Manual
00809-0100-4581, Rev HB
March 2026

Emerson Plantweb Insight™ - Platform User Manual

EMERSON™

Table of Contents

1. Introduction

Definitions

PWI – Plantweb Insight™

System – Plantweb Insight Platform and Applications

Platform/Framework – The virtual machine/PC platform that the applications run on

VM – Virtual machine

Data Sources – WirelessHART® gateways, OPC-UA® servers, Modbus® Servers, AMS Device Manager Data Server, Fisher™ ValveLink™ Software, and other PWI systems

Asset – The physical asset being monitored by a Plantweb Insight application (steam trap, pressure relief valve, control valve, pump, heat exchanger, power module, wirelessHART network, etc).

Using this manual

This document is intended for network or system administrators and will provide details on how to install and configure the Plantweb Insight platform. It is assumed that individuals using this manual have a basic understanding of networking and virtual machines. For more details and configuration information on specific Plantweb Insight applications, refer to the appropriate application reference manuals.
It is recommended administrators complete all steps in the order described. An overview of these steps is described below:

Installation and Commissioning Procedure

1. Ensure the host system meets minimum PWI system requirements
2. Determine the preferred PWI deployment mode and network architecture
3. Install the PWI virtual machine onto the hypervisor or as an edge solution
4. Launch PWI web interface from a supported web browser
5. Configure network settings
6. Rebuild default certificate with new PWI IP/FQDN or upload custom SSL certificate if secure connections are required to data sources and services
7. Configure data sources and services
8. Create user accounts and user access permissions
9. Install application(s)
10. Install license(s)
11. Configure application(s) for use

For direct PWI technical support, please submit a request through the link below or scan QR code PWI Technical Support Request Link

About Plantweb Insight

For cybersecurity information, please refer to the Emerson Plantweb Insight Platform – Product Security and Hardening Guide

For latest software version release details, refer to the Plantweb Insight Platform Release Notes

PWI is provided as a fully packaged virtual machine. Users will download a complete virtual machine image to install in a user-provided virtualization software or hypervisor. The PWI virtual machine or "platform" is required to host any of the PWI applications (i.e. Plantweb Insight Steam Trap Monitoring application). Multiple PWI applications can operate on a single PWI platform. PWI can be installed on a network server or PC/laptop with sufficient resources. Either installation has the same requirements and installation steps. PWI is also provided as a bare metal industrial PC solution. For more information on the PWI industrial PC solution, contact your local Emerson representative.

The PWI platform contains a web server accessible by any supported web client with network access.

In the case of PWI, Emerson maintains full responsibility for the entire system (applications and platform). Each software release brings in the latest security patches for all components of the system. This simplifies the customer experience while maintaining a high level of security. Software updates are easily applied through the web interface of the system. The user only interacts with the system via the web interface. Users, malicious or legitimate, cannot install software on the system, reducing the need for Antivirus software. Virtual machine snapshots can be periodically captured by end users and restored if a problem is suspected.

Software Lifecycle Management

Emerson manages the entire PWI system by providing regular platform and application updates that the user must install through the web interface. Aspects of the operating system are abstracted from the user. There is no need for users to manage any of the individual components within the virtual machine, as Emerson provides all necessary updates through upgrade bundles. Upgrade bundles are easily installed through the PWI web interface. Emerson also provides quarterly OS patches that allow users to keep the underlying OS up to date. The latest OS patches are always rolled into the PWI platform updates. All these updates and patches are made available to users through MyEmerson's Authorized Software Hub.

Database

PWI uses multiple databases that vary in size depending on the application(s) being used. All PWI databases are managed and do not require direct management by users. Users can access the database by downloading a diagnostic backup from their PWI system. The size is limited to the disk size of the PWI virtual machine out-of-the-box. Users are free to increase the disk size as their deployment gets bigger. Applications can grow as big as 35 GB and still be restorable into PWI.

Antivirus

Third-party antivirus software is inherently unnecessary based on the design of PWI. PWI is designed with a strict firewall system that only requires access to a few ports (web interface and communication to data sources) for basic functionality. Users can enable/disable any additional ports and whitelist certain IP addresses for other services.

Because PWI is a purpose-built operating system designed and maintained by Emerson, there is a high possibility that a user would unintentionally create more issues within their PWI system by installing third-party antivirus software.

However, Emerson understands that some users' IT/cybersecurity may still insist on antivirus software, so we have implemented an antivirus solution for PWI in version 3.3.1 and later. This is a licensed feature that allows users to perform and schedule scans as needed. The antivirus solution in PWI quarantines any potentially compromised components without inadvertently crashing or rendering PWI unusable to a user.

For more information on PWI's antivirus solution, refer to the Antivirus section.

System Recovery / Disaster Recovery / Backup-Restore

The backup/restore functionality within PWI was developed for migrating from one PWI VM to another. The backup/restore functionality is not necessarily intended as a disaster recovery (DR) solution. Emerson recommends using VM snapshots instead for DR. VM snapshots can be managed on a daily/periodic basis, and several iterations of PWI can be retained over a period of time, per your company's DR strategy. VM snapshots and VM Host are subject to the standard backup policies laid out by the user's IT department.

See Appendix A for an example of a backup strategy for a high-risk application.

2. System Requirements

Host Operating System

Virtualization software/hypervisor

- VMware® Virtual Hardware Version 18 or higher (requirements can be found online)
- Microsoft Hyper-V® Configuration Version 8.0 or higher

Note

When using a PC as the host machine for Plantweb Insight (PWI), consider the following settings:

- Set up PC power profile to ensure that the PC does not enter Sleep mode.
- Enable hyper threads in BIOS

Hardware Requirements

Minimum:

- Processors: 8 dedicated cores
- Memory: 16 GB RAM
- Hard drive: 512 GB free space

Application Access

Web Browsers (recent versions supported)

- Google Chrome™
- Microsoft Edge®

Firewall Rules

Firewall ports only need to be enabled for PWI when the corresponding feature or protocol is used. If a feature or protocol is not required, users do not need to open the associated port. Refer to the Protocols and Ports section for more information.

Default Port	Protocol	Traffic Direction	Server	Client	Notes
TCP 80	HTTP, HTTP redirect to HTTPS	Bidirectional	Plantweb Insight	Web Browser	Communication between client and PWI system

TCP 443	HTTPS	Bidirectional	Plantweb Insight	Web Browser/ AMS optics API	Communication between client and PWI system
TCP 443	HTTPS	Bidirectional	Wireless Gateways	Plantweb Insight	Initially, used to establish secure connections with gateways
TCP 4840	OPC-UA	Bidirectional	Historian or similar OPC-UA server	Plantweb Insight	Port number is dependent on port configured in OPC-UA server
TCP 4848	OPC-UA Secure	Bidirectional Secure	Historian or similar OPC-UA server	Plantweb Insight	Port number is dependent on port configured in OPC-UA server
TCP 4880	OPC-UA	Bidirectional	Plantweb Insight	Historian or similar OPC-UA client	
TCP 4884	OPC-UA Secure	Bidirectional Secure	Plantweb Insight	Historian or similar OPC-UA client	
TCP 5094	Wireless (HART-IP)	Bidirectional	Wireless Gateways	Plantweb Insight	
TCP 5095	Wireless (Secure HART-IP)	Bidirectional	Wireless Gateways	Plantweb Insight	
TCP 6094	Wireless (HART-IP)	Bidirectional	Dual Network Wireless Gateways	Plantweb Insight	This port must be enabled when PWI is connected to a

					Dual HART Gateway (unsecure)
TCP 6095	Wireless (Secure HART-IP)	Bidirectional	Dual Network Wireless Gateways	Plantweb Insight	This port must be enabled when PWI is connected to a Dual HART Gateway (secure)
UDP 514	Syslog Service	Bidirectional	Wireless Gateways	Plantweb Insight	
TCP 6514	Syslog Service Secure	Bidirectional Secure	Wireless Gateways	Plantweb Insight	
TCP 502	Modbus	Bidirectional	Plantweb Insight	Historian or similar Modbus clients	
TCP 1502	Modbus Secure	Bidirectional secure	Plantweb Insight	Historian or similar Modbus clients	
TCP 636	LDAP	Bidirectional	Plantweb Insight	LDAP Server	TCP 636 is used for Directory, Replication, User and Computer Authentication, Group Policy, Trusts
TCP 8883	MQTT	Bidirectional	Plantweb Insight On-Prem Connector	Plantweb Insight On-Prem App Only	

Other Requirements

Network Requirements

A DHCP server is required to assign a valid Internet protocol (IP) address. If a DHCP server is not available, a low-privileged console command can be used to assign a static IP address prior to web interface access. Refer to the Installation section for details.

Gateway Compatibility

Plantweb Insight is compatible with Emerson WirelessHART 1410/1420 Gateways on firmware version 4.7.68 or higher. Plantweb Insight may experience calculation response issues on certain applications when Gateway firmware is not up to date. These may especially affect the Steam Trap, Pump, Heat Exchanger, Air Cooled Heat Exchanger, and Pressure Relief Valve applications.

Device Compatibility

Emerson WirelessHART devices must be in Emerson Optimized burst configuration. If devices are not set to this, change using a device configuration tool.

Devices without this capability must be in either of the two configuration modes to be compatible with Plantweb Insight:

- command 9 and command 48
- command 3 and command 48

Non-Emerson measurement devices may be compatible if device data can be sent to PWI via an OPC-UA server, Modbus TCP server, or an Emerson AMS DataServer.

3. PWI Deployment Modes

PWI can connect to various sensors and data sources to collect measurement data related to a particular asset. With this data collected, PWI applications run calculations and provide visualizations and insight into each asset's health. PWI connects to measurement variables through various data sources like WirelessHART gateways, OPC-UA servers, Modbus servers, and MQTT.

PWI data sources are deployed throughout user networks and are normally available within the same network as PWI. However, scenarios may occur where data sources are in one network while visualization and access to PWI applications is intended to be in another network. Network access restrictions and network topology may require more complex

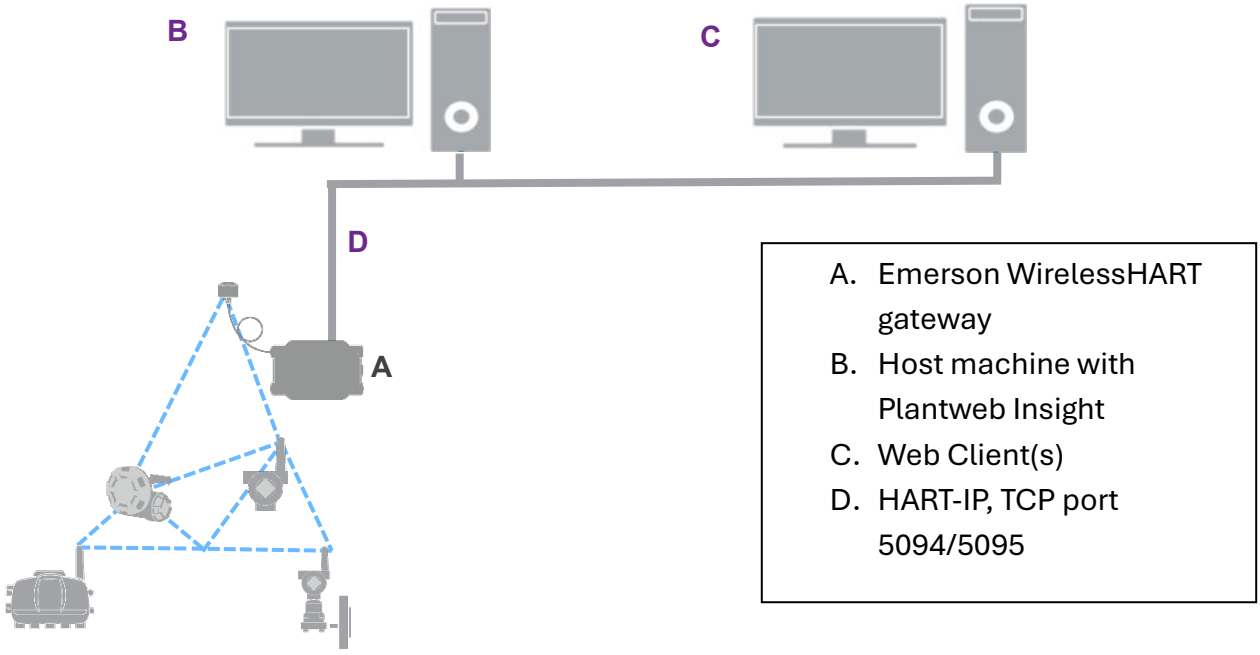
PWI solutions. For this reason, PWI can operate in different “modes” to achieve a desired network architecture.

NOTE: Changing a PWI system mode cannot be rolled back. Once the PWI mode has been changed, it should remain in that mode permanently.

Standard Deployment

PWI **Standard** systems are deployed on premises and communicate directly with data sources like WirelessHART Gateways, OPC & Modbus servers, or MQTT servers and host PWI applications that provide calculated insights. These systems are usually hosted on intranets where there is no internet connectivity permitted.

Below is an example of a simple PWI standard architecture:



On-Premises Connectivity Solution

PWI **On-Premises Connectivity Solution** systems enable users connect to data sources at different levels of their network and aggregate data to a single PWI system.

A common scenario is where WirelessHART gateways or AMS data sources are located at network level 2/2.5 and are only accessible from within this network, but a user may want visualization (web client) access to PWI at network level 3 or above. In this scenario, two or more PWI instances can be utilized to enable MQTT data bridging across networks. A PWI On-Premises Connectivity Solution is made up of at least two PWI systems:

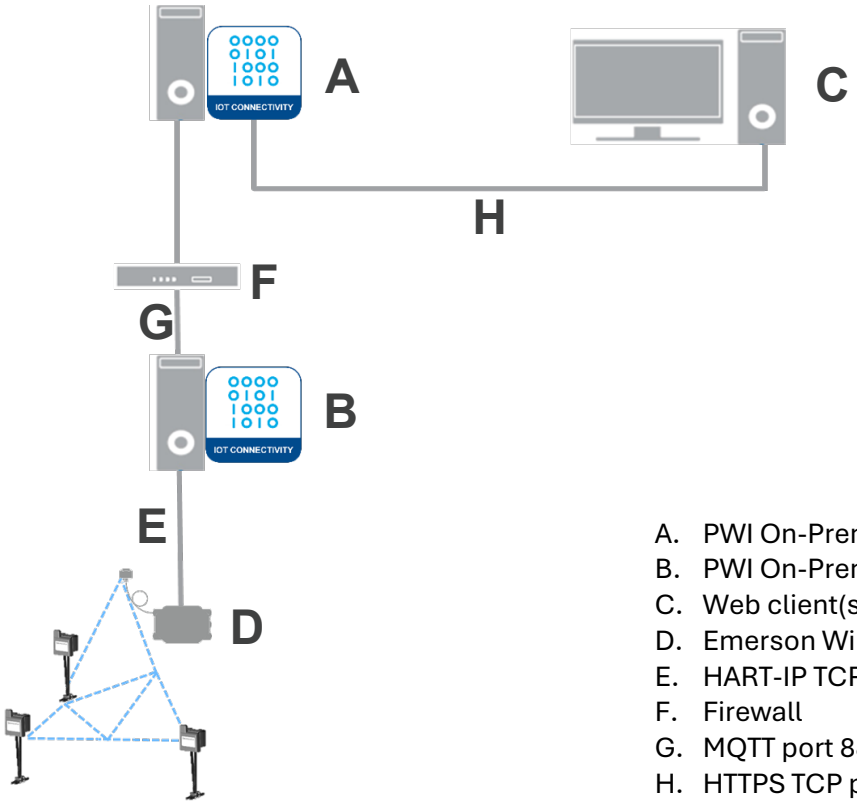
- **PWI On-Prem Connector** systems are hosted at lower network levels where data sources are accessible
- **PWI On-Prem App Only** systems are hosted at higher level network levels where data is aggregated, where applications are installed to perform calculations and provide visualization to users

In the previous scenario, the PWI instance at L2 operates as a PWI **On-Prem Connector** which will collect data directly from data sources, while another PWI instance at L3 or above operates as a PWI **On-Prem App Only** system which will collect data from the On-Prem Connector system and host PWI applications for calculation and visualization. With new features like location-based access control, users can allow access to specific locations for specific users.

Implementation details:

- Data bridging requires at least two PWI systems where one acts as a sender and the other as the receiver
- An On-Prem App Only system can connect and receive data from more than one On-Prem Connector system
- A PWI Standard system can change its mode to operate either as On-Prem Connector or On-Prem App Only

Below is an example of a simple PWI On-Premises Connectivity Solution architecture:



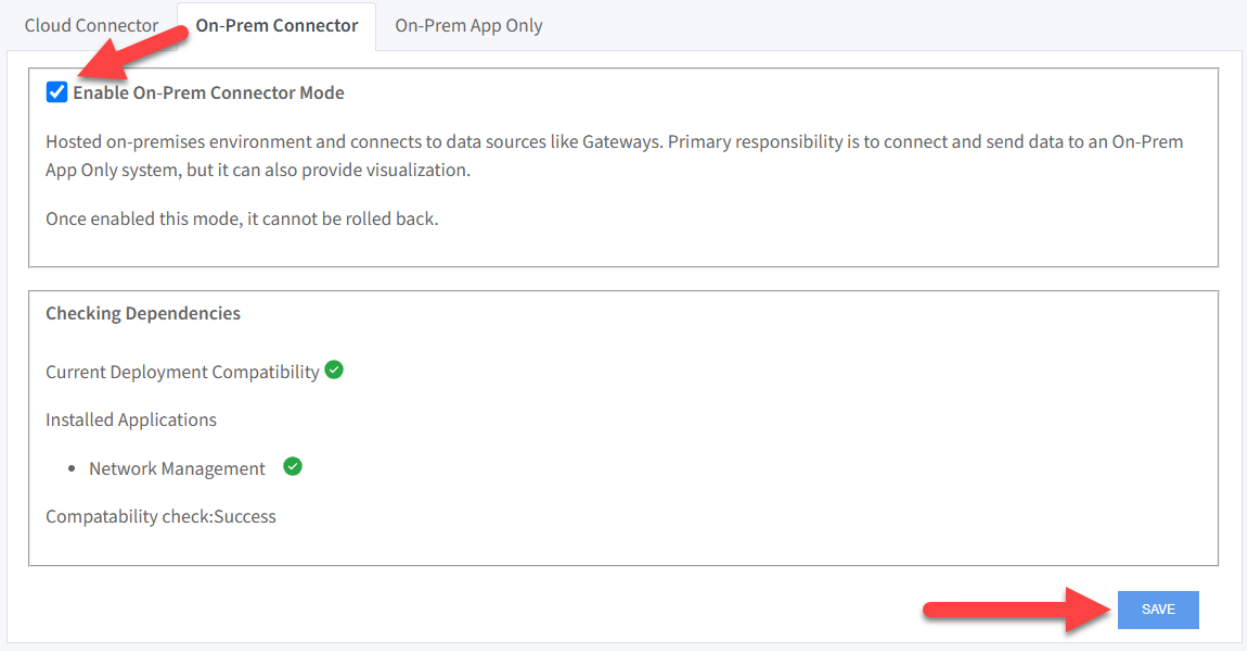
A. PWI On-Prem App Only
B. PWI On-Prem Connector
C. Web client(s)
D. Emerson WirelessHART gateway
E. HART-IP TCP port 5094, 5095
F. Firewall
G. MQTT port 8883
H. HTTPS TCP port 80, 443

PWI On-Prem Connector

- The On-Prem Connector should be installed where data sources are accessible
- The On-Prem Connector should be made aware of the receiving system to enable necessary outbound rules and proper transfer of data
- All data received by the On-Prem Connector is converted to MQTT and forwarded to the receiving system (On-Prem App Only)

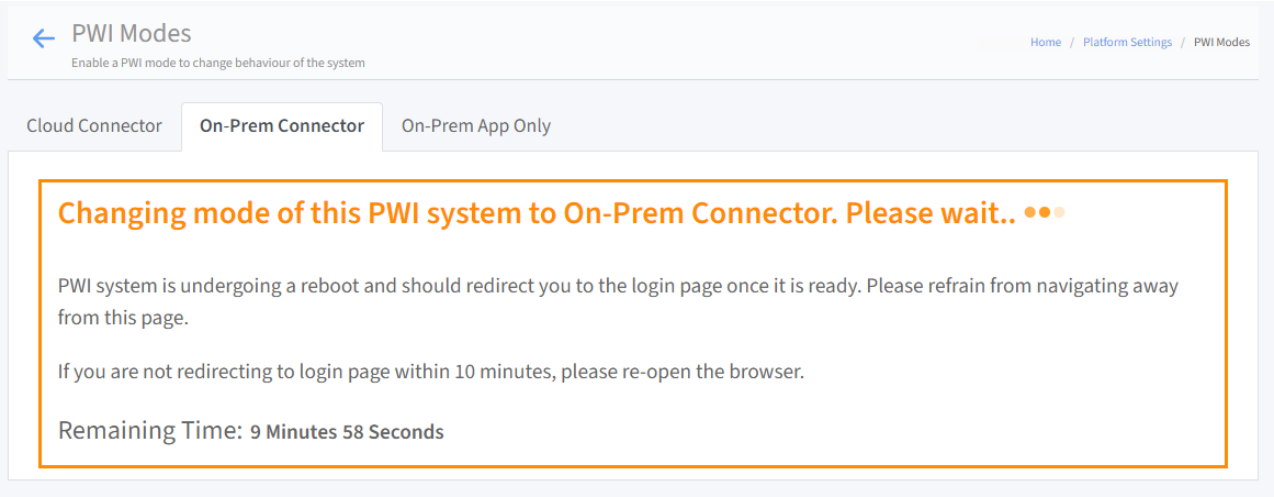
Step 1: Enable the On-Prem Connector Mode

The On-Prem Connector mode can be enabled by navigating from the PWI Home screen to (Settings) > ***Platform Settings > PWI Modes > On-Prem Connector.*** Upon enabling this mode, the PWI system will enable a new menu for “On-Prem Connectivity Settings”.

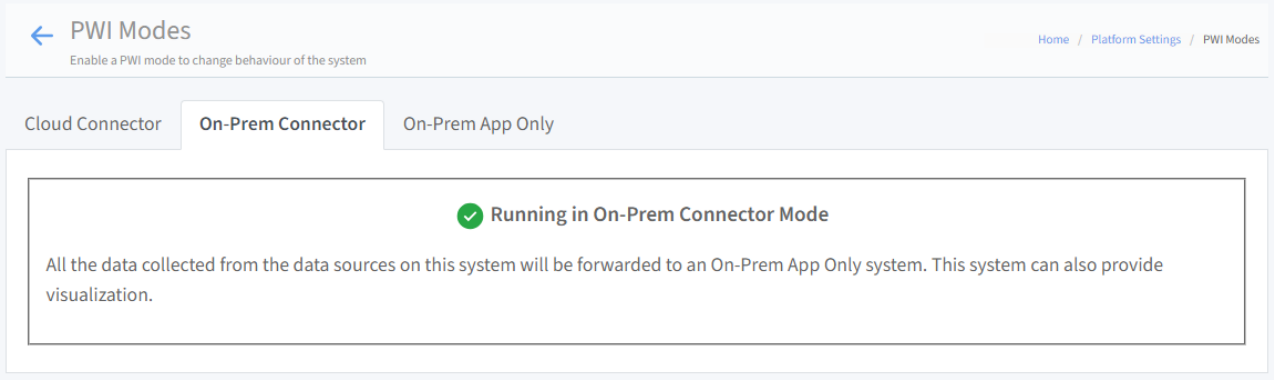


NOTE: All existing data sources will continue to send data to the On-Prem Connector system

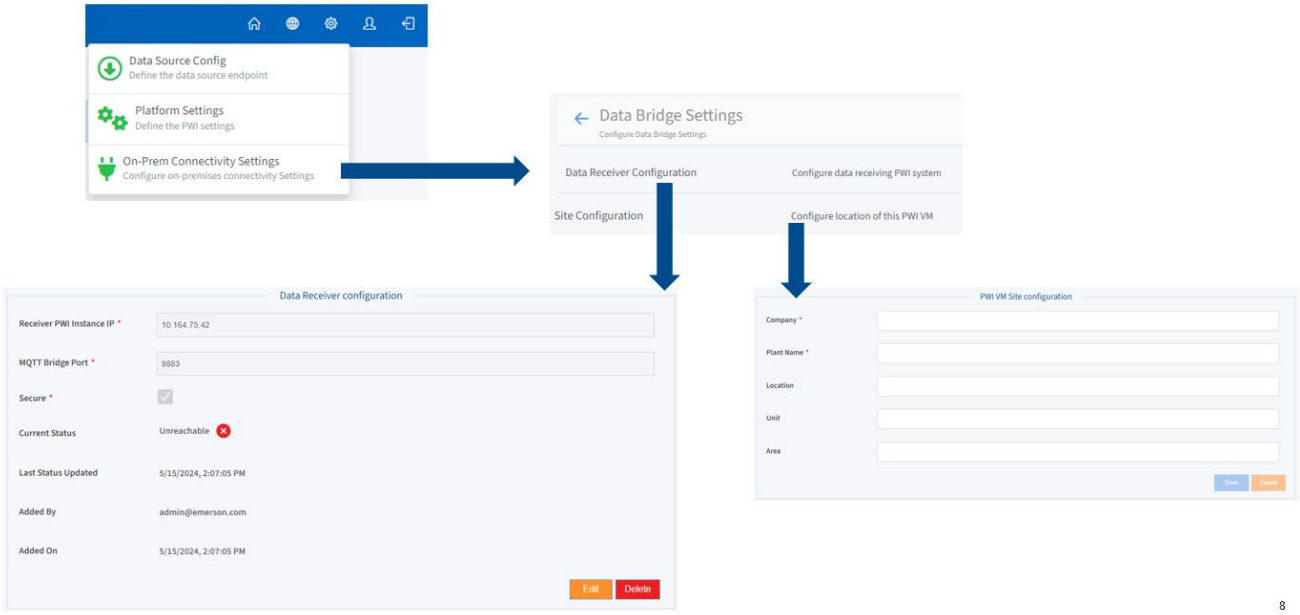
Step 2: Save the new mode



Step 3: Logout and login for new mode to take effect



Once the mode is enabled, new menus and settings become available to establish connectivity with an On-Prem App Only system.



Site Configuration

Site configuration will help convey the physical location of this On-Prem Connector system. All On-Prem Connector systems' location details are synced to the On-Prem App Only system, and users can see a glance at all the connected systems and their respective locations on the On-Prem App Only system.

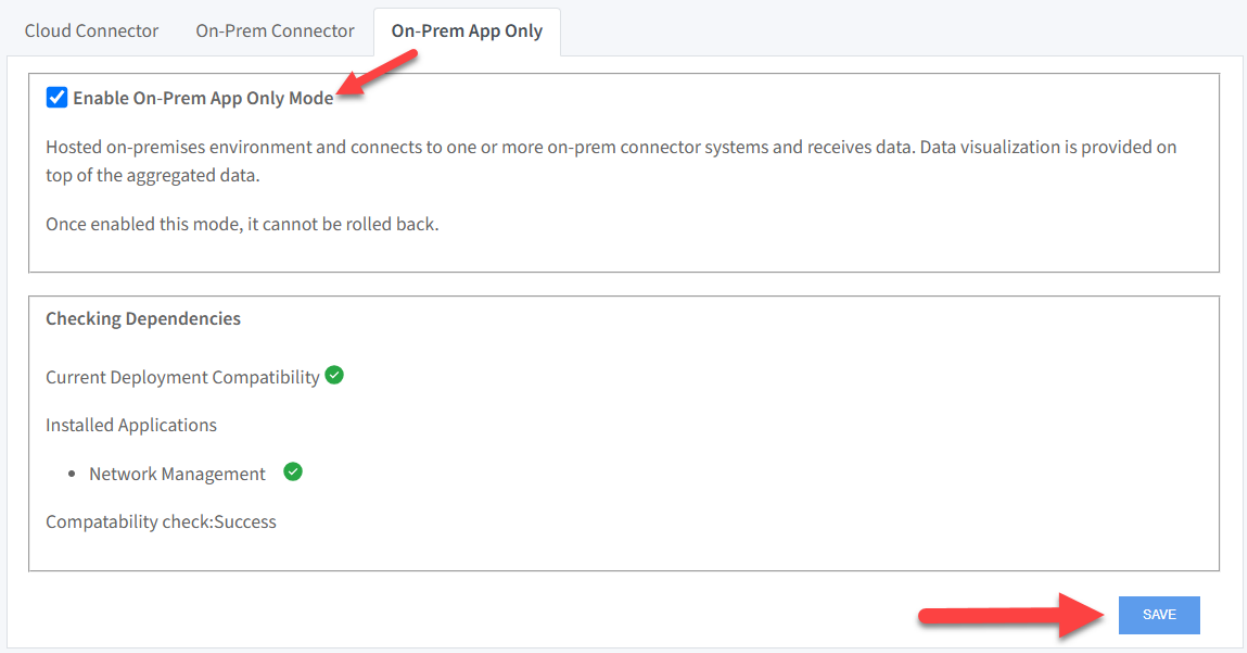
PWI On-Prem App Only

- The On-Prem App Only system should be installed where users will have access to PWI app visualizations and calculated outputs
- Applications are intended to be installed on the On-Prem App only system to have access to the aggregated data sources

- The On-Prem Connector must be registered with the On-Prem App Only system to enable required inbound data settings
- Applications in an On-Prem app Only system receive data via MQTT from the On-Prem Connector system in the same manner that they perceive data in a PWI Standard system
- Applications do not require any changes in configuration to be installed on an On-Prem App Only system
  NOTE: Network Management, Power Module, and Non-Intrusive Corrosion applications require downstream data handling to be performed on the On-Prem Connector. For this reason, these applications require a copy to be installed on both the On-Prem Connector and On-Prem App Only systems. The app installation on the On-Prem Connector system does not require a license to perform downstream data handling.

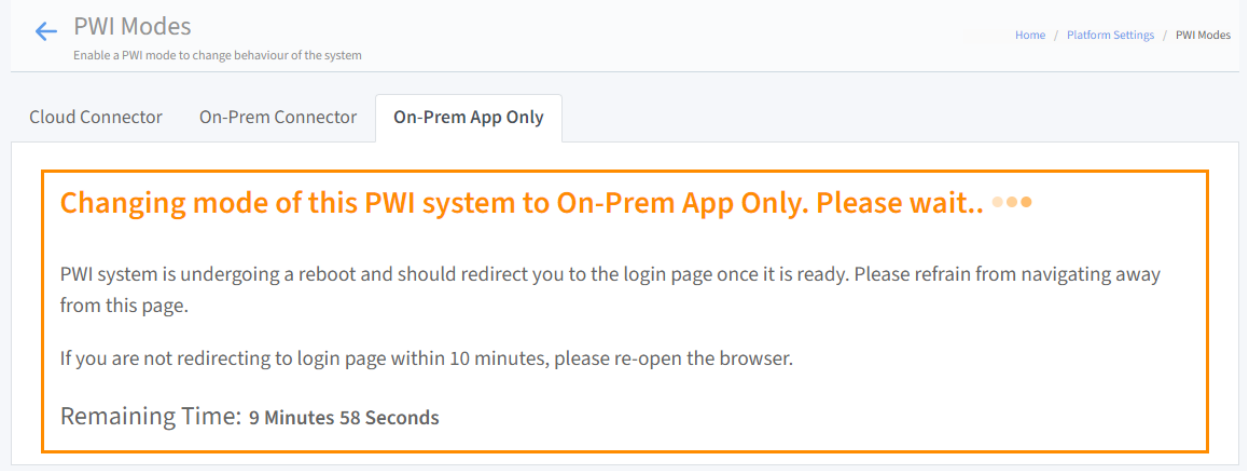
Step 1: Enable the On-Prem App Only mode

The On-Prem App Only mode can be enabled by navigating from the PWI Home screen to (Settings) > ***Platform Settings*** > ***PWI Modes*** > ***On-Prem App Only.*** Upon enabling this mode, the PWI system will enable a new menu for "Data Bridge Settings".

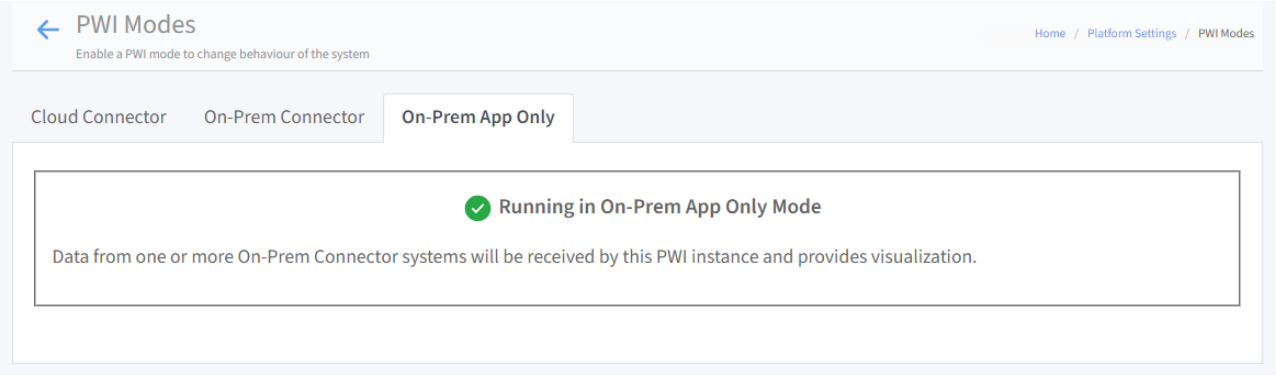


NOTE: Ensure no data sources are configured before converting to an On-Prem App Only system

Step 2: Save the new mode

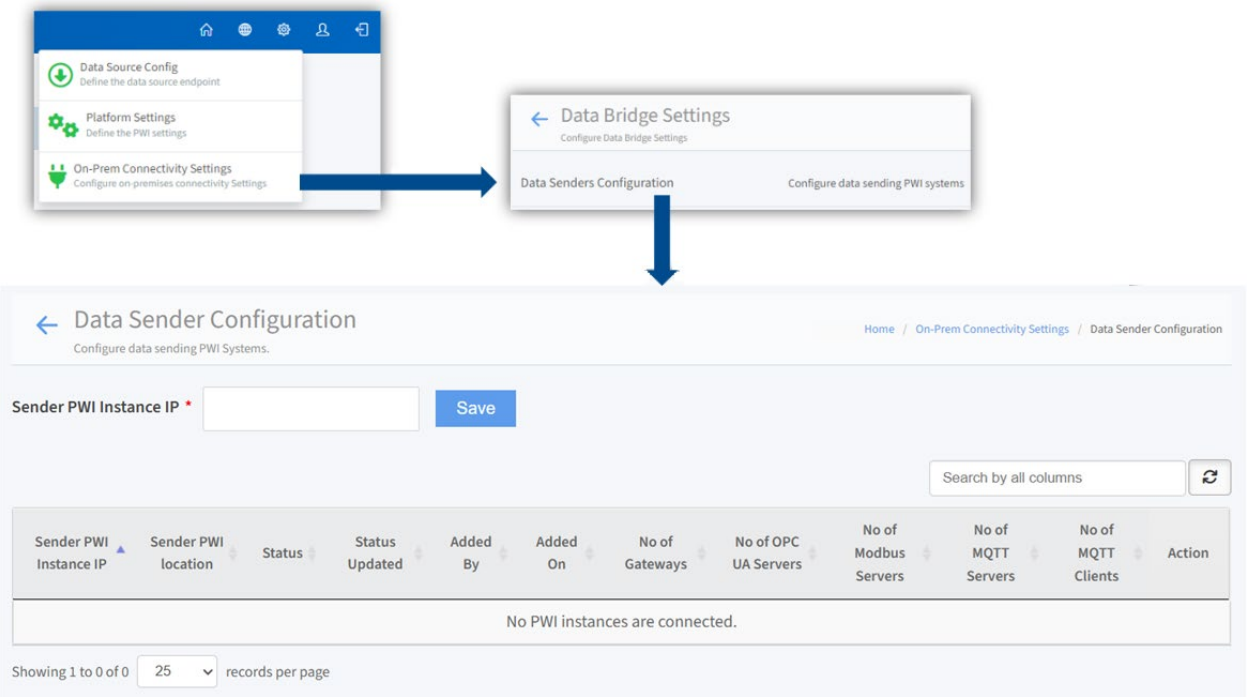


Step 3: Logout and login for new mode to take effect



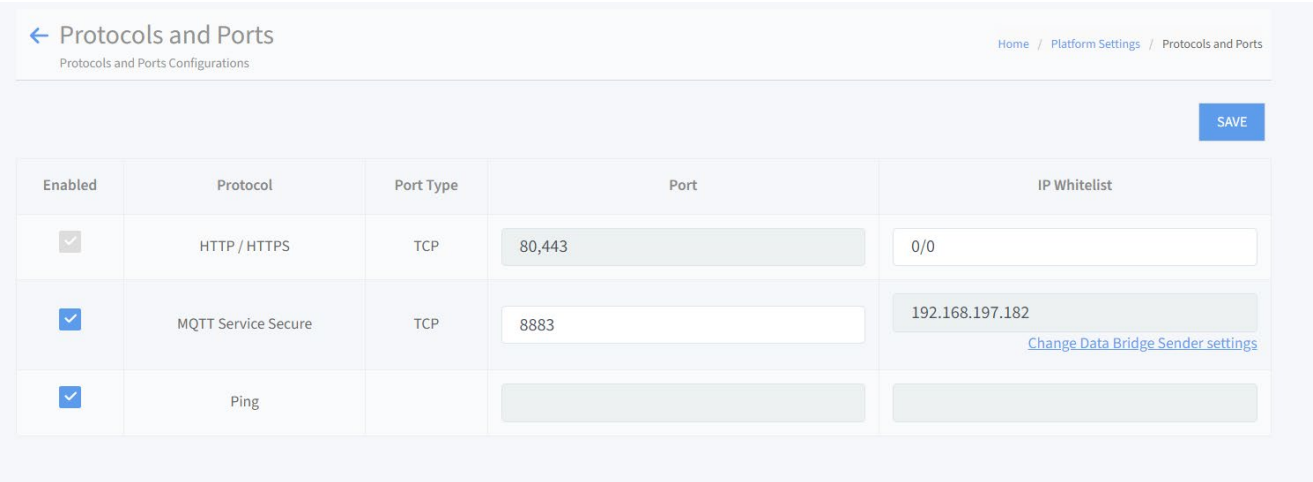
Data Sender Configuration

IP addresses of PWI On-Prem Connector systems from which data is expected to be received should be configured under this list. Once the IP address is configured, the On-Prem App Only system will try to detect location and connectivity details of the corresponding On-Prem Connector system(s).



Protocols and Ports

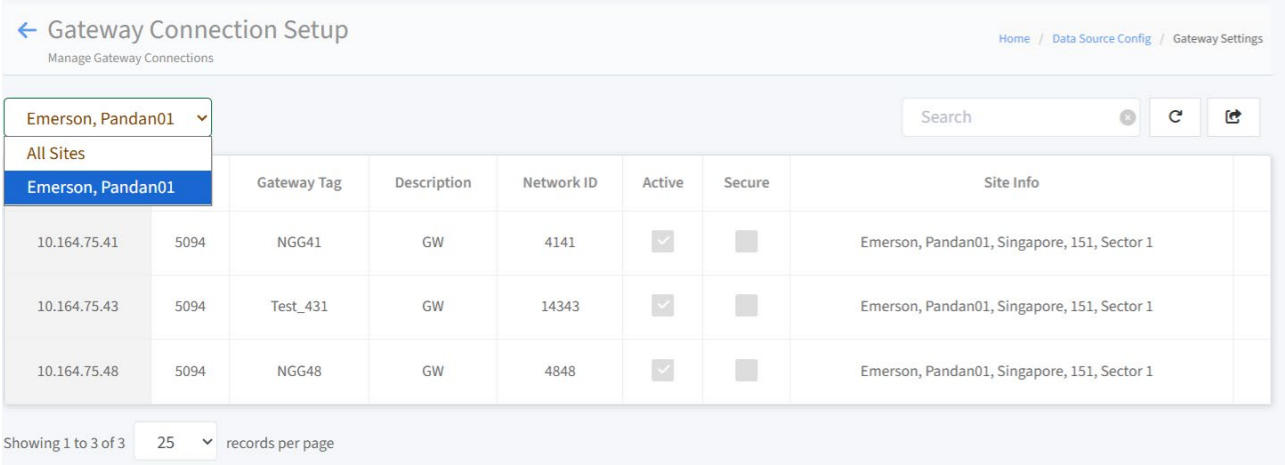
IP addresses added to Data Sender Configuration page are also displayed in the ***Protocols and Ports*** page. The default port for MQTT Service Secure is 8883 and an admin can change these services to run on different ports by updating the value of port. In the case a user doesn't need this service, they can completely disable it by unchecking the “Enabled” button in the left column.



Gateway Connections

The Gateway Connection Setup page in an On-Prem App Only system is a read only page. It lists all the gateways configured to On-Prem Connector systems that are sending data to

the On-Prem App Only system. Each gateway is tagged with site information of the On-Prem Connector system to understand the physical location of each gateway.



Cloud Connectivity Solution

The PWI **Cloud Connectivity Solution** enables users to aggregate and connect multiple on-premises OT data sources to a PWI instance hosted in Emerson's cloud environment. Rather than connecting field and device protocols directly to cloud, the PWI Cloud Connectivity Solution aggregates these on-prem data sources and converts them into a single MQTT output for connection to the Azure IoT Hub.

A common scenario for this solution is when multiple WirelessHART gateways or other data sources are geographically isolated across multiple locations, but a user would like to monitor a single PWI instance that covers all locations. In this scenario, two or more PWI instances can be utilized to enable MQTT data bridging across networks. A PWI Cloud Connectivity Solution is made up of at least two PWI systems:

- **PWI Cloud Connector** systems are hosted on-premises and aggregate data from a specific location
- **PWI Cloud App Only** systems are hosted in Emerson's Cloud where data is aggregated, where applications are installed to perform calculations and provide visualization to users

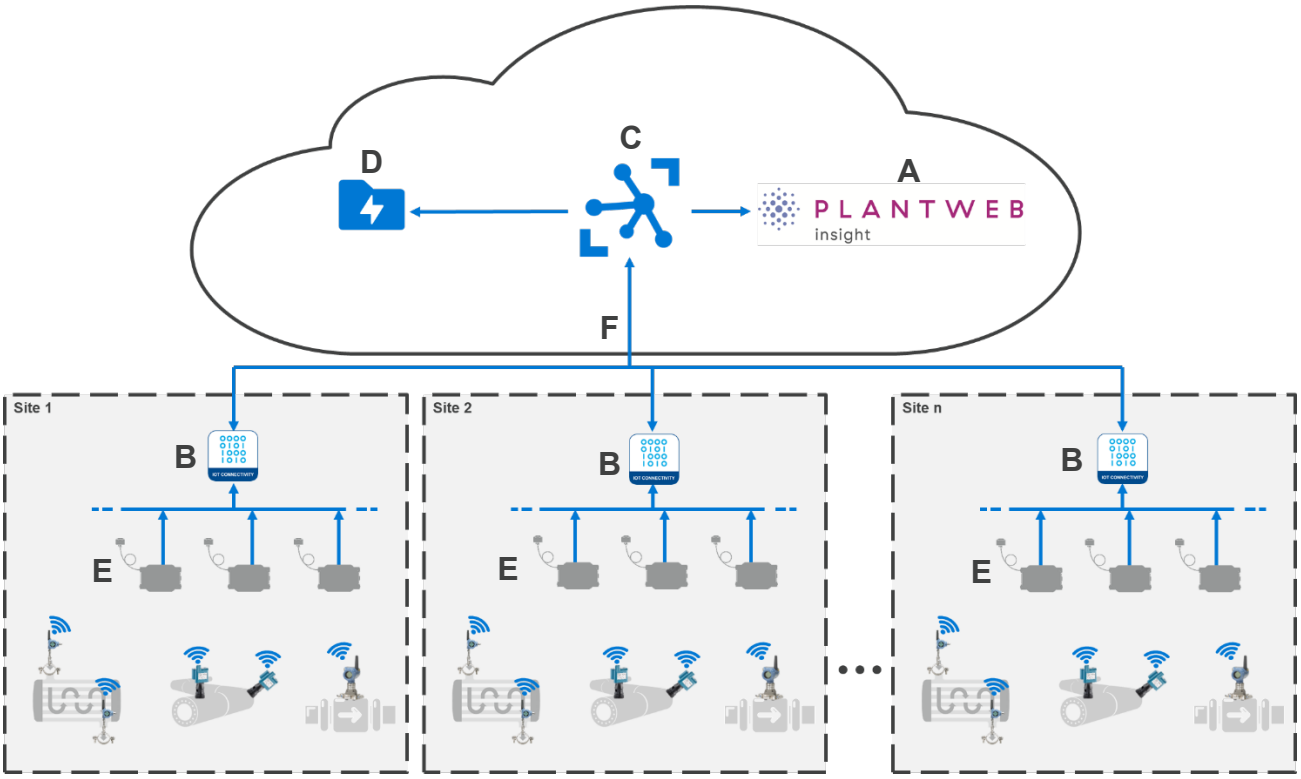
In the previous scenario, the PWI instance(s) on-premises operates as a PWI **Cloud Connector** which collects data directly from data sources and sends aggregated data to the Azure IoT Hub via MQTT. Another PWI instance, hosted in Emerson's Cloud, operates as a PWI **Cloud App Only** system which is designed to collect data from the Azure IoT Hub and host PWI applications for calculation and visualization. With new features like

location-based access control, users can allow access to specific locations for specific users.

Implementation details:

- An Azure IoT Hub is set up for each user and multiple IoT devices are created based on the number of PWI Cloud Connector systems and data sources associated with each
- Data bridging requires at least one Cloud Connector system and an Azure IoT Hub
- MQTT data transmission from site to Azure IoT Hub is typically facilitated by cellular backhaul or direct network connectivity
- A Cloud App Only system can connect and receive data from more than one Cloud Connector system
- A PWI Standard system can change its mode to operate as a Cloud Connector
- The PWI Cloud App Only variant is a unique build that must be deployed by Emerson experts

Below is an example of a simple PWI Cloud Connectivity Solution architecture:



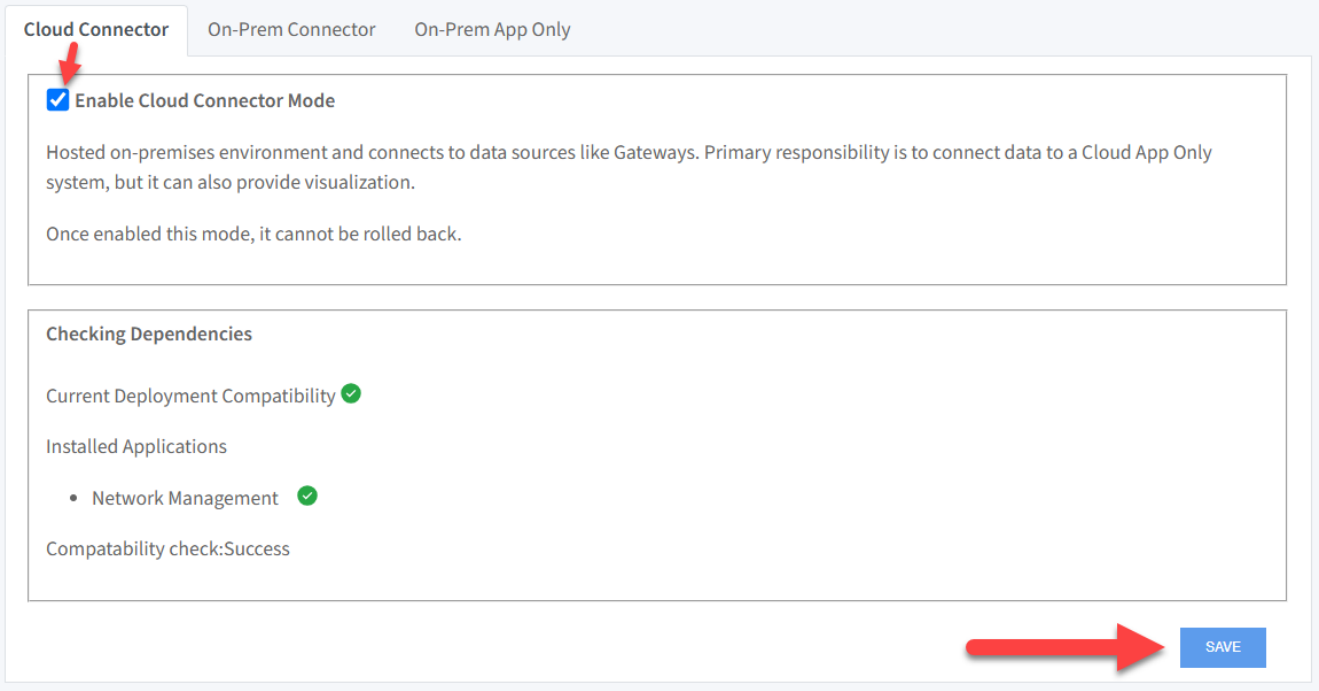
A. PWI Cloud App Only
B. PWI Cloud Connector
C. Azure IoT Hub
D. Data Lake
E. Emerson WirelessHART gateways
F. MQTT port 8883

PWI Cloud Connector

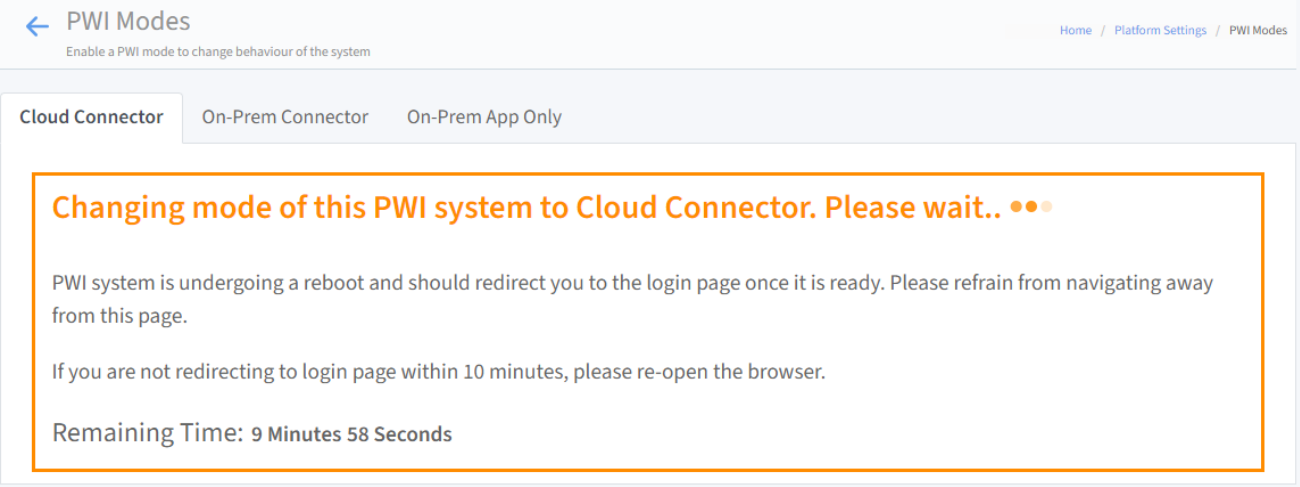
- The Cloud Connector should be installed where data sources are accessible
- All data received by the Cloud Connector is converted to MQTT and relayed to the Azure IoT Hub

Step 1: Enable the Cloud Connector Mode

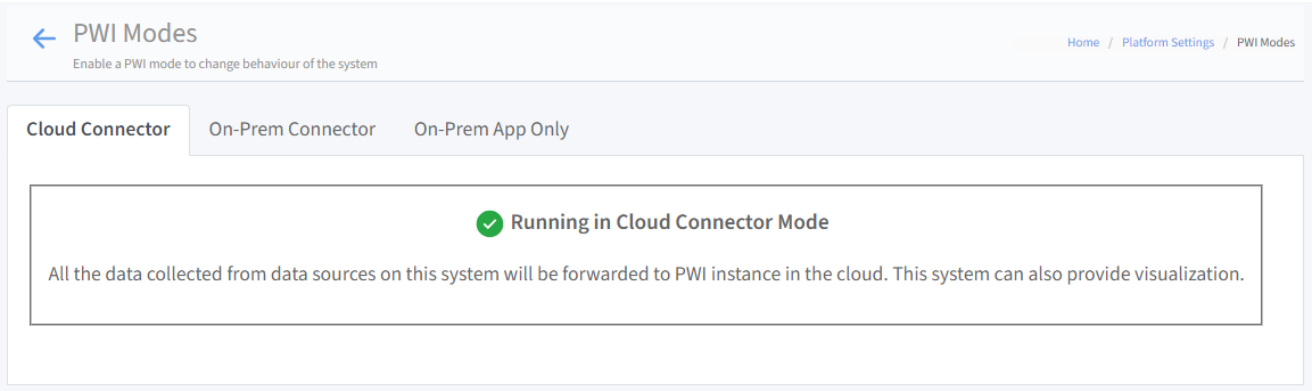
The Cloud Connector mode can be enabled by navigating from the PWI Home screen to (Settings) > ***Platform Settings*** > ***PWI Modes*** > ***Cloud Connector***



Step 2: Save the new mode

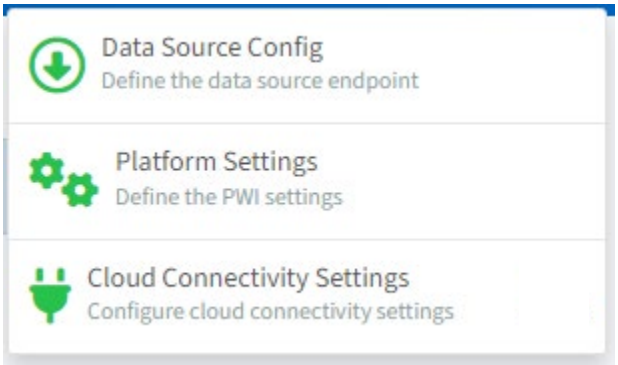


Step 3: Logout and login for new mode to take effect

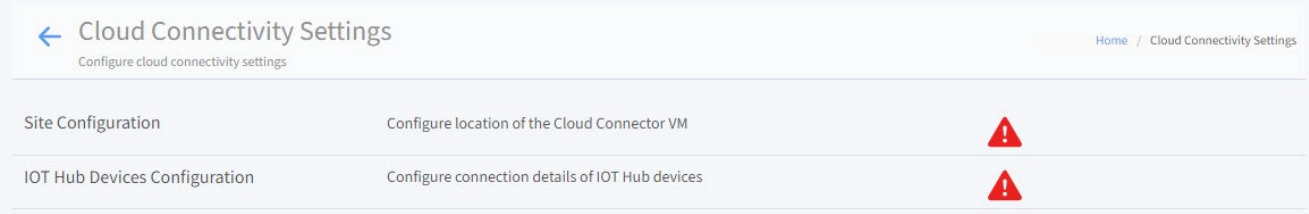


Cloud Connector Configuration

Once the mode is enabled, a new “Cloud Connectivity Settings” menu will be available under the Settings menu. These settings are required to properly send data to Azure resources.



Click the Cloud Connectivity Settings, and the system will display related configuration menus. A warning triangle icon next to "Site Configuration" or “IOT Hub Devices Configuration” indicates that configuration items aremissing.



To avoid any issues, the following steps are recommended for IOT device configuration:

1. Configure Site by navigating from the Home screen to (Settings) ***> Cloud Connectivity Settings > Site Configuration***
2. Configure Gateway data sources by navigating from Home screen to (Settings) > ***Data Source Config > Gateway Settings***
3. Ensure all gateways or other data sources have reached an active state (Refer to 'Active' column in Gateway Settings page, the box should be checked)
4. Navigate to IOT Devices configuration page by navigating from the Home screen to (Settings) > ***Cloud Connectivity Settings> IOT Hub Devices Configuration***
   - Download required IOT Devices list by clicking button "Download IOT Device IDs"
   - This will download a "data-source-to-device-mapping.csv” file
   - This file contains all expected gateway specific and generic device details.
   - The column "iot_device_available" indicates the existence of the IOT Device configuration in PWI
   - For any missing IOT device configurations, create an IOT device on IOT Hub as specified below and add the connection string in the screen

IoT Hub Devices Configuration

An IOT Hub device is a secured connectivity mechanism used between PWI on premises and PWI in the cloud. Every IOT device has a unique connection string.

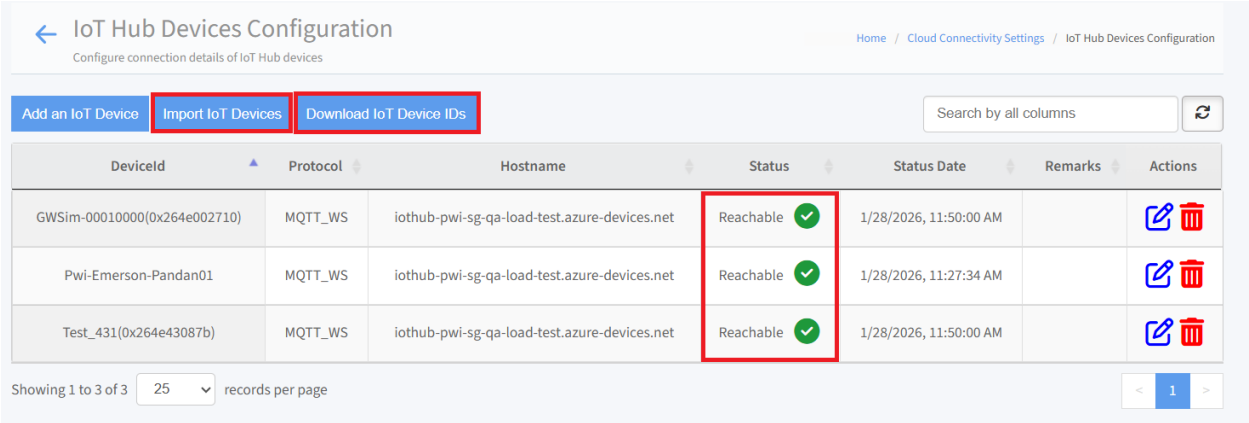
One IOT Hub device is created for every data source from a Cloud Connector system. All the telemetry data of the data source and its corresponding devices are sent through the dedicated Azure IOT Hub device.

In addition to the telemetry data, PWI also sends some processed and configuration data to the cloud. For this reason, one generic IOT Hub device for every Cloud Connector instance is required.

The following steps are required to complete the configuration of IOT hub devices:

- Configure required WirelessHART Gateways from settings menu > ***Data Source Config > Gateway Settings***
- Ensure that the gateways are in an active state
- Download required IOT Hub Devices list from ***Cloud Connectivity Settings > IOT Hub Devices Configuration***
- Share with Emerson <**plantwebinsightsupport@emerson.com**> to create the IOT Hub Devices
- Receive IOT Hub Device connection details from Emerson in a csv file
- Import the file into the device configuration screen ***Cloud Connectivity Settings > IOT Hub Devices Configuration > Import IOT Devices***

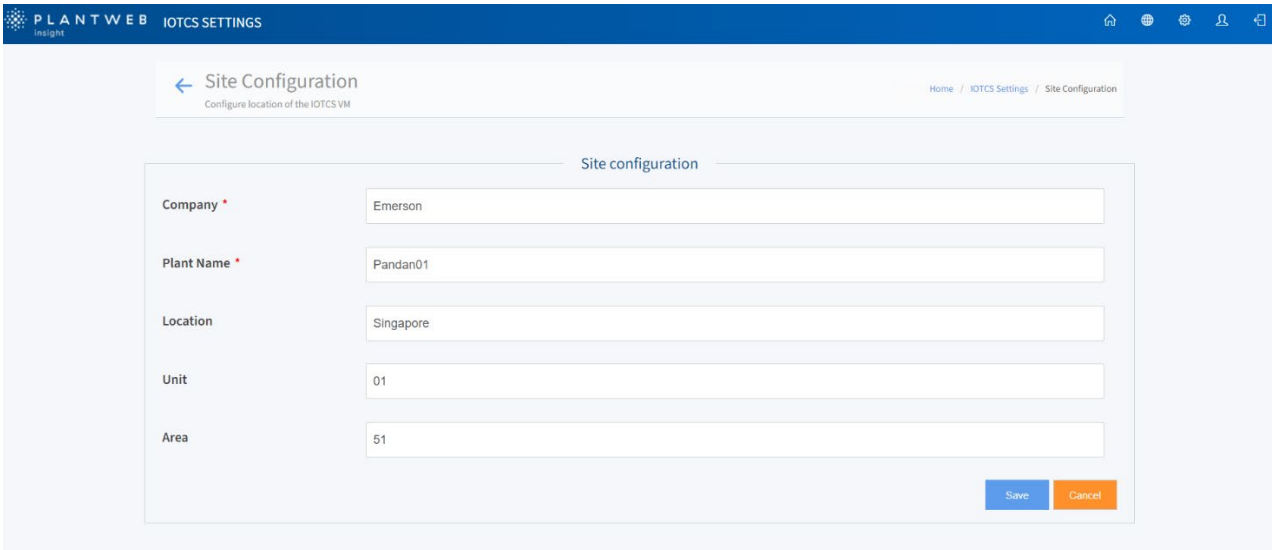
Ensure all the imported IOT devices are reachable
In order to verify whether required IOT Devices configured, Download IOT Device IDs file again and check the **iot_device_available** column for its availability
and **comments** column for more information.



Site Configuration

A Cloud Connector system is identified based on its site configuration when more than one Cloud Connector system is connected to a PWI Cloud App Only system. A site configuration should be unique among all a user's Cloud Connector systems.

Company and Plant Name are mandatory fields, and the combination of these two must be unique among all connected systems.

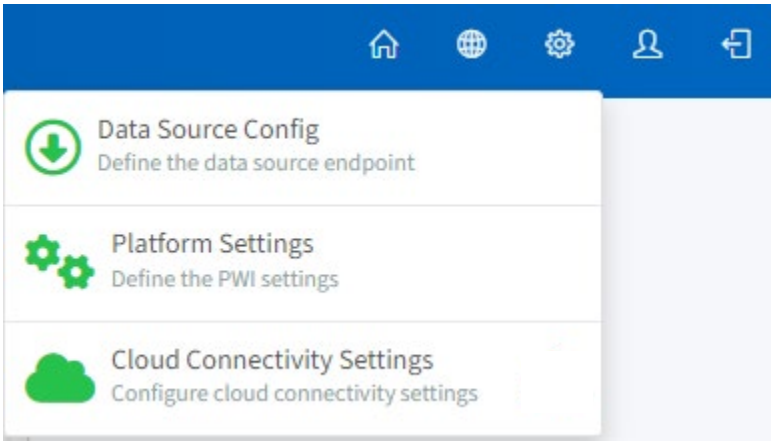


PWI Cloud App Only

- An Emerson Azure-hosted PWI system with the ability to connect to multiple Cloud Connector systems through a single Azure IoT Hub
- PWI Cloud App Only systems are a unique build only deployed by Emerson experts

Cloud Connectivity Settings

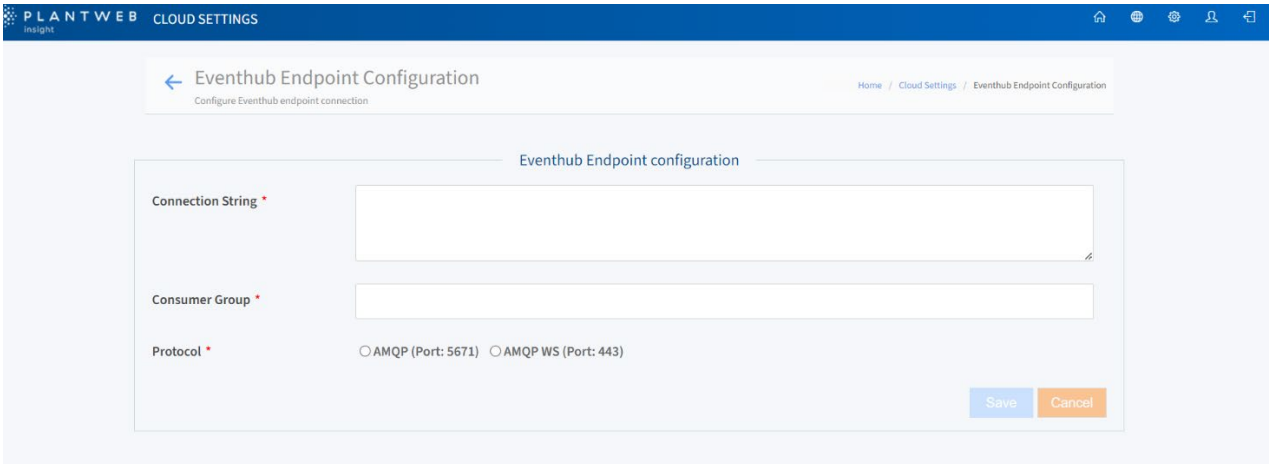
A new menu is available for this mode of system which lets you configure Azure IoT Hub connectivity details and view the connected “on-prem” systems. A warning triangle is displayed next to pages that are missing configuration details.



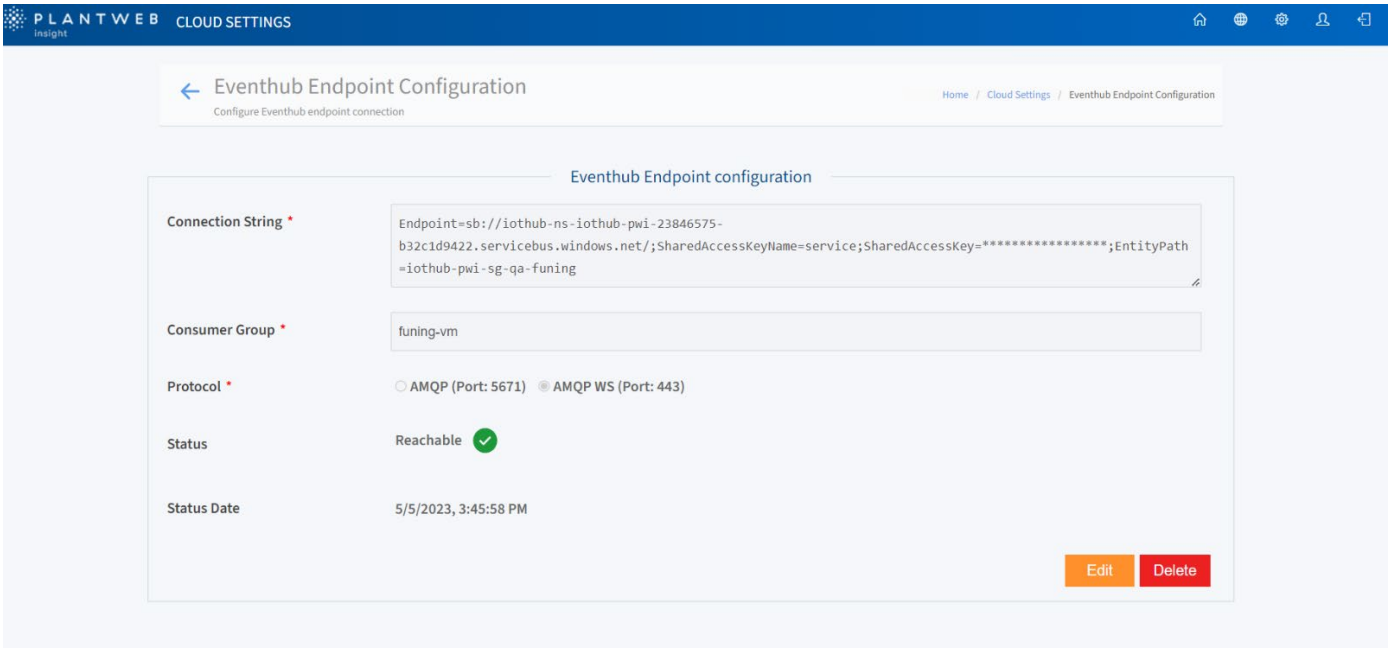
Event Hub Endpoint Configuration

Login to the Azure portal and select the IoT Hub configured during PWI Cloud Connector set-up. Select built-in endpoints under the Hub Settings and copy the Event Hub compatible endpoint.

Paste the connection string copied, enter the consumer group, and select the protocol to create an Event Hub Endpoint in the PWI Cloud App Only system.



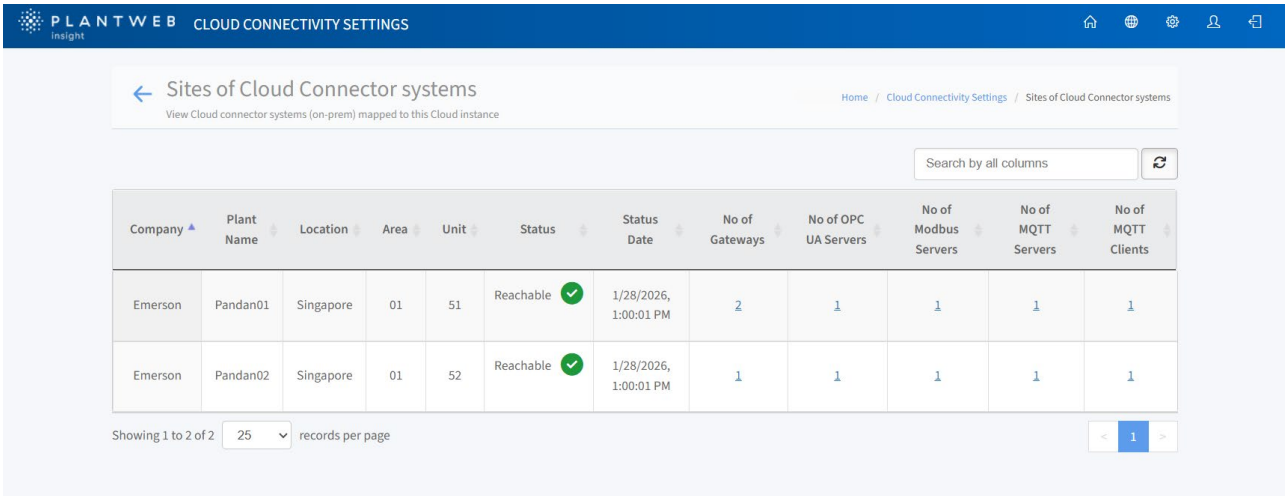
Once the endpoint is created, the status field will display the endpoint's connectivity status:



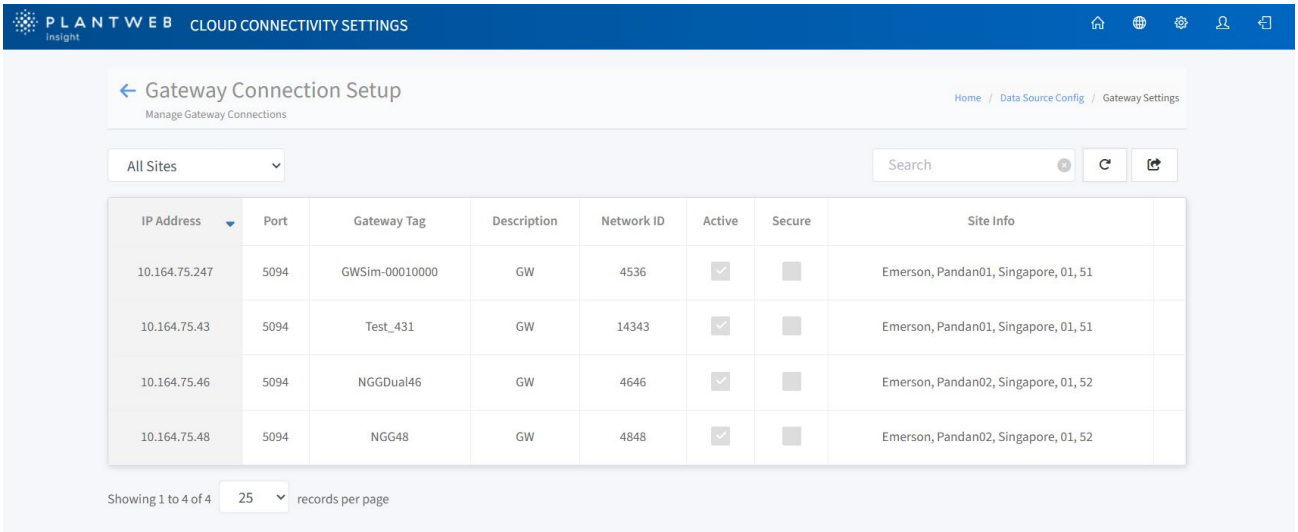
When the Cloud Connector and Event Hub endpoints are configured and status becomes reachable, data will begin flowing from the Cloud Connector to Cloud App Only system.

Sites of Cloud Connector Systems

This screen will display the Cloud Connector sites connected, site details, status, and a link to all data sources for each site (gateways, OPC-UA servers, Modbus servers, MQTT sources).



The Gateway Connection Setup page in the Cloud App Only system is a read-only screen that displays all the gateways configured across the Cloud Connectors feeding data to the Cloud App Only system. A dropdown menu is available to filter gateways based on the site.



There are similar pages for OPC-UA, Modbus, and MQTT data source connection setup.

Troubleshooting the PWI Cloud Connectivity Solution

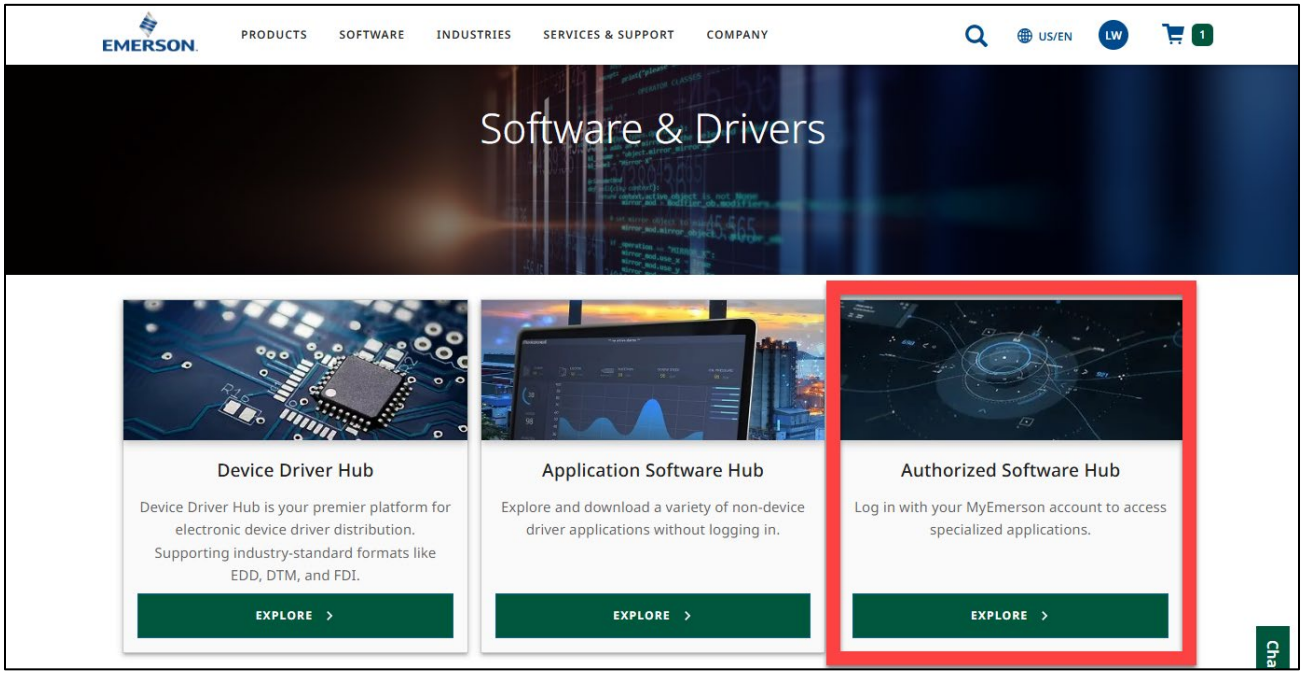
1. Verify the status in the “Eventhub Endpoint Configuration” page and ensure the Event Hub is reachable by the PWI Cloud App Only system.
2. Verify the status column in the “Connected IOTCS Sites” page corresponding to that site is reachable in cloud VM.

3. Check the IOT Hub device connections status from the PWI Cloud Connector "IoT Hub Devices Configuration" page. Make sure the IoT Hub devices are all reachable.
4. If the status is reachable in all the above steps, then verify if the IoT Hub message quota has been exceeded in the Azure portal.

5. Installation

Downloading Plantweb Insight Software

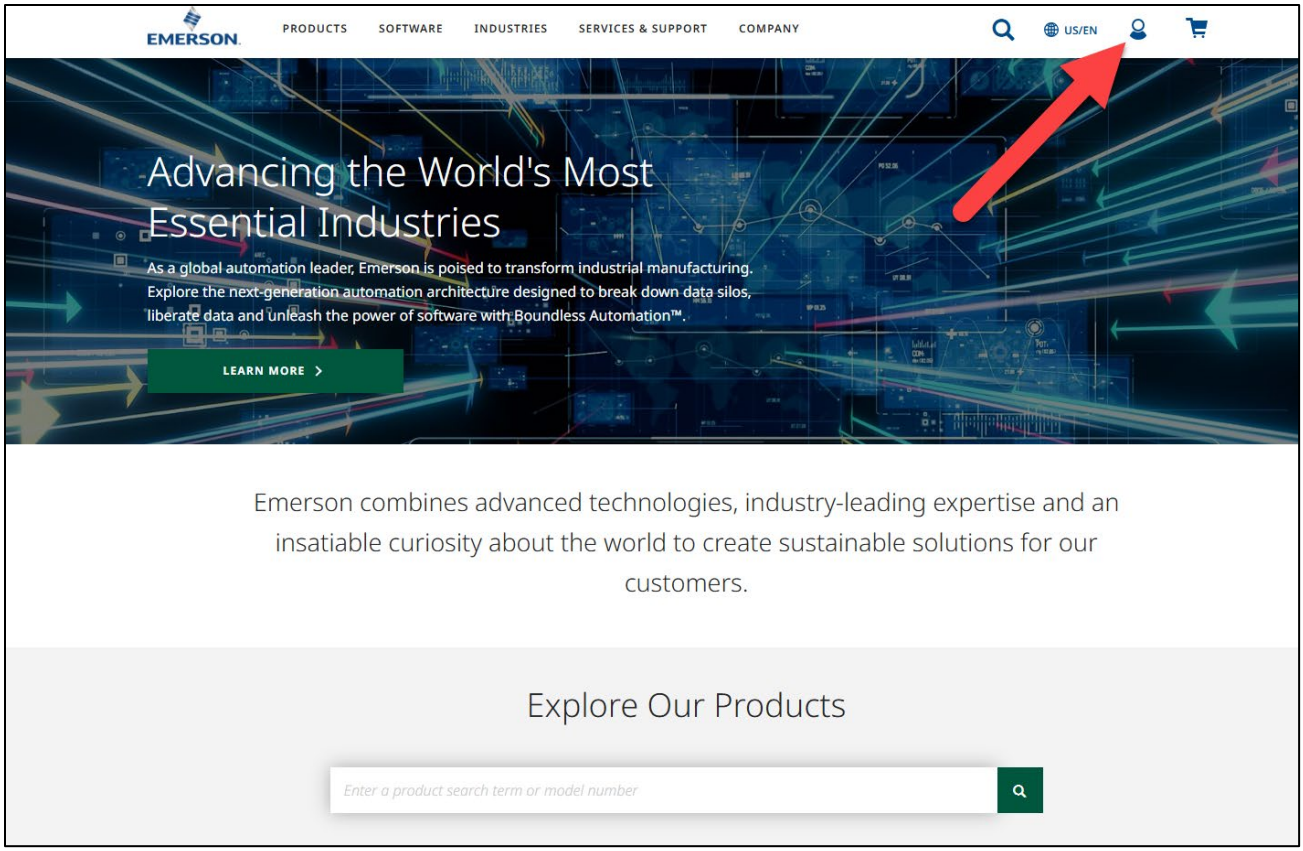
Plantweb Insight software is available for authorized users to download via the MyEmerson **Authorized Software Hub** which can be accessed from the Emerson Software & Drivers Download page



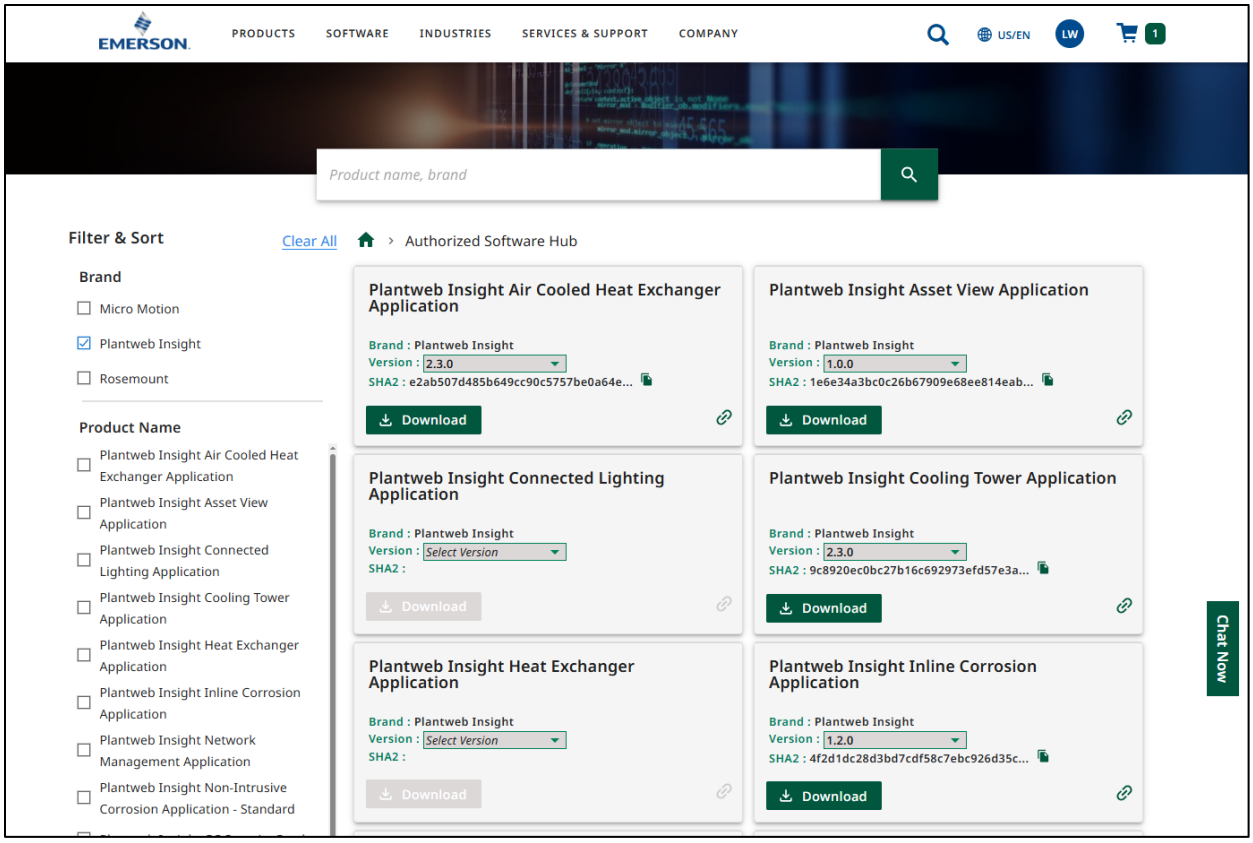
The Authorized Software Hub is where users can access and download the latest versions of:

- Plantweb Insight virtual machine images in .OVA or .VHD format
- Plantweb Insight system upgrade bundles
- Plantweb Insight OS security patches
- Plantweb Insight applications

Access to the MyEmerson Authorized Software Hub requires a MyEmerson account. Existing users will be prompted to sign in. New users can create an account by visiting Emerson.com and navigating to the MyEmerson sign-in icon in the upper right corner of the screen.



Upon accessing the Authorized Software Hub, users can scroll, search or filter for specific Plantweb Insight download packages. Latest versions are recommended if more than one version is available.



A user's initial download of a software package requires authorization of access. Requesting access to download a software package does not require a purchase order. Once a user is authorized to download a software package, they will be authorized to download any future versions of that software as well.

Download your desired software package.

NOTE: It is recommended to download software packages one at a time over stable internet connection. All download packages include a checksum file for download verification.

Plantweb Insight Factory Configuration Settings

The PWI virtual machine features two external network interfaces, a primary (eth0) and a secondary (eth1). Eth0 is routable, and Eth1 is non-routable. PWI's primary and secondary network interfaces are intended to allow PWI to connect to two separate networks, if necessary. Data source connectivity may utilize one network interface while web access for users utilizes the other network interface. If data sources and users' web clients exist on the same network, only Eth0 is required.

The default network adapter configuration is:

Primary Interface	**Eth0**	DHCP, reflected on the VM console
Secondary Interface (disabled)	**Eth1**	User-defined IP from web interface

NOTE: Users who wish to utilize Eth1 can enable the secondary interface from within the PWI web interface by navigating to ***Platform Settings > Network Configuration.***

NOTE: If a DHCP server is not available to assign Eth0 an IP address, refer to the next section, *PWI Rescue Console Access*.

NOTE: If using the PWI Edge Solution, the secondary interface is assigned to physical ethernet port ETH2 on the industrial PC.

Plantweb Insight – Rescue Console Access

Purpose

Rescue console helps a user change/view some of the PWI configurations from the system console. This is a low-privileged user that uses the following credentials:

Username: ***pwi-user***

Password: ***Emerson.1234***

In case a user loses connection with their PWI UI due to either assigning an incorrect static IP address in Network Configuration page OR setting an incorrect HTTP whitelist in the Ports and Protocols page, they can restore the UI connection by accessing the rescue-console as a low privileged user.

NOTE: As this is low privileged access, the console user will have permission only to perform the following restricted actions for e.g. list, clear, run the following scripts:

Set Static IP

This action allows the user to override the static IP ethernet settings for primary network interface (eth0).

1. User can assign a static IP by running the following script with appropriate parameters:

```
sudo ./set-static-ip <IP address> <Netmask> <Gateway IP>
```

```
E.g. : sudo ./set-static-ip 192.168.238.125 255.255.255.0 192.168.238.2
```

2. Enter `exit` and press **Enter/Return** to log out of the console

Once successful, user will be able to connect to the PWI web UI using the new static IP. The script will check for the following errors

- Invalid IP addresses or netmask
- IP and GW in different networks
- IP or netmask set to 0.0.0.0
- IP and/or GATEWAY set with last quad=0

Reset HTTP Whitelist

This action allows the user to reset the HTTP whitelist IP to 0/0.

1. User can reset the http whitelist by running the following script:

```
sudo ./http-whitelist-reset
```

2. Enter `exit` and press **Enter/Return** to log out of the console

Once successful, user will be able to connect to the PWI web UI from any IP in the same network.

Add New Disk

This action allows the user to add a new disk to increase the disk space.

NOTE: This feature is available only from PWI version 3.1.0 VM release or later

1. User must add a new virtual disk of required capacity to the system and run the following script:

```
sudo ./add_new_disk
```

2. Enter `exit` and press **Enter/Return** to log out of the console

The script will provide verbose guidance

NOTE: Once a disk is attached to the system it is committed and cannot be removed.

Check Disk Free Space

This action allows the user to monitor available free space on the disk.

NOTE: This feature is available only from PWI version 3.1.0 VM release or later

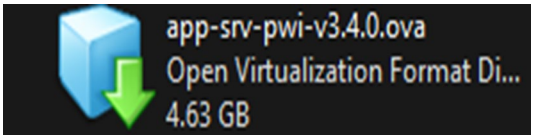
1. Run the following script:

```
sudo ./disk_free_status
```

PWI Installation on VMware Workstation

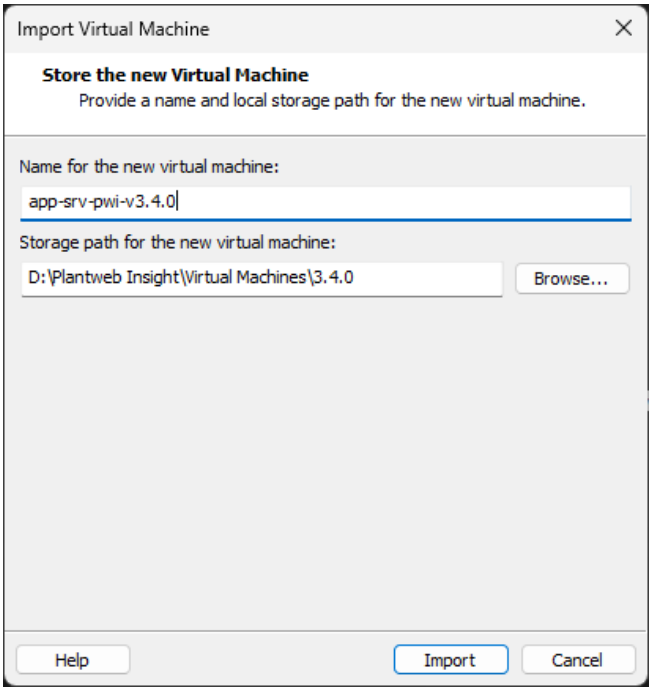
The PWI platform is provided as fully developed virtual machine (.OVA file) while applications and upgrade bundles are provided as separate .ASC files.

1. Ensure a compatible version of VMware is installed on the host machine
2. Download and unzip the latest .OVA image along with any applicable .ASC upgrade bundles. Ensure have been downloaded completely and successfully to the host machine
3. Import virtual machine onto hypervisor by either double clicking the .OVA file or right click → **Open with VMware Workstation** (or preferred hypervisor)

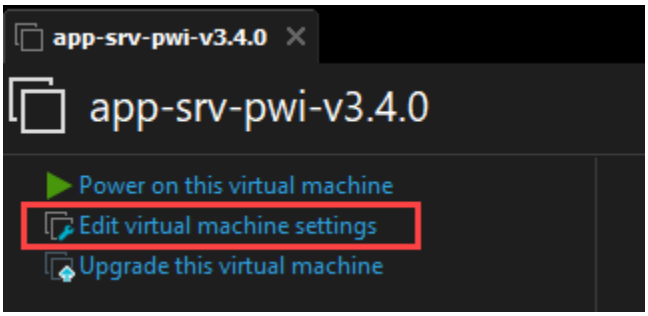


NOTE: This file name may change based on PWI version or user changes.

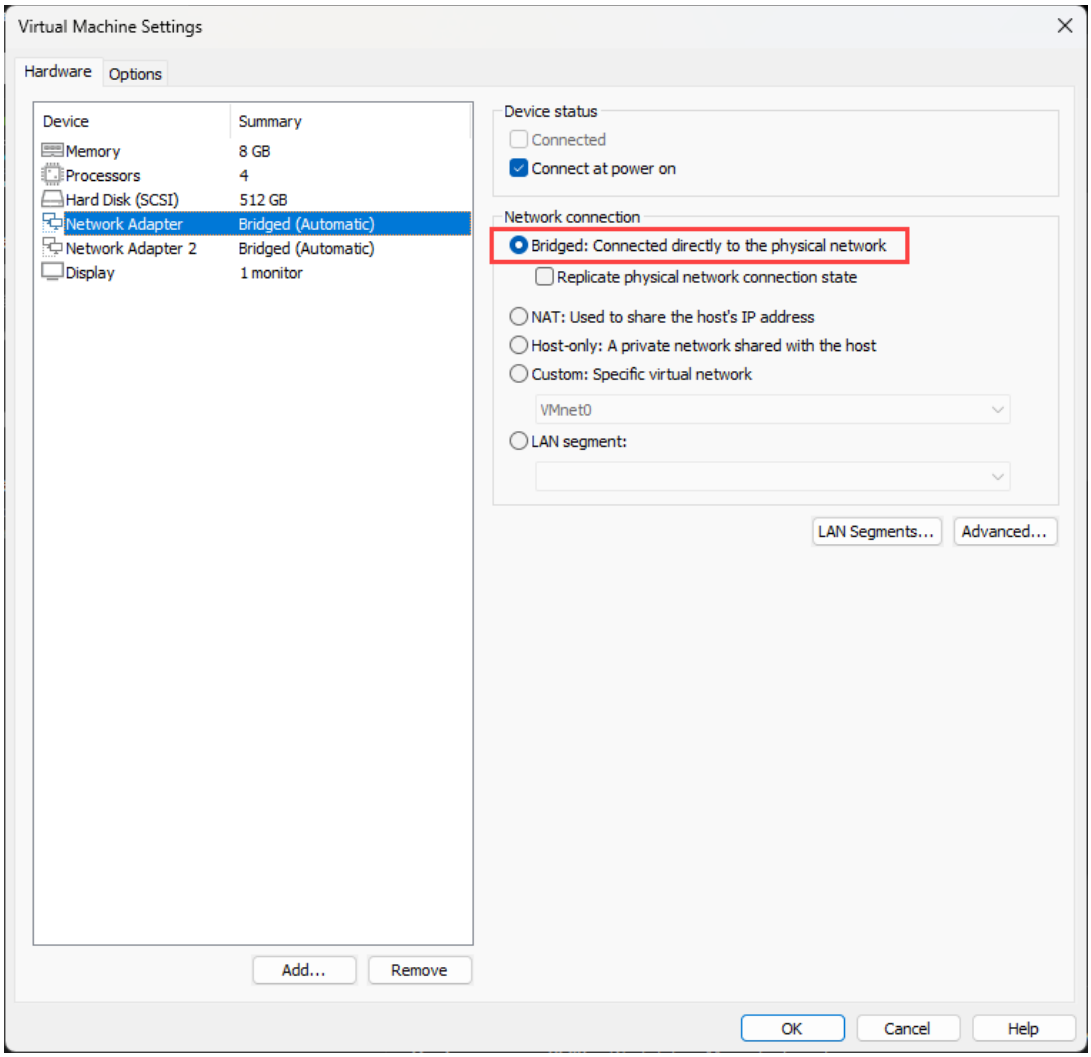
4. Choose a name and storage location for the new virtual machine, the select **Import**



5. Wait for the virtual machine to be imported
6. Select the PWI virtual machine and then select **Edit virtual machine settings**

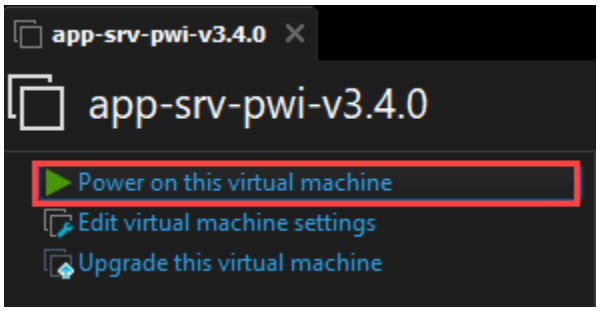


7. It is recommended that at least one of PWI's network adapters be set to "Bridged". Ensure it is bridged to the correct location: typically, the ethernet port of the host machine.
   Using a bridged connection allows the virtual machine to connect to the ethernet connections of the host machine. This is the most common setting for PWI as it allows multiple clients to access the user interface and can connect to multiple WirelessHART Gateways or other data sources.

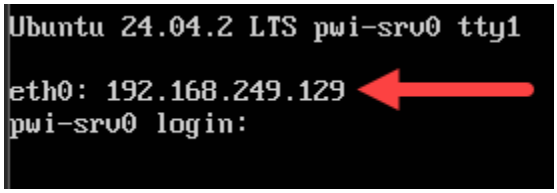


NOTE: If the VM is being set up on a corporate network, it is often required to use NAT for the network adapter settings. This will allow the VM to acquire an IP address locally. If a user's environment allows connection to their corporate network and can acquire an IP address, the network adapter(s) can be left as Bridged.
NOTE: The secondary adapter is disabled within PWI by default. Users who wish to utilize the secondary adapter should enable it from within the PWI web interface. Users who do not wish to utilize the secondary adapter can remove it from VM settings.

8. After finalizing the VM adapter settings, select the PWI virtual machine and then select **Power on this virtual machine**



9. Allow the VM to boot and then wait at least 5-10 minutes before navigating to the provided IP address to allow the web server to prepare. This delay occurs only once and subsequent reboots will not be affected.



NOTE: This IP address will vary depending on installation. What is shown here will not be your IP address.

A DHCP server is required to assign an IP address. If a DHCP server is not available on your network or eth0 fails to get an IP address at boot up, power off the virtual machine and set the primary network adapter to NAT to utilize the built-in DHCP server of your host machine. This will allow the user to access the PWI web interface from the host machine and assign a static IP address to eth0 from the web interface. Using a NAT connection will not allow access to PWI from other locations on the network.

If users have a desired static IP address for PWI, they can set a static IP directly from the VM console using the low-privilege Rescue Console Access provided in the previous section.

10. The VM is now installed and running. All further interaction with PWI is conducted through the web interface. Jump to the section, **Accessing the Web Interface**.

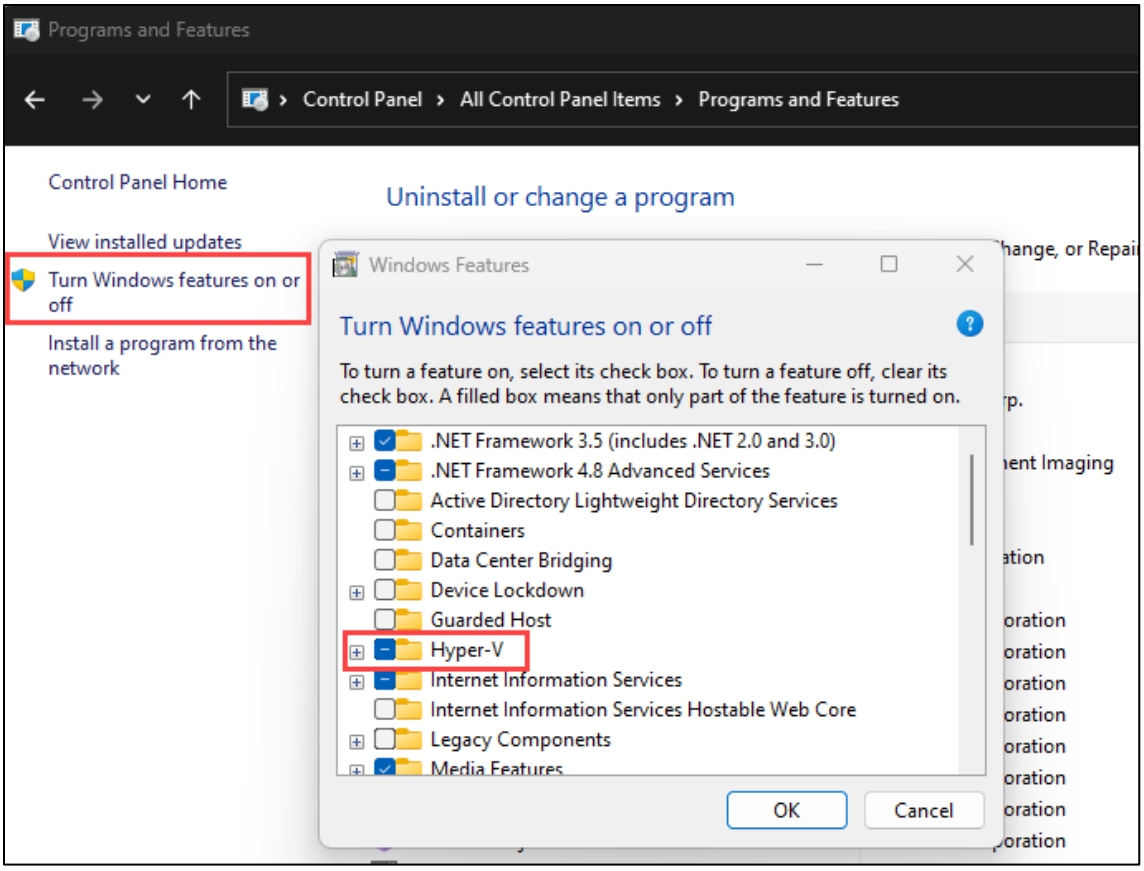
PWI Installation on Microsoft Hyper-V

PWI is also available as a virtual hard disk (.VHD) image for Hyper-V. Application files and PWI upgrade bundles in .ASC format an applicable on both .VHD and .OVA versions of PWI, since .ASC files are imported through the PWI web interface.

Enable Hyper-V

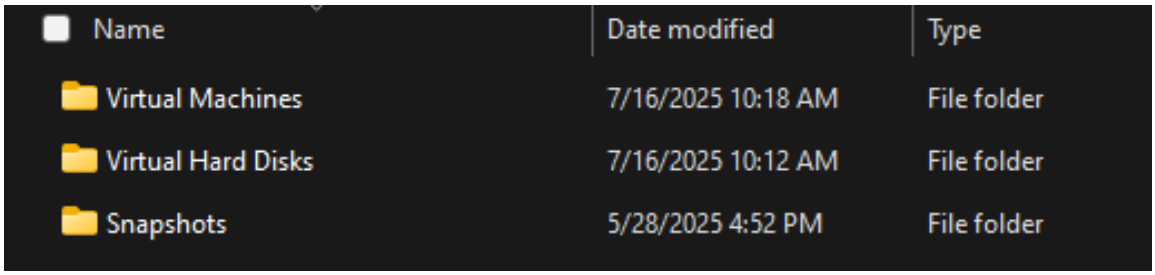
1. From the Windows Control Panel, navigate to **Programs and Features**

2. Select **Turn Windows features on or off**
3. Select **Hyper-V** and click “OK”
4. After the installation has completed, you will be prompted to restart your machine
5. After restarting, you will be able to launch the Windows Hyper-V application



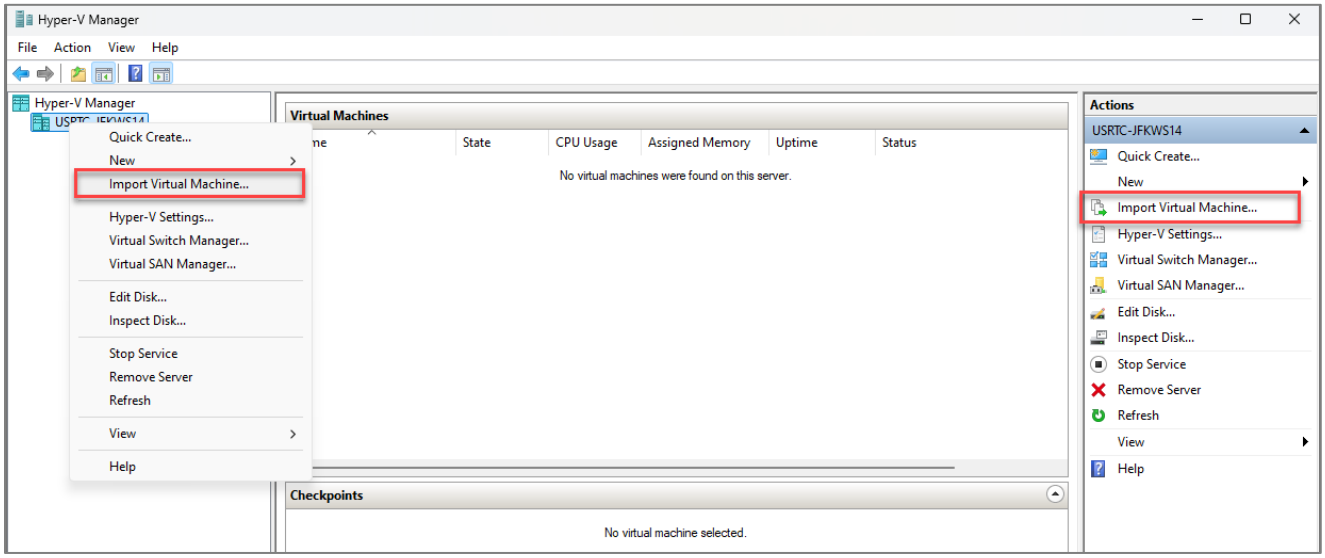
Set up the PWI VM

1. Download and unzip the latest PWI Hyper-V VM bundle (e.g. *app-srv-pwi-3.4.0-hyperv.zip)*

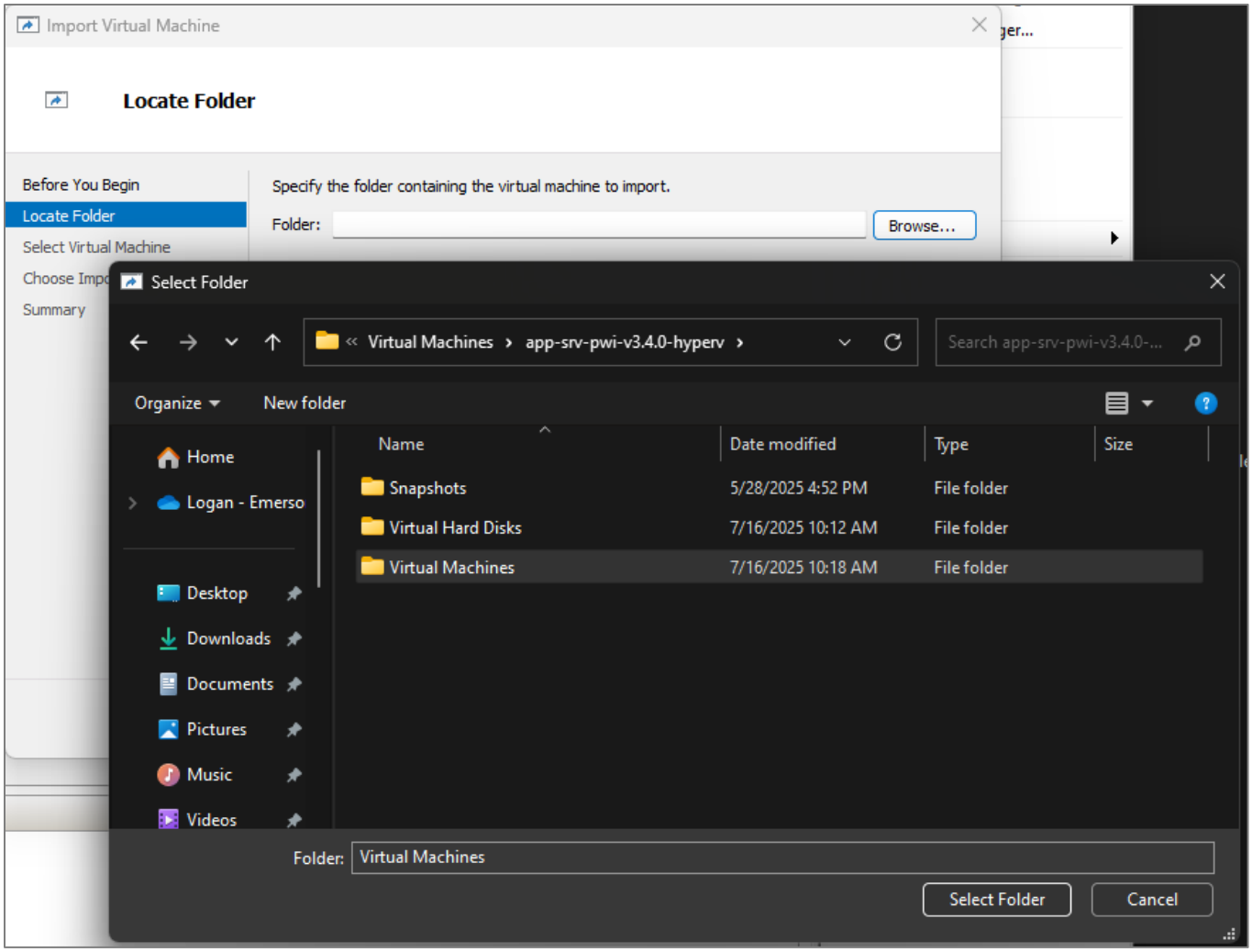


2. Open Hyper-V Manager with admin privileges
3. Import the PWI Virtual Machine:
    a. Option 1: Right click ***Hyper-V Manager > [Machine Name]*** and select “Import Virtual Machine”

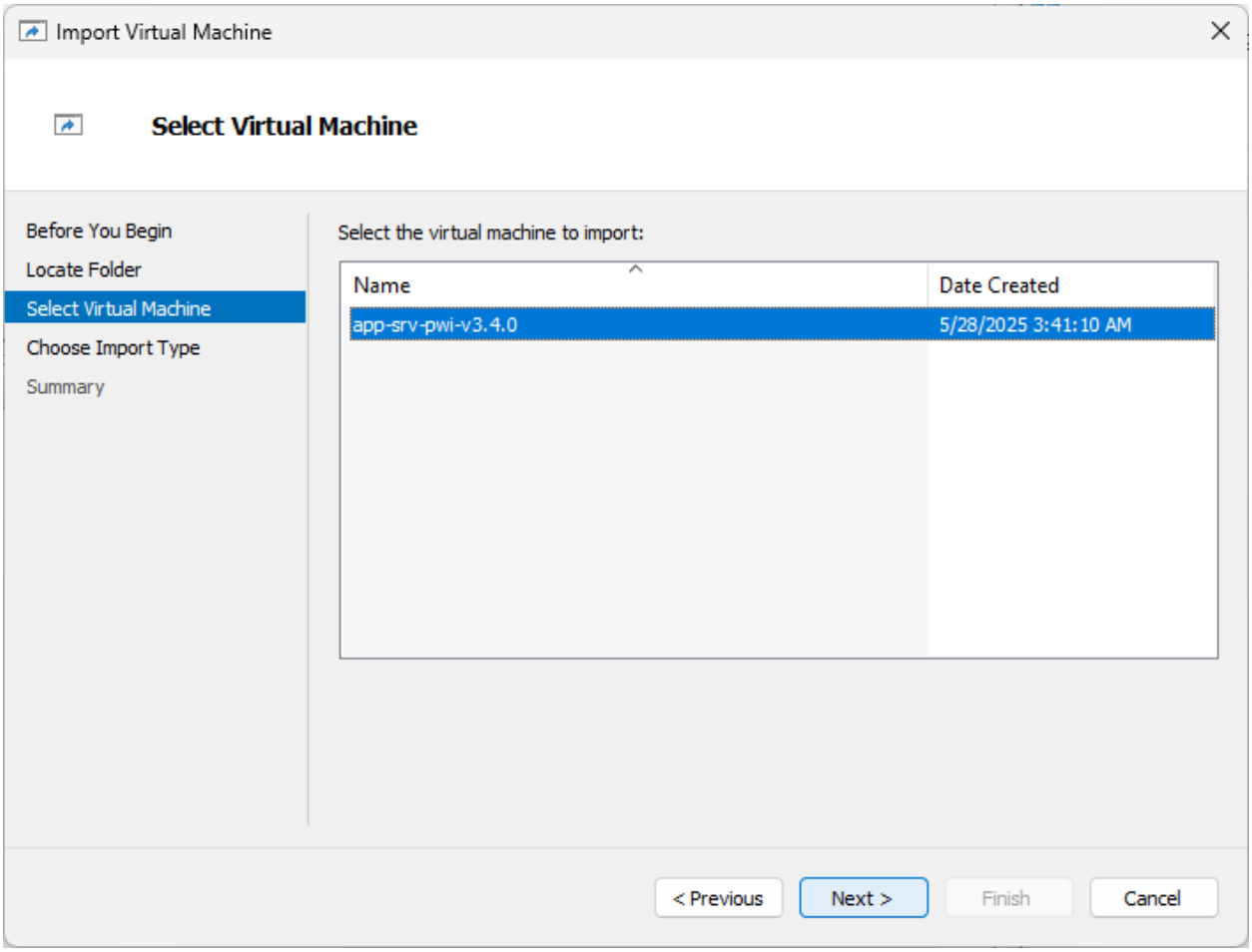
b. Option 2: Click ***Hyper-V Manager > [Machine Name]***, and then click “Import Virtual Machine” from Actions menu on the right side

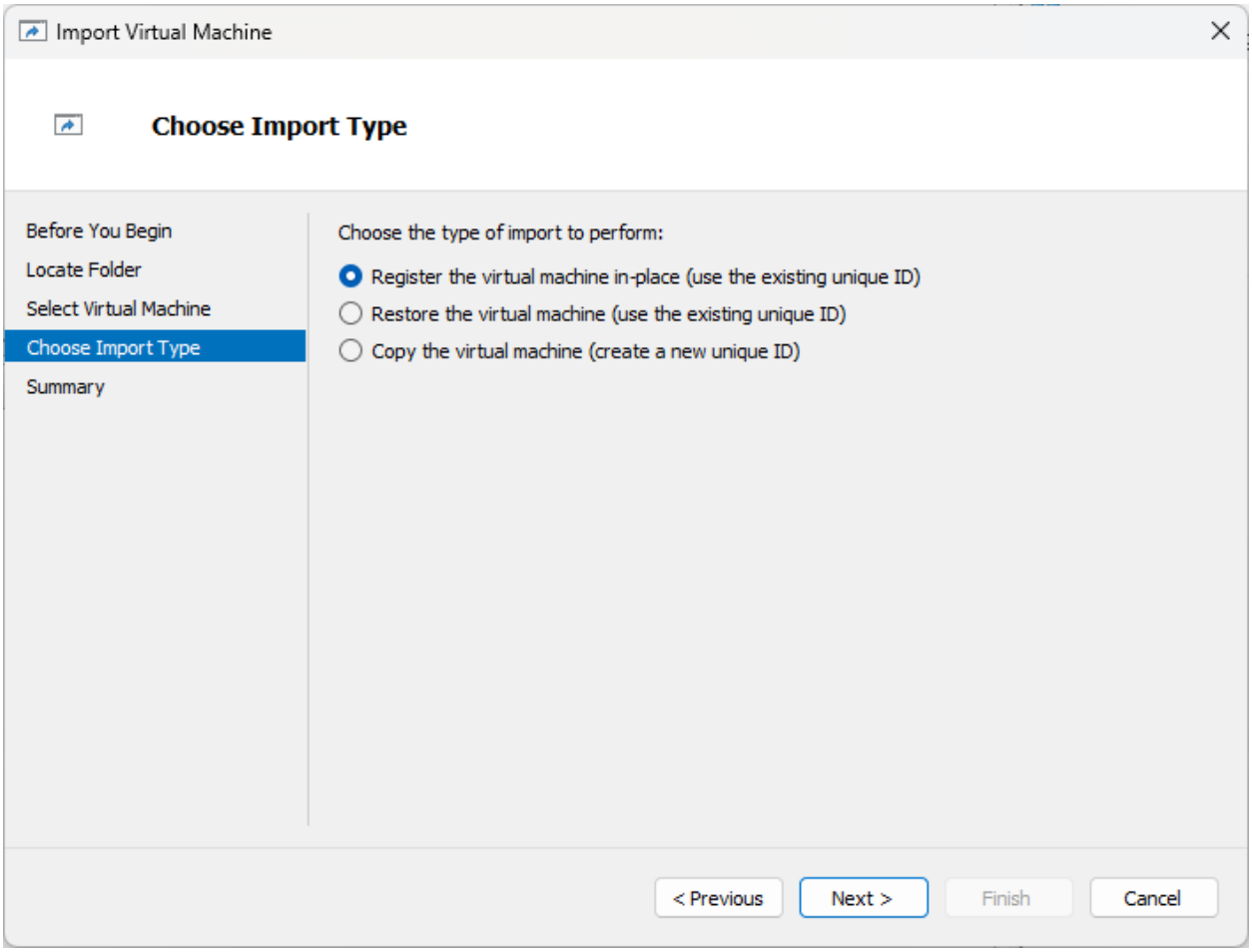


4. From Locate Folder, choose the “Virtual Machines” folder from the extracted download files

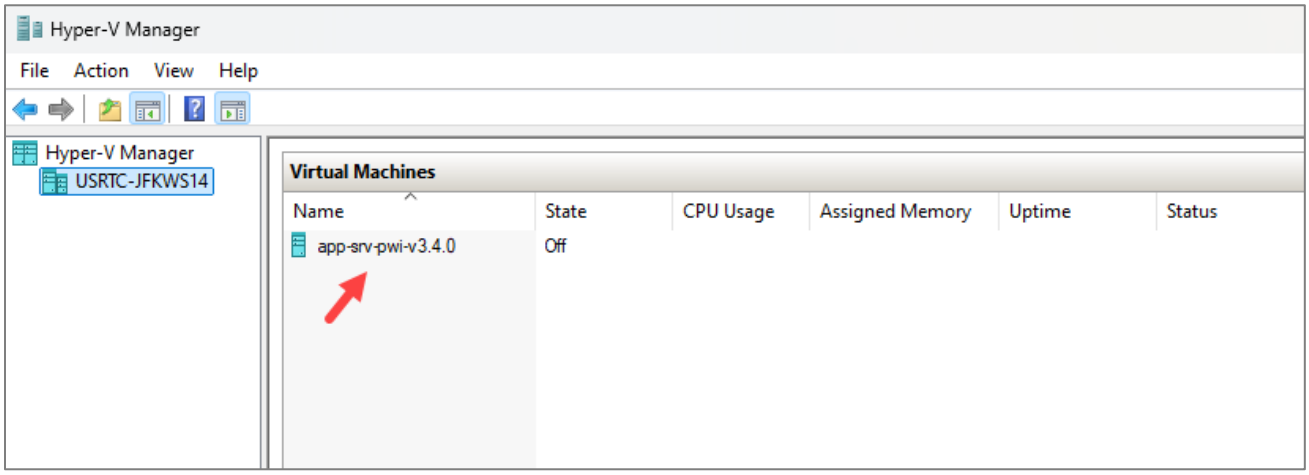


5. Continue with default selections and finish the setup


Import Virtual Machine
Select Virtual Machine
Before You Begin
Locate Folder
Select Virtual Machine
Choose Import Type
Summary
Select the virtual machine to import:
Name
Date Created
app-srv-pwi-v3.4.0
5/28/2025 3:41:10 AM
< Previous
Next >
Finish
Cancel

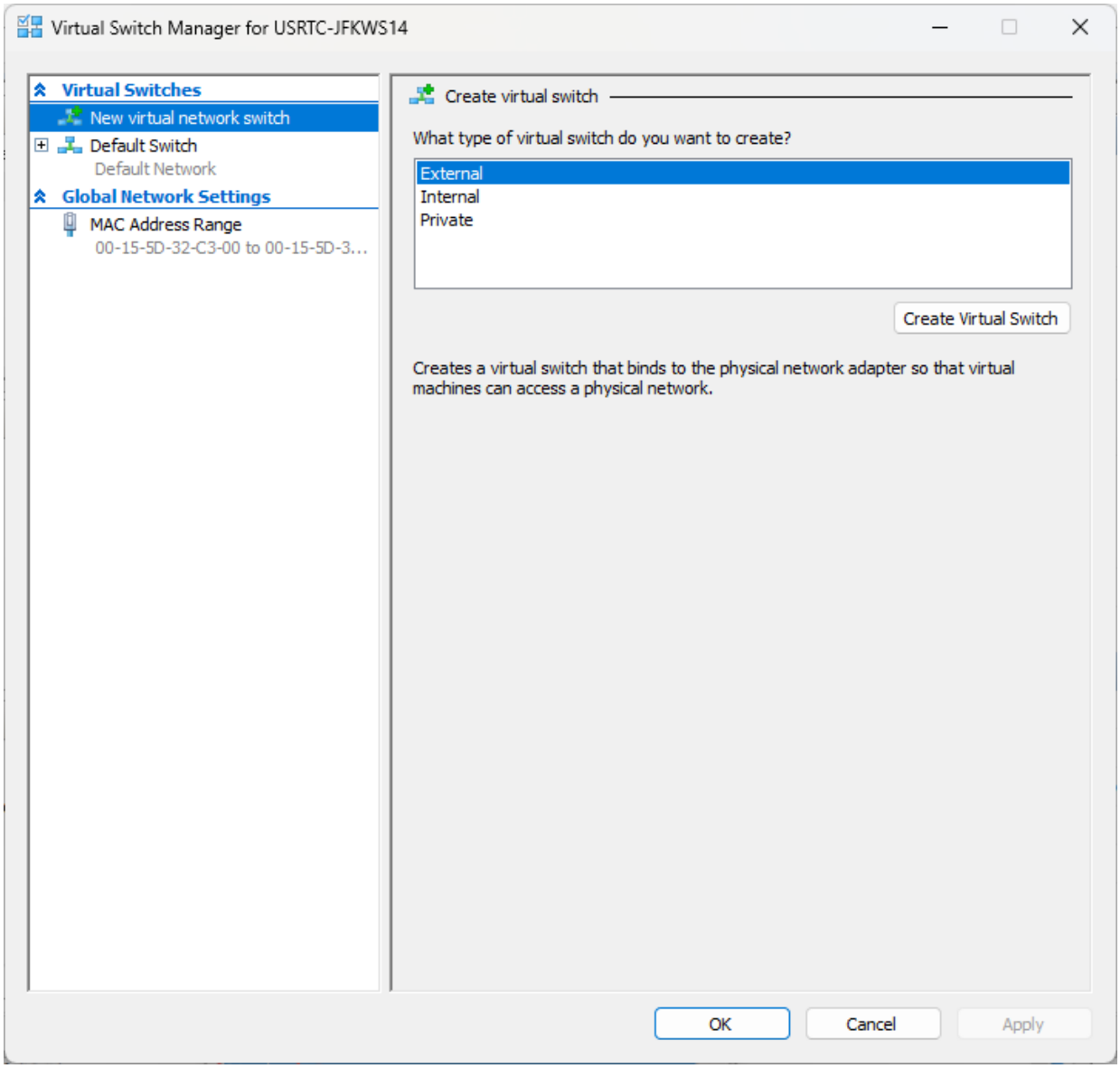


6. The PWI virtual machine should appear with a name like "*app-srv-pwi-v3.4.0"* in an "Off" state

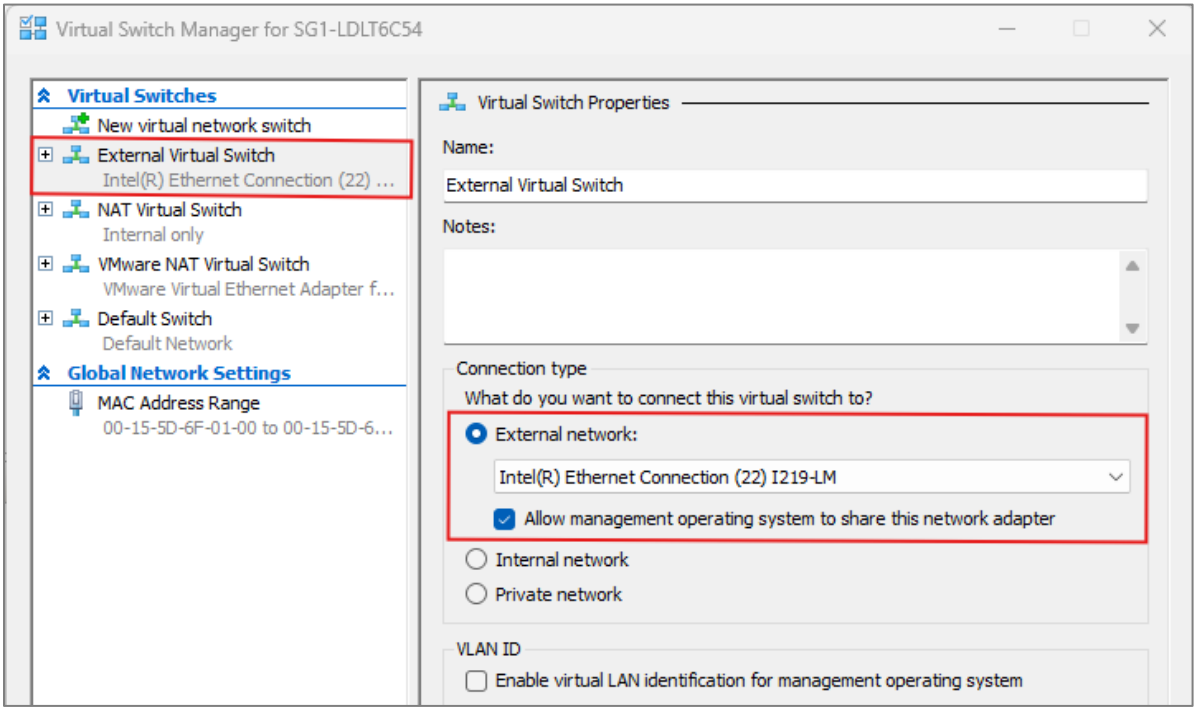


7. In the Actions menu on the right side, select "Virtual Switch Manager"

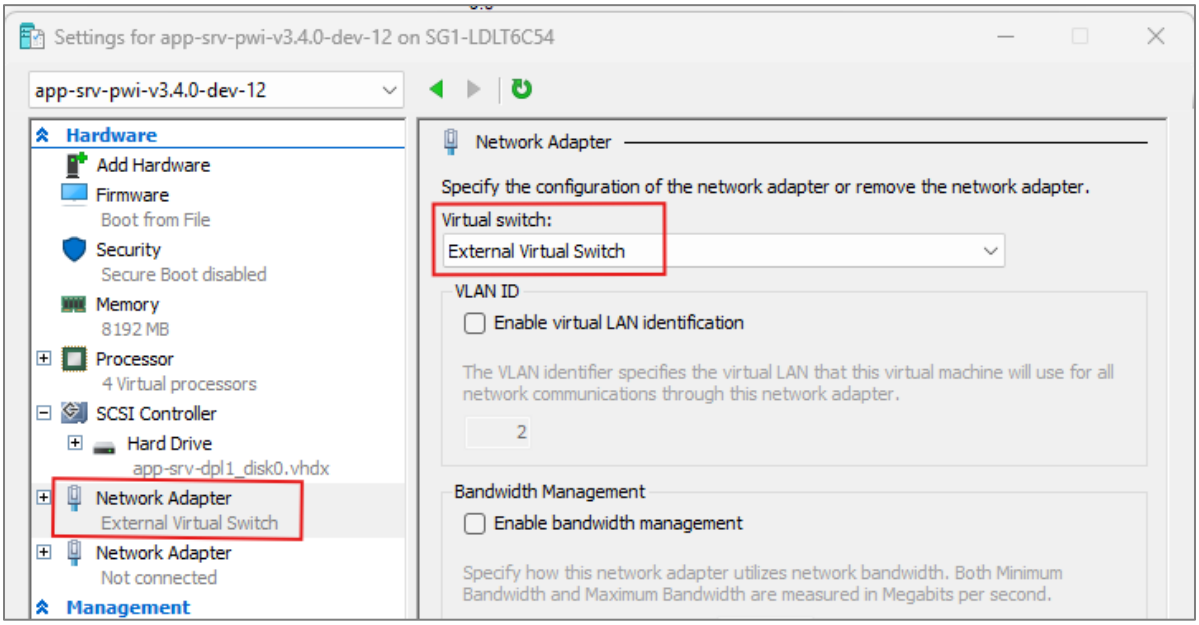
- Factory configuration of PWI is targeted at Hyper-V on the latest version of Windows Pro which provides a “Default Switch” virtual adapter. The Default Switch provides DHCP functionality to allocate an IP address
- For older versions of Hyper-V which do not have the “Default Switch” virtual adapter, users must manually configure and connect Network Adapters to the VM by selecting the Virtual Switch Manager in the Actions menu on the right side.
- An **external** type switch connects the PWI network adapter to an external virtual switch, which is directly linked to the host PC’s physical NIC. This allows PWI to operate as a real device on the physical network, enabling direct access to WirelessHART Gateways and other network resources.



External Virtual Switch Definition

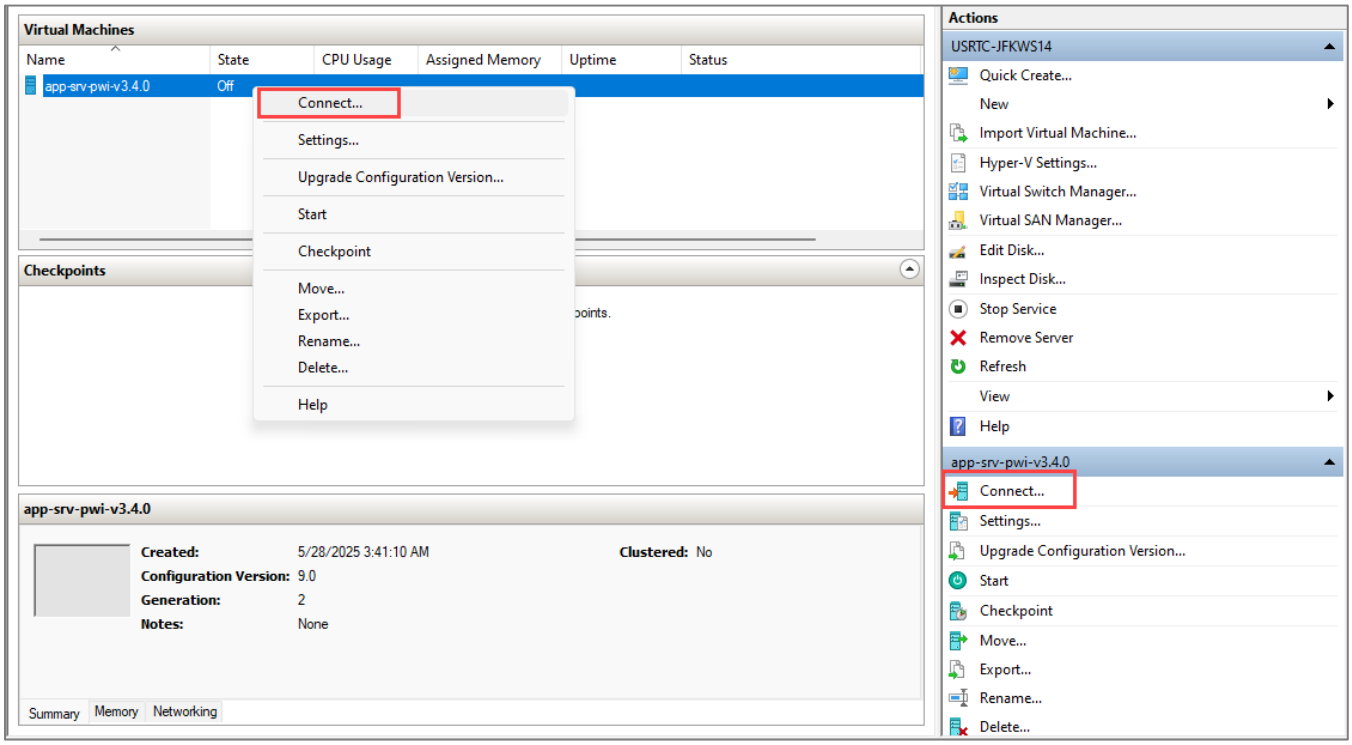


PWI Network Adapter Setting

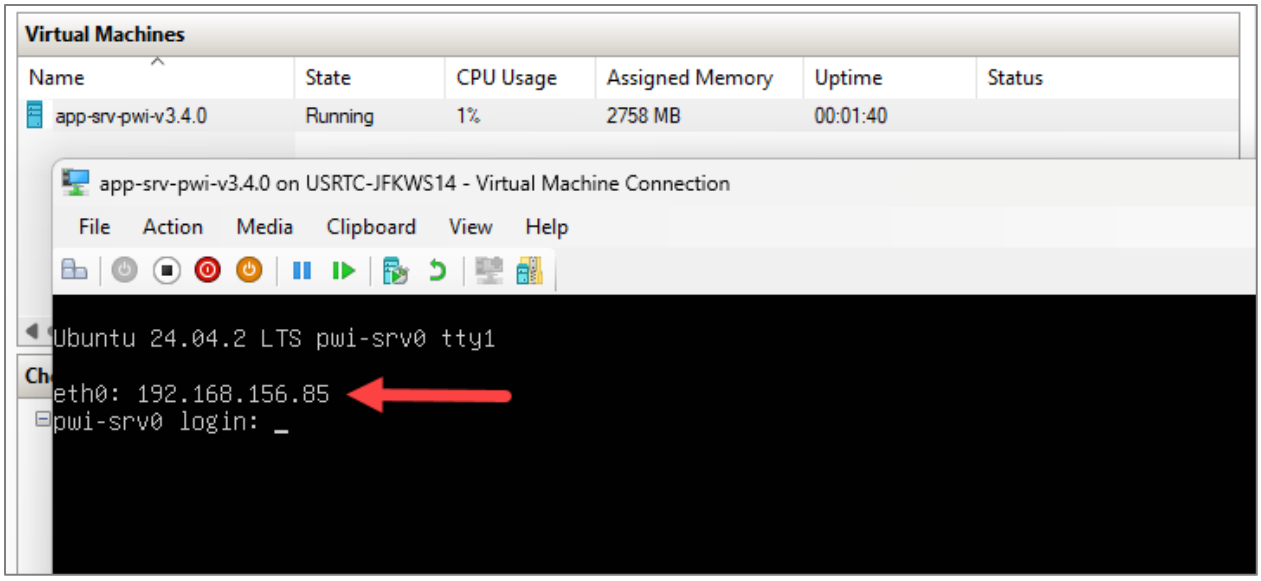


NOTE: Port forwarding does not work on the “Default Switch” network.

8. If a DHCP server is available, start the PWI VM either by right clicking the VM name and clicking “Start” or by clicking the Start button in the Actions menu on the right side.
   If a DHCP server is not available, or the console fails to display an IP address for eth0, refer to Rescue Console Access section on assigning a static IP.
   If PWI cannot directly access a desired network, refer to NAT and Port Forwarding on Hyper-V.
9. Connect to the PWI server by either right clicking the VM and clicking “Connect” or by clicking the Connect button in the Actions menu on the right side



9. The VM console should appear, and eventually an IP address should be displayed on the console. This IP address is the primary network interface of PWI.



10. The VM is now installed and running. All further interaction with PWI is conducted through the web interface which is access through the displayed IP address. Jump to the section, **Accessing the Web Interface**.

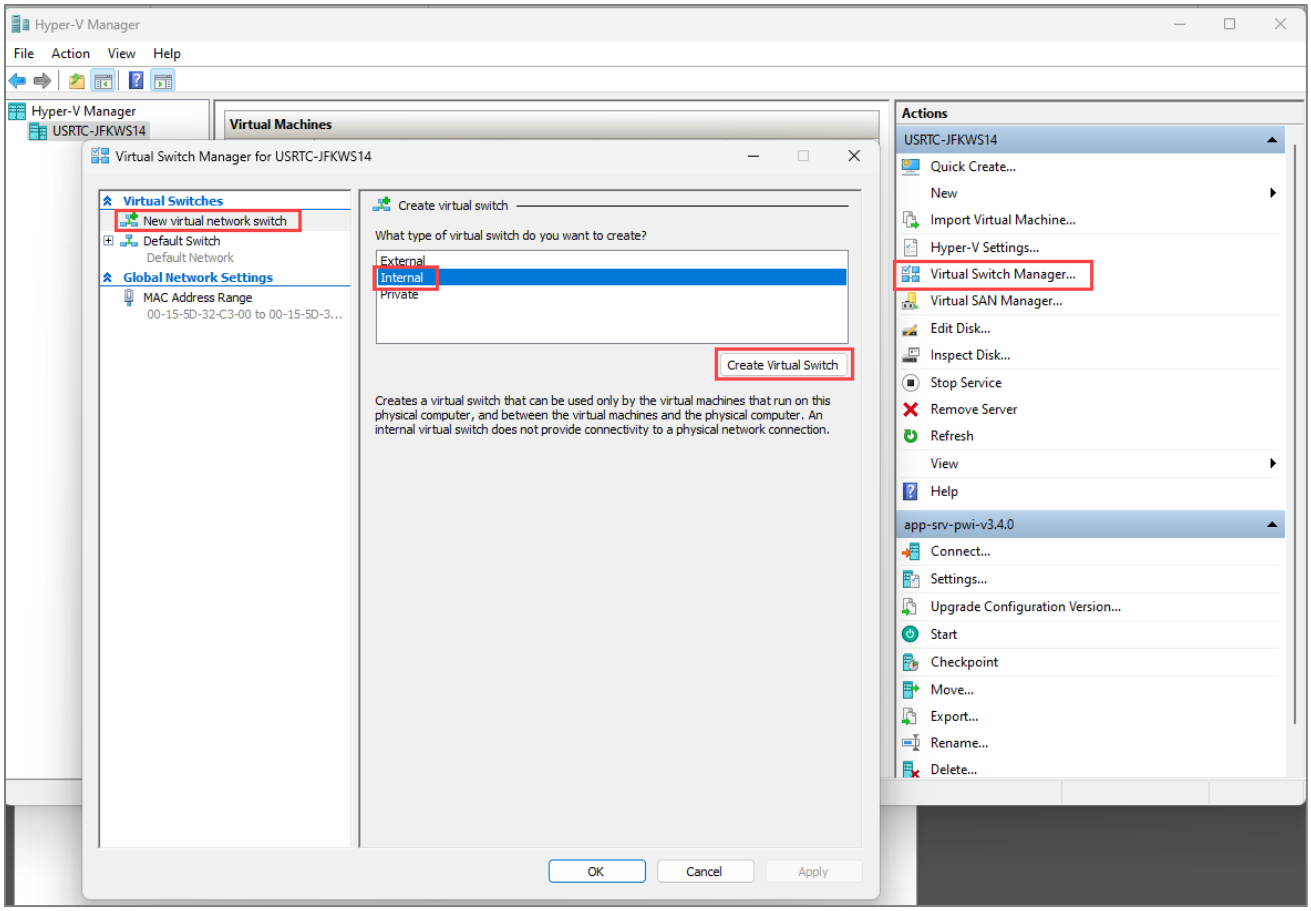
NAT and Port Forwarding on Hyper-V

To avoid PWI VM connectivity issues caused by network security policies, the Hyper-V virtual switch needs to be set up with NAT and port forwarding. In this configuration, the PWI network adapter is connected to a **NAT virtual switch**, and a **private IP address** is assigned within the NAT environment. Since this private IP is not accessible outside the host PC, **port forwarding** is required to enable external access to the PWI. This method is generally reliable and supports most outbound connections.

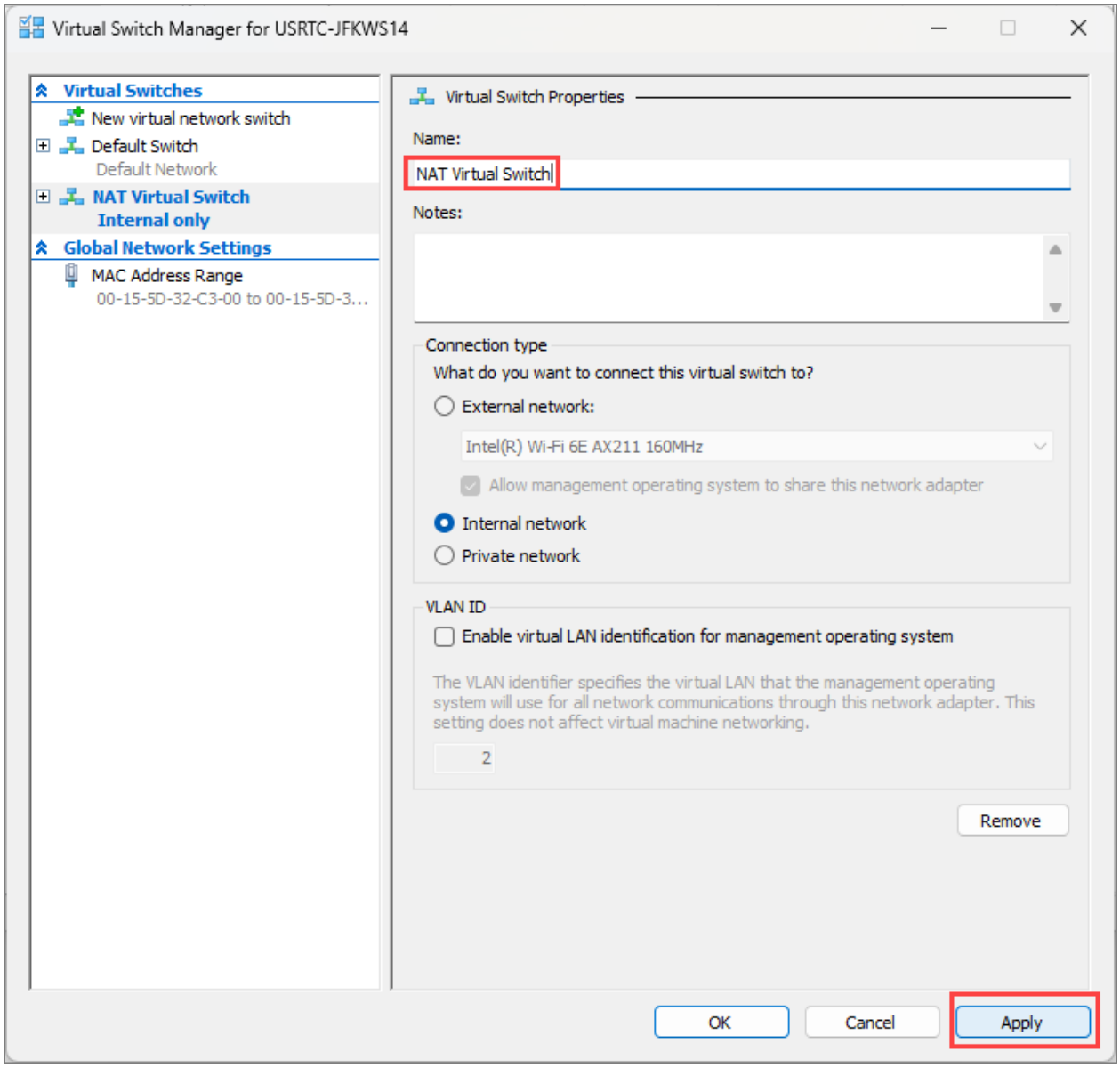
NAT + Port Forwarding generally does not interfere with **outbound connections**, including those to WirelessHART Gateways. **Inbound connections**, such as connections from an external OPC-UA client to the PWI OPC-UA server have been known to run into problems due to OPC-UA constraints. Other connectivity types are expected to function normally in NAT mode.

To set up a virtual network with NAT and Port Forwarding on Hyper-V, follow the steps below:

1. Create a new internal Virtual Switch manually. Users can create an internal virtual switch from Hyper-V manager or from Windows PowerShell.
    a. Select Virtual Switch Manager from Actions menu
    b. Select “New Virtual Network Switch” and select Internal for switch type, then click Create New Virtual Switch button.



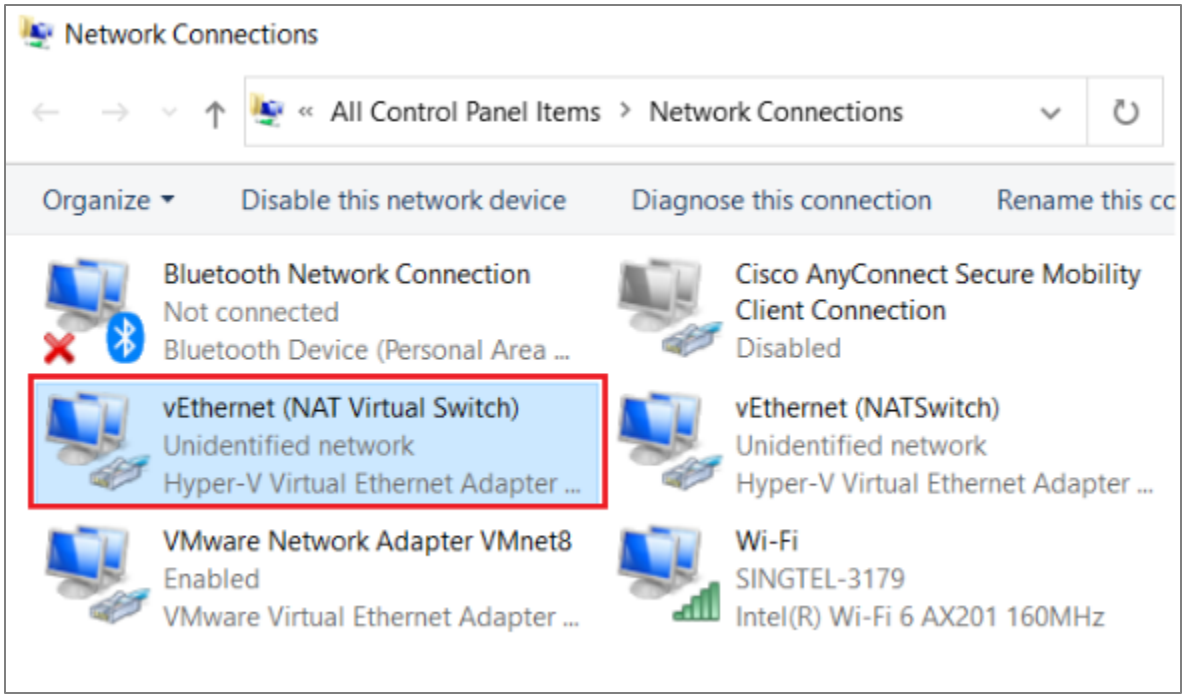
c. Rename the virtual switch to “NAT Virtual Switch” and click Apply.



Alternatively, Windows PowerShell can be used to create the virtual switch. Run the command shown below to create an internal virtual switch

```
New-VMSwitch -Name "NAT Virtual Switch" -SwitchType Internal
```

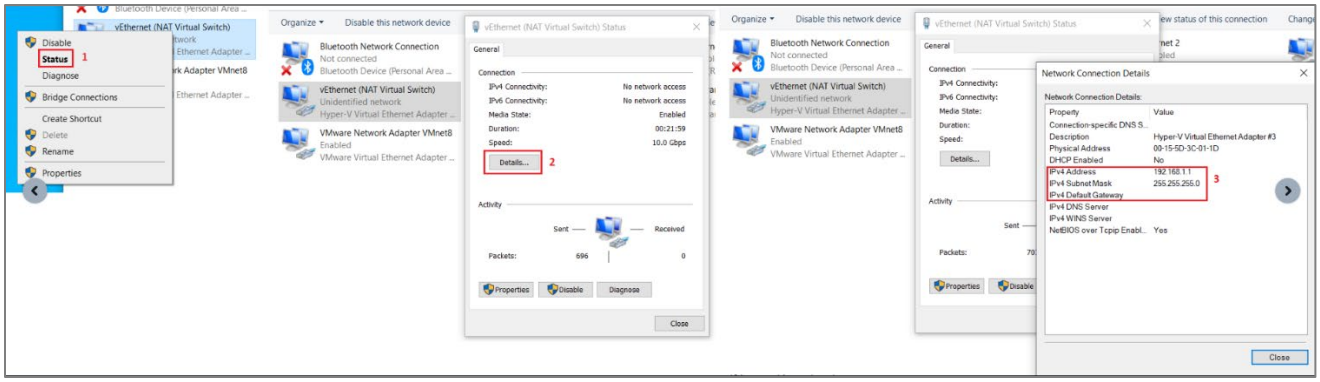
2. After creation, you will see a new network adapter with the name “vEthernet (NAT Virtual Switch)” created under Windows **Control Panel > All Control Panel Items > Network Connections**



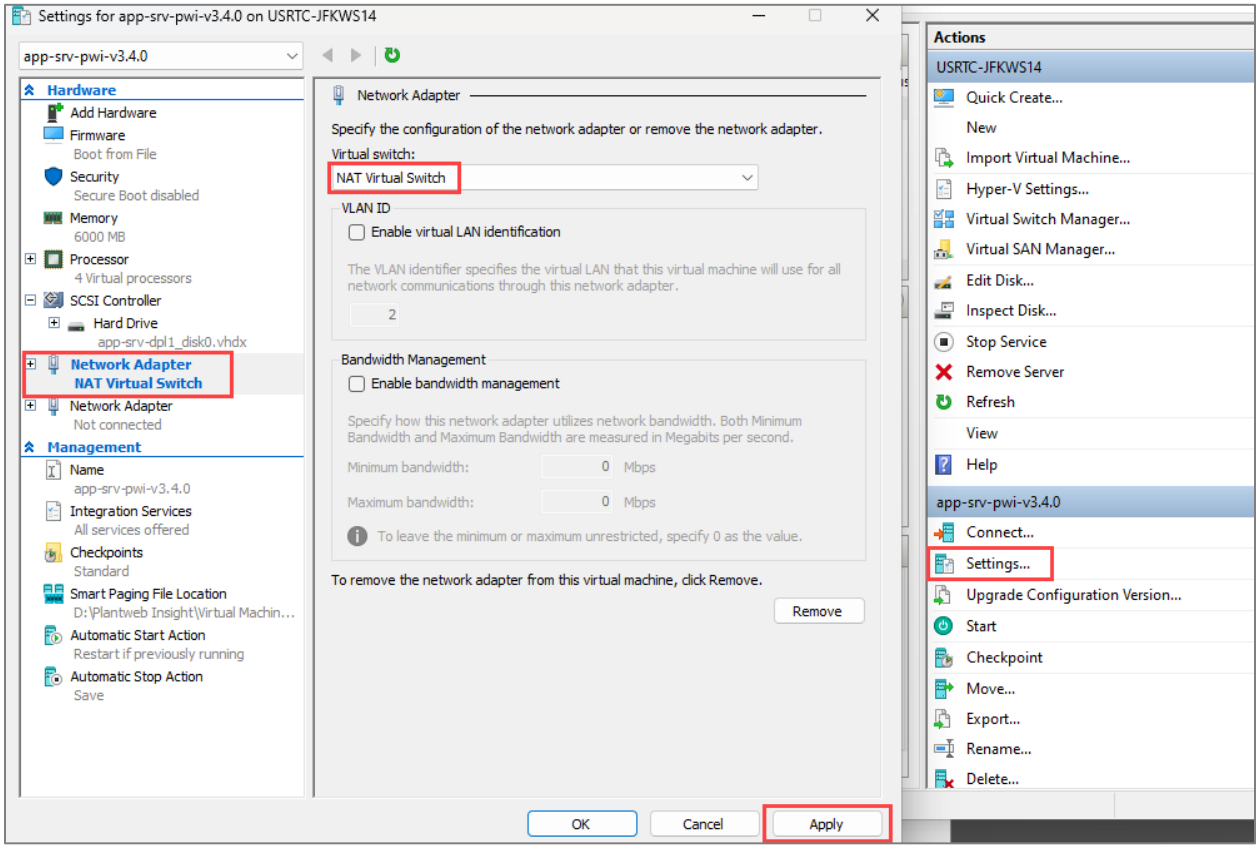
3. Set up and configure associated NAT network with the command below using Windows PowerShell

```
New-NetIPAddress -IPAddress 192.168.1.1 -PrefixLength 24 -
InterfaceAlias "vEthernet (NAT Virtual Switch)"
New-NetNat -Name "NATVirtualNetwork" -InternalIPInterfaceAddressPrefix
"192.168.1.0/24"


Get-NetIPAddress -IPAddress 192.168.1.1

<== This command will check newly created NetIPAddress info


Get-NetNat

<== This command will check newly created virtual NAT network info
```

4. Upon checking the new network adapter “vEthernet (NAT Virtual Switch)” status from the **Network Connections** window, users can see it set to IP address “192.168.1.1”



5. The Hyper-V user-configured NAT virtual network doesn't support DHCP, so PWI needs to be assigned a static IP configuration within the subnet. A static IP can be assigned through the web interface if web interface access is already available, by navigating to ***Platform Settings > Network Configuration > Ethernet Configuration*** or through the VM console by following the instructions in the Rescue Console Access - Set Static IP section.
6. Set the PWI VM's primary network to virtual switch "NAT Virtual Switch" from the Hyper-V Manager.
    a. Select Settings the select the primary network switch and change the configuration to "NAT Virtual Switch", then select click Apply.



11. At this point, the user should be able to power on and see the new static IP in the VM console. This internal IP address can be used to access PWI's web interface from the Windows host machine. Jump to the section, **Accessing the Web Interface**.
12. Setup Port Forwarding – (Port forwarding works on user-configured adapters) using Windows PowerShell.

    a. During the NAT static IP setup, users may encounter the error "**Add-NetNatStaticMapping : The process cannot access the file because it is being used by another process.**" This means port 443 is used by another process, so users need to stop that process by using command "**net stop http**" from Windows PowerShell before adding port forwarding mapping for port 443.

    b. If command "net stop http" does not fix the port conflict issue, users can run command "**netstat -aob**" from Windows PowerShell to check which process is using port 443, and stop that process from "Task Manager" before adding port forwarding map.

    ```
    Add-NetNatStaticMapping -ExternalIPAddress "0.0.0.0/24" -ExternalPort
    443 -Protocol TCP -InternalIPAddress "PWI_Internal_IP" -InternalPort 443
    -NatName "NATVirtualNetwork"

    Get-NetNatStaticMapping <== This command checks newly created port
    forwarding mapping
    ```

13. Users can now access the PWI UI with address "https://windows_host_ip" from another host using PWI's Windows host IP. Jump to section **Accessing the Web Interface.**

PWI Installation as an Edge Solution

Plantweb Insight can be delivered pre-configured onto an Emerson industrial PC as an edge compute solution. In this deployment scenario, the PWI software is imaged directly onto the Emerson hardware, running on "bare metal" which means there is no need for any underlying hypervisor software or additional hardware. The PWI Edge Solution is ideal for users who do not have host system hardware space readily available.

The PWI Edge Solution hardware platform has been tested and approved for use in most PWI deployment scenarios. PWI can also be deployed as a VM on a user-provided industrial PC if the industrial PC meets the PWI VM system requirements listed previously.

Contact your local Emerson representative for PWI Edge Solution ordering information.

PWI Edge Solution Requirements

- 24V – 2A power supply

- Web client (Google Chrome™ or Microsoft Edge™) with network connectivity to the PWI Edge Computer via ethernet connection
- Monitor with a DisplayPort++ cable for viewing the PWI console

PWI Edge Solution – Initial Startup Process

1. Power on the industrial PC (IPC) – the power button should be yellow green, not red
2. Connect a web client (browser) to the physical ethernet port "ETH0" on the industrial PC
   Default network configuration of the PWI Edge Solution:

Primary Interface	**ETH0**	DHCP, reflected on console
Secondary Interface (disabled)	**ETH2**	static IP: 192.168.254.10/24

   NOTE: ETH0 is routable and ETH2 is non-routable. ETH1 and other physical interfaces on the IPC are not used by PWI except for DisplayPort++.
3. Connect a monitor to the DisplayPort++ interface on the IPC to view the PWI console
   a. If a DHCP server is available to the IPC, an IP address should be displayed on the console for the primary network interface (eth0)
   b. If a DHCP server is not available, refer to the instructions on how to Set Static IP from Rescue Console and assign a preferred static IP to ETH0.
4. All further interaction with PWI is conducted through the web interface which is accessed through the displayed IP address. Jump to the section, **Accessing the Web Interface.**

Accessing the Web Interface

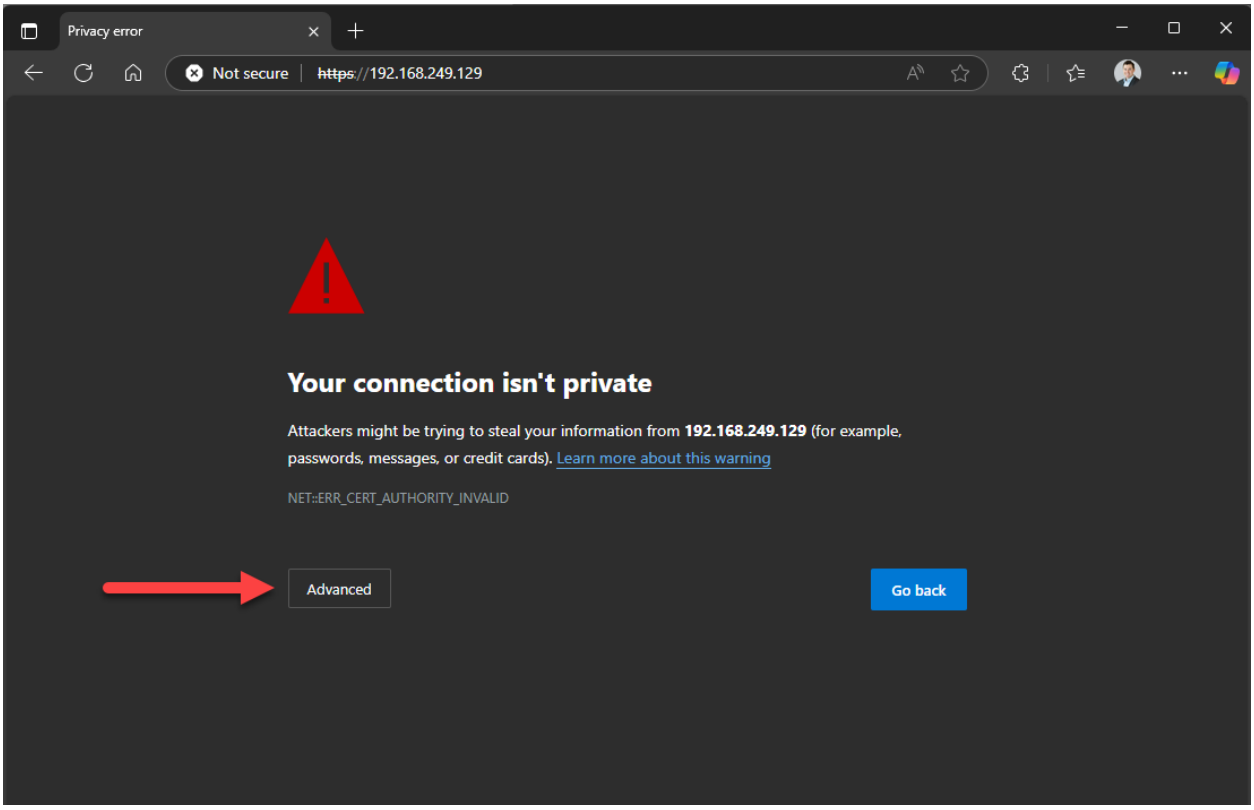
The PWI web interface can be accessed from any of the supported web browsers shown in Application Access.

Procedure

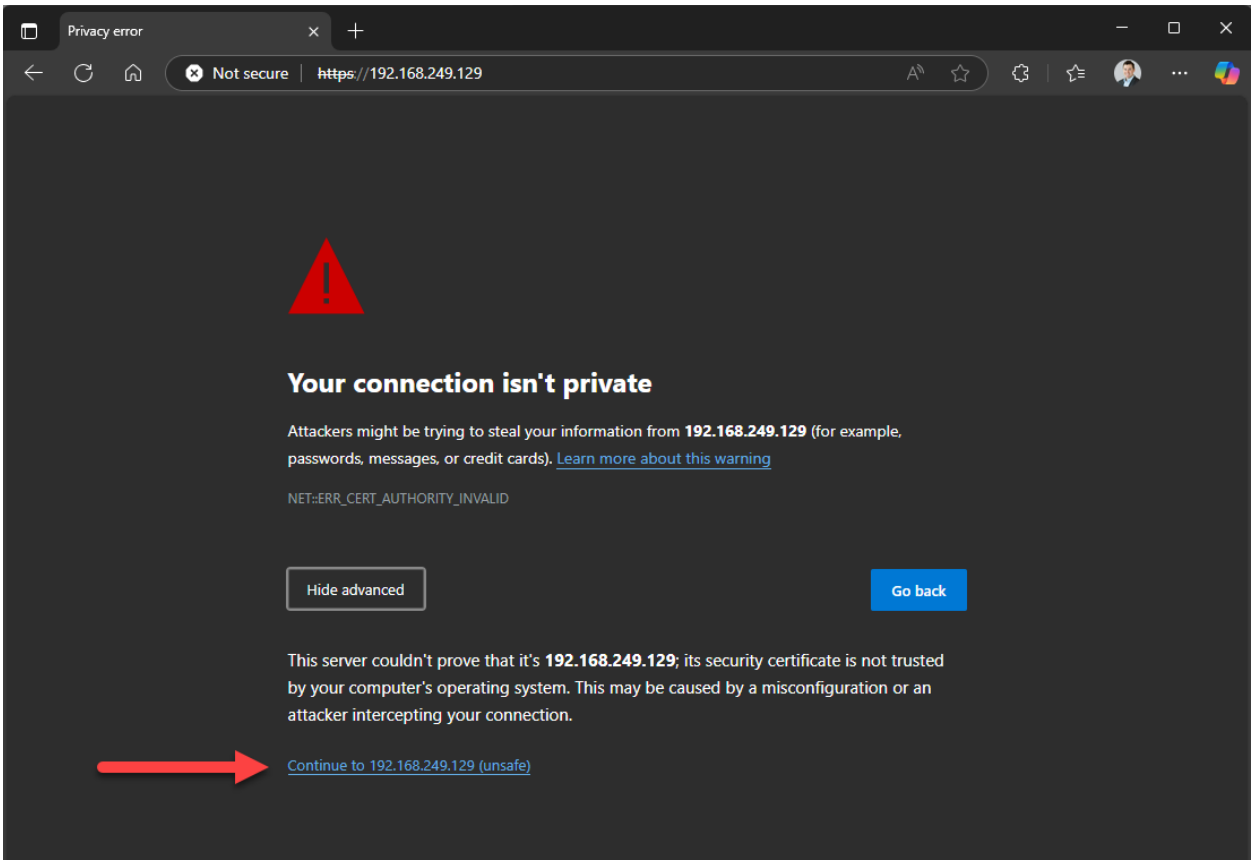
1. Open a supported web browser
2. Enter the IP address shown in the PWI console – it may take 5-10 minutes for necessary services to initialize upon first startup.

NOTE: PWI will respond to a ping command under factory configuration. Ping can be disabled from the Ports and Protocols page within PWI.

3. A security notification will appear in your browser window. This is not an error, but a certification authorization warning. Refer to the Certificate Management section for instructions on how to set up a secure (https) connection to remove this warning.
    a. Click **Advance**

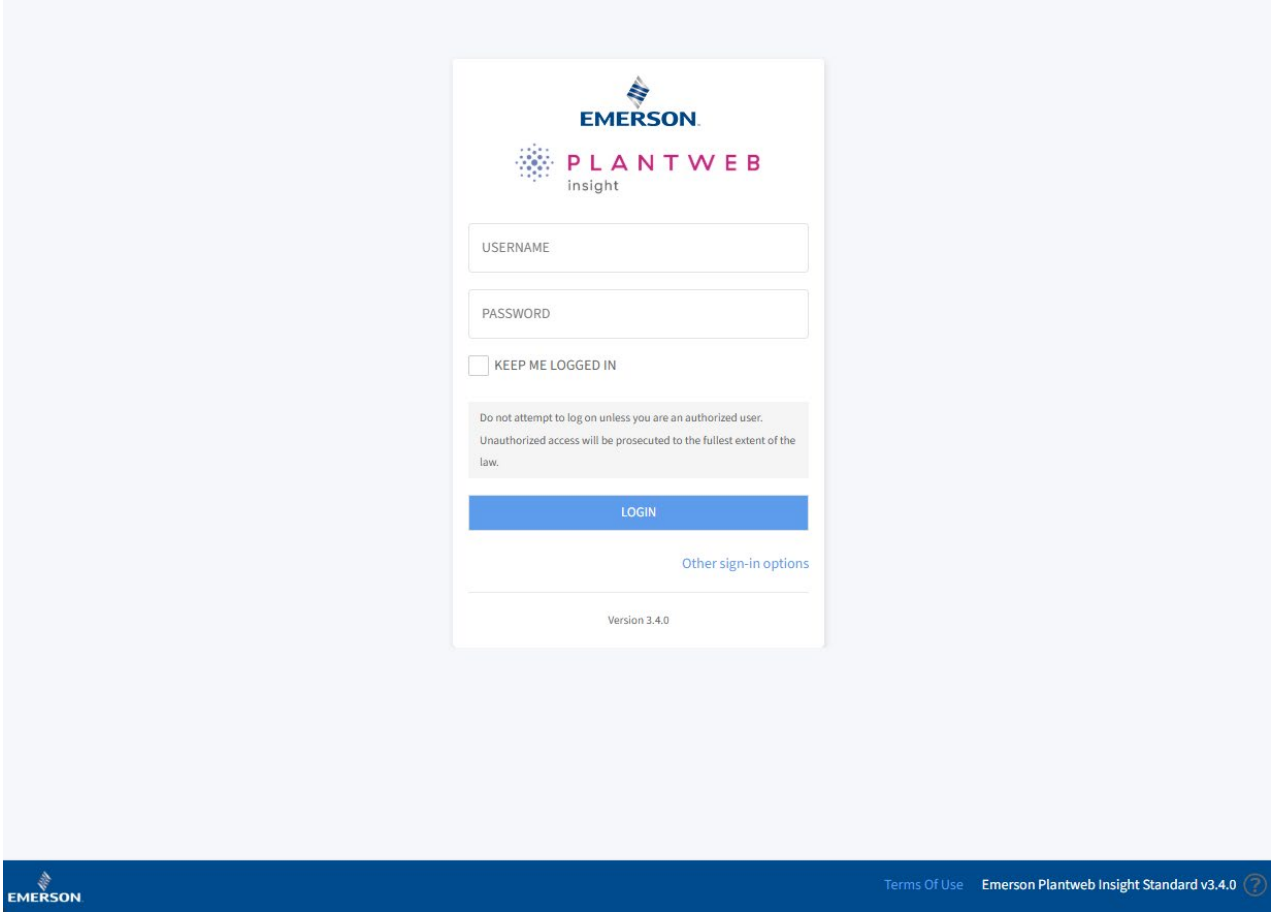


    b. Click **Proceed** or **Continue**



c. If you see a “Kong Error” or “Failed to discover Authentication options” message, wait a moment and then refresh the browser. Verify that the host system meets minimum hardware requirements.

4. The PWI log-in screen should appear.



Log in with the following default administrative user credentials:

Username: admin@emerson.com

Password: Default.1234

NOTE: Both username and password are case sensitive.

5. Users are prompted to change their password upon initial login. Change password as prompted (default settings are listed below and can be changed in ***User Settings***).

   Default password settings:

Minimum length	12
Minimum lowercase	1
Minimum uppercase	1
Minimum numbers	1

IMPORTANT: Keep login credentials in a secure location. Emerson cannot recover user-defined passwords, and there are no master-passwords. Passwords are the

user's responsibility. If a user forgets/loses all valid passwords, the PWI VM can be factory reset by re-installing the VM.

6. Log in with the updated credentials.
7. To verify the software version number, refer to the bottom right corner of the user interface. If a PWI platform upgrade is available, refer to the next section.

Install a Version Upgrade

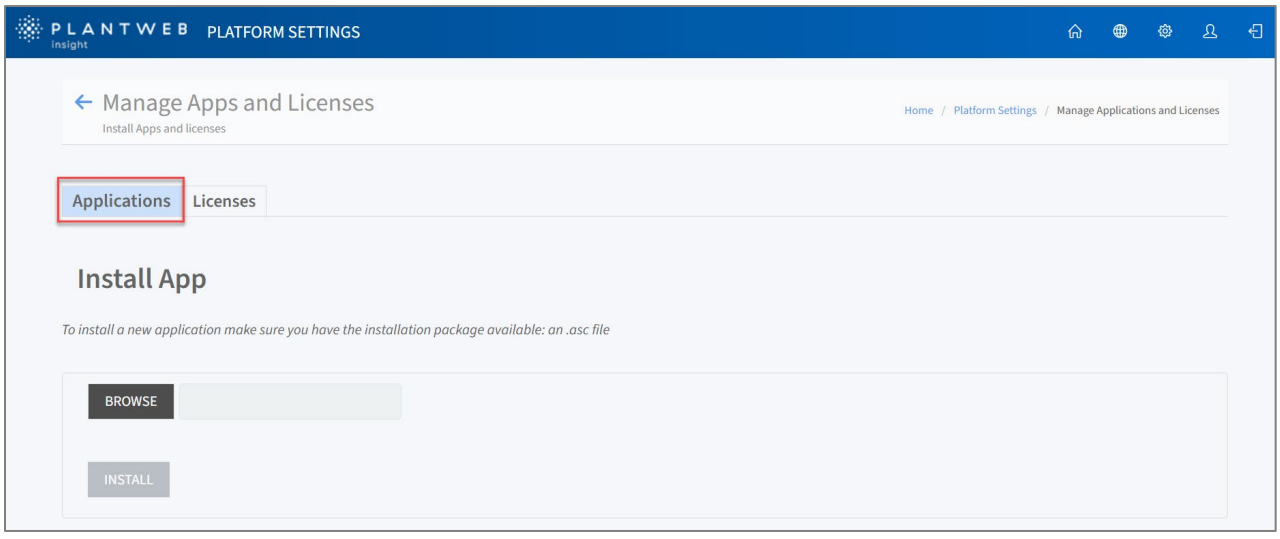
There are two types of PWI platform version upgrades:

- **In-place system upgrade** - this is a .ASC file that can be applied to an existing PWI system without disrupting the existing system.
- **Disruptive system upgrade** – these types of upgrades are rare and are typically associated with an underlying OS replacement. Disruptive upgrades require deployment of a new PWI system, where users must capture a backup from their existing system and restore it into the new system.

PWI platform version upgrade types are denoted in the Plantweb Insight Release Notes.

In-Place Upgrade Procedure

1. Download latest PWI upgrade bundle and refer to Plantweb Insight Release Notes for required upgrade paths, depending on current PWI version.
2. In PWI, navigate to the  (gear wheel) icon and go to ***Platform Settings*** > ***Manage Applications and Licenses*** > ***Applications*** tab



3. Browse for the platform upgrade bundle (.asc file).
4. Click **Install**.

Once the upgrade bundle has finished loading, PWI will prompt the user to log out and log in for the upgrade to take effect.

Disruptive Upgrade Procedure

For disruptive upgrades, refer to the appropriate Installation section and then refer to Restorable Backup section and Restoring from a Previous System section.

For disruptive upgrades with PWI Edge Solutions, please contact PWI Technical Support for assistance: PWI Technical Support Request Link

5. Configuration

Overview

This section contains information on customizing system settings and configuring PWI to the network and other systems.

Most customer configuration settings are optional. However, valid data sources and network connectivity to these sources are required for PWI applications and services to function properly. If you are unsure about network configuration settings or system architecture, please consult with your local Emerson Solutions Architect.

If you are restoring from a previous PWI system, refer to Restoring from a Previous System.

Editing of any PWI platform setting requires a user to be assigned an Admin role at the platform.

Network Configuration

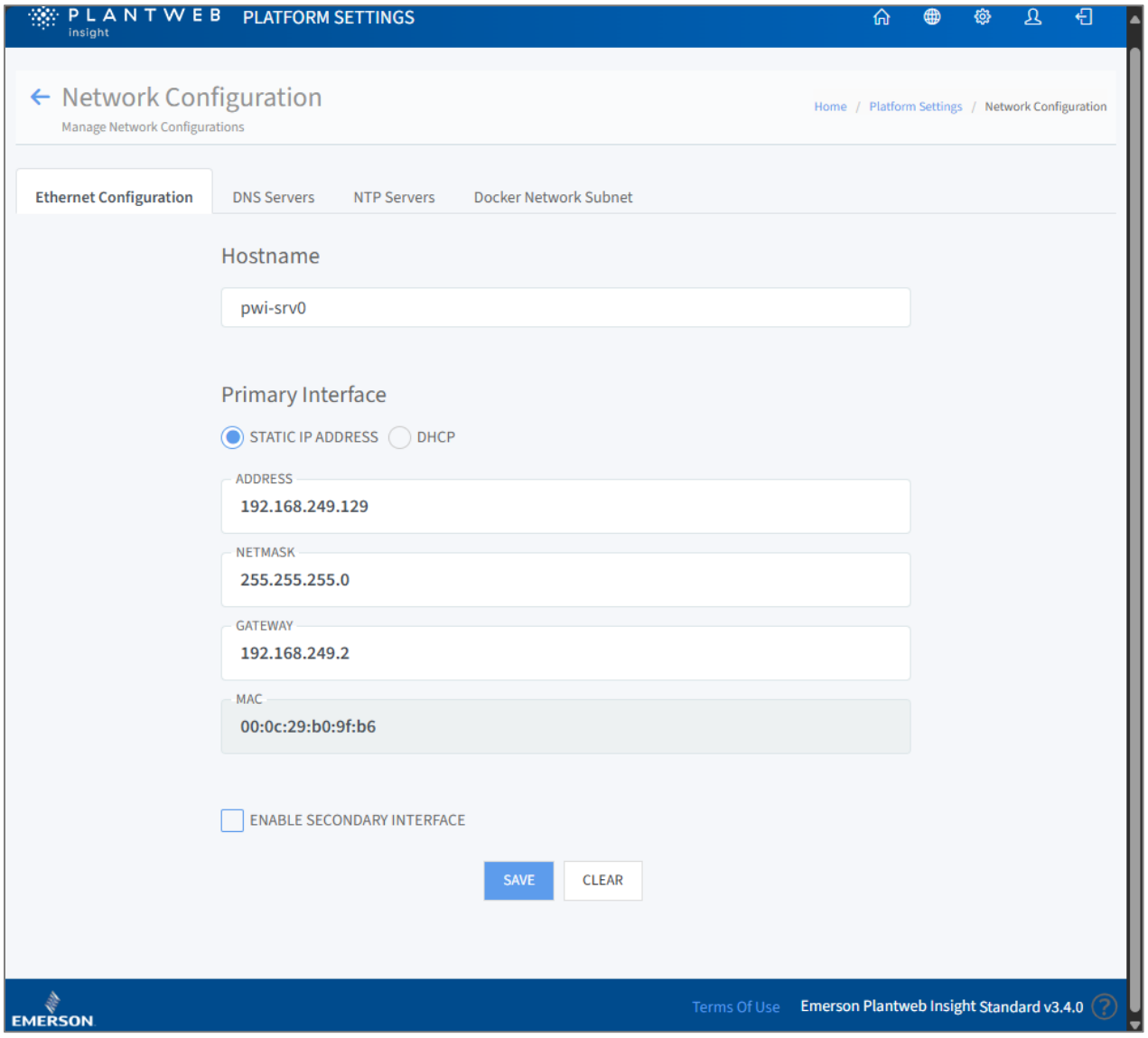
NOTICE: Exercise caution when modifying Internet Protocol (IP) network settings. If settings are lost or improperly configured, it may be difficult to access the application. Contact the system administrator for information on the proper IP network settings to apply. **Changing IP settings will invalidate any existing licenses installed in the system.**

PWI features two network interfaces. The primary interface (eth0) is associated with network adapter 1 of the virtual machine (VM). The secondary interface (eth1) is associated with network adapter 2 of the VM.

Procedure

1. From the PWI home screen, navigate to ***Platform Settings > Network Configuration > Ethernet Configuration***

2. From the ***Ethernet Configuration*** screen, users can manually assign a preferred host name and IP address to the system.
3. Enable the secondary interface, if required, and assign an IP address.



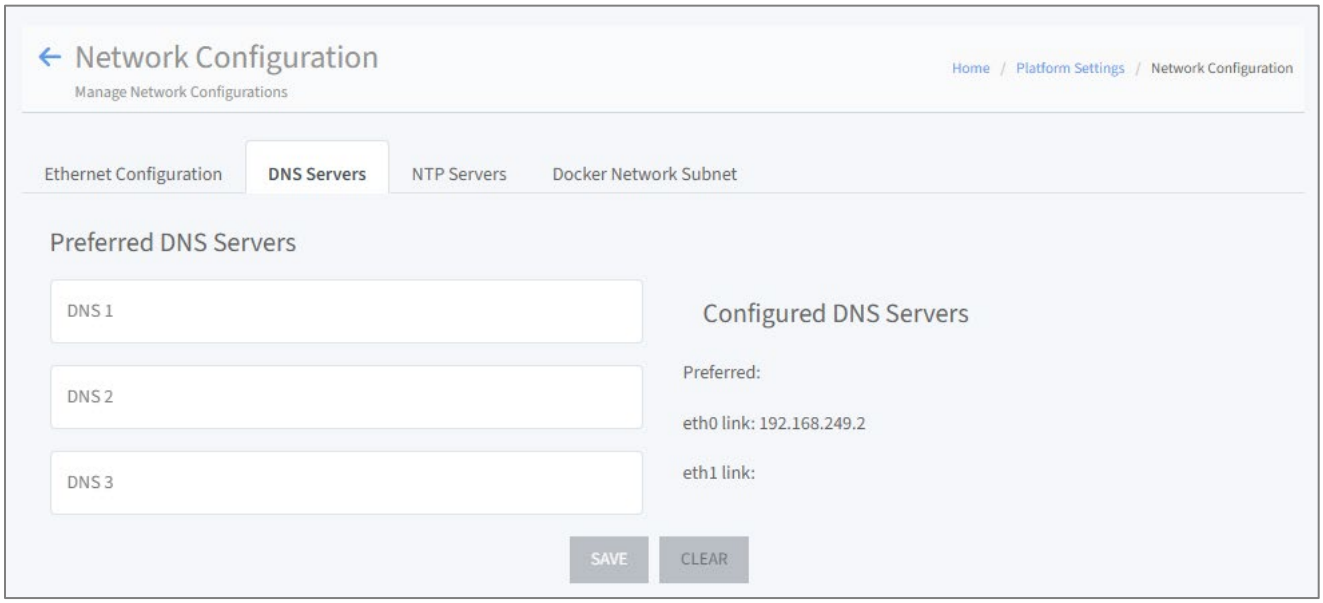
If using a DHCP server, Emerson recommends setting up static IP addresses or sticky IP addresses.

Most deployments use a single eth0 (primary) setup. Some deployments may segregate networks into eth0 (primary) and eth1 (secondary) for separate web interface access and data source access.

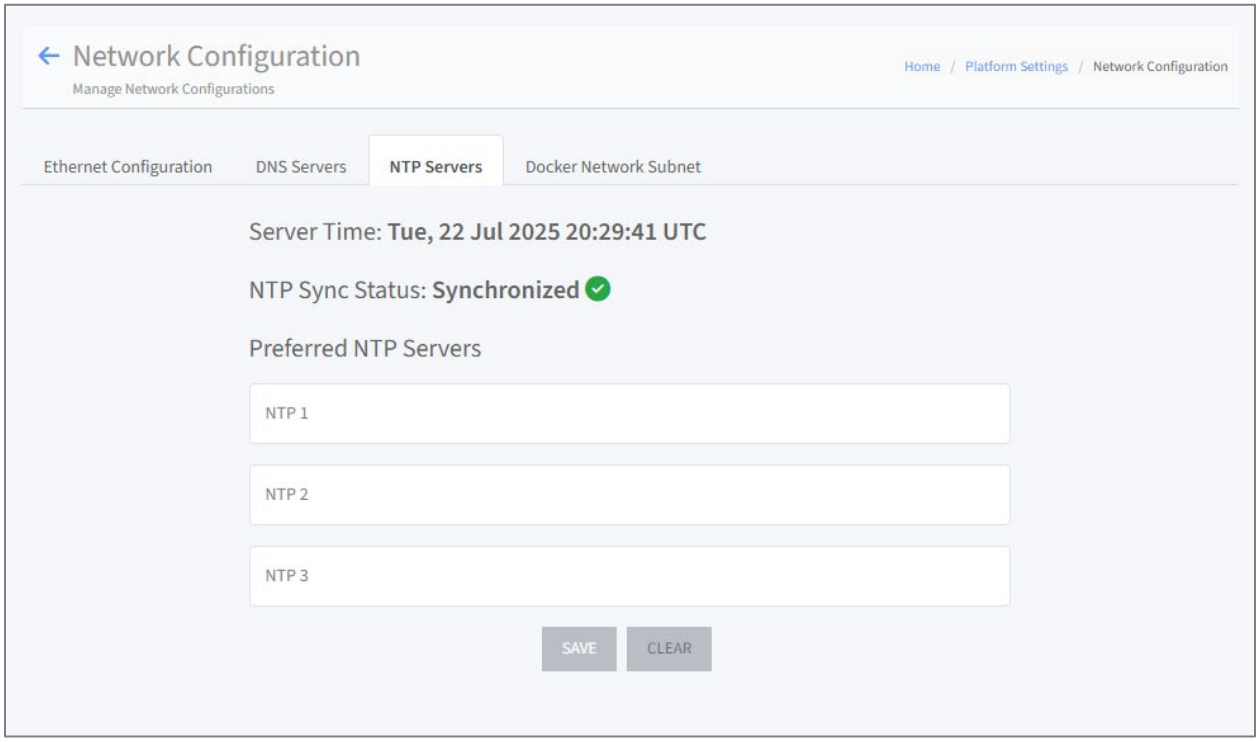
NOTE: PWI's internal Docker network resides on the **172.18.X.X** subnet. Assigning a static IP with this same subnet to either of PWI's network adapters will cause IP addressing conflict.

NOTE: Eth1 (secondary) is a non-routing network.

4. Navigate to ***Docker Network Subnet*** to assign the internal Docker network to a different subnet, if required
5. Navigate to ***DNS Servers*** to assign preferred DNS servers.



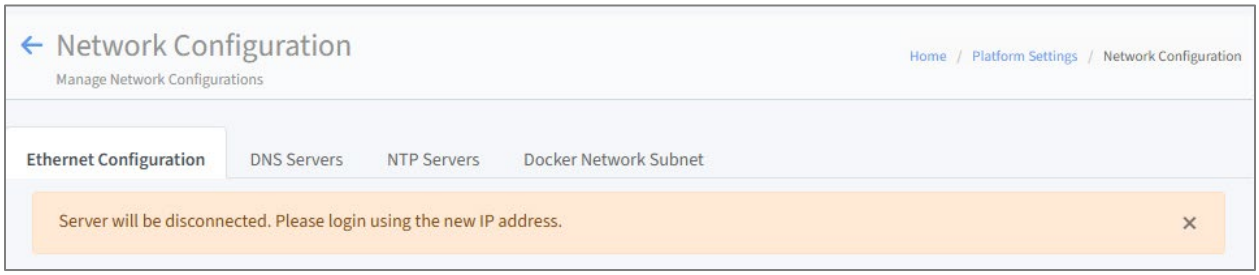
6. Navigate to ***NTP Servers*** to assign preferred NTP servers.



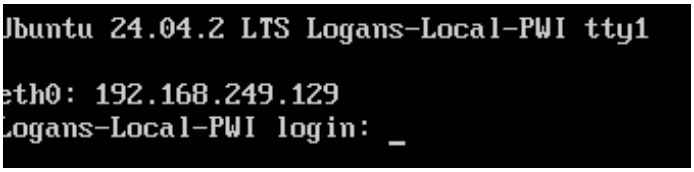
NOTE: PWI should have time synchronization enabled on the VM. It is necessary to sync PWI with an NTP server or at least use the internal NTP service for this purpose.

All PWI applications present event timestamps in local time based upon the user's web browser settings.

7. After Network Configuration changes are saved, the system prompts the user to disconnect.



8. Reboot the VM or restart the IPC for the IP changes to take effect. To restart the IPC, press and hold the power button for 5 seconds to properly power off the IPC.
9. After the changes are applied, the VM console displays the new host name and/or new eth0 (primary) IP address.



Location Hierarchy

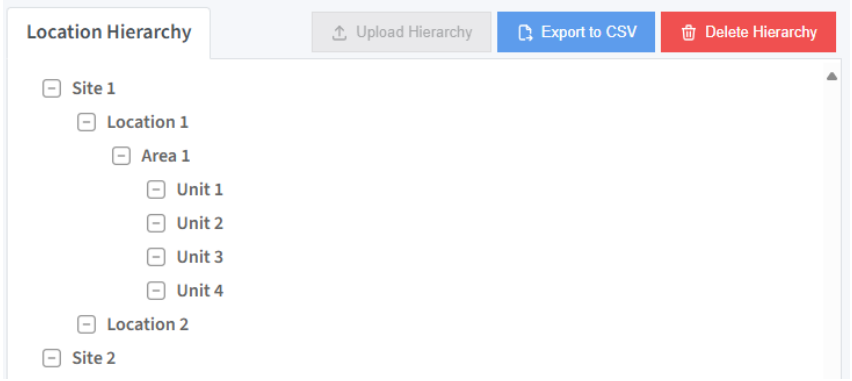
A flexible hierarchy configuration was introduced in PWI v3.2.0. This feature allows users to define their own location hierarchy that is specific to their PWI system. The location hierarchy is defined at the PWI platform and shared by applications and other services. The location hierarchy feature is used to provide location details to the applications. Users can then assign assets to these common locations. The location hierarchy is used to filter application screens by location, assign user access by location, and assign user roles by location. The location hierarchy also plays a key role in configuring alerts in each application.

The location hierarchy is defined through a .CSV file upload. The .CSV file can be prepared externally and uploaded into PWI. Each column represents a location node. The left column is the parent while the right columns are child nodes.

In the following example, for the location nodes, "Site" is the parent and "Location" is a child.

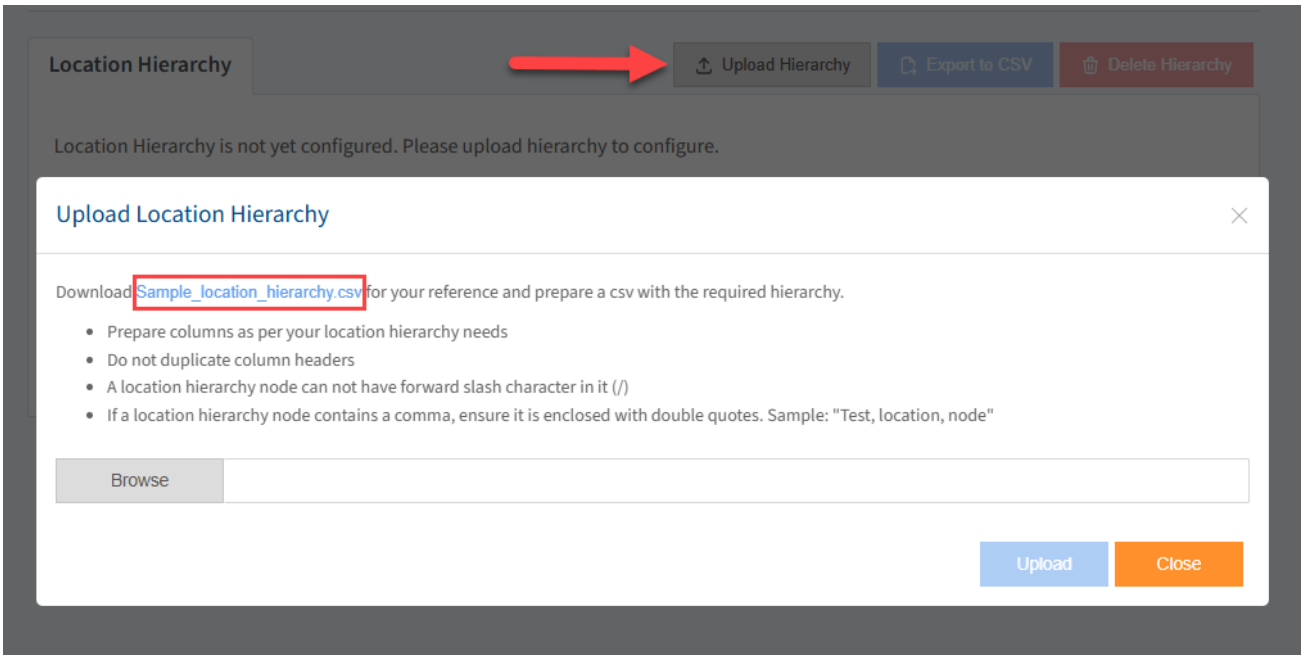
Location Hierarchy in CSV	Location Hierarchy shown in PWI

	A	B	C	D
1	Site	Location	Area	Unit
2	Site 1	Location 1	Area 1	Unit 1
3	Site 1	Location 1	Area 1	Unit 2
4	Site 1	Location 1	Area 1	Unit 3
5	Site 1	Location 1	Area 1	Unit 4
6	Site 1	Location 2		
7	Site 2			



Creating a New Location Hierarchy

1. Navigate from the home screen to ***Platform Settings > Location Hierarchy***
2. Download the sample hierarchy .CSV by clicking the "**Upload Hierarchy**" button and then download the Sample_location_hierarchy.csv file



3. Edit the sample location hierarchy .CSV file as needed. Below are guidelines for creating a location hierarchy:
   - No minimum number of columns required
   - No minimum number of rows required
   - Do not duplicate column headers

- A location hierarchy node cannot have forward slash character in it (/)
- If a location hierarchy node contains a comma, ensure it is enclosed with double quotes. Sample: "Site, Area, Location, Unit"
- All nodes must have a parent node
- Child nodes are optional
- Refer to the ISA-95 Equipment Model for guidance on creating a sufficient location hierarchy

4. Upload your location hierarchy into PWI by clicking the "**Upload Hierarchy**" button and browsing for your .CSV hierarchy.
5. Once the hierarchy is uploaded, the user must review and confirm that the hierarchy meets their needs by clicking the **"Continue"** button to save the hierarchy.
   CAUTION: Failing to click **"Continue"** will fail to save the uploaded hierarchy.

Editing an Existing Location Hierarchy

1. As an Admin user, navigate from the home screen to ***Platform Settings > Location Hierarchy***
2. Click the **"Export to CSV"** button to download the existing hierarchy
3. Open and edit the downloaded .CSV hierarchy as needed and save the file
4. In the PWI Location Hierarchy page, click **"Delete Hierarchy"** to allow upload of a new location hierarchy.
   NOTE: Deletion of an existing location hierarchy will unlink any associated assets or permissions. All unlinked assets will be grouped under an "Unallocated" category until valid locations are available again. If asset locations are no longer available after a new hierarchy upload, those assets will need to be re-assigned to valid locations.
5. Upload your location hierarchy into PWI by clicking the "**Upload Hierarchy**" button and browsing for your .CSV hierarchy.
6. Once the hierarchy is uploaded, the user must review and confirm the hierarchy meets their needs by clicking the **"Continue"** button to save the hierarchy.
   CAUTION: Failing to click **"Continue"** will fail to save the uploaded hierarchy.

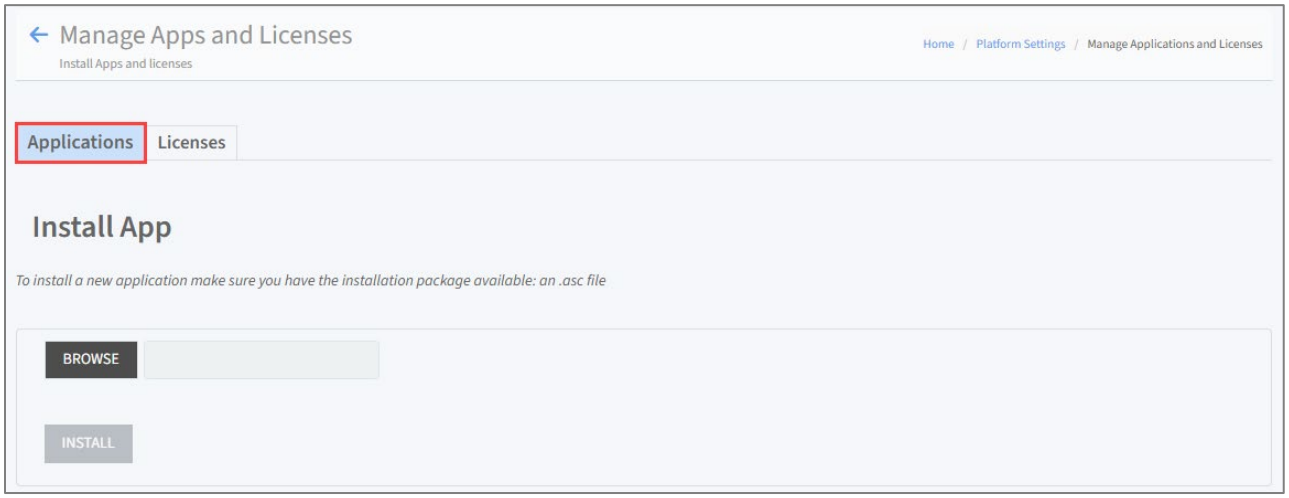
Application Installation

Overview

This section will provide basic instructions on installing PWI application files. Application files can be installed before or after license files. However, a valid license is required to access an application once it's installed. Refer to individual PWI application user manuals for specific configuration details.

Procedure

1. Ensure application files have been downloaded and are available to PWI. Refer to Downloading Plantweb Insight Software for instructions on how to download applications.
2. Navigate to ***Platform Settings > Manage Applications and Licenses > Applications*** tab



3. Browse for application .ASC file
4. Click **"Install"** button. Once the application has finished installing, the system will prompt the user to log out and log in for installation to be completed. Multiple application files can be installed before user logs out and logs in.

Backup and Restore

System backup capability

PWI has the ability capture a backup of its data and configuration content. There are two types of backups, depending on the purpose of the backup.

- **Diagnostic Backup** (available in all versions of PWI)
- **Restorable Backup** (available in v1.6.x, v2.1.5, v2.4.0 and later)

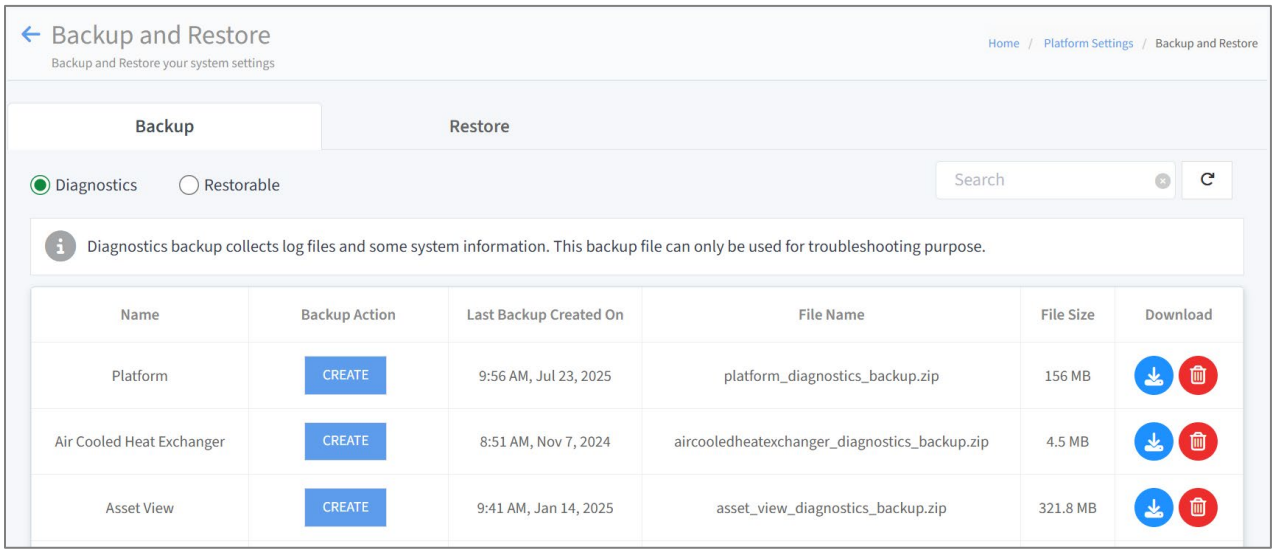
A backup of either type can be performed for either the platform and/or specific application(s). This activity can be performed by administrators from within the PWI user interface by navigating to ***Platform Settings > Backup and Restore > Backup***

Diagnostic Backup

When there are issues observed with a PWI system, users can choose to take a diagnostics backup of the platform and applications. The diagnostic backups will contain necessary

details to help with diagnosing issues and can be shared with Emerson for troubleshooting purposes. All these details are zipped and encrypted with a user-generated password at the time of backup file download. The downloaded file content can only be viewed by extracting it with a valid password.

Platform Settings > Backup and Restore > Backup - Diagnostics



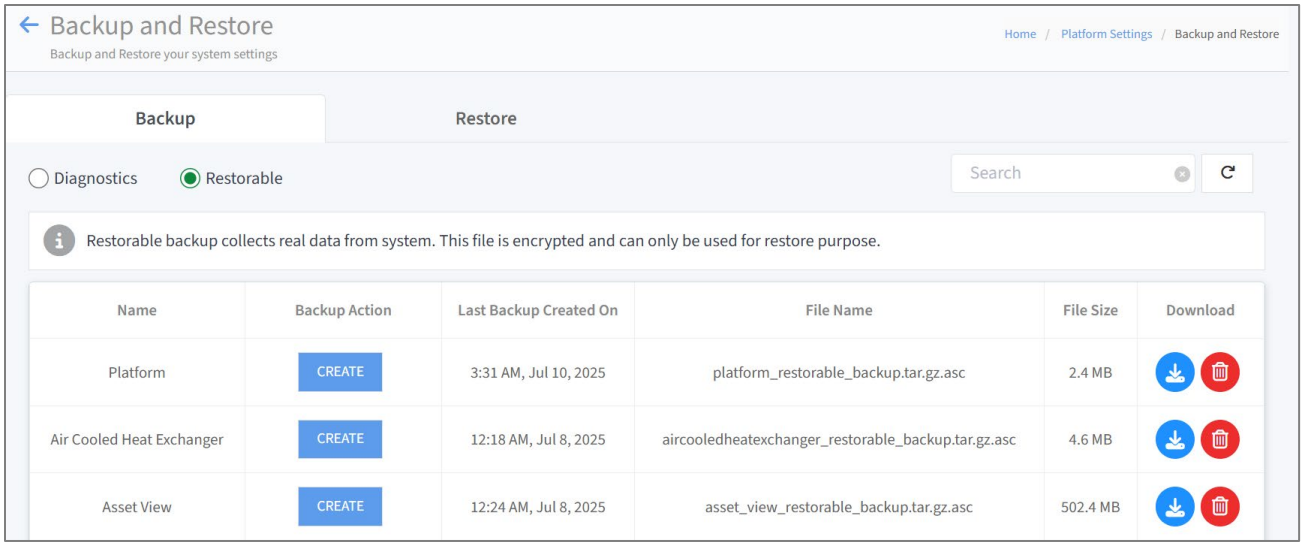
Restorable Backup

A restorable backup will gather specific data which is meant for system restoration purposes. For application backups, the application's manifest file will decide what content to be considered for restorable backup. All these details are zipped and encrypted with a user-generated password at the time of download. On top of this, the platform will also sign the backup bundle to ensure the integrity of the backup file. This backup file can be downloaded by a user, but a user cannot view the contents of it.

The restorable backup functionality within PWI was developed for migrating from one PWI system to another, such as with disruptive upgrades. It was not necessarily intended to be a disaster recovery solution. Refer to the System Recovery section for more information on recommendations for disaster recovery solutions.

The restorable backup is meant to be restored on a PWI system only. At the time of restoration, the user is required to input the password of the file to allow reading its contents.

Platform Settings > Backup and Restore > Backup - Restorable



The following configuration settings are included in the restorable backup:

Setting name	Sub menu	Included in Restore?	Reason
Data Sources	Gateways	Yes	
	OPC UA servers	Yes	
	Modbus servers	Yes	
	MQTT Sources	Yes	
Protocols and Ports	Ports & IP whitelisting details	Yes	
Active directory	AD server configurations	Yes	
SSO	SSO settings	Yes	

SMTP Settings	Server configuration	Yes	
	Sent Email history	Yes	
Modbus Mapping	Mappings file	Yes	
Users	User accounts	Yes	
	Password options	Yes	
	API Keys	**No**	API keys are dropped during the restore process. This ensures that the same API keys are not being used by multiple machines to access the APIs.
	Login and Session options	Yes	
Ethernet Configuration		**No**	Ethernet configuration is not considered for restore. If PWI assigns the same hostname/static IP to new system, there could be an IP/Host conflict, and both systems could risk unavailability.

Certificate management	Default SSL cert	Yes	
	User provided SSL cert	Yes	
	Peer Cert	Yes	
Manage Applications and Licenses	Installed Apps	**No**	Applications have their own restorable backups
	Bundle upgrade history	**No**	Bundle installation history is dropped, and new tracking begins on the new system.
	Installed Licenses	**No**	Licenses are tied to the locking code, and the locking code is unique to each PWI system
	License Installation History	**No**	License installation history is dropped, and new tracking begins on the new system.
Remote Audit Syslog	Configuration settings	**Yes**	
Location Hierarchy	Configuration	**Yes**	
Antivirus	Latest scan, infected files, scan history	**No**	Not relevant to new PWI system which backup is being restored to

	Scheduled scan settings	**Yes**	

License validity cannot be included in backup/restore since the PWI locking code is unique to each system instance. Users should work with the PWI license team at PlantwebInsight.SoftwareRequests@Emerson.com to ensure efficient delivery of replacement license keys.

Restoring from a previous PWI system

Restore capability is supported by PWI to move a complete PWI system from one virtual machine or edge solution to another. The following are scenarios where a user may need to utilize PWI's backup/restore functionality:

- A PWI platform release is non-backward compatible (disruptive upgrade)
- A user decides to upgrade to a later version of PWI for increased disc size
    - PWI introduced VM disc size increases in v3.0.0 and v3.2.0
- A user needs to relocate the PWI system to a new host

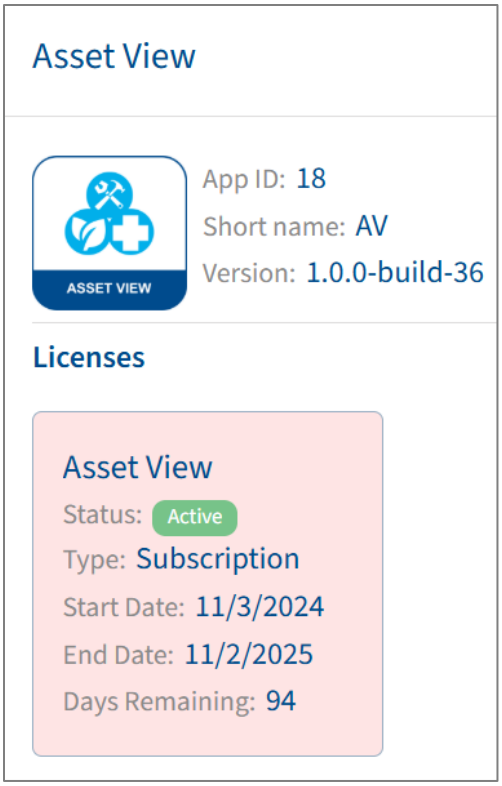
Refer to the PWI Platform Release Notes for version release details and upgrade paths to the latest version.

NOTE: For each PWI release, restoration from the most recent PWI version(s) available at that point in time is supported. Supported version details are captured in the PWI Platform Release Notes. Please contact PWI Technical Support if restoring a backup from an older, unsupported version.

Save a Restorable System Backup (Source/Old PWI System)

1. Navigate to ***Platform Settings > Backup and Restore > Backup > Restorable***
2. Create a restorable backup of the platform and each installed application and then download each backup file

   NOTE: Keep safe record of backup file passphrase(s) to ensure successful restore.
3. It is recommended that users also take a screen grab of their existing PWI license details by navigating to ***Platform Settings > Manage Applications and Licenses > Licenses*** and then clicking on each application card for license details.



Restore a System Backup (Destination/New PWI System)

When a restore operation is performed, any existing data or user accounts on the new PWI system will be replaced with the system data and configuration content of the backup (old) system.

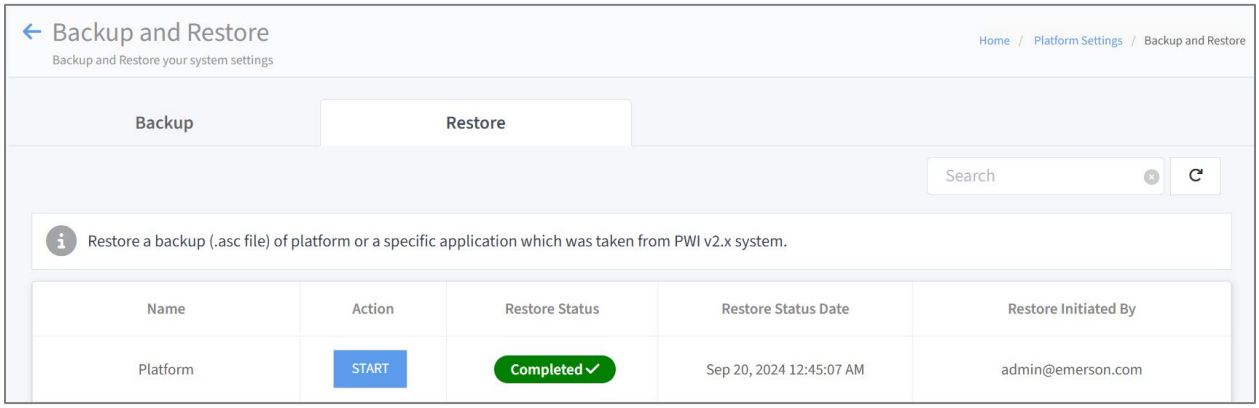
NOTE: PWI platform backups cannot be restored across different deployment modes. Backup and restore operations are only supported within the same PWI deployment mode.

1. Install latest PWI virtual machine or edge solution according to instructions in Installation section and login through the web interface using the default admin account credentials.

   CAUTION: If restoring from PWI 3.3.0, please make sure no OPC-UA servers are configured to the new PWI system while performing a restore operation. If servers are already configured, OPC-UA server data from the restorable backup will not be restored.

   NOTE: OPC-UA variables will be included in the variables dashboard once application data is restored, as long as the referenced OPC-UA server is already present in the PWI system.

2. Navigate to ***Platform Settings > Backup and Restore > Restore*** and click the "START" button to restore the platform backup



3. After restoring the platform, the user will be logged out and required to re-login. The user should then login using credentials from the source/old PWI system that the backup was taken from.

4. Perform required manual steps such as ethernet configuration, certificates, API keys, etc.

    a. If a user decides to keep the new dynamic IP assigned, the new IP address should be updated with any external clients such as external OPC-UA, Modbus, SMTP, Audit Log clients or AMS Optics

    b. Refrain from configuring the same IP address to both old and new PWI systems to avoid IP conflicts over network. Either assign a dynamic IP to the older system or shut it down before allocating the same static IP to the new PWI system.

    c. Recreate API keys that are shared with external systems such as AMS Optics by navigating to ***Users > Manage Access > API Keys***

5. Verify connectivity has re-established to all data sources (Gateways, OPC-UA or Modbus servers, MQTT sources) by navigating to ***Data Source Config > Gateway Settings / OPC UA Servers / Modbus Servers / MQTT Sources***

6. Install the latest versions of required applications

7. Install replacement licenses for applications and any platform features

8. Restore application backup files one by one

User Accounts

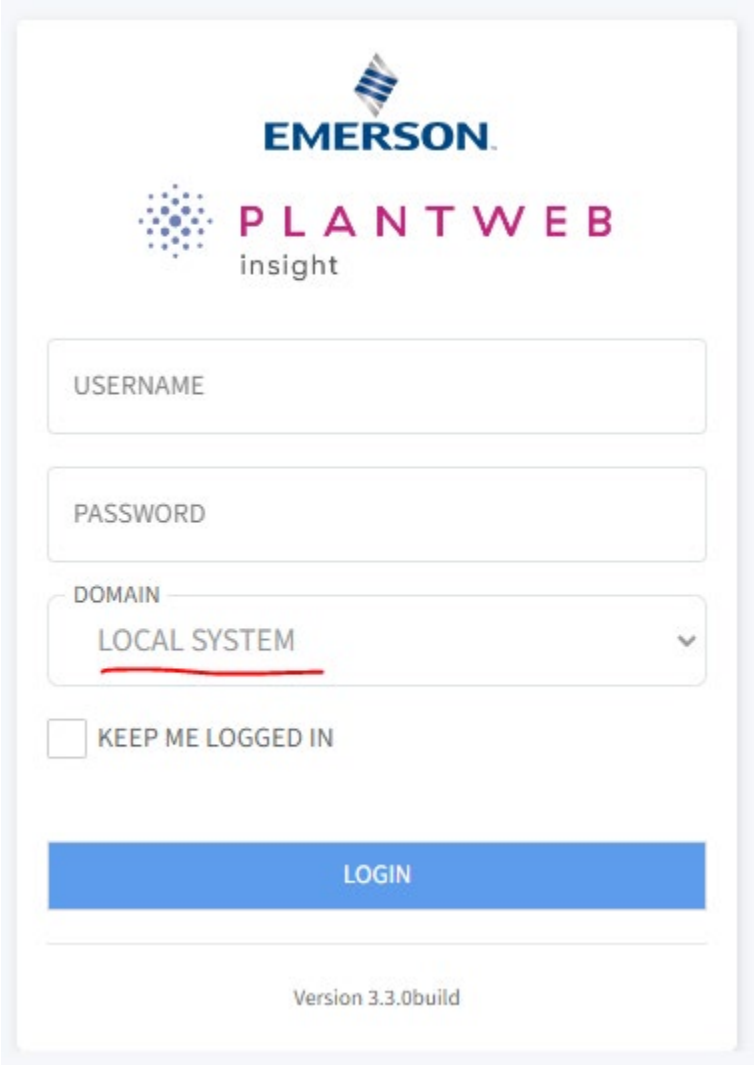
The PWI platform currently supports two user roles:

Role	Permissions at PWI platform
Admin	Read and write
User	Read-only

Some applications support custom roles. Users can have different roles in these applications from their platform role. Refer to the User Access Management (Authorization) section for more details on assigning application roles.

Adding Local User Accounts

If multiple authentication methods are available, PWI's login screen will default to the local user database.



Upon entering valid credentials, users are brought to the Home page with accessible app icons displayed. PWI maintains all usernames and their password hashes in the system and authenticates logins.

The following are actions permitted on local user accounts:

- Maintain local users (allowed by platform admins)
    - Add/Update/Delete accounts
    - Lock a user account
    - Change a user's password
- Set password rules (allowed by platform admins)
- Change their own password (allowed by all users)

Procedure

1. From the home screen, navigate to the ***Users*** icon  ***> User Settings > User Accounts***
2. Click **"Add User Account"** button
3. Enter email and password, then click **"Save"**. Users will be prompted to change their password upon initial log in.

   Checking the "Locked" box will suspend the users account until it is unchecked by another admin user.
4. Once all user accounts have been created, jump to Managing User Access section to assign access permissions.

Managing Local User Accounts

To add, edit, lock, or delete a user account:

1. Navigate to ***Users > User Settings > User Accounts***
2. Search for the user account(s) to be managed
    a. To edit a user's account, click the edit icon  next to the user account. Admin users will need to enter their password to change another user's password.
    b. To delete a user, click the discard  icon next to the user account.

Password Options

Admin users can edit password requirements for all users. These settings include:

- Password limitations and requirements
- Account locking details

To edit password requirements, navigate to ***Users > User Settings > Password Options***

Default password settings:

Minimum Length	12
Minimum Lowercase	1
Minimum Uppercase	1
Minimum Digits	1
Minimum Symbols	0
Maximum Password validity	60 days
Password history depth	3
Password Failure Lock	Yes
Password Failure Limit	15
Password Failure Waiting Time	1 minute

Active Directory Configuration

Admin users can configure their LDAP servers to authenticate PWI users instead of creating local user accounts.

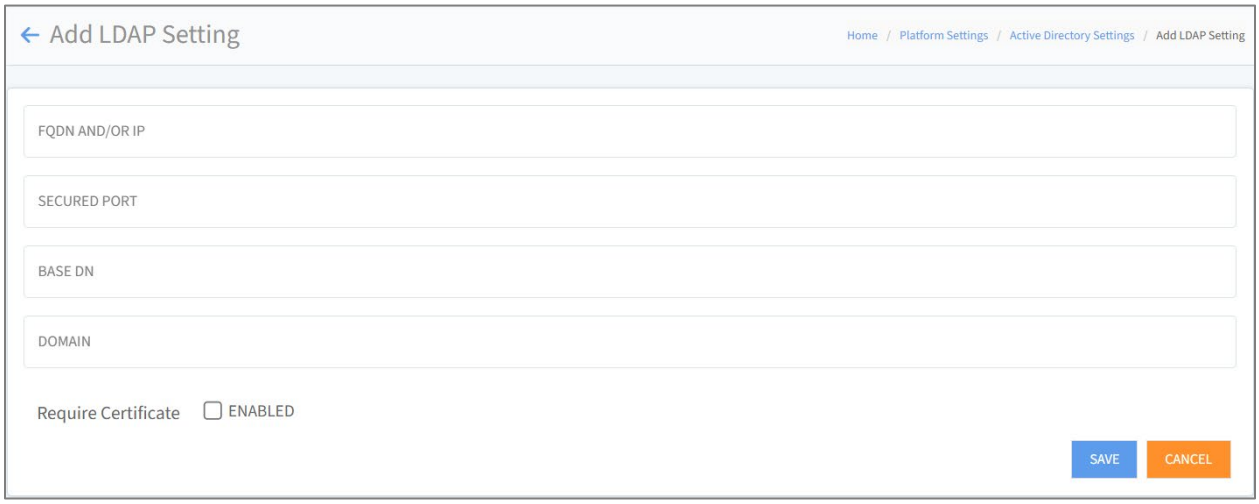
From PWI v3.3.0 and later, LDAP-based logins will allow users to authenticate into a PWI system, but specific access permissions must be assigned manually within PWI through the Manage User Access menu.

NOTE: PWI does not currently support the integration of active directory user groups. This is because PWI allows for very granular user access management within the system itself. Admin users can assign user access by application, location, and role within PWI.

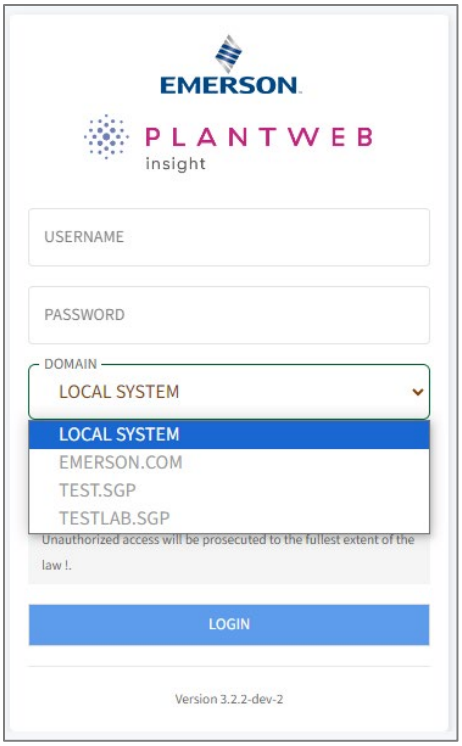
Procedure

1. From home screen, navigate to ***Platform Settings > Active Directory***
2. Click **"Add LDAP Setting"** button
3. Enter the required Active Directory details
    a. IP address (recommended) or FQDN
    b. Secured Port
    c. Base DN

d. Domain (this must be the domain of the userPrincipalName e.g. john.doe@**example.com**)
e. Certificate requirement
   NOTE: PWI active directory configuration does not require a certificate exchange as it is an anonymous TLS transaction (no certificate authentication but encrypted request). If "Require Certificate" is enabled, the LDAP server does not require a certificate for client authentication, but the LDAP server root CA cert should be uploaded to the PWI trust store (**Platform Settings > Certificate Management > Peer Cert**).



4. Click **"SAVE"** button
5. A maximum of 4 active directory settings can be configured to PWI.
6. Loggin in as an Active Directory User
   a. Login with PWI username as UserPrincipalName (john.doe@example.com)
   b. Login with username as sAMAccount (john.doe)
   c. User must select which Active Directory server they are logging into



General Tips for PWI Integration with Active Directory

- Users should connect over port 636 which is the standard secure port. This also means user's AD server should allow for a secure connection.
- Emerson recommends using an IP address rather than a FQDN for LDAP (if a load balancer is used, try to get the IP of one of the AD servers. The load will be quite small for PWI usage. Issues have been observed around resolving a FQDN.
- Once LDAP is set up, users sign in with their AD username (it has been observed that some systems require the full name while others will need your domain/username)
- Change log on domain to same domain PWI is on if experiencing issues

PWI Active Directory Error Messages

"Authorization Failed" = password or username is incorrect

" You do not have access to this system. Please contact administrator to get access. " = the user that is trying to login has not been granted any level of access to the system by their administrator

"LDAP Server Port is unsecure" = Error occurred during LDAP connection: read ECONNRESET

“If set Require Certificate and LDAP server key is too weak” = Error occurred during LDAP connection: Authentication failed. <FQDN> Server certificate key is too weak.

“If set Require Certificate but not upload server Root CA” = Error occurred during LDAP connection: unable to verify the first certificate

Single Sign On (SSO) Configuration

Overview

Single Sign On (SSO) is supported from PWI v3.4.0 and later. The capability allows users to utilize their organization’s authentication server and launch PWI without needing to re-enter their credentials.

Inputting credentials is handled by the SSO process based on the trust of the device from which PWI is being accessed. Workstations that have joined their organization’s domain will be allowed direct access to PWI with SSO.

SSO Options in PWI

1. **None**

By default, SSO is disabled in PWI. In this case, local user account authentication is applicable. Users are initially required to enter their local credentials known to the PWI system to begin configuring SSO options.

Existing LDAP capability remains unchanged. Users can still choose to configure LDAP servers and use their active directory for authentication into their PWI system.

2. **SSO with Microsoft Entra ID (formerly known as Azure Active Directory)**

MS Entra ID-based SSO allows users to access their PWI system over their corporate intranet as well as the internet. When accessed from within a corporate intranet, SSO performs a seamless authentication with tickets. However, when accessed over internet, SSO requires company credentials validated against MS Entra ID and allows users to access PWI upon successful verification.

3. **SSO with Kerberos**

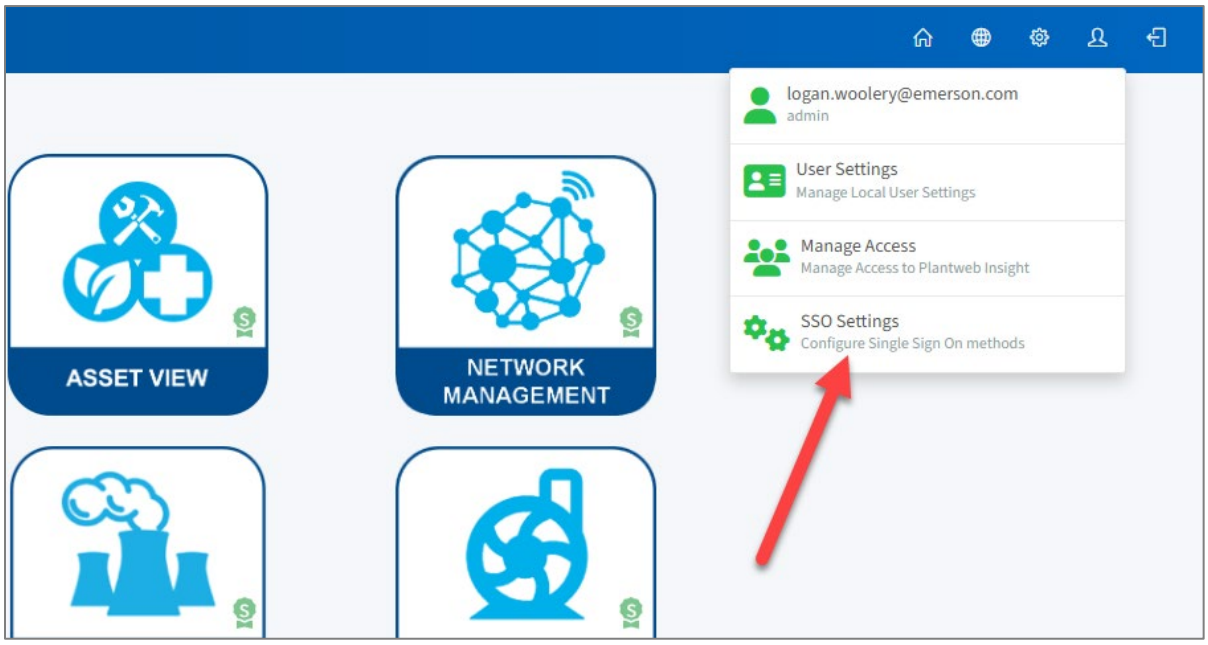
Users may choose Kerberos-based SSO if they are accessing PWI within their corporate on-premises domain. This option still allows users to access PWI without the need to enter any credentials. There is a background process of acquiring a KDC service ticket and verifying

it, but this happens without users noticing and appears to as a seamless authentication method.

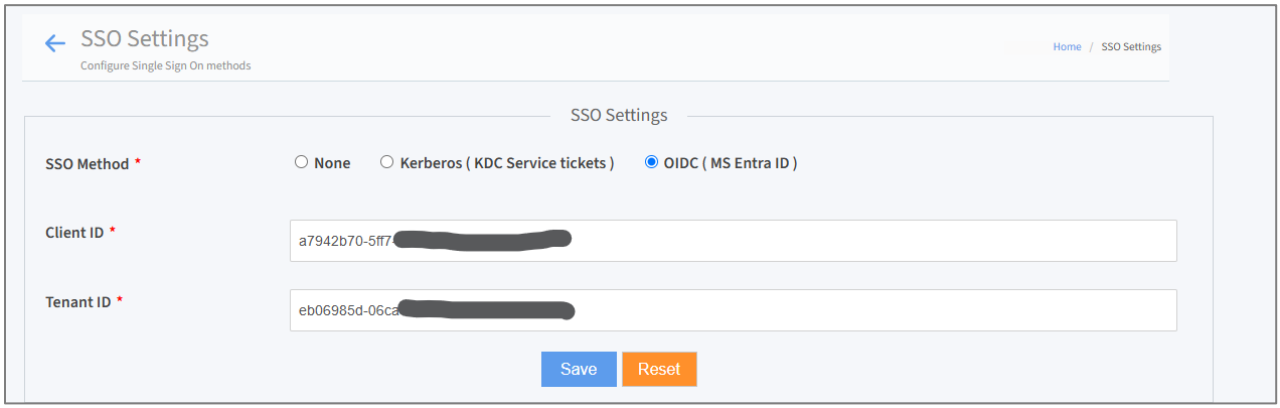
If a user tries to access PWI from a workstation which has not joined their domain, the system will fail to authenticate the user due to a failure in the ticket verification. Users must use other sign-in options in this case.

Procedure for SSO with Microsoft Entra ID Tokens

1. Users can configure SSO by navigating to ***Users > SSO Settings***



2. Select the **OIDC (MS Entra ID)** radio button



3. Enter **Client ID** and **Tenant ID** in UUID format. Once you've registered an application with Entra ID, you can get them from the overview section of app registration.

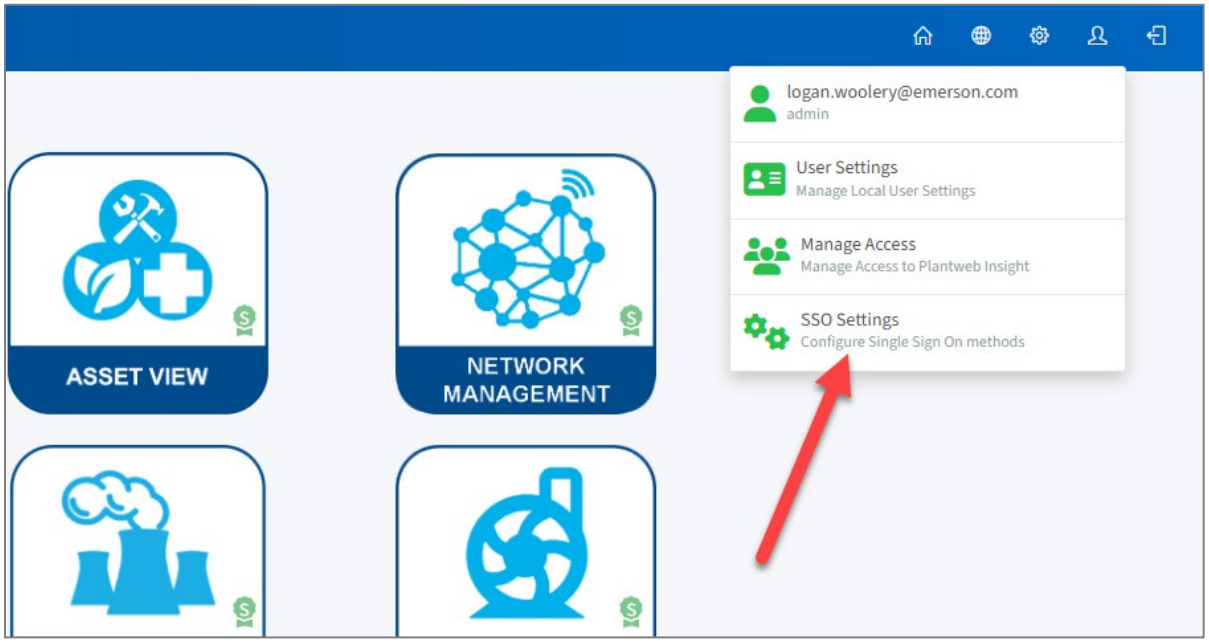
How To Register Your PWI Application with Entra ID

This document from Microsoft explains how to register an application with MS Entra ID platform

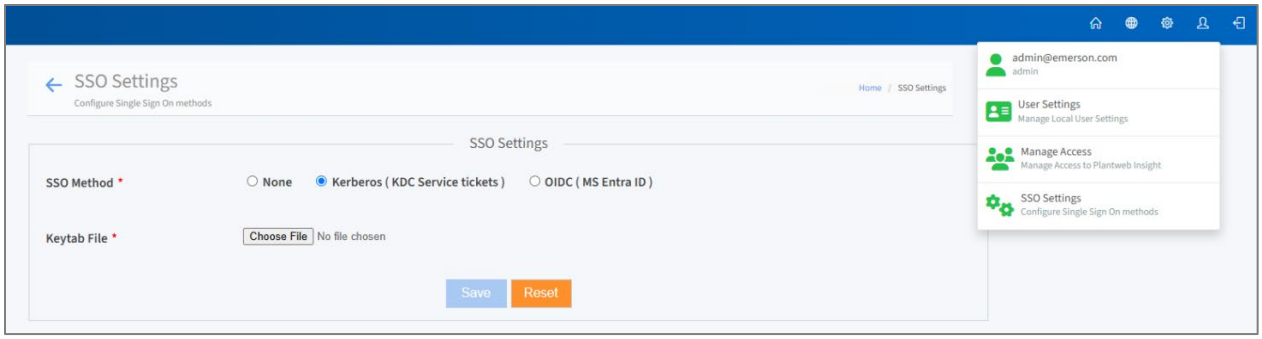
- Provide PWI URL under "Redirect URI" section of app registration page. This can be an IP address or FQDN of the PWI system.
    - For instance, if PWI is running on IP address **192.168.175.5**, then the redirect URL should be configured as **https://192.168.175.5** .
    - If PWI is configured to run on a FQDN such as **customer.pwi.com** , then the redirect URL is **https://customer.pwi.com** .
- PWI is a single page application and you can choose "Single-page application" under the "Platform Configuration" option.
- Since it is a Single page app, it does not require configuration of any credentials (Certificates/secrets) under this application registration.

Procedure for SSO with Kerberos

1. Users can configure SSO by navigating to ***Users > SSO Settings***



2. Select the **Kerberos (KDC Service tickets)** radio button



3. A keytab file with necessary verification details is required for configuration
    a. A keytab file should be prepared by the user's IT administrator
    b. PWI should be accessed through a FQDN from web browsers
    c. A group policy should be added to the domain controller to trust the FQDN and initiate SSO

User Access Management (Authorization)

From PWI v3.3.0 onwards, all users of PWI must explicitly be granted access to the platform and applications.

In the earlier versions of PWI, LDAP user's access was derived based on the service principles owned by a user.

After the introduction of location hierarchy-based access control and multi-role support in PWI v3.3.0, it is no longer feasible to assign hierarchy and role information to users in an automated way. Therefore, each PWI user must be assigned access to apps/role/locations by a PWI platform administrator before they can access an app.

A new menu is introduced in the PWI user settings to manage user entitlements and access: **User Settings > Manage Access > Manage User Access**

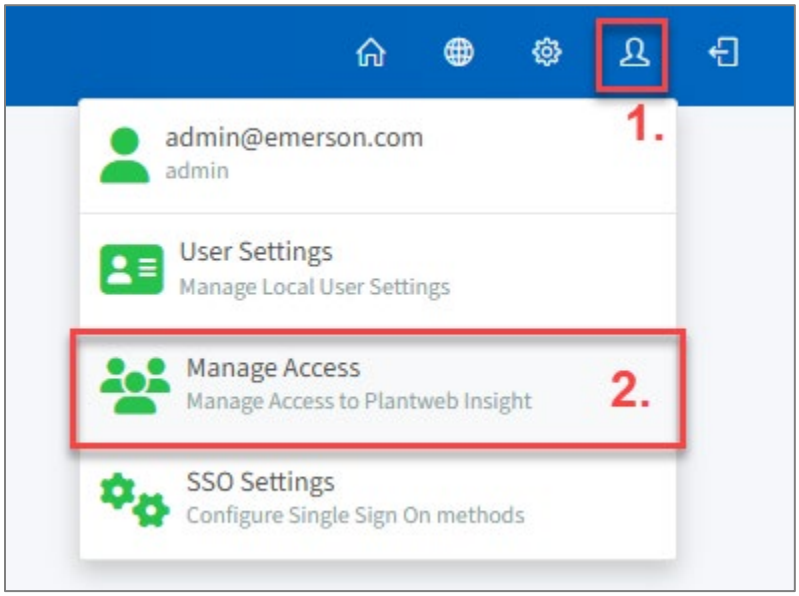
Manage User Access

This menu allows platform administrators to grant and revoke access to existing user accounts.
A user's access to an application is granted based on how the application has implemented authorization support.

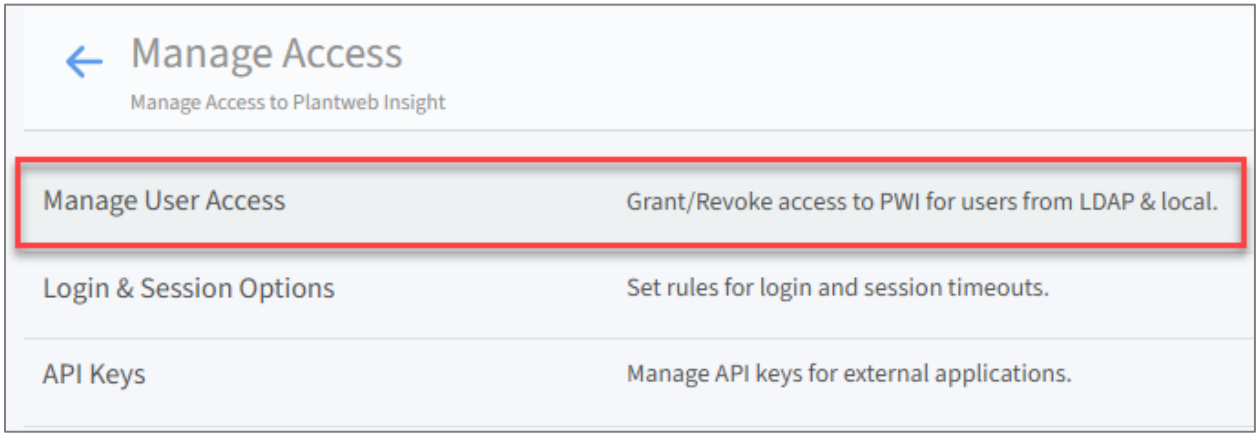
The Manage User Access page provides various authorization data like roles, sites, etc. based on the approach that is chosen by an app.

Assigning Access to a User Account

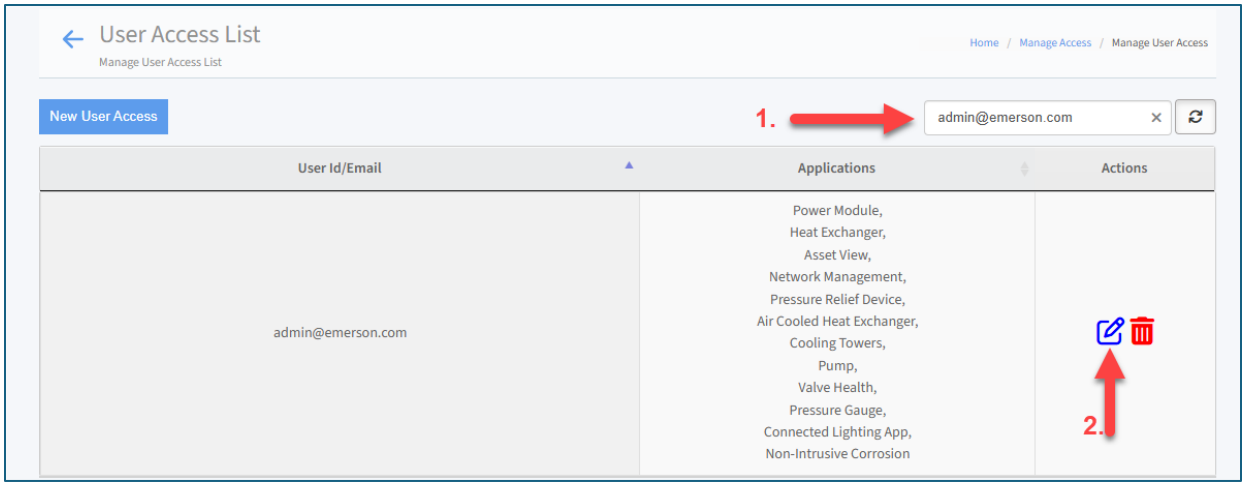
1. To assign access to your own account, you must be an Admin user at the PWI platform. If you are not an Admin user, you will need another user with an Admin account to assign you access.
2. In the upper right corner of PWI's home screen, click on the Users icon (1) and then click ***Manage Access*** (2)



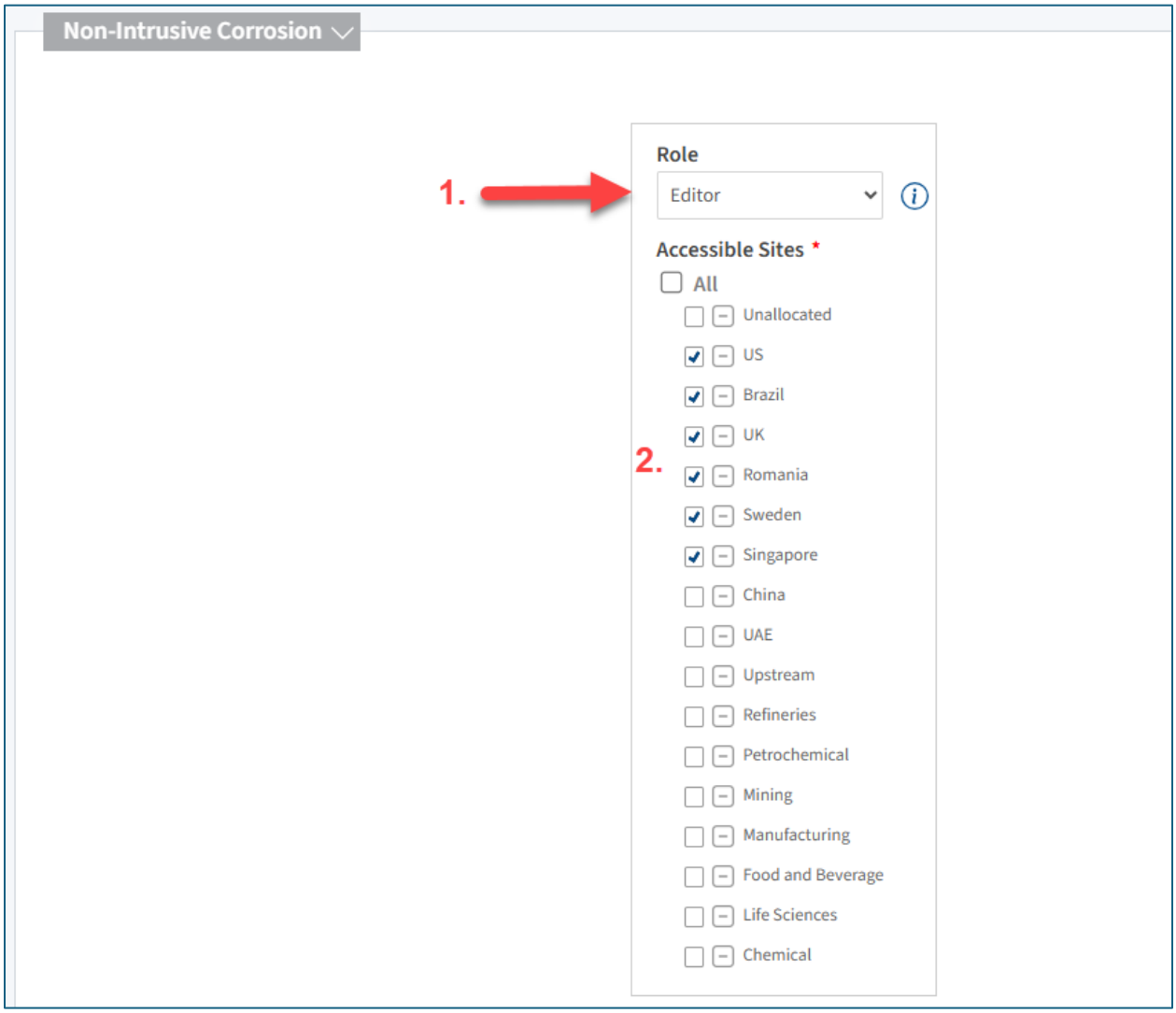
3. Select ***Manage User Access***



4. Search for the username that requires access (1) and click the edit button (2)



5. Find the application(s) the user requires access to and select a **Role** (1) for that user in that application and select the **Accessible Sites** (2) for that user in that application.

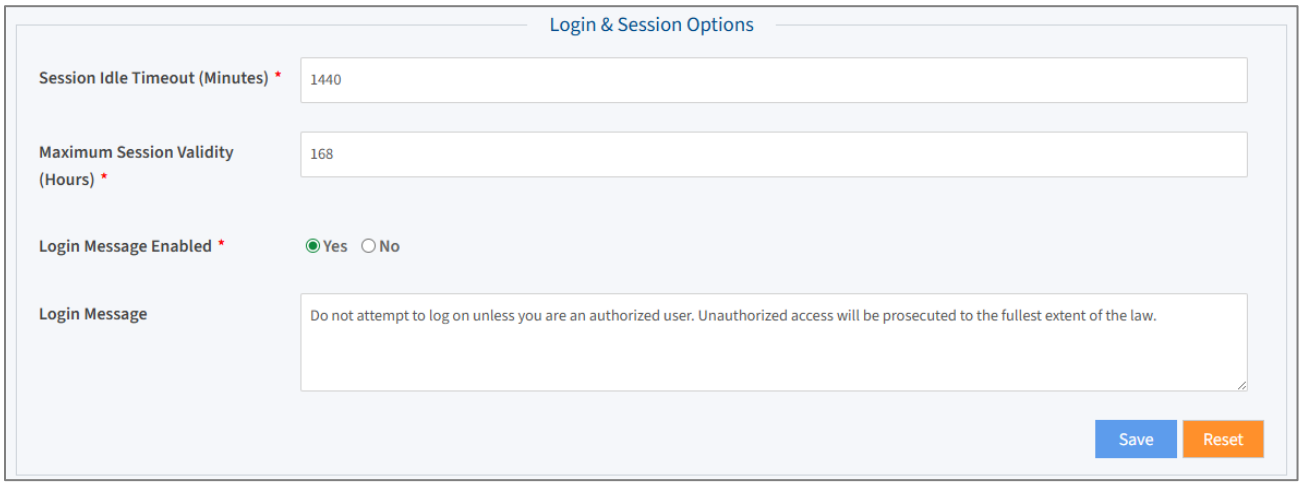


Note: Some applications do not support custom role or location-based access control yet. In these applications, the user's role will be derived from the PWI platform role, and the user will have access to all locations. Refer to information bubble for details on application-specific roles.

Login & Session Options

Navigate to ***User Settings > Manage Access > Login & Session Options***

This menu allows administrators to manage session settings for all users.

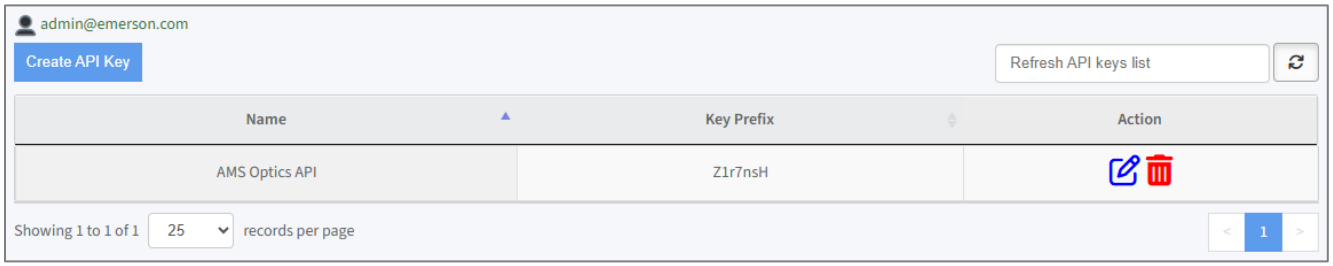


API Keys

Navigate to ***User Settings > Manage Access > API Keys***

This menu allows administrators to create API keys that are expected to be used by other business systems like Emerson's AMS Optics. These keys do not expire and will have access to all applications' alerts and asset states.

API keys are tied to user accounts and only visible to the user who creates them.



License Management

A valid license key is required to activate and access any PWI application.

1. Locking Code

A PWI locking code is required to generate licenses for your PWI system. The locking code is a unique machine fingerprint that is specific to your PWI system.

The Locking Code locks to the following parameters:

- Machine ID
- VM UUID
- IP Address of eth0 (primary) & eth1 (secondary) interfaces

  If using the PWI EDGE solution, the secondary interface is assigned to **ETH2** rather than ETH1. ETH1 and other ports are not used by PWI on the edge computer.

- MAC Address of both eth0 & eth1 interfaces

If any of these parameters change, the locking code will change, which will invalidate any existing licenses and require new licenses. It is recommended to assign static IP addresses and finalize network configurations before requesting your license(s). Please contact your Emerson representative if you wish to change any of these parameters so they can coordinate replacement license delivery.

The locking code locks specifically to the “eth0” and “eth1” interfaces. It will assume that “eth0” is present and proceeds to get the info for “eth1”. If “eth1” is not present, it will set the parameters of “eth1” as empty.

NOTE for versions earlier than 3.4.0: Before PWI v3.4.0, PWI was delivered with both network interfaces enabled by default. Ensure that the secondary interface is configured in the virtual machine settings or has an ethernet cable plugged into eth2 on the RXi2 edge device during initial startup. If the secondary interface is not required, it should be disabled from within the PWI user interface first, before disabling at the virtual machine settings or unplugging from ETH2 on the edge device.

Migration of the PWI Virtual Machine

When the PWI VM is migrated to new Servers/clusters, ensure that the VM has retained the machine ID, UUID, MAC & IP addresses of both network adapters. Change to any of these properties requires new licenses.

Exporting the PWI VM

Typically, the PWI VM is expected to be exported when the user performs migration to a new HCI cluster. There are additional points to consider when a VM is exported.

When a VM is exported:

- MAC addresses are usually not preserved
    - The user will have to configure the VM with the exact same MAC address when importing it to a new HCI cluster.
- VM UUID may be preserved (Hypervisor should prompt the user to retain the existing UUID or generate a new UUID)
    - VM UUID must be retained when importing a new HCI cluster.
- The IP address is not preserved since it is bound to the ethernet interface
    - The user will have to configure the VM with the exact same IP address when importing it to a new HCI cluster.

Dos and Don'ts

Below are several user scenarios that are allowed when it comes to administering the PWI VM.

Users may:

- Move PWI VM to another hypervisor host within the same HCI cluster during Migrate/failover. In this case, there is no change to any of the locking criteria properties
- Move the VM to a new HCI cluster, decommission the old HCI cluster (HCI full migration case)
- Migrate from an older PWI VM to a newer PWI VM, keeping both PWI VMs running concurrently
    - The new PWI VM would have a different machine ID, hence licenses would have to be re-generated.

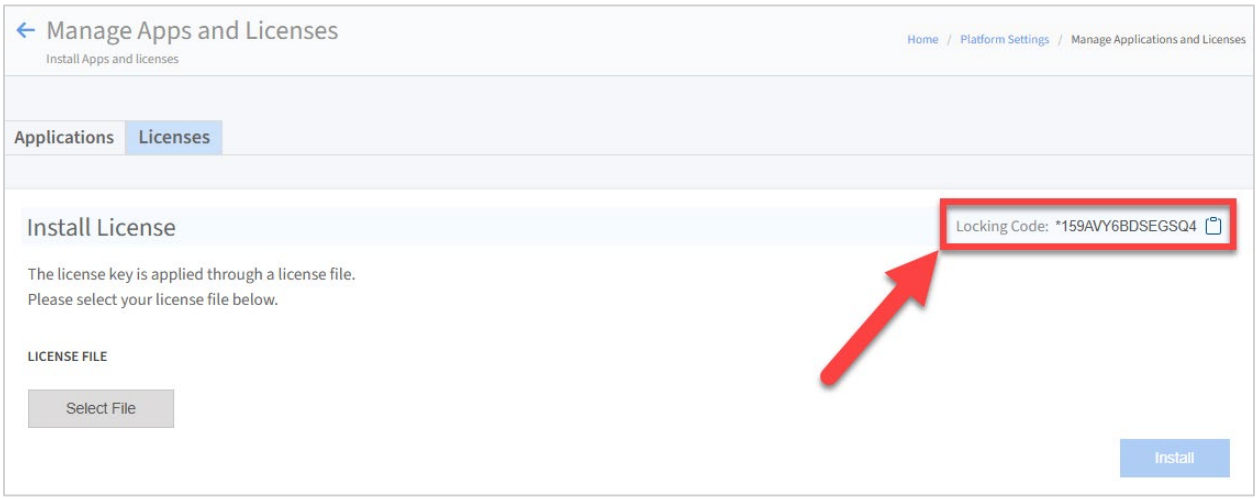
Users may NOT:

- Clone and duplicate the PWI VM within the deployment.

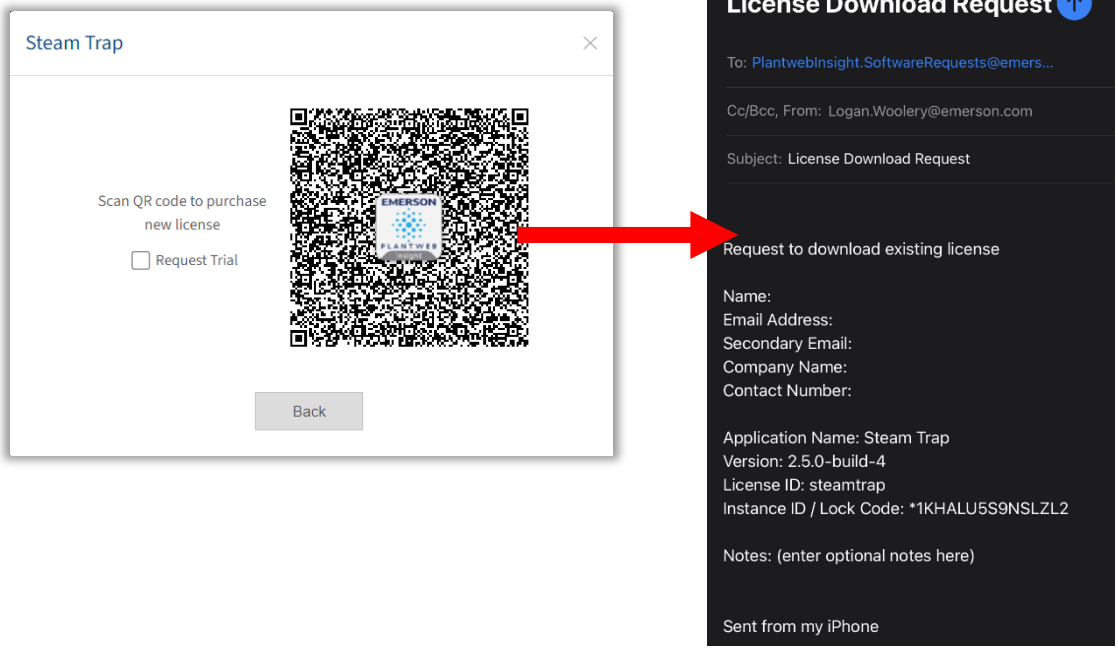
2. Requesting a License

A purchase order must be placed before a license can be generated. Please refer to the individual PWI application product data sheets for license ordering details. License keys begin on the date the license is generated, not necessarily the date of the purchase order. 90-day free trial licenses are available upon request.

1. Install PWI (either as a virtual machine or edge device) and finalize network parameters listed above in locking code section.
2. Copy your PWI locking code by navigating to ***Platform Settings > Manage Applications and Licenses > Licenses.*** The locking code is shown in the upper right corner of the screen.



a. Alternatively, if a valid license is currently not installed, users can click the disabled application icon which will bring up a QR code. Scanning the QR code will draft an email on your mobile device that will include your locking code and license request details.

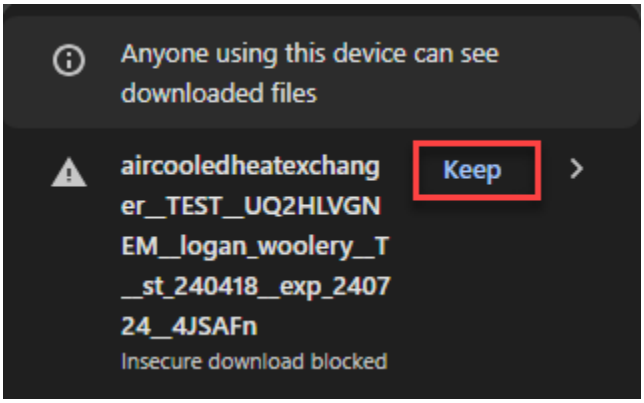


3. Email your **locking code** and **purchase order** or **sales order number** to PlantwebInsight.SoftwareRequests@Emerson.com
4. License keys will be generated according to your purchase order details and locking code and then emailed back to you.

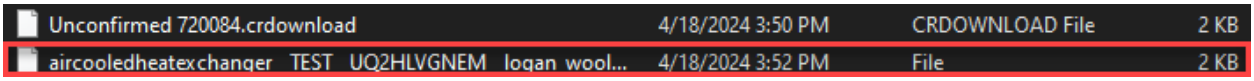
3. Installing Your License Key

1. PWI license keys are delivered via email as a file attachment. You will receive 1 license key file per application.
2. Download your license key file(s) to a PC/machine that can be used to access the PWI web interface.

   NOTE: Some web browsers do not recognize the PWI license file type. Verify that your browser has accepted the download and successfully downloaded the file before installing your license key.

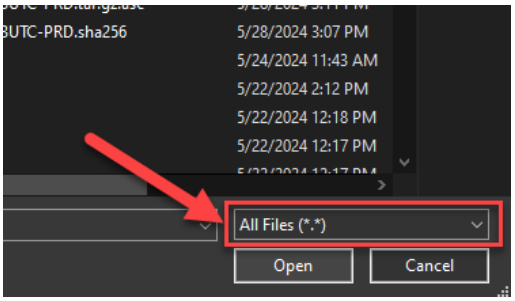


   Example: Google Chrome prompts user to 'Keep' file before downloading.

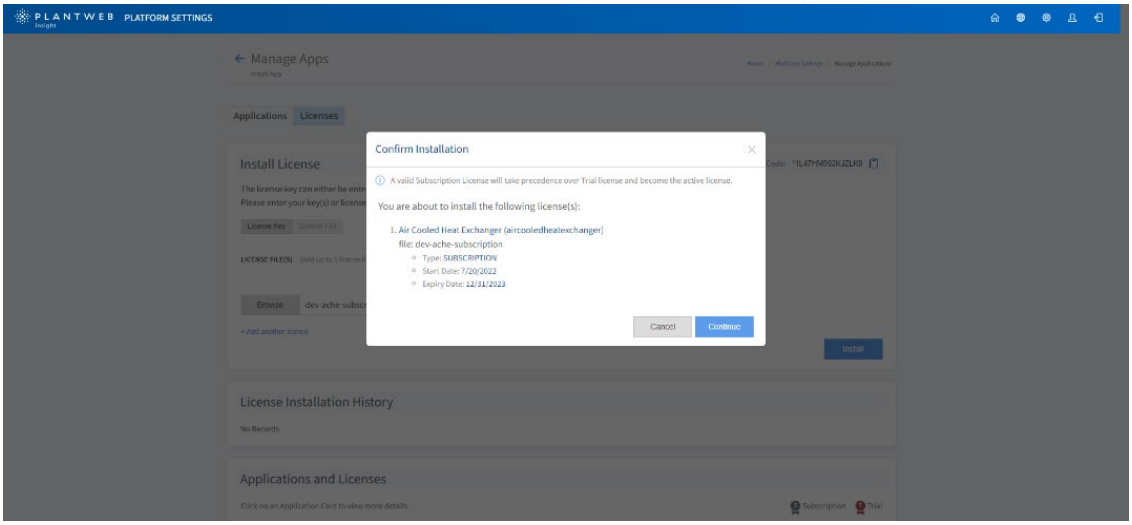


   Example: A successful download will display the full license file name. File type is "File".

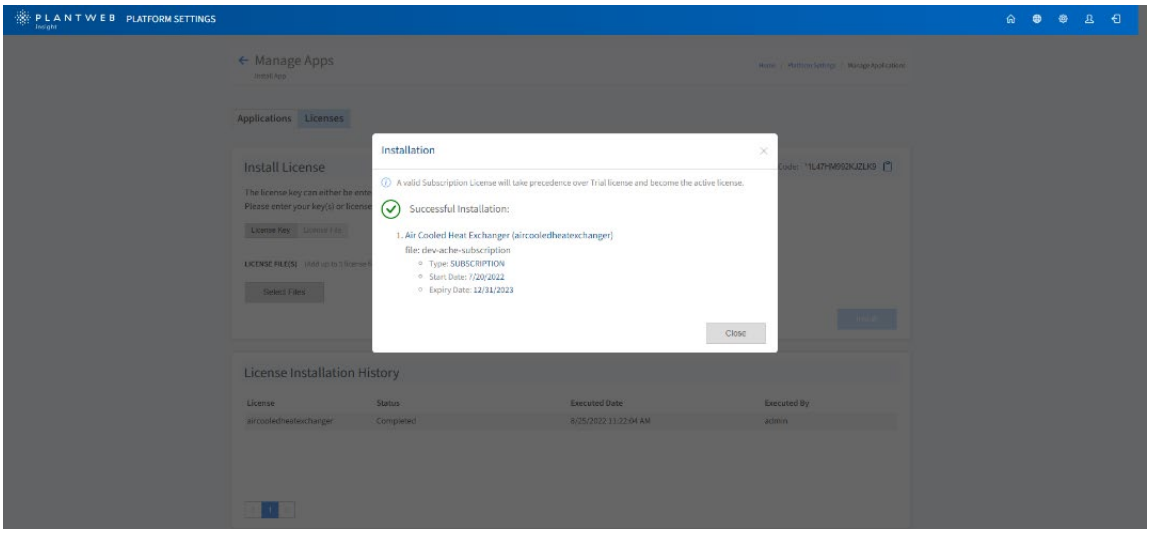
3. In PWI, navigate to ***Platform Settings > Manage Applications and Licenses > Licenses***
4. Click "Select Files" to browse for your license file. Ensure "All Files (*.*)" is selected from the dropdown menu on the bottom-right area of the file selection window



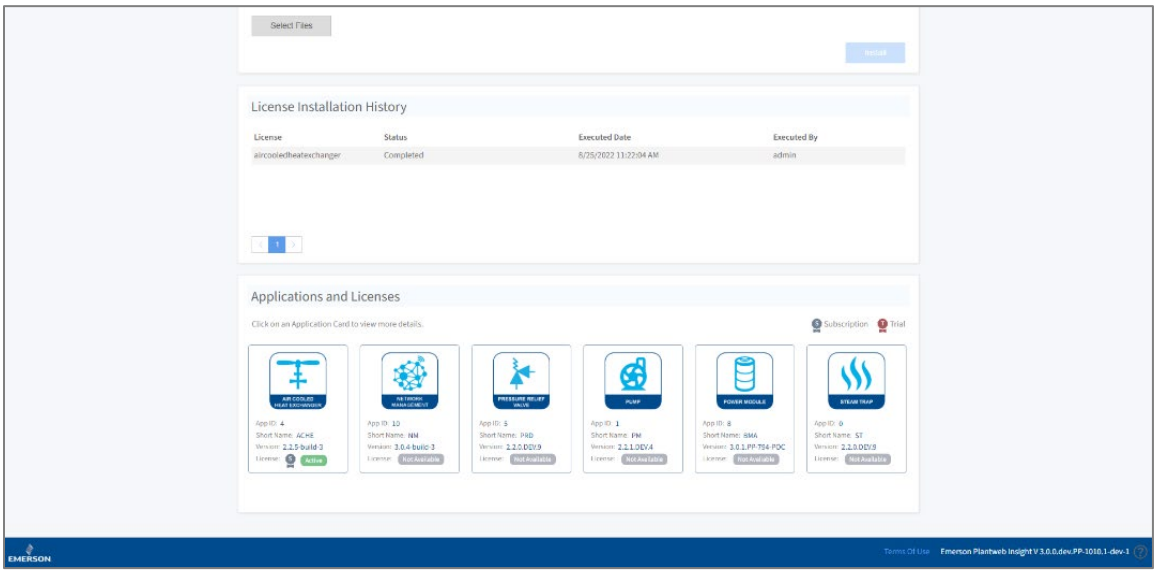
5. Select the license file(s) and click the “Open” button.
6. Click “Install” button to install license key.
7. Review license details on the confirmation window that pops up. Click “Continue” button.



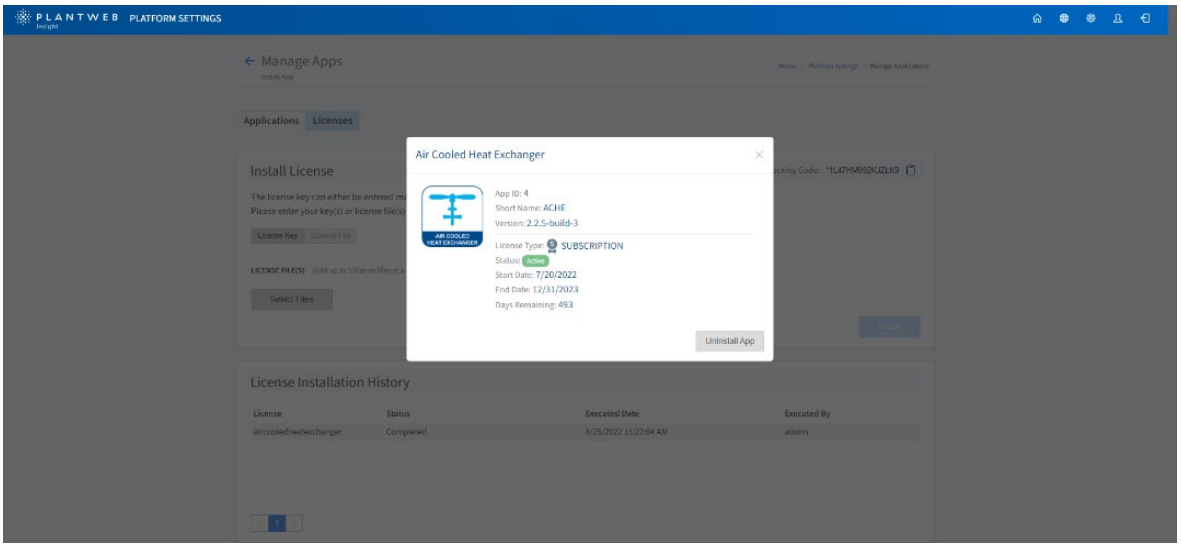
8. Click “Continue” and read through End User License Agreement and click “Agree” to complete license installation. The new license will overwrite any previous existing license (trial or subscription).



9. Check license statuses in the Application Card listed in the Applications and Licenses panel at the bottom of the screen.



10. Click on the Application Card to view more license details.



11. Return to homepage and the app should be enabled. There should be a License Badge on it (Refer to item 1 in PWI License Details about License Badges). If you see a restricted icon, refer to the Manage User Access section.

4. License Details

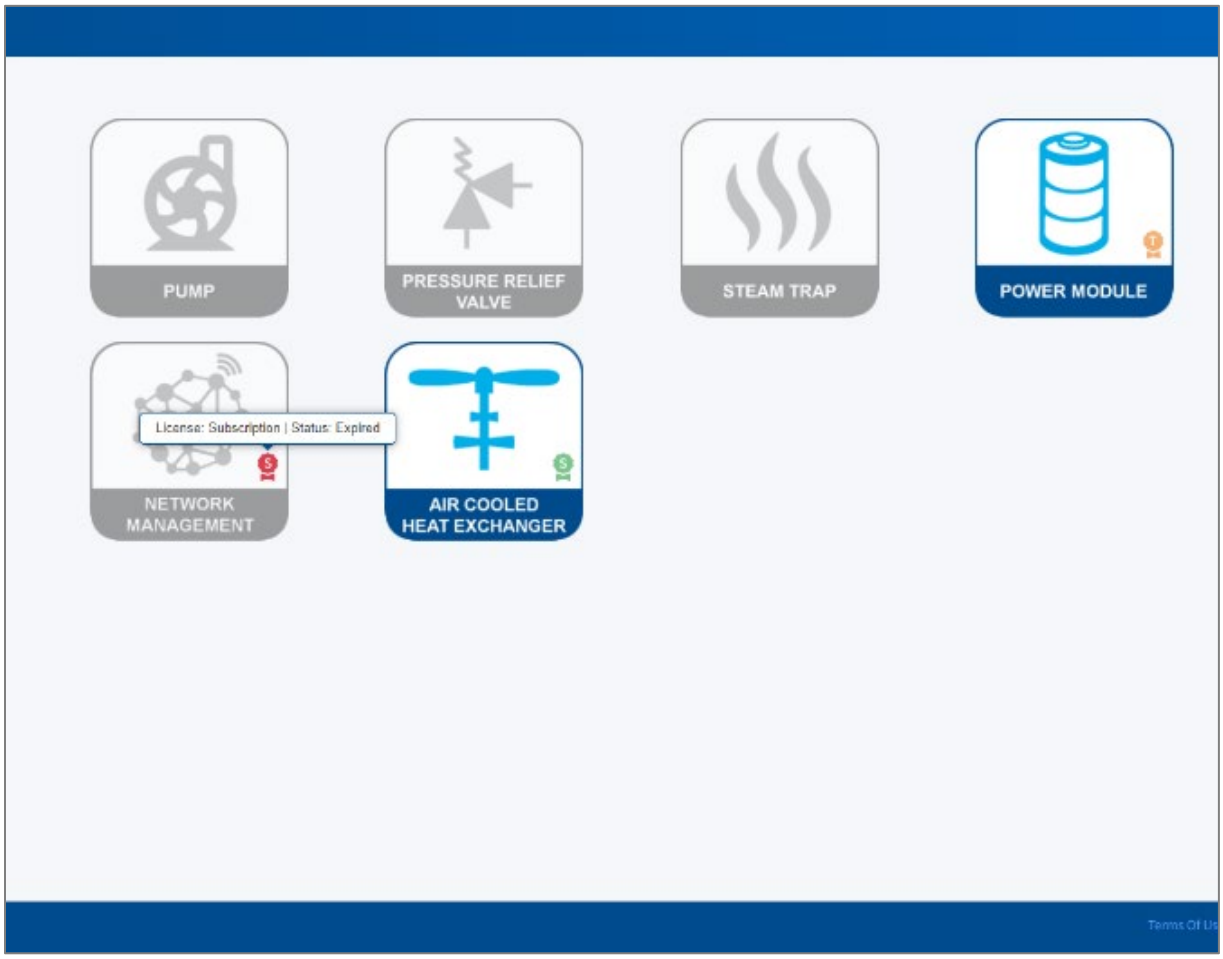
These are the different app icon license badges and licensing messages that may appear on your homepage.

License badges on App Icons:

Hover over the License Badge (ribbon icon), to see a quick view of the license type and status.

The License Badge represents license type and status:
- (S) symbol means **SUBSCRIPTION LICENSE**
- (T) symbol means **TRIAL LICENSE**

Color codes
Green → Active
Amber → Expiring within next 90 days
Red → Expired



License Expiration

PWI will begin to warn users at 90 days from expiration about expiring licenses with a pop-up window that appears each time a user opens the application, showing the number of days remaining. Email alerts can be configured in the ***Platform Settings > SMTP and***

Platform Notifications menu to notify users via email of expiring licenses. The platform will notify users via email at 90, 60, and 30 days until expiration. The summary email will consolidate all the expiring/within grace period/expired licenses. Once a PWI application license reaches its expiration date, the badge icon changes to red, and the application will will become inaccessible. The application will shut down and stop processing any new data. Any previous data will remain in the application and can be accessed by entering a new license. Application data can only be permanently removed if the application itself is uninstalled from the platform, and the user chooses to perform a "clean uninstall".

5. Common Errors

Error Code	Error Message on UI	Description
210150	Locking Code is invalid	Lock code used to generate the license is invalid (Most likely because it does not "match" the lock code on this PWI installation)
214109	Expired License	License is expired
210093	License was already installed	License was already installed.
210188	License can only be activated on or after start date	License start date not yet reached

NOTE: If a trial license is installed for an application where a subscription license is still active, the trial license will not take effect until the subscription license has completely expired.

6. Data Source Configuration

1. WirelessHART® Gateways (HART-IP connection)

The PWI HART-IP client establishes a TCP connection to each gateway and issues various HART-IP commands to retrieve network and device information periodically. The collected data is then consumed by application(s) which subscribe to this data.

1. Navigate to  (Settings button) **>** ***Data Source Config*** **>** ***Gateway Settings*** **>** click **"Add Gateway"** button
2. Enter the IP address, Port, and Description for the gateway. Select the "secure" checkbox to establish an encrypted connection between PWI and the gateway.

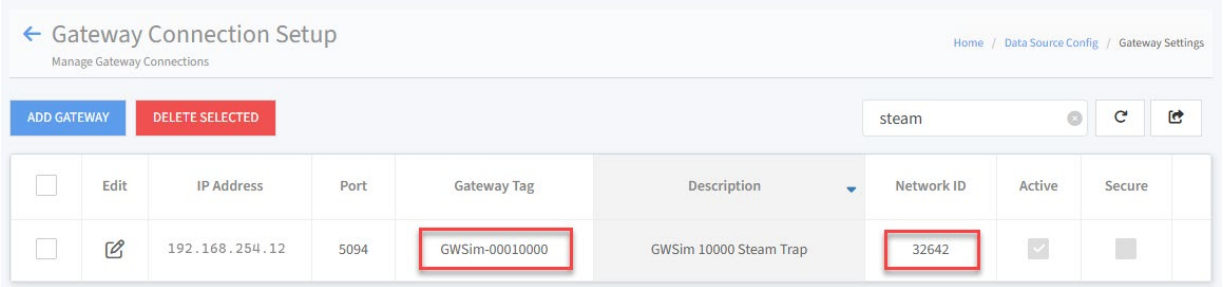
i. Insecure Connection: Port 5094 is used for insecure HART-IP communication. This port must be open across the network when PWI connects to the Gateway in insecure mode.

ii. Secure Connection: Port 5095 is used for secure HART-IP communication. Port 443 is required for certificate exchange when configuring the Gateway in secure mode. Both ports 443 and 5095 must be enabled across the network for secure communication.

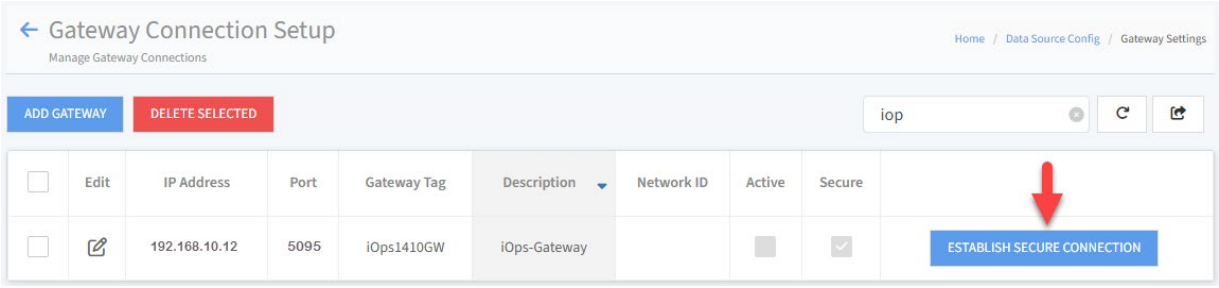
NOTE: TCP Ports 6094 and 6095 are used when PWI communicates with a Dual WirelessHART Gateway. These ports must be enabled when PWI is connected in either secure (6095) or insecure (6094) mode.

When PWI is connected to a standard Gateway, enabling ports 6094/6095 is not required.

3. Once the gateway connection is established, the Gateway Tag and Network ID information will appear, and the active box will be checked in the Gateway Connection Setup page



4. For secure gateway connections, the secure box will be checked, and an “Establish Secure Connection” blue button should appear in the right column.



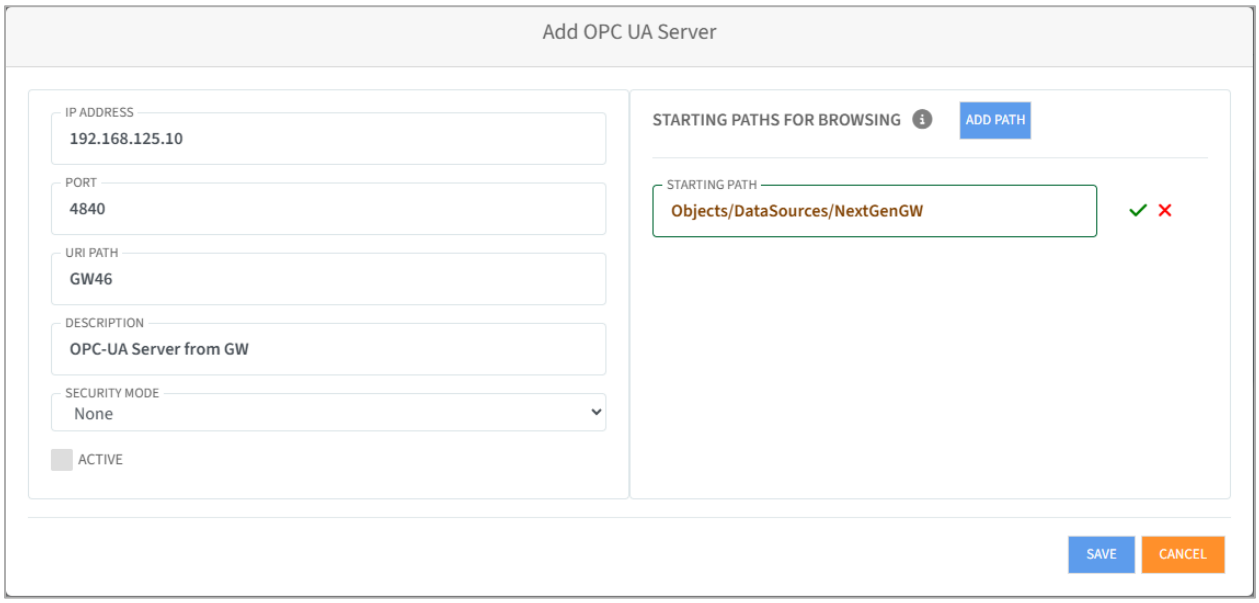
5. Press the “Establish Secure Connection” button. The user will be prompted to enter valid credentials for this gateway.
6. Once the gateway tag and network ID appear, the connection is successfully established.

NOTE: The HART-IP client can take a little over 5 minutes to show the Active check mark when a new gateway is configured.

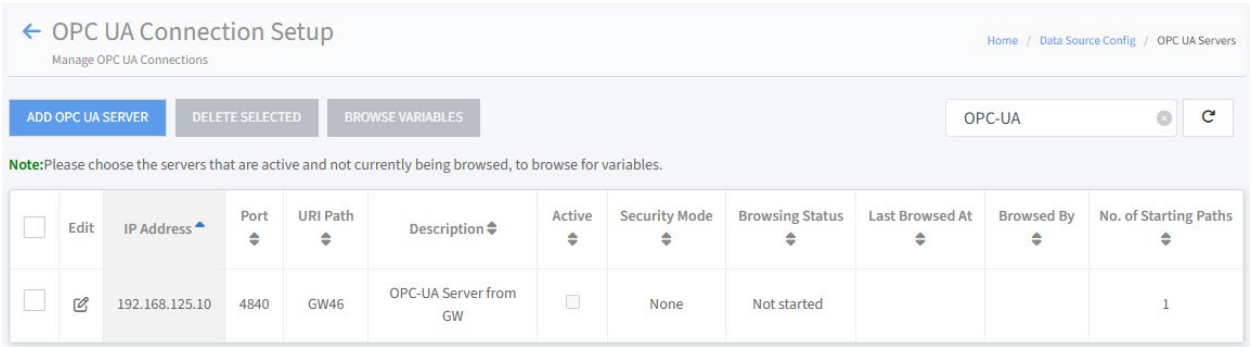
2. OPC-UA® Servers

Add OPC-UA Servers

1. Navigate to (Settings button) **> *Data Source Config* > *OPC UA Servers* >** click **“Add OPC UA Server”** button
2. Enter the IP address, Port, URI path, and description for the OPC UA server. The "Starting Path" feature, introduced in version 3.4.0, enables variable browsing. If you prefer not to browse the entire server, you can configure specific starting paths to limit browsing to those designated paths and save the connection details.



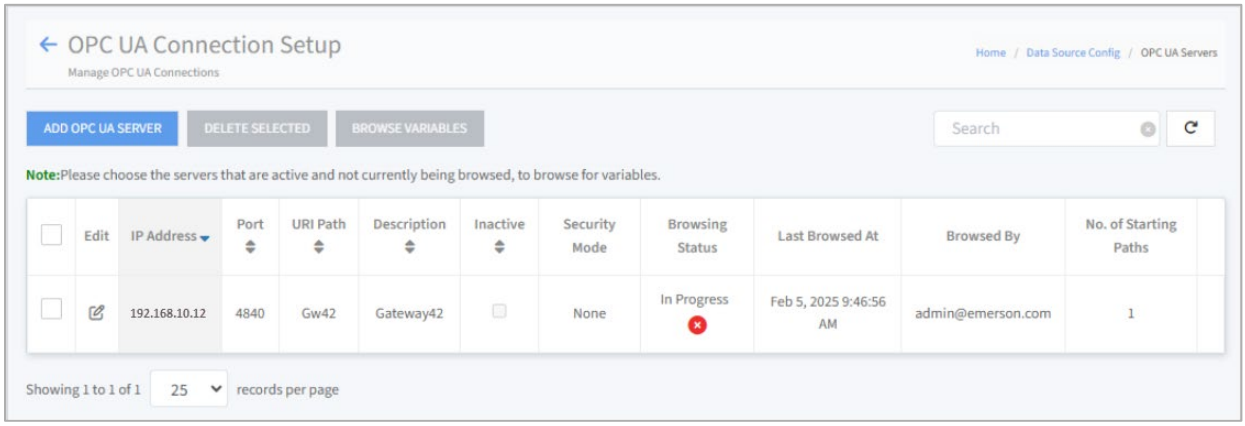
3. Once the details are added, the Active box will be unchecked, and the Browsing Status will show “Not Started”



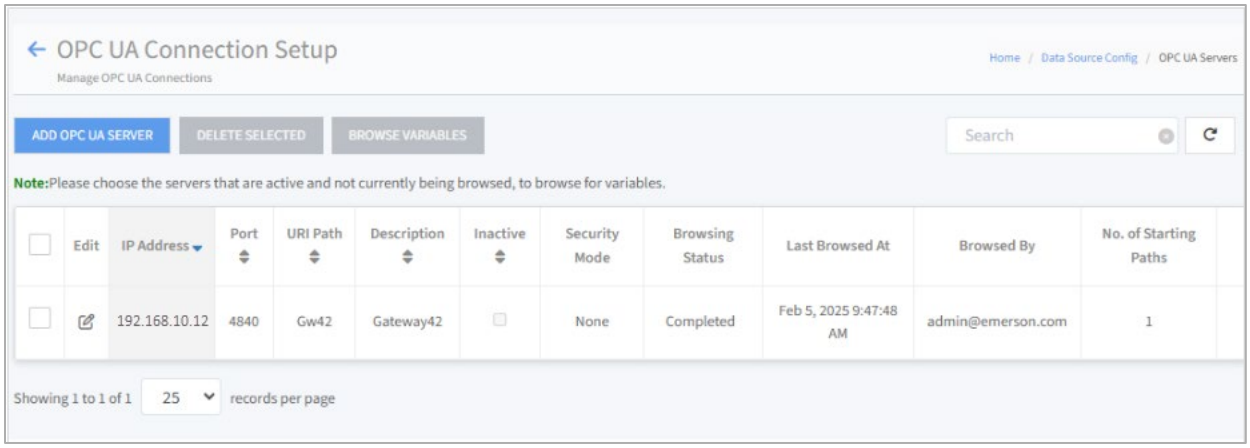
Browse Variables

4. Wait for the connection status to become active (active box is checked) and it will trigger the variable browsing automatically. Browsing Status will update to “In

Progress”. You can also cancel the current browsing by clicking the cross icon in the browsing status.



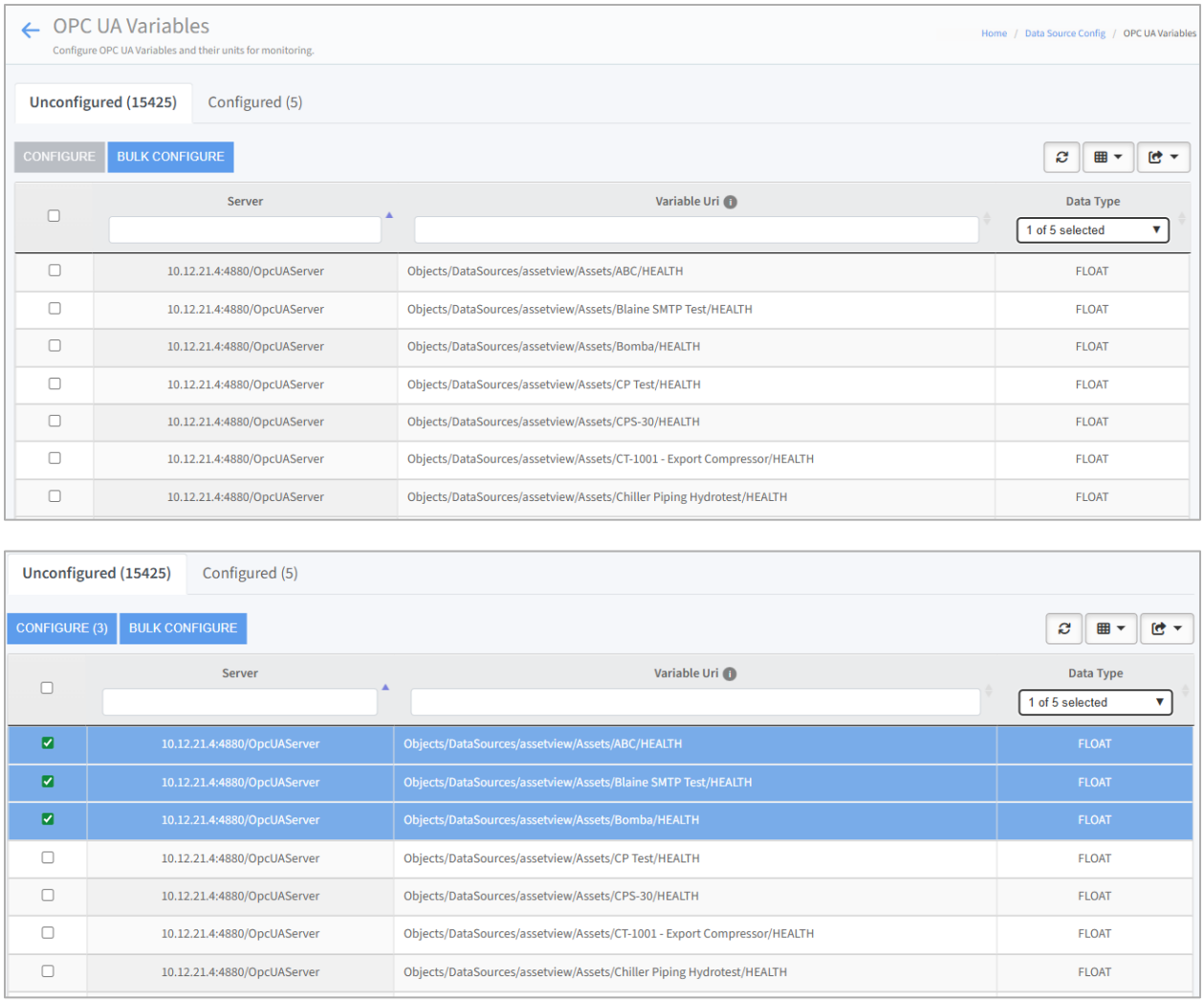
5. The OPC UA client will establish a connection with the OPC UA server and retrieve the variables from it. Once the browsing is complete, the Browsing Status will be updated to "Completed," along with the "Last Browsed At" and "Browsed By" details.



Browsing can also be initiated manually by selecting the checkbox and clicking the "BROWSE VARIABLES" button. Ensure that the selected servers are active and do not have a browsing status of "In Progress." Automatic hierarchy browsing will also be triggered whenever there is a change in the starting path.

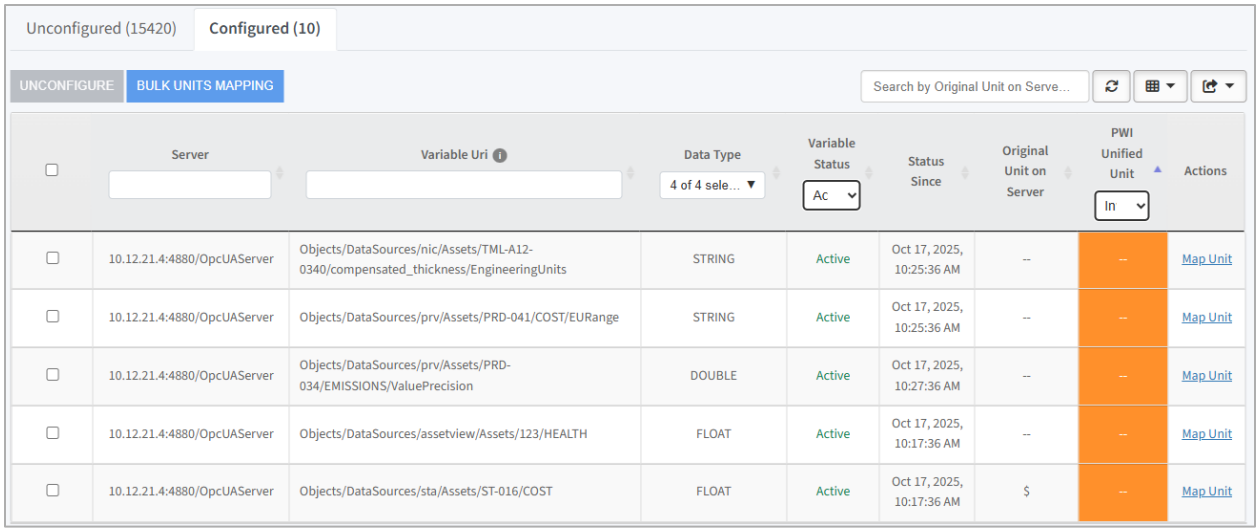
Configure OPC-UA Variables

6. Click the submenu under ***Data Source Config > OPC UA Servers > OPC UA Variables***. This will display a list of all variables retrieved from the OPC-UA servers. You can configure the variables by selecting their checkboxes and then clicking the “CONFIGURE” button.



Selected variables are moved from "Unconfigured" to "Configured". The OPC-UA client then verifies the availability of the variables on the server and publishes a status message, including the variable's current status and its original unit of measurement as defined on the server.

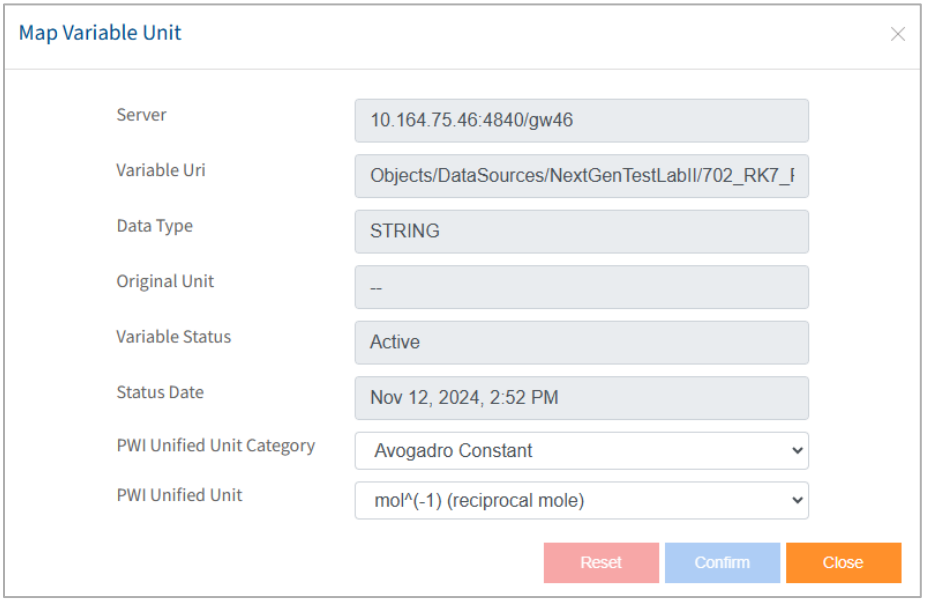
The system will compare the original unit of the variable with the units of measurement available in the PWI system. If it exactly matches (case sensitive), then the Unified Unit is automatically mapped.



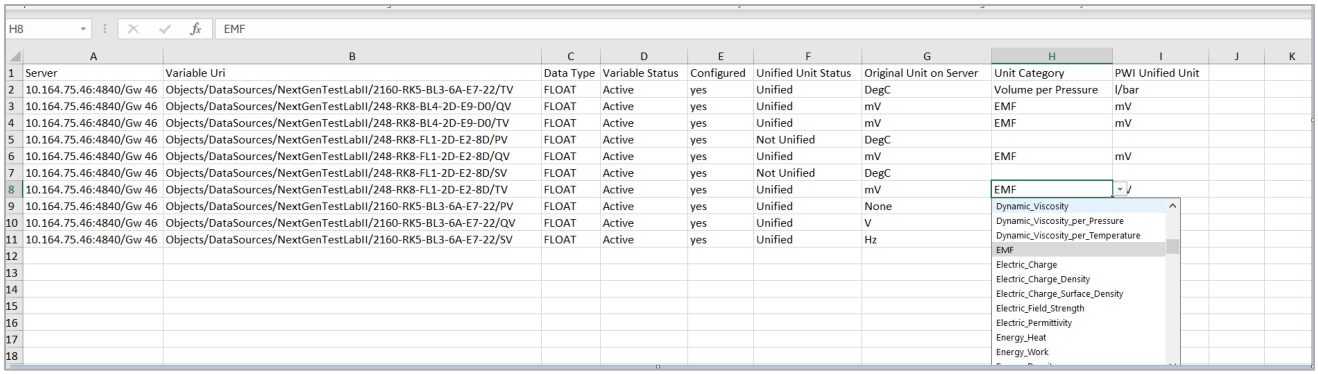
You can also configure in bulk by downloading the CSV file, marking the "Configure" column as "Yes," and then uploading the file.

Map Units

7. If a variable's units are not mapped automatically, users can map them in two ways:
   i. Use the "Map Unit" link to configure variables one at a time



   ii. Use the "Bulk Units Mapping" button to configure several variables at once via CSV file.



	A	B	C	D	E	F	G	H	I
1	Server	Variable Uri	Data Type	Variable Status	Configured	Unified Unit Status	Original Unit on Server	Unit Category	PWI Unified Unit
2	10.164.75.46:4840/Gw 46	Objects/DataSources/NextGenTestLabII/2160-RK5-BL3-6A-E7-22/TV	FLOAT	Active	yes	Unified	DegC	Volume per Pressure	l/bar
3	10.164.75.46:4840/Gw 46	Objects/DataSources/NextGenTestLabII/248-RK8-BL4-2D-E9-D0/QV	FLOAT	Active	yes	Unified	mV	EMF	mV
4	10.164.75.46:4840/Gw 46	Objects/DataSources/NextGenTestLabII/248-RK8-BL4-2D-E9-D0/TV	FLOAT	Active	yes	Unified	mV	EMF	mV
5	10.164.75.46:4840/Gw 46	Objects/DataSources/NextGenTestLabII/248-RK8-FL1-2D-E2-8D/PV	FLOAT	Active	yes	Not Unified	DegC		
6	10.164.75.46:4840/Gw 46	Objects/DataSources/NextGenTestLabII/248-RK8-FL1-2D-E2-8D/QV	FLOAT	Active	yes	Unified	mV	EMF	mV
7	10.164.75.46:4840/Gw 46	Objects/DataSources/NextGenTestLabII/248-RK8-FL1-2D-E2-8D/SV	FLOAT	Active	yes	Not Unified	DegC		
8	10.164.75.46:4840/Gw 46	Objects/DataSources/NextGenTestLabII/248-RK8-FL1-2D-E2-8D/TV	FLOAT	Active	yes	Unified	mV	EMF	
9	10.164.75.46:4840/Gw 46	Objects/DataSources/NextGenTestLabII/2160-RK5-BL3-6A-E7-22/PV	FLOAT	Active	yes	Unified	None		
10	10.164.75.46:4840/Gw 46	Objects/DataSources/NextGenTestLabII/2160-RK5-BL3-6A-E7-22/QV	FLOAT	Active	yes	Unified	V		
11	10.164.75.46:4840/Gw 46	Objects/DataSources/NextGenTestLabII/2160-RK5-BL3-6A-E7-22/SV	FLOAT	Active	yes	Unified	Hz		

Dynamic_Viscosity
Dynamic_Viscosity_per_Pressure
Dynamic_Viscosity_per_Temperature
EMF
Electric_Charge
Electric_Charge_Density
Electric_Charge_Surface_Density
Electric_Field_Strength
Electric_Permittivity
Energy_Heat
Energy_Work

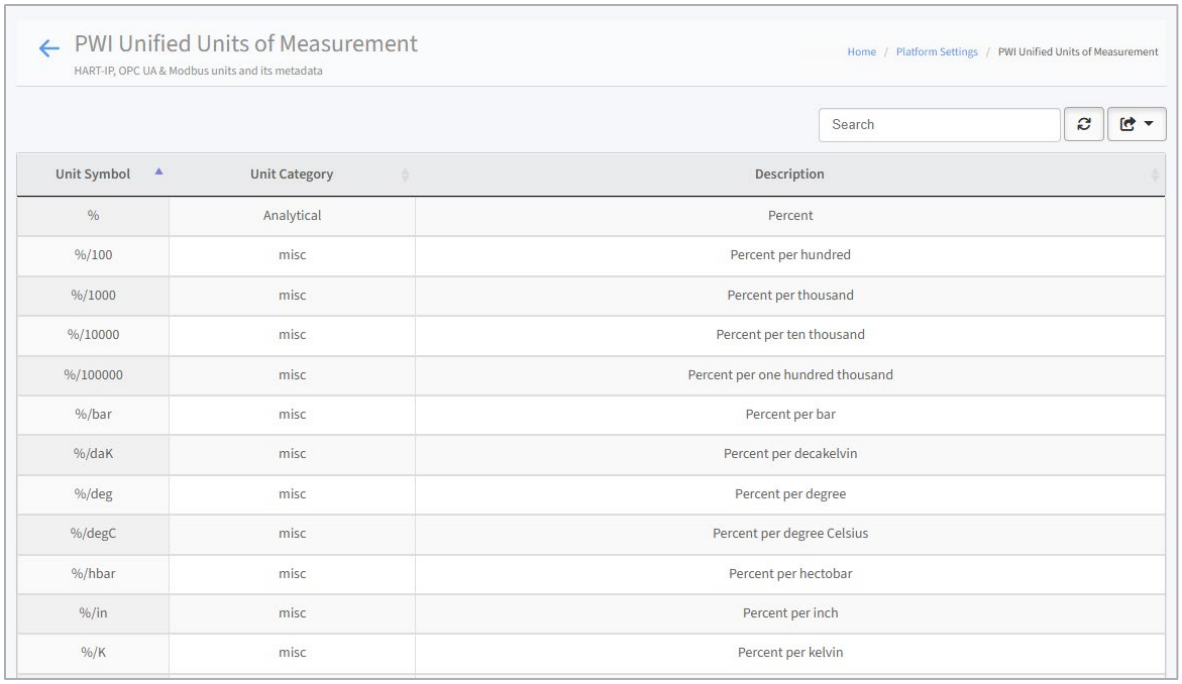
Export the configured variables into MS-Excel file format. This file allows the user to select the unit category and corresponding units from the dropdown.

To map a unit, enter the units in the "PWI Unified Unit" column and make sure that the units entered in that column are available in the PWI Unified Units of measurements (case sensitive). Save this file as CSV and upload it into PWI using the "Bulk Unit Mapping" button.

Configured variables can also be moved to the Unconfigured list by selecting the checkbox and clicking the unconfigure button or by marking the “Configure” column as “No” in the OPC-UA unit mapping CSV file and uploading.

PWI Unified Units

1. A UI screen is available under ***Platform Settings > PWI Unified Units of Measurement*** to show and allow CSV export of the well-known HART-IP, OPC-UA & Modbus unit categories and other units metadata.

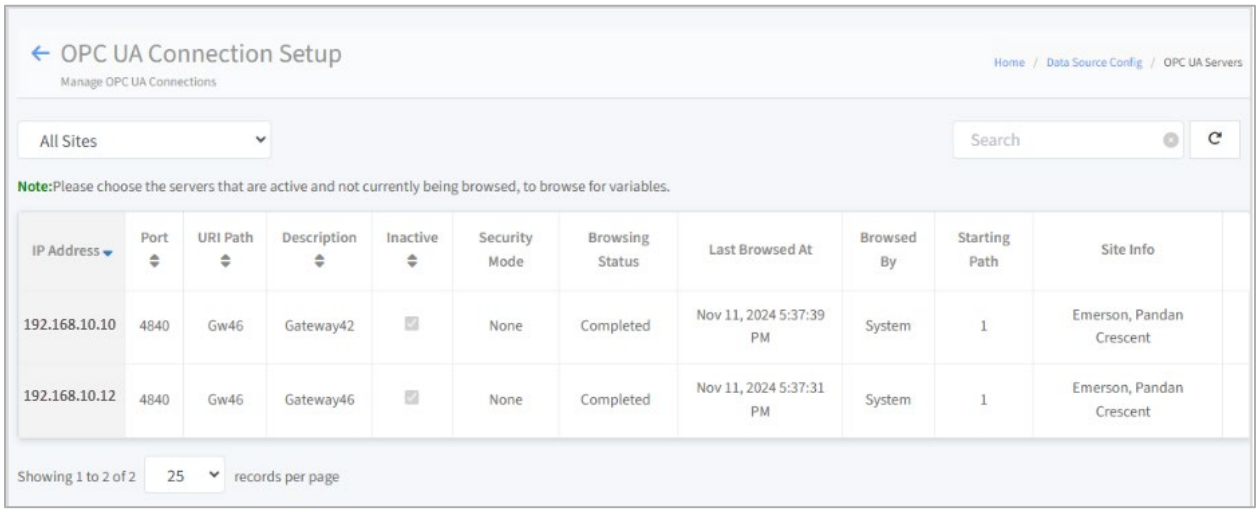


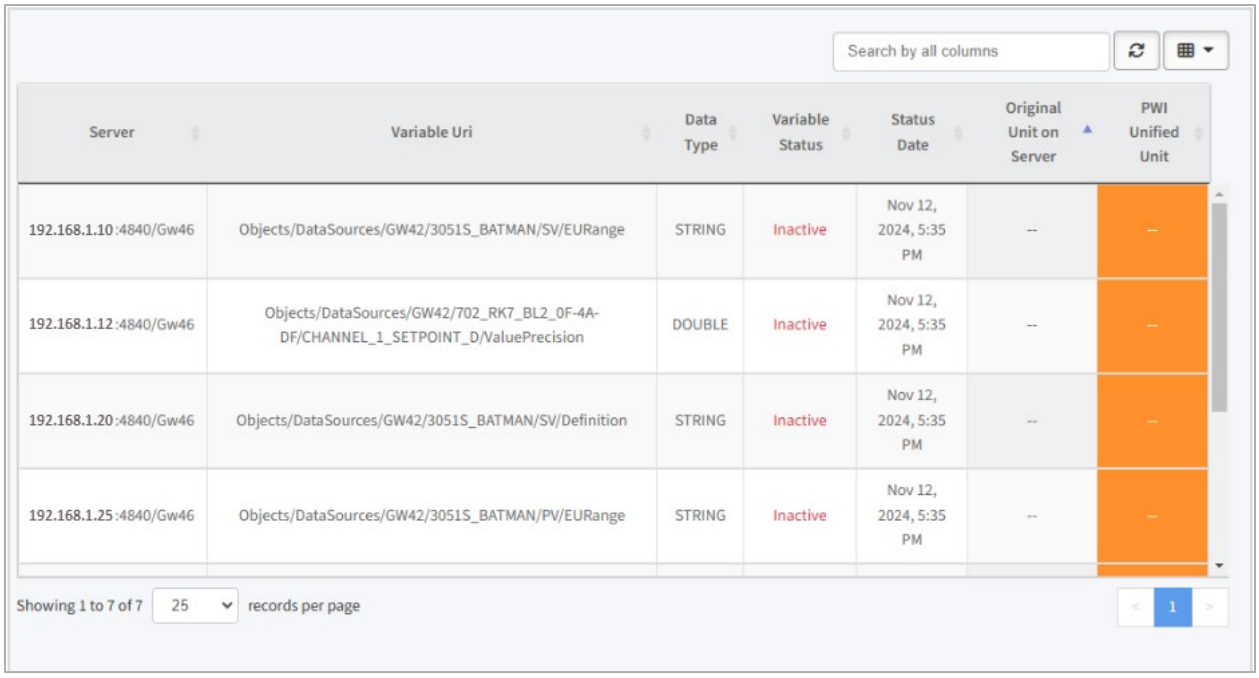
Unit Symbol	Unit Category	Description
%	Analytical	Percent
%/100	misc	Percent per hundred
%/1000	misc	Percent per thousand
%/10000	misc	Percent per ten thousand
%/100000	misc	Percent per one hundred thousand
%/bar	misc	Percent per bar
%/daK	misc	Percent per decakelvin
%/deg	misc	Percent per degree
%/degC	misc	Percent per degree Celsius
%/hbar	misc	Percent per hectobar
%/in	misc	Percent per inch
%/K	misc	Percent per kelvin

OPC-UA Data Sync Across PWI Connector Systems

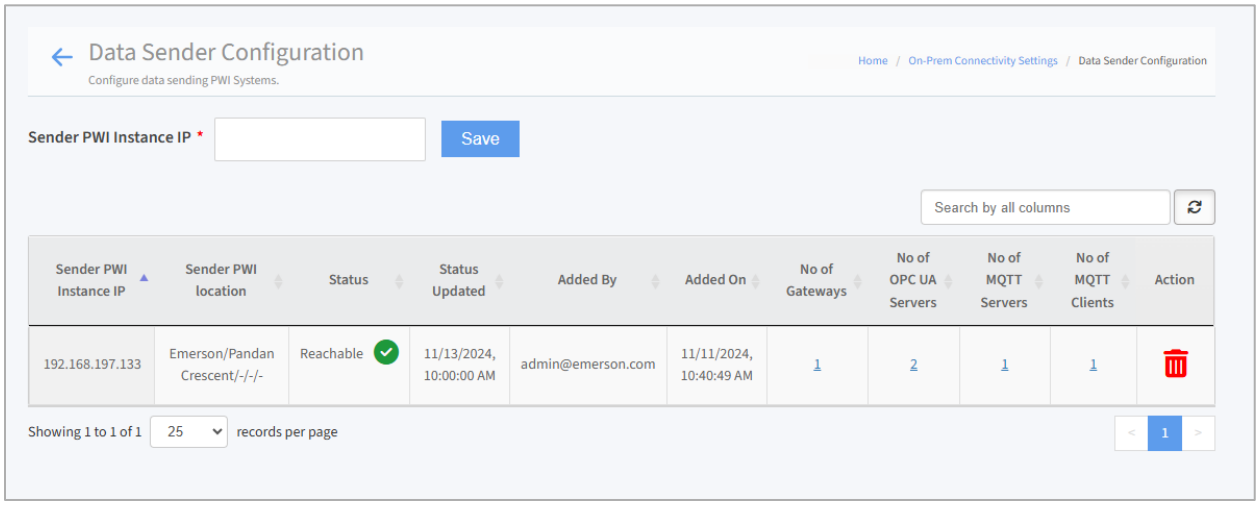
OPC-UA Servers and the variables configured in a PWI On-Prem Connector or PWI Cloud Connector system are sent to the respective On-Prem App Only and Cloud App Only system via MQTT publish. Applications installed in the PWI App Only system can select the variables configured in the connector system and subscribe to their values.

OPC-UA server and variable synchronization occurs whenever they are added, updated, or deleted. There is also a periodic sync which occurs once an hour to avoid any data loss. The OPC-UA data connections and configured variables page in the App Only system are read-only, and the connections page will display site info along with filtering for sites.





The number of data sources configured between the On-Prem Connector and App-Only system is displayed under ***On-Prem Connectivity Settings > Data Sender Configuration***.



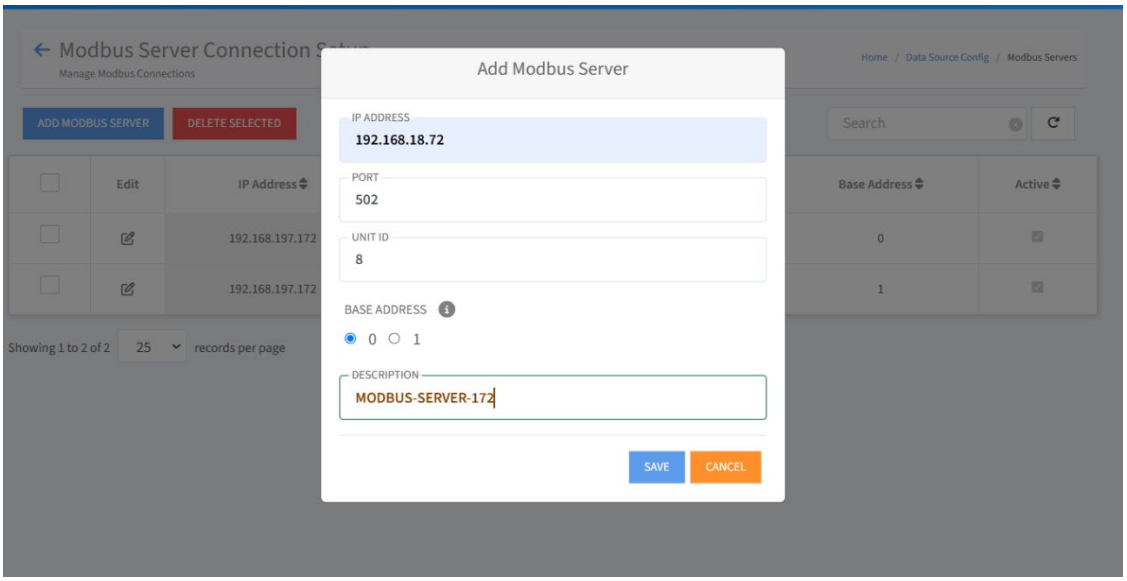
3. Modbus® TCP Servers

PWI has a default polling rate of 30 seconds for Modbus variables unless an application specifies otherwise. If an application requires a different polling rate, users can set the Modbus variable polling rate in their Modbus register Excel file and specify these Modbus variables via CSV upload. In the downloaded CSV sample, the column "Polling Rate" is **NOT** added by default. Users can manually add a new column with the name "Polling Rate" and input the corresponding desired polling interval. Refer to Adding Variables via CSV Upload section below for instructions on where to find CSV sample variable sheet.

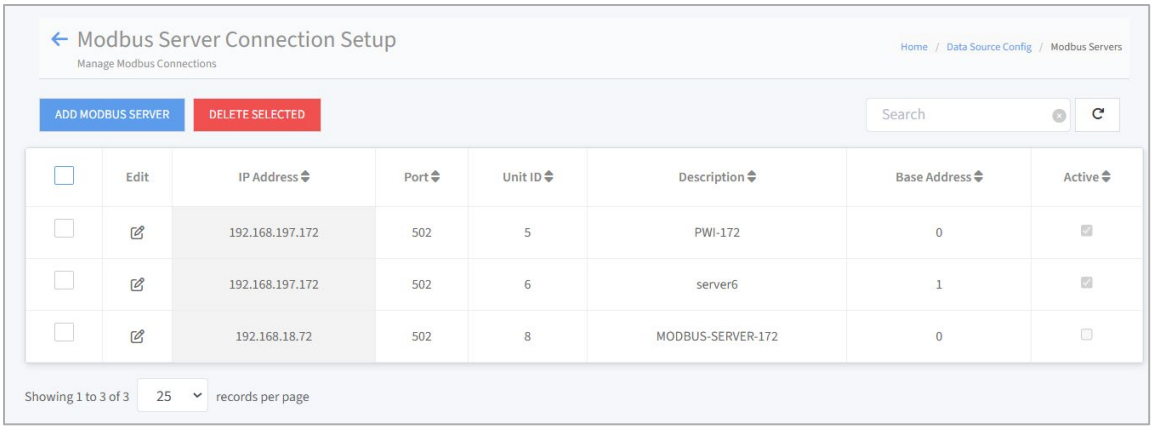
CAUTION: Users who modify the default polling rate should follow application spec guidance to avoid causing potential performance issues in PWI. Contact PWI technical support for guidance.

Add Modbus TCP Server

1. Navigate to (Settings button) **> *Data Source Config* > *Modbus Servers* >** click **"Add Modbus Server"** button.
2. Enter the server details by entering the IP Address, port, unit ID, description and select the base address and click "Save" button.
   - The combination of IP address, port, and unit ID must be unique and not duplicated.
   - If the base address is 0, the valid range of register addresses for the variables would be from 0 to 65535.
   - If the base address is 1, the valid range of register addresses for the variables would be from 1 to 65536.



When a Modbus server is added, the system firewall is opened for the IP and Port. Once the PWI Modbus Client gets the server list, it will connect to each server if the connection is not established yet. Servers with the same IP address and port share one TCP session/connection.



Configure Modbus Variables

3. Once the Modbus server is configured, its corresponding variables can be added in two ways:
    i. UI Form
    ii. CSV file upload

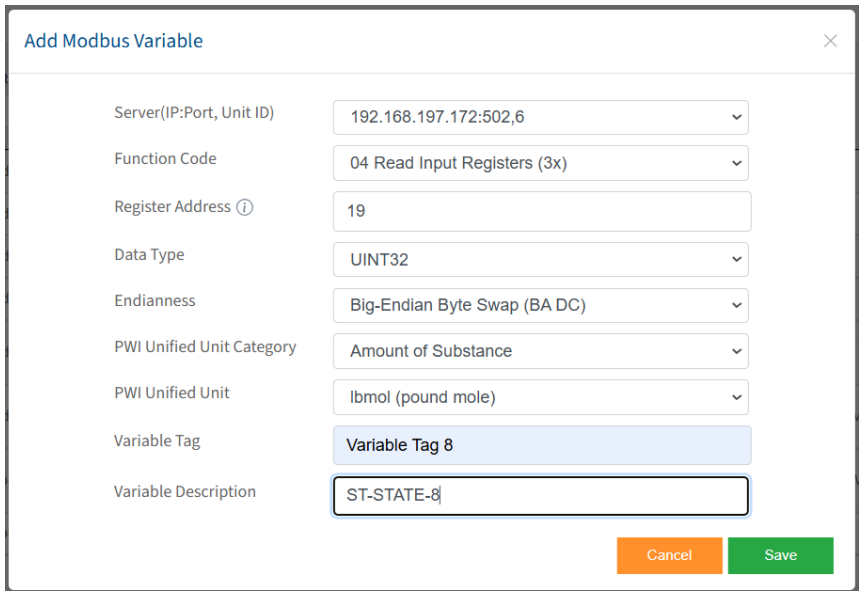
    Validation is performed when adding/editing the variables.

    - Variables can only be added for the servers that already exist as a Modbus data source.
    - The variable tag must be unique for each server.
    - Function codes supported for variables are:
        - 3 - Read Holding Registers
        - 4 - Read Input Registers
    - Register Address
        - Modbus server URI + Function code + Register Address should be unique.
        - Overlapping register addresses are not allowed (For example: A 32-bit data type occupies 2 registers- these two registers cannot be added again).
        - Register address should comply with base address of the server. If the base address is 0, then the register address should be [0, 65535]. Similarly, if the base address is 1, then the register address should be [1, 65536]
    - Data Types supported for Modbus variables are INT16, UINT16, INT32, UINT32, FLT32, INT64, UINT64 and DOUBLE64.

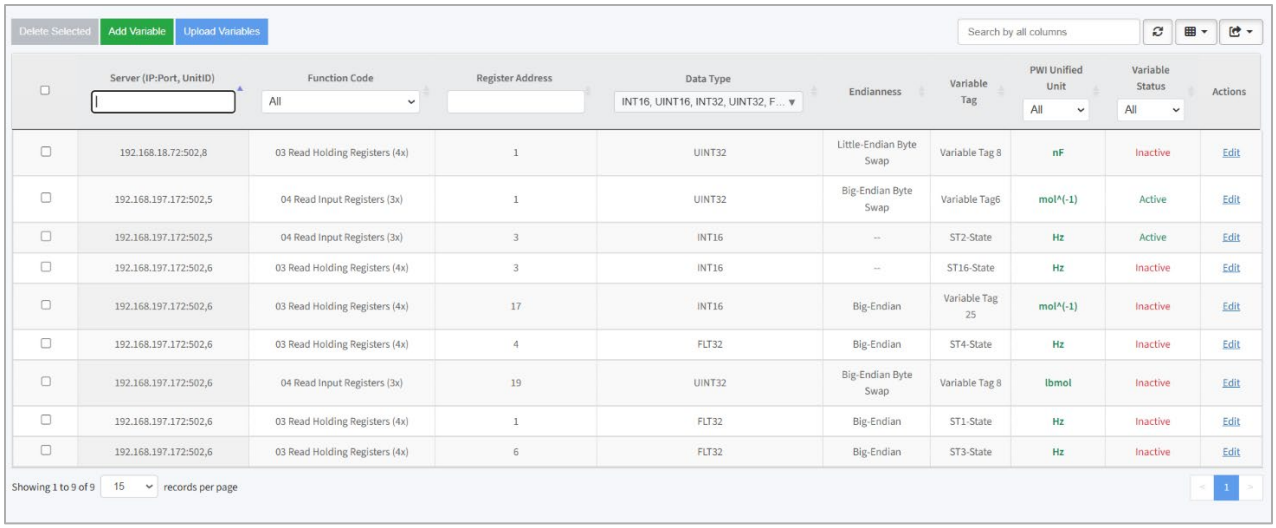
- Endianness is not required for 16-bit data types. If the data type is 32-bit or 64-bit, endianness is required, and the possible options are big-endian, little-endian, big-endian byte swap and little-endian byte swap.
- The unified unit must be one of the values provided by the PWI Unified Units of Measurement.

Adding Variables via UI Form

4. Click the submenu under ***Data Source Config > Modbus Servers > Modbus Variables*** and click the "Add Variable" button.
5. Select the Modbus server to configure a variable for and complete all required fields, then click "Save".



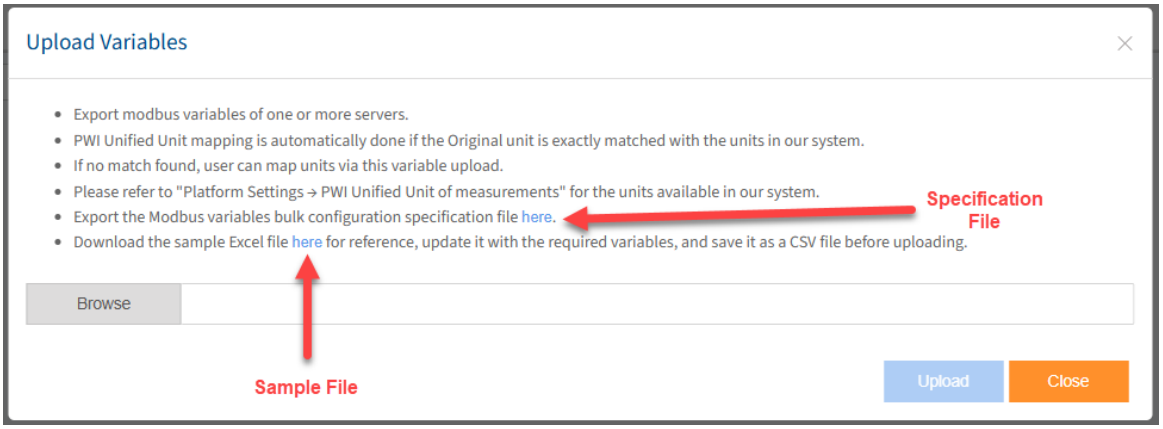
If all validations are met, the variable will be successfully added and appear in the data table. Users can apply column-level filters to customize the data in the table and export it.



Individual variables can be updated by using the Edit link corresponding to the rows. Multiple variables can be removed using the check boxes and “Delete Selected” button.

Adding Variables via CSV Upload

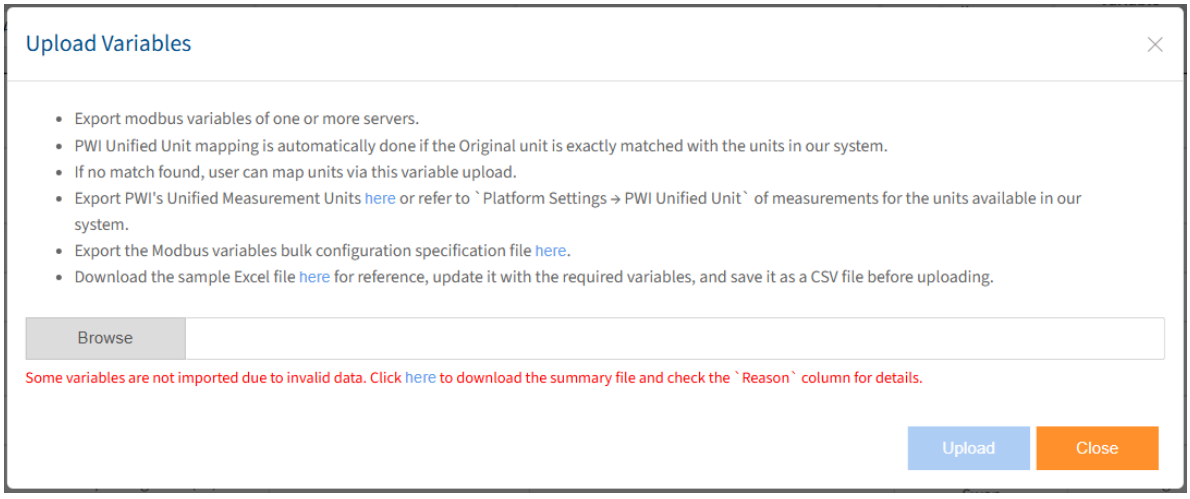
6. Click the submenu under ***Data Source Config > Modbus Servers > Modbus Variables*** and click the “Upload Variables” button.
7. Download the import specification file from the “Upload Variables” pop-up, which provides details about each column, the validations applied, and accepted values to use for the import.



A sample Excel file can also be downloaded from the pop-up, containing headers, sample values, and pre-defined dropdown options for columns such as Function Code, Data Type, Endianness, Unit Category, and Unified Unit, to help prevent any validation errors during the import process.

8. Once all variables are populated in the Excel file, it should be saved as a CSV file and then imported through the “Upload Variables” button pop-up.

The system will check to ensure that all validations mentioned above are applied to each row, and the data is either added or updated in the system's database. Once processing is complete, if any validation errors occur, a CSV file is generated with two additional columns displaying the status and reason for failure. Users can download this file, correct the errors, and re-import it.

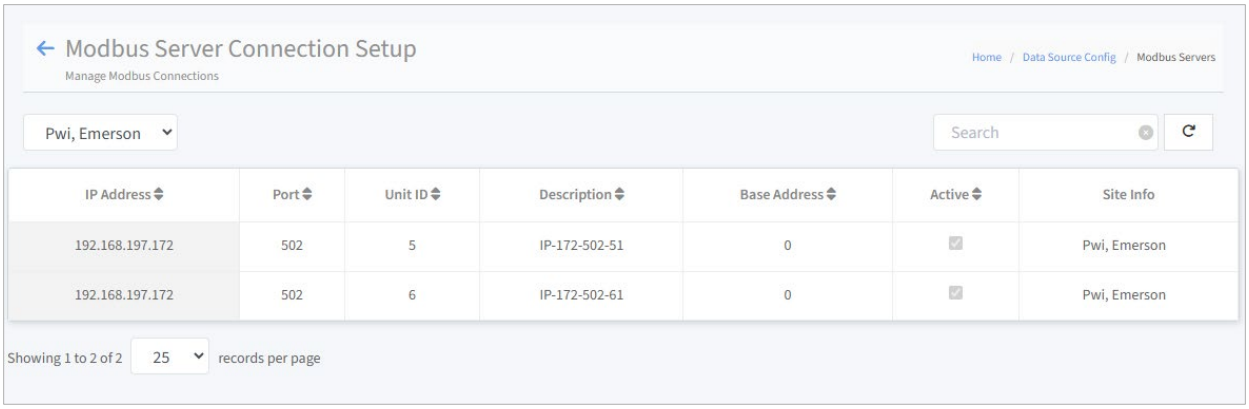


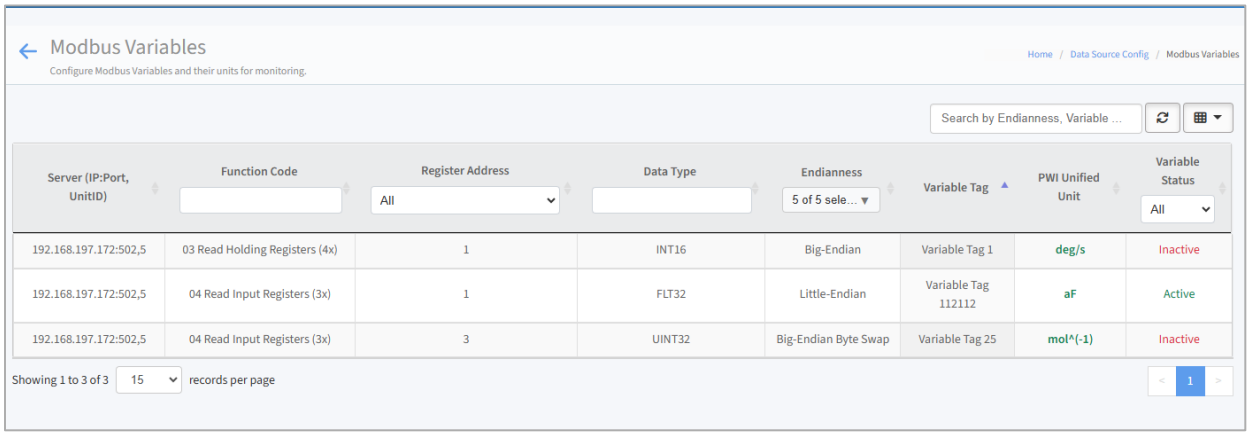
Server IPaddr	Server Port	Server UnitID	Function Code	Register Address	Data Type	Endianness	Unit Category	Unified Unit	Variable Tag	Description	Import Status	Reason
1.1.1.0	4840	3	3-Read Holding Registers	4	INT_32	big-endian	Temperature	degC	Temperature	Temperature of the room	Failed	Modbus Server connection does not exist.
1.1.1.0	4840	3	4-Read Input Registers	4	INT_32	big-endian byte swap	Angle	rad	Radius	Radius	Failed	Modbus Server connection does not exist.

Modbus Data Sync Across PWI Connector Systems

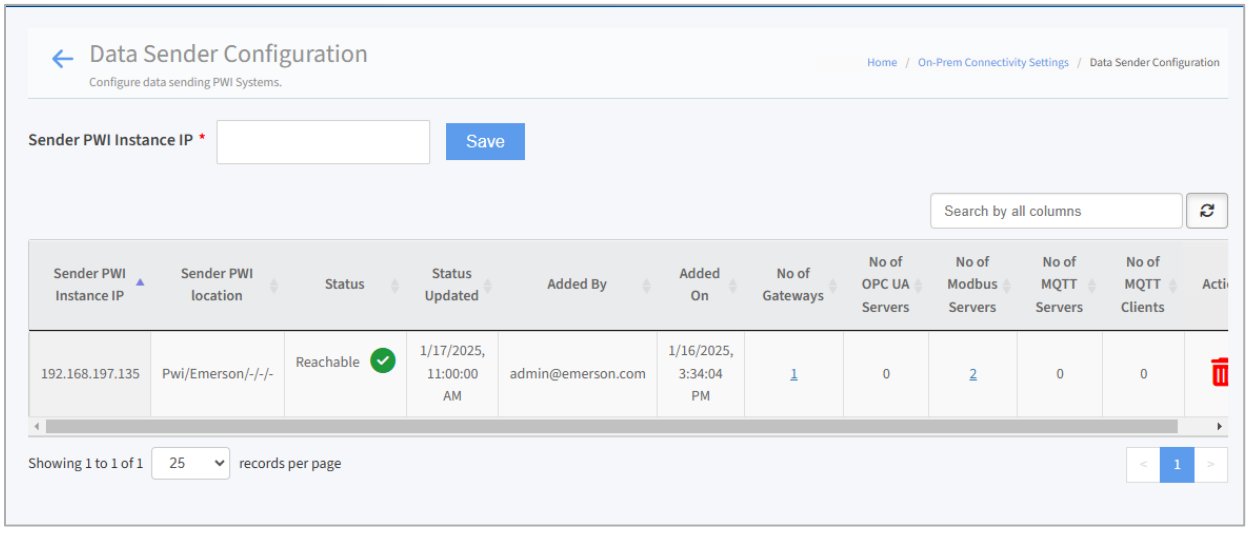
Modbus servers and the variables configured in PWI On-Prem Connector and PWI Cloud Connector systems are sent to the respective On-Prem App Only and Cloud App Only system via MQTT publish. Applications installed in the App Only system can select the variables configured in the Connector system and subscribe to their values.

Modbus server and variable synchronization occurs whenever they are added, updated, or deleted. There is also a periodic sync which occurs once an hour to avoid any data loss. The Modbus data connections and configured variables page in the App Only system are read-only, and the connections page will display site info along with filtering for sites.





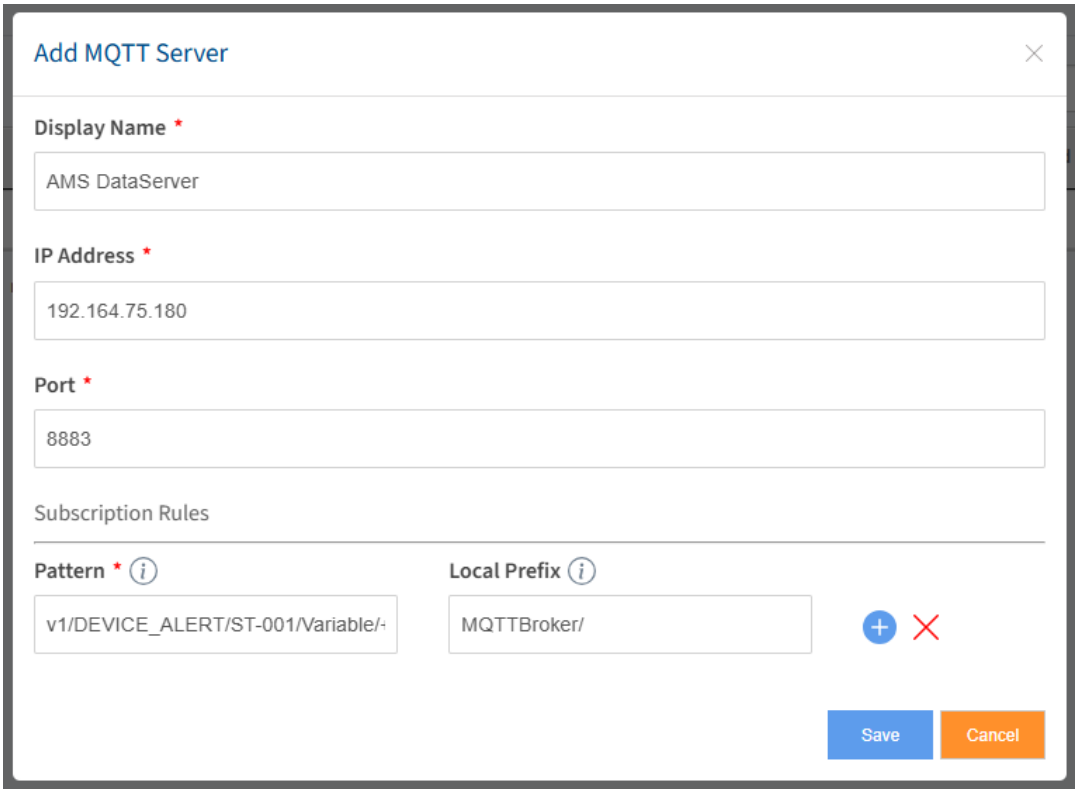
The number of data sources configured between the On-Prem Connector and App-Only system is displayed under ***On-Prem Connectivity Settings > Data Sender Configuration***.



4. MQTT Servers

Add MQTT Servers

1. Navigate to (Settings button) **> *Data Source Config* > *MQTT Sources* > *Servers*** tab and click **"Add MQTT Server"** button.
2. Enter a display name for the MQTT Client, IP address, and port (typically 8883)



Pattern

Topics matching the pattern will be shared between the brokers. The pattern must adhere to the following conditions:

1. The plus sign must follow this pattern **/+/** (in the middle) or **/+** (at the end)
2. **#** is only allowed at the end of the pattern
3. Spaces are not allowed in the pattern
4. When more than one pattern is found, the first pattern will take precedence

Local Prefix

This option allows topics to be remapped when receiving from remote brokers

Establishing Secure Connections to External MQTT Servers

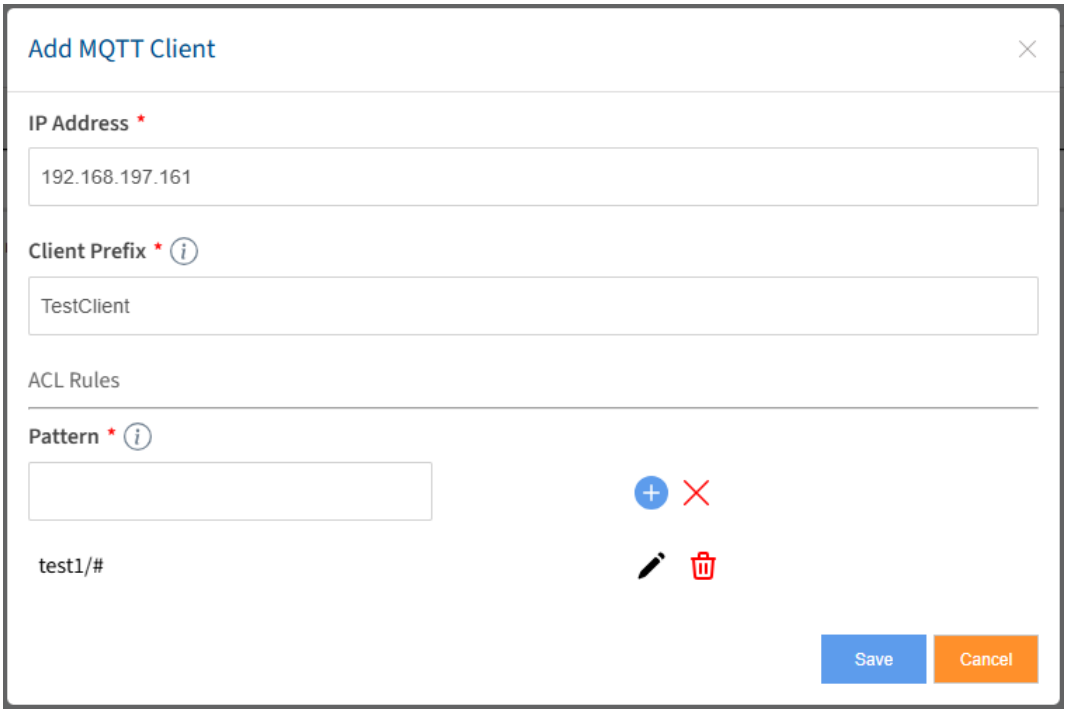
The MQTT secure connection is covered by PWI's default SSL certificate. Refer to the Certificate Management – Secure Connection Setup section. To setup a certificate for a MQTT secure server connection, download the PWI default CA certificate from ***Platform Settings > Certificate Management > Default SSL Cert*** tab and upload it to the MQTT server's trust store. Upload the MQTT server's certificate to the PWI trust store located in the **Peer Cert** tab of the **Certificate Management** page.

5. MQTT Clients

The default MQTT Service listening port for connecting to external MQTT Clients is 8883. This port is configurable from the **Ports and Protocols** page. On the MQTT Client side, users need to configure the PWI MQTT Service IP and port to establish MQTT connection.

Add MQTT Clients

1. Navigate to (settings button) ***Data Source Config > MQTT Sources > Clients*** tab and click **"Add MQTT Client"** button.
2. Enter the MQTT client IP address, Client Prefix, and the pattern(s).



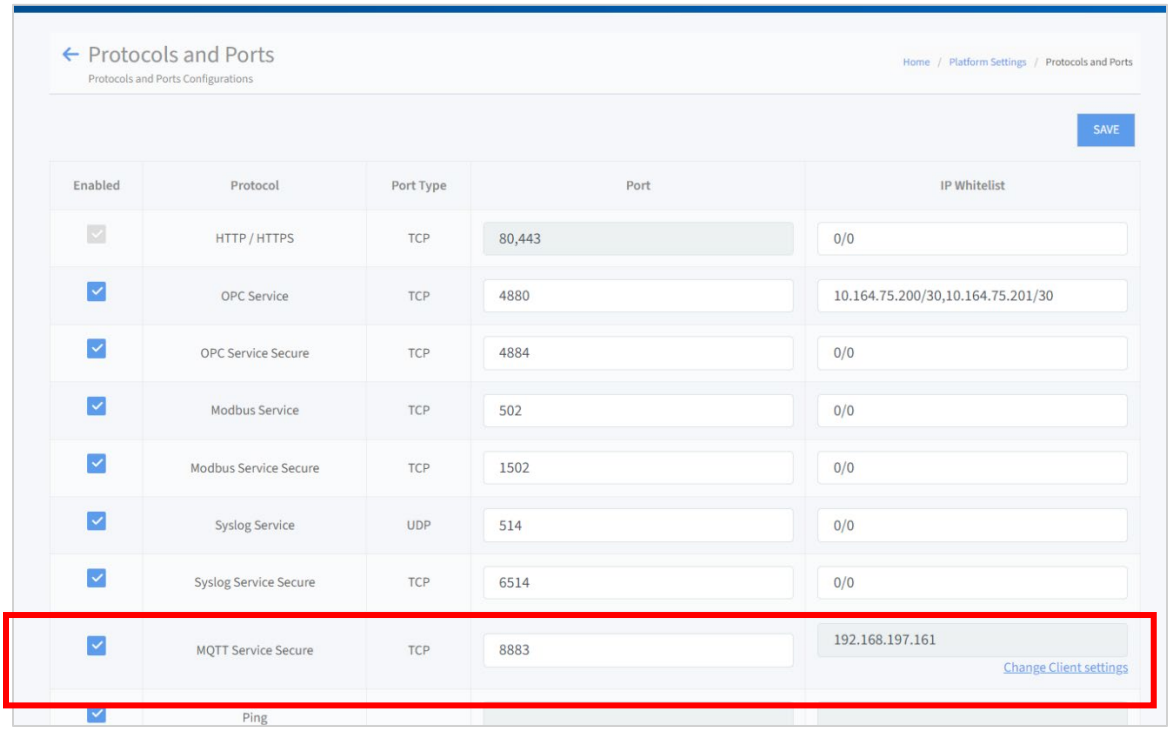
Pattern

Topics matching the pattern will be shared between the brokers. The pattern must adhere to the following conditions:

1. The plus sign must follow this pattern **/+/** (in the middle) or **/+** (at the end)
2. **#** is only allowed at the end of the pattern
3. Spaces are not allowed in the pattern
4. When more than one pattern is found, the first pattern will take precedence

NOTE: IP addresses configured as MQTT clients are automatically whitelisted and will be displayed on the **Ports and Protocols** page. Users can update the MQTT Client

configuration by clicking on the "Change Client Settings" hyperlink available in the MQTT Service Secure row.



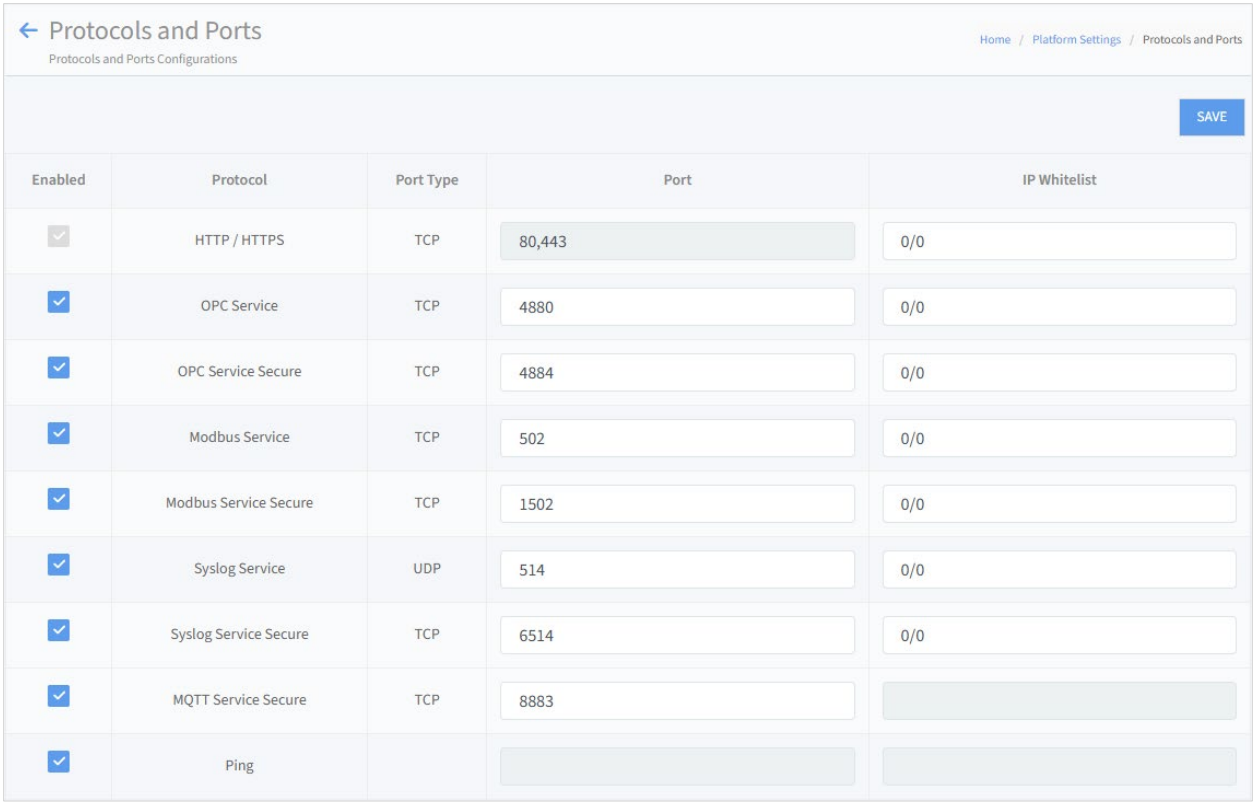
Establishing Secure Connections with External MQTT Clients

The MQTT secure connection is covered by PWI's default SSL certificate. Refer to the Certificate Management – Secure Connection Setup section. To setup a certificate for a MQTT secure client connection, download the PWI default CA certificate from ***Platform Settings > Certificate Management > Default SSL Cert*** tab and upload it to the MQTT client's trust store.

7. Data Service Configuration

1. Protocols and Ports

Navigate to (Settings button) ***> Platform Settings > Protocols and Ports***



The Protocols and Ports configuration page enables administrators to allow or disallow incoming connections from various clients.

PWI runs its services on the recommended ports by default. However, an administrator may need to change these ports due to their network policies. In such cases, port values can be updated, and the system will consider the specific port for that particular service.

IP Whitelisting

Administrators can specify particular IP addresses under the IP whitelist section as shown in the image above. By default, all IP addresses (0/0) are allowed to establish inbound connections to a PWI system. Adding IP addresses to the whitelist restricts inbound connections to only those IPs.

Service Options

The following are the available PWI services which clients can connect and communicate with. However, based on the deployment mode of the PWI system, certain services may be toggled off to simplify and secure the system.

If a user does not need a certain service, they can completely disable it by unchecking the enable button on the left column.

1. **HTTP Secure & Non-Secure**
    - Ports 80 and 443 are enabled for HTTP/HTTPS using the TCP port type to connect to the PWI system via web browser
    - Port 80 is enabled on PWI solely to redirect HTTP requests to HTTPS. This ensures that when a user enters only the IP address or hostname (without specifying protocol), the browser's initial HTTP request is automatically redirected to HTTPS, allowing the login page to load. If port 80 is disabled, the user must explicitly enter https://<PWI_IP>; otherwise, the PWI login page will not load.
    - Modification of these ports is not allowed as the system highly relies on these default ports
    - Whitelisting of specific IP addresses is possible by configuring the required IP addresses
2. **OPC-UA Secure & Non-Secure**
    - By default, this service runs on port 4880 for non-secure and 4884 for secure connections
    - The ports for this service are configurable, and IP whitelisting is supported
3. **Modbus Secure & Non-Secure:**
    - By default, this service runs on port 502 for non-secure and 1502 for secure connections
    - The ports for this service are configurable, and IP whitelisting is supported
4. **Syslog Secure & Non-Secure:**
    - Syslog service from PWI is available to receive logs from Emerson WirelessHART gateways. In this scenario, the gateway is the client and PWI is the server.
    - By default, this service runs on port 514 for non-secure and 6514 for secure connections
    - The ports for this service are configurable, and IP whitelisting is supported
5. **MQTT Secure Service:**
    - PWI features an MQTT broker that is available to interact with external MQTT servers and clients.

- When PWI is deployed as an On-Prem Connectivity Solution, the MQTT broker on the PWI systems establishes a bridge and transmits data.
- By default, this service runs on port 8883
- The ports for this service are configurable
- Whitelisting of specific IPs is done through client configuration. Users are not allowed to whitelist IP addresses for PWI's MQTT services. MQTT clients can be configured by configuring MQTT clients from **Data Source Config**
- If there are no MQTT clients configured, the PWI system will block all connections to this service

6. **Ping**

- Ping can be enabled/disabled, but the port and IP whitelist is not configurable

This section explains how to access data outputs from specific Plantweb Insight applications to use in host systems, data historians, and other network connected systems. Calculated asset variables are only available for applications that have been installed and configured with data sources. Refer to individual application manuals for specific application details. For OPC-UA® and Modbus® service, the following information is provided for installed applications:

- Asset State
- Calculated App Values
- Out of Service
- Health Index (if applicabl)
- Alert state (if applicable). This is not the same as the events and alerts being sent through API keys.

2. OPC-UA® Service

Plantweb Insight provides OPC-UA service through an internal OPC-UA server. The OPC-UA Server can accept connections from multiple OPC-UA clients.

- The OPC-UA server should be able to handle "read" requests from the clients in both polling mode and subscription mode
- The OPC-UA server should be able to handle the "write" requests from clients when the permission of the variable is "read/write". Otherwise, it will reject the request. After writing the value to the variable, the OPC-UA server will publish the data change to the applications.

- If the OPC-UA server receives the “read” or “write” operation on a non-existing variable, it will ignore it or report an error.
- If the OPC-UA server receives the “write” operation on a non-writable variable, it will reject the request.

The PWI OPC-UA server supports the following security modes:

- None
- Sign
- SignAndEncryption

The PWI OPC-UA server supports the following sets of Security Algorithm Suites:

- None (No security)
- Basic256Sha256 (Average security)
- Aes128_Sha256_RsaOaep (High security)
- Aes256Sha256RsaPss (Ultra high security)

Users can configure “Security Mode” and “Security Algorithm Suite” at the client side before initiating the connection to the PWI OPC-UA server. When “Security Mode” is set to “None”, “Security Algorithm Suite” must also be “None”.

The OPC-UA server provides an endpoint URL for both secure and insecure connections. Make sure to set the correct URL on the client side to make sure the connection is established successfully.

- URL format is: **`opc.tcp://<<opcua_server_ip>>:<<port>>/OpcUAServer`**

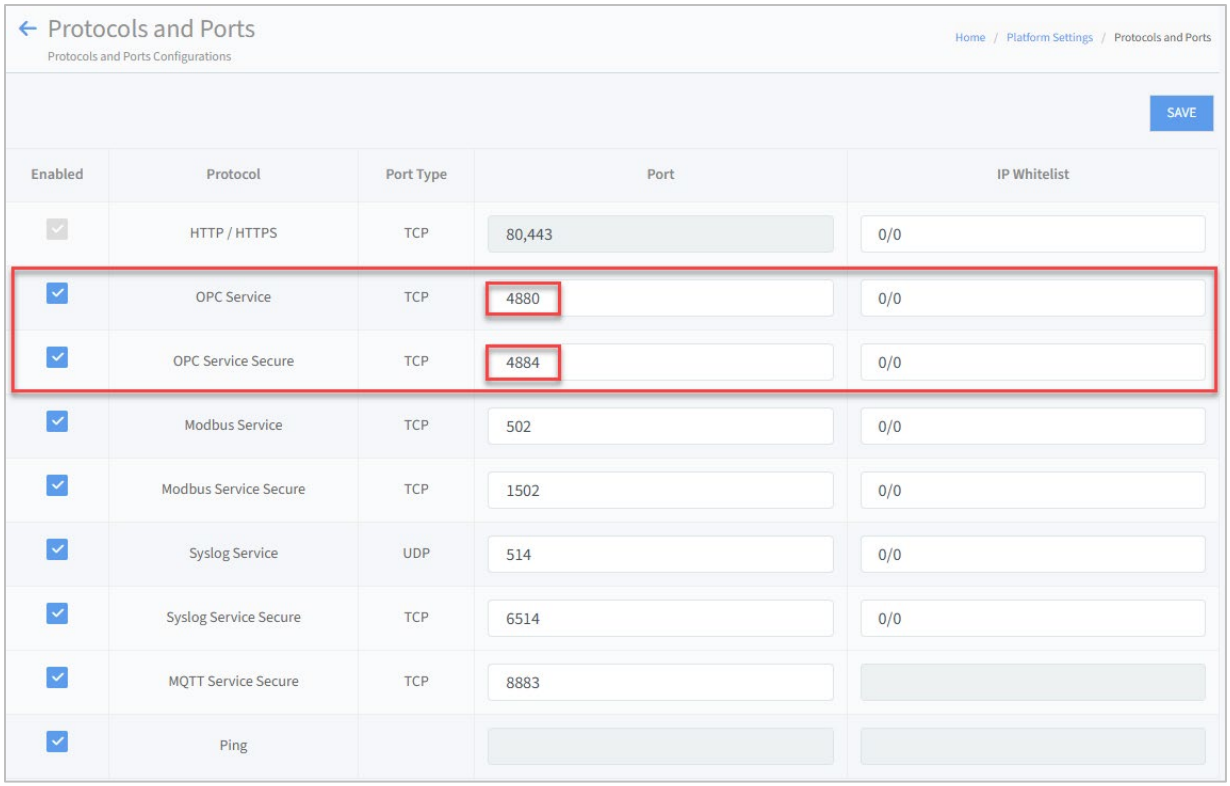
- Insecure endpoint URL. The default insecure connection port is *4880*.
  `opc.tcp://<<opcua_server_ip>>:4880/OpcUAServer`

- Secure endpoint URL. The default secure connection port is *4884*.
  `opc.tcp://<<opcua_server_ip>>:4884/OpcUAServer`

Set Ports

CAUTION: With PWI, it is possible to customize the ports for both OPC-UA® server secure and insecure connections, but we do not recommend this. Each time the port settings are updated, it will terminate and restart all services.

1. Navigate to  (Settings button) ***> Platform Settings > Protocols and Ports***.



2. Verify that the OPC-UA Service and OPC-UA Service Secure ports are enabled and update them if necessary.
3. Click the “Save” button in the top right corner.

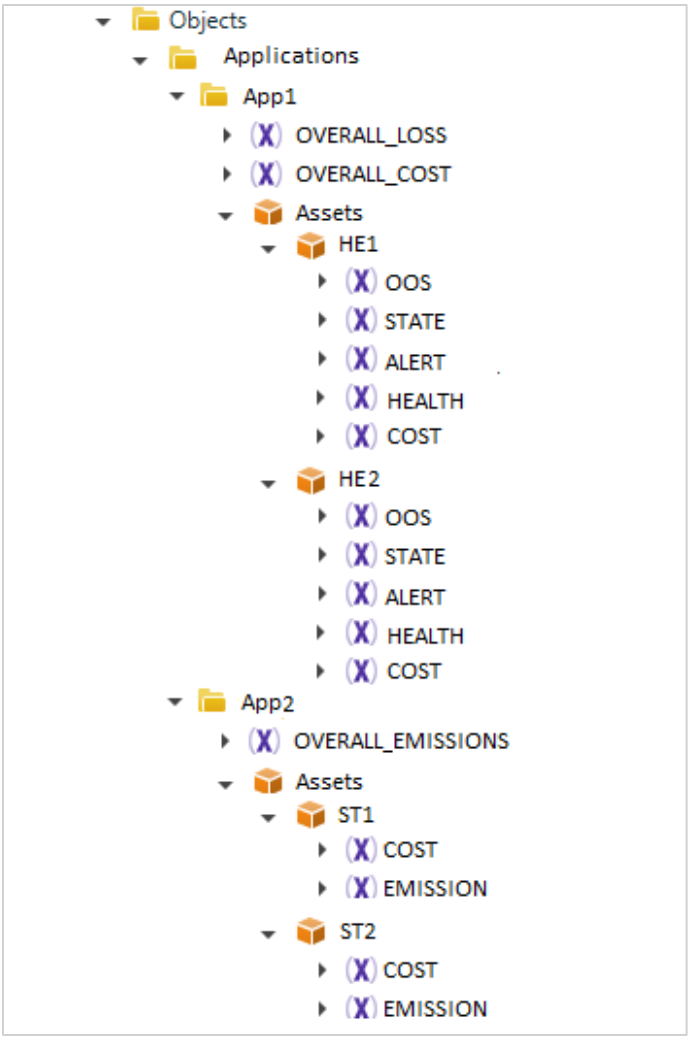
Variables Hierarchy

The PWI OPC-UA server has two types of variables:

- Asset variables
- HART-IP client variables

Asset Variables

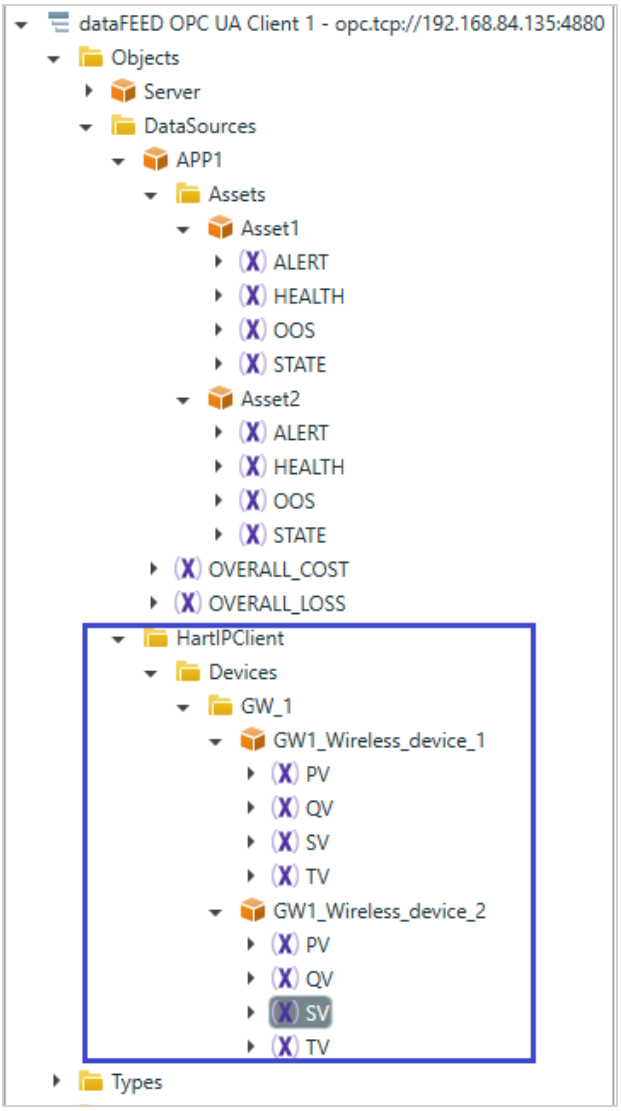
Asset variables are published from applications and organized by application and asset. Below is an example of the asset variables hierarchy inside the OPC-UA server:



- Variable path for asset variables:
  `Objects/DataSources/<<application_name>>/Assets/<<asset_name>> / <<variagble_name>>`
  Example for pump application asset: `Objects/DataSources/pump/Assets/Pump-001/ALERT`
- Among the asset variables, only the OOS variable is writable by the client. Other variables are read only.
- Refer to individual PWI Application User Manuals for full details on asset variables.

HART-IP® Client Variables

These variables are published by the HART-IP client and organized by gateway name and device name. Below is an example of HART-IP client variables hierarchy inside the OPC-UA server:



- Variable path for HART IP client variables:
  `Objects/DataSources/HartIPClient/Devices/<<gateway_name>>/<<device_name>>/<<variable_name>>`

  Example for a HART-IP client asset if the gateway name is APPVALIDATION and the device name is 708-RK1-BL1-0F-4A-7D:
  `Objects/DataSources/HartIPClient/Devices/APPVALIDATION4/708-RK1- BL1-0F-4A-7D/PV`

- All variables under gateway devices are read-only; the client cannot write these variables.

NOTE: For those not familiar with the hierarchy, Emerson recommends using an OPC-UA client with a GUI to connect to PWI's OPC-UA server to verify the hierarchy manually.

For setting up a secure connection with an external OPC-UA client, refer to the Secure Connection Setup section of this manual as well as the steps listed below:

1. **Trust the PWI Certificate in the OPC-UA Client**
   If PWI is using the default certificate, convert the PWI CA certificate to DER format using the following command:

   openssl x509 -inform PEM -in ca_pwi.crt -outform DER -out ca_pwi.der

   Upload the generated ca_pwi.der file to the OPC-UA client's trusted certificate store.

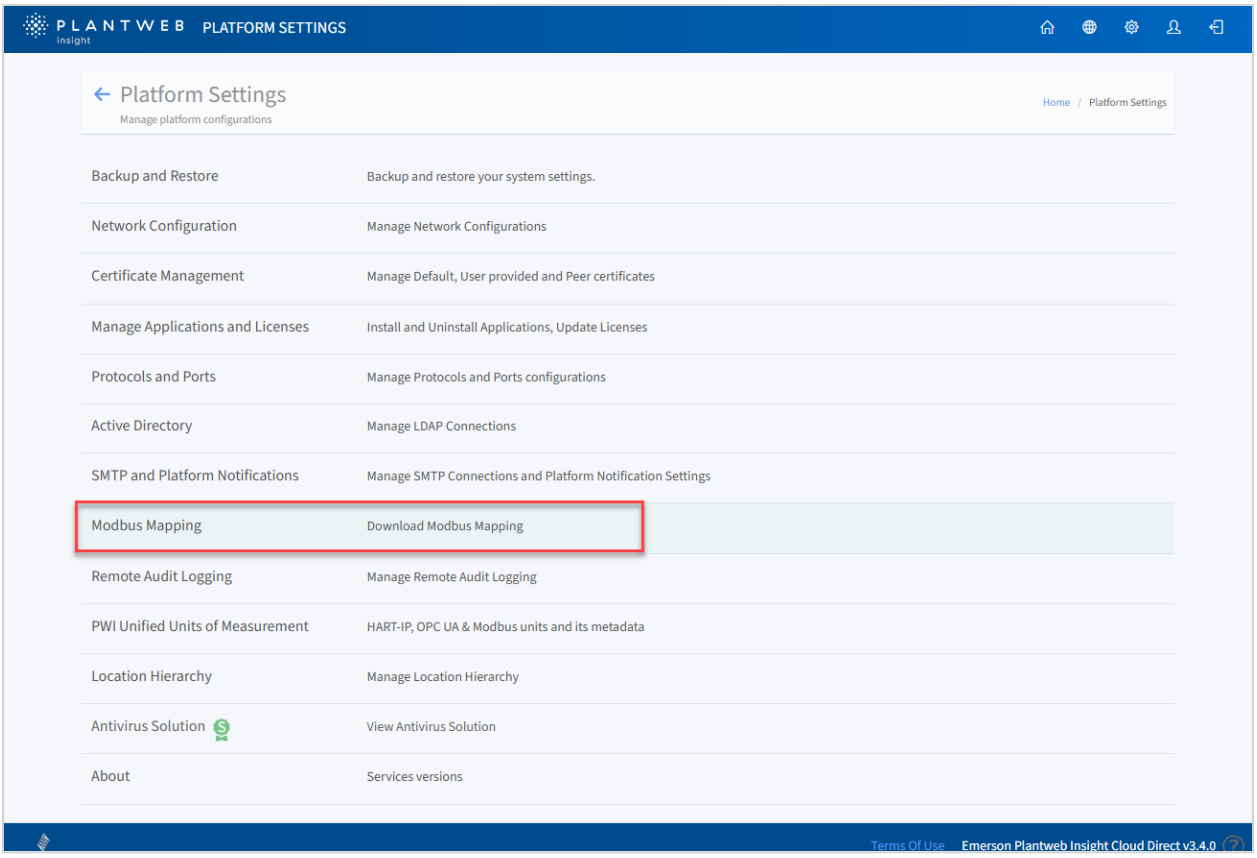
   If PWI is using a user-provided (custom) certificate, upload the corresponding DER-formatted certificate directly to the OPC-UA client's trusted store.
2. **Trust the OPC-UA Client Certificate in PWI**
   Upload the OPC UA client certificate to the PWI Peer Certificate page to establish trust on the PWI side.

3. Modbus® TCP Service

Plantweb Insight uses TCP port **502** by default for Modbus outputs from all installed applications.

Registers and tags are pre-populated for the specific Plantweb Insight applications installed. To access them, navigate to ***Platform Settings > Modbus Mapping*** and click **Download Modbus Mapping** to download a csv file.

Refer to individual application user manuals for Modbus output details.



Sample CSV File

Application ID	Function	Register	Tag	Units	Format
99	01	0	ST-001.OOS		boolean
99	04	0	ST-001.STATE		UINT16
99	04	1	ST-001.EMISSIONS	Lbs/day	FLT32
99	04	3	ST-001.COST	$	FLT32

The application ID in the first column refers to the server or slave ID.

The function in the second column refers to the generic Modbus TCP function codes.

The third column refers to the register address. For example, ST-001.STATE uses function code 4 (read input registers), starting at 300000.

Application IDs

Application ID	Application
99	Steam Trap
1	Pump
3	Heat Exchanger
4	Air Cooled Heat Exchanger
5	Pressure Relief Valve
6	Cooling Tower
8	Power Module

10	Network Management
12	Non-Intrusive Corrosion
18	Asset View

Functions

Function Code	Function	Description
01	Read coil	Obtain status of one or more discrete outputs
02	Read discrete input	Obtain status of one or more discrete inputs
03	Read holding register	Obtain value of one or more output data registers
04	Read input registers	Obtain value of one or more input data registers
05	Write single coil	Force a single discrete output
06	Write single holding register	Force a single date register to a specified value
15	Write multiple coils	Force multiple discrete outputs
16	Write holding registers	Force multiple data registers to a specified value

Registers

Function	Register Addresses	Read	Write single
Coil	00000- 065535	FC01	FC05
Discrete input	100000-165535	FC02	N/A
Input register	300000-365535	FC04	N/A
Holding register	400000-465535	FC03	FC06

Data Format

Format	Example Output	Data Format
boolean	Out of service (OOS) flag	Single bit coil
UINT16	State/Alert	16-bit unsigned register
FLT32	PV/Emissions/Cost/Health	32-bit signed float big-endian

4. REST API Service

API Keys for Emerson AMS Optics and other systems

PWI exposes an API to gather all applications and their API URL details. Only platform Admin users are allowed to create API keys. API keys can only be edited by the user(s) that created them.

```
{{url}}/api/v2/general/apps?apikey=<A valid api key>
```

The following is a sample response file:

```
{"status":true,"data":[{"id":8,"name":"bma","status":"Installed","displ
ay_name":"Smart Power Solutions","assets_service":"api/bma-
```

```
consumer/asset/all","alerts_service":"api/bma-
consumer/asset/alert/:asset_tag/:start_date","short_name":"BMA","icon":
"src/apps/battery/assets/images/icon.png?v=bkrVSGKcChK37Wq","thirdParty
Logo":null,"version":"3.0.0.DEV.7","ui_entry":null,"options_menu":null,"cu
stomBackup":false,"volumeDirectoryName":"bma"},{"id":10,"name":"nma","s
tatus":"Installed","display_name":"Network
Management","assets_service":"api/nma-
consumer/asset/all","alerts_service":"api/nma-
consumer/asset/alert/:asset_tag/:start_date","short_name":"NM","icon":"
src/apps/networkmanagement/assets/images/icons/icon.png?v=T4rJZ3Iz1k3Ah
wX","thirdPartyLogo":null,"version":"3.0.0.DEV.5","ui_entry":null,"option
s_menu":null,"customBackup":false,"volumeDirectoryName":"nma"}]}
```


This response is an array of application definitions:

- The “asset_service” property holds the URL of the Assets API
- The “alerts_service” property holds the URL of the Alerts API

Assets API

This API returns all the configured assets under a specific application. The following is an example URL:

```
{{url}}/api/<application_name>-consumer/asset/all (pass apikey in headers)
or
{{url}}/api/<application_name>-consumer/asset/all?apikey=<A valid apikey> (apikey
as a querystring)
```

All application URLs look similar except the <application_name> in the center of the URL

Alerts API

Alerts of a specific asset from a specific date onwards can be fetched from this API. The following is an example URL:

```
{{url}}/api/<application_name>-consumer/asset/alert/<asset_tag>/<from_date>
or
{{url}}/api/<application_name>-
consumer/asset/alert/<asset_tag>/<from_date>?apikey=<A valid apikey>
```

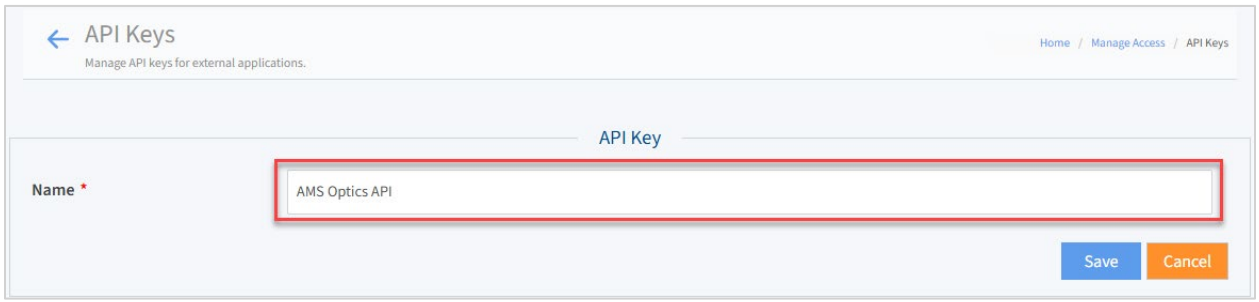
For application-specific API key information, please refer to individual application user manuals.

NOTE: Application URLs may change over time with new PWI versions. It is recommended to rely on the Get Apps API mentioned at the beginning of this section to know the applications and their URLs.

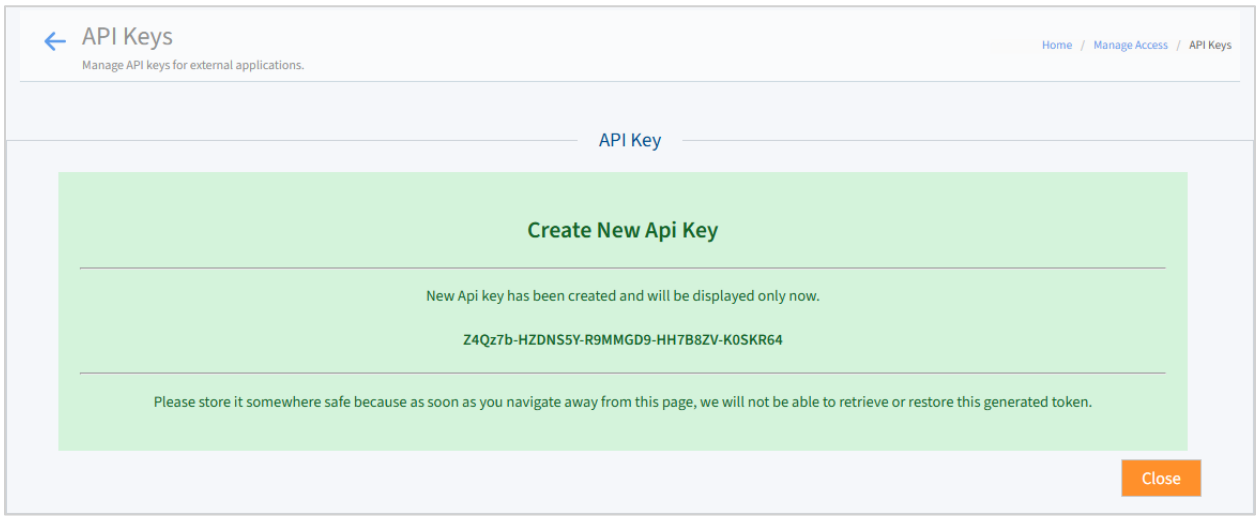
Procedure

1. Navigate to ***User Settings > Manage Access > API Keys*** and click **CREATE NEW API KEY** button.

2. Enter a name for the API key in the NAME text box and click **SAVE.**



3. The newly created API key is displayed. Copy the key and save it somewhere secure. The API key will not be retrievable after the form is closed.



4. Click **CLOSE.** The new API key will appear on the API key table.

5. To delete an API key, click the trash can icon in the **Action** column next to the key to be deleted. Then click "Delete" to confirm.

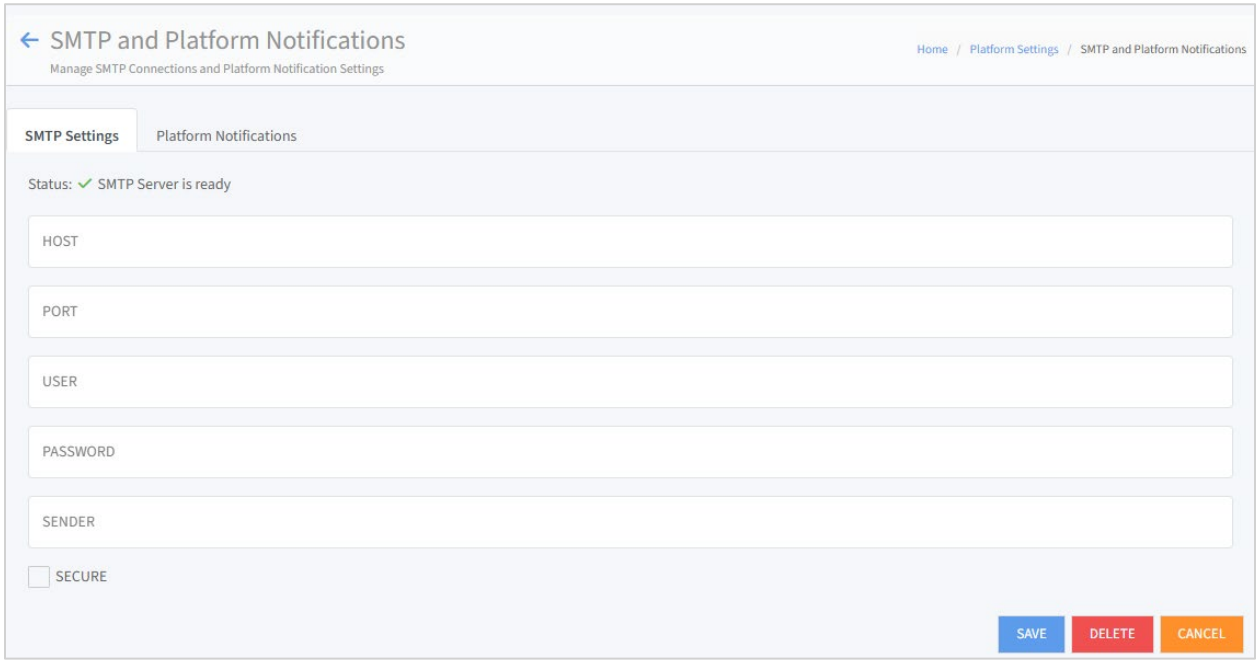
6. SMTP (Email) Notifications

PWI features an SMTP client for configuring email notifications from applications and the platform. Refer to individual application user manuals for application-specific email notification content.

A SMTP server must be available to PWI via network connection for email alerts to be configured.

Procedure

Navigate to  (Settings button) ***> Platform Settings > SMTP and Platform Notifications***



1. **Non-TLS Configuration**

Default Setting – "Secure" checkbox is unchecked and transmission will be unencrypted. Users can enable TLS connection by checking the "Secure" checkbox which enables STARTTLS

a. Enter Host name
b. Enter Port **25**
c. Enter Sender email address
d. Click **SAVE**

2. **STARTTLS Configuration with Username and Password (Gmail example)**
    a. Enter Host name (e.g. smtp.gmail.com)
    b. Enter Port **587**
    c. Check **"Secure"** (enables TLS)
    d. Enter User Gmail ID and password
    e. Enter Sender email address
    f. Click **SAVE**
3. **Implicit TLS with Username and Password (Gmail example)**
    a. Enter Host name (e.g. smtp.gmail.com)
    b. Enter Port **465** (encrypts connection)
    c. "Secure" is checked automatically
    d. Enter User Gmail ID and app password
    e. Enter Sender email address
    f. Click **SAVE**

NOTE: To configure email alerts using Gmail SMTP with TLS, generate a Google App Password from https://myaccount.google.com/apppasswords and use it as the value for the Password field on the PWI SMTP page.

The Gmail account must have 2-Step Verification enabled in order to generate an App Password.

8. Advanced Configuration

1. Certificate Management – Secure Connection Setup

PWI Certificate Management Guidelines

The following PWI components support secure connections:

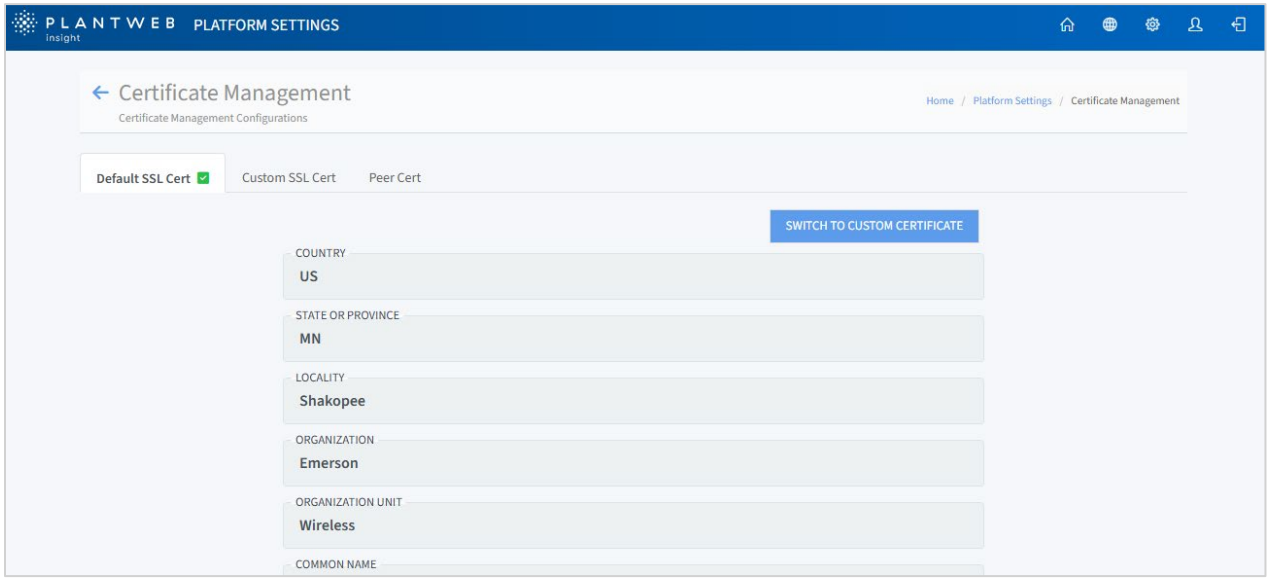
PWI Endpoint	PWI-Cert	AUTH	Peer	Required Fields

Web Server / RESTful Server	Default/Custom	Server only	Browser, REST API Client	IP/FQDN in SAN (not enforced)
OPC-UA Server	Default/Custom	Mutual	OPC-UA Client	URI in SAN (enforced)
OPC-UA Client	Default/Custom	Mutual	OPC-UA Server	URI in SAN (enforced)
MODBUS Server	Default	Mutual	MODBUS Client	
Syslog-ng Server	Default	Mutual	WiHART-GW (syslog-ng client)	IP in SAN (not enforced)
Syslog-ng Client	Default	Server only / Mutual	Remote logging syslog-ng server (Audit logs)	IP in SAN (not enforced) - depend on Remote Server configuration
SMTP	None	Server only	Mail Server (public/private)	
LDAP Client	None	Anonymous	Active Directory Server	
HART-IP Client	Default	Mutual + Whitelist	WiHART-GW (HART-IP Server)	
MQTT Client	Default	Mutual	MQTT Server (VH data server)	IP in SAN (not enforced)
MQTT Server	Default	Server only	MQTT Client (VH data link)	IP in SAN (not enforced)
IoT Hub Data Sender	None	Server only	Azure IoT Hub	
IoT Hub Data Reader	None	Server only	Azure IoT Hub	

***SAN** = Subject Alternative Name

Default SSL Certificate

Navigate to  (Settings button) ***> Platform Settings > Certificate Management > Default SSL Cert*** tab



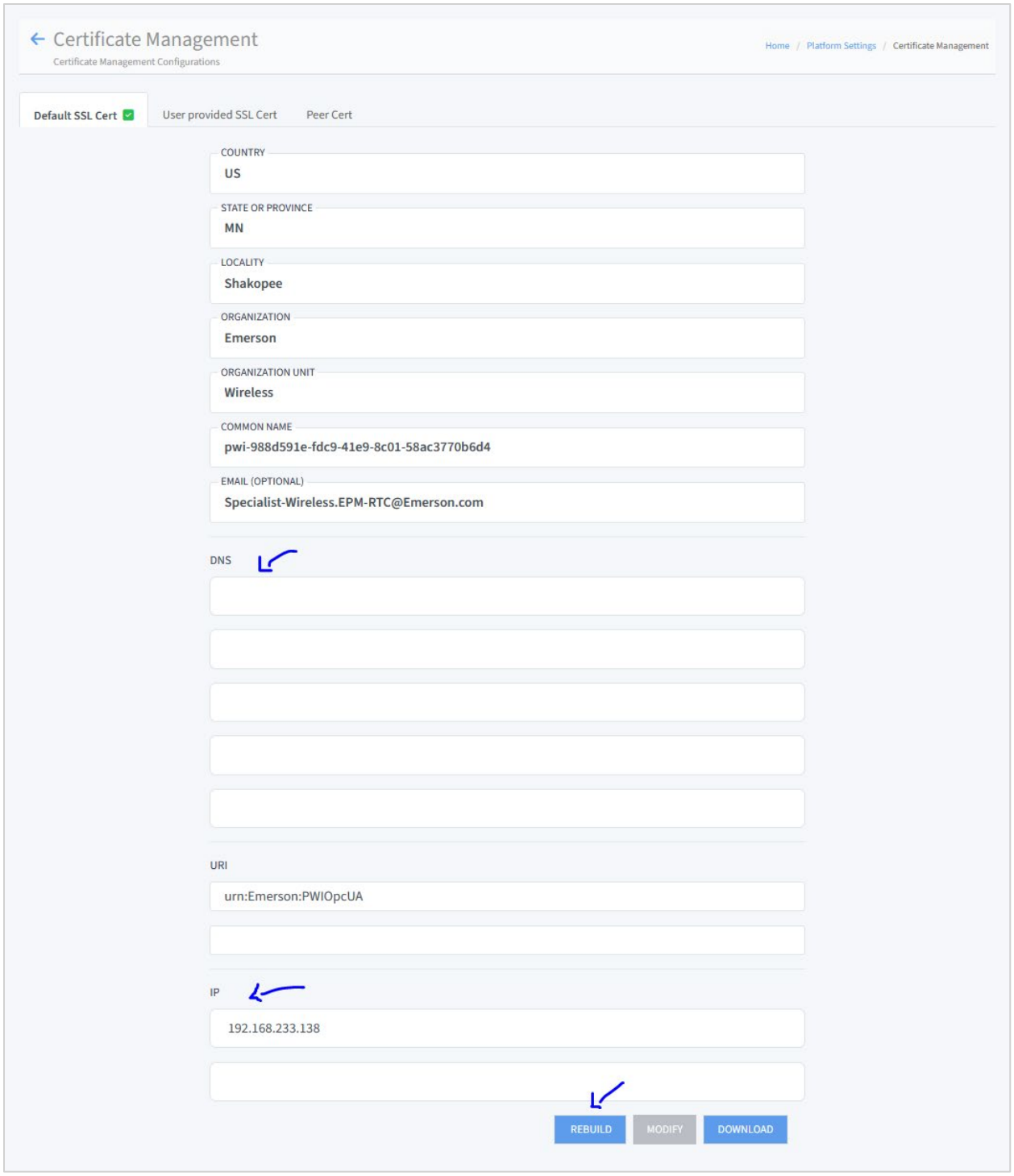
As the name suggests, the Default SSL Cert is the SSL certificate that comes with PWI by default. This SSL certificate is used by the respective PWI components listed in the table in PWI Certificate Management Guidelines.

Modifying Fields in PWI's Default SSL Certificate

To modify fields in the PWI Default Certificate, click on the **MODIFY** button to edit the fields of the Default Certificate.

The input fields of the Default Certificate will become editable.

NOTE: Users who want to connect their PWI to external syslog servers via **TLS** must ensure the IP address is included in the SAN field as shown in the screenshot, as IP addresses in SAN are **enforced**. If PWI uses a hostname, users should also include the hostname and FQDN in the DNS field.



Once all the modifications are made, click on the **REBUILD** button to rebuild the certificates.

Downloading the PWI Default Certificates

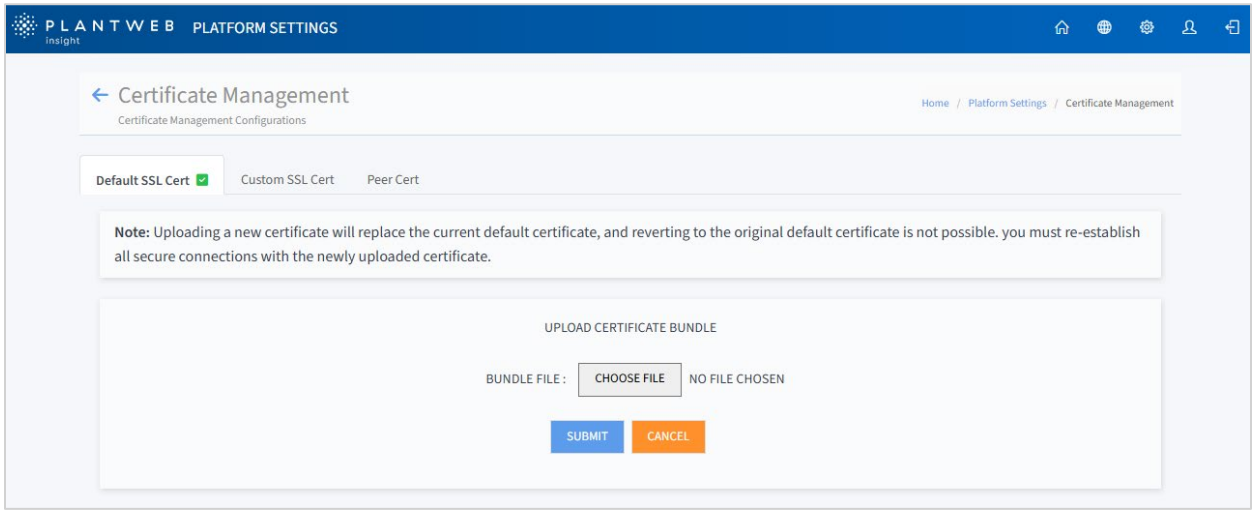
To download the PWI Default Certificates, users can click on the **DOWNLOAD** button to download the certificates.

Clicking the **DOWNLOAD** button will download 3 files from PWI:

1. **`ca_pwi.crt`** - This is the CA certificate
2. **`pwi_cert.crt`** - This is the PWI certificate issued by the CA
3. **`pwi.pem.crl`** - This is the PWI Certificate Revocation List

Uploading Third-Party Certificates

Users can upload their third-party certificates to replace the default certificates by clicking the **SWITCH TO CUSTOM CERTIFICATE** button.



Users are expected to upload the following items as a **single file bundle in PEM or PFX format**:

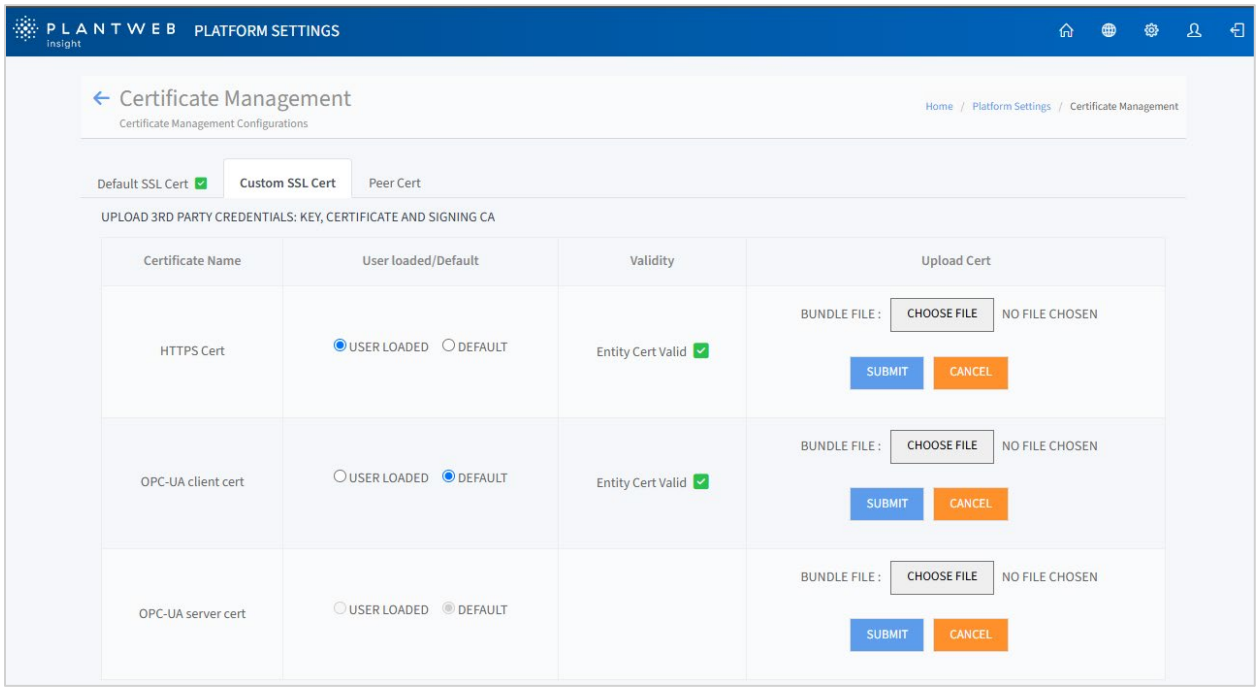
1. **Entity Certificate (cert that PWI will use)**
2. **Entity Certificate Private Key (private key of entity certificate – must be RSA key type)**
3. **Intermediary CA Certificates (if applicable)**
4. **Root CA Certificate (if applicable)**

Upon uploading this certificate bundle, PWI will verify and validate the certificate chain, entity certificate's private key, and expiration date. If PFX format is used, PWI will prompt the user to enter the certificate password.

The **URI** in the **Subject Alternative Name** is required in the default certificate upload as the Default certs may be used for **OPC-UA Server/Client** connections which requires the URI entry in SAN.

Custom SSL Certificate Upload

Navigate to (Settings button) **> *Platform Settings* > *Certificate Management* > *Custom SSL Cert*** tab



In the Custom SSL Cert tab, users can upload their third-party certs for the respective services. The file format expected to be uploaded is the **same as the Default SSL Custom Certificate upload**.

Users are expected to upload the following items as a **single file bundle in PEM or PFX format**:

1. **Entity Certificate (cert that PWI will use)**
2. **Entity Certificate Private Key (private key of entity certificate – must be RSA key type)**
3. **Intermediary CA Certificates (if applicable)**
4. **Root CA Certificate (if applicable)**

Upon uploading this certificate bundle, PWI will verify and validate the certificate chain, entity certificate's private key, and expiration date. If PFX format is used, PWI will prompt the user to enter the certificate password.

The **URI** in the **Subject Alternative Name** is required in both the OPC-UA Server and Client certificate upload.

Users can choose between using the Default certificate or User uploaded certs for the respective services. The radio toggle buttons are disabled until the user uploads their certificate for the respective services.

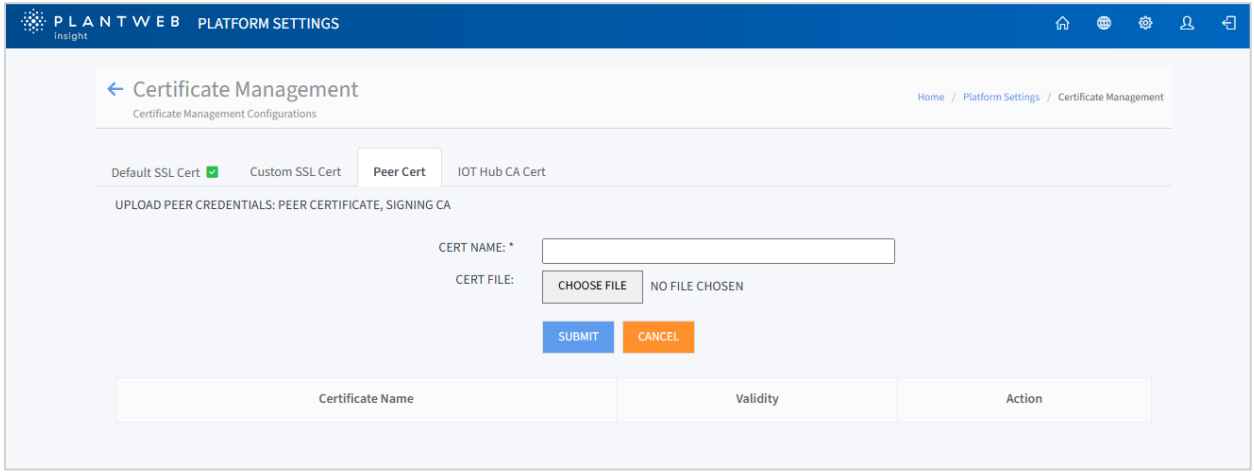
Peer Certificate Upload

Navigate to (Settings button) > ***Platform Settings*** > ***Certificate Management*** > ***Peer Cert*** tab

Users can upload certificates into the PWI trust store via the Peer Cert tab.

Accepted certificate types:

- **DER**
- **PEM**



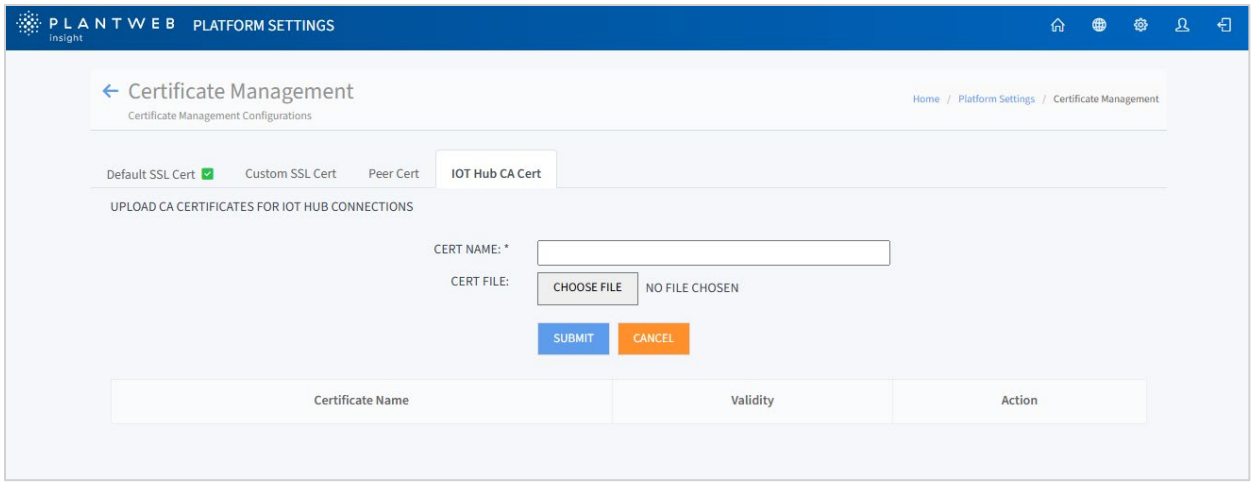
Microsoft Azure IOT Hub CA Cert Upload

Navigate to (Settings button) > ***Platform Settings*** > ***Certificate Management*** > ***IOT Hub CA Cert*** tab

This tab is only available for **Cloud Connector Mode (PWI-IOTCS)** and **PWI Cloud App Only** variants. Users may need to upload their corporate certificate if their corporate network has **SSL Bridging devices** and is **affecting connections to Microsoft Azure**.

Accepted certificate types:

- **DER**
- **PEM**



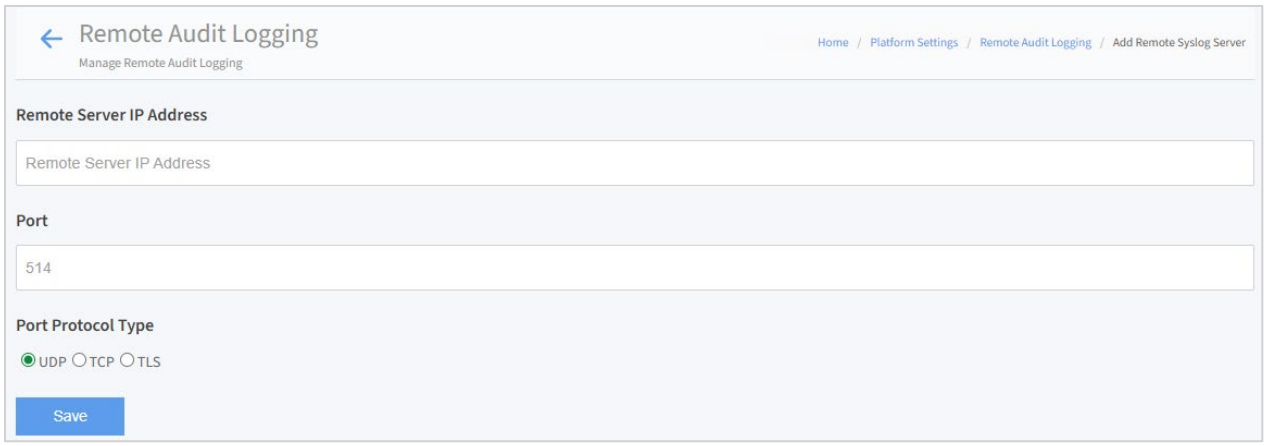
2. Audit Logs (Remote Syslog Servers)

Connecting to an External Syslog Server

Syslog-ng logs can be forwarded to external syslog servers. For a full list of events captured in the PWI Platform Audit Log, refer to Appendix B – Events Captured in Platform Audit Log

Navigate to  (Settings button) **> *Platform Settings* > *Remote Audit Logging*** and click **Add Remote Syslog Server** button. Enter the remote server IP address and desired port number. Choose desired protocol and click **Save.**

The supported port protocols are UDP, TCP & TLS.



Certificates

PWI CA Certificate

Ensure the IP address is included in the SAN field, as IP in SAN are enforced.
If PWI uses a hostname, users should also include the hostname and FQDN in the DNS field.

After adding, click on the **REBUILD** button to rebuild the certificates.

Once the modifications are complete, you can click on the **DOWNLOAD** button to download the CA certificate.

Refer to the Modifying Fields in PWI's Default SSL Certificate section.

Adding a Peer Certificate

If syslog-ng is using TLS protocol to connect to external syslog servers, ensure that the CA certificate of the external syslog servers is included in the PWI platform.

To add a peer certificate to the syslog-ng trust store, users can upload it via ***Platform Settings > Certificate Management > Peer Cert***

Refer to the Peer Certificate Upload section.

If the CA certificate is updated and remote syslog servers were previously configured using the TLS protocol, ensure you remove the existing remote syslog server configuration and reconfigure it. This guarantees that a new TLS connection is successfully established with the updated certificate.

Log Rotation

The audit logs are retained for **90 days**, with daily rotation of the log file. Log rotations occur at **1-hour intervals**. All containers in the platform are consolidated into a single platform log file, while each application maintains its standalone log file.
Files are deleted in a first in, first out sequence (oldest file deleted first).

Platform Logs

The current log file rotates under the following conditions:

- The log file exceeds 100MB in size
- 1 day has passed

Rotated log files will be deleted if:

- 90 days have passed
- There are more than 450 log files (an estimation based on five rotations per day)

Application Logs

The current log file rotates under the following conditions:

- The log file exceeds 10MB in size
- 1 day has passed

Rotated log files will be deleted if:

- 90 days have passed
- There are more than 450 log files (an estimation based on five rotations per day)

Backup and Restore

Remote syslog servers and filesystem logs are included in PWI restorable backups.

You can perform backup and restore via ***Platform Settings > Backup and Restore***.

To create a restorable backup, refer to the Restorable Backup section.

3. Antivirus

PWI contains an internal antivirus solution as of version 3.3.1 and later. Use of the antivirus solution requires a valid license to activate the functionality.

Install the PWI antivirus license in ***Platform Settings > Manage Applications and Licenses > Licenses*** tab.

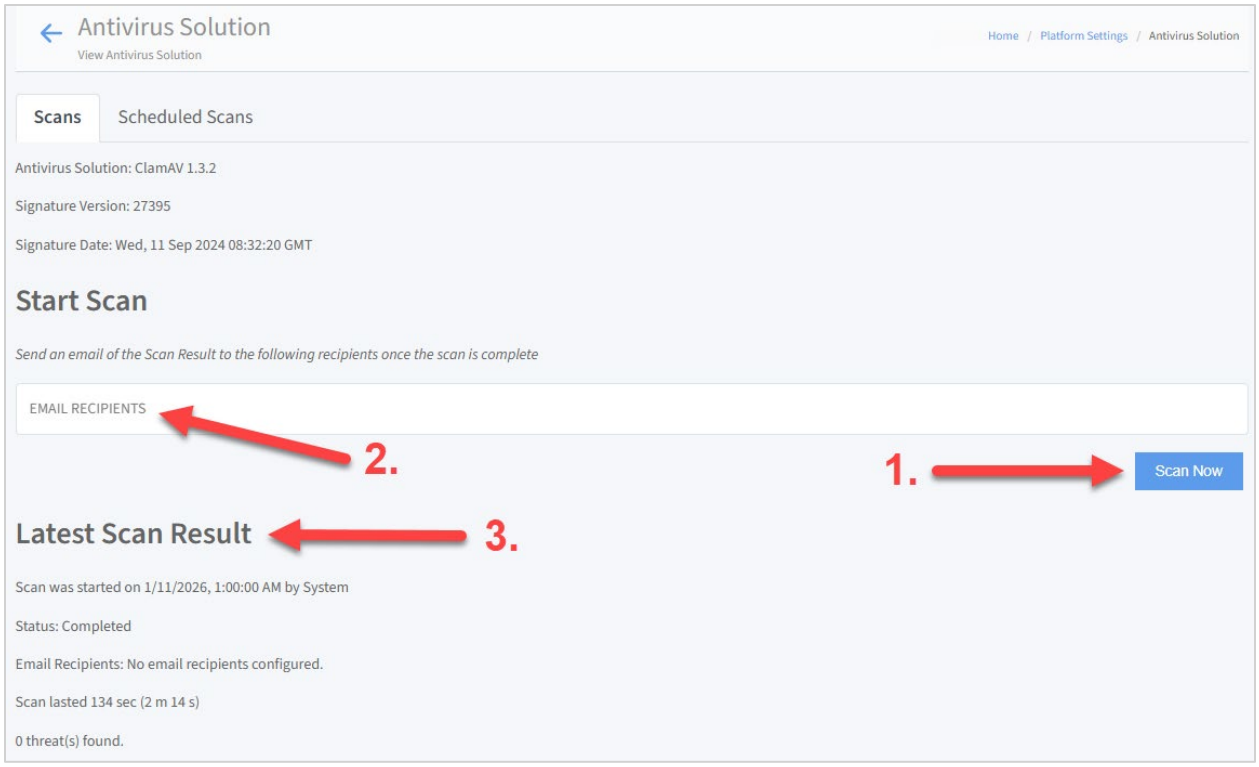
Once a valid license has been entered, navigate to ***Platform Settings > Antivirus Solution***

Scans Tab

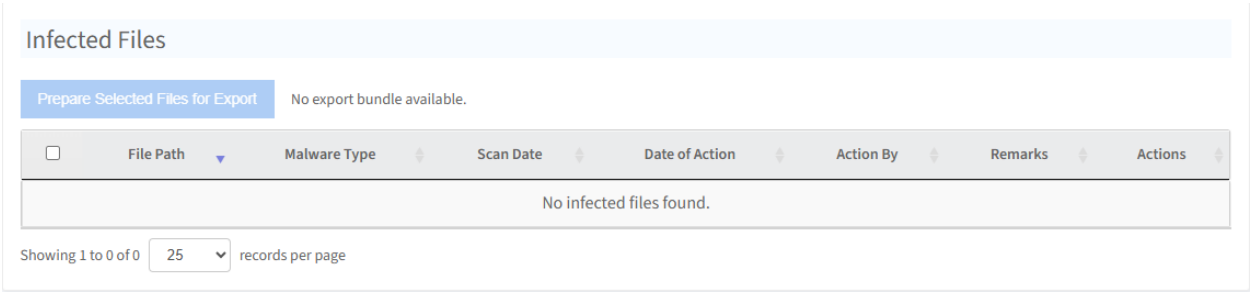
To perform an antivirus scan, click the **Scan Now** button (1).

To configure email recipients to receive scan results, enter valid email addresses in the email recipients' field (2). A SMTP server must be available to PWI via network connection for email alerts to be configured. Refer to SMTP (Email) Notifications for more information.

View details of latest scan results (3).



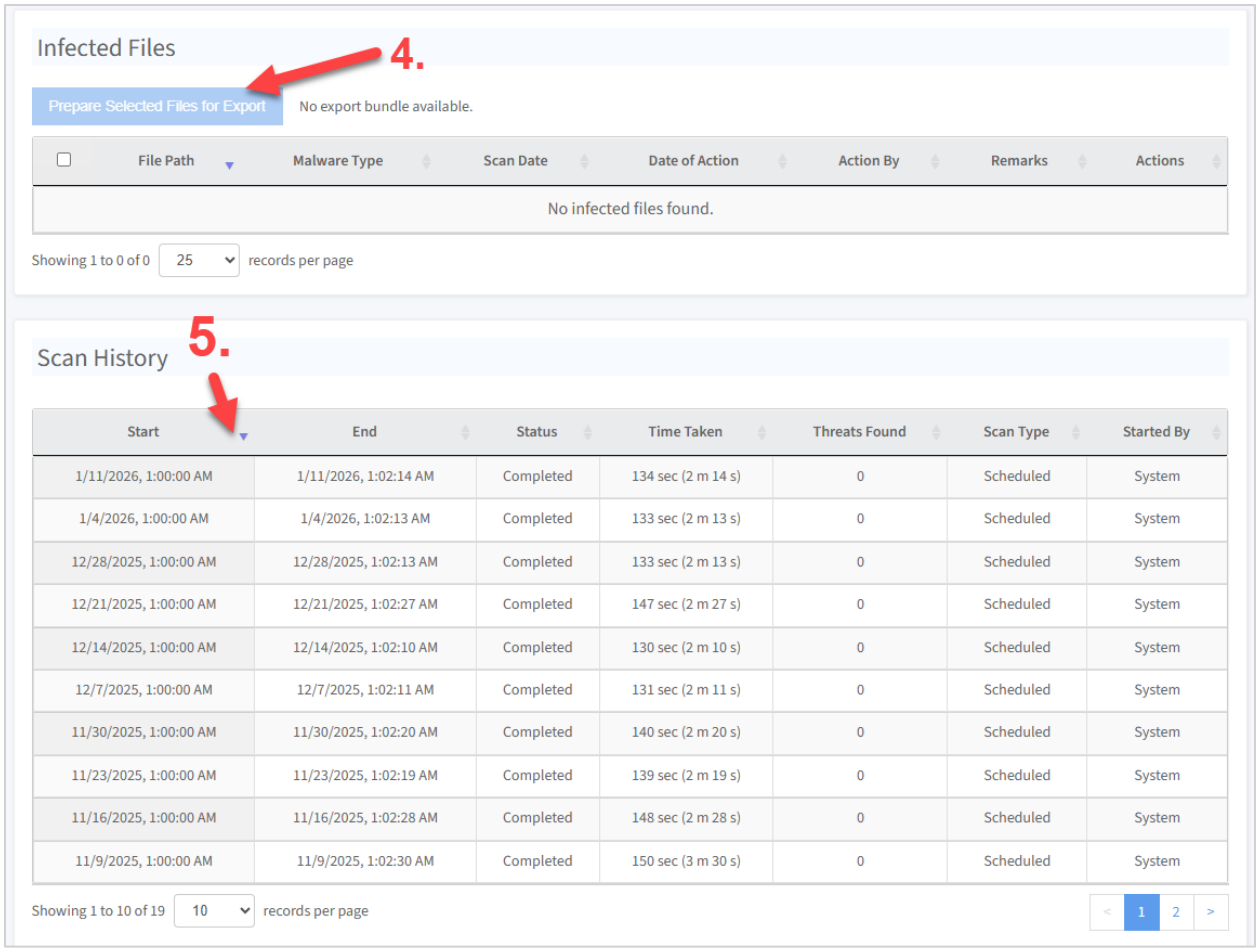
View and export infected files (4). PWI's antivirus solution provides the flexibility to quarantine any files determined to be potentially infected. Users can quarantine the infected file from the Actions column. Later, the user can choose to delete or restore the quarantined file.



Please share any potentially infected files with plantwebinsightsupport@emerson.com for diagnoses and confirmation. The exported file will be in encrypted format . To decrypt the extracted infected file, Please use the following command:

```
openssl aes-256-cbc -d -a -pbkdf2 -in infected_files_export.encrypted -out
infected_files_export.zip
```

The Scan History table (5) provides a log of all antivirus scans, both scheduled and user initiated.

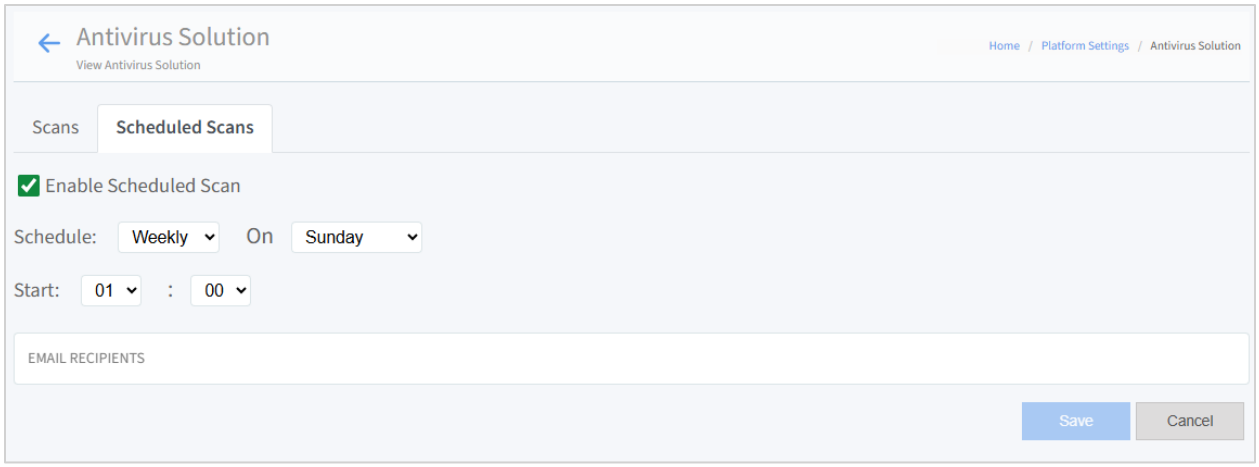


Scheduled Scans Tab

To configure scheduled antivirus scans, check the box next to **Enable Scheduled Scan**. Configure the frequency, day and time for scheduled scans to occur. Users can choose Daily, Weekly, or Monthly frequency, and can specify the day and time for the scan to initiate.

Email recipients configured on this screen will receive results of scheduled scans.

Click **Save** button to save antivirus scan configuration.


Antivirus Solution
View Antivirus Solution
Home / Platform Settings / Antivirus Solution
Scans
Scheduled Scans
Enable Scheduled Scan
Schedule: Weekly On Sunday
Start: 01 : 00
EMAIL RECIPIENTS
Save
Cancel

9. Post-Installation Checklist for New Deployment

When creating a new PWI virtual machine, please ensure the following configurations are verified and properly set before proceeding with application installation:

1. **DNS Configuration**

   If the PWI network interface is configured with a static IP address, the DNS server settings must be manually configured to enable access to network services and devices via Fully Qualified Domain Names (FQDN).
   You can verify and configure DNS settings via:
   PWI UI → Platform Settings → Network Configuration → DNS Servers

2. **Time Synchronization**

   Ensure that the PWI system time is synchronized with a valid NTP (Network Time Protocol) server.
   Check the synchronization status via:
   PWI UI → Platform Settings → Network Configuration → NTP Servers
   The status should display **"Synchronized"**, and the server time (in UTC) should align closely with the NTP server time.

3. **Docker Network Subnet Conflicts**

   PWI utilizes Docker containers that operate on the default Docker network subnet **172.18.0.0/16.** This subnet must not conflict with the external network to which the PWI is connected. If a conflict is detected, you must modify the Docker network subnet via:
   PWI UI → Platform Settings → Network Configuration → Docker Network Subnet
   Note: Changing the Docker network subnet requires a PWI VM restart to take effect.

4. **Rebuild PWI Default Certificate with PWI IP and Hostname**

   Rebuild PWI Default certificate with PWI IP address and hostname via:
   PWI UI → Platform Settings → Certificate Management → Default SSL Cert

5. **Network Port enabled for Data source Connection**

   Please ensure that all necessary ports are enabled and accessible based on your data source configuration to avoid communication issues.

   Gateway HART-IP Communication

- Insecure Connection: **Port 5094** is used for insecure HART-IP communication. This port must be open across the network when PWI connects to the Gateway in insecure mode.
- Secure Connection: **Port 5095** is used for secure HART-IP communication. Port 443 is required for certificate exchange when configuring the Gateway in secure mode. Both **ports 443** and 5095 must be enabled across the network for secure communication.

Other Data Sources

If PWI is configured to connect to other data sources such as OPC-UA servers, Modbus servers, or MQTT brokers, the corresponding ports for each protocol must also be enabled across the network to ensure proper connectivity.

10. Troubleshooting

For direct PWI technical support, please submit a request through the link below or scan QR code PWI Technical Support Request Link

1. Unable to Access PWI UI

a) Verify that the PWI is reachable from the browser host using the ping command.
b) Ensure that **port 443** is accessible using the following PowerShell command:
`Test-NetConnection -ComputerName <PWI_IP> -Port 443`

2. PWI Cannot Connect to Wireless*HART* Gateway

a) Confirm that **port 5094** is open and accessible across the network.
b) Check the PWI diagnostic backup file (`vm_diagnostics`) `iptables` section. Ensure a firewall rule named `pwi_cont_egress` exists for the Gateway IP and port 5094.
    - If the rule is missing, delete the Gateway configuration from the PWI UI and re-add it to regenerate the rule.
c) Review the ARP table in PWI diagnostic backup file (`vm_diagnostics`):
    - For PWI versions **3.3.0 and earlier**: check `arp` section.
    - For versions **3.4.0 and later**: check `ip neigh show` section.
    - If the Gateway and PWI are on the **same subnet**, verify that the MAC address of the Gateway IP is resolved.
    - If they are on **different subnets**, ensure the MAC address of the **default gateway** for the PWI network is resolved.

3. PWI Cannot Establish Secure Connection to Gateway

a) Ensure that the system time is synchronized on both the PWI and the Gateway.
b) Confirm that **ports 443 and 5095** are open and accessible across the network.
c) Check the `iptables` section in the `vm_diagnostics` file to verify that a firewall rule named `pwi_cont_egress` exists for the Gateway IP and port 5095.
d) Review the ARP table as described in section 2c to ensure proper MAC address resolution.
e) Verify the presence of the Gateway certificate:
    - Navigate to diagnostic backup `opt_pwi/volume/security/trusted_store`
    - Ensure a certificate file named after the Gateway IP exists.
    - Use the following command to retrieve the certificate hash: `openssl x509 -noout -hash -in <cert_name>`
    - Confirm that a symbolic link file named `<certificate_hash>.0` is present.
    - If either the certificate file or the hash link is missing, the secure connection cannot be established.

4. License Failure After Network Settings Change

- The PWI locking code is generated based on the IP and MAC address of the PWI network interface. Therefore, any changes to the network settings will alter the locking code, causing the installed license to become invalid.
- To reduce the need for frequent license regeneration, we recommend using a static IP address instead of DHCP. Ensure all network settings are finalized before generating the license.
- Refer to License Management – Locking Code for more information.

5. PWI Certificate Conversion for OPC UA Secure Connection

- OPC-UA secure connections require certificate exchange in DER format between the client and server. However, the default certificate downloaded from the PWI UI is in PEM format.
- Users must manually convert the certificate using the following command: `openssl x509 -inform PEM -in ca_pwi.crt -outform DER -out ca_pwi.der`

6. Lost User Password

- Users with an Admin role can reset passwords for other users.
- If a user forgets their password, an Admin can reset it on their behalf.

- It is strongly recommended to always maintain at least one Admin user in the system. If the last Admin account is deleted or its password is lost, the PWI system settings cannot be modified, potentially rendering the system unusable.
- If a user has lost their username and password, and there are no other valid credentials to access the PWI system, the last option is to re-install the virtual machine file to reset the system back to factory default settings.
- Emerson takes cybersecurity very seriously, and for this reason, does not currently offer any sort of master password or backdoor for password reset. Once the default credentials have been changed, it is ultimately the user's responsibility to securely manage their passwords.

7. Test Connectivity

Test TCP connectivity

To check server TCP connectivity from **Windows** machine, it need launch PowerShell and test connectivity using below command

```
Test-NetConnection -ComputerName <IP> -Port <Port>
```

To check server TCP connectivity from **Linux** machine, start the console and test connectivity using below command:

```
nc -vz <IP> <Port>
```

Test Secure Conntivity (TLS) to Server

To test server secure/TLS connectivity, a command called "openssl s_client" is required. This command can be used to test secure connection from PWI to a LDAP server, SMTP server, Remote Audit Log Server etc:

```
openssl s_client -connect <IP>:<Port> -showcerts
openssl s_client -connect <IP>:<Port> -tls1_2 -showcerts
```

8. Fail to Login PWI by LDAP

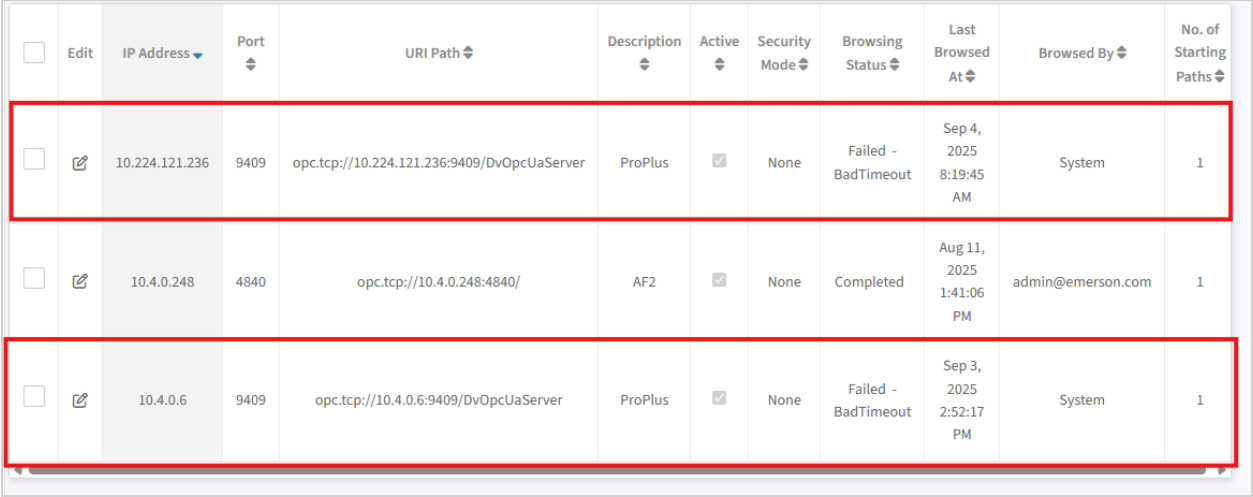
- Make sure AD Server Certificate Service is configured. Verify AD server port 636 secure connection using Microsoft Windows Server built-in LDAP client ldp.exe from AD server.
- Make sure LDAP Settings (BASE DN, DOMAIN) are correctly configured from the PWI Web page.
- Make sure AD server IP and Port are enabled in network firewall.
- Check AD secure connection using "openssl s_client" command. This command will print the AD certificate in output. Save AD certificate into a .crt file and check its

validity.

```
openssl s_client -connect <AD_IP>:636 -showcerts
```

9. OPC-UA Server Auto Browsing Failed with BadTimeout

OPC-UA auto browsing timeout failure is reported. Below is an example of the failure path "Objects/DA/MODULES/IPE/IPE_EM/T01".



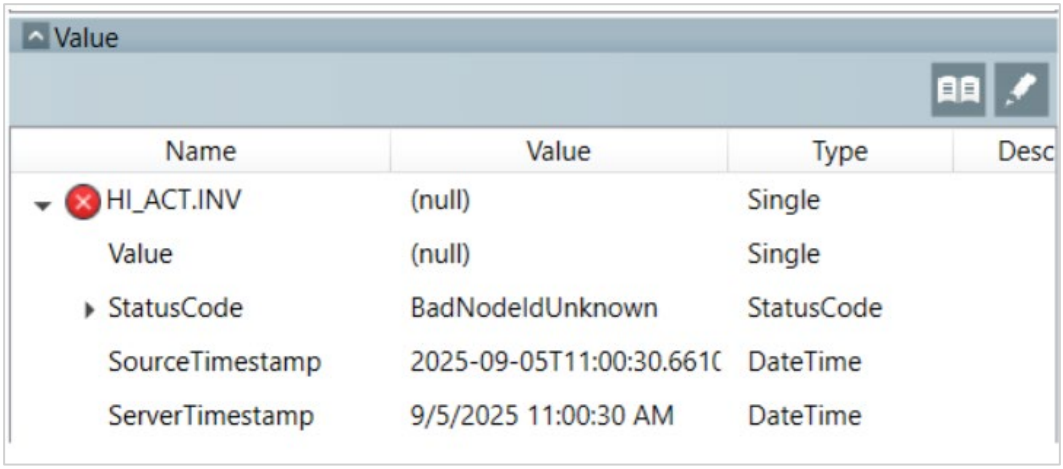
Edit	IP Address	Port	URI Path	Description	Active	Security Mode	Browsing Status	Last Browsed At	Browsed By	No. of Starting Paths
	10.224.121.236	9409	opc.tcp://10.224.121.236:9409/DvOpcUaServer	ProPlus	☑	None	Failed - BadTimeout	Sep 4, 2025 8:19:45 AM	System	1
	10.4.0.248	4840	opc.tcp://10.4.0.248:4840/	AF2	☑	None	Completed	Aug 11, 2025 1:41:06 PM	admin@emerson.com	1
	10.4.0.6	9409	opc.tcp://10.4.0.6:9409/DvOpcUaServer	ProPlus	☑	None	Failed - BadTimeout	Sep 3, 2025 2:52:17 PM	System	1

- Check the volume/log/syslog-ng/pwi-all.log, filter the opc-client log. One log complains browsing timeout and specifies the variable path with issue:

```
1757040490.468|2025-09-05T02:48:10.468+00:00|opc-client[956]:
09/05/25 02:48:10,467.797 ERROR
Session::browse_node_references_batch:
Session[10.224.121.236:9409/DVOpvUaServer] Error [BadTimeout] in
browsing the references under
"Objects/DA/MODULES/IPE/IPE_EM/T01/DI0183/AI1/HI_ACT"
[/opc_client/src/wrapper/session.cpp:2101]
```

- Connect to this OPC-UA server using a 3rd party OPC-UA client and browse this path. Note that there are several variables with invalid status ("**BadNodeIdInvalid**" or "**BadNodeIdUnknown**") under this path. These variables with invalid status cause the

browsing timeout. Users should remove those variables or bypass the path for browsing.



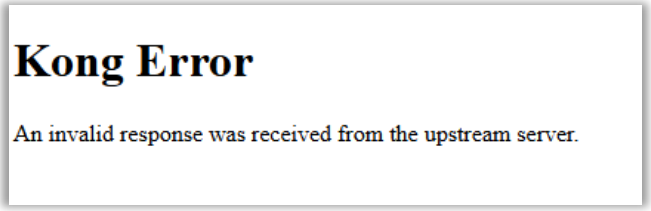
10. User Cannot Login PWI via SSO/LDAP

Login via SSO needs access to an Azure server by FQDN, so it requires PWI to shave configured DNS settings. Without DNS, PWI cannot access the SSO servers. If PWI is set with a static IP, users need to manually add a DNS server from ***PWI > Network Configuration > DNS Server page.*** Similarly, if LDAP is configured with FQDN, it also requires DNS settings on PWI.

11. User Does Not Have Access to System (Failed Login Attempt)

If a user has attempted to enter valid username and password but receives a message stating *"You do not have access to this system. Please contact administrator to get access",* this means they have a valid account, but an Admin user must grant the user access to the system. Refer to the Manage User Access section for instructions.

12. Web Interface Shows "Kong Error"



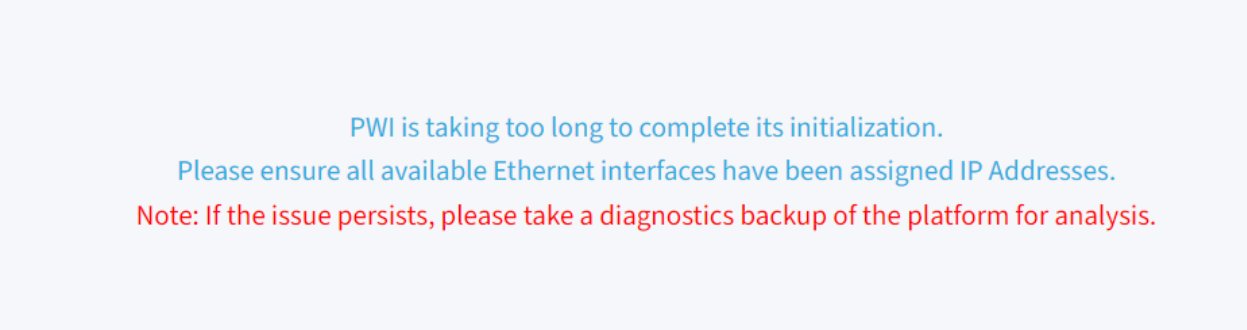
This error message occurs when a user's web browser fails to connect to PWI's web server. Please allow 5-10 minutes upon initial startup for PWI's web server to stabilize. If this issue

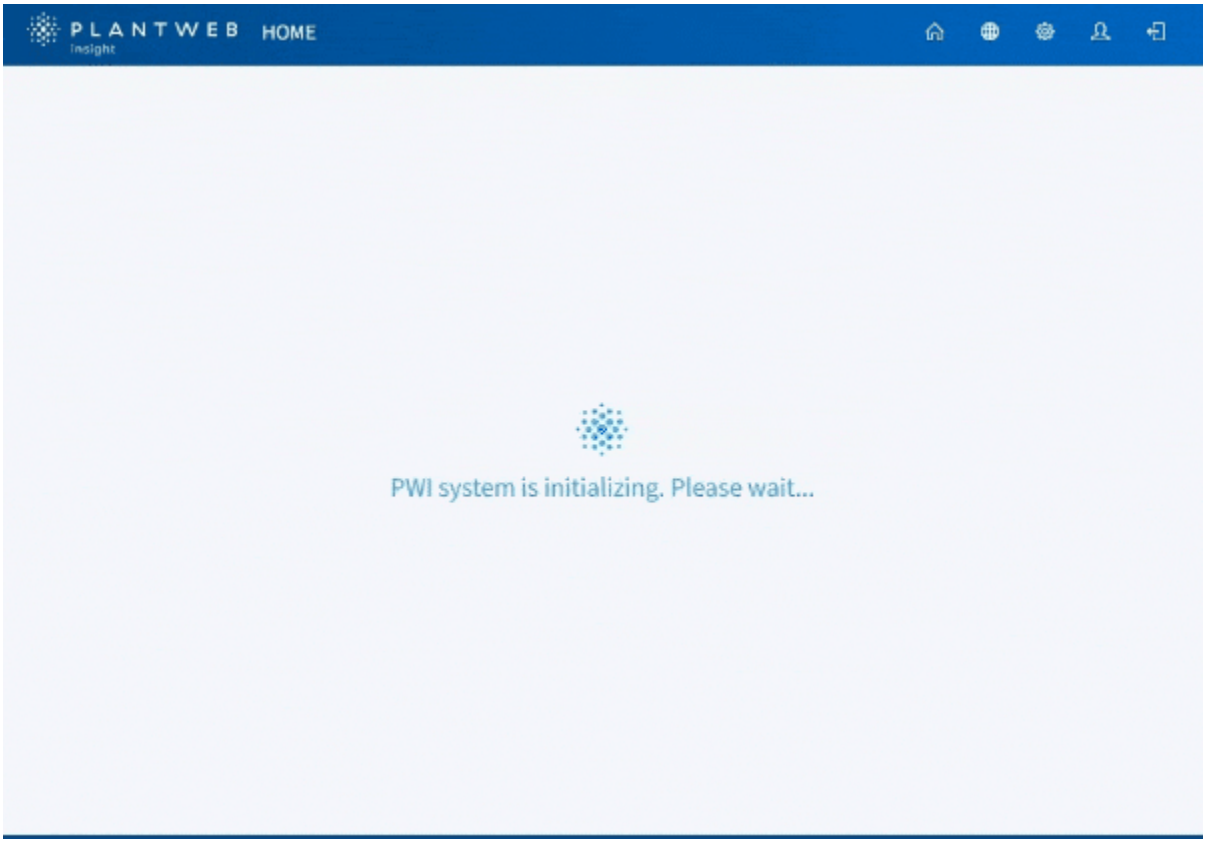
persists for more than 10 minutes, contact PWI technical support at plantwebinsightsupport@emerson.com

13. “PWI system is initializing” Perpetual State

When the "**PWI system is initializing**" message is shown, the license service attempts to get a fingerprint from the system. Once the license service obtains a fingerprint from the system, the message will go away. However, if the message is shown on PWI for a prolonged period, it means the license service is not able to obtain a fingerprint from the system. The user will see the message on the Home page of PWI.

After 5 minutes, the animation will be removed, and the message will be updated.
Note: The user is still able to navigate to other pages as the menu will still be accessible in the header.

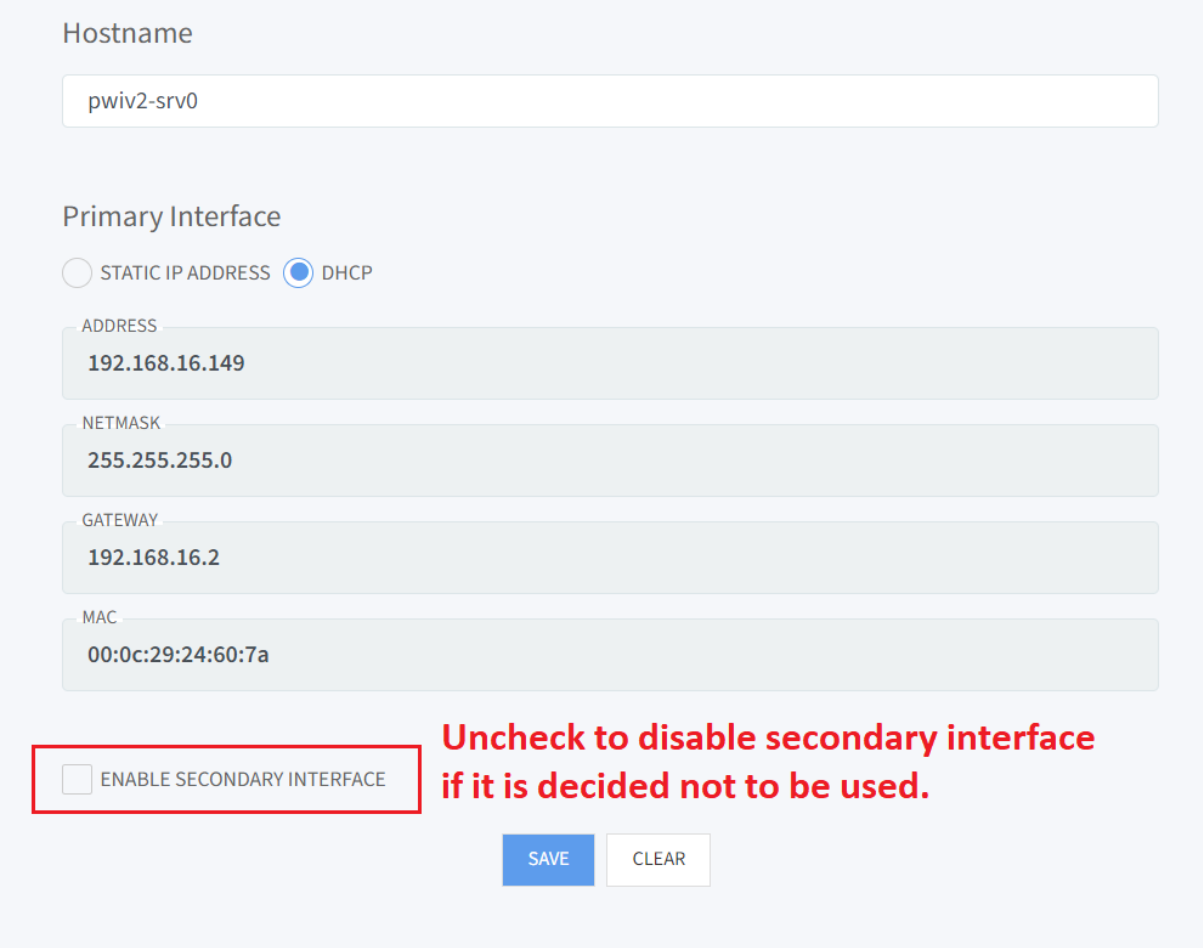




Users can take a diagnostic backup of the PWI Platform and make network configuration changes while in this state. All other operations are not recommended for system stability reasons.

Exiting PWI Initializing State

Users are to check ethernet configurations when they see the "**PWI system is initializing**" message for prolonged periods. The usual case is that the secondary ethernet interface is not able to get an IP address. If the User decides that the secondary ethernet interface is not going to be in use, the **user should disable the secondary interface in PWI** rather than just leaving the secondary ethernet interface unplugged.


Hostname
pwiv2-srv0
Primary Interface
STATIC IP ADDRESS
DHCP
ADDRESS
192.168.16.149
NETMASK
255.255.255.0
GATEWAY
192.168.16.2
MAC
00:0c:29:24:60:7a
ENABLE SECONDARY INTERFACE
Uncheck to disable secondary interface if it is decided not to be used.
SAVE
CLEAR

Appendix A – Example Critical Application Backup Schedule

- **Week 1:**
  - Daily Snap
    - Su, Mo, Tu, We, Th, Fr, Sa
- **Week 2:**
  - Retain Daily Snaps from Week 1
  - Daily Snap
    - Su, Mo, Tu, We, Th, Fr, Sa
- **Week 3:**
  - Retain Daily Snaps from Week 2
  - Daily Snaps (Begin to replace the Daily from Week 1)
    - Su, Mo, Tu, We, Th, Fr, Sa
  - End of Week (EoW) Snap Retained
    - EoW 1 *(Sa)*
- **Week 4:**
  - Retain Daily Snaps from Week 3
  - Daily Snaps (Begin to replace the Daily from Week 2)
    - Su, Mo, Tu, We, Th, Fr, Sa
  - End of Week (EoW) Snap Retained
    - EoW 1 *(Sa)*
    - EoW 2 *(Sa)*
- **Week 5:**
  - Retain Daily Snaps from Week 4
  - Daily Snaps (Begin to replace the Daily from Week 3)

        - Su, Mo, Tu, We, Th, Fr, Sa
    - End of Week (EoW) Snap Retained *(Begin to replace the End of Week Snaps from Wk1)*
        - EoW 2 *(Sa)*
        - EoW 3 *(Sa)*
- **Week 6:**
    - Retain Daily Snaps from Week 5
    - Daily Snaps *(Begin to replace the Daily from Week 4)*
        - Su, Mo, Tu, We, Th, Fr, Sa
    - End of Week (EoW) Snap Retained *(Begin to replace the End of Week Snaps from Wk2)*
        - EoW 3 *(Sa)*
        - EoW 4 *(Sa)*

When doing a restore, the admin should locate the VM snapshot iteration from which they want to restore; delete the corrupted VM; then restores the VM Snapshot to the same host: this should provide an exact mirror copy of the original.

Appendix B – Events Captured in the Platform Audit Log

Events Captured Under PWI v3.2.3 Release

Category	Sub-category	Event Scenario	Message logged	signature_id	Severity (1-10)
User	User	Preference settings changed	User {userId} has changed {Existing userId} preference settings	p_accessMgr_1	5
User settings	User accounts	User platform role changed	{userId} changed platform role of user account {Existing userId}	p_accessMgr_2	1
Active Directory Settings	Active Directory Settings	LDAP Configuration entry added	User added a LDAP Server {Server address}	p_adConnMgr_1	5
Active Directory Settings	Active Directory Settings	LDAP Configuration entry edited	User edited a LDAP Server {Server address}	p_adConnMgr_2	5
Active Directory Settings	Active Directory Settings	LDAP Configuration entry deleted	User deleted a LDAP Server {Server address}	p_adConnMgr_3	5
User	User	First time Login	User {userId} login to system for the first time	p_iamSvc_1	5
User	User	login successful	User {userId} login successful	p_iamSvc_2	5
User	User	Failed to login with unknown reason	User {userId} login failed due to {Failure reason}	p_iamSvc_3	5
User	User	Logout	User logout successful	p_iamSvc_4	5
User	User	User account blocked due to exceeded invalid password attempts	User account {userId} is blocked due to exceeded invalid password attempts	p_iamSvc_5	5
User	User	User is informed about password expiration	User {userId} is informed about password expiry	p_iamSvc_6	5
User	User	Reset password upon a first login	User has changed password on first login	p_localIDMgr_1	1
User	User	Failed to change Password	User {userId} failed to change password due to {Failure reason}	p_localIDMgr_2	5
User	User	User Change Own Password	User has changed password	p_localIDMgr_3	5

User settings	User accounts	A User account is added	{userId} Added a new user account {new userId}	p_localIDMgr_4	1
User settings	User accounts	A User account is edited	{userId} edited user account {Existing userId}	p_localIDMgr_5	1
User settings	User accounts	A user edit is not successful	{userId} failed to edit user {Existing userId} due to {Failure reason}	p_localIDMgr_6	1
User settings	User accounts	A User account is deleted	{userId} deleted user account {Existing userId}	p_localIDMgr_7	1
User settings	User accounts	A User account is locked	{userId} locked user account {Existing userId}	p_localIDMgr_8	1
User settings	User accounts	A User account is unlocked	{userId} unlocked user account {Existing userId}	p_localIDMgr_9	1
User settings	Password Options	Password restrictions changed	User {userId} has changed password options	p_localIDMgr_10	5
Ports & Protocol	Ports & Protocol	A Protocol (XXXX) is enabled	User has enabled protocol {Protocol name}	p_security_1	5
Ports & Protocol	Ports & Protocol	A Protocol (XXXX) is disabled	User has disabled protocol {Protocol name}	p_security_2	5
Ports & Protocol	Ports & Protocol	Port modified	User has modified port for protocol {Protocol name}	p_security_3	5
Ports & Protocol	Ports & Protocol	IP Whitelist changed	User has modified IP Whitelist for protocol {Protocol name}	p_security_4	5
User	User	Accessed an API which has no access to	User tried accessing API {API Url} with out access rights	p_security_5	1
Certificate Management	Default Cert	Downloaded Default Certificate	User has downloaded default certificate	p_security_6	5
Certificate Management	Default Cert	Rebuilt Default Certificate	User has rebuilt default certificate	p_security_7	5
Certificate Management	User Provided SSL Cert	HTTPS Cert uploaded	User has uploaded a new HTTPS certificate	p_security_9	5
Certificate Management	User Provided SSL Cert	OPC UA Client Cert uploaded	User has uploaded a new OPC UA Client certificate	p_security_10	5
Certificate Management	User Provided SSL Cert	OPC UA server Cert uploaded	User has uploaded a new OPC UA Server certificate	p_security_11	5
Certificate Management	Peer Cert	Peer certificate uploaded	User has uploaded a new peer certificate {Cert Name}	p_security_12	5

Certificate Management	Peer Cert	Peer certificate deleted	User has deleted a peer certificate {Cert Name}	p_security_13	5
Certificate Management	User Provided SSL Cert	User Updates Type of HTTPS Certificates to Use	User has changed the type of HTTPS certificate to be used: {certType}	p_security_15	5
Certificate Management	User Provided SSL Cert	User Updates Type of OPC-UA Client Certificates to Use	User has changed the type of OPC-UA Client certificate to be used: {certType}	p_security_16	5
Certificate Management	User Provided SSL Cert	User Updates Type of OPC-UA Server Certificates to Use	User has changed the type of OPC-UA Server certificate to be used: {certType}	p_security_17	5

Events Captured under PWI v3.3.0 Release

Category	**Sub-category**	**Event Scenario**	**Message logged**	**signature_id**	**Severity (1-10)**
User	User	Preference settings changed	User {userId} has changed {Existing userId} preference settings	p_accessMgr_1	5
User settings	User accounts	User platform role changed	{userId} changed platform role of user account {Existing userId}	p_accessMgr_2	1
Active Directory Settings	Active Directory Settings	LDAP Configuration entry added	User added a LDAP Server {Server address}	p_adConnMgr_1	5
Active Directory Settings	Active Directory Settings	LDAP Configuration entry edited	User edited a LDAP Server {Server address}	p_adConnMgr_2	5
Active Directory Settings	Active Directory Settings	LDAP Configuration entry deleted	User deleted a LDAP Server {Server address}	p_adConnMgr_3	5
User	User	First time Login	User {userId} login to system for the first time	p_iamSvc_1	5

User	User	login successful	User {userId} login successful	p_iamSvc_2	5
User	User	Failed to login with unknown reason	User {userId} login failed due to {Failure reason}	p_iamSvc_3	5
User	User	Logout	User logout successful	p_iamSvc_4	5
User	User	User account blocked due to exceeded invalid password attempts	User account {userId} is blocked due to exceeded invalid password attempts	p_iamSvc_5	5
User	User	User is informed about password expiration	User {userId} is informed about password expiry	p_iamSvc_6	5
User	User	Reset password upon a first login	User has changed password on first login	p_localIDMgr_1	1
User	User	Failed to change Password	User {userId} failed to change password due to {Failure reason}	p_localIDMgr_2	5
User	User	User Change Own Password	User has changed password	p_localIDMgr_3	5
User settings	User accounts	A User account is added	{userId} Added a new user account {new userId}	p_localIDMgr_4	1
User settings	User accounts	A User account is edited	{userId} edited user account {Existing userId}	p_localIDMgr_5	1
User settings	User accounts	A user edit is not successful	{userId} failed to edit user {Existing userId} due to {Failure reason}	p_localIDMgr_6	1

User settings	User accounts	A User account is deleted	{userId} deleted user account {Existing userId}	p_localIDMgr_7	1
User settings	User accounts	A User account is locked	{userId} locked user account {Existing userId}	p_localIDMgr_8	1
User settings	User accounts	A User account is unlocked	{userId} unlocked user account {Existing userId}	p_localIDMgr_9	1
User settings	Password Options	Password restrictions changed	User {userId} has changed password options	p_localIDMgr_10	5
Ports & Protocol	Ports & Protocol	A Protocol (XXXX) is enabled	User has enabled protocol {Protocol name}	p_security_1	5
Ports & Protocol	Ports & Protocol	A Protocol (XXXX) is disabled	User has disabled protocol {Protocol name}	p_security_2	5
Ports & Protocol	Ports & Protocol	Port modified	User has modified port for protocol {Protocol name}	p_security_3	5
Ports & Protocol	Ports & Protocol	IP Whitelist changed	User has modified IP Whitelist for protocol {Protocol name}	p_security_4	5
User	User	Accessed an API which has no access to	User tried accessing API {API Url} with out access rights	p_security_5	1
Certificate Management	Default Cert	Downloaded Default Certificate	User has downloaded default certificate	p_security_6	5
Certificate Management	Default Cert	Rebuilt Default Certificate	User has rebuilt default certificate	p_security_7	5
Certificate Management	Default Cert	Failed to rebuild Default Certificate	User has failed to rebuild default certificate	p_security_8	1

Certificate Management	User Provided SSL Cert	HTTPS Cert uploaded	User has uploaded a new HTTPS certificate	p_security_9	5
Certificate Management	User Provided SSL Cert	OPC UA Client Cert uploaded	User has uploaded a new OPC UA Client certificate	p_security_10	5
Certificate Management	User Provided SSL Cert	OPC UA server Cert uploaded	User has uploaded a new OPC UA Server certificate	p_security_11	5
Certificate Management	Peer Cert	Peer certificate uploaded	User has uploaded a new peer certificate {Cert Name}	p_security_12	5
Certificate Management	Peer Cert	Peer certificate deleted	User has deleted a peer certificate {Cert Name}	p_security_13	5
Certificate Management	Default Cert	Custom Default Certificates uploaded	User has uploaded new default certificates	p_security_14	5
Certificate Management	User Provided SSL Cert	User Updates Type of HTTPS Certificates to Use	User has changed the type of HTTPS certificate to be used: {certType}	p_security_15	5
Certificate Management	User Provided SSL Cert	User Updates Type of OPC-UA Client Certificates to Use	User has changed the type of OPC-UA Client certificate to be used: {certType}	p_security_16	5
Certificate Management	User Provided SSL Cert	User Updates Type of OPC-UA Server Certificates to Use	User has changed the type of OPC-UA Server certificate to be used: {certType}	p_security_17	5
Certificate Management	IOT Hub CA Cert	IOT Hub CA Certificate uploaded	User has uploaded a new IOT Hub CA Certificate {CertName}	p_security_18	5

Certificate Management	IOT Hub CA Cert	IOT Hub CA Certificate deleted	User has deleted an IOT Hub CA Certificate {Cert Name}	p_security_19	5

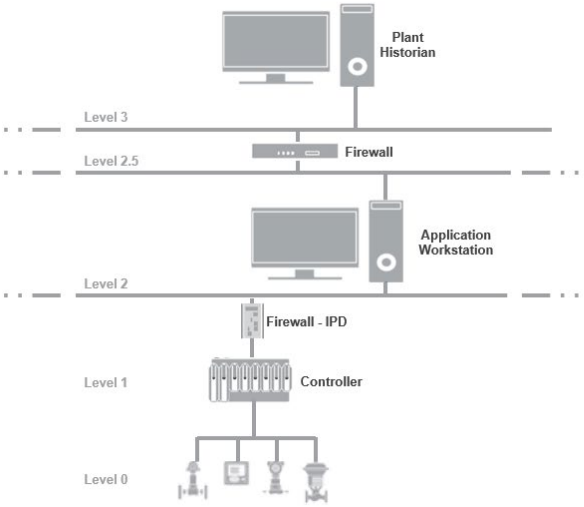
Events Captured Under PWI v3.4.0 Release

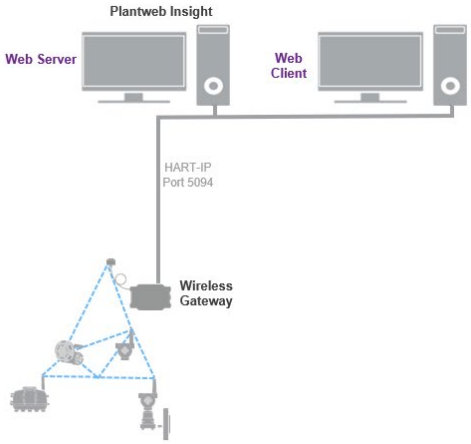
Category	Sub-category	Event Scenario	Message to be logged	signature_id	severity (1-10)
SMTP Settings	SMTP Settings	SMTP configuration added	User {username} added SMTP Server {server address}	p_notification_1	1
SMTP Settings	SMTP Settings	SMTP configuration edited	User {username} changed SMTP Server to {server address}	p_notification_2	5
SMTP Settings	SMTP Settings	SMTP configuration deleted	User {username} deleted SMTP Server {server address}	p_notification_3	5
SMTP Settings	SMTP Settings	Failed to save SMTP configuration	User {username} failed to save SMTP configuration {server address} due to ${failureReason}	p_notification_4	1
User	User	Accessed an API which has no access to	User {username} tried accessing {api Url} without access rights	p_notification_5	1
Email Notification	Email Sent	Sent an email to user	System sent an email from {from_email} to {to_email} for email subject: <{email subject}>	p_notification_6	1
Email Notification	Email Not Sent	Failed to send an email	System failed to send an email from {from_email} to {to_email} for email subject: <{email subject}>	p_notification_7	1
Platform Notification Settings	Platform Notification Settings	Platform Notifications settings updated	User {username} updated Platform Notification settings	p_notification_8	1

Appendix C – Reference Architectures

Standalone

This architecture provides ultimate separation of control systems and reliability networks. PWI is perfectly capable of operating independently provided it has access to necessary data sources.

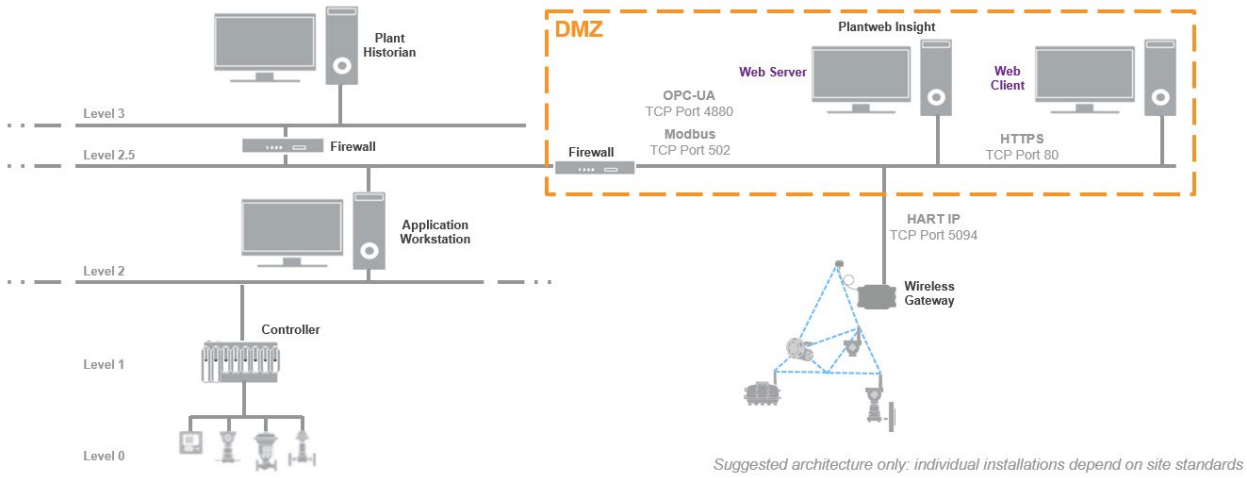




DMZ Level 2.5

This architecture allows connection to the control system to allow passage of existing data sources and PWI-generated alerts. This architecture is ideal when some measurement points already exist in the control system, or users would like to have the PWI alerts go to their control system.

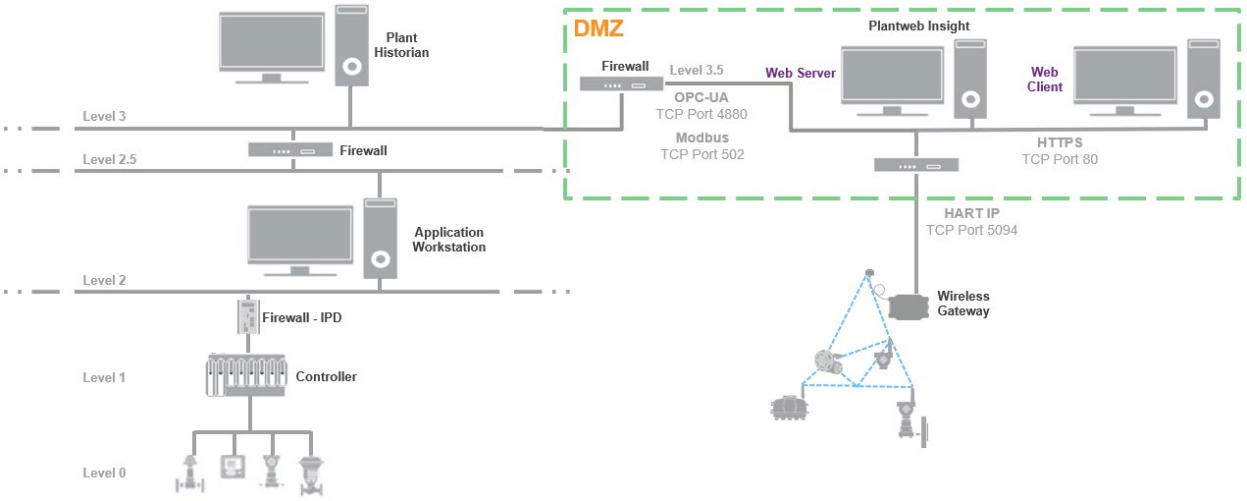
Communication to the control system uses OPC-UA or Modbus.



DMZ Level 3.5

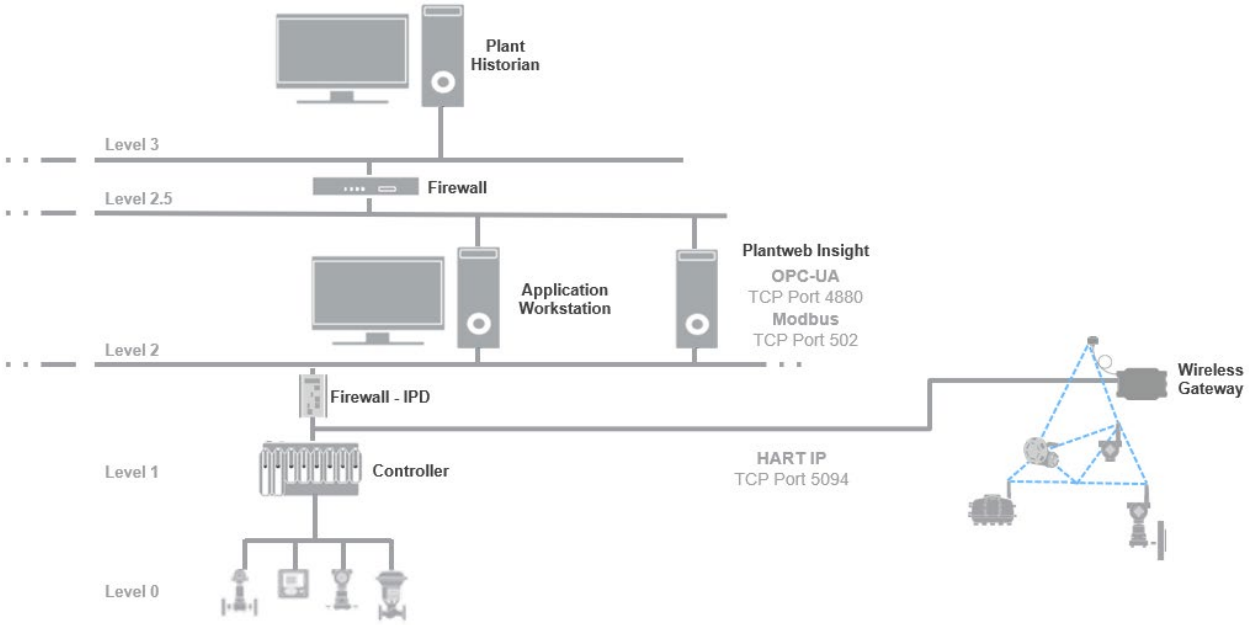
This architecture allows connection to the plant historian to allow passage of existing data sources and PWI-generated alerts. This architecture is ideal when some measurement points already exist in the historian, or users would like to have the PWI alerts go to their alarm management system or historian.

Communication to the historian uses OPC-UA or Modbus.



Level 2 – Control System

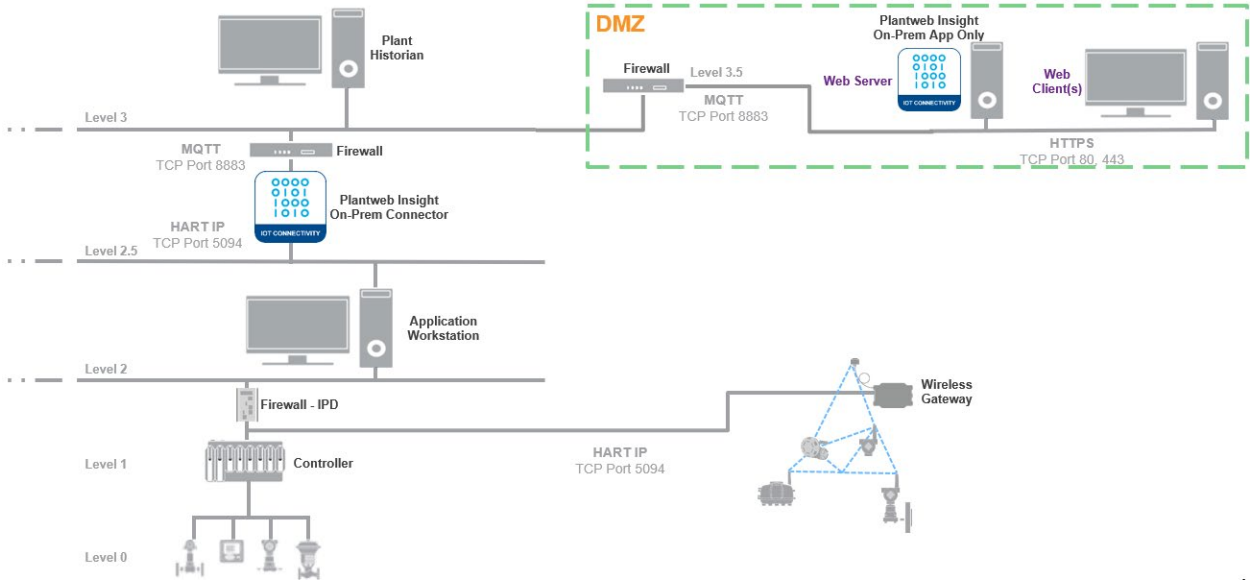
This architecture may be required if all data sources already reside within the control system network. Refer to the On-Premises Connectivity Solution if this scenario exists and users outside of the control system need access to PWI.



Level 2 MQTT Connection to Level 3.5

This architecture utilizes the PWI On-Prem Connector to convert DCS-locked data sources to MQTT before passing data to the PWI On-Prem App Only System at a higher, more accessible location in the network.

Refer to the On-Premises Connectivity Solution for more information.

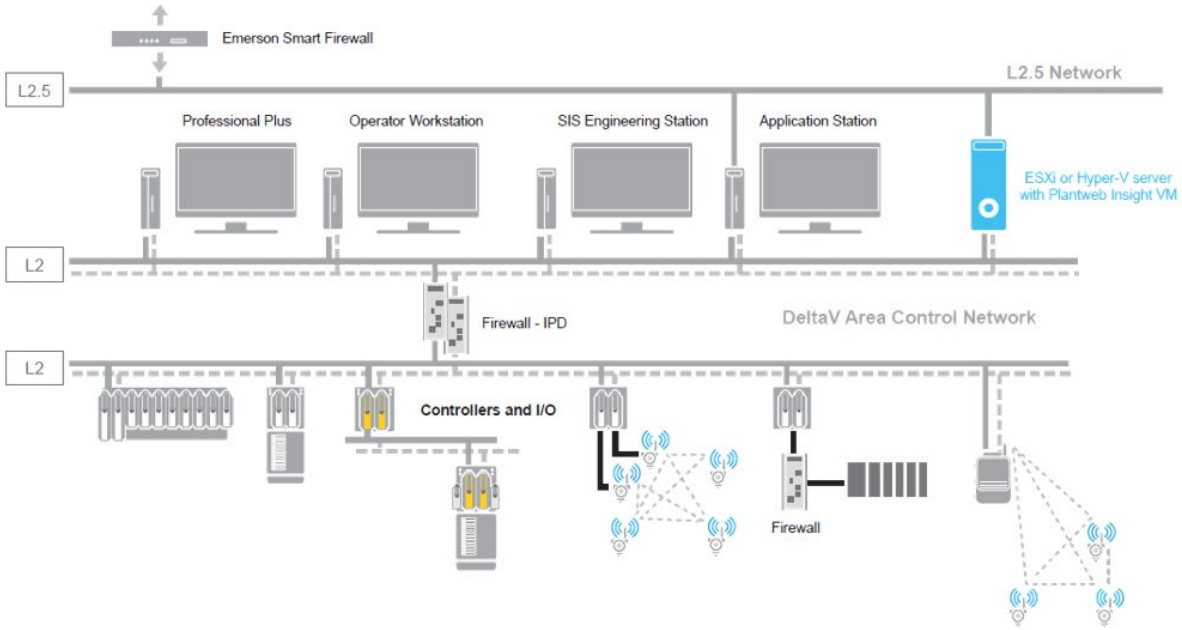


DeltaV™ Compatible

While PWI is typically kept separate from control system, it does have support to run on DeltaV systems. The architecture shown below displays how this is accomplished by using

a separate PWI server on the level 2 network. This allows PWI to access data coming directly from WirelessHART gateways that are feeding DeltaV.

Refer to the Plantweb Insight Support on DeltaV™ Systems White Paper for more information.



Manual
00809-0100-4581, Rev HB
March 2026

For more information: **Emerson.com/global**

EMERSON™