

1. Open your Unity Edge application and go to Deploy > Communications > Protocols > Modbus in the navigation tree.

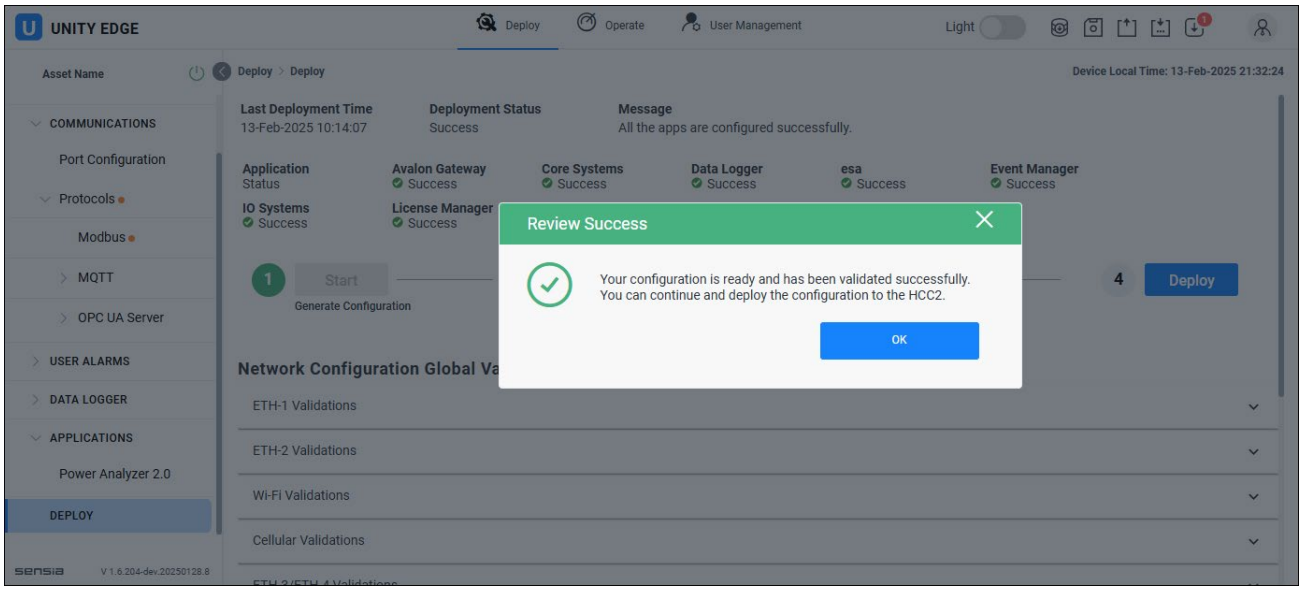


2. Select the client or server protocol instance you want to enable.
3. Under Protocol Def File, click to open File Manager. Search for, select, and load the recently created .PDEF file for the selected server or client instance.
4. In the Server Data Point ID or Client Data Point ID field, enter a short data point ID that will be appended to the path name of the data points you select for mapping: for example, server502. This prefix identifies all HCC2 data points having diagnostic and statistical information associated with the target server.

5. In the Unit ID field, enter the Modbus server unit identification number. The Modbus client does not have a unit ID as it uses the ID of the target server or servers to which it connects. This server ID is specified in the protocol definition file.
6. Move the Enabled on Display slider to the ON position if you want to enable the protocol settings immediately on deployment. Move the slider to the OFF position if you want to enable the settings after deployment (for example, if you want to do additional configuration first).
7. Click Deploy in the navigation tree and use the Deploy wizard to deploy the configuration to your HCC2 system.



8. Click Start to launch the deployment process. If the configuration of the .PDEF passes the system checks, you receive a Review Success confirmation message. Review the network configuration and tag connection validations and click OK to proceed.



9. Click Deploy to apply the configuration to the HCC2 system.

8.9 VERIFYING THE DEPLOYED CONFIGURATION

To view the tags that you assigned to the protocol definition file, do the following:

1. Go to Operate > Live Data to display the tags available to the HCC2.
2. To display your protocol definition files, enter the tag ID next to the search icon.
3. Verify that the data quality and current values of the tags are appropriate.

8.10 WORKING WITH A DEPLOYED PROTOCOL DEFINITION FILE

Sections 8.6 and 8.7 describe how to create a new Modbus protocol definition from scratch and deploy it to your HCC2 device.

You can, however, retrieve, edit, and re-deploy a Modbus protocol definition file currently being used by HCC2 device.

To retrieve a currently deployed Modbus protocol definition file, follow these steps:

1. Launch a window in your Google Chrome or Microsoft Edge web browser and enter your HCC2 IP address followed by a colon and the port number 7070 (as described in section 8.1, Modbus Protocol Map Editor, page 101).

   The Modbus Protocol Map Editor interface is displayed.

2. Click 

in the menu bar.

3. In the Open Protocol Definition window, click **Device Library**.

   The Device Library lists available Modbus protocol definition files under the App Title category.

4. Enter any filtering criteria to narrow the search to a specific type of definition file: for example, type `ModbusServer` in the Modbus Processor Type field.

5. Expand the App Title panel to reveal the available Modbus protocol definition files, as in the following example:

6. Select the desired protocol definition file and click Open Selected File.

   The header information of the selected file is displayed under the Protocol Definition Header.

7. Do the following tasks:
   a. Edit the existing data in the protocol definition file following the client or server configuration guidelines.
   b. Validate the updated definition file and download the updated revision to your local system.
   c. Deploy (re-deploy) the updated definition file to your HCC2 device.

Section 9: Installing and Configuring MQTT Sparkplug B

MQTT (MQ Telemetry Transport) is a lightweight TCP/IP based publish/subscribe protocol that is easy to implement and suitable for transporting a variety of data types. All MQTT endpoints connect to a centralized piece of software called a broker and do not connect to each other.

MQTT payloads are extremely flexible, which means that devices are interoperable only when they all use a common payload format. A popular payload format for MQTT communications is Sparkplug B. This is a binary format based on Google's protocol buffers technology that allows a variety of MQTT-equipped devices to exchange data.

Sparkplug is an open-source specification hosted by the Eclipse Foundation that gives MQTT clients the framework to seamlessly integrate data from their applications, sensors, devices, and gateways within the MQTT Infrastructure. It is developed on GitHub. The evolution of Sparkplug is governed by the Eclipse Foundation Specification Process (EFSP), and the specification can be accessed with this web link:

https://sparkplug.eclipse.org/specification/version/3.0/documents/sparkplug-specification-3.0.0.pdf

The aim of the Sparkplug Specification is to define an MQTT topic namespace, payload, and session state management that can be applied generically to the overall IIoT market sector while meeting the specific requirements of real-time SCADA/Control HMI solutions.

9.1 AUDIENCE

This guide is designed to give field engineers and operators a working knowledge of the MQTT application for the HCC2 and the steps for configuring and monitoring MQTT operations using the Unity Edge user interface. A basic understanding of MQTT communications is helpful.

9.2 MQTT FUNCTIONALITY FOR THE HCC2

The MQTT/Sparkplug B driver for the HCC2 is designed to operate within the HCC2 communication framework, providing access to HCC2 data over the MQTT protocol in the defined Sparkplug B payload. The data presented by the HCC2 is highly configurable, offering control over bandwidth usage, if desired.

The MQTT driver is a containerized HCC2 application that performs the following functions:

- Allows you to configure connections to two MQTT brokers, creating a high-availability system. Only one broker connection is active at a time, but if a broker fails, the MQTT driver will attempt to connect to the next enabled broker.
- Implements standard MQTT authentication types for broker connections, including:
  - No authentication
  - Username and password-based authentication
  - Certificate-based authentication
- Implements an encrypted Transport Layer Security (TLS) connection to the MQTT broker if configured to do so.
- Publishes the values and metadata (e.g., units) for user-selected data points using MQTT transport and Sparkplug B payload definitions.
- Updates data point values in the HCC2 via MQTT when the MQTT driver is configured for this optional function.

9.2.1 Theory of Operation

When the application is started, the following series of actions is triggered:

1. If a broker connection is configured, the driver tries to create a TCP/IP connection with the broker using the configured encryption method. If no broker is enabled, then the app does nothing.
2. If a connection cannot be made to the first broker, the app attempts to connect to a second broker if a second broker is enabled.
3. The app will try to connect once per second six consecutive times. If a connection cannot be made, the app will attempt a connection once per minute to reduce the demand on resources.
4. Once a connection is made with a broker, the driver will authenticate the broker, if required.
5. If authentication is successful, the driver will send a Sparkplug B NBIRTH (node birth) message. This message contains all the configured data points names and metadata at the node level, as well as initial values. Review the Sparkplug B specification for information about the Sparkplug B data model.
6. Next, the driver will send node level data point values as needed. The number of updates is limited by the data point's configured Maximum Update Time. An update will also be sent at a rate equal to or greater than each data point's configured Minimum Update Time.
7. Next, the driver will send DBIRTH (device birth) messages to bring devices online. Data points have a hierarchical name and are assigned to devices using their name. Most HCC2 data points have "this" in their name, which means that they are node level data points and not device level data points. If a device level data point does not exist, a DBIRTH message will not be issued.
8. If the configuration (which results in reconnection) changes, the driver determines whether any DDEATH (device death) or NDEATH (node death) messages are required. A death message indicates that the device or node has gone offline. The node or any device must go offline if the data point collection devices go offline. If an NDEATH or DDEATH message is sent, a new set of NBIRTH and DBIRTH messages will be issued as required.

9.3 INSTALLING AND CONFIGURING THE MQTT/SPARKPLUG B APPLICATION

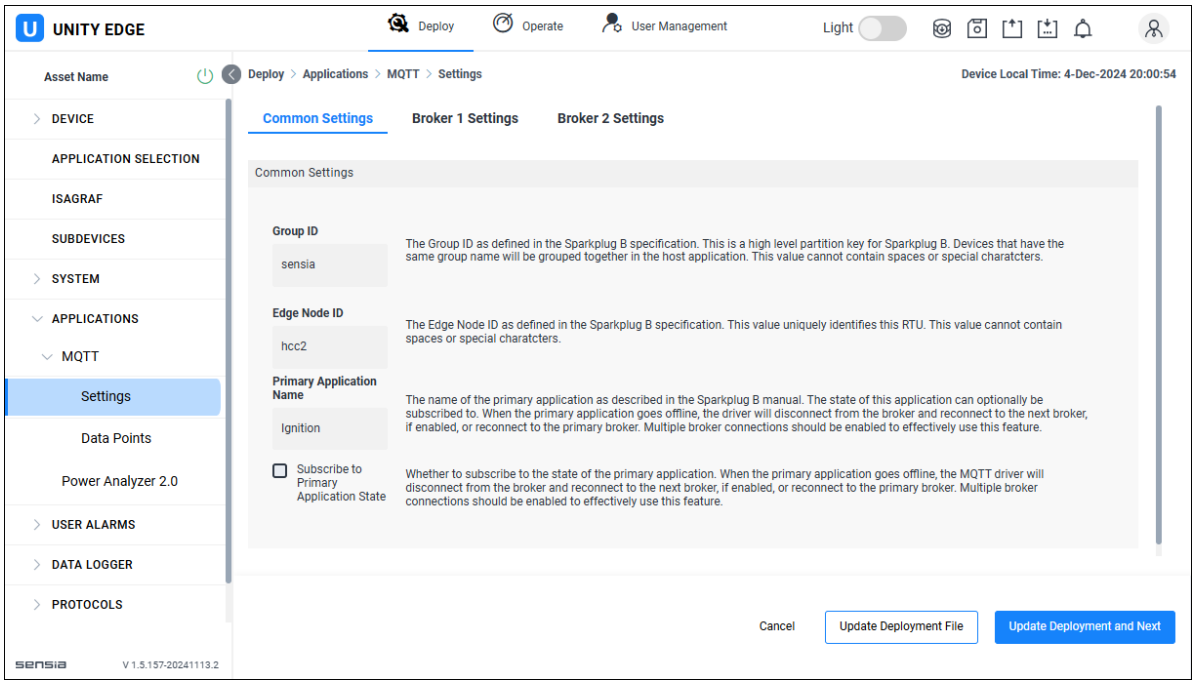
The MQTT/Sparkplug B application is among the core apps that are factory installed in the HCC2. The following sections describe how to configure the MQTT/Sparkplug B driver in the HCC2 and select HCC2 data points for exposing to Sparkplug B protocol.

If your HCC2 was manufactured before the MQTT application was commercially released, you will need to update your bundle installation to access this feature. See Section 4: Updating and Managing HCC2 Software, page 41, for details.

9.3.1 Configure the MQTT/Sparkplug B Driver

To configure the MQTT/Sparkplug B driver

1. Choose the Deploy menu in Unity Edge.
2. Navigate to Communications > Protocols > MQTT > Settings to access three tabbed screens with selections for specifying the common and broker settings for your Sparkplug B application.



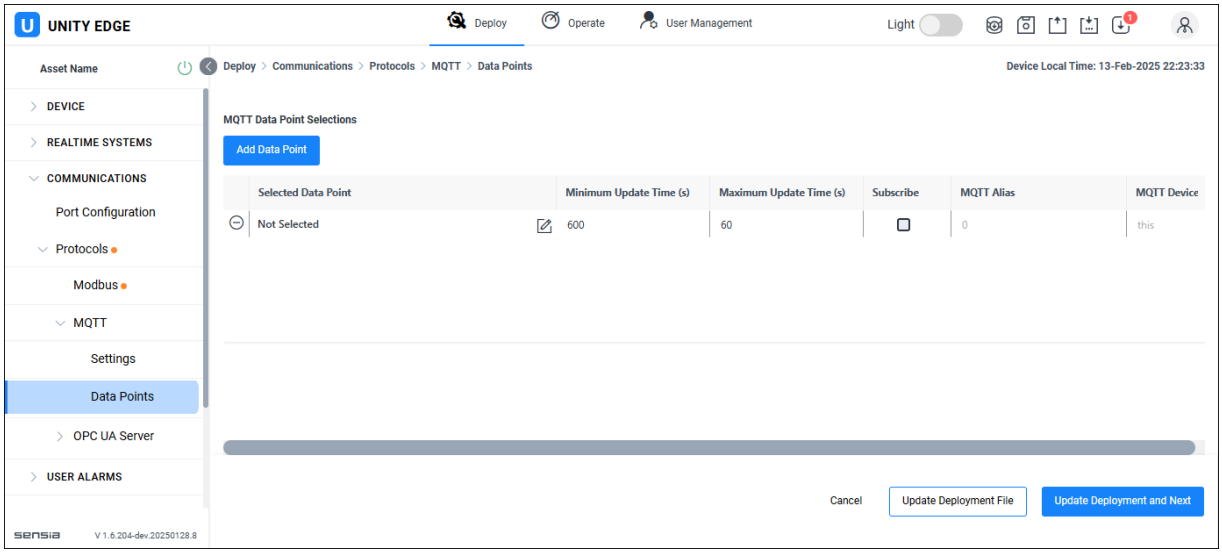
3. Review the default settings and change as needed to suit your application needs. Read the onscreen usage tips for help in making selections.

9.3.2 Select HCC2 Data Points for MQTT Communications

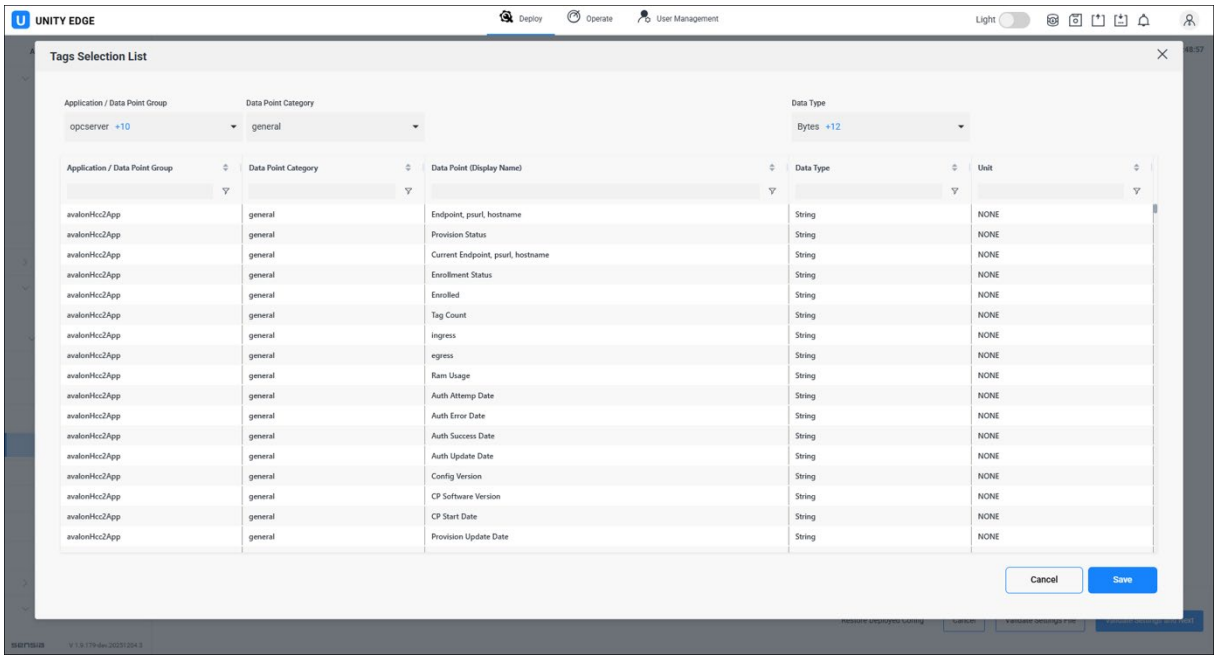
The ability to select HCC2 data points to expose to the Sparkplug B protocol is particularly useful in bandwidth-limited applications, where you only want to expose a certain amount of data over the network.

To make a data point selection

1. Click on the Communications > Protocols > MQTT > Data Points menu in the navigation tree.
2. Click on Add Data Point to add an entry row to an MQTT Data Point Selections table.



3. Click on the picker tool, select an HCC2 data point from the Tags Selection List, and click Save.



4. Update the minimum and maximum update times if necessary to suit your application.
5. Check the Subscribe checkbox to enable data points to be changed/updated via MQTT. The Subscribe function is disabled by default.

Note: The MQTT Alias and Device fields are not editable, but they provide information about the MQTT-specific identifiers for each data point.

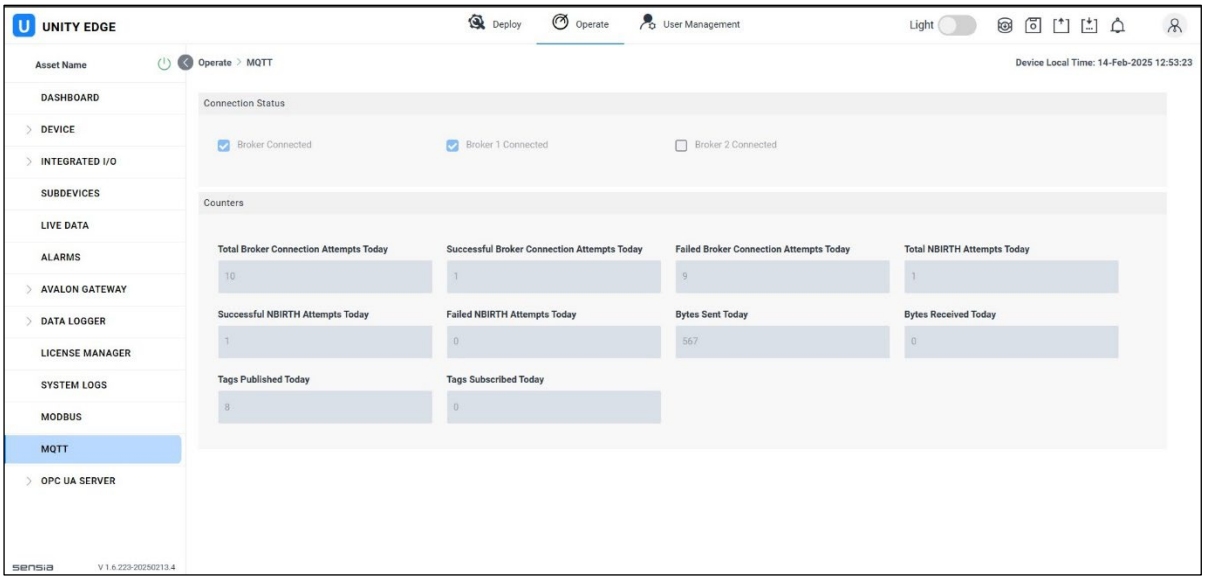
---

6. Repeat steps 2 through 5 to configure each new data point.
7. Perform a Deploy to write the changes to the HCC2.

9.4 MONITORING MQTT OPERATIONS

When your MQTT driver is fully configured and you have selected the data points you wish to expose to Sparkplug B protocol, you can monitor MQTT operations as follows:

1. Click the Operate > MQTT menu in Unity Edge.
2. Monitor the readouts for changes in broker connection status or counters indicating the health (success) of MQTT communications.


UNITY EDGE
Deploy
Operate
User Management
Light
Asset Name
Operate > MQTT
Device Local Time: 14-Feb-2025 12:53:23
DASHBOARD
DEVICE
INTEGRATED I/O
SUBDEVICES
LIVE DATA
ALARMS
AVALON GATEWAY
DATA LOGGER
LICENSE MANAGER
SYSTEM LOGS
MODBUS
MQTT
OPC UA SERVER
Connection Status
Broker Connected
Broker 1 Connected
Broker 2 Connected
Counters
Total Broker Connection Attempts Today
10
Successful Broker Connection Attempts Today
1
Failed Broker Connection Attempts Today
9
Total NBIRTH Attempts Today
1
Successful NBIRTH Attempts Today
1
Failed NBIRTH Attempts Today
0
Bytes Sent Today
567
Bytes Received Today
0
Tags Published Today
8
Tags Subscribed Today
0
sensia
V 1.6.223-20250213.4

Section 10: Setting Up and Configuring an OPC UA Server

The QRATE HCC2 controller's core applications now include an OPC UA Server application for visibility of HCC2 data and interoperability with OPC UA clients.

The application, which is compliant with the OPC Unified Architecture IEC62541 standard for data exchange, offers programmable control of the generated OPC address space, allowing OPC UA clients to read and write to HCC2 data points. This guide will step you through the process of configuring your HCC2 as an OPC UA server, selecting the data to be exposed to the server address space, and checking the OPC connectivity with an authenticated Client.

OPC UA address space is easily set up and logically organized by application and functionality. The versatile HCC2 data structures are preserved in the OPC address space and are constructed with arrays, structures, and folders where appropriate.

Access to the OPC UA server is controlled with programmable Security and Authentication modes. Once incoming clients are granted access, users can monitor OPC UA data in real time. Those who have write permissions can change writeable HCC2 data values and/or configuration settings from their client interface, creating new ways to control and configure the HCC2 and its applications.

10.1 CONFIGURING YOUR HCC2 AS AN OPC UA SERVER

The first step in adding OPC UA functionality to your HCC2 controller is to configure an OPC UA server driver in the HCC2's Unity Edge interface.

OPC UA is accessible through any of the HCC2's Ethernet and wireless network interfaces. If accessing the server from a non-local network, it must be on the interface selected as the *Internet Selection.* See section 2.4, Internet Interface Selection, page 24, for more information.

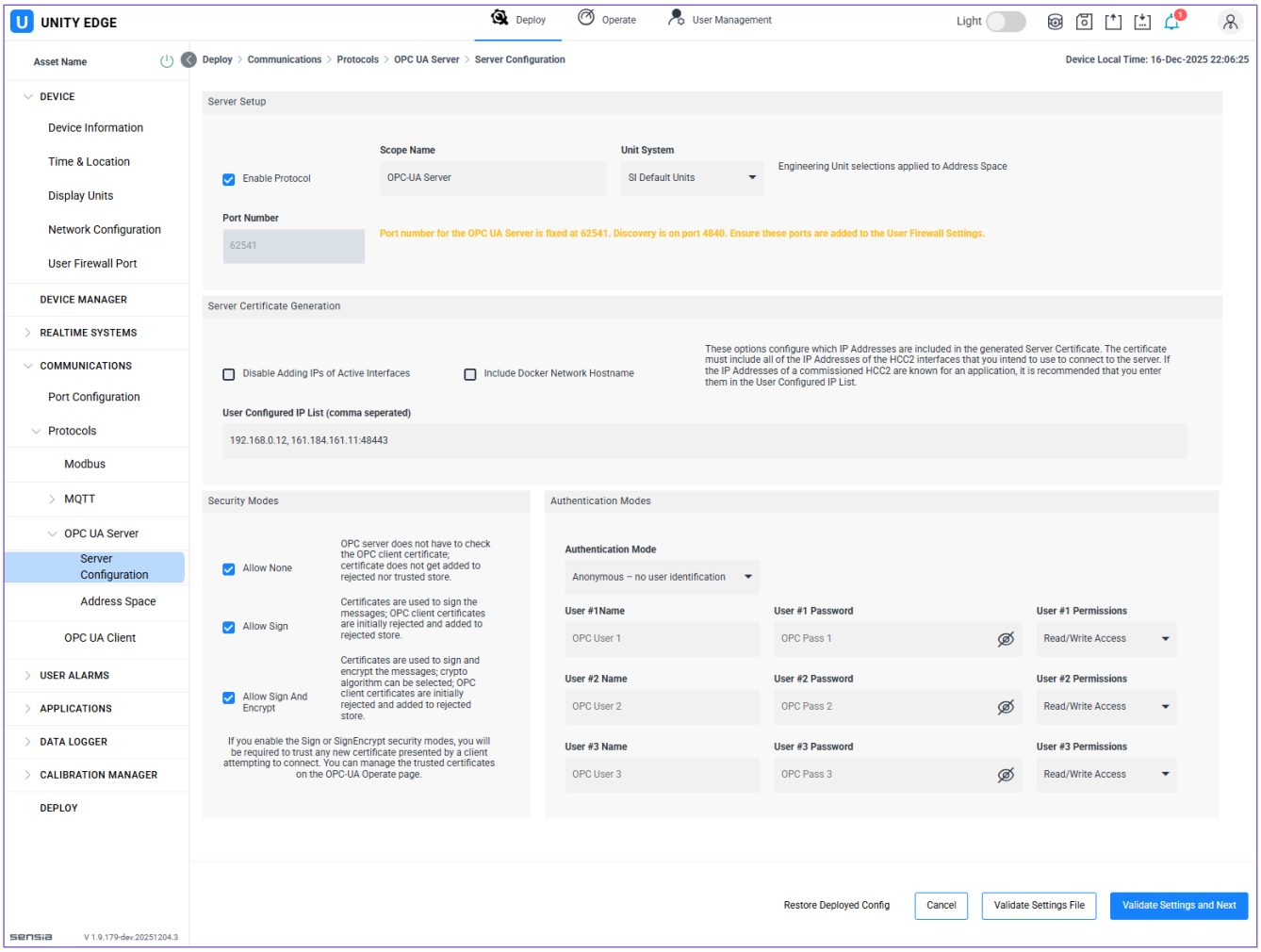
The OPC UA application is among the core apps that are factory installed in the HCC2. The following sections describe how to configure the OPC UA server driver, open server ports, and configure the OPC UA address space.

If your HCC2 was manufactured before the OPC UA application was commercially released, you will need to update your bundle installation to access this feature. See Section 4: Updating and Managing HCC2 Software, page 41, for details.

10.1.1 Configure the Server Driver

To configure the server driver, perform the following steps:

1. Navigate to Deploy > Communications > Protocols > OPC UA Server > Server Configuration.



2. Click the Enable Protocol checkbox.
3. Enter a Scope Name to uniquely describe the HCC2 you are configuring.
4. Select the unit system to be applied to data in the OPC address space using the dropdown menu. Selections include
    - HCC2 Base Units
    - SI Default Units
    - US Customary Units
    - Unity Selected Units

Important The first three selections comprise preset units. Unity Selected Units, by contrast, provides full customized control over unit selection, allowing you to specify units from any measurement category. When you deploy the HCC2 OPC UA configuration, the server will be instantiated with those settings.

5. Note the server port number 62541 that is fixed for OPC UA support. To access the server, you will need to open this port and an OPC UA discovery port in the HCC2 Firewall settings in a later step.
6. Configure the server certificate generation. An OPC UA server must generate and present a security certificate to requesting clients. This certificate must contain a list of all valid IP addresses you intend to use to connect to the server. There are three options for specifying the source of an IP address included in the HCC2 certificate.

- Add the IP address of each HCC2 active Ethernet interface. This method is enabled by default. It captures only the IP addresses of interfaces that are enabled and linked at the time of deployment.
- Include the Docker Hostname. Enable this option if you are connecting to the server from within the HCC2 Docker network.
- User Configured IP List. If the IP addresses of a commissioned HCC2 are known for an application, enter them in the User Configured IP List.

7. Choose the message security (data transfer) mode(s) that control the types of connections clients are allowed to make. For either “signed” mode, the client and the server will exchange certificates and authenticate the connection so that we know which client is attempting to connect to an HCC2 and to which OPC UA server.

   - Allow None - OPC server does not check for an OPC client certificate. Any client can connect, and no shared certificate will be stored.
   - Allow Sign - Certificates are used to sign all messages.
   - Allow Sign and Encrypt - Certificates are used to sign and encrypt all messages; crypto algorithm can be selected by the connecting client.

When either or both “signed” modes are selected, the client and the server will exchange certificates to authenticate the identity of the client attempting to connect to an HCC2 and the HCC2 OPC UA server targeted.

Important Initially, exchanged certificates will be rejected by both the server and the client. Within Unity Edge, you must manually trust certificates presented by clients on the Operate > OPC UA Server > Trusted Certificates page.

8. Choose an Authentication Mode.

   a. Choose *Anonymous* if no user authentication is desired. Anonymous users will have read and write access as established when configuring the Address Space.

   b. Choose *Username and Password* to enable authentication by user identity. Up to three users can be configured. Each user name must be unique and cannot be the reserved “Anonymous” user name. There are no restrictions on the password that the OPC UA standard or that the HCC2 driver imposes, other than not accepting blank passwords. A blank username or blank password will generate the `BadIdentityTokenRejected` error response.

      In the User Permissions column, select a permission level for each user. Here, you can grant a user *Read/Write Access* or restrict the user to *Read Only Access*. A user with write permissions can only write to applications and functionalities that were configured to permit writes when the Address Space was configured.

10.1.2 Open the Server Ports

The TCP ports required by the OPC UA Server are not opened in the HCC2 firewall in the default state. These TCP ports must be opened by the user manually as follows:

1. Click Deploy > Device > User Firewall Port.
2. Click Add Port.
3. Enter the OPC Server Port with the following parameters (see step 6 in section 10.1.1, Configure the Server Driver, page 131).

   a. Port Number 62541. This is the fixed HCC2 OPC UA Server port.

   b. Select the connected network interface over which the client will connect.*

   c. Select TCP as the Port Type.

   d. Provide a description of “OPC-UA Server.”

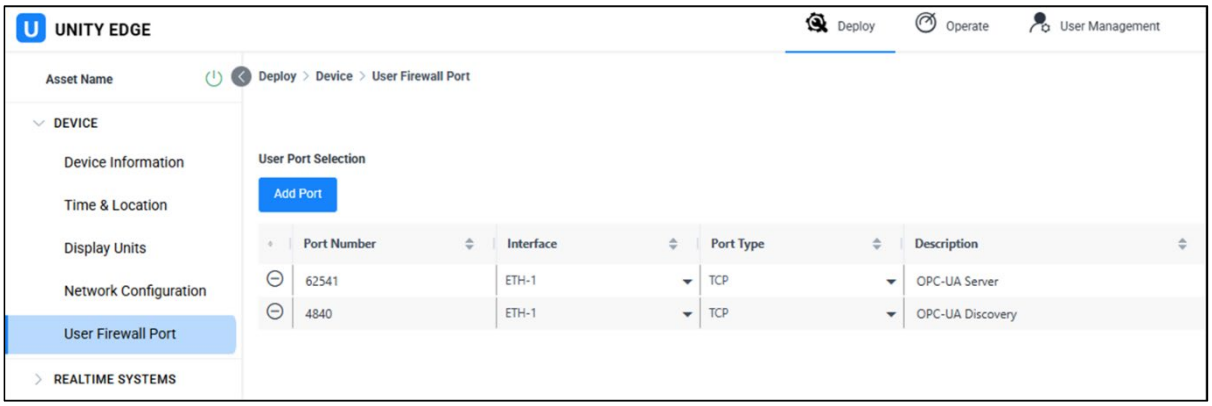
4. Enter the OPC Discovery Port with the following parameters.

a. Port Number 4840. This is the standard HCC2 OPC UA discovery port.

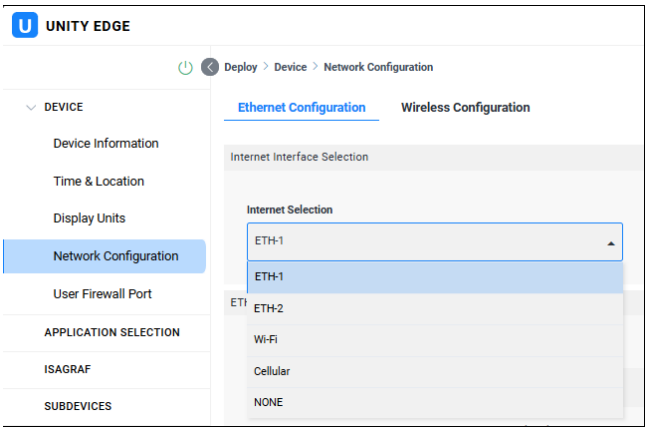
b. Select the connected network interface over which the client will connect.*

c. Select TCP as the Port Type.

d. Provide a description of “OPC-UA Discovery.”



5. If you are connecting to the OPC UA Server from an IP address external to the HCC2 network, you must select the attached network interface as the Internet Selection on the Deploy > Device > Network Configuration page.

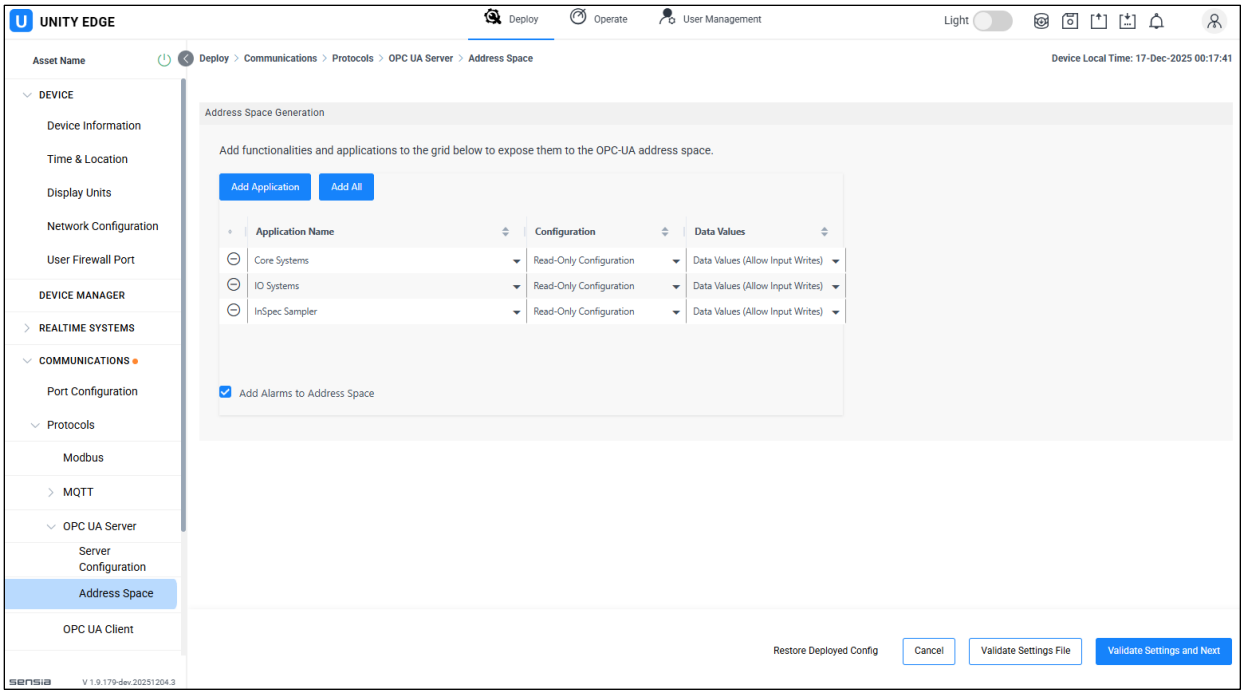


10.2 CONFIGURING THE OPC UA ADDRESS SPACE

When you have added an OPC UA server to your HCC2, you are ready to choose the applications and functionalities you wish to expose to clients in the OPC UA address space.

1. Click Deploy > Communications > Protocols > OPC UA Server > Address Space.

   By default, the Core Systems and I/O Systems are pre-selected to be added to the address space. However, you can add or delete applications using the buttons provided. Customize the selected Application Names to expand or restrict the exposure of HCC2 configuration and data values to suit your specific needs.



2. Add one or more applications as follows:
   - Click *Add Application*. A row will appear with a dropdown selection containing all applications that are not already populated in the Application list. Select the application you desire.
   - Click *Add All* to add all of the available applications in one step. You can easily delete any unwanted applications by pressing the Delete icon at the start of each row.

Note — If the Add Application and Add All buttons are inactive (grayed out), all available applications are already added to the Address Space Generation list.

3. For each of the selected applications, select the level of configuration access you will allow OPC UA clients to have:
   - Exclude Configuration – configuration settings will not be available
   - Read-Only Configuration – configuration settings will be present but not writable
   - Read-Write Configuration – configuration settings will be present and writable
4. For each of the selected applications, select the level of data value access you will allow OPC UA clients to have:
   - Exclude Data Values – data values will not be available
   - Read-Only Data Values – data values will be available but not writable
   - Data Values (Allow Input Writes) – data values will be available and writable

Note — If you want OPC UA clients to provide inputs to an application, you should configure the application to allow input data point writes to data values, and possibly enable read-write access to configuration settings.

5. If you wish to include all HCC2 alarms registered by Core services and applications in the address space, make sure the *Add Alarms to Address Space* checkbox is checked.
6. Click the Validate Settings File button to save your settings.
7. Deploy the OPC UA configuration to the HCC2 using the Deploy menu in the navigation tree.
   a. Click Start.

b. Click OK in the Review Success validation popup message. If conflicts are identified, resolve them before proceeding.

c. Click the Deploy button to propagate the changes to the HCC2.

10.3 CHECKING OPC UA SERVER-CLIENT CONNECTIVITY

When your HCC2 server driver has been configured and deployed, you are ready to configure a client connection and check connectivity with the server.

Note	For demonstration purposes, this manual describes the generic operations required for an OPC UA Client. Actual client software or client device configuration will vary and small differences in nomenclature and parameter selections can be expected.

10.3.1 Add the OPC UA Server to a Client

1. Locate the IP address of the HCC2 on the network interface that provides the connection to the client. This can be viewed within Unity Edge on the Operate > Device > Network Status page in the Assigned IP address field of the connected network interface.
2. Ensure that the server port and discovery port have been added to the Deploy > Device > User Firewall Port screen and the configuration has been deployed. See section 10.1.2, Open the Server Ports, page 133.
3. Provide the client, Global Discovery Server (GDS), or Local Discovery Server (LDS) with the server's discovery endpoint URL which will be of the form:
4. `opc.tcp://X.X.X.X:4840` where "x.x.x.x" is the IP address from step 1
5. If using a client application, you should be able to perform a custom discovery at that endpoint URL.
6. An OPC UA client can then browse the HCC2 "4840" discovery port (identified in step 3) to discover the available nodes on the server. From the browse results, select the server on port 62541. Typically, this node will appear in the form:

   `opc.tcp://X.X.X.X:62541/HCC2/OPCServer` where "x.x.x.x" is the IP address from step 1
7. Depending on the security modes selected during the server configuration, some or all of the following connection options will be available:
   - None (uatcp-uasc-uabinary)
   - Sign – Basic256Sha256
   - Sign – Aes128_Sha256
   - Sign – Aes256_Sha256
   - Sign & Encrypt – Basic256Sha256
   - Sign & Encrypt – Aes128_Sha256
   - Sign & Encrypt – Aes256_Sha256
8. Configure the client Authentication settings to match the configured server Authentication modes. The HCC2 OPC UA server supports one of the following:

   a. If the Server authentication is Anonymous – No User Identification, configure the Client authentication setting to be Anonymous.

   b. If the Server authentication is Username and Password, provide the Client with the configured username/password credentials for one of the users programmed on the Unity Edge page Deploy > Communications > Protocols > OPC UA Server > Server Configuration.

10.3.2 Connect to the Server

Because OPC UA connections often require some level of authentication, it is common to receive an error message on your initial attempt to connect to the HCC2 OPC UA server.

On a connection attempt, the Server and Client will each initiate an exchange of certificates (unless connected with the None security mode). By default, any new certificates received by either side will be rejected. You must manually trust the certificate in both the Client and Server to achieve a connection.

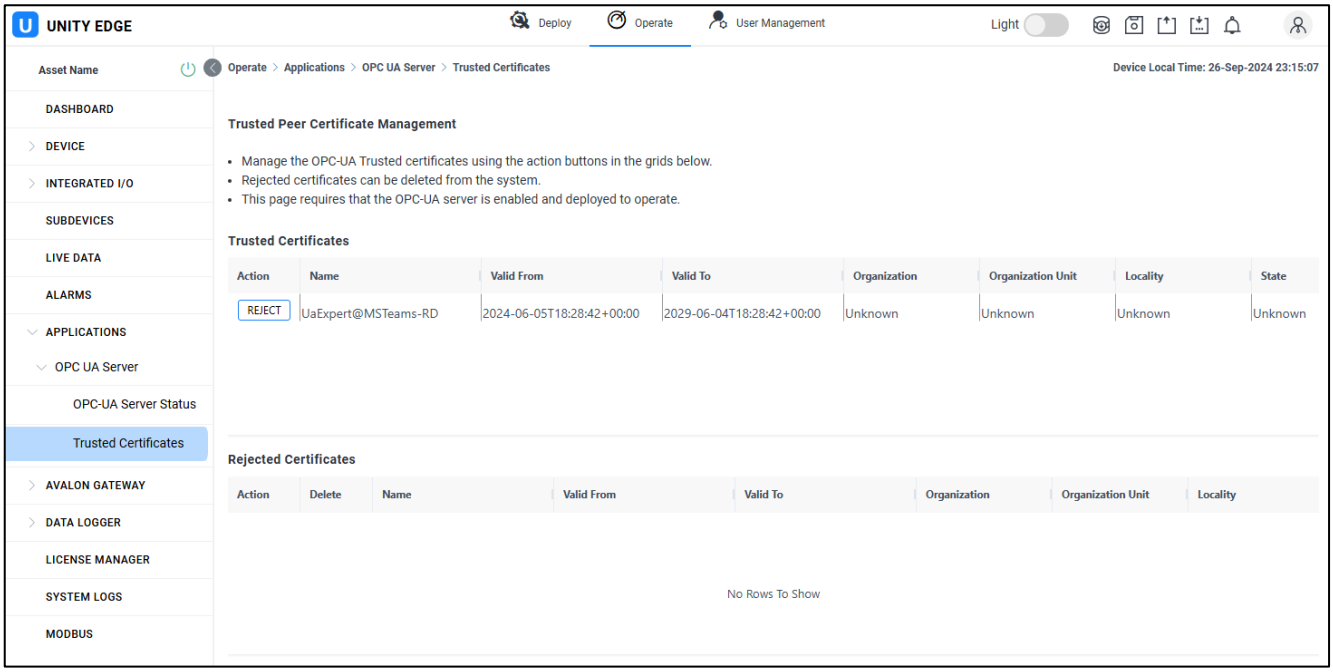
For PC software clients, the first connection attempt to a server will usually cause a BadRejectedCertificate exception response and you will be prompted if the new certificate should be moved to the Trusted store. Some client devices may require a transfer of the new certificate file from a Rejected folder to a Trusted folder on the device.

On the HCC2, the Trusted Certifications for the OPC UA Server are managed within the Unity Edge interface.

Manage Trusted Certificates

After the client attempts to connect to the HCC2 OPC UA server and the connection fails due to a BadRejectedCertificate, return to Unity Edge and navigate to the Operate > OPC UA Server >Trusted Certificates menu.

Important The functions supported by the Trusted Certificates screen are accessible only when the OPC UA server application is enabled and deployed in Unity Edge.



From the Trusted Certificates screen, you can identify each client certificate that has been exchanged with the server. All unknown certificates are categorized as “rejected” when you attempt a first-time connection, so do not be alarmed when the Client logs an error message.

If you have the Trusted Certificates window open in Unity Edge while you initiate a connection in the Client interface, you will see that even though an error is logged in the Client, the HCC2 responds by creating a certificate and storing it in the Rejected Certificates list.

To accept the certificate as a trusted Client of the HCC2 Server application, click TRUST. The certificate will be moved to the Trusted Certificates list and connection requests from that client will be permitted.

To decline the rejected client certificate and remove it from the system, click DELETE.

You can also remove a Trusted Certificate from the system if necessary. Simply click the REJECT button next to any trusted certificate to move it to the Rejected Certificates list. Then click DELETE to remove it from the system.

First-Time Connection

When the client is configured with the server's endpoint URL, connection security mode, and connection authentication mode, you are ready to connect the client to the OPC UA server. The following steps are typically used to create the connection:

1. Initiate a connection (or reconnection) in the client interface.
2. For first-time connections, check the Client log for error messages. A "BadSecurityCheck" error is commonly generated but is only an indication that a client certificate has not yet been "trusted" by the server.
3. Trust the HCC2 OPC UA Server certificate in the client when prompted. Some systems may require the certificate to be moved from a Rejected folder to a Trusted folder.
4. From Unity Edge, open the Operate > OPC UA Server > Trusted Certificates page.
5. Click TRUST to accept the Client certificate and authorize the HCC2 to transfer all available OPC UA server data to the address space of the Client.
6. Repeat the connection attempt in the client interface. With the certificates now trusted by both the client and the server, the connection should succeed.

Unsupported Security Policy

If a client attempts to connect to the OPC UA Server with a security policy that is not allowed by the server configuration at deployment, you will receive an Unsupported Security Policy notification. Confirm/update your settings and attempt another connection.

10.4 OPC ADDRESS SPACE VARIABLE MAPPING

All of the data variables available to a client are presented in the server address space. The client can form Data Access Views with the server to begin collecting HCC2 data points.

When the HCC2 is deployed, any changes to the OPC-UA address space will cause the server to temporarily go off-line so that the address space can be modified with all changes. Nodes that persist over the deployment will not experience any pathing changes or broken links.

In this section, we will examine some of the application groupings commonly displayed in the Archive Space after you make a connection to the OPC UA server. For each application and functionality, a description of the constructed folders and available Nodes is provided.

10.4.1 Address Space Data Formats

NodeIDs created within the server address space will match the definitions provided in HCC2 data point metadata as closely as possible. No datatype conversions are required because OPC UA supports all the datatypes of the HCC2.

OPC Analog Items will be used to construct NodeIDs for HCC2 data points that have non-Unity measurement categories. These Analog Items will have scalars to follow the Units System option setting for the relevant measurement category chosen when configuring the server driver in Unity Edge. See section 10.1.1, Configure the Server Driver, page 131.

HCC2 data points that contain data arrays will be created as NodeIDs with array data.

Complex HCC2 data points represent atomic structures and can contain multiple sub data points all sent in a single publication. These complex data points are created within the address space as an Object Node Class and will contain a Variable Node Class item for each sub data point. Because the complex data point represents an atomic structure in the HCC2, if a write operation is performed on any of the items in the Object, the entire complex data point is published within the HCC2 data bus.

10.4.2 Address Space Data Grouping

HCC2 automatically groups data in accordance with the data point structure as it populates the address space. You can customize the content of the address space by adding or removing applications and functionalities. This section details the structure and capabilities of the individual applications and functionalities available.

Core Systems

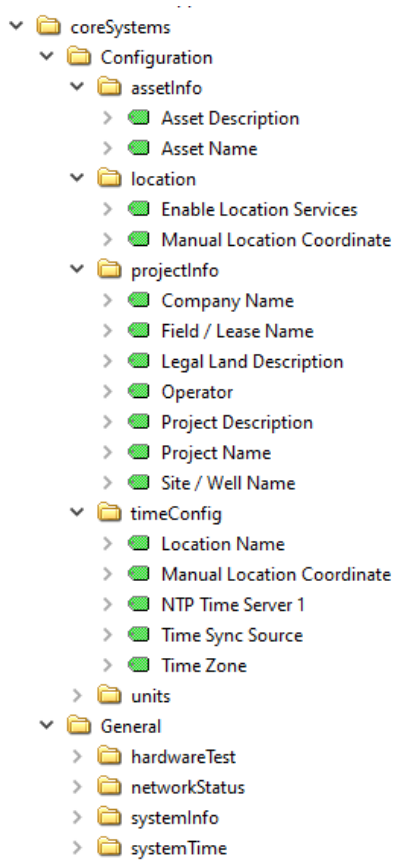
The coreSystems folder contains HCC2 configuration information as well as system status.

Core System Configuration (coreSystems/Configuration folder):

- Allows reading and writing of HCC2 identification information: Asset Info, Location, and Project Info. Writes are permitted when enabled during address space configuration.
- Time Configuration settings are available.

Core System General Status (coreSystems/General folder):

- The network status of all network interfaces is available.
- System Info folder contains system values such as CPU usage, disk usages, memory usage, hardware details, OS details, and device temperature.
- System time and the status of the device time servers and server connections are available.



Integrated I/O

The integrated I/O of the HCC2 is represented within the OPC address space in the context of how each input and output is configured within Unity. The inputs are outputs are organized in the following folders.

Analog Inputs (analogIn folder):

- Each analog input channel (Ch1 through Ch8) has a percentage value. This is the percentage of the configured input range of each input.
- For each Analog Input channel that was mapped to a HCC2 data point, the data point will be included in the folder. The Node display name will be constructed with a prefix of “(aiX)” where “X” is the analog input channel number. Following this prefix is the Display name of the data point.

Analog Outputs (analogOut folder):

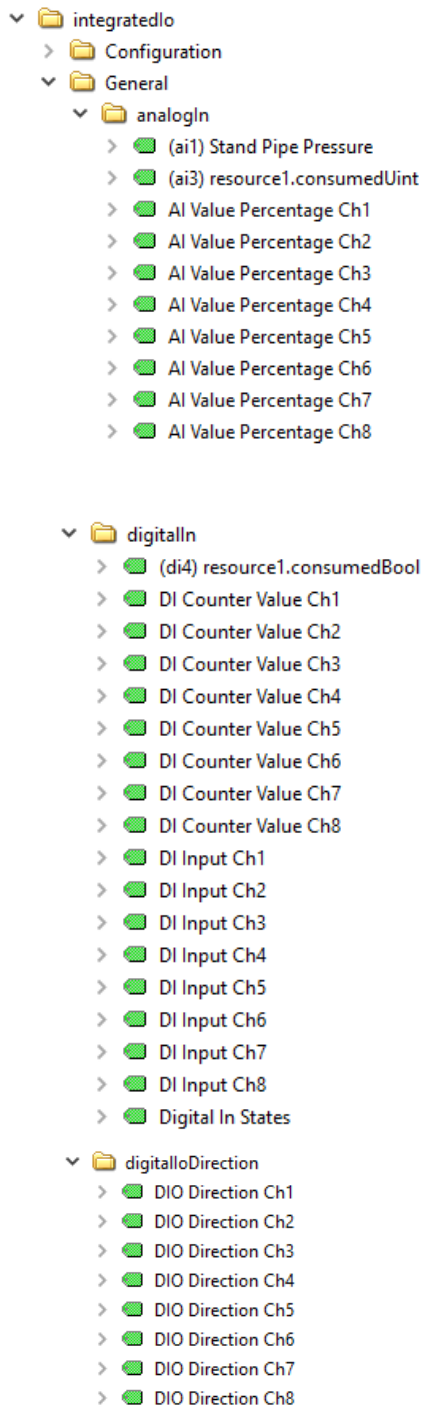
- AnalogOut Ch1 and Ch2 each have a percentage output value. This is the percentage of the configured output range of each output.

Digital Inputs (digitalIn folder):

- Digital In Ch1 through Ch8 each have a Boolean state value. This is the current state measured by the digital input.
- Digital In Ch1 through Ch8 each have a Counter Value. This is the rolling digital input pulse count measured by the digital input.
- Each HCC2 data point that is mapped to a Digital Input channel is included in the folder. The Node display name contains a prefix of “(diX)” where “X” is the analog input channel and the Display name of the HCC2 data point.
- The folder also includes a Digital In States Node. This is a bitmask Byte for which di1 is the least significant bit and di8 is the most significant bit.

Digital Input/Output Direction (digitalIoDirection folder):

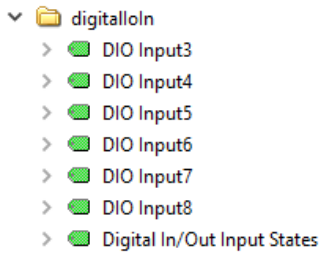
- This folder contains a Node for each of the digital Input/Output ports. A value of 0 indicates the port is configured as an output. A value of 1 indicates it is configured as an input.



Digital Input/Output Inputs (digitalloIn folder):

- Each digital Input/Output port configured as an input has a Node indication of its current state.

- The folder also includes a Digital In/Out Input States Node. This is a bitmask Byte for which dio1 is the least significant bit and dio8 is the most significant bit.

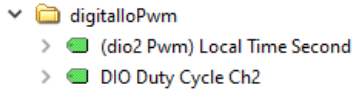


Digital Input/Output Outputs (digitalloOut folder):

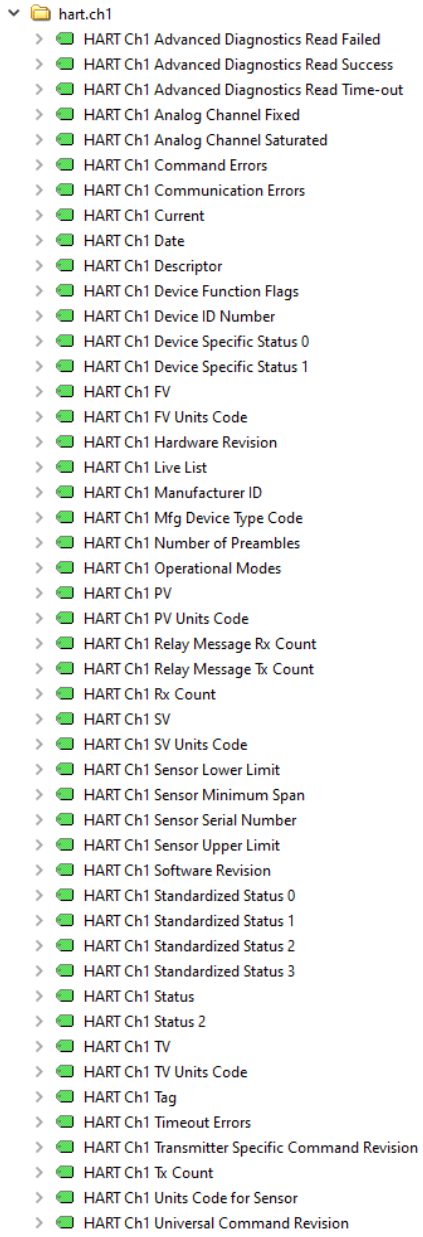
- Each digital Input/Output port configured as an output has a Node indication of its current state.
- Each HCC2 data point that is mapped to a Digital Input/Output channel is included in the folder. The Node display name contains a prefix of “(dioX Out)” where “X” is the DIO channel, and the Display name of the HCC2 data point.
- The folder also includes a Digital In/Out Output States Node. This is a bitmask Byte for which dio1 is the least significant bit and dio8 is the most significant bit.

Digital Input/Output PWM Output (digitalloPwm folder):

- Each digital Input/Output port configured as a Pulse Width Modulated (PWM) output has a Node indication of its current Duty Cycle value.
- Each HCC2 data point mapped to a Digital Input/Output channel is included in the folder. The Node display name contains a prefix of “(dioX PWM)” where “X” is the DIO channel, and the Display name of the HCC2 data point.



- **HART Channels 1 to 4 (hart.chX folders):**



- Analog Inputs 1 through 4 can each be configured as a HART transmitter input. If enabled, all of the HART data values and transmitter states are available.

I/O Supply Power Status (supplyPower folder):

The following Nodes are available:

- Supply Current
- Supply Power (computed)
- Supply Voltage
- Supply Power Input A Energized
- Supply Power Input B Energized

I/O System Status (systemReadings folder):

The following Nodes are available:

- IO Board Temperature
- IO Rail Voltage 1.2V
- IO Rail Voltage 3.3V
- IO Rail Voltage 5V

ISaGRAF Resources

The four available HCC2 ISaGRAF resources are added to the address space when user_customISaGRAF is selected on the Address Space Generation page. The resources have designated folders named “isagraf1”, “isagraf2”, “isagraf3”, and “isagraf4”. The resource folders each contain “consumed”, “produced”, and “status” folders.

Mapped ISaGRAF Consumed Variables (consumed folder):

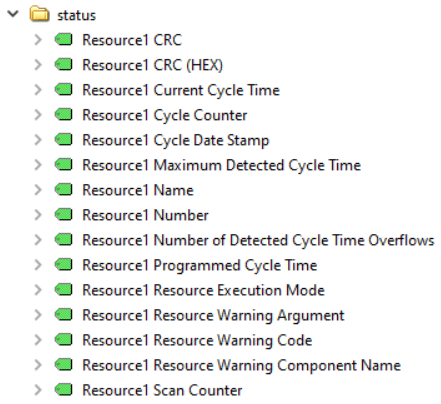
- Each variable that is a consumed ISaGRAF variable (an input to the ISaGRAF resource) is present.
- Each Node has the same datatype and measurement category as the HCC2 data point mapped to the ISaGRAF variable.
- The Node name follows this format: “(ISaGRAF variable name) Data Point Name”

Mapped ISaGRAF Produced Variables (produced folder):

- Each variable that is a produced ISaGRAF variable (an output from the ISaGRAF resource) will be present.
- Each Node has the same datatype and measurement category as the HCC2 data point mapped to the ISaGRAF variable.
- The Node name follows this format: “(ISaGRAF variable name) Data Point Name”

ISaGRAF Resource Status (status folder):

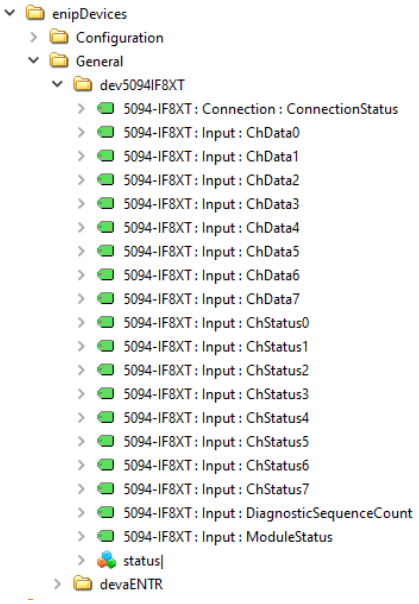
- The Resource CRC (or HASH) can be viewed to verify the program binary being executed.
- All of the standard ISaGRAF runtime metrics can be monitored during runtime.



ENIP Subdevices

Each connected ENIP Subdevice will be represented as a subfolder in the enipDevices/General folder. This subfolder will contain the following:

- Each mapped attribute is present and in the datatype and data format presented by the ENIP device.
- If a Node represents an ENIP output attribute, write permissions are available to users and address spaces configured to permit writes.



- Each ENIP device folder will contain a status structure with metrics on the ENIP device communication and connection.

User Applications

User applications added to the address space each have a Configuration and General folder. Folder contents of are driven by the data points created within the application.

Application Configuration Data Points (Configuration folder):

- Application configuration data points marked with the `_noprotobuf = true` metadata field are changed only during deployment. These data points will always be read only within the OPC address space.
- Configuration data points can only be written to if configuration writes are enabled when constructing the address space.
- When a client writes to a configuration data point, the updated value is sent to the internal bus for validation. Any `_callback` validation functions assigned to the data point by the application will be performed. If the validations fail, the value will not be stored within the persistence system and the Node will indicate a bad quality.
- Application data points are grouped by sub-topic hierarchy. For logical grouping of application data points in the address space, include associated data points under a sub-topic such as the following: `Livevalue.postvalidConfig.this.myFunctionality.0.subtopic.dataPointName.`
- Application data points that are not grouped under a sub-topic are placed in an `ungrouped` folder.

Application Data Points (General folder):

- Application data points marked with the `_input = true` metadata field may be written to if writes to inputs was enabled when constructing the address space.
- Application data points are grouped by sub-topic hierarchy. For logical grouping of application data points in the address space, include associated data points under a sub-topic such as the following: `Livevalue.producation.this.myFunctionality.0.subtopic.dataPointName.`
- Application data points that are not grouped under a sub-topic are placed in an `ungrouped` folder.

User Modbus Maps

The OPC server can provide access to the current values presented by HCC2 Modbus Servers and HCC2 Modbus Clients.

Adding an active Modbus Server map to your address space is a powerful way to create custom collections of data points in an address space. It can also serve as a debugging tool to review values being presented to Modbus clients.

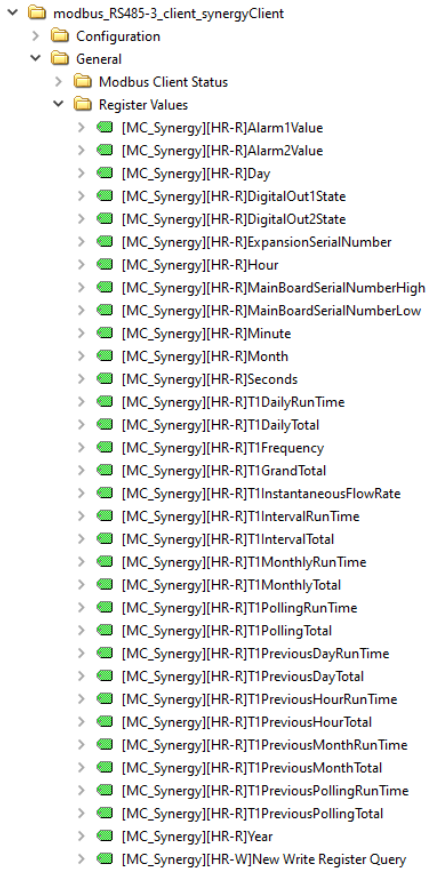
Adding an active Modbus Client to your address space allows you to view the status of all active Modbus read queries. The timestamp and data quality will indicate when the last transaction was performed and if it was successful. Modbus write queries can also be triggered by writing to the OPC address space.

Modbus Server Configuration Data Points (modbus_Port_server_serverID folder):

- The Modbus serverID is provided by the user when configurating the Modbus server protocol.
- The Modbus Server statistics are available in a subfolder named Modbus Server Status. This folder also contains writable Nodes for enabling/disabling the server and resetting the statistics.
- All register values from the Modbus Server are presented in a Register Values folder. Nodes in this folder are writable only if the HCC2 data point assigned to the Modbus register is marked as an Input and writes to inputs are allowed in the address space.
- The data quality of the register values indicates the quality of the HCC2 data point, not that of a Modbus transaction state.

Modbus Client Configuration Data Points (modbus_Port_client_clientID folder):

- The Modbus clientID is provided by the user when configurating the Modbus client protocol.
- The Modbus Client statistics are available in a subfolder named Modbus Client Status. This folder also contains writable Nodes for enabling/disabling the client and resetting the statistics.
- All register values from the Modbus Client are presented in a Register Values folder. Nodes in this folder are writable only if the HCC2 data point assigned to the Modbus register is marked as an Input and writes to inputs are allowed in the address space.
- If the Modbus PDEF was used to construct the HCC2 data points, the Node name will include the remote server name, register type, data direction, and register name.
- The data quality of the register value Nodes indicates the success of the Modbus read queries. For each query, a status of good, stale, or communications lost may be indicated. Exception codes or timeouts of transactions lead to these states as the HCC2 Modbus client attempts to get the remote server data.



Section 11: Setting Up and Configuring an OPC UA Client

The QRATE HCC2 controller's core applications include an OPC UA Client application for connecting to remote servers to exchange process data, alarms, and events.

This guide will step you through the process of configuring your HCC2 as an OPC UA client to include

- Enabling and deploying the OPC UA Client Protocol to the HCC2.
- Setting up a remote server to retrieve its address space.
- Creating a protocol definition (PDEF) file that defines your subscriptions to all remote server targets.
- Mounting and deploying the PDEF.

The HCC2's Client protocol uses the Discovery method to simplify the process of locating a remote server. However, with basic information about the server you are connecting to, you can locate and connect to servers that are not discoverable.

11.1 CONFIGURING YOUR HCC2 AS AN OPC UA CLIENT

To set up the HCC2 as an OPC UA Client, you will configure settings in both Deploy and Operate menu screens. Selections on the Deploy page are made to a static configuration, whereas selections on the Operate page involve interaction with physical network devices.

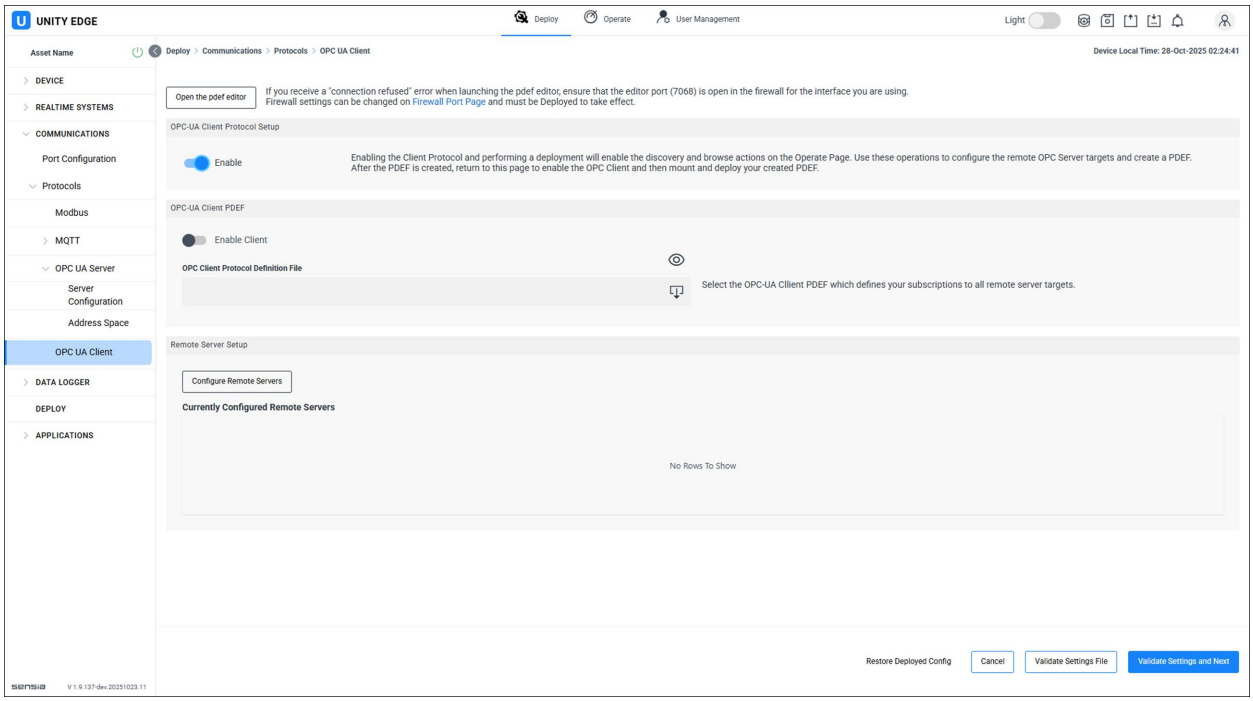
This section describes three different types of server configuration, and explains how to navigate errors to successfully connect to a remote server.

11.1.1 Pre-Configuration Setup (Deploy)

Before you attempt to set up a remote server, you must configure a few settings in the Deploy menu.

1. With Deploy selected at the top of the interface, select Communications>Protocols>OPC UA Client in the navigation tree.
2. In the pane labeled OPCUA Client Protocol Setup, move the Enable slider button to the right to enable the client protocol.

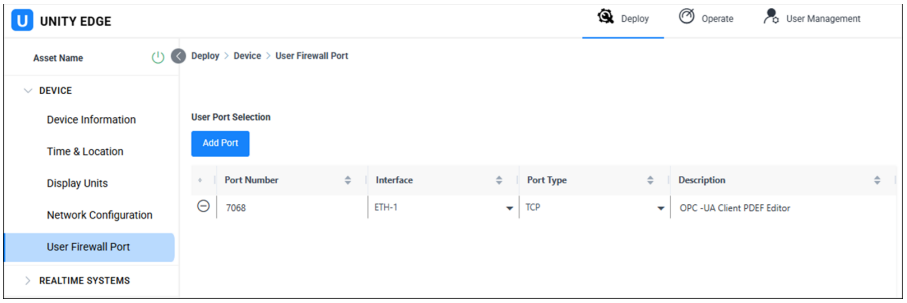
   This setting allows servers to be discoverable and allows browsing of actions on the Operate page. You will use these operations to configure the remote OPC server targets and create a protocol definition file (PDEF). You will then return to this page to enable the OPC Client, and mount and deploy your PDEF.



Note — You can disregard the Enable Client button located below the Enable slider button you just activated. This button will be used later when you mount and deploy an OPC Client PDEF file.

3. Open the Deploy>User Firewall Port menu screen and add all required OPC Client/Server ports using the Add Port button and the configurable table selections.

   a. Add the OPC Client PDEF Editor (port 7068), specify your connection interface and port type, and enter a description as shown.



   b. If you are using the local HCC2 OPC UA server, add the OPC server port (62541) and OPC Discovery server port (4840) to your User Port list. Specifying your connection interface and port type and enter a description for each.

4. Click Deploy in the navigation tree and use the Deploy wizard to deploy the configuration to the HCC2. Acknowledge any prompts alerting you to changes found and the successful validation of the configuration by clicking OK in the dialog boxes.

5. You are now ready to configure a connection to a remote server using the Operate menu (as described in sections 11.1.3, 11.1.4, and 11.1.5).

11.1.2 Browsing Remote Servers to Collect Address Spaces

To activate the client for an application, an OPC Client PDEF must be created, loaded, and deployed. The PDEF will contain all of the read and write mappings established for each remote server target. However, in order to create these mappings in the PDEF editor, we must first retrieve the address spaces containing the NodeIDs for

all of the remote servers. This information is collected using the Operate>Protocols>OPC UA…>Browse Target Servers screen. This page allows you to define each of the remote servers and download their address spaces. When the PDEF editor is then launched, the data collected will be available for selecting the read and write mappings of remote server NodeIDs to HCC2 data points.

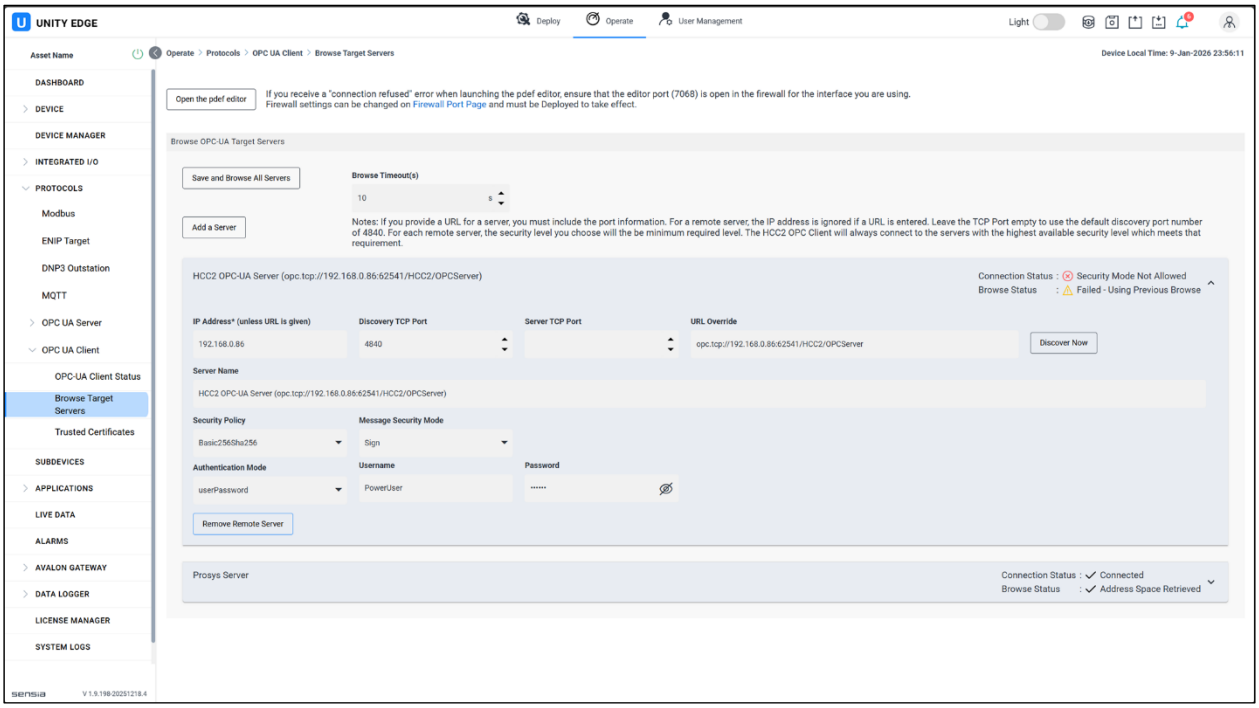
Important The server configuration performed on the Operate>Protocols>OPC UA…>Browse Target Servers screen is only required for the collection of remote server address spaces used in the construction of an OPC Client PDEF.

Connections and data flow at runtime is performed only with remote servers configured within the deployed OPC Client PDEF.

11.1.3 Understanding Connection Status

When you attempt a connection to a remote server, there are a number of potential barriers to overcome. When a connection attempt fails, the HCC2 Operate screen displays a connection status to indicate the type of error involved, which aids in troubleshooting.

Connection statuses are displayed on the Target Servers screen (to be discussed in more detail in the next section), providing immediate feedback to guide your steps in resolving connection barriers.



Connection statuses include:

- Not connected – No connection attempt has been made.
- Server not found – Data provided is incorrect or address is not accessible.
- Security mode not allowed - The security mode you are attempting to connect to is not supported by the remote server. This security mode designates how data is protected while it is in transport.
- Authentication mode is not allowed - The authentication mode you are attempting to use is not supported by the remote server. A supported mode is necessary to validate the device requesting a connection with a remote server. Certificates cannot be exchanged until the authentication mode is accepted.
- Certificate rejected by remote server. The user must take the necessary actions to enable the remote server to accept the HCC2 certificate. These actions will vary among servers.

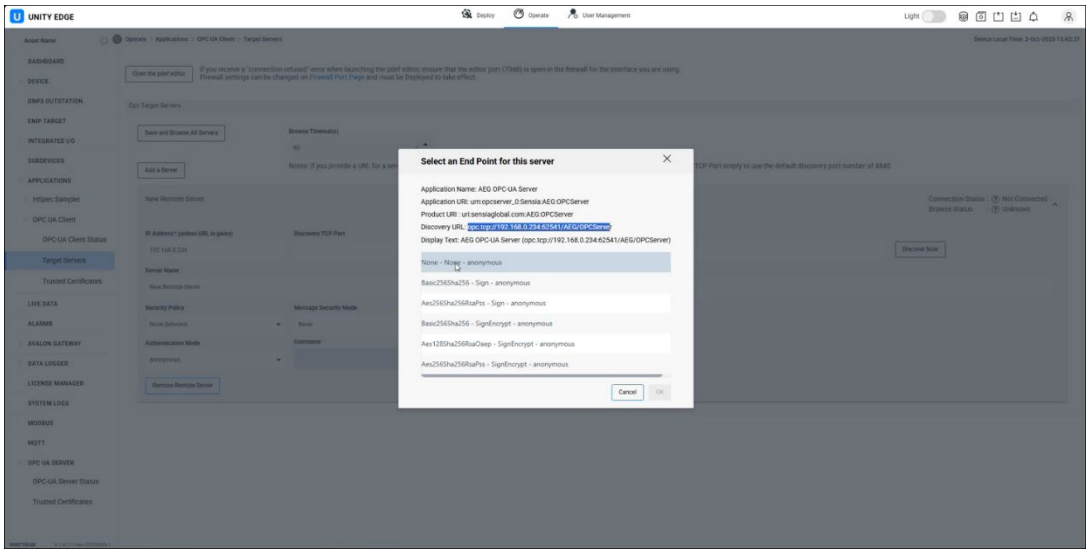
- Certificate rejected by OPC UA client. The user must navigate to the Operate>Protocols>OPC UA…>Trusted Certificate screen and perform the action to trust the rejected certificate.
- User authentication rejected – The authentication mode selected is supported by the remote server, but the remote server has rejected the user name and password provided.
- Connected - When all of the above barriers are eliminated, a Connected status is displayed and the client can connect with the remote server and browse the address space in the remote device.

11.1.4 Adding a Server using the Discovery Method

Use the following Operate procedure to add a remote server that is discoverable. This discoverability significantly reduces the amount of information you must supply to establish a connection. In this example, the server is on an internal network.

From the Operate menu, select the Protocols>OPC UA Client > Target Servers screen and follow these steps.

1. Click the gray panel labeled New Remote Server to expand the view and provide access to selectable configuration settings. (Conversely, clicking the gray panel again contracts the view to display only the server name and status.)
2. Enter the server's IP address in the field provided.
3. Click the Discover Now button.
4. A dialog box will display various details identifying the server, including its URL, and prompt you to select a security policy/authentication mode from a list provided.



5. Select a security policy/authentication mode and click OK. In this example, the most basic security level (None – None) is chosen.
6. The next steps will vary, depending on your mode selection. When None – None is selected, all supported configuration fields are automatically populated in the screen. If a "signed" mode is selected, more information is required to support an exchange of certificates for authenticating the devices attempting a connection.
7. Note that the Discovery TCP Port is populated as 4840 and the Server TCP Port is empty. Leaving these fields empty causes the default settings to be applied—the default standard port for OPC discovery service is 4840 and the server port is 62541.

Important If the device is behind a firewall, the default port values may not be adequate. For advanced networking, you must provide the external facing discovery and server ports, which are internally forwarded to the server on the internal network behind the firewall.

8. Note that the Connection status and Browse status are populated along the right side of the target server pane.
9. Click Save and Browse All Servers and watch for any changes in the statuses displayed.
    - If the browse action reaches the server, the Connection Status will update to “Connected” and the Browser Status will display “Address Space Retrieved.”
    - If a “signed” authentication mode was selected, a Certificate Rejected connection status will be posted, alerting you to the need to trust the incoming client request. Authorize the connection by accepting the trust prompt.

Important Initially, exchanged certificates will be rejected by both the server and the client. Within Unity Edge, you must manually trust certificates presented on the Operate > OPC UA Client > Trusted Certificates and Operate > OPC UA Server > Trusted Certificates pages. See Manage Trusted Certificates, page 137, for details. The interface for trusting certificates varies by product but all servers that support signed security will provide a tool for authenticating devices via certificate exchange.

Adding and Removing Servers

To add another server, click the Add a Server button provided on the Operate>Target Servers screen.

To delete a server, click the server panel to expand the view and click on the Remove Remote Server button.

11.1.5 Adding a Server that is Not Discoverable

Firewall restrictions may prevent a server from being discoverable. Also, some OPC UA servers may not have a discovery service. However, with knowledge of server configuration details, you may still achieve a connection with your OPC-UA Client.

Before you attempt a connection to the server, identify the following details for your server’s configuration:

- URL address of the server
- Security modes and encryption methods supported by the server
- User authentication methods supported by the server. If username/password authentication is enabled, you will need to know those specific credentials to connect to the server.

To configure this connection

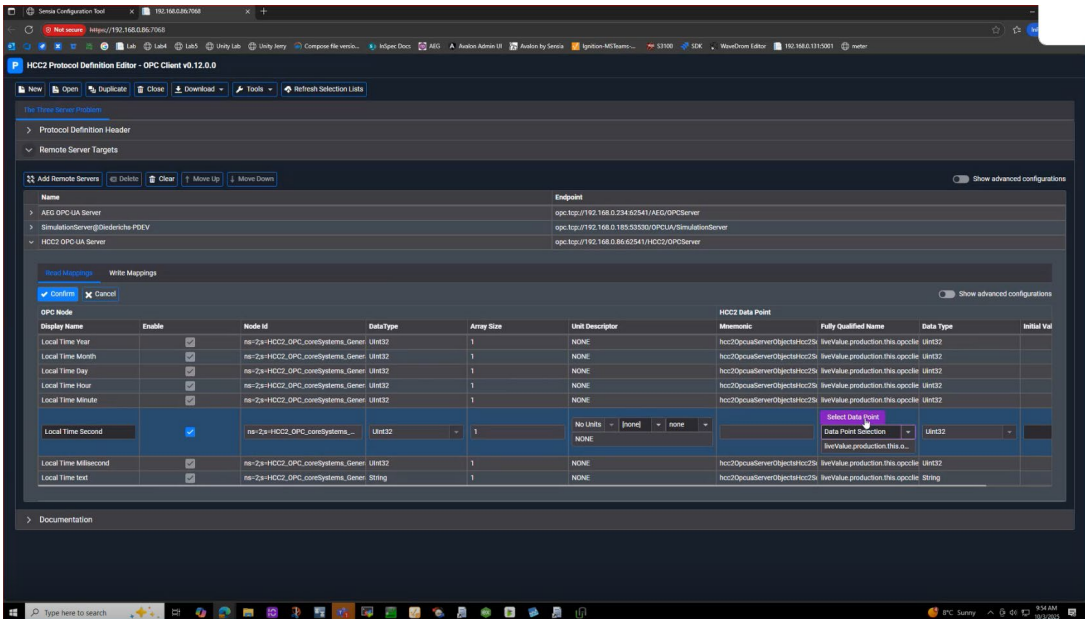
1. Select the OPC UA Client > Target Servers screen.
2. Enter the server URL in the URL Override field. (DO NOT click Discover Now. This button has no function for devices that are not discoverable.)
3. Click Save and Browse All Servers. If any of the above server credentials are not met, failure indicators will appear in the Connection Status and/or Browser Status displays, along with an error description to guide you in troubleshooting. For example, “User authentication rejected” indicates that the user authentication was entered incorrectly.
4. Attempt to resolve errors, clicking Save and Browse All Servers after each change until the Connection status is “Connected” and the Browser status is “Address Space Retrieved.”

11.1.6 Map HCC2 Tags with the OPC Client PDEF Editor

1. From the Deploy menu, open the OPC Client PDEF Editor using the button provided.
2. Enter a name for a new protocol and assign a protocol map version number.
3. Open the Remote Server Targets pane to view connected remote servers. If you wish to view more details, enable the Show advanced configurations slider at the right side of the screen.

4. Click the chevron to the left of the server name to access tools for mapping tags for reading and writing data.
5. Configure Read mappings – that is, nodes you wish to read and publish to tags in the HCC2.
   a. Select the Read Mappings tab.
   b. Click Select Nodes to view a node selection list in the address space.
   c. Click the chevrons to drill into node groups and click the checkboxes of the registers you want to poll. You can multi-select registers using the standard shift-click technique; or select a group by clicking the checkbox associated with a group name.
   d. Click OK to return to the data access view.

      A custom HCC2 data tag is automatically created for each selected register. By default, these tags will be assigned a Fully Qualified Name constructed from information provided in the retrieved address space.
6. To publish a data point to a specific app, follow these steps:
   a. In the Fully Qualified Name column, change the configuration setting from Create Mnemonic Value to Data Point Selection.
   b. Click Select Data Point (as shown below in the violet box).
   c. At the prompt to apply the selection, click Yes. A list of data points grouped by application will appear.
   d. Filter data points if required, select the data point you wish to write to, and click OK. The data point in the Fully Qualified Name column will display the name of your application and the name of your data point.
7. Click the blue Confirm button just below the Read Mappings tab to save your mappings.



8. Configure Write mappings – that is, tags that exist inside the system that you want to write to the server as they are updated. Simply click on the Write Mappings tab and follow the instructions listed in steps 5b through 5d to select the registers you want to write rather than poll.
9. Click the Download button at the top of the PDEF Editor screen to download the PDEF file, and save it.

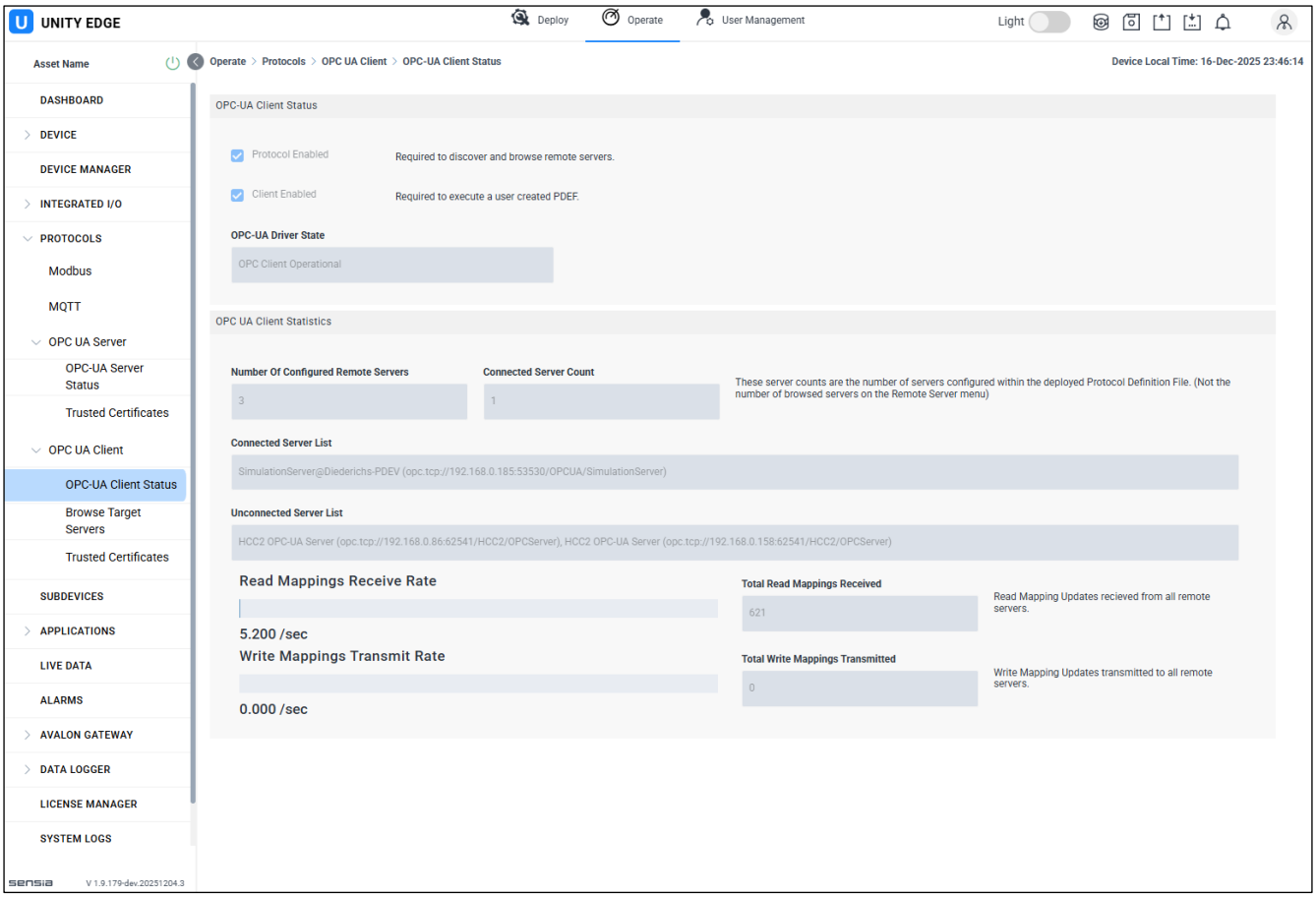
11.1.7 Install the PDEF

1. Return to the Deploy > Protocols > OPC UA Client screen.
2. In the OPC-UA Client PDEF section of the screen, toggle the Enable Client slider to the enabled position.

3. Click the Downloads icon to open the Downloads folder and select the PDEF file.
4. To confirm that the PDEF you selected is the correct one, click the eyeball icon to view a summary of the connected servers and the number of mappings configured for each one.
5. Click Deploy. The Client will connect to the servers and begin pulling in the data.
6. Click Live Data.
7. In the search field, type “opcclientpdef” to filter on the data points from the configured servers.
8. If you configured tags to publish data to an application data point, you can also view data inputs on the application page of Unity Edge.

11.1.8 OPC UA Client Status

To confirm the status of an OPC Client configuration, navigate to the Operate menu and select OPC-UA Client from the navigation tree.



Status is defined by three settings:

- Protocol Enabled: When this checkbox is checked, the OPC Client has been deployed with the protocol enabled and remote server targets can be discovered and browsed.
- Client Deployed: When this checkbox is checked, a successful PDEF has been loaded and deployed.
- Driver State: Provides a message indicating the state of the software driver application.
  - OPC Client Operational: The OPC Client has been successfully configured and deployed with a PDEF file.
  - Awaiting Provisional Data: The OPC Client has not yet been deployed. Configure the OPC Client and perform a deploy action.

In addition, you can reference a variety of statistics to assess the configuration and health of client-server connections.

- Number of Configured Remote Servers: The number of remote server targets defined in the deployed PDEF.
- Connected Server Count: The number of remote server targets defined in the deployed PDEF that are currently in a connected state.
- Connected Server List: A comma separated list of remote server targets defined in the deployed PDEF that are currently in a connected state.
- Unconnected Server List: A comma separated list of remote server targets defined in the deployed PDEF that are currently in an unconnected state.
- Read Mappings Receive Rate: A computed rate at which value updates are received from all of the remote servers (updates per second).
- Write Mappings Transmit Rate: A computed rate at which value updates are transmitted to all of the remote servers (updates per second).
- Total Read Mappings Received: The total number of values received from remote servers since application start-up.
- Total Write Mappings Transmitted: The total number of values transmitted to remote servers since application start-up.

Section 12: Using EtherNet/IP Driver for Data Exchange

An EtherNet Industrial Protocol (EtherNet/IP or ENIP) target driver enables the sharing of HCC2 data points with Rockwell Automation controllers over Ethernet networks. In short, the driver allows for the efficient transfer of HCC2 data points in and out of the Rockwell Automation ecosystem, and can be used as a protocol bridge to any other HCC2 driver.

This section describes the features of the ENIP target driver, and provides instructions for installing the driver, building a protocol definition file to facilitate the transfer of input and output data point assemblies, and configuring a ControlLogix controller to receive and decode the HCC2 data.

The ENIP target driver supports Class 1 and Class 3 CIP connections and constructs a custom user data type (UDT) for use with either of two Rockwell Automation controller families:

- ControlLogix 5570 Controller (1756-L7X)
- ControlLogix 5580 Controller (1756-L8X)

12.1 INSTALLING THE ENIP TARGET DRIVER

The ENIP target protocol driver is distributed as a custom application, packaged separately from the HCC2 core application bundles and easily installed using the Edge Package Manager.

1. Download the driver as follows.
   a. Visit URL https://www.sensiaglobal.com/Technical-Support.
   b. Click Customer Support Portal Access in the top right corner of the screen and search for RTU and Edge Devices Firmware and Software Download Procedure. Or use this link to navigate to the procedure: Knowledge Article KA-04676.
   c. Follow the procedure to connect to the Microsoft Azure Storage Explorer repository and download the target driver.
2. Install the application using the Edge Package Manager. See section 4.3 Updating HCC2 Applications with EPM, page 43, for details.
3. Log in to Unity Edge and navigate to file path Deploy > Communications > Protocols > ENIP Target to verify the installation.

The HCC2 ENIP target is configured with a Protocol Definition File (PDEF) created with Unity Edge and an integrated PDEF Editor tool enabled by the installation of the ENIP target container.

12.2 CONFIGURING THE ENIP TARGET

The ENIP target driver becomes active when a PDEF file is mounted in Unity Edge and the HCC2 is deployed with that configuration. Only one instance of the ENIP Target is active on the HCC2.

To configure the ENIP target, you must first open a couple of ports in the HCC2 firewall; then, you create a protocol definition (PDEF) file using the PDEF Editor application and mount it in Unity Edge.

Note	Required firewall ports are identified in on-screen messaging in the ENIP Target screen as well as in the procedure below.

12.2.1 Open Firewall Ports

Open the required firewall ports in the Device > User Firewall Port screen.

1. Open TCP port 7067 on the network interface you are using. This port is required to access the PDEF editor
2. Open TCP port 44818 on the network interface you are using. This port is the standard ENIP target port.
3. Update the deployment file.
4. Click Deploy in the navigation tree to deploy your changes to the HCC2. The newly created firewall port rules will not be active until the deployment is completed.

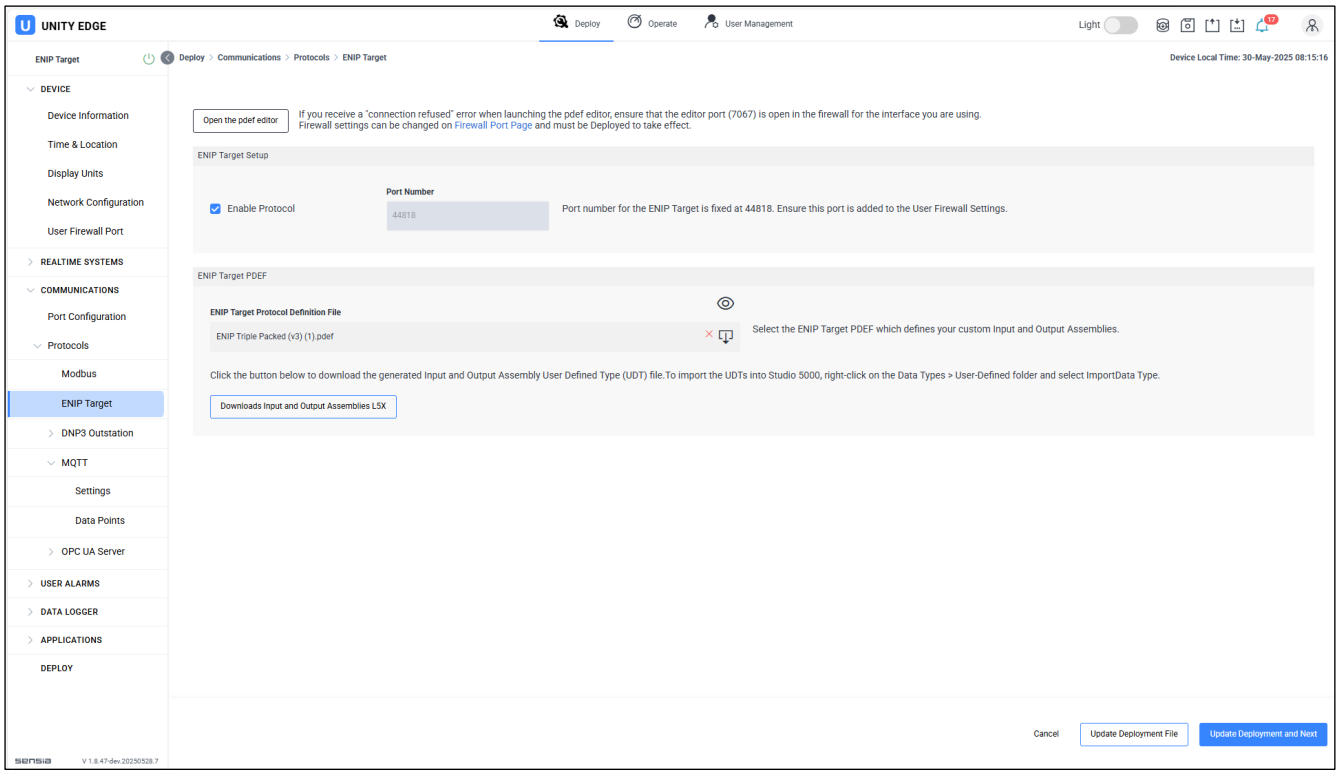
You are now ready to create a PDEF file to configure the HCC2 as an ENIP target device.

12.2.2 Create a PDEF File

The ENIP Target PDEF file contains two data point assemblies for use with Rockwell Automation (RA) controllers.

- An input assembly contains all of the data points to be sent to the RA controller.
- An output assembly contains the data points to be sent by the RA controller and received by the HCC2.

With the required firewall ports open, return to the ENIP Target screen (Deploy > Communications > Protocols > ENIP Target) and click the Open the pdef editor button. The HCC2 Protocol Definition Editor will open in a new browser window, and the Protocol Definition Header tab will open by default.



Configure a Protocol Definition Header

Under the Protocol Definition Header tab, make the following entries as needed. This information will be available to Unity Edge users and presented within the generated documentation.

Parameter	Description
User Protocol Name	Assign a unique, descriptive name to the map.
Protocol Map Version	Defaults to zero. Enter a numeric sequence identifier. Increment this version number with each PDEF release you make.
User Description	Optional. Enter a helpful description that indicates the purpose of the map.
Author	Optional. Enter the name of the organization or person who creates the map.
Owner	Optional. Enter the name of the organization or person who is responsible for the map.
Creation Date	Defaults to the local time
Modified Date	Defaults to the local time
Release Notes	Optional. Add any explanatory text.

Define Your Target

The ENIP target driver can automatically build a User Defined Data type (in .L5X form) for two Rockwell Automation controller families:

- ControlLogix 5570 Controller (1756-L7X)
- ControlLogix 5580 Controller (1756-L8X)

To define your target for the PDEF file

1. Select the Target Definition tab in the PDEF Editor.
2. Select the controller family from the dropdown menu under Target Definition.
3. Enter a prefix to uniquely define all HCC2 fully qualified data point names you create in your PDEF. This prefix should reflect the name or function of the controller you are connecting to. It is used to construct the fully qualified HCC2 data point name when using the Construct Data Point from Mnemonic option to create input and output assemblies.

Note

Controller families differ in the data types they support. The ControlLogix 5570 family does not support UINTs (of any size) or 64-bit floats. When you replace a 558x controller with a 557x controller, the system automatically replaces unsupported data types with a best case substitute data type that is supported by the 557x device.

Controller families also differ in the number of bytes consumed by data points because the families pack data differently within the transmitted assembly data blocks.

Switching from one controller family to another does not change the data types used in the HCC2.

Create an Input Assembly

All data types are available for selection in building the input assembly.

To create an input assembly

1. Select the Assembly Definition tab in the PDEF Editor.
2. Click Add HCC2 Data Points to view a list of all available data points.

3. Select the data points you want to share with the controller by individually selecting a data point or using standard Windows multi-select tools (Shift+Click, Control+Click) to select groups of data points.
4. Click OK to add the selections to your assembly.
5. Monitor the number of bytes used as you build your assembly. Input and output assemblies are limited to 416 bytes of data, and an onscreen counter in the top right corner of the Input Assembly grid displays a running total of bytes used.

Note	The Bytes count displayed does not correlate directly to the sum of individual data type sizes because the byte packing process causes a small variance. Byte packing differences among controller families can also significantly impact byte size. The number of bytes required to pack your selected data points can be greatly reduced by grouping 8 bit, 16 bit, 32 bit, and 64 bit data types together in sequence. Alternating between 8 bit and 64 bit data types creates the least optimal packing result.

Observe the arrangement of the Input Assembly grid with content divided into two parts:

- ENIP Attribute (data presented to the target device) in the first three columns of the grid
- HCC2 Data Point (data displayed in the HCC2) beginning in the fourth column of the grid

Note that “Data Type” is used to describe both the data type classes for the controller (in the ENIP Attribute Data Type column) and the data types natively supported by the HCC2 (in the HCC2 Data Point Data Type column).

To view all available data, click the Show advanced configurations toggle slider in the top right corner of the Input Assembly grid.

Consider the following options for optimizing the presentation of your input assembly to the RA controller.

- Configure a data point to indicate data quality. By default, the *value* of an HCC2 data point is presented to the controller. You can change this by editing the Property Selection setting of a data point in the advanced configurations view. (A quality output can be useful for verifying the status of a mapped data point that is being read or written from a remote server. Quality data can also indicate if the data point is stale, out of service, not initialized, etc.)

  To configure a data point to present data quality, duplicate your data point, select the duplicated row, and double-click it to enable the edit mode. Change the Property Selection setting from *Value* to *Quality*.

- Change the unit used to present a data point value to the RA controller. As you add measurement data points to your input assembly, they appear in the base units of the HCC2’s measurement category. To present the data in a different unit, edit the unit using either of two methods.
  - Double-click the row of the unit to access a dropdown menu within the grid, and select a new unit.
  - Select the Edit (via Form) tool in the Input Assembly toolbar and choose a preferred data point unit in a popup form.

  The data in the assembly will be presented to the controller in the units you specified. Internally to the HCC2, the data point values will continue to be published in base units, and in Unity Edge, users will see their user-selected units for data point values.

- Edit an array in the assembly before sending data to the controller. If you add an array to your assembly, all elements are automatically added (as seen in the Array Index column in the advanced configurations view). Delete elements you do not want, or reorder/rename them, if desired.

Create an Output Assembly

An output assembly contains the data points to be sent from the controller to the HCC2.

Important	You can only select data points that have been registered by an application as an input. However you can create a new custom data point to bring into the HCC2 controller data that is not yet selectable using the PDEF Editor.

To create an output assembly

1. Select the Output Assembly tab in the Assembly Definition screen.
2. Click Add HCC2 Data Points, select desired data points using standard Windows multi-select tools (Shift+Click, Control+Click).
3. Click OK to add the selections to your assembly.

To bring new data from the controller into the HCC2 (using data points that are not available for selection in step 2 above)

1. Click Add New.
2. Complete the required data entries.
   - Add New allows you to enter the data type presented to the controller, unit descriptor, HCC2 data point mnemonic, data type for HCC2, etc.
   - Making these selections will construct the metadata for a new HCC2 data point that will be added to the system when the PDEF is mounted within Unity Edge.
3. Click OK to add the data point to your assembly.

If desired, enter an initial value for your assembly data points. For example, you could enter a “-1” initial value to make data points that have not been received easy to recognize. (All data points will have a quality of “not yet initialized” until the HCC2 receives its first value from the controller, but a unique initial value may be more visible.) To apply an initial value to multiple data points, select the data points (grid rows), choose the Multi-Edit tool to enable edits, enter “-1” in the Initial Value field, and click Confirm.

Important	Initial values entered with the PDEF are only used by the ENIP driver if the HCC2 data point has not been published within the system. If the selected data point has been previously published when the driver starts or has been deployed, the existing published value is used, and the Initial Value is ignored.

Viewing ENIP Documentation

When the input and output assemblies are complete, you can view a summary of your configuration details in a printable report.

To view the report from within the PDEF Editor, click the Documentation expander. From there, you can print it or export it to a variety of formats to share with others. See Documentation for ENIP Decoding, page 159.

When the PDEF file is mounted in Unity Edge, you can also inspect the assembly data report from the ENIP Target screen using the eye icon.

12.2.3 Mount the PDEF File in Unity Edge

To mount the PDEF file in Unity Edge

1. From the PDEF Editor, open the Download dropdown menu and select the .PDEF Protocol Definition format to download the PDEF file to your PC.
2. Return to the Unity Edge ENIP Target screen and select the .PDEF file.
3. Update the deployment file in Unity Edge.
4. Deploy the update to the HCC2 by selecting Deploy in the navigation tree.

12.2.4 Integrate HCC2 Data into a Control Application

Documentation for ENIP Decoding

From the PDEF Editor, click the Documentation tab to view the input and output assembly data and other ENIP target details in a printable report.

This report is ideal for users who have a generic ENIP scanner and must process the HCC2 data point bytes manually. The report provides all of the required assembly data, including data point names, data types, units of measure, and byte index for decoding.

You can print the report or export it to a wide range of formats including CSV, XLS, or pdf for handoff to a system integrator.

UDT Download for Studio 5000 Logix Designer

Assembly data is also auto-generated in a custom user data type (UDT) that can be imported directly into Studio 5000 Logix Designer.

To download the file to your PC, return to the Unity Edge ENIP Target screen and click the button labeled Downloads Input and Output Assemblies.L5x. The download file is named (hcc2_userDataTypes.L5x).

See section 12.3.2 Import and Decode UDT Files, page 160, for instructions on importing these files into the Studio 5000 Logix Designer.

12.3 CONFIGURING AN RA CONTROLLER CLASS 1 CONNECTION

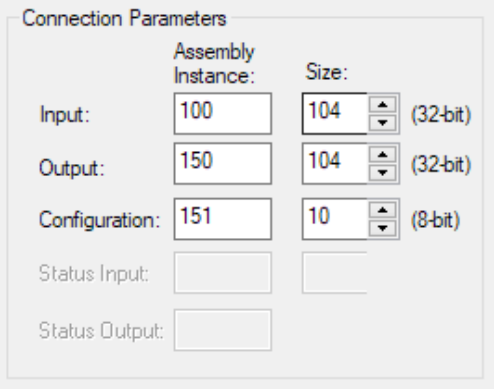
This section describes the steps to configure a Class 1 HCC2 connection to a ControlLogix controller using Studio 5000 Logix Designer and the UDT assembly data downloaded from the HCC2.

In a Class 1 (implicit I/O) connection, messages are sent repeatedly at a requested packet interval.

The HCC2 is configured as a generic Ethernet module.

12.3.1 Configure the HCC2 as a Generic Ethernet Module

1. In Logix Designer, create a new generic Ethernet module.
2. Assign an IP address to the module. This is the IP address of the HCC2 CPU board Ethernet port that is connected to the Logix controller.
3. Enter the following connection parameters for your ENIP target driver:



4. Click OK to save your settings.
5. Update the following settings on your Module Properties Report.

a. On the Connection tab, enter your desired Requested Packet Interval (RPI). The HCC2 ENIP target driver supports packet intervals down to 10 ms.

b. Make sure the Use Unicast Connection over EtherNet/IP checkbox is checked.

c. Click OK to save your settings.

d. On the Module Info tab, the vendor ID field should display as Sensia, and the Product Name should reflect the HCC2 ENIP Target.

12.3.2 Import and Decode UDT Files

Import your UDT files into Studio 5000 Logix Designer as follows. If you have not downloaded your ENIP assemblies file (hcc2_userDataTypes.L5x) from Unity Edge, see UDT Download for Studio 5000, page 159, before continuing.

1. In Logix Designer, navigate to Assets > DataTypes, right-click the User-Defined folder, and select Import Data Type.
2. In the resulting dialog box, map to and select the downloaded .L5X file, and click OK to import the UDTs into Logix Designer.
3. Verify that two UDT files have been added to the Assets > DataTypes > User Defined filepath:
   - HCC2_InputAssembly
   - HCC2_OutputAssembly

   The contents of the UDT files should match the ENIP Attribute content of your PDEF file.
4. Under Controller Tags, create a new tag for each UDT assembly (HCC2_InputAssem and HCC2_OutputAssem, for example). Be sure to update the Data Type field to reflect the UDT file names before saving each respective tag.
5. Set up a routine that copies data from the Input Assembly DINT array into the HCC2_InputAssem UDT.
6. Set up a routine that copies data from HCC2_OutputAssem UDT into the Output Assembly DINT array.

Note	You can view the ENIP target driver status, connections, originator information, and packet rate statistics in the Unity Edge Operate > ENIP Target screen.

12.4 SUPPORT FOR A CLASS 3 CONNECTION

For applications that require explicit messaging, the ENIP target driver also supports Class 3 reads and writes of the user-defined Input and Output assembly data blocks.

To create a Class 3 connection

1. Create the PDEF file to define the Input and Output Assemblies as described above for a Class 1 connection.
2. Download the PDEF file.
3. Mount the PDEF file within Unity Edge.
4. Deploy the HCC2.

The Input Assembly data block can be read with the explicit message command `Get Attribute Single` using the following parameters: Class 4, Instance 100, Attribute 3. The response will contain the 416 bytes of the Input Assembly to be sent to the HCC2.

The Output Assembly data block can be written with the explicit message command `Set Attribute Single` using the following parameters: Class 4, Instance 150, Attribute 3. The message should contain the 416 bytes of the Output Assembly to be sent to the HCC2.

Section 13: Configuring a DNP3 Outstation Driver

Sensia's distributed network protocol 3 (DNP3) driver equips the HCC2 to efficiently manage processes at the edge and is well suited for applications in which communication bandwidth is limited or costly.

Sensia's implementation of the DNP3 protocol transmits data from point A to point B using TCP communications. The term *outstation* denotes remote devices in the field, and the term *master* is used for the computers in control centers.

When the DNP3 driver is installed, the HCC2 acts as an outstation at the edge, collecting and reporting data to a master station. Using DNP3 protocol, you can train the outstation as to what constitutes an important change and then create an event to record these changes. These events can later be polled or reported by exception with a message to the master station.

HCC2 allows you to configure two outstations as either redundant or exclusive outstations.

13.1 DRIVER SPECIFICATIONS

The DNP3 outstation driver supports the following:

- Compliance to DNP release Level 3, as well as Levels 4 and 4+
- Support for Class 0, 1, 2, and 3 data
- Timestamp and flags on all data points
- TCP Outstation only (no serial support)
- Secure Authentication Level 2 (SAv2) and Level 5 (SAv5)
- Secure Authentication Aggressive Mode
- Outstation unsolicited response (report by exception)
- Data buffering with deep memory (50,000 events)
- Non-volatile storage of un-transmitted events in communication loss conditions
- Configurable time synchronization integrated with HCC2 time systems
- Set-Before-Operate operations

13.2 INSTALLING THE DNP3 DRIVER

The DNP3 protocol driver is packaged separately from the Sensia's HCC2 core application bundles and installed using the Edge Package Manager. The installer name is hcc2_dnp3outstation***.mender.

1. Download the driver as follows.
   a. Visit URL https://www.sensiaglobal.com/Technical-Support.
   b. Click Customer Support Portal Access in the top right corner of the screen and search for RTU and Edge Devices Firmware and Software Download Procedure. Or use this link to navigate to the procedure: Knowledge Article KA-04676.
   c. Follow the procedure to connect to the Microsoft Azure Storage Explorer repository and download the target driver.
2. Install the application using the Edge Package Manager.
3. Log in to Unity Edge and navigate to file path Deploy > Communications > Protocols > DNP3 Outstation to verify the installation.

13.3 CONFIGURING YOUR OUTSTATION CONNECTIONS

This section describes part 1 of a two-part configuration process – enabling DNP3 protocol and configuring DNP3 connection and security settings.

Part 2 - the creation of a Protocol Definition File (PDEF) to define your outstation - is described in section 13.4, page 167.

Dividing configuration settings in this way so that all of the configuration information specific to a master is in Unity and not in the PDEF allows the PDEF file to be reused with multiple masters without editing settings for each application. Likewise, security settings are configured in Unity alone, and are considered part of the connection information.

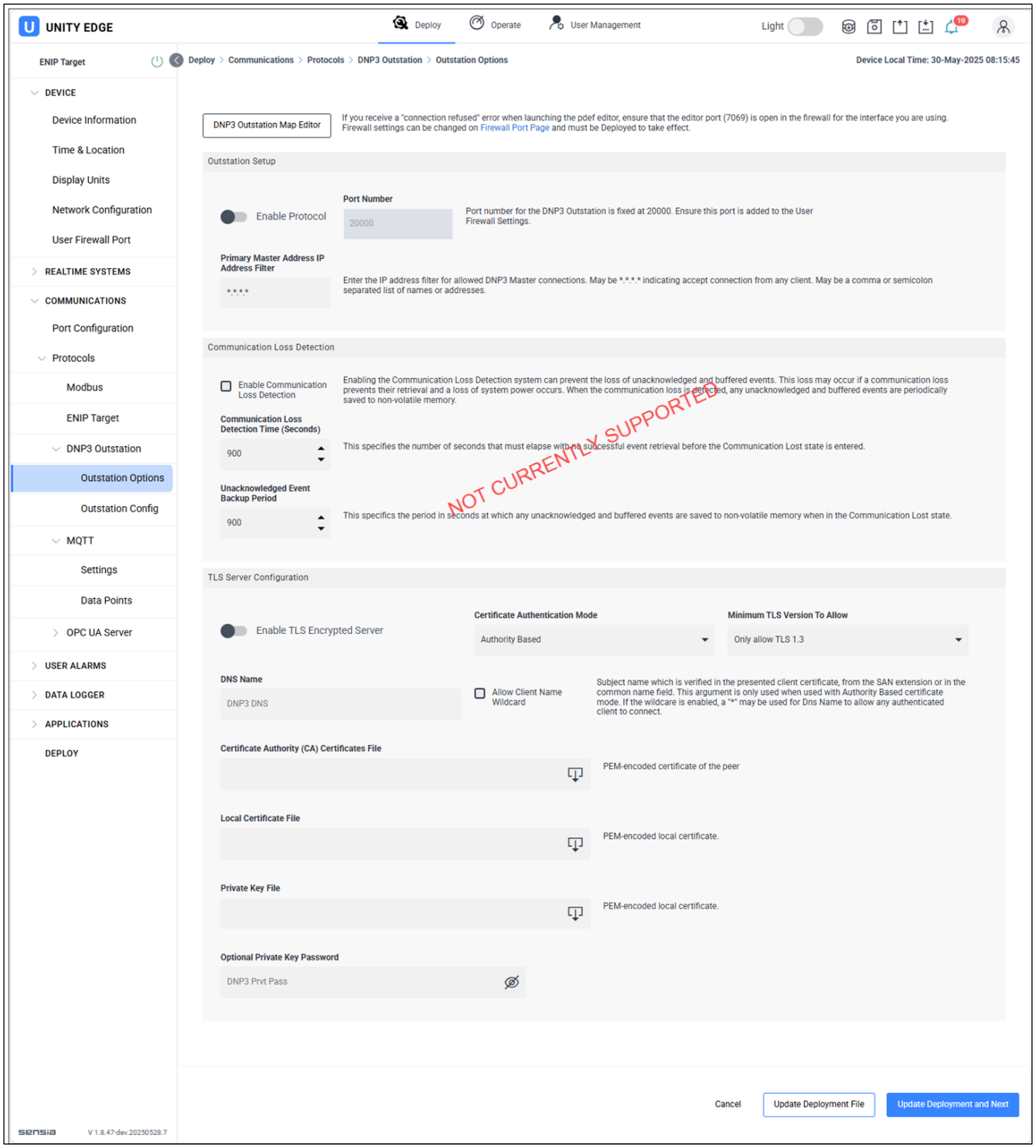
In this section, we will examine the DNP3 settings provided in two DNP3 screens in Unity Edge: Outstation Options and Outstation Config.

13.3.1 Outstation Options

When the driver is installed, you will find the DNP3 configuration screens located at this menu path: Deploy > Communications > Protocols > DNP3 Outstation.

Click the Outstation Options screen and observe a few key buttons and settings:

- Near the top of the screen is the DNP3 Outstation Map Editor button. You will use this to create the outstation PDEF file later in the configuration process.
- The PDEF editor requires TCP port 7069 to be open.
- The Enable Protocol setting is active by default. When set to false, this setting globally disables all Outstation services on the HCC2.
- The Port Number is not editable. For the DNP3 Outstation, this port number is fixed at TCP port 20000.
- From this screen, you can filter to the IP address of any incoming Master station using the Primary Master Address IP Address Filter field.



Open Firewall Ports

Before you configure an outstation, you must open a couple of ports in the HCC2 firewall.

To achieve this

1. Navigate to the Device > User Firewall Port screen.

2. Open TCP port 7069 on the network interface you are using. This port is required to access the PDEF editor.
3. Open TCP port 20000 on the network interface you are using. This port is the standard DNP3 Outstation port.
4. Update the deployment file.
5. Click Deploy in the navigation tree to deploy your changes to the HCC2. The newly added ports will not be open until deployment is completed.

Update Time Setting (Optional)

To allow the DNP3 Master to set the time on the HCC2

1. Navigate to the Device > Time & Location screen.
2. Change the Time Source to Manual. The default setting is Auto.
3. Update the deployment file.
4. Click Deploy in the navigation tree to deploy your changes to the HCC2.
5. Return to the Deploy > Communications > Protocols > DNP3 Outstation > Outstation Options screen.

Communication and Power Loss

The Communication Loss Detection feature displayed in the DNP3 Outstation>Outstation Options screen is not currently supported. However, if communication is lost, the HCC2 DNP3 Outstation Driver will continue to record up to 10,000 events of each object type. When communication is later restored, all accumulated events will be transmitted.

If power is interrupted to the HCC2, any untransmitted events will be lost. To minimize this risk, consider adjusting your Unsolicited Events settings (described in section 13.4.2). Set the Event Count Trigger Level and the Transmit Holdoff Time to low values to ensure that all collected events are transmitted responsibly. For example, setting the trigger level to 1 and the holdoff time to 5 minutes will help ensure that no more than 5 minutes of events are lost from a power interruption.

Enable TLS Server Configuration

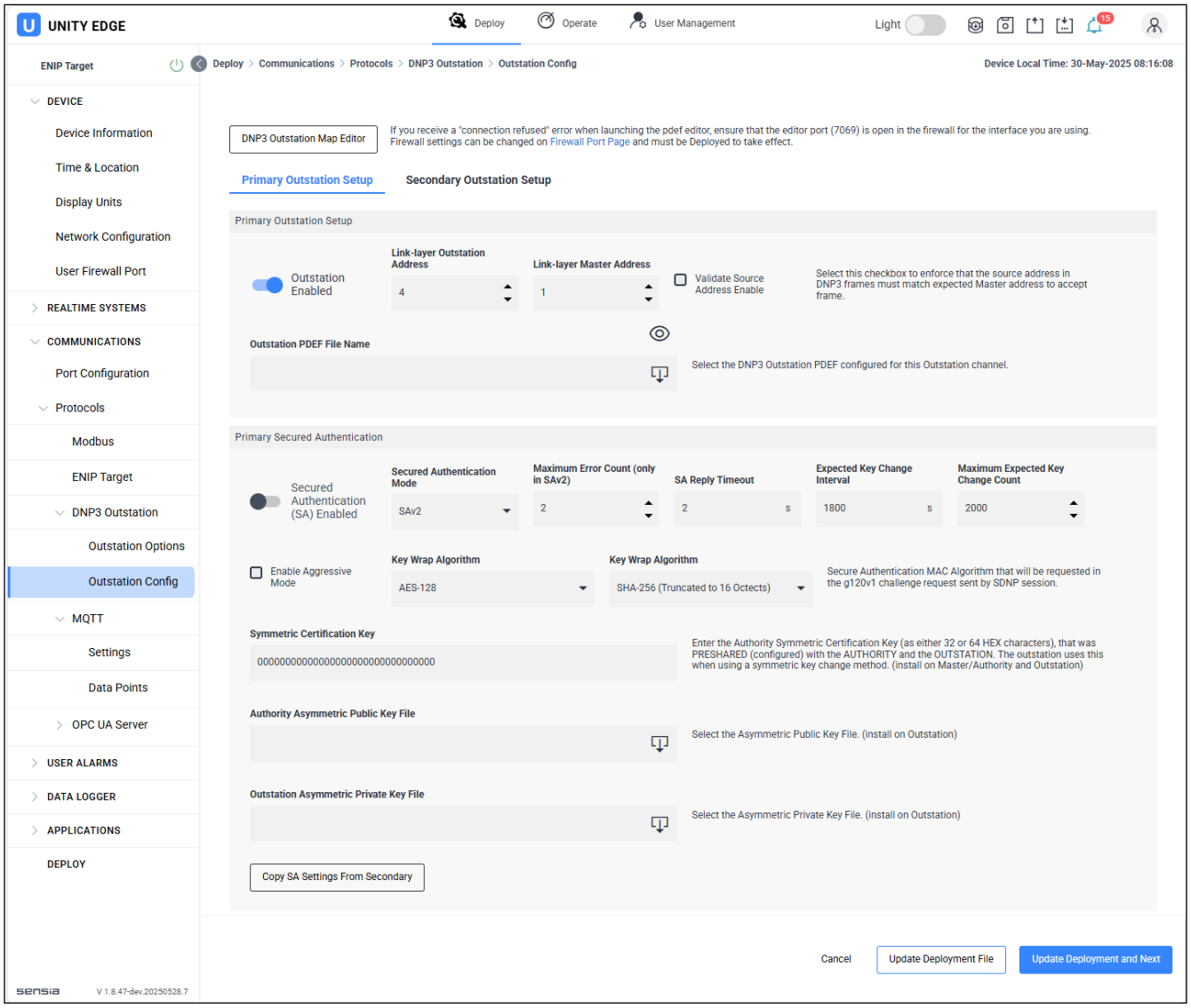
TLS server encryption allows encryption of all DNP traffic at a network level, which is superior to the Secured Authentication security configured in the Outstation Config screen.

Note	The TLS Server encryption feature is not fully supported in the initial releases of the HCC2 DNP3 Outstation Driver.

13.3.2 Outstation Configuration

Click on the Outstation Config screen in the navigation tree to view settings for primary and secondary outstation setup. The Outstation configuration within Unity Edge is focused on enabling and connection information. By having all of the connection information for a specific DNP3 master within Unity Edge (and not in the PDEF), then the DNP3 Outstation PDEF can be reused with different masters without being edited.

Likewise, security options in the bottom half of the screen provide the structure for configuring Secured Authentication. The security is configured in Unity Edge alone and is considered a part of connection information. The PDEF files will not contain any security settings or authentication certificates. The outstation map is defined in a separate PDEF file (described in section 13.4, page 167), but you will use the Outstation Config screen to select your PDEF file when it is complete and ready to mount in the HCC2.



Outstation Setup

Configure the following settings on the Primary Outstation Setup and Secondary Outstation Setup tabs:

- **Outstation Enabled:** Primary and Secondary Outstations can be individually enabled. If an outstation is enabled, the configuration page will not validate unless a valid PDEF file is loaded.
- **Link-Layer Outstation Address:** The DNP3 address that must be in requests from the master station. Values of 1 through 65,519 are configurable. Data link addresses 65520 (0xFFF0) through 65535 (0xFFFF) are reserved for broadcast or other special purposes.
- **Link-Layer Master Address:** The DNP3 address of the expected master station.
- **Validate Source Address Enable:** If enabled, the Outstation will filter out any requests from addresses other than the specified master address. Select this checkbox to require the source address in DNP3 frames to match the expected master address as a condition for accepting the frame.
- **Outstation PDEF File Name:** Click the download button within the field to select the DNP3 Outstation PDEF file configured for the Outstation channel. Once the PDEF file is loaded, the eye icon will present the documentation for the loaded file.

Enabling Secure Authentication

DNP3 Secure Authentication enhances the security of DNP3 communications by allowing master stations and remote terminal units (RTUs) to mutually verify each other's identity and ensure data integrity.

The DNP3 standard supports many forms of encryption, and the settings required for an outstation can vary among master stations.

To enable DNP3 Secure Authentication

1. Navigate to the Unity Edge Outstation Config screen.
2. Click on Secured Authentication (SA) Enabled in the bottom half of the screen.
3. Update the following settings if applicable. The default settings shown are acceptable for most applications.
   - Maximum Error Count (default: 2)
   - SA Reply Timeout (default: 2)
   - Expected Key Change Interval (default: 1800)
   - Maximum Expected Key Change Count (default: 2000)
4. Choose a Secured Authentication Mode – Version 2 (SAv2) or Version 5 (SAv5).
   - If you choose Version 2, you must choose an SAv2 Key Wrap Algorithm. The algorithms use a User Update Key also displayed on the screen. A symmetric *AES-128* algorithm requires a 32 hex character update key. A symmetric *AES-256* algorithm requires a 64-hex character update key.
   - If you choose Version 5, you must choose an SAv5 Key Wrap Algorithm. As with Version 2 algorithms, *symmetric* algorithms use the User Update Key. The standard also supports *asymmetric* encryption, which requires the upload of Private Encryption Management Systems (PEMs) files for a public and private key. In DNP3 secure authentication with asymmetric encryption, the PEMs on the master must match the PEMs on the outstation.
5. Check the Enable aggressive mode checkbox if the aggressive mode optimization is desired. See Aggressive Mode below for details.
6. Update the deployment file in Unity Edge.
7. Deploy the update to the HCC2 by selecting Deploy in the navigation tree.
8. Update the master station with your outstation authentication settings and update key authentication settings.

Aggressive Mode

DNP Secure Authentication uses a challenge and response system to verify the authenticity of critical messages. Upon receiving a control command from an outstation, a master issues a challenge to the outstation, and the outstation must respond with a valid authentication token or value within a given time limit. If it does not or if the token or value it sends is incorrect, the command is rejected.

The aggressive mode feature supported by the DNP3 standard allows the Master Station to attempt to bypass the extra challenge steps during critical operations by including the precomputed challenge response in the initial query. This can reduce bandwidth usage and is particularly useful for operations where bandwidth is limited or latency is high.

Redundant Outstation Configuration

The primary and secondary outstations reside in the HCC2 DNP3 Outstation driver. Each outstation must present a unique outstation address. The required master address can be uniquely configured for each. Both outstations are addressed at the IP address of the attached HCC2 Ethernet port on TCP port 20000.

The two outstations can be similarly configured to provide a set of completely redundant outstations. Alternatively, they can also be configured as independent outstations, each with a unique PDEF file to serve two separate masters.

To create a redundant outstation, you can avoid tedious entry of data already entered in the setup of your primary outstation data entry process by using a built-in copy feature.

Assuming you have already configured a primary outstation, proceed as follows:

1. Select the Secondary Outstation Setup tab in the Outstation Config screen.
2. Enter a unique outstation address. The configuration page will report configuration validation errors if the outstation addresses of the primary and secondary outstations are the same.
3. Load the PDEF file that was used in the primary outstation setup.
4. Under the Secondary Secured Authentication section, click the button titled Copy SA Settings from Primary.

Conversely, you can copy Secure Authentication settings from a secondary outstation into a primary outstation configuration using the same procedure and clicking the Copy SA Settings from Secondary button on the Primary Outstation Setup tab.

13.4 DEFINING YOUR OUTSTATION IN A PDEF FILE

The DNP3 Outstation becomes active when the driver is loaded into the HCC2, the DNP3 protocol is enabled and configured in Unity Edge, a PDEF file is mounted in Unity Edge, and the HCC2 is deployed with that configuration.

Note	Because PDEF files are intended to be shared and reused with various masters, they contain no security settings or authentication certificates.

To create an outstation PDEF file, make sure required firewall ports are open, and click the DNP3 Outstation Map Editor button found on either of the Unity Edge DNP3 Outstation screens.

The HCC2 Protocol Definition Editor will open in a new browser window, and the Protocol Definition Header tab will open by default.

13.4.1 Configure a Protocol Definition Header

Note	The metadata collected in the header is published in an auto-generated summary report and in Unity Edge for user reference.

Under the Protocol Definition Header tab, make the following entries as needed.

Parameter	Description
User Protocol Name	Assign a unique, descriptive name to the map.
Protocol Map Version	Defaults to zero. Enter a numeric sequence identifier.
User Description	Optional. Enter a helpful description that indicates the purpose of the map.
Author	Optional. Enter the name of the organization or person who creates the map.
Owner	Optional. Enter the name of the organization or person who is responsible for the map.
Creation Date	Defaults to the local time
Modified Date	Defaults to the local time
Release Notes	Optional. Add any explanatory text.

13.4.2 Define Your Outstation

To create an outstation definition,

1. Select a DNP3 compliance level (Level 3, Level 4, or Level 4+), depending on the level your DNP3 outstation master supports. Levels 3 and below are officially released. Level 3 supports up to Int32 data types.
   - Level 4 supports up to F32 data types but is not an officially released standard.
   - Level 4+ supports up to F64 data types but is not an officially released standard.
2. It is common for enterprise level DNP3 master software suites to support both float and double variations within the analog input groups. Unless you are certain that you require strict Level 3 compliance in your application, leave this option at the default of Level 4+.
3. Configure timeout settings, if desired. The default settings for a new PDEF should be suitable for most applications.
4. Choose the action to be taken when the event buffer overflows – discard the oldest event or discard the newest event.
5. Configure startup default settings for the following items (the state of the outstation at the time it starts). Be aware that, at runtime, the master can globally disable unsolicited reports or change which classes are reported.
   - Configure the frequency of outstation requests for time synchronization with the master.
   - Enable support for unsolicited responses, if desired, and configure default settings for timeouts and retries, if applicable.
   - Enable or disable support for unsolicited responses for each event class, and configure default settings for event count trigger level and transmit holdoff time, if applicable. These settings allow for events to be collected and sent in one packet for a more efficient transfer of data. (For example, if the trigger level value is 5, a packet of events will be sent to the master when 5 unsolicited events are collected. The holdoff time is the length of time (milliseconds) the application will wait before sending an event packet to the master if the count trigger level is not reached.

13.4.3 Adding Data Points for Analog Inputs

DNP3 categorizes all of the data into preset predefined groups, which appear as tabs in the Data Points Definitions screen (analog inputs, analog outputs, binary inputs, binary outputs, and strings).

To create analog inputs,

1. Select the Analog Inputs tab in the PDEF Editor.
2. Click Add HCC2 Data Points to view a list of all available data points. HCC2 data points which are not boolean and string types are selectable as analog inputs. In addition, only data points that are registered as an output of an HCC2 application or functionality are available to send as an input to the master.
3. Select the analog input data points by individually selecting a data point or using standard Windows multi-select tools (Shift+Click, Control+Click) to select groups of data points.
4. Refine your configuration of data points as needed by selecting or deselecting settings for Class Zero Response, event classes, and deadbands described below.

HCC2 “Most Useful” Variations

The HCC2 automatically sorts each selected data point into DNP3 groups and variations. The types of data are organized into groups and the form of the data (the data type, whether the timestamp and flags are included, etc.) is organized into variations.

A master can request any variation, but when variation 0 is requested, the HCC2 provides the variation that it computes to be most useful, based on factors including the compliance level selected, the object or group you are operating in, and the HCC2 data point. If the master sends a command code requesting all of the data in the default variation selected, the HCC2 will respond with data from these “most useful” variations.

Class 0 Response (Integrity Poll)

An integrity poll is a request for current values and is not event-based. All data points are included by default in a Class 0 response. However, you can remove a data point from the response by selecting the row and double-clicking to enter an Edit mode.

Event Classes

Event classes 1, 2, and 3 are provided for organizing events by priority or polling frequency desired. For example, you might assign Class 1 to the group of data points that require most frequent polling.

To assign multiple data points to a single event class

1. Use the Windows standard Shift+Click and Ctrl+Click functions to select the files desired.
2. Click the MultiEdit (in Grid) tool (which appears at the top of the I/O grid when multiple rows are selected) to put the selection in Edit mode and access dropdown menu selections, etc.
3. Choose an event to apply it to all selected data points in one step.
4. Click Confirm to save each class selection.
5. Repeat steps 1 through 4 to assign event classes to all applicable data points.

Unit Descriptor

After a data point is added to your collection of analog inputs, the units of measurement presented to the master can be customized. When added, a data point defaults to the internal base units of its measurement category. Changing the selected units will only alter how the data point is presented to the master. The value will remain as the base unit selection internal to the HCC2 and the Unity Edge interface will continue to display the value in the user-selected units configured.

To change the presented units of measurement, select and then double-click on a row to enter the Edit mode. All options of numerator and denominator units for a measurement category will be presented as a drop-down selection.

Deadbands

Adjust deadband values as needed to control a noisy channel and help ensure that the events triggered are based on a substantive or material change in the value. Defaults are 0.5 for integer values and 0.1 for floating point values. The deadband values are in the selected measurement category and units are selected within the Unit Descriptor column.

13.4.4 Adding Data Points for Analog Outputs

Analog outputs allow the master station to send a request for a change to the outstation. HCC2 data points which are not boolean and string types are selectable as analog outputs. In addition, only data points that are registered as an input of an HCC2 application or functionality are available to be written as an output from the master.

13.4.5 Adding Data Points for Binary Inputs and Outputs

Configuring binary inputs and outputs uses the same basic selections as analog inputs and outputs except you filter the data type to exclude all types but booleans.

13.4.6 Adding Data Points for Strings

Strings are fairly new to the standard but are increasingly supported by many masters. HCC2 data points that are string types and are registered as an output of an HCC2 application or functionality are available to send as an input to the master.

13.5 VIEWING DNP3 DOCUMENTATION

Click the Documentation tab of the PDEF Editor to view a summary of your DNP3 configuration in a printable report. This document presents the data in several different arrangements – listed by index and organized by data groups, sorted by class to show data points included in event classes 1 through 3 and data points in your class 0 integrity poll.

From the PDEF Editor, you can print the report or export the data to multiple formats including pdf for handoff to an integrator.

13.6 DOWNLOADING AND MOUNTING THE PDEF

To mount the PDEF file in Unity Edge

1. From the PDEF Editor, open the Download dropdown menu and select the .PDEF Protocol Definition format to download the PDEF file to your PC.
2. Return to the Unity Edge Outstation Config screen and select the .PDEF file.
3. Update the deployment file in Unity Edge.
4. Deploy the update to the HCC2 by selecting Deploy in the navigation tree.

When the PDEF file is mounted in Unity Edge, you can inspect the DNP3 documentation using the eye icon in Outstation Config screen without leaving Unity Edge.

Section 14: Serial Communication over Bluetooth

The HCC2 allows you to connect wirelessly to Bluetooth devices that support the Serial Port Profile (SPP). This wireless link mimics a traditional serial connection, making it possible for software in the HCC2 to communicate wirelessly with SPP devices as though they are directly connected via wired serial ports. Use cases include using a serial to Bluetooth adapter to connect existing protocol drivers to devices wirelessly, or implementing containerized applications to handle communication with Bluetooth devices supporting SPP.

The setup of an HCC2 Bluetooth connection with another device requires configuration of both Operate and Deploy settings in the HCC2.

14.1 BLUETOOTH STATUS

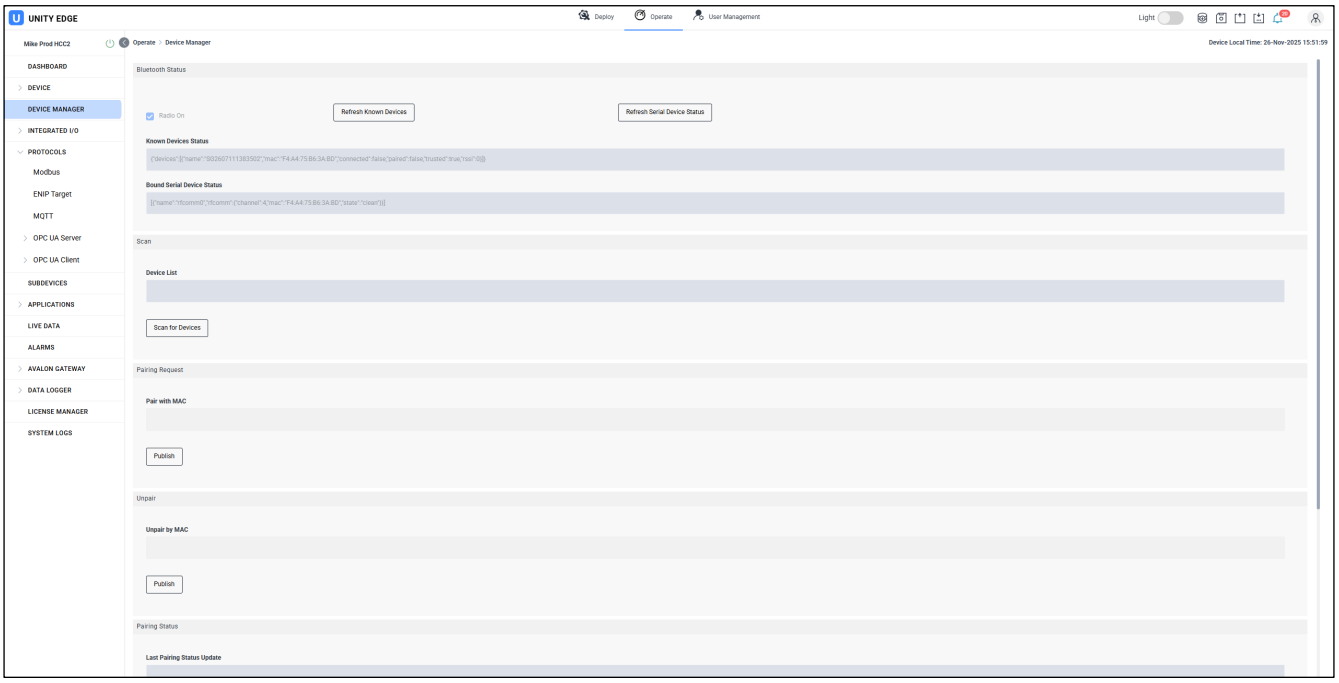
The Operate menu is your source for Bluetooth connection status information. To check the status of your HCC2 Bluetooth connections

1. Navigate to Operate>Device Manager.
2. Under the Bluetooth Status banner, examine the Known Devices Status field.

The text string in this field identifies all detected devices and provides important status details such as whether a device is connected, paired, or trusted, and the quality of the signal.

The status information will update periodically and whenever actions such as adding a new device or pairing are performed. You can also force an instantaneous refresh of device status by pressing the Refresh Known Devices button.

NOTE: The status information can be misleading, depending on when the refresh occurs, and the rate of data exchange. For example, the device could be shown as disconnected and unpaired, however, this status changes as data is transmitted/received. The same with the Serial status – it could show “closed,” but will show “attached” when data is being transmitted.

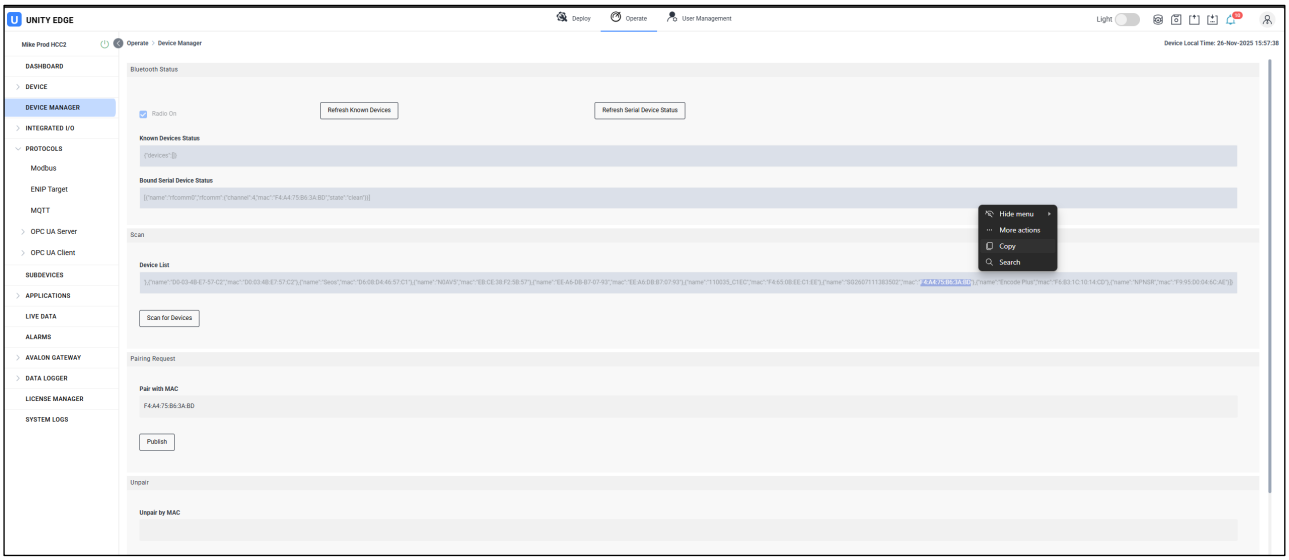


14.2 PAIR THE HCC2 WITH A NEW DEVICE

Device pairing is necessary to establish a secure, one-to-one connection between two devices. To pair the HCC2 with a new device via Bluetooth communications

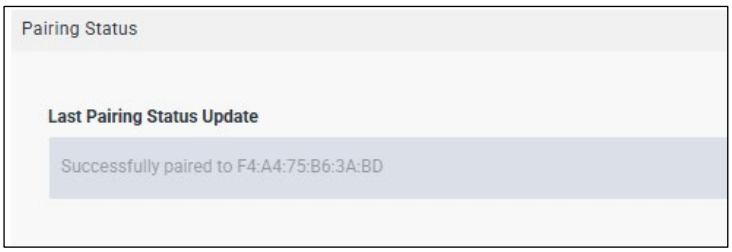
1. Navigate to Operate>Device Manager. Check that the Radio On button is checked, indicating the Bluetooth radio is enabled. If enabled, skip to step 3.
2. If the radio is not enabled
   a. Navigate to Deploy>Device Manager. Toggle the Enable button and deploy this change.
   b. Navigate back to Operate>Device Manager. Check that the Radio On button is checked.
3. Click Scan for Devices to initiate an approximate 2-minute search for nearby devices. A list of detected Bluetooth devices will be displayed in the Device List text string.
4. Locate your device within the list and copy its MAC address.

Note	If the list contains many devices, you may find it easier to copy the entire list (as shown in the popup below) and paste it into the Notepad app, and then locate and copy your device MAC address from there.



5. In the Pairing Request box, paste the address in the Pair with MAC field and click Publish to send the request. The HCC2 will quickly locate the device, authenticate it as a trusted device, and then pair.

   If the pairing is successful, a confirmation message will appear under Pairing Status.



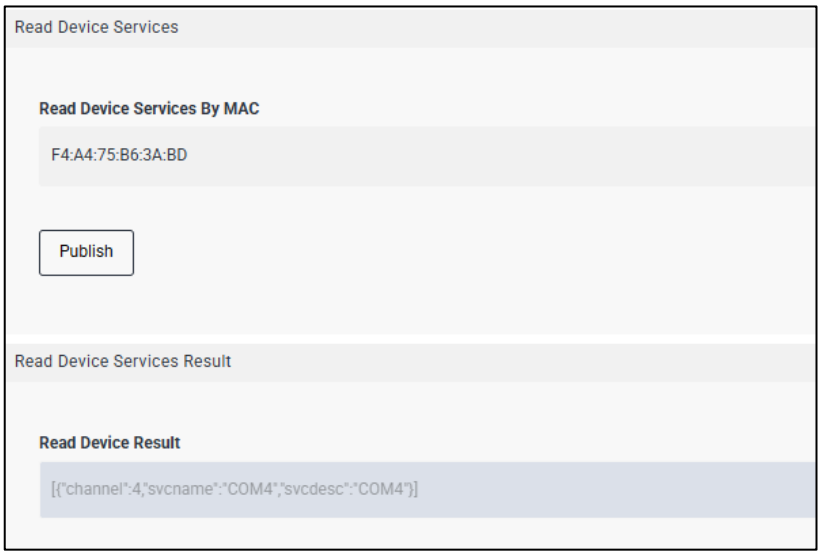
To remove a device from the list of HCC2-paired devices, perform an “unpair” as follows.

1. Copy the MAC address for the device you wish to unpair.
2. In the Unpair box, paste the address in the Unpair by MAC field.

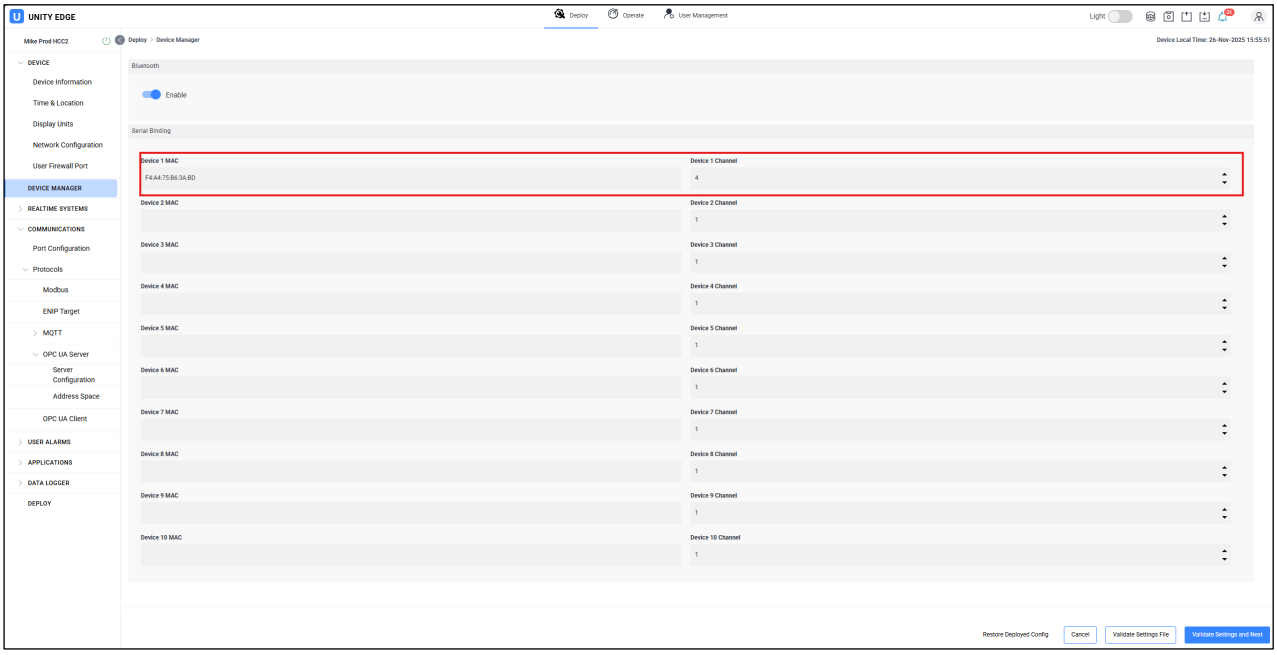
14.3 CONFIGURE A SERIAL COMMUNICATION CHANNEL

To configure a serial communication channel over Bluetooth

1. From the Operate>Device Manager screen, copy the MAC address of a paired device.
2. In the Read Device Services box near the bottom of the screen, paste the address in the Read Device Services by MAC field and click Publish to initiate a search for serial ports.
3. Examine the contents of the Read Device Services Result box. The text string displayed will identify the channel and port number associated with any serial ports detected in the connected device.



4. Navigate to the Deploy>Device Manager screen.
5. Paste the MAC address of your device into the Device 1 MAC field.
6. Enter the channel number of your serial port into the corresponding Device 1 Channel field.



Note that this screen can accommodate up to 10 simultaneous serial port connections.

7. Click Validate Settings.

8. Click Deploy in the navigation tree and use the Deploy wizard to send the configuration change to the HCC2 device.
9. Return to the Operate>Device Manager screen to verify the status of your newly configured serial communication channel under the Bluetooth Status banner in the Bound Serial Device Status field.
10. If the newly configured serial channel does not appear, click the Refresh Serial Device Status button to force a refresh of the display.

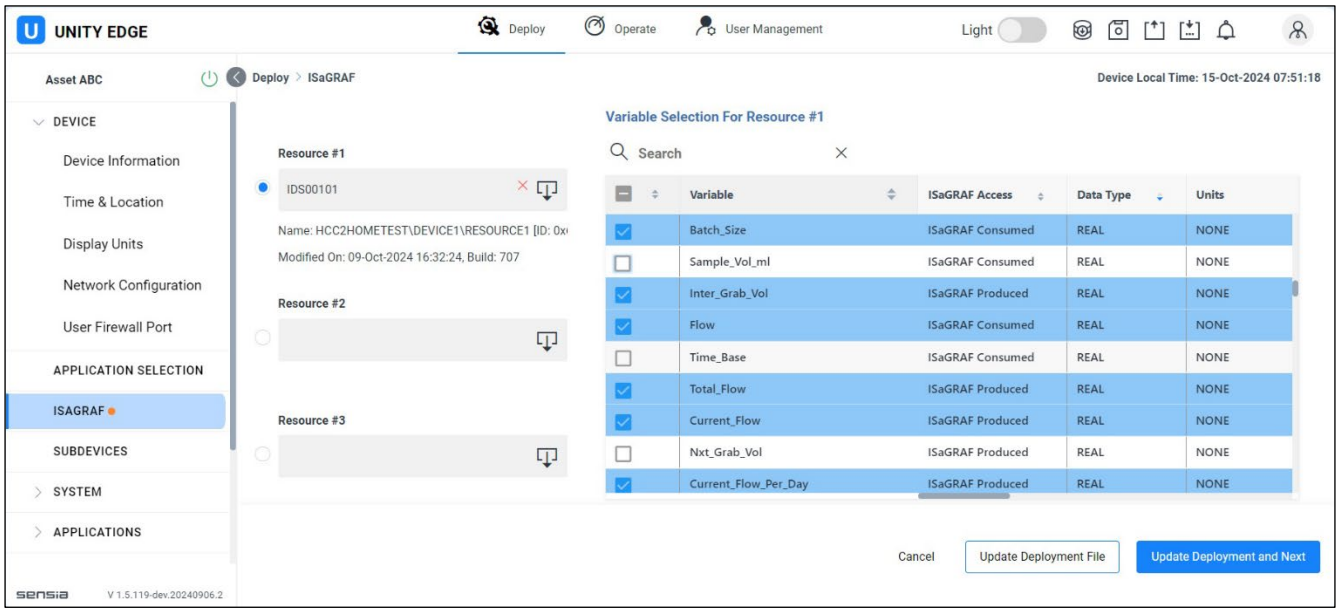
Your Bluetooth device is now configured to send and receive serial data over the configured serial device channel.

Section 15: Developing an ISaGRAF Application for HCC2

The HCC2 supports applications developed in the ISaGRAF Workbench 6.6 with the HCC2 ISaGRAF Add-In installed.

By installing an HCC2 ISaGRAF Add-in, you can use ISaGRAF Workbench to integrate ISaGRAF variables with HCC2 data and inputs/outputs via a data point mapping process.

Inputs and outputs from various applications can be mapped to ISaGRAF data points, and process data points from ISaGRAF can be mapped to Unity Edge data points for use in other applications.



15.1 HCC2 ARCHITECTURE CONSIDERATIONS

15.1.1 Operational Risk Management

The HCC2 data point mapping feature binds various parts of the system together with complex data exchange and manipulation mechanisms. Because these mechanisms involve and affect ISaGRAF resource execution, changes to the system configuration can temporarily stop ISaGRAF resources.

CAUTION

HCC2 deployments affecting the IO board will stop and reload ALL ISaGRAF resources. To avoid unexpected and potentially critical impact to operations, application developers must understand and plan for this behavior when designing applications.

The following changes to HCC2 configuration cause ISaGRAF programs to be stopped and reloaded:

- IO settings (analog, digital, inputs or outputs) or related data point mappings
- Subdevice settings (EtherNet/IP Client) or related data point mappings
- ISaGRAF resource settings or related mappings

15.2 INSTALLING ISAGRAF

15.2.1 Prerequisite Installation

Before attempting to install ISaGRAF Workbench, verify that the Windows feature .NET Framework 3.5 is enabled on your PC or laptop.

Important .NET Framework 3.5 is required for ISaGRAF installation and is supplied (but disabled by default) in recent versions of Windows. If it is not enabled, the ISaGRAF installation will abort with a message indicating this as a pre-requisite.

To check the status of this feature,

1. Open the “Control Panel.”
2. Open the “Programs” window.
3. Select “Turn Windows features on or off.”
4. Ensure the “.NET Framework 3.5 (includes .NET 2.0 and 3.0)” node is enabled.
5. If it is not enabled, change the setting to enable it and reboot your workstation.

Important Enabling (installing) this feature requires a reboot of your workstation for Windows to detect and apply the changes systemwide.

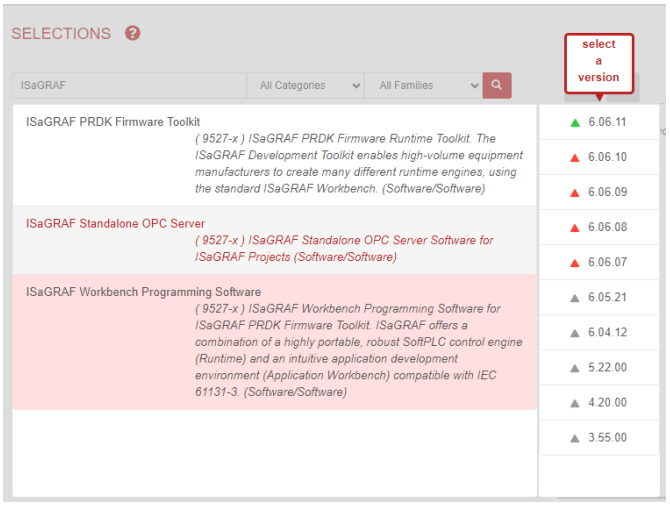
15.2.2 Download the ISaGRAF Workbench

The ISaGRAF Workbench software can be downloaded from Rockwell Automation’s Product Compatibility and Download Center (PCDC).

Important If you do not already have a Rockwell Automation user account, create one. You must be logged in to an account to complete the download.

To download the ISaGRAF Workbench:

1. Open Rockwell Automation’s Product Compatibility and Download Center (PCDC).
2. Under Download, select Downloads by Product.
3. Search for ISaGRAF and click on ISaGRAF Workbench Programming Software ISaGRAF 6.
4. Select the ISaGRAF 6.06.xx version indicated with a green triangle.



5. Click the red Downloads button.
6. Click Select Files to open the list of available downloads.
7. When prompted, log in to your Rockwell Automation user account.
8. Click the checkbox next to ISaGRAF Workbench v6.06.xx - Offline Installer, click the Downloads button and follow the prompts to complete the download.

15.2.3 Install the ISaGRAF Workbench

To install the ISaGRAF Workbench software:

1. Double-click the offline installer executable to extract the files. This download will take several minutes to complete. It will store the .exe at the root of your drive.
2. Click the .exe to unpack a folder containing a compressed .zip file. Extract the contents of the compressed .zip file.
3. Double-click Setup.exe to run the installation wizard.
4. Follow the installation wizard instructions to remove older versions and install the pre-requisites and the ISaGRAF Workbench software.

15.2.4 License the ISaGRAF Workbench

The ISaGRAF Workbench is a licensed software. To license the software after installation:

1. Open the ISaGRAF Workbench software. The software will appear in your Programs list under the name Automation Collaborative Platform.
2. Go to Help > Licensing CAM 5.
3. Copy the three User Codes and email them to keymaster@rockwellautomation.com. Include proof of purchase. The key master will send the two registration keys in response.
4. Enter the received registration keys in the Licensing window.
5. Click Validate.

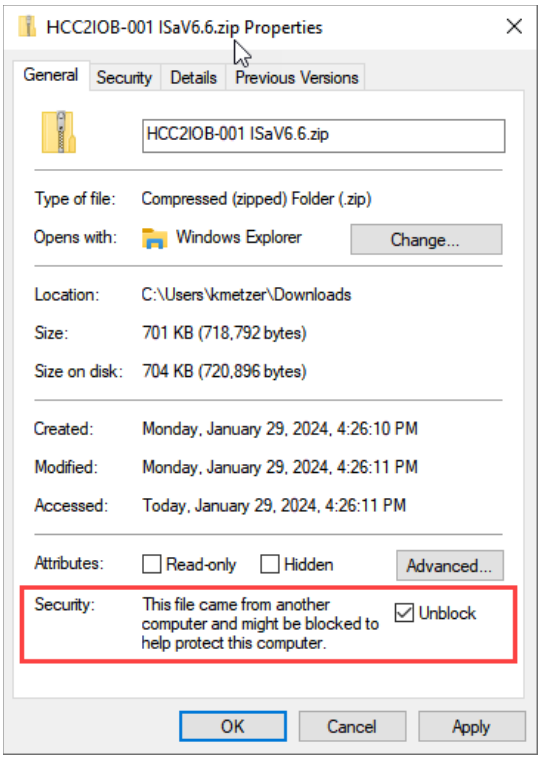
15.2.5 Install the HCC2 ISaGRAF Add-In

The HCC2 ISaGRAF Add-in must be installed to make the ISaGRAF Workbench software compatible with the HCC2.

To install the HCC2 ISaGRAF Add-In:

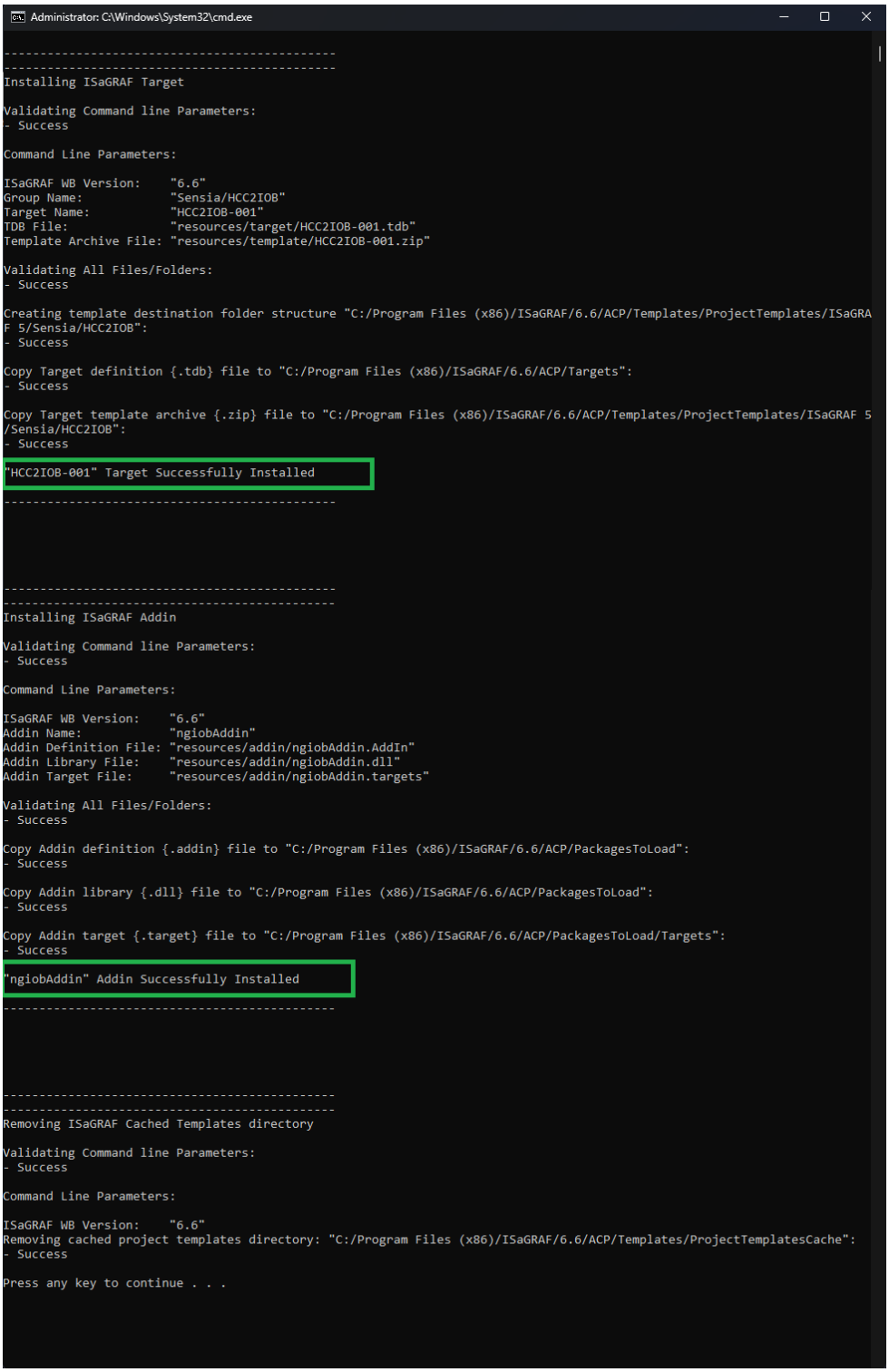
1. Download the HCC2 ISaGRAF Add-in (zip file) from the Sensia website:

   https://www.sensiaglobal.com/Products/RTU-Controllers/QRATE-HCC2-Hyperconverged-Controller
2. Ensure the ISaGRAF Workbench software is closed.
3. Ensure the downloaded zip file is not blocked. Right-click the file and view its properties. If the security message shown in the red box below appears in your dialog, select “Unblock” and click Apply.



4. Extract the downloaded HCC2 ISaGRAF Add-In.
5. Run the Install HCC2IOB-001_ISaGRAF_v6.6.bat batch script file as administrator. The installation status will be displayed in a command prompt window.

   After a successful installation, the command prompt window displays the message “`ngiobAddin`” `Addin Successfully Installed`.



6. Open the ISaGRAF Workbench and verify that the Output window displays: “HCC2 Addin Instantiation : Connect : Version 1.00 (2000-01-01)”.

15.3 CREATING AN HCC2 ISAGRAF APPLICATION

The HCC2 supports ISaGRAF applications created using the HCC2 template, new ISaGRAF applications created by importing an existing HCC2 project, and existing applications converted to run in the HCC2.

15.3.1 Create an HCC2 ISaGRAF Project

To create a new ISaGRAF project for the HCC2 using the HCC2 template:

1. Open the ISaGRAF Workbench.
2. Ensure the HCC2 ISaGRAF Add-In is installed. The Output window should display: “HCC2 Addin Instantiation : Connect : Version 1.00 (2000-01-01)”.
   If it is not installed, follow the HCC2 ISaGRAF Add-In installation instructions (section 15.2.5, Install the HCC2 ISaGRAF Add-In, page 177).
3. Go to New > Project > CAM Projects > ISaGRAF 5 > Sensia > HCC2IOB.
4. Select the HCC2IOB-001 template.
5. Enter a name for the new project and click OK.

15.3.2 Import an HCC2 ISaGRAF Project

To create a new ISaGRAF project by importing an existing HCC2 project:

1. Open the ISaGRAF Workbench.
2. Ensure the HCC2 ISaGRAF Add-In is installed.
   - The Output window should display: “HCC2 Addin Instantiation : Connect : Version 1.00 (2000-01-01)”.
   - If it is not installed, follow the HCC2 ISaGRAF Add-In installation instructions.
3. Go to New > Project > CAM Projects > ISaGRAF 5 > Import > Import ISaGRAF 5 Project.
4. Enter a Name for the new project and click OK.
5. Browse for the PrjLibrary.mdb database file located in the ISaGRAF project folder of the project to be imported and click OK. For projects stored in the default location, the database file can be found under:
   C:\Users\<UserName>\Documents\ISaGRAF 6.6\Projects\<ProjectName>\<ProjectName>\<ProjectName>\PrjLibrary.mdb
6. Save the project and close the ISaGRAF Workbench.
7. Go to the ISaGRAF project folder and locate the project configuration file. For projects stored in the default location, the project configuration file can be found under:

   C:\Users\<UserName>\Documents\ISaGRAF 6.6\Projects\<ProjectName>\<ProjectName>\<ProjectName>.acfproj
8. Open the project configuration file with a text editor (e.g., Notepad).
9. Look for the line:
   <Import Project="$(DevEnvDir)\PackagesToLoad\Targets\ISaGRAF.ISaGRAF5.targets" />
10. Add a new line (under the line in step 9):
    <Import Project="$(DevEnvDir)\PackagesToLoad\Targets\ngiobAddin.targets" />
11. Save and close the project configuration file.

15.4 CONVERTING AN ISAGRAF PROJECT TO AN HCC2 PROJECT

To convert an existing ISaGRAF project that uses the built-in simulator or a third-party target to a project that can run in an HCC2 target:

1. Create a copy of the ISaGRAF project folder you wish to convert.
2. Open the ISaGRAF Workbench.
3. Ensure the HCC2 ISaGRAF Add-In is installed.
   - The Output window should display: “HCC2 Addin Instantiation : Connect : Version 1.00 (2000-01-01)”.
   - If it is not installed, follow the HCC2 ISaGRAF Add-In installation instructions.
4. Open the existing project.
5. Right-click the project name and select Import > Import Target Definitions.
6. Browse to C:\Program Files (x86)\ISaGRAF\6.6\ACP\Targets.
7. Select the HCC2IOB-001.tdb target definition and click Open.
8. Go to View > Deployment View.
9. Click on the existing target to display its Properties window.
10. Under Target, replace the existing target with the HCC2IOB-001 target.
11. If displayed, review the Proposed Changes in the Target Change pop-up window. Consider this list of behaviors when replacing a third-party target with the HCC2 target.

Device-specific Components	Device-specific Program Organization Units (POU) and DataTypes are embedded in the target definition. The new target definition will not include any device-specific functions, function blocks, arrays, structures and defined words that were available in the original target definition.
	The device-specific components will be listed in the Proposed Changes list as: This POU 'POU Name' does not exist in the new target definition. Using this POU in your project may cause compilation errors.
	When possible, convert the device-specific components into user-defined components to be imported or recreated in the updated project.
I/O Devices	I/O devices are embedded in the target definition. All instances of the I/O devices from the original target definition will be removed from the project.
	Variables with the Direction setting configured as VarInput and VarOutput will be unwired, and a compilation error will be generated for each unwired variable.
	The instances of the I/O devices will be listed in the Proposed Changes list as: The new target 'HCC2IOB-001'does not support the I/O device 'I/O Device Name'. This instance will be removed from the project and all its related I/O variables.
	The HCC2 target does not require I/O devices to communicate with the I/O. The input and output variables must have their Direction changed to Var and will be treated as internal variables.
	The values from the HCC2 integrated I/O, Modbus data, and subdevices connected to the HCC2 can be mapped to these data points via Unity Edge. In addition, the integrated I/O can be accessed via device-specific function blocks.

12. Click Yes if you wish to continue with the target change operation.
13. Save the project and close the ISaGRAF Workbench software.

14. Go to the ISaGRAF project folder and locate the project configuration file. For projects stored in the default location, the project configuration file can be found under:

    C:\Users\<UserName>\Documents\ISaGRAF 6.6\Projects\<ProjectName>\<ProjectName>\<ProjectName>.acfproj

15. Open the project configuration file with a text editor (e.g., Notepad).
16. Look for the line:
    `<Import Project="$(DevEnvDir)\PackagesToLoad\Targets\ISaGRAF.ISaGRAF5.targets" />`
17. Add a new line (under the line in step 16):
    <Import Project="$(DevEnvDir)\PackagesToLoad\Targets\ngiobAddin.targets" />
18. Save and close the project configuration file.

15.5 CONFIGURING COMMUNICATIONS TO THE HCC2

The ISaGRAF HCC2 template uses the default IP address of ETH-2 as the communication path between the ISaGRAF Workbench workstation and the HCC2. To define a different IP address:

1. Go to View > Deployment View.
2. Right-click the connection between the HCC2 target and the ETCP (enhanced TCP/IP) network and select Properties.
3. Under IP Address, enter the required IP address.

15.6 CONFIGURING ISAGRAF RESOURCES

ISaGRAF Resources are unique memory instances inside the ISaGRAF runtime, each with its own execution time, global variables, and POUs (program organization units).

All ISaGRAF Resources running in the HCC2 must be developed using the ISaGRAF Workbench software installed with the HCC2 ISaGRAF Add-In. See section 15.2, Installing ISaGRAF, page 176, for installation instructions.

Before Resources can be loaded into an HCC2, you must configure the following properties in ISaGRAF Workbench software.

15.6.1 Resource Number

Each ISaGRAF Resource must have a unique identification number. The Resource Number is assigned automatically when adding a new Resource. ISaGRAF Resources running in the HCC2 must be numbered from 1 to 4.

To edit the Resource Number:

1. Go to View > Solution Explorer.
2. Right-click the Resource and select Properties.
3. Under Info, configure the Number property as required.

15.6.2 Cycle Time

The ISaGRAF HCC2 template preconfigures Resources to execute the application as fast as possible, without waiting for an elapsed cycle time to trigger the next cycle.

The following Resource properties are available for configuring cycle time:

- Cycle Time - Amount of time given to each cycle. If an execution cycle is configured within the cycle time period, the system waits until this period has elapsed before starting a new cycle. The Cycle Time property is only enforced when the Trigger Cycles property is set to True.
- Cycle Time Units - Milliseconds (ms)
- Trigger Cycles - Indication of whether a Resource executes according to the defined Cycle Time. When set to True, if a cycle is completed within the Cycle Time, the system waits until the cycle time has elapsed before starting a new cycle. When set to False, the system starts a new cycle as soon as the previous cycle is completed.

To configure the Resource Cycle Time:

1. Go to View > Solution Explorer.
2. Right-click the Resource and select Properties.
3. Under Settings configure the Cycle Time and Trigger Cycle properties as required.

15.6.3 Symbol Table

The ISaGRAF Workbench generates a symbol table file for each Resource.

The symbol table file for each Resource running in the HCC2 must be loaded in Unity Edge to allow the Resource variables to be mapped to the integrated I/O, CIP subdevices, Modbus registers and other applications running in the HCC2.

By default, the ISaGRAF HCC2 template preconfigures the Resource symbol table type as Complete. The Complete setting ensures that all Resource variables are included in the symbol table file. If the symbol table type is configured as Reduced or None, the symbol table type will be rejected by Unity Edge.

To verify the Resource symbol table type as Complete:

1. Go to View > Solution Explorer.
2. Right-click the Resource and select Properties.
3. Under Code > Embedded Table Type, select Complete.

15.7 CONFIGURING ISAGRAF VARIABLES FOR UNITY EDGE INTEGRATION

You can map ISaGRAF variables to the HCC2 integrated I/O, CIP subdevices, Modbus registers, and tags from other ISaGRAF Resources and HCC2 applications by making them accessible from Unity Edge.

The integration of ISaGRAF variables in Unity Edge is done via the Attribute property which controls their read and write access.

15.7.1 Configure Read and Write Access

The read and write access attribute defined for each ISaGRAF variable determines the type of mapping that can be done when the variable is available as an HCC2 data point.

- Read - Variables configured as Read are consumed by the ISaGRAF application and can be mapped to read from analog and digital input channels, diagnostic information from CIP subdevices, Modbus registers, and tags from other applications running in the HCC2.

  When a variable attribute is set to Read and subsequently selected to be mapped to Unity, then it can no longer be manually set to a value using ISaGRAF, all data values must come from Unity.

- Write - Variables configured as Write are produced by the ISaGRAF application and can be mapped to write to analog and digital output channels, outputs to CIP subdevices, Modbus registers, and tags from other applications running in the HCC2.

  Variables with Write attribute can only be written to by logic, their value cannot be read. If reading and writing of value is desired, the attribute must be set to Read/Write.

- Read/Write - Variables configured as Read/Write are produced by the ISaGRAF application and can be mapped to write to analog and digital output channels, outputs to CIP subdevices, Modbus registers, and tags from other applications running in the HCC2. The difference between Write and Read/Write variables is that Read/Write access allows the ISaGRAF to read from the variable and use them as inputs in the logic.

For HCC2 data points that need to be read by the ISaGRAF application and written to the ISaGRAF application, create two separate ISaGRAF variables (i.e., one ISaGRAF variable with Read access and one ISaGRAF variable with Write access).

To configure the read and write access of an ISaGRAF variable:

1. Go to View > Solution Explorer.
2. Expand the Resource and double-click Global Variables.
3. Locate the Attribute property of the required variable and configure it as Read or Write.

15.7.2 Configure Direction Property

You must set the Direction property to *Var* for all ISaGRAF variables in an HCC2 application. Do not use the VarInput and VarOutput options.

In HCC2 applications, the I/O is accessed via mapping in Unity Edge. The Direction property of ISaGRAF variables is not used, as the ISaGRAF resources do not require ISaGRAF I/O Devices (also known as I/O boards).

15.8 MAPPING VARIABLES BETWEEN RESOURCES

Use the Unity Edge interface to map variables between ISaGRAF resources. The use of internal bindings between Resources is not recommended.

Refer to section 6.6.2, Select Variables for Data Point Mapping, page 56, for information about mapping variables and other HCC2 data points between Resources using Unity Edge.

15.9 BUILDING AN ISAGRAF APPLICATION

The Build operation compiles the code and the configuration settings programmed in an ISaGRAF application. You can build the entire ISaGRAF project, a single Resource, and/or individual programs, functions, or function blocks.

You must build the code in an ISaGRAF Resource before downloading it to the HCC2. Errors in the Build results will prevent the download of the code to HCC2. If the results include warnings, you should investigate and resolve them before downloading the Resource to the HCC2. However, warnings will not prevent a download.

15.9.1 Build All ISaGRAF Resources

The Build operation for the entire solution compiles all ISaGRAF Resources and creates and updates the symbol table files of each Resource used by Unity Edge to load the Resource variables.

To build all the Resources:

1. Right-click the Project or the Device and select Build, or right-click the solution name at the top of the Solutions Explorer window and select Build Solution. You can also use the Build Solution toolbar icon.
2. Monitor the Output window and confirm that the results show: “0 error(s), 0 warning(s)” for all Resources.

The symbol file is located in the ISaGRAF project folder. For projects stored in the default location, the symbol file can be found under:

C:\Users\<UserName>\Documents\ISaGRAF 6.6\Projects\<ProjectName>\<ProjectName>\IDSnnn01

where 'nnn' is the Resource Number in hexadecimal (i.e., IDS00101 for Resource #1, IDS00201for Resource #2, IDS00301 for Resource #3, and IDS00401for Resource #4).

15.9.2 Build a Single ISaGRAF Resource

To build a single Resource:

1. Right-click the required Resource and select Build. You can also use the Build toolbar icon.
2. Monitor the Output window and confirm that the results show: “0 error(s), 0 warning(s)”.

15.9.3 Build a Program, Function, or Function Block

To build an individual program, function, or function block:

1. Right-click the required program, function, or function block and select Build. You can also use the Build toolbar icon.
2. Monitor the Output window and confirm that the results show: “0 error(s), 0 warning(s)”.

15.10 DOWNLOADING AN ISAGRAF APPLICATION TO THE HCC2

The Download operation sends the compiled code and configuration settings of ISaGRAF Resources to the target in the HCC2. The ISaGRAF Resource code must be built before it can be downloaded to the HCC2 (see section 15.9.1, Build All ISaGRAF Resources, page 184). You can download all Resources in one Download operation or download an individual Resource to the HCC2.

15.10.1 Download All ISaGRAF Resources

To download all the Resources:

1. Right-click the Project or the Device and select Download. You can also use the Download toolbar icon.
2. If a Resource is already running, you will be asked to stop it before downloading. Click Yes to stop the Resource and download it, or No to cancel the download.
3. Monitor the Output window and confirm that the results show: “Download: n succeeded”, where 'n' is the number of downloaded Resources.

15.10.2 Download a Single ISaGRAF Resource

To download a single Resource:

1. Right-click the required Resource and select Download. You can also use the Download toolbar icon.
2. If the Resource is already running, you will be asked to stop it before downloading. Click Yes to stop the Resource and download it, or No to cancel the download.
3. Monitor the Output window and confirm that the results show: “Download: 1 succeeded”.

15.11 MONITORING AN ISAGRAF APPLICATION

The ISaGRAF application running in the HCC2 can be monitored online using the ISaGRAF Workbench Debug functionality.

When debugging an ISaGRAF application, you can

- Monitor program execution
- Monitor variable values
- Modify variable values
- Modify cycle timing

15.11.1 Debug an ISaGRAF Application

The ISaGRAF Workbench will attempt to go online simultaneously with all the Resources that are part of the application. To go online, the application in the ISaGRAF Workbench must match what has been downloaded to the HCC2. When there is no match found, an error message is displayed and online monitoring is not possible.

To debug an ISaGRAF application, go to Debug > Start Debugging. You can also use the Start Debugging toolbar icon.

15.11.2 Monitor and Modify Variable Values

You can monitor and modify the values of ISaGRAF variables from the Global Variables and Local Variables views, from user-defined Spy Lists, and from programs developed in Function Block Diagram or Ladder Logic.

From the ISaGRAF Workbench software, you can modify the values of ISaGRAF variables with the Attribute property defined as Write or Read/Write. When the application logic is writing a value to a variable, this value will overwrite a user-written value.

To modify the value of a variable from the Global Variables and Local Variables views or from a Spy List:

1. Locate the variable. For structures, expand the variable list until the desired element is visible.
2. In the Logical Value column, toggle the digital value using the checkbox or enter the new analog value.

To modify the value of a variable from a program:

1. Double-click the Program to open it.
2. Double-click the variable to open its Write Logical Value window.
3. For digital variables, choose TRUE or FALSE. For analog variables, enter the new value.
4. Click Write to write the value to the variable.

15.11.3 Lock Variable Values

HCC2 ISaGRAF applications do not support locking (forcing) of input and output variables from the ISaGRAF Workbench. The Direction property of all ISaGRAF variables in the application must be set to Var, defining all variables as internal.

To connect ISaGRAF variables to HCC2 data points, including input and output data points, refer to the configuration requirements in

- Configuring ISaGRAF Variables for Unity Edge Integration (section 15.7)
- Select Variables for Data Point Mapping (section 6.6.2)
- Mapping Variables Between Resources (section 15.8)

Make provisions in the ISaGRAF application logic for maintenance operations that require modifying HCC2 inputs and outputs values. These provisions can include maintenance bypasses, out-of-service overrides, substitute input process value logic, proof testing logic, etc.

15.12 PERFORMING ONLINE CHANGES

You can modify ISaGRAF Resources running in the HCC2 without stopping the running application by making an online change.

Use online changes with care and make sure you understand their impact on the running application before executing the online change(s).

The following cannot be modified online:

- User-defined arrays and structures
- Device and Resource properties

15.12.1 Online Change Considerations

When you are planning an online change, review the impact of each available online change task as described in the ISaGRAF Workbench documentation. The following must be considered:

- Bindings are not available, and all consumed variables follow their defined update behavior.
- Initial values of variables are applied upon restarting a Resource, and Resources do not restart after an online update.
  - To change the current value of a variable, refer to section 15.11.2, Monitor and Modify Variable Values, page 186.
  - To prevent undesired values after a future Resource restart, change the initial value online in addition to changing the current value online.
- The Resource cycle time could be impacted by the modification. Adding additional logic or new mapped variables could increase the cycle time.
- Depending on the type of change, variables, functions, and function blocks could be reinitialized.

15.12.2 Perform an Online Change

You can modify all Resources in one online operation or modify a single Resource online. You must build the ISaGRAF Resource code before it can be sent to the HCC2 via an online change.

CAUTION

Write and test your ISaGRAF Resource changes in ISaGRAF Workbench before deploying to the HCC2. Once you deploy an ISaGRAF application, Edge devices will immediately handle the writing to all tags, and you will lose the ability to make online changes to ISaGRAF resources.

Change All ISaGRAF Resources Online

To change all the Resources:

1. Right-click the Project or the Device and select Online Change. You can also use the Online Change toolbar icon.
2. Monitor the Output window and confirm that the results show: “Online change: n succeeded”, where 'n' is the number of downloaded Resources.

Change One ISaGRAF Resource Online

To perform an online change to a single Resource:

1. Right-click the required Resource and select Online Change. You can also use the Online Change toolbar icon.
2. Monitor the Output window and confirm that the results show: “Online change: 1 succeeded”.

15.13 PROTECTING AN ISAGRAF APPLICATION

The ISaGRAF Workbench allows you to define access control for various software elements of the project as well as the physical target device in the HCC2.

Password definitions are limited to eight characters and can consist of letters, digits, and symbols.

New passwords will be enabled the next time the project is opened from the ISaGRAF Workbench.

The following table shows the user actions that can be password protected.

Protected Element	Protection Provided by Password
Project	Cannot open for editing
Device	Cannot add, edit, or delete resources, programs, functions, function blocks, and variables and variable groups
Program	Cannot open for editing
Function	Cannot open for editing
Function Block	Cannot open for editing
Target Device (HCC2)	Cannot connect to the device or start or stop Resources. Cannot perform downloads, make online changes, or modify variable values

15.13.1 Protect Software Elements

To protect a software element with a password:

1. Right-click the element and select Password.
2. In the Set Password window, type and confirm the required password, then click OK.

To remove a password from a software element:

1. Right-click the element and select Password.
2. Type the current password in the Old Password field.
3. Leave the New Password and Confirm Password fields blank, then click OK. The element will no longer be password-protected.

15.13.2 Protect the HCC2 Target Device

The target device password is embedded in the HCC2 and must be set and changed online. A connection to the device is required to set and change the target device password.

To protect a target device with a password:

1. Right-click the Device element and select Target Password.
2. In the Set Target Password window, type and confirm the required password, and then click OK.
3. Monitor the Output window and confirm that it shows: “The target password was set successfully”.

To remove a password from a target device:

1. Right-click the Device element and select Target Password.
2. Type the current password in the Old Password field.
3. Leave the New Password and Confirm Password fields blank, then click OK. The element will no longer be password-protected.
4. Monitor the Output window and confirm that it shows: “The target password was removed successfully”.

Section 16: Factory Talk Optix

FactoryTalk Optix (FT Optix), a data visualization tool supplied by Rockwell Automation, can now be integrated with the HCC2 to create customized HMI displays for monitoring and controlling a variety of oilfield operations.

With the proper installation of a runtime file provided by Sensia and a license purchased from Rockwell Automation, you can quickly configure custom projects and push them to the HCC2 to enable displays on your connected HMI.

Adding this feature requires the installation of a runtime file and an FT Optix license. This will add three new applications to the HCC2: *ftoptix-api-server, edge_optixruntime and edge_optixentitlement.*

Important Internet connection with the HCC2 is required to activate the FT Optix license. After activation the HCC2 can be disconnected from the internet.

16.1 INSTALL AND SETUP HCC2 RUNTIME

1. Download and install the FT Optix bundle.
   a. Download the ***hcc2OptixBundle.mender*** file from Sensia's Microsoft Azure Storage Explorer repository. See section 1.3.3, Software Downloads, page 12, for instructions.
   b. Use the EPM tool to transfer the ***hcc2OptixBundle.mender*** file to the HCC2. See Section 4: Updating and Managing HCC2 Software, page 41, for instructions.
2. Obtain an FT Optix License from a Rockwell Automation Distributor, or purchase it from the FactoryTalk Hub, FactoryTalkHub.com.
3. Establish an internet connection on your HCC2.
4. Install the FT Optix license on the HCC2.
   a. Copy the license key from the FactoryTalk Hub website.
   b. Open Unity Edge in a web browser and navigate to **Operate > License Manager.**
   c. In the FT Optix Licensing section, click Add License.
   d. At the dialog prompt, paste your license key and click Apply.

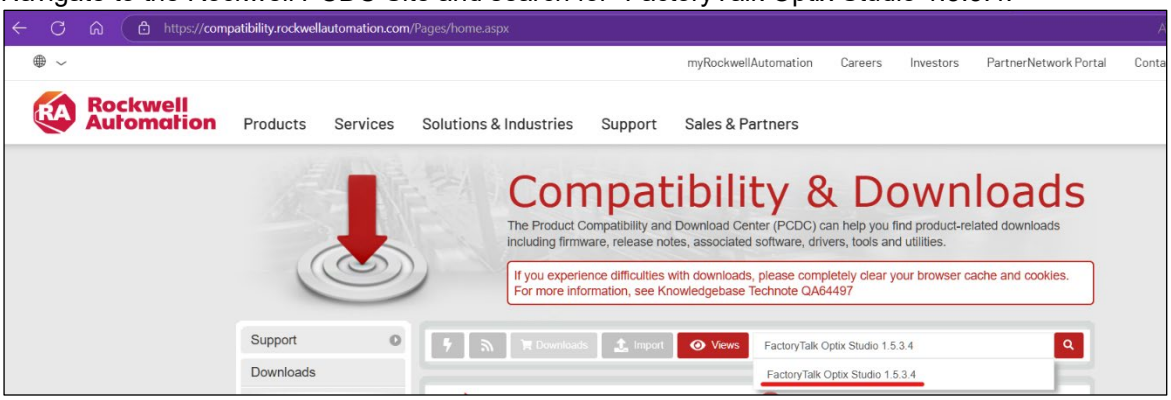
   When the upload completes, the license key will appear in the FT Optix Licensing table. The license status, type, and expiration date (if applicable) are also captured.
5. Deactivate your HCC2 internet connection, if desired.

16.2 DOWNLOAD AND INSTALL FACTORYTALK OPTIX STUDIO

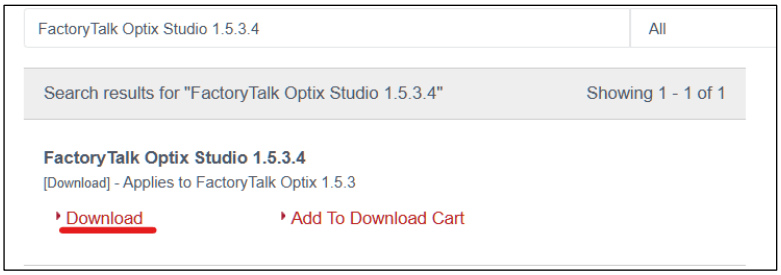
FactoryTalk Optix Studio is required to develop and download a project on the HCC2.

FactoryTalk Optix Studio can be downloaded from the Rockwell Automation PCDC site, https://compatibility.rockwellautomation.com/Pages/home.aspx.

1. Navigate to the Rockwell PCDC Site and search for “FactoryTalk Optix Studio 1.5.3.4.”



2. Select the Download link.



3. Sign in with your credentials for Rockwell PCDC.
4. Follow the instructions in the popup windows to initiate the download.
5. Run the .exe file to install FactoryTalk Optix Studio on your computer.

16.3 COMMUNICATION DRIVER

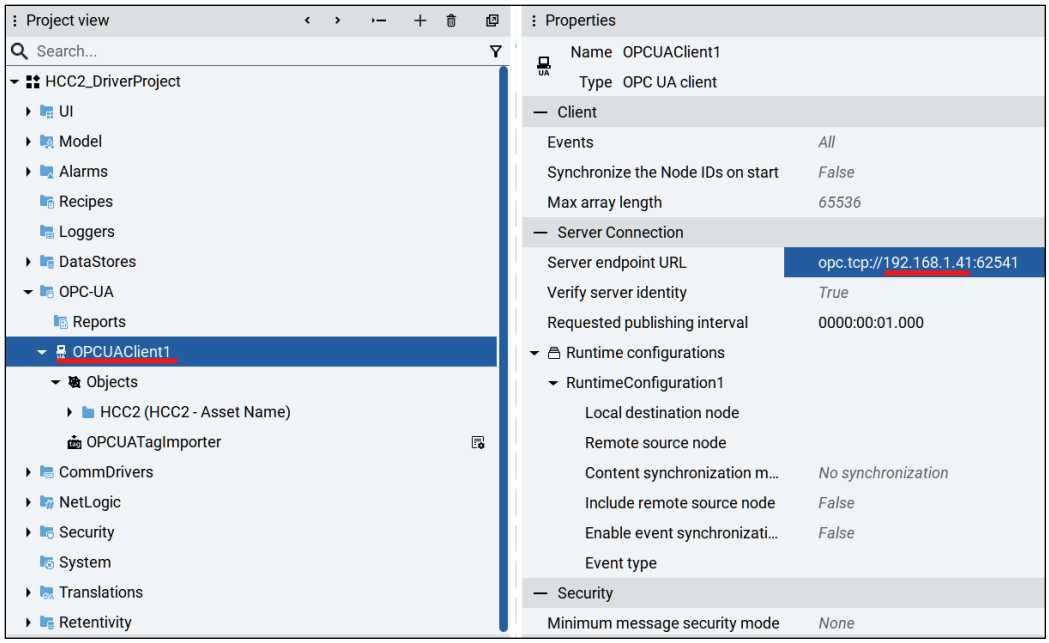
Users can read and write data using the OPC UA protocol. HCC2 firmware includes an OPC UA Server that can be configured with Unity Edge. An OPC UA Client must be set up in FT Optix using FactoryTalk Optix Studio software.

When using OPC UA in FT Optix, the project’s **Server endpoint URL** is a critical setting. Take care to set the correct network address for the endpoint, depending on where the client is running. The examples below describe running the project from FactoryTalk Optix Studio vs. running it in the HCC2.

16.3.1 Running the Project from FT Optix Studio

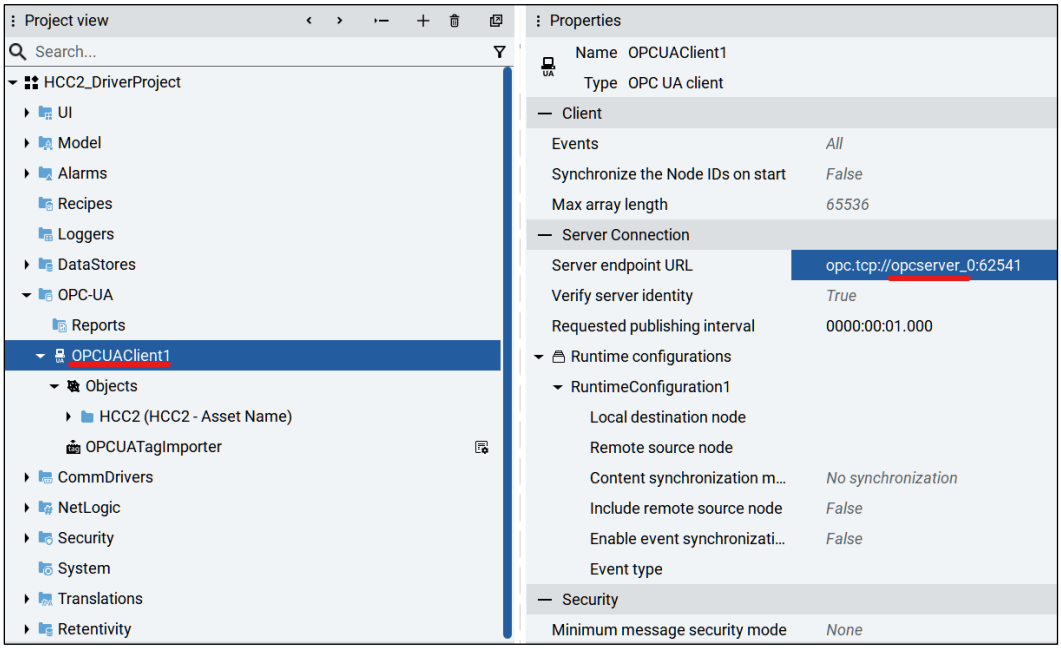
In this example, we are connecting to the HCC2 through the static IP address on Eth-2 (192.168.1.41). This will enable communication from FactoryTalk Optix Studio to the HCC2 OPC UA Server for tasks such as importing data points and emulating the project.

Make sure the **Server endpoint URL** is set to connect to the HCC2 IP address.



16.3.2 Running the Project from the HCC2

Before downloading your project to the HCC2, change the **Server endpoint URL** to the internal host name of the OPC UA Server "*opcserver_0*". This will enable the project to communicate on the internal network inside of the HCC2.



16.4 USER HELP

You can find manuals, online help, and Getting Started videos for FactoryTalk Optix on the Rockwell Automation website:

https://www.rockwellautomation.com/en-us/support/documentation/technical/capabilities/optix-portfolio.html#gate-d7236618-f4b1-4839-8648-6f313e966a55

Appendix A: HCC2 Data Quality Codes

The Quality value in an HCC2 data point is used to represent the validity of the data point's value. The HCC2 uses OPC codes which fall into three main categories:

A.1 DATA QUALITY RANGES

Category	Low Range	Upper Range	Description
Bad	0	63	generally indicates the data are not valid
Uncertain	64	191	generally indicates the data are speculative in some manner
Good	192	219	generally indicates the data are valid

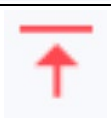
A.2 CODE DESCRIPTIONS AND LOGIC

Each quality category is divided into sub-categories. The table below presents the typical OPC criteria for each code value and the HCC2 usage of the code.

If two or more quality codes apply to an HCC2 datum value, an application should adhere to the following logic:

- If one or more qualities are Bad, present the highest value in the Bad Category.
- Else if one or more qualities are Uncertain, present the highest value in the Uncertain Category.
- Else if one or more qualities are Good, present the highest value in the Good Category.

Quality Code	OPC Criteria	HCC2 Criteria	HCC2 Description & Application Usages	Unity Glyph
0	Bad [Non-Specific]	Bad	The value is bad but no specific reason is known or given. Generally used by all applications. **Event Manager:** Event contains a condition that is watching a data point that has reported this state. No higher priority quality code present in all event conditions.	
4	Bad [Configuration Error]	Unable to Parse	There is a server-specific problem with the configuration. **Modbus:** Protocol Definition File not valid.	
8	Bad [Not Connected]	Device Not Connected	The input is required to be logically connected to something but the connection couldn't be established. **Modbus:** The remote server connection is lost.	
20	Bad [Last Known Value]	Last Known Value	Communications have failed. Last known value is available. **Modbus:** Data query failed a transaction attempt and has previously received a value, but the query has not yet qualified as stale.	
24	Bad [Communication Failure]	Communication Failure	Communications have failed. No last known value is available. **Modbus:** Data query failed a transaction attempt and has not yet received a value, but the query has not yet qualified as stale.	

28	Bad [Out of Service]	Out Of Service	The data point publisher is off or otherwise locked. Value has not been updated. **Event Manager:** Event is not enabled. **Modbus:** When a PDEF is removed, any data points it was producing are marked as Out of Service. **IOB Manager:** When an ISaGRAF, Ethernet/IP, or Custom data point is removed during the Deployment action, it is marked as Out Of Service.	
64	Uncertain [Non-Specific]	Data Stale	The value is known to not be updated within a watched time period (Stale). **Modbus:** Data query age has exceeded the stale alarm but the remote server has not yet qualified as lost. **Event Manager:** Event contains a condition that is watching a data point that has reported this state. No higher priority quality code present in all event conditions.	
65	Uncertain [Non-Specific] (Low Limited)	Minimum Out Of Range		
66	Uncertain [Non-Specific] (High Limited)	Maximum Out Of Range		
67	Uncertain [Non-Specific] (Constant)	Frozen	HCC2 applications should use code 216 for overridden and bypassed values if quality category is good.	
192	Good [Non-Specific]	Good	The value is good. Generally used by all applications.	
216	Good [Local Override]	Local Override	The value has been overridden or bypassed but the state is considered good. HCC2 applications should use code 67 for overridden and bypassed values if quality category is uncertain. **Event Manager:** An event is bypassed.	
219	Good [Local Override] (Constant)	Constant Override	Value is computed with a constant overridden value. **Event Manager:** Event contains a condition that is watching a data point that has reported a quality code of 216-219. No higher priority quality code present in all event conditions.	

Appendix B: Troubleshooting Connectivity

B.1 UNITY EDGE NOT LOADING

Upon device startup, Unity Edge takes about 1 to 2 minutes to load. Therefore, upon initial connection of the device or after a reboot, you may need to wait a few minutes before loading.

B.2 UNITY EDGE NOT LOADED PROPERLY

Though the website may come up, there may be compiling going on in the background. For example, the expected menu is not fully displayed. In Chrome, the reload button indicates that the page is loading. When it is complete, the page should refresh. You can safely refresh the browser page as all changes saved to the deployment file will not be lost.

B.3 LOST CONNECTION

Verify that the USB or Ethernet cable has not come disconnected from the device and that the device is running. If a cable has come unattached upon reattached connection should be restored. If both appear to be correct you could verify that Unity Edge is running by using the EPM utility.

B.4 PROTECTED MODE

If you are experiencing issues deploying a new configuration to your device, making any run-time changes, or downloading and changing ISaGRAF applications, make sure your device is not in Protected Mode. An HCC2 in Protected Mode is meant to be in a known/running condition, and no changes are expected. This is a security mechanism, intended to reject any unwanted changes to the device. If you need to make changes to the HCC2, you will need physical access to the DIP switches on the side of the device. Put your HCC2 in Protected Mode only if you are sure that you don’t need to make changes and/or have easy physical access to the device.

This page is intentionally blank.

Appendix C: Subdevices

The HCC2 supports the addition and configuration of the subdevices in the table below.

For help in adding a subdevice or a child I/O device to your deployment configuration, see section 6.7, Adding Subdevices, page 57.

For help in mapping ISaGRAF variables to a configured subdevice, see section 15.7, Configuring ISaGRAF Variables for Unity Edge Integration, page 183.

For help in monitoring your subdevices, see section 7.4, Monitoring SubDevices, page 84.

To confirm if a subdevice has been added, view the Operate > Subdevices screen.

Catalog Number	Description
1794-AENT	1794-AENT Ethernet Flex Adapter
1794-AENTR	1794-AENTR FLEX Ethernet Flex Adapter Redundant
1794-IA16/A	1794-16 Point 120V AC Input
1794-IA8/A	1794-8 Point 120V AC Input
1794-IB10XOB6/A	1794-10 Input/ 6 Output 24V DC, Sink/Source
1794-IB16/A	1794-16 Point 24V DC Input, Sink
1794-IB16D/A	1794-16 Point 24V DC Diagnostic Input Module
1794-IB32/A	1794-32 Point 24V DC Input, Sink
1794-IB8/A	1794-8 Point 24V DC Input, Sink
1794-IE4XOE2/B	1794-4 Input/ 2 Output 24V DC Non-Isolated Analog
1794-IE8/B	1794-8 Channel 24V DC Non-Isolated Voltage/Analog Current Input
1794-IE8H/B	1794-8 Channel HART Analog Current Input
1794-IF2XOF2I/A	1794-10 Input/ 6 Output 24V DC, Sink/Source
1794-IF41/A	1794-4 Channel 24V DC Isolated Analog Input
1794-IF8IH/A	1794-8 Channel HART Analog Current Isolated Input
1794-IJ2/A	1794-2 Input Frequency Module
1794-IRT8	1794-8 Channel 24V DC RTD/Thermocouple Analog Input
1794-OA16/A	1794-16 Point 120V AC Output
1794-OB16D/A	1794-16 Point 24V DC Diagnostic Output Module
1794-OB16P/A	1794-16 Point 24V DC Protected Output, Source
1794-OB8EP/A	1794-16 Point 24V DC Electronically Fused Protected Output, Source
1794-OE4/B	1794-4 Channel 24V DC Non-Isolated Voltage/Analog Current Output
1794-OF41/A	1794-4 Channel 24V DC Isolated Analog Output, Source
1794-OF8IH/A	1794-8 Channel Isolated Analog HART Output
1794-OW8/A	1794-8 Point Relay Output, Sink/Source
5094-AEN2TR(XT)	5094XT Ethernet Adapter 16 Modules RJ45

5094-AENTR**(XT)**	5094 Ethernet Adapter 8 Modules RJ45
5094-IB16(XT)	Digital Input
5094-IB32(XT)	Digital Input
5094-IF8IH(XT)	Analog In HART
5094-IF8(XT)	Analog Input
5094-IY8/B(XT)	Universal Analog Input
5094-OB16(XT)	12 Point 24V DC
5094-OB32(XT)	Relay Output
5094-OB8(XT)	Relay Output
5094-OF8(XT)	Analog Output
5094-OW8I(XT)	Relay Output
1426-M8E	PM5000
PowerFlex 525 DataLinks	PowerFlex 525-EENET AC Drive with Configurable DataLinks
PowerFlex 525-E	PowerFlex 525-E via 20-COMM-E
PowerFlex 700H-E	PowerFlex 700H-E AC Drive via 20-COMM-E
PowerFlex 700S	PowerFlex 700S 2P-400V Phase 2 AC Drive via 20-COMM-E
PowerFlex 755 DataLinks	PowerFlex 755-ENETR AC Drive with Configurable DataLinks
PowerFlex 755	PowerFlex 755-ENETR AC Drive
PowerFlex 755T VHz DataLinks	PowerFlex 755T ControlMode VHz V1.0
PowerFlex 755T DataLinks	PowerFlex 755T Drive with Configurable DataLinks V4.7
PowerFlex 755TL	PowerFlex 755TL
PowerFlex 755TR DataLinks	PowerFlex 755TR Drive with Configurable DataLinks V2.3
PowerFlex 755TS	PowerFlex 755TS

Scan a QR for

Technical Support

Customer Care

sensiaglobal.com
1-866 7 SENSIA (+1-866-773-6742)
info@sensiaglobal.com

Add intelligent action to your oil & gas solutions

SENSIA