

Emerson Plantweb™ Insight



Safety

▲ WARNING

Physical access

Unauthorized personnel may potentially cause significant damage to and/or misconfiguration of end users' equipment. This could be intentional or unintentional and needs to be protected against.

Physical security is an important part of any security program and fundamental to protecting your system. Restrict physical access by unauthorized personnel to protect end users' assets. This is true for all systems used within the facility.

Contents

Chapter 1	Introduction.....	5
	1.1 Definitions.....	5
	1.2 Using this manual.....	5
	1.3 Product recycling/disposal.....	5
Chapter 2	Installation.....	7
	2.1 System requirements.....	7
	2.2 Install software.....	8
	2.3 Launch Plantweb Insight (PWI).....	11
Chapter 3	Configuration.....	15
	3.1 Overview.....	15
	3.2 Customize system settings.....	15
	3.3 Application configuration.....	21
	3.4 Data services (output) configuration.....	24
	3.5 Certificate management.....	35
Chapter 4	System updates.....	41
	4.1 Updating Plantweb Insight.....	41
Chapter 5	Backing up and restoring the system.....	43
	5.1 System backup capability.....	43
	5.2 Diagnostics backup.....	43
	5.3 Restorable backup.....	43
	5.4 Restoring the software.....	44
Chapter 6	Troubleshooting.....	49
	6.1 Unable to load Plantweb Insight virtual machine.....	49
	6.2 Virtual machine displays: IP Address Unknown.....	50
	6.3 OVF file error.....	50
	6.4 Web interface cannot be accessed.....	50
	6.5 Web interface login continues to spin after inputting email and password.....	51
	6.6 Cannot connect to <i>WirelessHART</i> [®] Gateway.....	51
	6.7 Nothing happens when clicking the application logo.....	52
	6.8 Active directory (LDAP) configuration fails.....	52
Appendix A	Installation on Hyper-V.....	55
	A.1 Enable Hyper-V on Windows [®] 10.....	55
	A.2 Hyper-V network settings for DHCP.....	56
	A.3 Set up the Plantweb Insight virtual machine.....	57
Appendix B	Console rescue.....	61
	B.1 Set static IP.....	61
	B.2 Reset HTTP white list.....	61
Appendix C	Reference architectures.....	63
Appendix D	Licensing in Plantweb Insight.....	73

D.1 License types.....	73
D.2 Home page licensing pop-up messages.....	74
D.3 Request a subscription or trial license.....	76
D.4 Install subscription or trial license from Home page.....	78
D.5 License installation errors.....	83

1 Introduction

1.1 Definitions

PWI Plantweb Insight

System Plantweb Insight framework and applications

Framework Virtual machine platform that is required to operate Plantweb Insight applications

1.2 Using this manual

This document is intended for system administrators and will provide details on how to set up Plantweb Insight (PWI). For more details and configuration information on specific applications, refer to the appropriate appendix sections and application manuals.

Emerson recommends administrators complete procedures as described in the order given.

1.3 Product recycling/disposal

Consider recycling equipment. Dispose of packaging in accordance with local and national legislation/regulations.

2 Installation

2.1 System requirements

Plantweb Insight (PWI) is delivered as a fully developed virtual machine (.ova file). The customer receives a complete virtual machine image to install in customer-provided virtualization software or hypervisors.

The PWI virtual machine contains a web server accessible by any web client with network access. Use the web browser user interface to configure and visualize the software.

PWI can be installed on a network server or PC/laptop. Either installation has the same requirements and installation steps. When configuring network settings, verify settings are in accordance with organization's policies. Any applicable *WirelessHART*[®] Gateways must be accessible on the network.

Before beginning PWI installation, verify system meets the following minimum requirements.

2.1.1 Host operating system

Virtualization software/hypervisor

- VMware[®] Virtual Hardware Version 16 or higher (requirements can be found on the [VMWare website](#))
- 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 hyperthreads in BIOS.
-

2.1.2 Hardware requirements

Minimum:

- Processors: 4 dedicated cores
- Memory: 8 GB RAM minimum
- Hard drive: 250 GB of free space

Recommended:

- Memory: 16 GB RAM
- Processors: 8 dedicated cores

2.1.3 Application access

Web browsers (recent versions supported)

- Google Chrome™
- Mozilla Firefox

- Microsoft Edge®

2.1.4 Other requirements

A DHCP server is required to assign a valid Internet protocol (IP) address.

Plantweb Insight (PWI) can also be accessed from a pre-configured static IP address.

Related information

[Install software](#)

2.1.5 Gateway compatibility

Plantweb Insight is compatible with Emerson Wireless 1410/1420 Gateways on firmware version 4.7.68 or higher.

If Gateway firmware is not up to date, Plantweb Insight may experience calculation response issues on certain applications. A delay in calculation response could negatively impact the following applications:

- Steam Trap
- Pump
- Heat Exchanger
- Air Cooled Heat Exchanger
- Pressure Relief Device

2.1.6 Device compatibility

Emerson devices must be in Emerson Optimized burst configuration. If an Emerson device needs to be modified, use the device configuration tool.

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

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

2.2 Install software

Plantweb Insight framework is provided as fully developed virtual machine (.ova) files, while applications and upgrade bundles are provided as separate ASC files.

Important

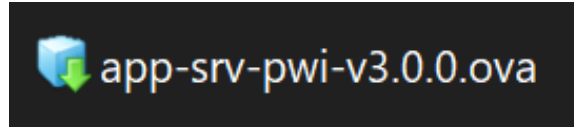
Only modify settings as described in the following procedure. Additional modifications could negatively impact the performance and functionality of Plantweb Insight.

For Hyper-V installation, refer to [Installation on Hyper-V](#).

Procedure

1. Verify that the .ova and .asc files have been completely downloaded to the host machine.
2. Exit/close all programs, including any running in the background.

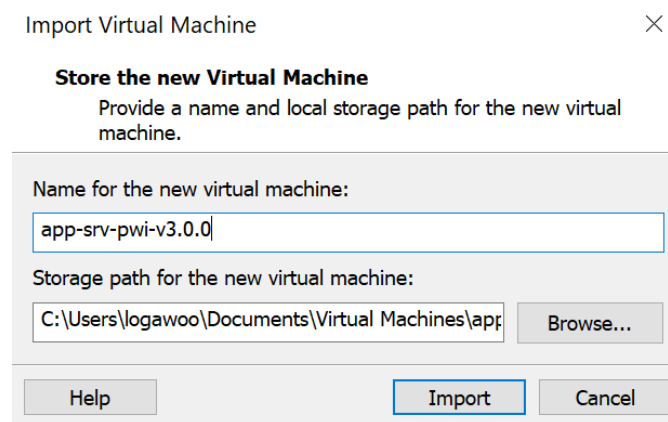
3. Import the virtual machine onto hypervisor:
 - Double click the .ova file.
 - Right click and select **Open with VMware Workstation** (or preferred hypervisor).



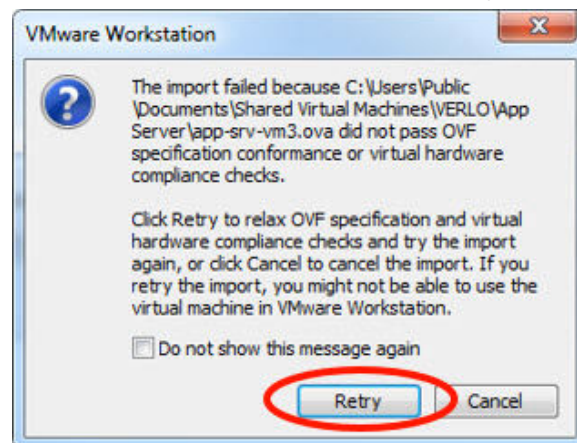
Note

The file name may change based on version and type.

4. Populate the designated fields with VM name and storage path; then click **Import**.

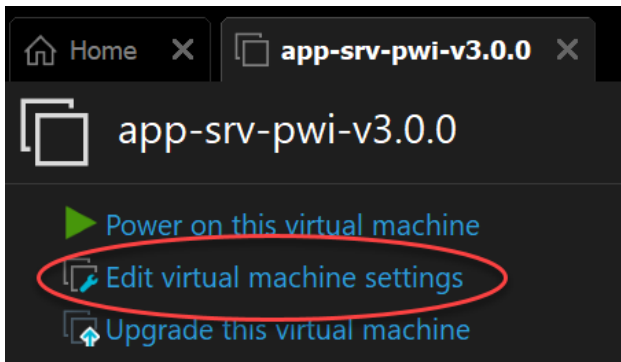


5. If the following prompt appears, click **Retry**.

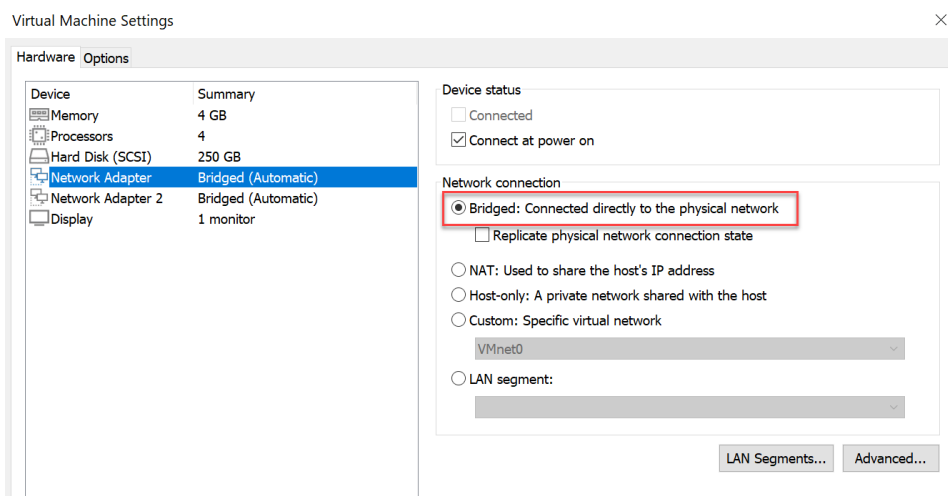


6. Wait for the virtual machine to import.
7. Select the Plantweb Insight virtual machine.

8. Select **Edit virtual machine settings**.



9. Set at least one of Plantweb Insight's network adapters to *Bridged*. Ensure that the adapter is bridged to the correct spot, typically the Ethernet port of the machine.



Note

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 Plantweb Insight, as it allows multiple clients to access the user interface and can connect multiple *WirelessHART*[®] Gateways or data sources.

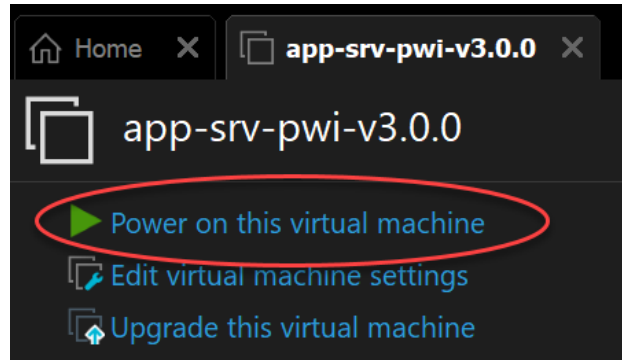
Default Ethernet configuration

The virtual machine features two external network adapters, a primary (eth0) and a secondary (eth1). The default network adapter configuration is:

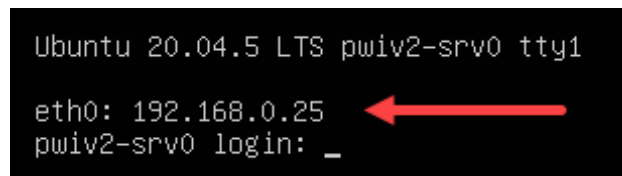
- eth0** DHCP, reflected on the virtual machine (VM) console
- eth1** Static, default IP address: 192.168.254.10

10. Select the Plantweb Insight virtual machine.

11. Select **Power on this virtual machine**.



12. Allow the virtual machine to boot.
13. Wait at least five minutes to allow the web server to prepare.
14. Navigate to the provided IP address.



Note

IP address will vary depending on installation. Image contains representative data, not actual.

A DHCP server will be required to assign an IP address. If no DHCP server is available on the network or **eth0** does not get an IP address at boot up, either:

- Use the default static IP assigned to **eth1** if possible.

Or

- Power off the virtual machine and set the primary network adapter to NAT to use the built-in DHCP server.

Note

The virtual machine login and password are not necessary and are not provided. There is a low-access login that allows static IP assignment and HTTP white listing reset. For more information on the low-access login, refer to [Console rescue](#).

Note

A pop-up window may appear during the installation process. Click **OK**.

2.3 Launch Plantweb Insight (PWI)

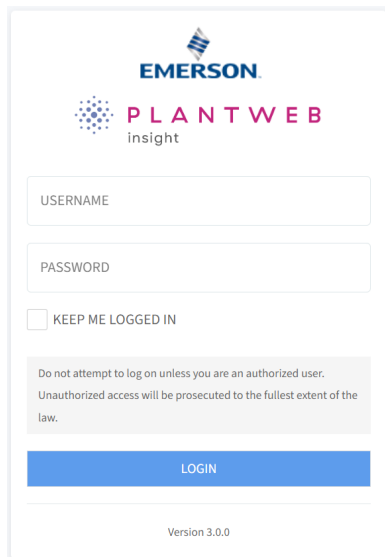
The PWI web interface can be accessed from any of the supported web browsers shown in [Application access](#).

Procedure

1. Open a supported web browser.
2. Beginning with *https://*, enter the IP address found in [Step 12](#) of [Install software](#).

A security notification opens. This is not an error, but a certification authorization warning (similar to when Gateways is used). Refer to [Certificate management](#) for instructions on setting up a certificate to remove this warning.

3. Click **Advanced**.
4. Click **Proceed** to move past the security warning.
5. Log in with the following credentials:
 - Username: **admin@emerson.com**
 - Password: **Default.1234**



Note

Both the username and password are case sensitive.


6. Change password as prompted (default settings are listed below and can be changed in **User Settings**).

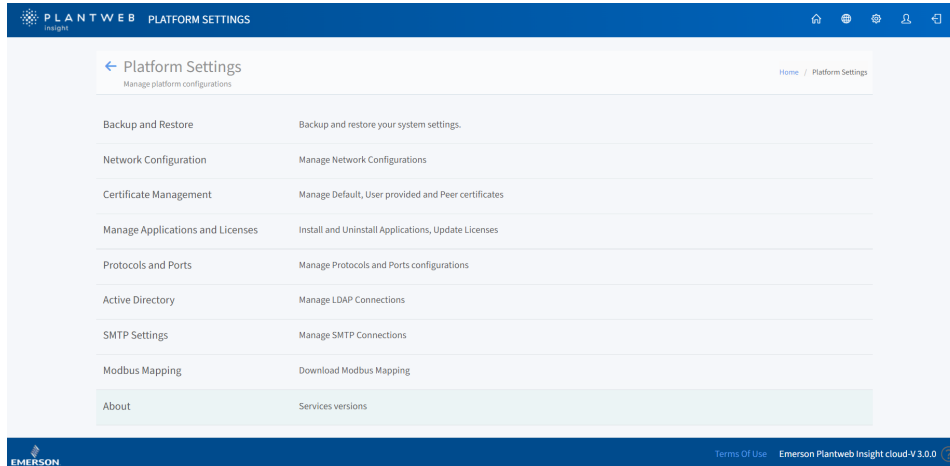
The default settings are:

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.

7. Log in with the updated credentials.
8. To verify the software version number, check the bottom right corner of the user interface.
9. If available, install the upgrade bundle. To do this, click .
10. Go to **Platform Settings** → **Manage Applications and Licenses**.



11. Browse to the upgrade bundle (.asc file).
After upgrade bundle is finished loading, the software prompts the user to log out and log in.
12. To install application files, go to **Platform Settings** → **Manage Applications and Licenses** and browse for the application file (.asc file).
After application is finished loading, software prompts the user to log out and log in. Multiple applications can be installed before user logs out and logs in.
13. Follow the prompts.

See the new application(s) on the **Home** screen. For license key instructions, see [Licensing in Plantweb Insight](#).

3 Configuration

3.1 Overview

This section contains information on customizing system settings and configuring Plantweb Insight.

Most custom configuration settings are optional. However, valid data inputs are required for Plantweb Insight applications and services to function properly.

3.2 Customize system settings

Configure system settings during the initial setup of Plantweb Insight as needed.

If you are restoring from a previous system, refer to [Backing up and restoring the system](#).


3.2.1 Configure Ethernet connection

NOTICE

Exercise caution when modifying to 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.

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

Procedure

1. Click .
2. Go to **Platform Settings** → **Ethernet Communication**.
3. From the **Ethernet Configuration** screen, manually assign a host name and IP address to the system.

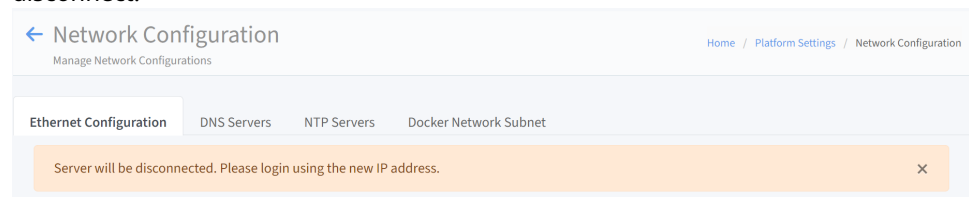
If using a DHCP server, Emerson recommends setting up static IP addresses or sticky IP addresses.

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 process data access.

NOTICE

Eth1 (secondary) is a non-routing network.

After Ethernet configuration changes are saved, the server prompts the user to disconnect.



After making IP changes, reboot the VM.

After the changes are applied, the VM console displays the new host name and/or new eth0 (primary) IP address.

```

Ubuntu 20.04.5 LTS Logan-Woolerys-PWI tty1
eth0: 192.168.0.25
Logan-Woolerys-PWI login: _
    
```

3.2.2 User accounts

Add users

Procedure


1. Click .
2. Go to **Users** → **User Accounts**.
3. Select **Add User Account**.
4. Enter email, role, and password; then click **Save**.
Users will be prompted to change their passwords when they first log in.

Table 3-1: Roles and privileges



Role	Privileges
Admin	Read and write
User	Read

Edit users and user passwords

NOTICE

Only an admin can edit users and passwords.

Procedure

1. Click .
2. Go to **Users** → **User Accounts**.
3. Click  next to the user name to be edited.

Note

To enable a disabled user, use the **Edit User** window.

To delete a user, select the **Delete this account** box.

4. Update the information.
5. Click **Save**.

Password options

Use the **Login and Password Options** page to set password requirements and settings.

Settings include:

- Password limitations and requirements (such as uppercase letters, lowercase letters, numbers, and special characters)
- Session idle timeouts
- Account locking details

Change password

Use the **Change Password** page to change login password.

NOTICE


The password change only applies to the user currently logged in.

3.2.3 Data client (input) configuration

Gateway connections

Add Gateway

Procedure

1. Click .
2. Select **Data Source Config** → **Gateway Settings**.
3. Click **Add Gateway**.
4. Enter the IP Address, Port, and Description.

Note

HART-IP™ uses port 5094 in the gateway. Ensure both HART-IP TCP and HART-IP UDP are enabled in the gateway and set to 5094.



Secure (encrypted) gateway connections require HART IP port 5095.

5. Click **Save**.

Once Plantweb Insight establishes connection, the Gateway tag and Network ID will populate. Please allow up to five minutes for the Gateway to establish a connection.


Edit Gateway

Procedure

1. Click .
2. Go to **Data Source Config** → **Gateway Settings**.
3. Click  next to the Gateway to be edited.
4. Update the information.
5. Click **Save**.

Delete Gateway

Procedure

1. Click .
2. Go to **Data Source Config** → **Gateway Settings**.
3. Select the check box/boxes next to the Gateway/s to be deleted.
4. Click **Delete Selected**.

OPC UA server connections


Add OPC UA server

Prerequisites

Note

The OPC UA® port in Plantweb Insight is designated as 4880. Ensure that the OPC UA server is set up for port 4880. Plantweb Insight uses a `opc.tcp://` connection to the OPC UA server.

Procedure

1. Click .
2. Go to **Data Source Config** → **OPC UA Servers**.
3. Click **Add OPC UA Server**.
4. Enter the IP Address, Port, Tag, and Description. and click **Save**.

Note



Because Plantweb Insight assumes the `opc.tcp://`, it will not accept full URLs. The Tag and Description fields are to help identify the server.

Configure the OPC UA server security configuration to **none** and **allow anonymous login**.

5. Click **Save**.


Edit OPC UA server

Procedure

1. Click  and select **Data Source Config** → **OPC UA Servers**.
2. Click  next to the server to be edited.
3. Update the information and click **Save**.

Delete OPC UA server

Procedure

1. Click  and select **Data Source Config** → **OPC UA Servers**.
2. Select the check box/boxes next to the server/s to be deleted.
3. Click **Delete Selected**.

Modbus® server connections

Plantweb Insight applications are not currently configured to use Modbus data.

3.2.4 Active directory (LDAP) configuration

Add active directory server

Note

Active directory servers should allow for a secure connection over port 636. Emerson recommends using an IP address rather than an FQDN for LDAP.

Emerson recommends mapping some user profiles in both active directory and Plantweb Insight to match each other.

Procedure

1. Go to **Platform Settings** → **Active Directory**.
2. Click **Add LDAP Setting**.
The **Edit LDAP Settings** screen appears.

Figure 3-1: Edit LDAP Settings screen

The figure displays two screenshots of the 'Edit LDAP Setting' configuration screen. Both screens have a title bar 'Edit LDAP Setting' and a 'STATUS' section at the bottom with 'ENABLED' checked and 'DELETE THIS SETTING' unchecked. Buttons for 'SAVE' and 'CANCEL' are at the bottom right.

Top Screenshot:

- FQDN OR IP: amrldap01.emrsn.org
- SECURED PORT: 636
- BASE DN: DC=emrsn,DC=org
- DOMAIN: emerson.com
- ROLE MAPPING:
 - Local Role: Active Directory Security Groups
 - Admin: SG1-Appliances-DeviceRoles-Admin
 - User: SG1-Appliances-DeviceRoles-Oper, SG1-Appliances-DeviceRoles-Maint, SG1-Appliances-DeviceRoles-Exec

Bottom Screenshot:

- FQDN OR IP: 10.164.75.3
- SECURED PORT: 636
- BASE DN: DC=testlab,DC=sgp
- DOMAIN: testlab.sgp
- ROLE MAPPING:
 - Local Role: Active Directory Security Groups
 - Admin: Admin
 - User: Exec, Maint, Oper

3. Fill in the required active directory details:

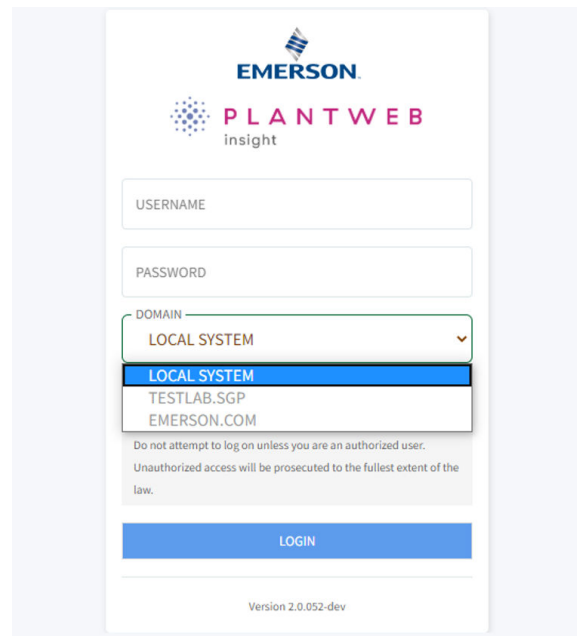
- a. FQDN or IP address
 - b. Secured port (port 636 is the standard secure port)
 - c. Base Domain Name
 - d. Domain. This must be the domain of the user's Principle Name (such as john.doe@example.com).
4. Map roles.
 - a) Create a new security group or choose the local roles from existing active directory that correlates with local roles.
 - b) Local roles can be mapped to multiple active directory security groups.
 5. If desired, add settings.
Up to four active directory settings can be added.

Figure 3-2: Active Directory Settings screen

FQDN or IP	Secured Port	Base DN	Domain	Edit	Status
svr1.emrslab.com	636	DC=svr1,DC=emrslab,DC=com	emrslab1.com		
192.168.101.3	636	DC=emrslab,DC=com	emrslab.com		
amrldap01.emrsl.org	636	DC=emrsl,DC=org	emerson.com		
10.164.75.3	636	DC=testlab,DC=sgp	testlab.sgp		

6. Update the information and click **Save**.
Once the LDAP is configured, users can log in with their active directory usernames. They can login as either:
 - Principle username (such as john.doe@example.com)
 - SAM account (such as john.doe)
 Users must select the Active Directory server they are logging into.

Figure 3-3: Login screen



3.2.5 Configure ports and protocols

NOTICE

Since Plantweb Insight will terminate and restart all services whenever port settings are updated, Emerson does not recommend customizing ports for service connections.

Procedure

1. Go to **Platform Settings** → **Protocols and Ports**.
2. Configure the service ports and enable or disable as needed.
3. Set up client white lists as needed.

3.3 Application configuration

This is a general guide for configuring applications. Applications must be set up before configuring data export in Plantweb Insight.

Refer to individual application manuals for specific configuration instructions.

3.3.1 Global settings

Each Plantweb Insight application contains specific global settings that should be set before any asset configuration. Global settings apply to all assets.

These settings could include units used for inputs (such as inlet pressure units), units used for calculations (such as currency), or key performance indicators to be tracked on the dashboard (such as overall health index).

3.3.2 Adding and editing assets

There are two ways to add or edit assets in an application: individually or via bulk upload. Devices are configured as assets are added.

Devices must be available within connected data sources to map them to an asset.

Add an asset

Use this method to add a single asset.

Procedure

1. Go to the **Asset Summary** screen and then click **Add an Asset**.
2. Complete all required fields in the **New Asset** window and then click **Save**.
Required fields are denoted with an asterisk (*).

Add a HART® IP measurement point from an Emerson Wireless Gateway

Depending on the application, wireless devices are added with either a drop-down list or a search function.

Procedure

1. For applications requiring specific devices (such as steam trap or PRV), select the appropriate device tag from the drop-down list.
The drop-down list will contain all devices with the pertinent device type.
2. For applications with generic measurements (pressure, temperature, flow, etc.) add wireless devices as follows:
 - a) Select Source: **HART-IP**
 - b) Begin to type the device tag.
After a few characters, a drop-down list of recognized devices will appear.
 - c) Select the relevant device.
Only devices on gateways connected to Plantweb Insight will appear.
 - d) Select the appropriate variable for the measurement (such as PV).

Process Inlet Temp Source	HART-IP
Device Tag	848(164518184355) ⓘ
Process Inlet Temp	PV

Add wired or other device via OPC-UA tag

OPC-UA® tags can be set up for certain measurement points.

Procedure

1. Select Source: **OPC-UA**

2. Select the relevant OPC-UA server.
3. Type in the complete path to the pertinent measurement point (for example, *Objects/Devices/OPC_Server1/3051S/PV*).
 - Use forward slashes, "/", for path breaks
 - The entire path is case sensitive

The screenshot shows a configuration window for 'Process Inlet Temp Source'. It contains three main input fields: a dropdown menu for 'Process Inlet Temp Source' set to 'OPC-UA', a dropdown menu for 'Server list' set to '192.168.80.133:488', and a text input field for 'Process Inlet Temp' containing the path 'Objects/Devices/OPC'. A green plus icon is visible to the right of the path field.

Manual input

Use manual inputs sparingly for measurement points. Only consider them for known consistent conditions (such as motor speed).

Procedure

1. Select Source: **Manual**
2. Type in the manual value.
3. Select the appropriate units.

The screenshot shows a configuration window for 'Process Inlet Temp Source' set to 'MANUAL'. It contains three main input fields: a dropdown menu for 'Process Inlet Temp Source' set to 'MANUAL', a text input field for 'Process Inlet Temp' containing the value '100', and a dropdown menu for 'Units' set to 'Fahrenheit Degrees'.

Note

Time needed for calculations to begin will depend on the application. Certain applications require capturing a baseline. This process is described in individual application manuals.

Import asset configuration

Use this method to add and/or edit multiple assets at the same time.

Procedure

1. Go to the **Asset Summary** screen and then click **Import Asset Config**.

Note

Data fields have strict requirements for entries. To find the requirements, download the **Import Specs File** after clicking **Import Asset Config**.

2. Select **Download asset configuration** to download the csv file.

Note

Select the **Empty File** box to download a blank template.

3. Complete the csv file and save it.
4. Browse and upload the csv file with the **Import Asset Config** window. Then select **Save**.
5. Verify that all assets were successfully imported.
If assets fail to import, check that all fields are filled out correctly and try downloading again. Device tags should match exactly how they appear in the gateway.

3.4 Data services (output) configuration

This section explains how to access the data outputs from specific Plantweb Insight applications to use in host systems, data historians, and other 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
- Estimated annual values (these remain constant for each asset since they are the annual estimate)
- Out of Service
- Health Index (if applicable)
- Alert state (if applicable). This is not the same as the events and alerts being sent through API keys.

3.4.1 OPC-UA® service

Plantweb Insight version 2.0 and later provide OPC-UA service using an internal OPC-UA server.

OPC-UA® server URL

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 can establish 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 Plantweb Insight version 2 default secure connection port is **4884**. `opc.tcp://<<opcua_server_ip>>:4884/OpcUAServer`

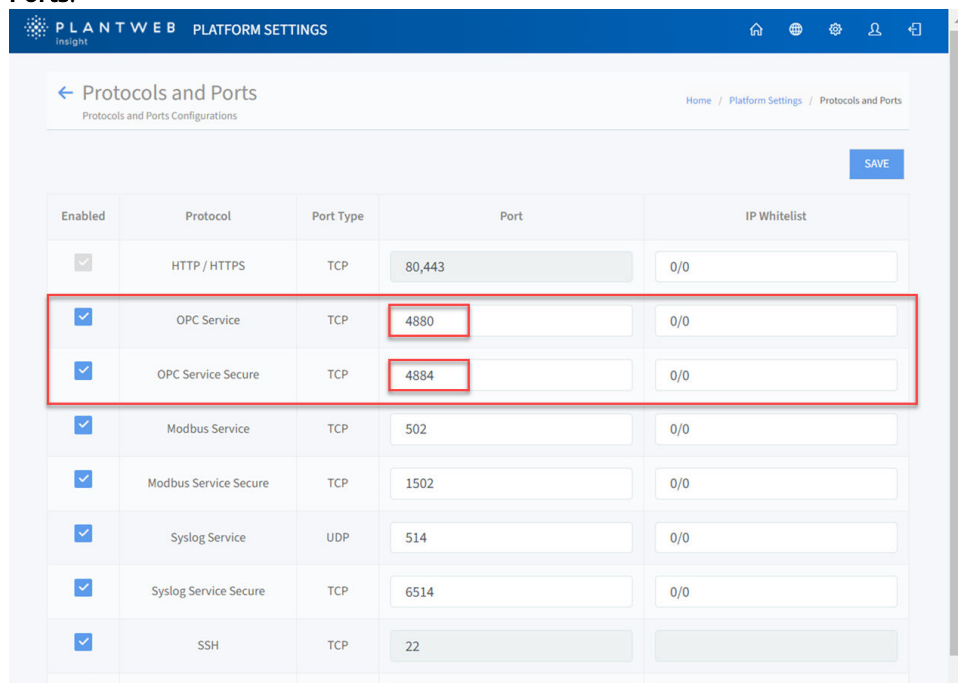
Set ports

Important

With Plantweb Insight, 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.

Procedure

1. Within the Plantweb Insight, web interface, go to **Platform Settings** → **Protocols and Ports**.



2. Verify that the OPC Service and OPC Service Secure ports are enabled and update them if necessary.
3. Click **Save** in the top right corner.

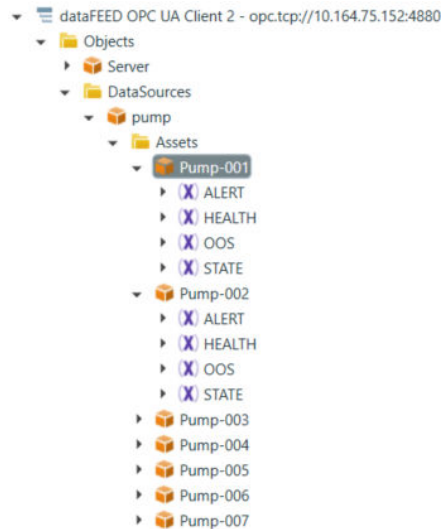
Variables hierarchy

The Plantweb Insight OPC-UA server has two types of variables: asset variables and HART® IP client variables.

Asset variables

Asset variables are published from applications and organized by application and asset.

- Asset variables hierarchy inside the OPC-UA® server



- Variable path for asset variables:
Objects/DataSources/⟨⟨application_name⟩⟩/Assets/⟨⟨asset_name⟩⟩/
⟨⟨variable_name⟩⟩

Example for pump application asset: Objects/DataSources/pump/Assets/
Pump-001/ALERT

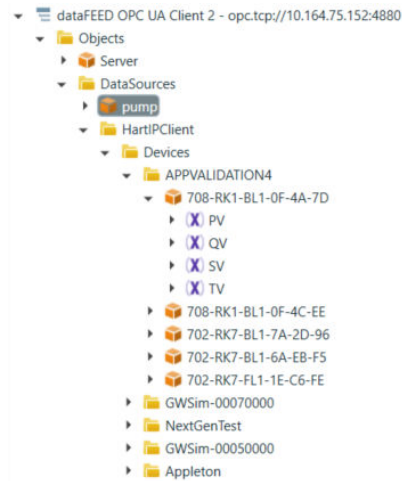
- Among the asset variables, only the OOS variable is writable by the client. Other variables are read only.
- Application name examples:

Steam trap	sta
Pressure relief valve	prv
Heat exchanger	heatexchanger
Cooling Tower	coolingtowers
Air cooled heat exchanger	aircooledheatexchanger
Pump	pump

HART IP client variables

These variables are published from the HART IP client and organized by gateway name and device name.

- 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 HART IP client asset if the Gateway name is APPVALIDATION4 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.

NOTICE

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

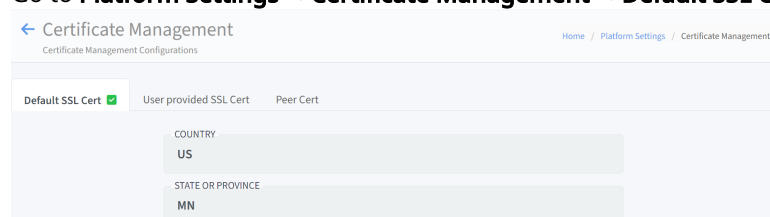
Set up a secure connection with an external OPC-UA® client

Plantweb Insight's OPC-UA secure connection can use either the default certificate or a user provided third party certificate.

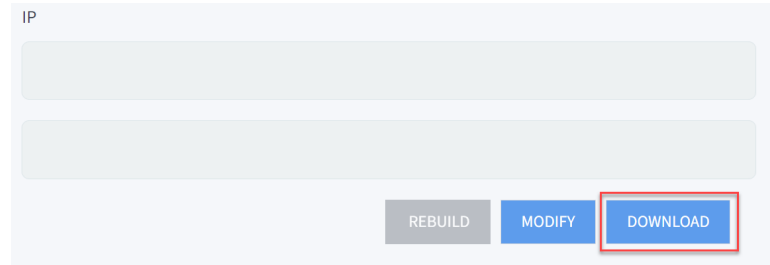
User-provided third party certificates should be in DER format, and validity should be longer than 90 days. The certificate should define the URI field.

Procedure

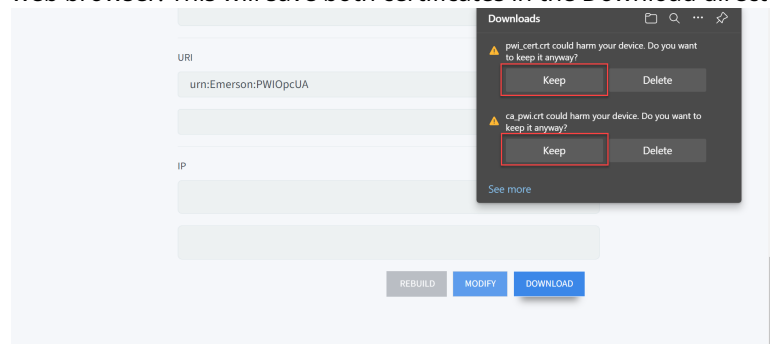
1. Prepare the Plantweb Insight OPC-UA server certificates.
 - If the secure connection uses the system's default certificate, download the default CA certificate from the system:
 - a. Go to **Platform Settings** → **Certificate Management** → **Default SSL Cert**.



- b. Click the **Download** button at the bottom of the page.



- c. If the web browser window asks to download multiple files, click **Allow**.
- d. Click the **Keep** button for both CA and Entity certificates if prompted by web browser. This will save both certificates in the Download directory.



- e. Convert the default CA certificate from PEM to DER format. Because the downloaded Plantweb Insight CA certificates are in PEM format and OPC-UA clients only support DER format certificates, the CA certificate must be manually converted from PEM to DER. The following commands can be run on the Ubuntu VM or Windows with installed openssl:
 1. `openssl x509 -inform PEM -in ca_pwi.crt -outform DER -out ca_pwi.der`
 2. `openssl x509 -inform PEM -in pwi_cert.crt -outform DER -out pwi_cert.der`

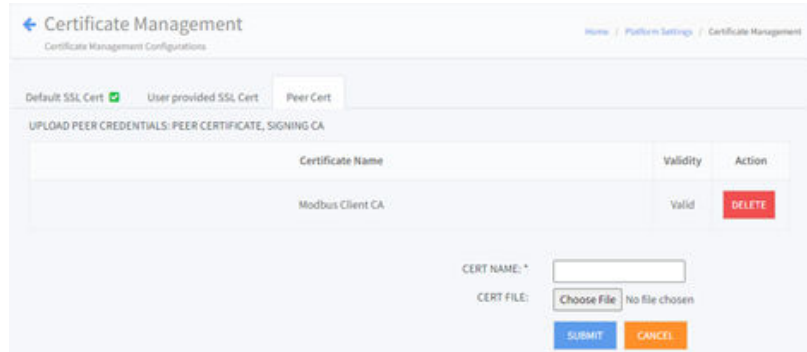
- If the OPC-UA connection uses a third party certificate, prepare this CA certificate in DER format.

Note

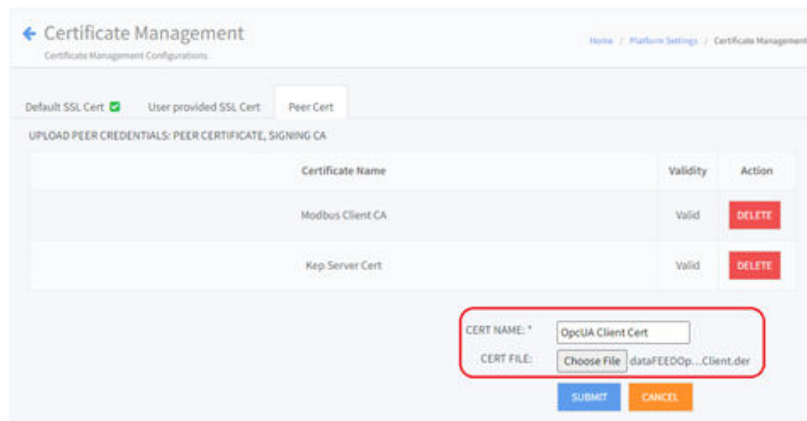
OPC-UA servers only support DER format certificates:

- The third party certificate must be valid for at 90 days or longer.
- The third party certificate must include the URI definition. For example:
`urn:Emerson:PWIOpcUA`
- To upload a third party certificate for the OPC-UA server, please refer to Certificate management, specifically OPC-UA server certificate.

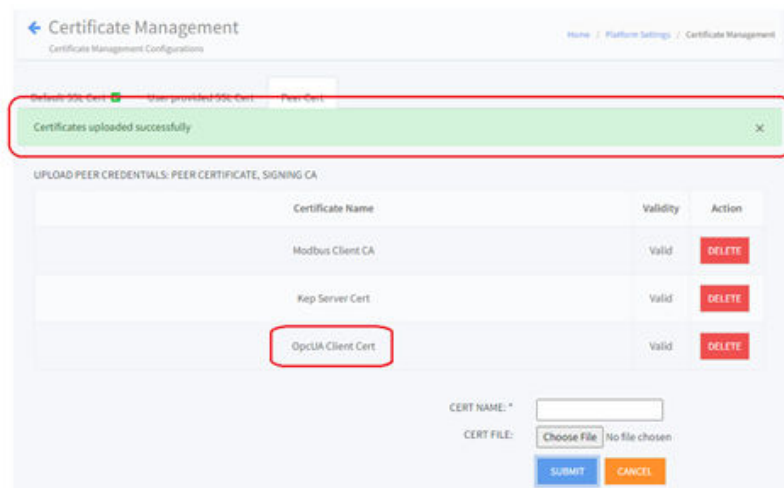
- 2. Exchange a certificate.
 - a) Upload the OPC-UA client certificate to Plantweb Insight's trust store.
 1. First validate the OPC-UA client certificate. The certificate must be valid for 90 days or longer.
 2. Go to **Platform Settings** → **Certificate Management** → **Peer Cert**.



3. Enter the certificate name in the CERT NAME text box. This is the name which will be listed in the peer certificate list. Click **Choose File** to choose the OPC-UA client certificate. Click **SUBMIT** to upload the certificate.



4. A notification saying *Certificates uploaded successfully* will display, and the OPC-UA certificate will be listed.



5. To remove a listed peer certificate, click the **DELETE** button in the same row as the unwanted peer certificate.

- b) Upload the Plantweb Insight OPC-UA server certificate to the OPC-UA client trust store.
- 3. Add Plantweb Insight's OPC-UA server information to the OPC-UA client.

Related information

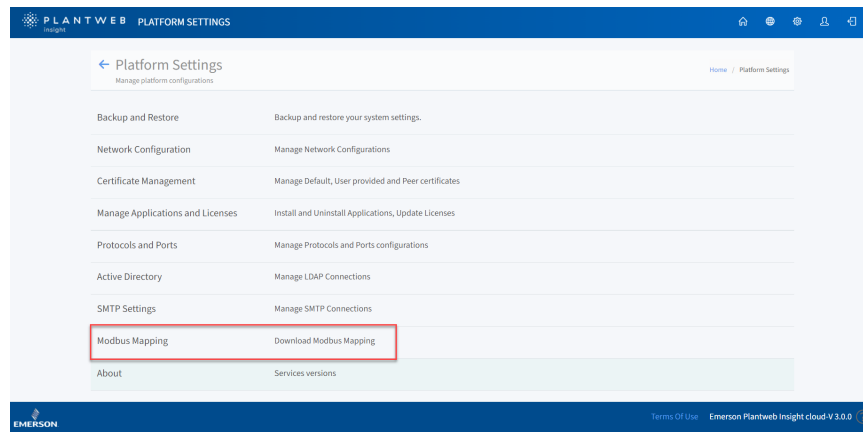
- [OPC-UA server URL](#)
- [Variables hierarchy](#)

3.4.2 Modbus® TCP service

Plantweb Insight version 2.0 and later use 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, click **Download Modbus Mapping** on the **Platform Settings** page to download a csv file.

Figure 3-4: Platform Settings page



For a sample csv file, see [Table 3-2](#).

Table 3-2: 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.

Table 3-3: Applications and IDs

Application ID	Application
99	Steam trap
1	Pump
3	Heat exchanger

Table 3-3: Applications and IDs (continued)

Application ID	Application
4	Air cooled heat exchanger
5	Pressure relief valve
6	Cooling tower
8	Power module
10	Network management
12	Non-intrusive corrosion

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

Table 3-4: 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 data 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

The third column refers to the register number. For example, ST-001.STATE uses function code 4 (read input registers), starting at 30000.

Table 3-5: Registers

Function	Register numbers (data addresses)	Read	Write single	Write multiple
Coil	00000-09999	FC01	FC05	FC15
Discrete input	10000-19999	FC02	N/A	N/A
Input register	30000-39999	FC04	N/A	N/A
Holding register	40000-49999	FC03	FC06	FC16

The data in the registers are formatted according to [Table 3-6](#)

Table 3-6: Data formats

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

3.4.3 REST API service

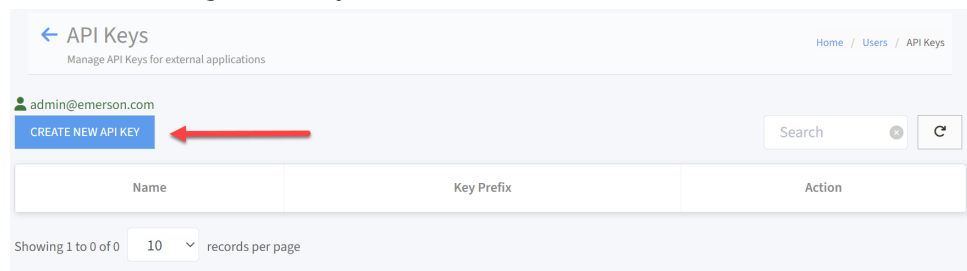
Requirements:

- Plantweb Insight version 2.3.0 or later
- Admin user role

Create and delete API keys

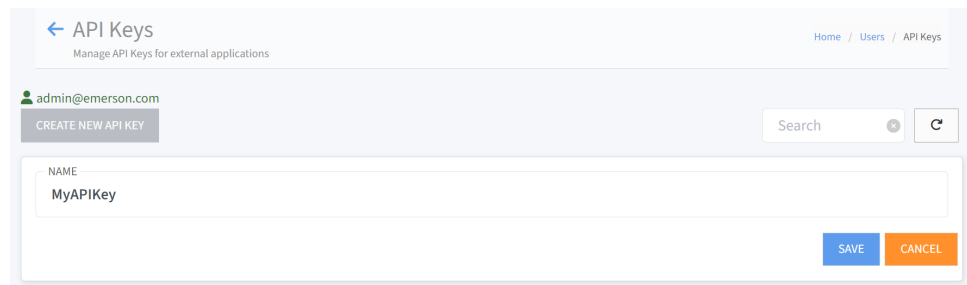
Procedure

1. Go to **User Settings** → **API Keys** and click **CREATE NEW API KEY**.

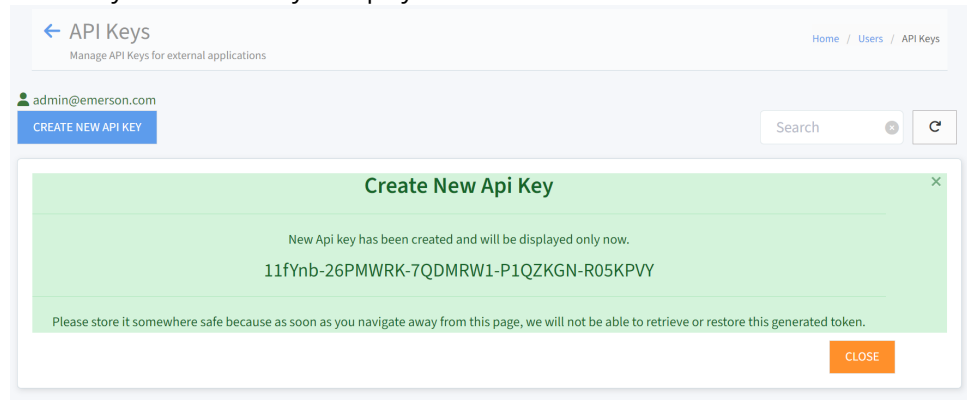


The **Create New API Key** form is displayed.

2. Enter the key name in the NAME text box.

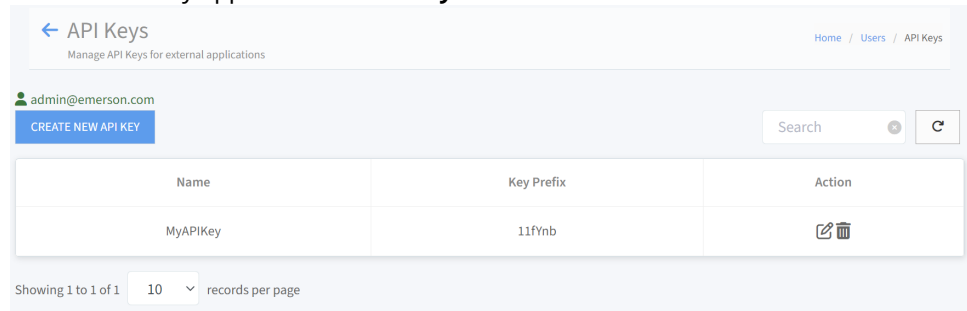


3. Click **SAVE**.
The newly created API key is displayed.

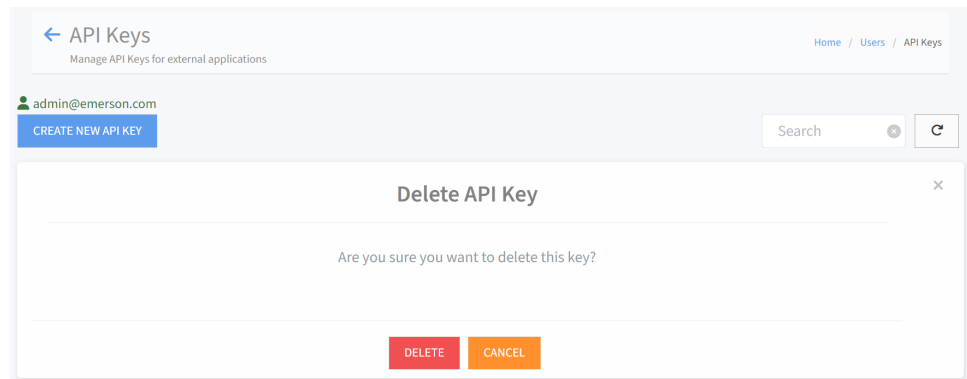


4. **Note**
The key will not be retrievable after the form is closed.
Copy the key and save it somewhere safe.

5. Click **CLOSE**.
The new API key appears in the **API Key** table.



6. 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.



API keys for Plantweb Insight Optics and other systems

The Plantweb Insight system exposes an API for all the applications and their API URL details.

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

The following is a sample response file:

```
{ "status": true, "data":  
  [ { "id": 8, "name": "bma", "status": "Installed", "display_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", "thirdPartyLogo":  
null, "version": "3.0.0.DEV.7", "ui_entry": null, "options_menu": null,  
"customBackup": false, "volumeDirectoryName": "bma" },  
  { "id": 10, "name": "nma", "status": "Installed", "display_name": "Networ  
k  
    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=T4rJZ3Iz1k3AhwX", "thirdPartyLogo": null, "version": "3.0.0.DEV.5",  
"ui_entry": null, "options_menu": null, "customBackup": false, "volumeD  
irectoryName": "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.

A valid API key is required to invoke the Assets and Alerts APIs. Keys can be generated from Plantweb Insight system in **User Settings** → **API Keys**. Only the creator of the API keys can edit them.

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 API key in headers) or

```
{{url}}/api/<<application_name>>-consumer/asset/all?apikey=<<A  
valid apikey>>
```

(API key as a query string)

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

Alerts API

Retrieve alerts of a specific asset from a specific date onwards from the 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 the application manual.

Note

Application URLs may change over time with new Plantweb Insight versions. We recommend relying on the Get Apps API mentioned in [API keys for Plantweb Insight Optics and other systems](#) to learn the applications and their URLs.

3.5 Certificate management

3.5.1 HTTPS service certificates

Plantweb Insight's default certificate is "self-signed". Users currently cannot use their own certificates, but instead must use a well-known certificate from a public certificate authority (such as Digicert or Verisign).

Tips for a clean TLS connection

- The signing CA certificate must be installed in the browser. Well-known CA certificates are pre-installed and kept updated in the Windows Certificate Store. Self-signed certificates must be manually installed.
- The Plantweb Insight certificate must have at least one *Subject Alternative Name*.
- Hostname resolution on the network: if the local DNS is unable to resolve the hostname on the network, set up hostname:ip_address mapping in C:\Windows\System32\Drivers\etc\hosts.

Install an HTTPS certificate for the first time

Procedure

1. Depending on the certificate type being used, perform one of the following steps:
 - If using a default certificate, download the default certificate from **Certificate Management** → **Default SSL Cert**.
 - If using a user-defined certificate, upload the certificate from **Certificate Management** → **User Provided SSL Cert**. The HTTPS certificate must be in PEM format.
2. Install the CA certificate to the web browser trust store.
3. Add the Plantweb Insight version 2 IP address into the default certificate and rebuild the default certificate.

Rebuild default certificate

Procedure

1. Download the new default certificate from **Certificate Management** → **Default SSL Cert**.
2. Install the default CA certificate to the web browser trust store.

Switch to a user-defined certificate

Procedure

1. Upload the user-defined certificate to **Certificate Management** → **User Provided SSL Cert**.
The HTTPS certificate must be in PEM format.
2. Install the user-defined HTTPS CA certificate to the web browser trust store.

Switch to a default certificate

This is the same procedure as [Rebuild default certificate](#).

Procedure

1. Download the default certificate from **Certificate Management** → **Default SSL Cert**.
2. Install the default CA certificate to the web browser trust store.

3.5.2 OPC UA service certificates

Install an OPC UA certificate for the first time

Procedure

1. Upload the peer OPC UA client certificate to **Certificate Management** → **Peer Cert**.
2. Depending on the certificate type being used, perform one of the following steps:
 - If using a default certificate, download the certificate from **Certificate Management** → **Default SSL Cert** and convert the CA certificate to DER format.
 - If using a user-defined certificate, upload the certificate to **Certificate Management** → **User Provided SSL Cert**. Make sure the OPC UA server certificate is in DER format.
3. Install the OPC UA server certificate to the peer OPC UA client trust store.

Rebuild a default OPC UA certificate

Procedure

1. Download the new default certificate from **Certificate Management** → **Default SSL Cert**.
2. Convert the default CA certificate to DER format using the following command:
`openssl x509 -in ca_pwi.crt -outform DER -out ca_pwi.der`
3. Install the DER formatted certificate to the peer OPC UA client trust store.

Switch to a user-defined OPC UA certificate

Procedure

1. Upload the user-defined OPC UA server certificate to **Certificate Management** → **User provided SSL Cert**.
Make sure the certificate is in DER format.
2. Install the user-defined OPC UA server CA certificate to the peer OPC UA client trust store.

Switch to a default OPC UA certificate

This is the same procedure used in [Rebuild a default OPC UA certificate](#).

Procedure

1. Download the default certificate from **Certificate Management** → **Default SSL Cert**.
2. Convert the default CA certificate to DER format using the following command:
`openssl x509 -in ca_pwi.crt -outform DER -out ca_pwi.der`
3. Install the DER formatted CA certificate to the peer OPC UA client trust store.

3.5.3 Modbus® service certificates

Install a Modbus® certificate for the first time

Procedure

1. Upload the peer Modbus client certificate to **Certificate Management** → **Peer Cert.**
2. Download the default certificate from **Certificate Management** → **Default SSL Cert.**
3. Install the default CA certificate to the peer Modbus client trust store.

Rebuild a Modbus® default certificate

Procedure

1. Download the new default certificate from **Certificate Management** → **Default SSL Cert.**
2. Install the default CA certificate to the peer Modbus client trust store.

Switch to a user-defined certificate

This is not applicable for Modbus® certificates.

Switch to a default certificate

This is not applicable for Modbus® certificates.

3.5.4 Syslog-ng service certificates

Install a Syslog-ng service certificate for the first time

No action needed. The HART® IP client action will handle the Syslog-ng secure connection with the gateway.

Note

Make sure to add the Plantweb Insight version 2 IP address to the default certificate and rebuild the default certificate before establishing a secure connection with the gateway.

Rebuild a default Syslog-ng certificate

No action needed. The HART® IP client action will handle the Syslog-ng secure connection with the gateway.

Note

Make sure to add the Plantweb Insight version 2 IP address into the default certificate before rebuilding the default certificate.

Switch to a user-defined certificate

This is not applicable for Syslog-ng certificates.

Switch to a default certificate

This is not applicable for Syslog-ng certificates.

3.5.5 OPC UA client certificates

Install an OPC UA client certificate for the first time

Procedure

1. Upload the peer OPC UA server certificate to **Certificate Management** → **Peer Cert.**
2. Depending on whether you are using the default certificate or a user-defined certificate, do one of the following:
 - If using the default certificate, download the certificate from **Certificate Management** → **Default SSL Cert.** Convert the CA certificate to DER format.
 - If using a user-defined certificate, upload the certificate to **Certificate Management** → **User provided SSL Cert.** Make sure the certificate is in DER format.
3. Install the OPC UA client certificate to the peer OPC UA server trust store.
4. Add the OPC UA server information to the **OPC UA Connection Setup** page. For Secure mode, select **Sign** or **Sign Encrypt**.

Rebuild the default OPC UA client certificate

Procedure

1. Download the new default certificate from **Certificate Management** → **Default SSL Cert.**
2. Convert the default CA certificate to DER format using the following command:
`openssl x509 -in ca_pwi.crt -outform DER -out ca_pwi.der`
3. Install the DER formatted CA certificate to the peer OPC UA server trust store.

Switch to a user-defined OPC UA client certificate

Procedure

1. Upload the user-defined OPC UA client certificate to **Certificate Management** → **Default SSL Cert.**
The certificate should be in DER format.
2. Install the user-defined CA certificate to the peer OPC UA server trust store.

Switch to the default OPC UA client certificate

Procedure

1. Download the default certificate from **Certificate Management** → **Default SSL Cert.**
2. Convert the default CA certificate to DER format using the following command:
`openssl x509 -in ca_pwi.crt -outform DER -out ca_pwi.der`
3. Install the DER formatted CA certificate to the peer OPC UA server trust store.

3.5.6 LDAP client certificates

Install an LDAP client certificate for the first time

No action needed.

Rebuild the default LDAP client certificate

No action needed.

Switch to a user-defined certificate

Not applicable for LDAP client certificates.

Switch to a default certificate

Not applicable for LDAP client certificates.

4 System updates

Emerson manages the Plantweb Insight virtual machine and applications by providing regular framework and application updates that the user must install through the web interface.

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.

4.1 Updating Plantweb Insight

Framework updates frequently require updated versions of the applications as well.

Be sure to check for application updates when updating the framework. For information on the latest version of Plantweb Insight and compatible application versions, refer to the release notes.

4.1.1 In-Place system updates

Procedure

1. In the Plantweb Insight web interface, go to **Platform Settings** → **Manage Applications**.
2. Uninstall any applications that have a newer version available.
Do not check **Clean Uninstall** unless necessary.
3. Install applicable upgrade bundle(s) (ASC files).
To initiate update effectivity, software prompts user to log out and log in.
4. Install compatible versions of any applications that have been updated.

4.1.2 Disruptive system updates

Disruptive system updates require deployment of a new virtual machine (OVA).

For instructions on backing up and restoring a system into a new virtual machine, refer to [Backing up and restoring the system](#).

4.1.3 Update applications

Procedure

1. In Plantweb Insight, go to **Platform Settings** → **Manage Applications**.
2. Uninstall any applications that have a newer version available.
Do not check **Clean Uninstall** unless necessary.
3. Install compatible versions of any applications that have been updated.

5 Backing up and restoring the system

5.1 System backup capability

Plantweb Insight version 2.1.5 and versions 2.4.0 or later can take two different types of backups of system data and configuration content.

- Diagnostic backup: available in all versions of Plantweb Insight
- Restorable backup: available in version 1.6.x, version 2.1.5, and version 2.4.0 and later

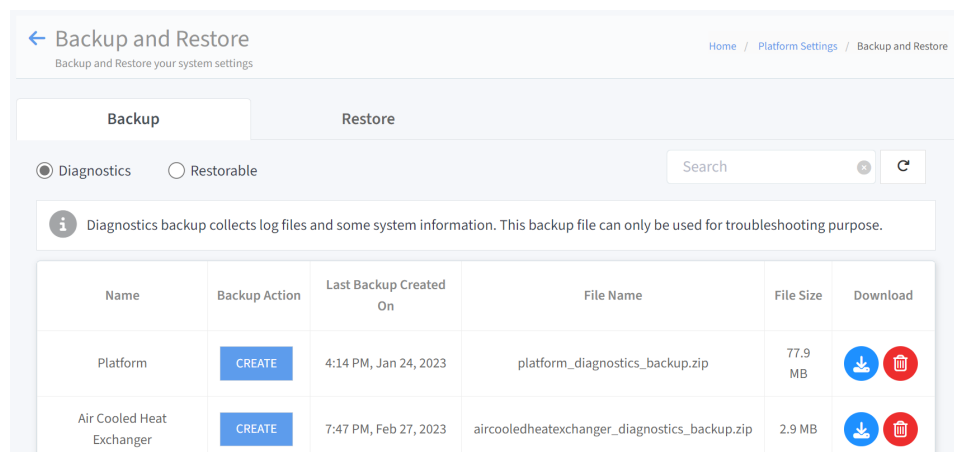
Either type of backup can be used for either the platform and/or specific application(s). Administrators can do this from within the user interface by going to **Platform Settings** → **Backup and Restore** → **Backup**.

5.2 Diagnostics backup

When performing a diagnostics backup, the software gathers the necessary troubleshooting details from the system.

The software zips these details and encrypts them with a user-generated password. To view the downloaded content, extract it from the zip file with a valid password. To access the diagnostics backup, go to **Platform Settings** → **Backup and Restore** → **Backup** → **Diagnostics**.

Figure 5-1: Diagnostics Backup screen



5.3 Restorable backup

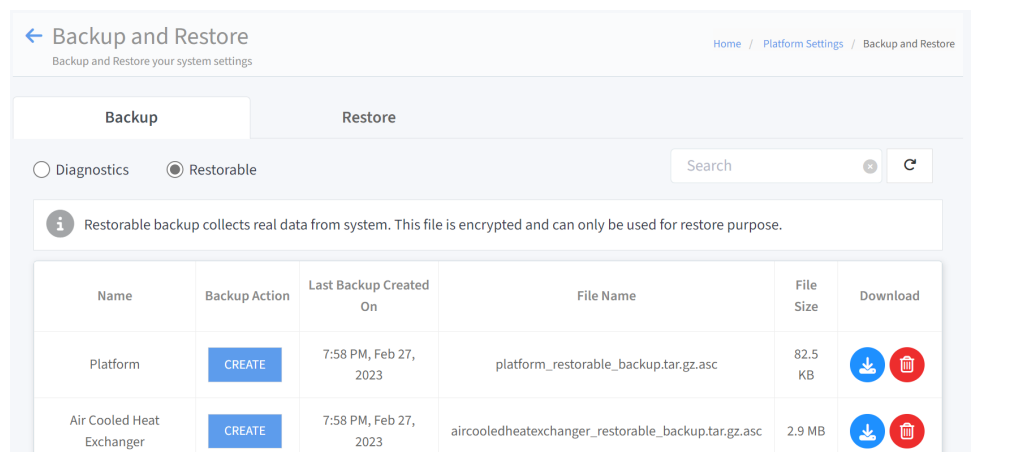
When performing a restorable backup, the software gathers specific data for system restoration.

For application backups, the application's manifest file will decide what content needs to be considered for restorable backup. The software zips these details and encrypts them with a user-generated password. The platform also signs the backup bundle to ensure the integrity of the backup file. A user can download the backup file, but cannot view its contents. The restorable backup is meant to be restored on a Plantweb Insight system

only. At the time of restore, the user must enter the password of the file to allow the software to read its contents.

To perform a restorable backup, go to **Platform Settings** → **Backup and Restore** → **Backup** → **Restorable**.

Figure 5-2: Restorable Backup screen



Note

Restorable backups are only available on Plantweb Insight versions 1.6.x, 2.1.5, and 2.4.0 and later.

5.4 Restoring the software

Plantweb Insight supports a restore capability to move customers from one virtual machine to another.

This feature is required in scenarios where a Plantweb Insight release is only available as a new virtual machine (OVA file) rather than a simple upgrade bundle.

Note

Plantweb Insight version 2.x.x supports restores from two version categories: version 1.6.x and 2.1.5.

Plantweb Insight platform and application specific restorable backups can only be restored on version 2.4.0 and later.

5.4.1 Restoring from Plantweb Insight version 1.6.x to 2.x.x

This capability is intended to help migrate users from older Plantweb Insight version 1.6.x systems to version 2.x.x systems.

A backup taken from a version 1.6.x system consists of both platform and applications content consolidated to a single backup file. This is a single zip file encrypted with a user-generated password.

Save a Plantweb Insight version 1.6.x system backup

Procedure

1. Go to **System Settings** → **Platform Settings** → **Backup and Restore**.
2. Create a password and then click **Save Backup**.

Restore a Plantweb Insight version 1.6.x system backup into version 2.x.x

When performing a restore operation, the existing data (if any) on Plantweb Insight version 2.x.x will be replaced with the backup content from Plantweb Insight version 1.6.x.

Procedure

1. Install the latest Plantweb Insight version 2.x.x virtual machine and log in through the web interface.
2. Perform the required manual steps, such as Ethernet configuration and certificates. If keeping the new dynamic IP assigned, update the new IP address with any clients, such as external OPC UA/Modbus® clients or Plantweb Optics.
3. Configure and connect data sources (gateways or OPC UA servers).
 - If using a gateway, go to **Data Source Config** → **Gateway Settings**.
 - If using an OPC UA server, go to **Data Source Config** → **OPC UA Servers**.
4. Install the latest versions of required applications.
5. Go to **Platform Settings** → **Backup and Restore** → **Restore** → **PWI V1**.

← Backup and Restore
Backup and Restore your system settings

Home / Platform Settings / Backup and Restore

Backup Restore

PWI V1 PWI V2

i Restore a backup (.zip file) which was taken from PWI v1.6 system.

BROWSE

BACKUP FILE PASSWORD

RESTORE

Important

Make sure to choose the correct restore type based on the Plantweb Insight system the backup is coming from.

5.4.2

Restoring from Plantweb Insight version 2.x.x to version 2.4.x or later

Plantweb Insight 2.x.x has a restore capability to move a complete Plantweb Insight system from one virtual machine to another when there is a non-backwards compatible framework release.

In this case, the new Plantweb Insight release will be in the form of a new OVA. Users must set up the new virtual machine and move their system data to it.

Note

If using Plantweb Insight version 2.1.x or earlier, first upgrade to Plantweb Insight version 2.1.5 in order to create restorable system and application backups. Plantweb Insight version 2.1.5 also requires application versions that support restorable backups. For a list of compatible application versions for version 2.1.5, see [Table 5-1](#).

If using version 2.3.x, upgrade to version 2.4.0 with a simple in-place system update.

Table 5-1: Application versions required to save a restorable backup on Plantweb Insight version 2.1.5

Application name	Allows restore from
Steam Trap	2.1.2
Pump	2.2.0
Pressure Gauge	2.1.0
Heat Exchanger	2.1.3
Air Cooled Heat Exchanger	2.1.3
Pressure Relief Valve	2.1.1
Cooling Towers	2.1.1
Power Module	2.1.0
Network Management	2.3.0
Inline Corrosion	1.1.0
Location	N/A
Non-Intrusive Corrosion	N/A
Connected Lighting App	N/A

Save a version 2.x.x system backup from an old Plantweb Insight system

Procedure

1. Go 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.

Restore a version 2.x.x system backup to a new Plantweb Insight system

When performing a restore operation, any existing data or accounts on Plantweb Insight version 2.x.x will be replaced with the system data and configuration content of the backed up system.

Procedure

1. Install the latest Plantweb Insight version 2.x.x virtual machine and log in through the web interface.
2. Navigate to **Platform Settings** → **Backup and Restore** → **Restore** and restore the platform backup.
After restoring the platform, the software automatically logs out user.
3. Log back in using credentials from the Plantweb Insight version 2.x.x system from which the backup was taken.
4. Perform the required manual steps, such as Ethernet configuration, certificates, API keys, etc.
 - a) If keeping the new dynamic IP assigned, update the new IP address with any clients, such as external OPC UA/Modbus® clients or Plantweb Optics.
 - b) To avoid IP conflicts over the network, do not configure the same IP address for both old and new Plantweb Insight systems. Either assign a dynamic IP to

the older system or shut it down before allocating the same static IP to the new Plantweb Insight 2.4.0 system.

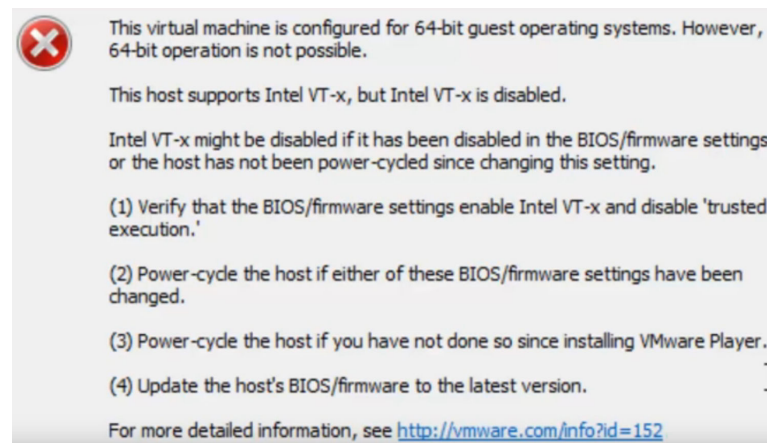
- c) Recreate API keys shared with external systems, such as Plantweb Optics by going to **Users** → **API Keys**.
5. Verify connectivity to data sources (gateways or OPC UA servers).
 - If using a gateway, go to **Data Source Config** → **Gateway Settings**.
 - If using an OPC UA server go to **Data Source Config** → **OPC UA Servers**.
6. Install the latest versions of required applications.
7. Restore application backup files one at a time.

6 Troubleshooting

Before troubleshooting, verify the latest version of the Plantweb Insight framework and the compatible application versions are being used.

Refer to Plantweb Insight release notes for information on the latest version and compatible applications.

6.1 Unable to load Plantweb Insight virtual machine



Possible cause

Intel VT-x is disabled.

Recommended actions

1. Verify that the BIOS/firmware settings enable Intel VT-x and disable **trusted execution**.
2. Power cycle the host if either BIOS/firmware settings has changed.
3. If the power has not been cycled since installing the VMware Player, cycle power.
4. Update the host's BIOS/firmware to the latest version.
5. For more detailed information, see [VMWare Knowledge Base](#).

Possible cause

System settings configuration

Recommended action

Follow the steps in the [video](#) to resolve.

Different operating systems and hardware have similar procedures.

6.2 Virtual machine displays: IP Address Unknown

```
Ubuntu 20.04.5 LTS pwiv2-srv0 tty1
eth0: --IP Address unknown--
pwiv2-srv0 login:
```

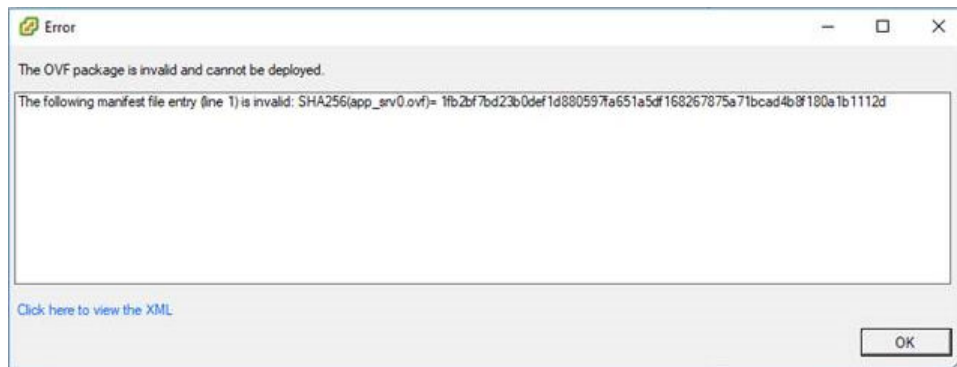
Possible cause

No available DHCP server to assign a valid IP address

Recommended actions

1. Ensure the Plantweb Insight machine has access to a DHCP server.
2. Check both VMware Workstation Pro™/ESXi virtual network editor settings and the Ethernet adapter settings. Verify the primary adapter is set to Bridged connection.
3. If a static IP address is necessary from the start, try using the static IP from the secondary Ethernet adapter (192.168.254.10) or changing the primary Ethernet adapter to a NAT connection within VMware. This uses the host system's internal DHCP to provide an IP. Once in the web-based user interface, a static IP can be assigned. If neither option works, refer to [Console rescue](#).

6.3 OVF file error



Possible cause

Plantweb Insight virtual machine is installed in the VMware vSphere® client

Recommended action

Install the Plantweb Insight virtual machine in the VMware vSphere Web Client or ESXi Embedded Host Client.

6.4 Web interface cannot be accessed

Recommended actions

1. Verify host machine meets minimum hardware requirements.

2. Verify that Plantweb Insight has a valid IP address assigned to the primary Ethernet connection (displayed in the VM console) or that a static IP on the secondary port is being used.
3. After turning on the virtual machine, allow Plantweb Insight virtual machine to run for at least five to ten minutes before navigating to the web interface.
4. Ping Plantweb Insight IP address to check for connection (ping is open).
5. Ensure client and Plantweb Insight are connected to the same subnet.
6. Ensure "https://" precedes IP address.
7. Clear the cache on the web browser.

6.5 Web interface login continues to spin after inputting email and password

Possible cause

External connections that are port forwarded to the Plantweb Insight framework can cause issues.

Recommended action

If necessary to port forward external connections, consult Rosemount Customer Central.

6.6 Cannot connect to *WirelessHART*[®] Gateway

Recommended actions

1. Go to **System Settings** → **Data Source Config** → **Gateway Connections** and verify that the correct Gateway IP address, port (5094 or 5095), and description were entered correctly and if the **Inactive** box is still checked.
2. Ensure that HART-IP UDP and HART-IP TCP are both enabled in the Gateway.
 - a) In the Gateway, navigate to **System Setting** → **Protocols** → **Protocols and Ports**.
 - b) Make sure that either port **5094** or **5095** is enabled, but not both.

3. Ensure that Plantweb Insight has access to the *WirelessHART* Gateway.
 - a. The Plantweb Insight machine needs to be able to see and communicate with the Gateway.
 - b. Both must be on the same subnet.
 - c. HART-IP traffic must be allowed through the communication channel.

Figure 6-1: Protocols And Ports screen

Protocols And Ports				
Enabled	Protocol	Port Type	Port	Port Upper Range [UDP]
<input checked="" type="checkbox"/>	DHCP	UDP	68	
<input checked="" type="checkbox"/>	HART-IP	TCP	<input type="text" value="5094"/>	
<input checked="" type="checkbox"/>	HART-IP	UDP	<input type="text" value="5094"/>	5126
<input checked="" type="checkbox"/>	HART-IP Secure	TCP	<input type="text" value="5095"/>	
<input checked="" type="checkbox"/>	HTTP	TCP	80	
<input checked="" type="checkbox"/>	HTTPS	TCP	<input type="text" value="443"/>	
<input type="checkbox"/>	NTP	UDP	123	
<input checked="" type="checkbox"/>	Ping			

1 - 8 of 8 results « ‹ › » 15 ▾

4. If Gateway Tag, Description, and Network ID are not visible on the **Gateway Connection** setup page, check the firewall and network.

6.7 Nothing happens when clicking the application logo

Clicking the application on the home page after install has no results.

Possible cause

Application installed is not compatible with the Plantweb Insight framework version.

Recommended action

1. Ensure a valid license key has been entered for any applications that require one.
2. Check the release notes for the installed version of Plantweb Insight and refer to the compatible application versions. If a different application and/or framework is required, contact your Emerson representative to request new software.

6.8 Active directory (LDAP) configuration fails

Error messages

- Unauthorized** The user that is trying to log in is not a member of any security group that is mapped to Plantweb Insight roles.
- Authorization Failed** The password or username is incorrect.

Recommended actions

1. Verify connection over port **636**, the standard secure port and that the active directory server allows for a secure connection.
2. Use an IP address, rather than an FQDN for LDAP. If a load balancer is used, try to get the IP of one of the active directory servers.
The load will be quite small for Plantweb Insight usage. There can be issues around resolving an FQDN.
3. Map some user profiles in both active directory and Plantweb Insight to match each other.
There are only two types of users in Plantweb Insight: Admin and User.
4. Once the LDAP is set up, sign in with an active directory username.
Some systems require the full name, while others will need domain/username.

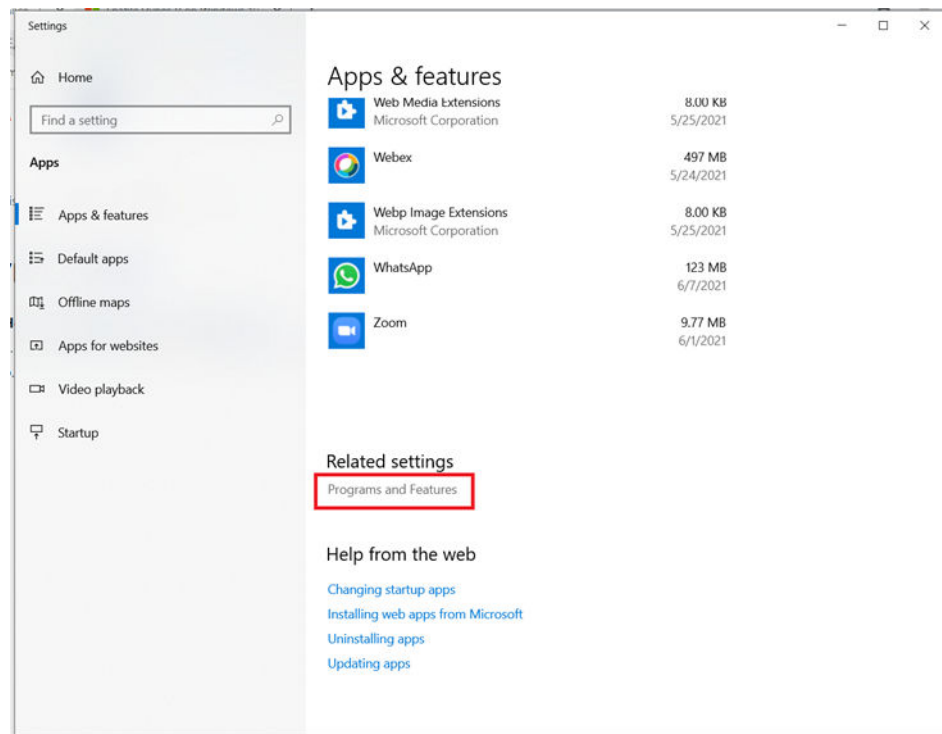
A Installation on Hyper-V

A.1 Enable Hyper-V on Windows® 10

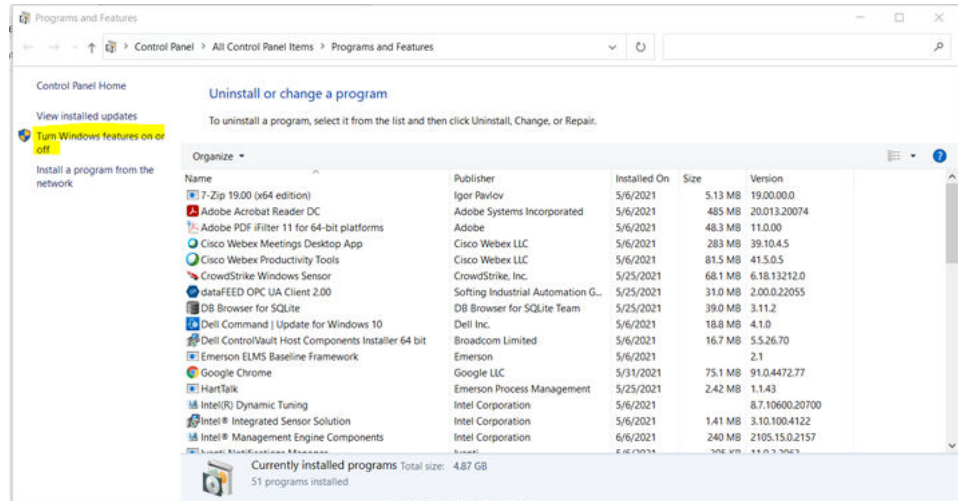
Procedure

1. Search for Apps & features.
2. On the **Apps & features** screen, click **Programs and Features**.

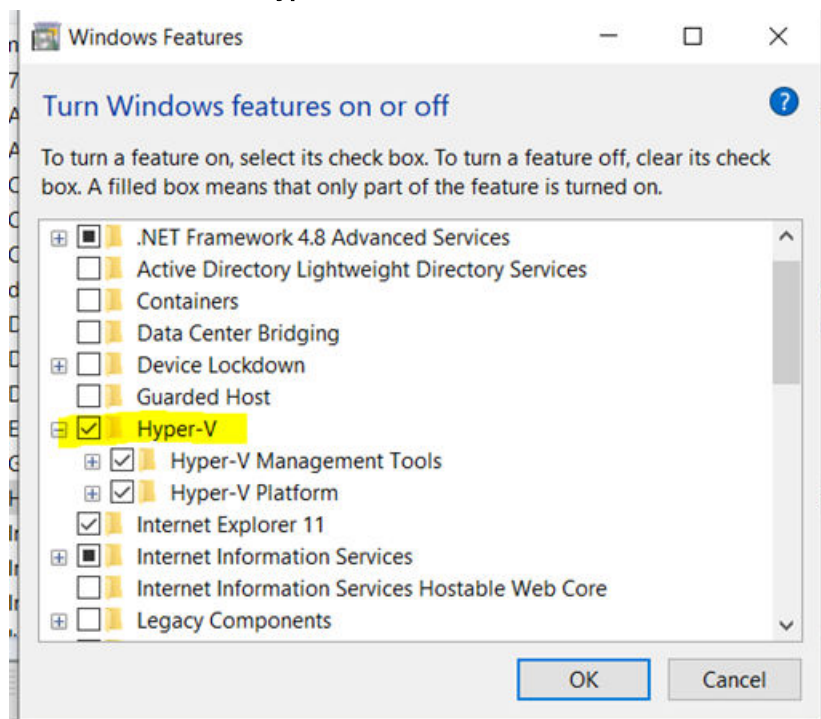
Figure A-1: Apps & features screen



3. Select **Turn Windows features on or off**.



4. Select the box next to **Hyper-V** and click **OK**.



When the installation is complete, Windows will prompt a machine restart.

5. After restarting, launch Hyper-V Manager and pin it to the task bar.

A.2 Hyper-V network settings for DHCP

The default Plantweb Insight configuration is targeted for Hyper-V on the latest version of Windows®, which provides a Default Switch virtual adapter.

The Default Switch provides DHCP functionality to assign Plantweb Insight an IP address.

Note

Port forwarding does not work on the Default Switch network configuration.

For older Hyper-V versions (which do not have a Default Switch virtual adapter), manually configure and connect network adapters.

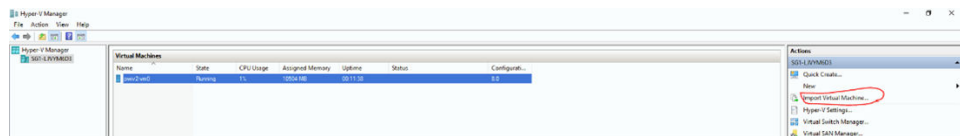
A.3 Set up the Plantweb Insight virtual machine

Procedure

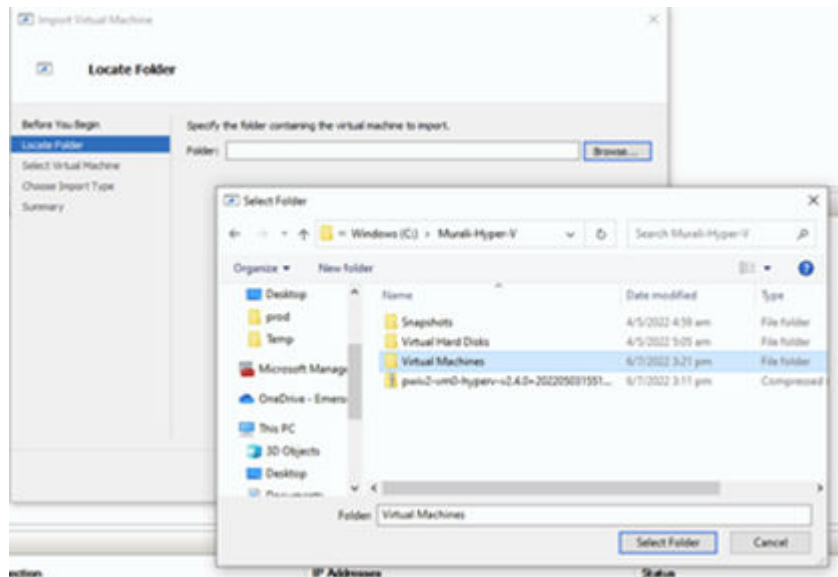
1. Download and unzip the Plantweb Insight Hyper-V zip file.



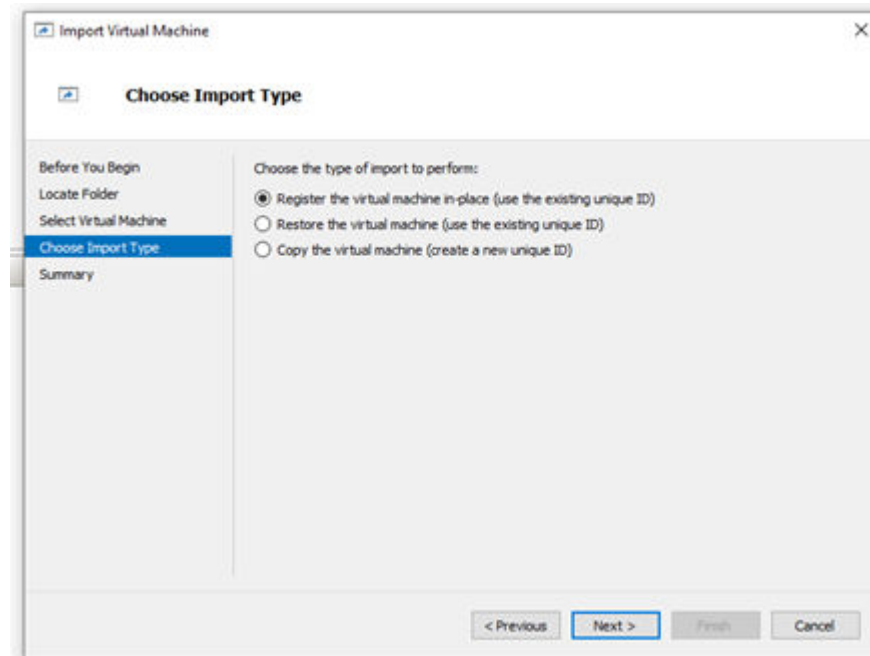
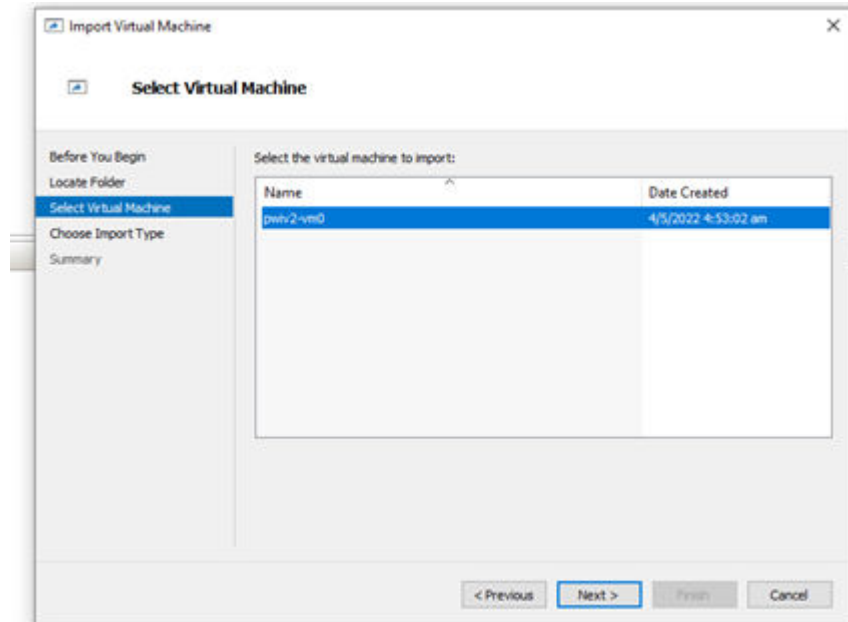
2. In the **Hyper-V Manager**, select **Import Virtual Machine**.



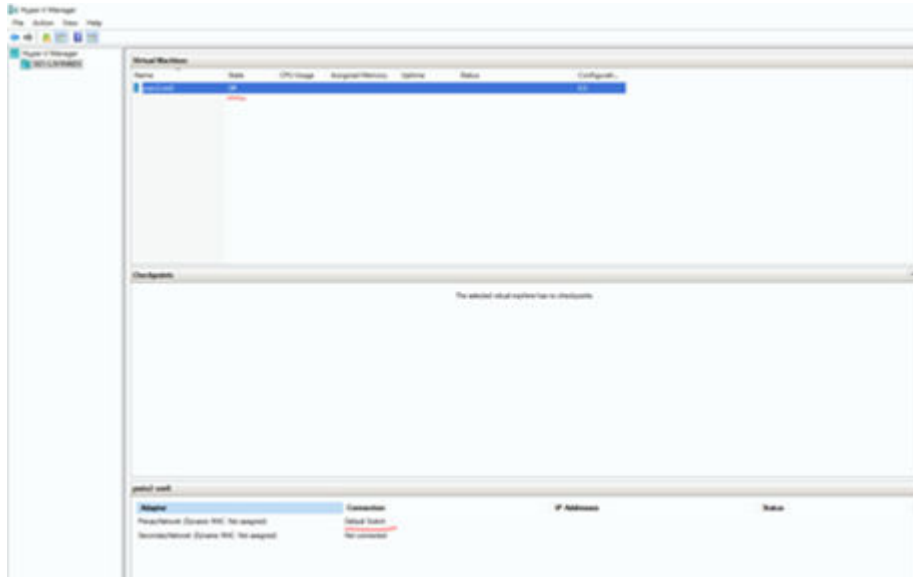
3. From the **File Explorer**, choose the **Virtual Machines** folder from the extracted path.



4. Continue with default selections and finish the setup.



You will see a virtual machine with a name that starts with *pwiv2*.

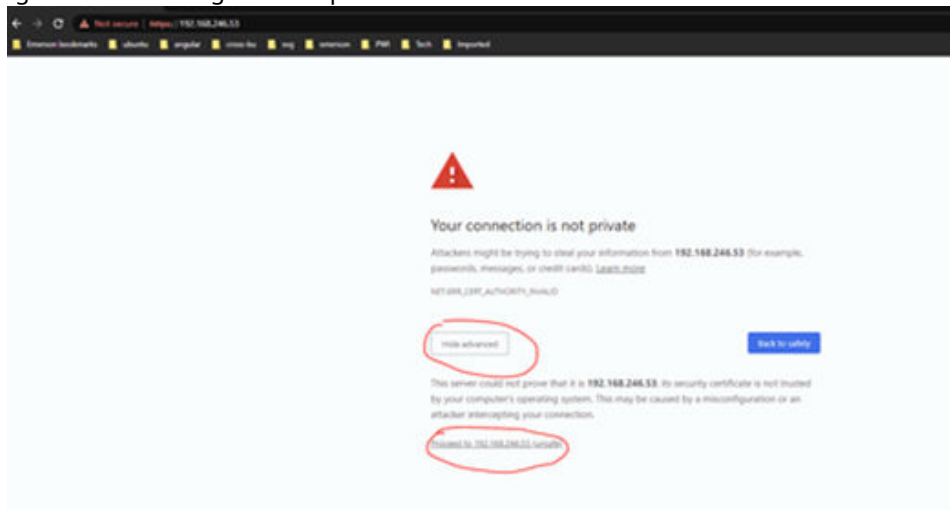


5. In the **Virtual Machines** screen, select the virtual machine and then select **Start** in the **Actions** bar on the right.
6. Once the virtual machine is running, select **Connect**.
An IP address appears on the console.



Now the Plantweb Insight server is running.

7. Wait five to ten minutes for the software to bring up necessary services before accessing the IP address from the web browser (<https://<IP Address>>). Click to proceed past any authorization warnings. Ignore the warnings with https certificates.



8. Refer to [Launch Plantweb Insight \(PWI\)](#) for the start-up procedure.

B Console rescue

If Plantweb Insight (PWI) user interface connection is lost due to either setting an incorrect static IP configuration on the **Ethernet Configuration** page or setting an incorrect HTTP white list on the **Ports and Protocols** page, restore the connection with this procedure as a low-privileged user.

Note

This is applicable for PWI version 2.3.0 and above.

Use the following credentials:

Username	pwi-user
Password	Emerson.1234

Note

As this is a low-privileged access account, only limited actions (such as list or clear) can be performed.

B.1 Set static IP

To override the Ethernet static IP settings for the primary Ethernet interface, set the static IP by running a script.

Procedure

1. Run this script: `sudo ./set-static-ip<<IP addr>> <<Netmask>> <<GW IP>>`
For example: `sudo ./set-static-ip192.168.238.125 255.255.255.0 192.168.238.2`
2. Enter `exit` and press **Enter** to log out of the console.
3. Reboot the virtual machine.

Once successful, connection to the Plantweb Insight (PWI) user interface is possible using the new static IP.

The script will check for the following errors:

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

B.2 Reset HTTP white list

Procedure

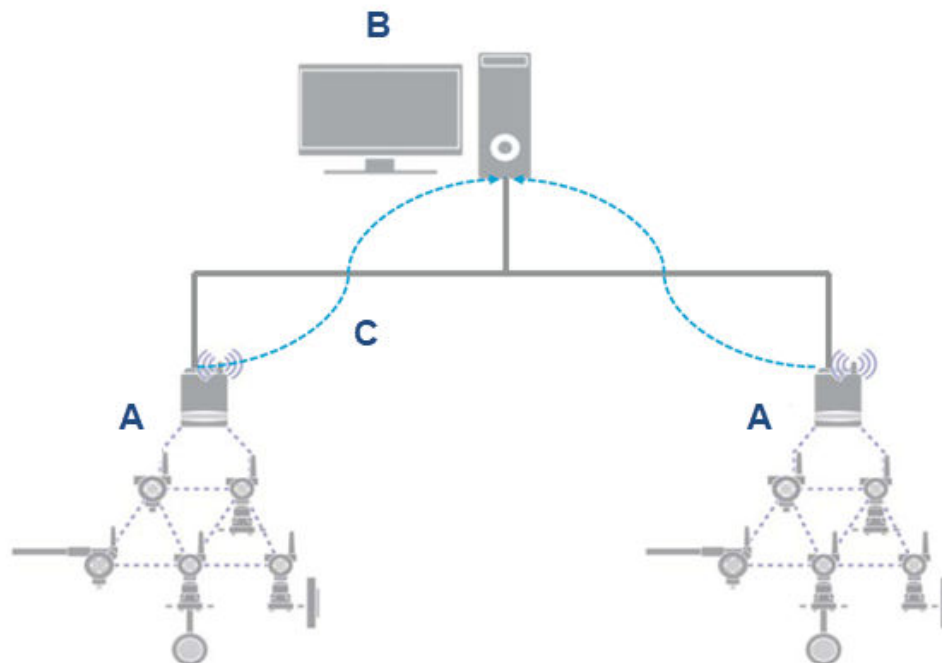
To reset the HTTP white list IP to 0/0, run the following script: `sudo ./http-whitelist-reset`

Once this is complete, connection to the Plantweb Insight (PWI) user interface from any IP in the same network is possible.

C Reference architectures

The following are sample architecture options for installing and configuring the Plantweb Insight system.

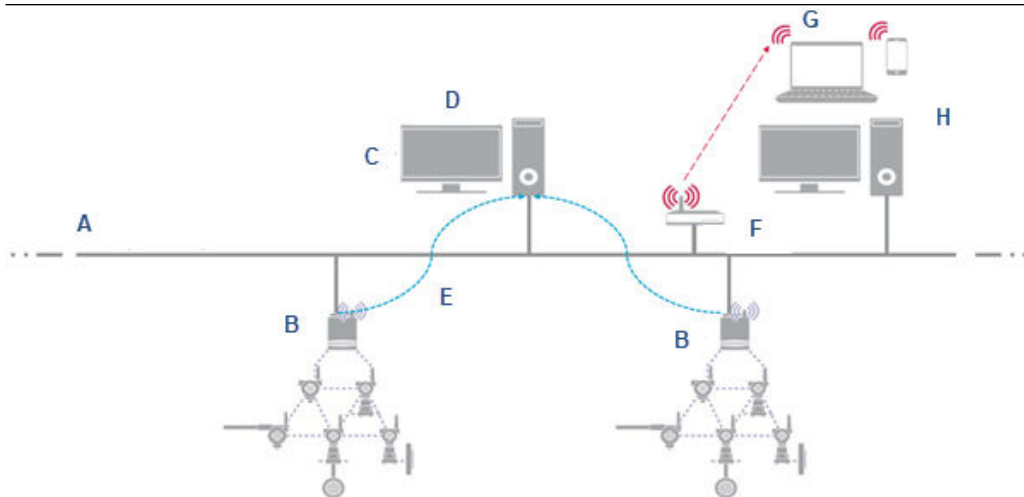
Standalone network architecture: example 1



- A. Emerson wireless Gateway
 - B. Plantweb Insight
 - C. HART[®]-IP: TCP Port 5094
-

This simple standalone architecture includes a host machine to run Plantweb Insight, which is connected to the *WirelessHART* Gateway(s). The Emerson wireless sensors are connected to these Gateways. Plantweb Insight can be accessed directly from the host machine's web client.

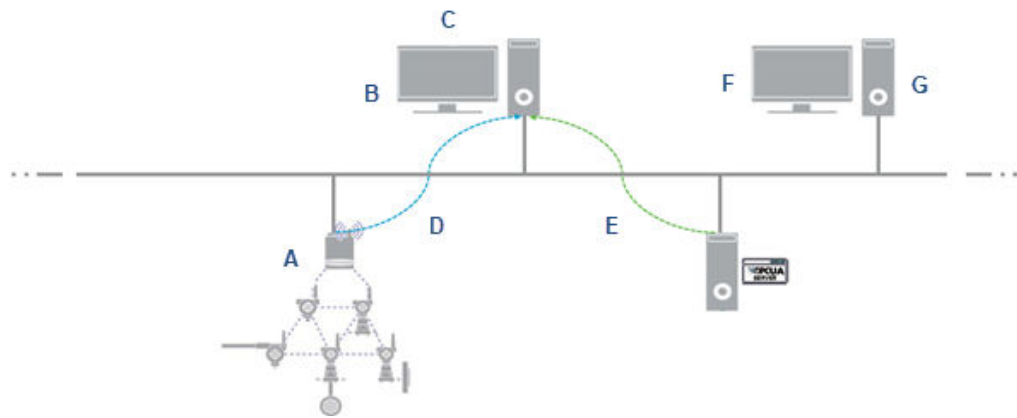
Standalone network architecture: example 2



- A. Network (DHCP server)
- B. Emerson wireless Gateway
- C. Web server
- D. Plantweb Insight
- E. HART-IP: TCP Port 5094
- F. Wireless router
- G. Web client
- H. HTTPS: TCP Port 80

This standalone architecture includes a host machine to run Plantweb Insight, which is connected to the *WirelessHART* Gateway(s). Emerson wireless sensors are connected to these Gateways. Plantweb Insight can be accessed directly from the host machine's web client or from any web client with network access. Bridge the network adapter of the Plantweb Insight virtual machine.

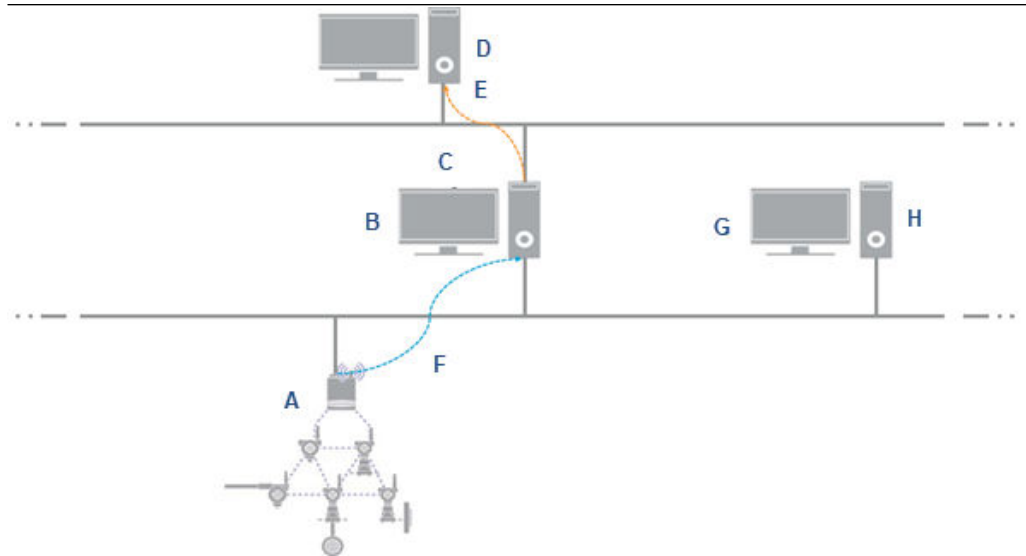
Simplified wired and wireless network architecture



- A. Emerson wireless Gateway
 - B. Web server
 - C. Plantweb Insight
 - D. HART-IP: TCP Port 5094
 - E. OPC UA: TCP Port 4880
 - F. Web client
 - G. HTTPS: TCP Port 80
-

This simplified architecture shows how Plantweb Insight can receive both wireless data (via *WirelessHART*) and wired data (via OPC UA).

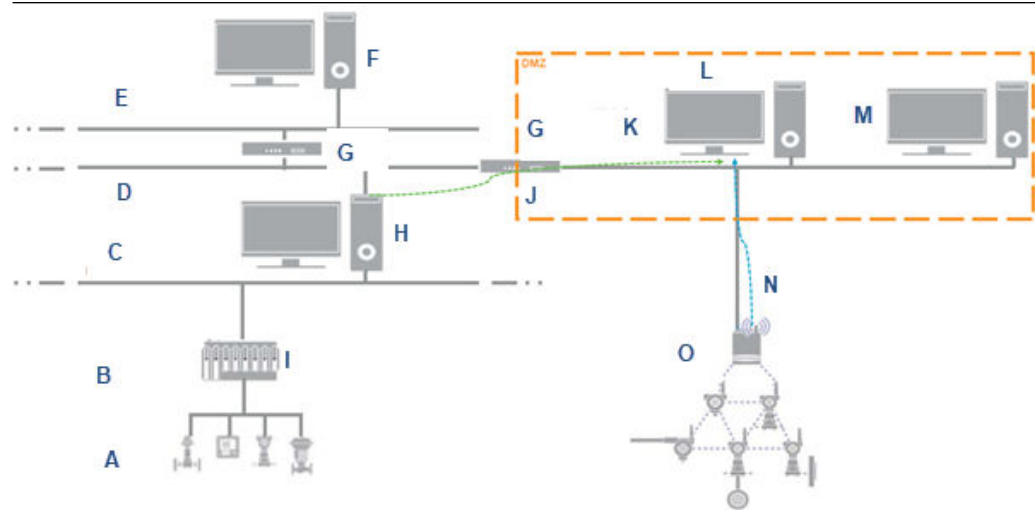
Pushing alerts to historian network architecture



- A. Emerson wireless Gateway
- B. Web server
- C. Plantweb Insight
- D. Plant historian
- E. Modbus® TCP: TCP Port 502
- F. HART-IP: TCP Port 5094
- G. Web client
- H. HTTPS: TCP Port 80

This simplified architecture shows how Plantweb Insight can receive wireless data (via *WirelessHART*) and send calculated data (via *Modbus*) to a historian.

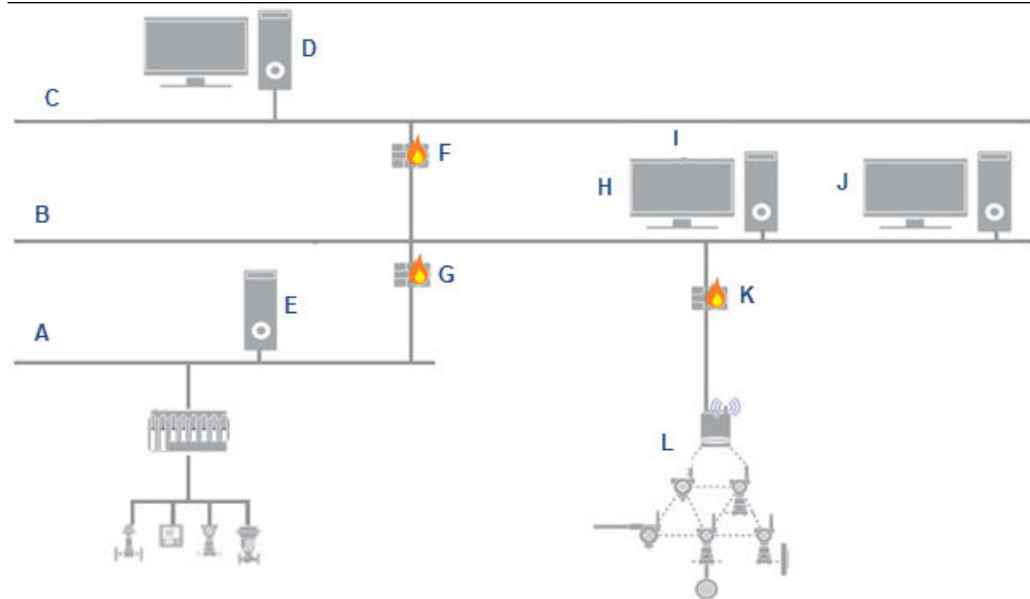
DMZ network architecture level 2.5: example 1



- A. Level 0
- B. Level 1
- C. Level 2
- D. Level 2.5
- E. Level 3
- F. Plant historian
- G. Firewall
- H. Application workstation
- I. Controller
- J. OPC UA: TCP Port 4880
- K. Web server
- L. Plantweb Insight
- M. Web client
- N. HART-IP: TCP Port 5094
- O. Emerson wireless Gateway

This DMZ architecture is a typical situation where both wired data (via OPC UA) and wireless data (via HART-IP) are used within Plantweb Insight. This is typically done by using a DMZ architecture where the wired data comes from the DCS or PLC and wireless data comes directly from the *WirelessHART* Gateway(s).

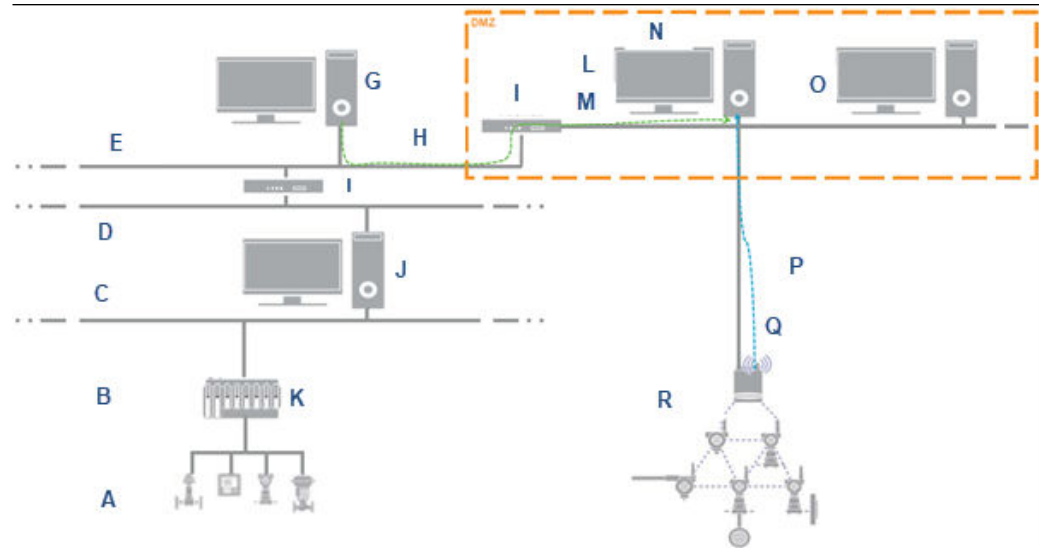
DMZ network architecture level 2.5: example 2



- A. Level 2
- B. Level 2.5
- C. Level 3
- D. Plant historian
- E. Application workstation
- F. Modbus TCP: TCP Port 502 from Plantweb Insight
- G. OPC UA: TCP Port 4880 to Plantweb Insight
- H. Web server
- I. Plantweb Insight
- J. Web client
- K. HART-IP: TCP Port 5094
- L. Emerson wireless Gateway

This DMZ architecture is a typical situation where both wired data (via OPC UA) and wireless data (via HART-IP) are used within Plantweb Insight and calculated data from Plantweb Insight is sent to a historian via Modbus.

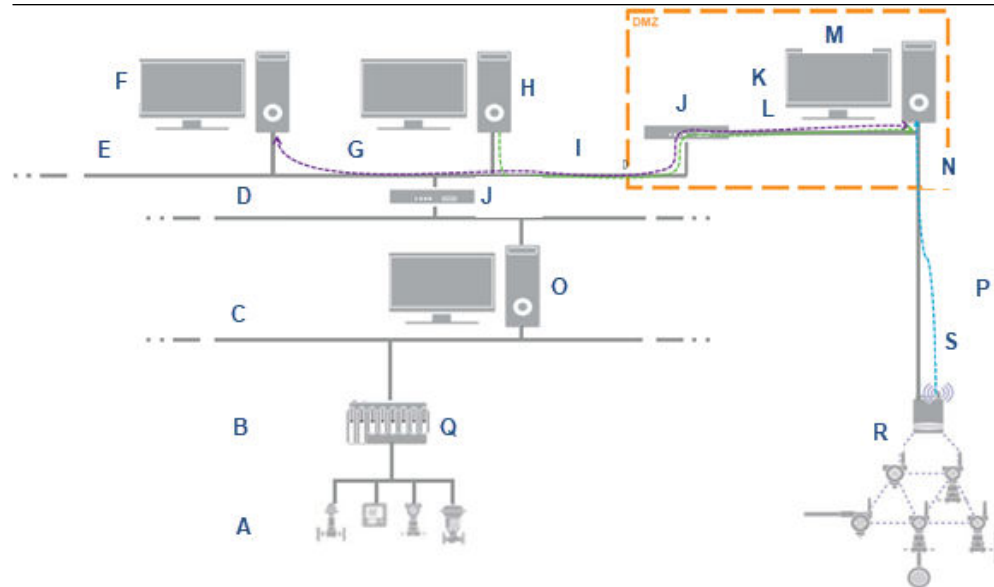
DMZ network architecture level 3.5: example 1



- A. Level 0
- B. Level 1
- C. Level 2
- D. Level 2.5
- E. Level 3
- F. Plant historian
- G. OPC UA Port 4880
- H. Firewall
- I. Application workstation
- J. Controller
- K. Web server
- L. Level 3.5
- M. Plantweb Insight
- N. Web client
- O. Standalone network
- P. HART-IP: TCP Port 5094
- Q. Emerson wireless Gateway

This DMZ architecture uses the standalone wireless network to bring wireless data to Plantweb Insight and to access the web interface. Data can also be delivered or retrieved from a historian at level 3 in the control network via OPC UA.

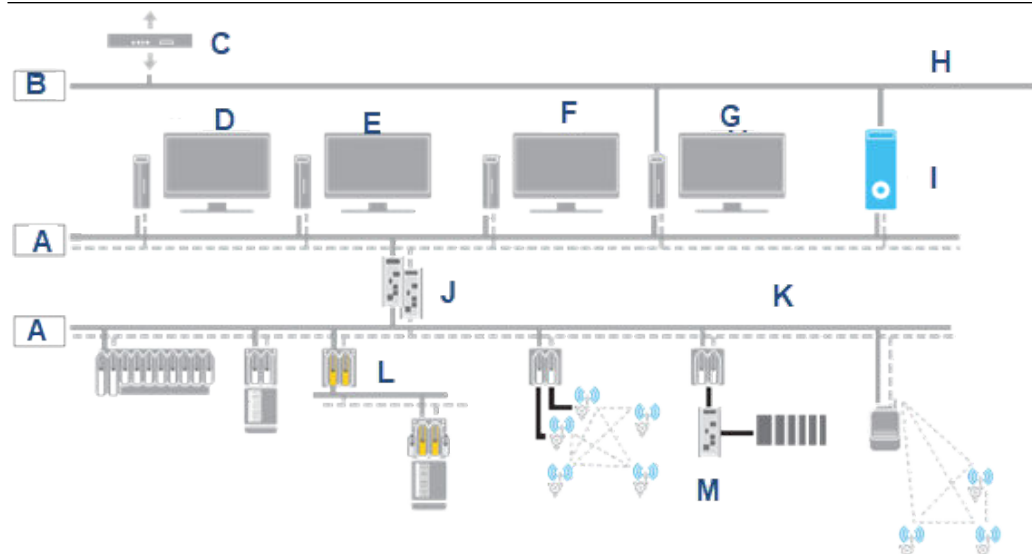
DMZ network architecture level 3.5: example 2



- A. Level 0
- B. Level 1
- C. Level 2
- D. Level 2.5
- E. Level 3
- F. Web client
- G. HTTPS: TCP Port 80
- H. Plant historian
- I. OPC UA: TCP Port 4880
- J. Firewall
- K. Web server
- L. Level 3.5
- M. Plantweb Insight
- N. HART-IP
- O. Standalone network
- P. HART-IP: TCP Port 5094
- Q. Emerson wireless Gateway

This DMZ architecture uses the standalone wireless network to bring wireless data to Plantweb Insight. Data can also be delivered or retrieved from a historian (via OPC UA). Plantweb Insight can be accessed from a web client at level 3 in the control network.

DeltaV compatible network architecture



- A. Level 2
- B. Level 2.5
- C. Emerson smart firewall
- D. Professional plus
- E. Operator workstation
- F. SIS engineering station
- G. Level 2.5 network
- H. ESXi or Hyper-V server with Plantweb Insight virtual machine
- I. Firewall - IPD
- J. DeltaV area control network
- K. Controllers, inputs, and outputs
- L. Firewall

While Plantweb Insight is typically kept separate from the control system, it can run on DeltaV systems. The architecture diagram displays how this is accomplished by using a separate Plantweb Insight server on the level 2 network. This allows Plantweb Insight to access data coming directly from the Gateways that are feeding DeltaV. For more information, refer to Plantweb Insight support on this [DeltaV Systems White Paper](#).

D Licensing in Plantweb Insight

D.1 License types

D.1.1 Subscription licenses

A subscription license has a start date and end date.

- Subscription licenses can only be installed during the validity period. Installation of a license that has expired or one which has a validity starting at a future date is not permitted.
- License expiration warnings begin 90 days before the license end date.

Figure D-1: Subscription license



D.1.2 Trial licenses

A trial license has a shorter validity period than a subscription license.

Trial licenses use a fixed number of days (90 days) instead of start and end dates.

Figure D-2: Trial license



D.1.3 License states

Unlicensed	Valid	Expiring	Grace period	Expired
App is not accessible. App is shut down and no data is processed.	App is accessible.	Accessible with a warning message at app launch.	Accessible with a higher warning message at app launch.	App is not accessible. App is shut down and no data is processed.

Grace period

Both subscription and trial licenses have a grace period (seven days) in addition to the original validity.

When the validity period ends, the license enters the grace period. There is no difference in the capabilities of the application during the valid license period and grace period. The only difference is that higher level warning messages will be displayed.

D.2 Home page licensing pop-up messages

Described are the different app icon license badges and licensing messages that could appear on the home page.

License badges on app icons

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

Figure D-3: Subscription license



The license badge represents the license type and status.

- S** Subscription license
- T** Trial license

Color codes

- Green** Active
- Amber** Expiring within the next 90 days
- Red** Expired

Figure D-4: Home page showing apps with licenses

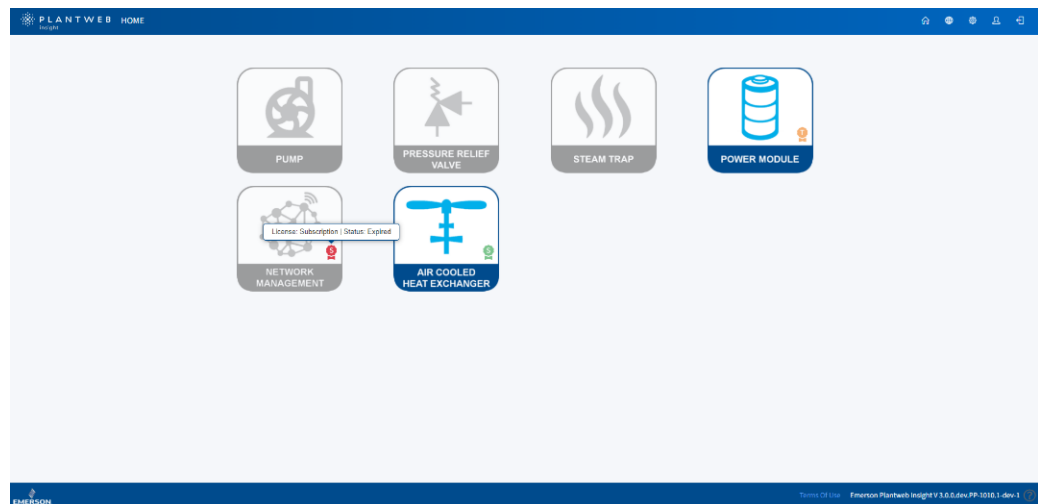


Figure D-5: Pop-up message when app has no license installed

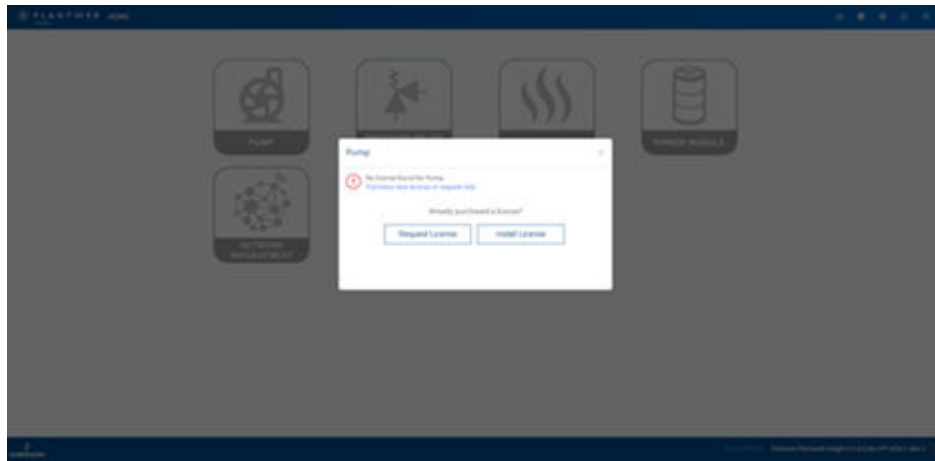


Figure D-6: Pop-up message for app with an expiring license

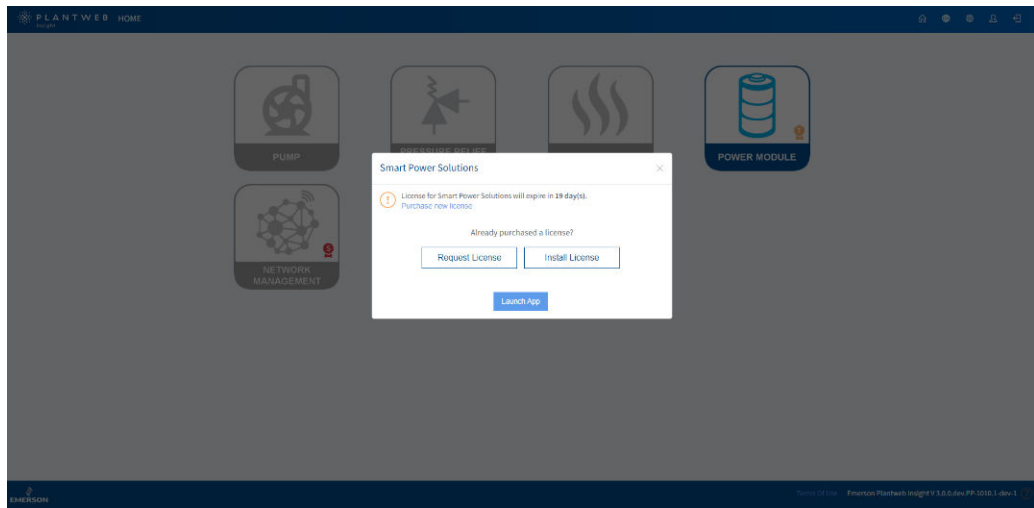
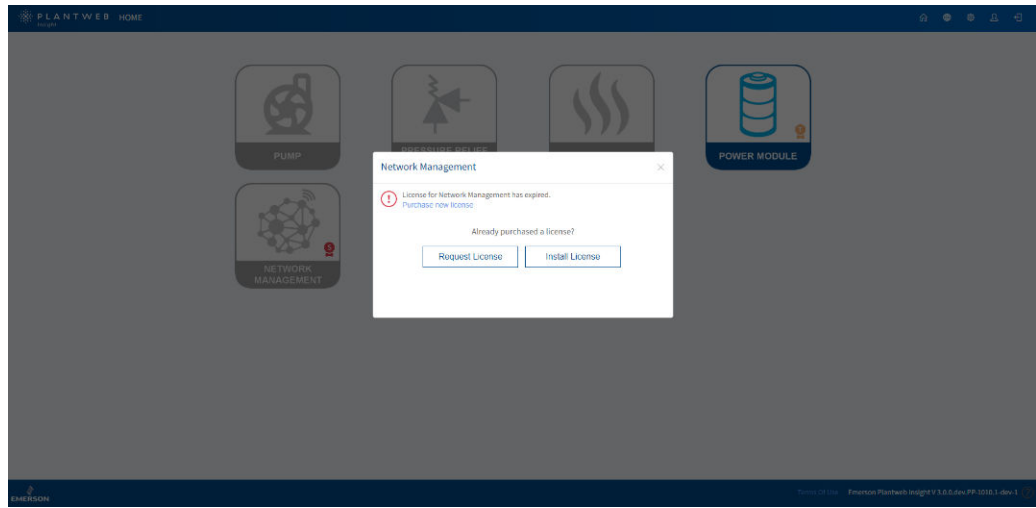


Figure D-7: Pop-up message for app with an expired license



D.3 Request a subscription or trial license

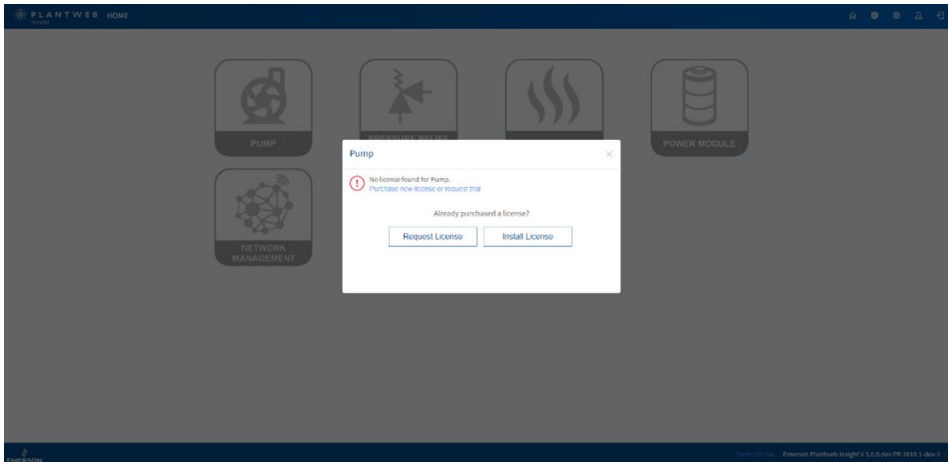
On the Plantweb Insight (PWI) **Home** page, applications that have no licenses installed are grayed out.

Procedure

1. On the PWI **Home** page, click a gray app icon.

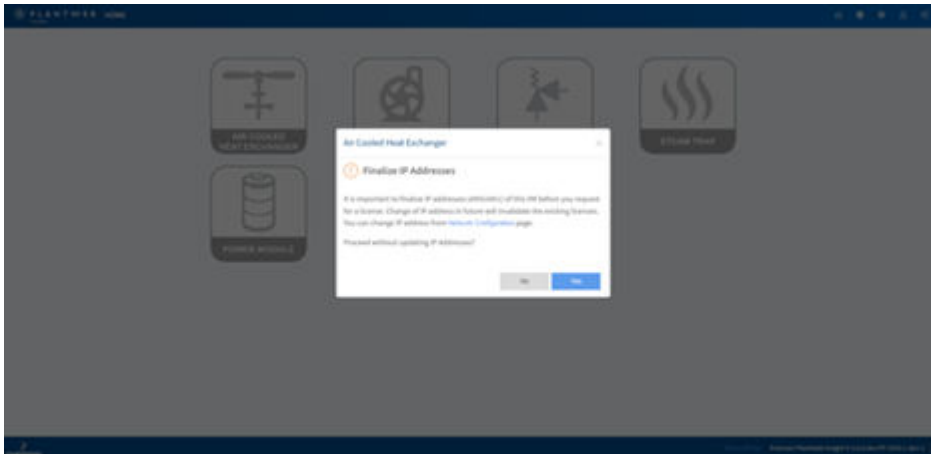


2. On the dialog that pops up, click **Purchase new license** or **Request trial**.



On a PWI installation where no license has ever been installed, a **Finalize IP Addresses** message pops up.

3. To update IP addresses, click **Network Configuration**. If IP addresses are updated, click **Yes**.



4. To request a trial license, check the Request for Trial box. To purchase a subscription license, leave the Request for Trial box unchecked.



5. Scan the QR code to open email. Fill in the details on the email template.
Lock Code should already be in the template.
To include other applications in the request, enter their names in the **Notes** section.
6. Send the email.

D.4 Install subscription or trial license from Home page

On the Plantweb Insight (PWI) **Home** page, applications which do not have licenses installed are grayed out.

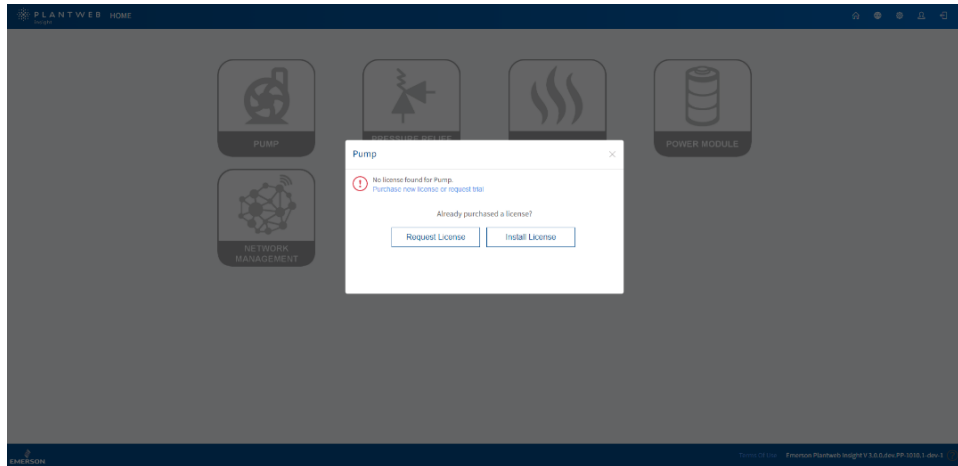
Procedure

1. Click the gray icon of the app for which a license is to be installed.



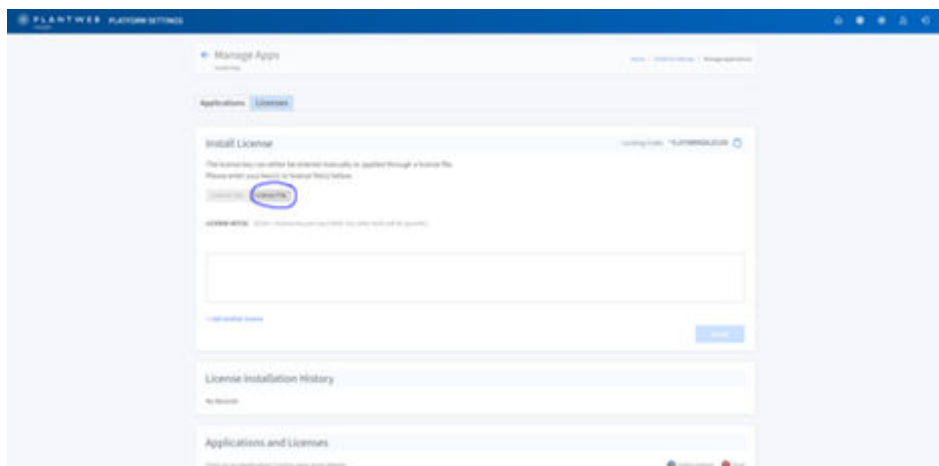
The **Licensing** dialog appears.

2. Click **Install License**.

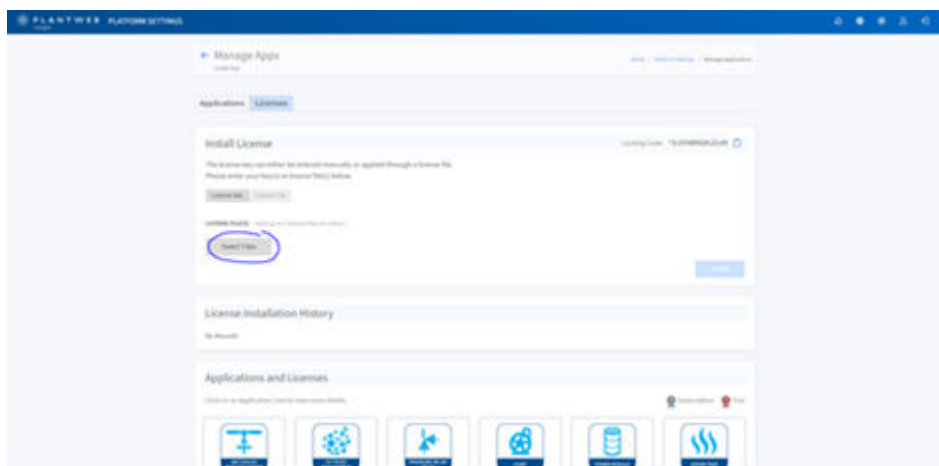


The **Application Manager** → **Install License** page is displayed.

3. Click **License File** to switch to File mode.



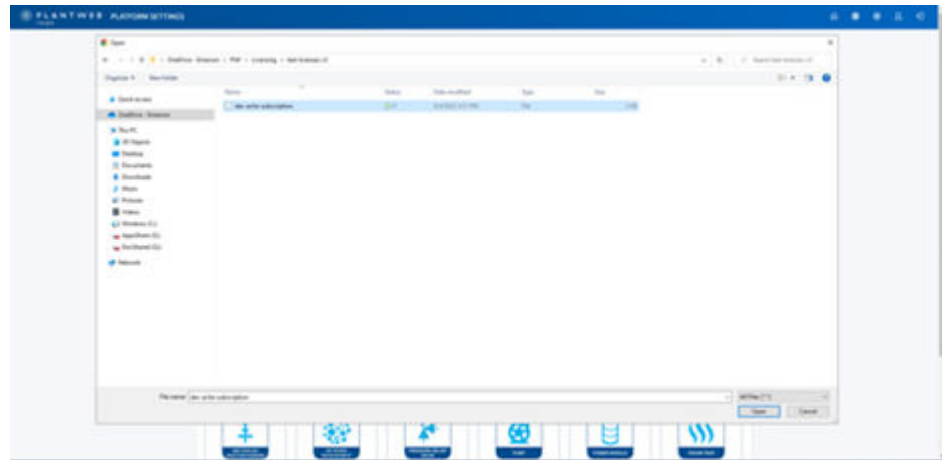
4. Click **Select Files**.



5. Browse to the license file location. Make sure to select **All Files (*.*)** from the drop-down list at the bottom right of the **File Selection** window.
6. Select the license file(s) and click **Open**.

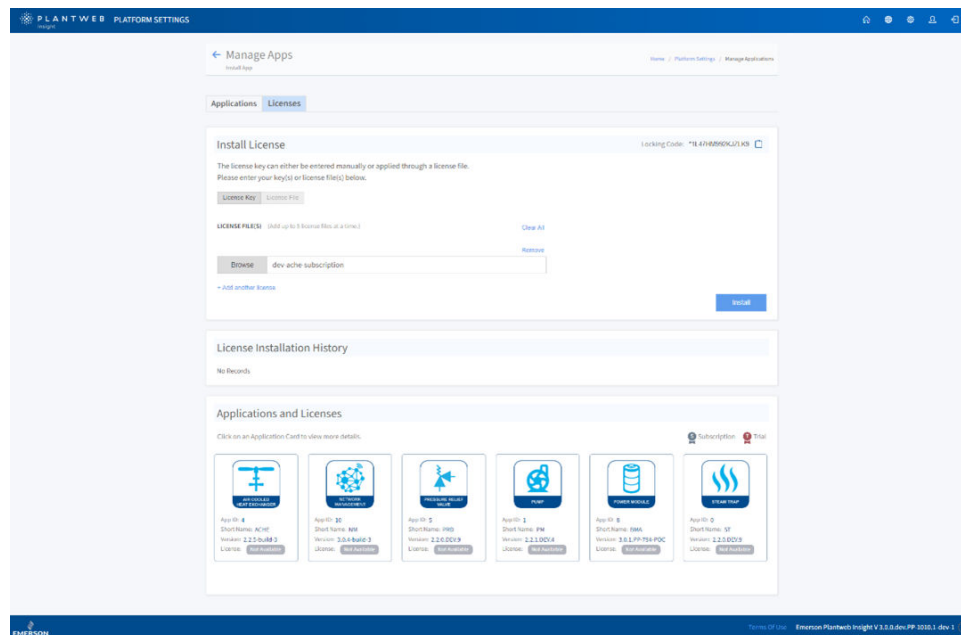
Note

Up to five license files can be selected.



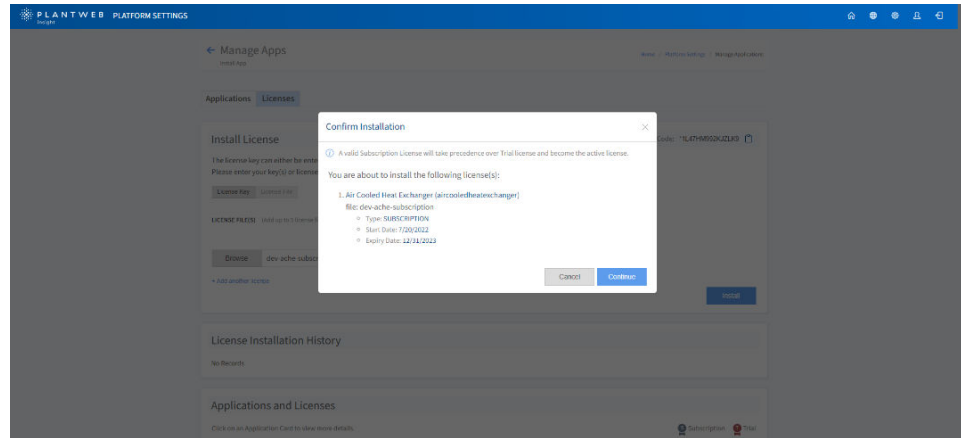
The selected license file(s) will appear on the **Install License** page. Invalid or larger files will be filtered out.

7. Click **Install**.

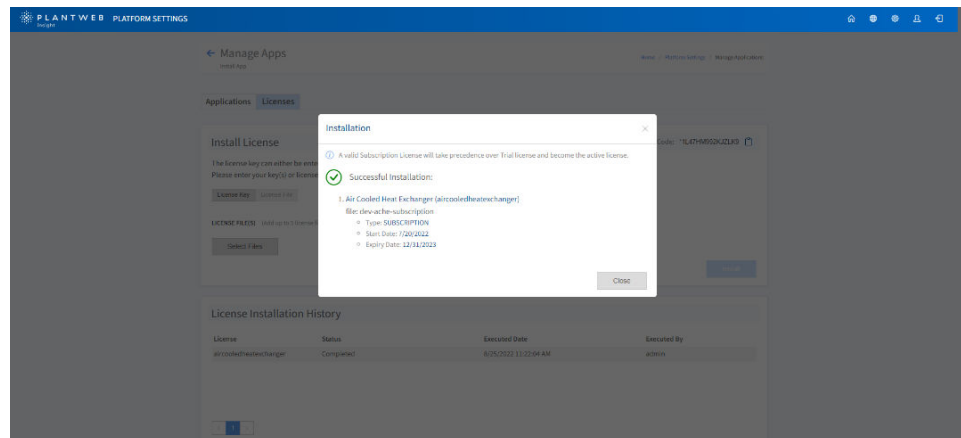


A **Confirmation** dialog pops up.

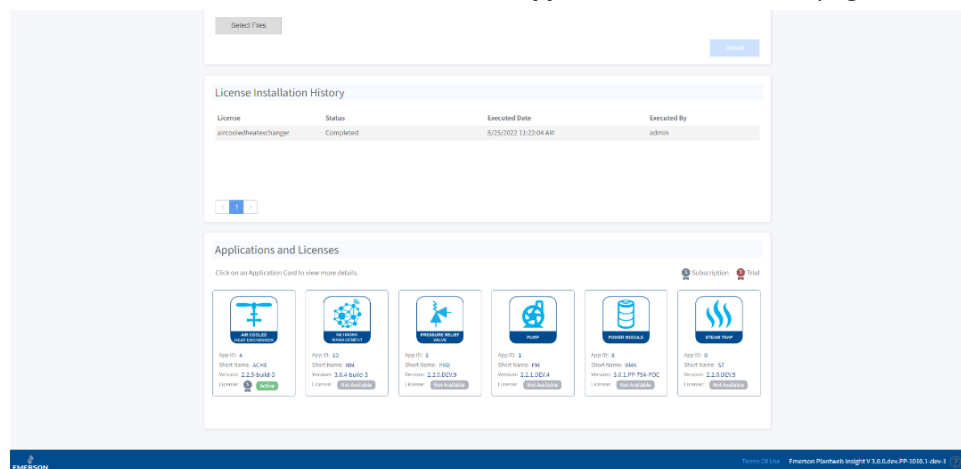
8. Review the license details on the **Confirmation** dialog. Then click **Continue**.



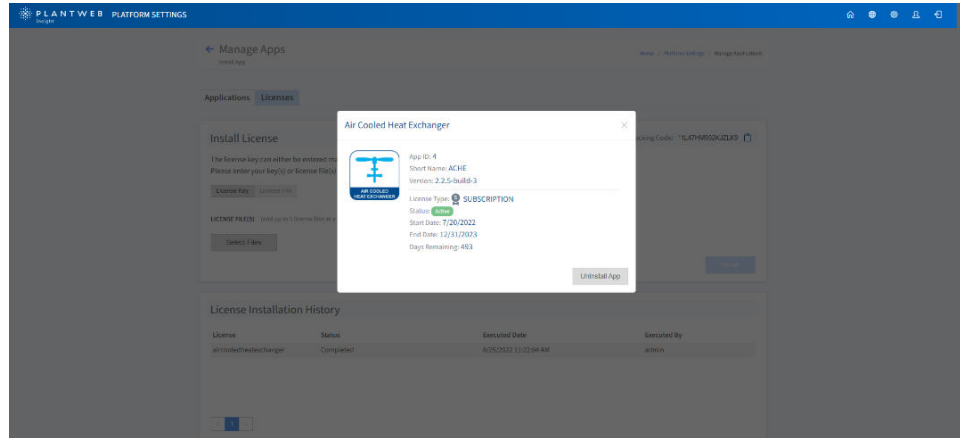
9. Click **Close** on the **Installation Result** dialog.



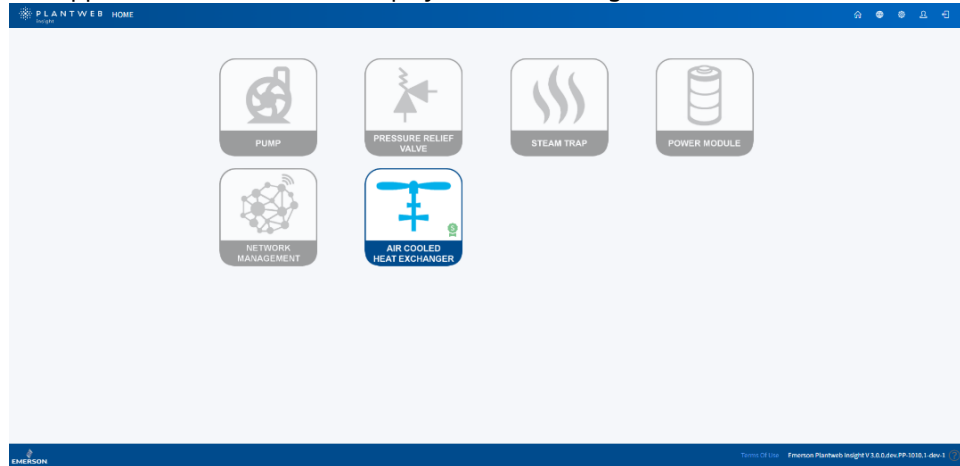
10. Check the license status at the bottom of the **Applications and Licenses** page.



11. Click the application icon to view the license details.



- Return to the **Home** page.
The application is enabled and displays a License badge.



See [Home page licensing pop-up messages](#) for information about License badges.

D.5 License installation errors

If the license installation fails, error information will be displayed on the **Installation Result** dialog and below the License Input field.

Figure D-8: Installation Result dialog

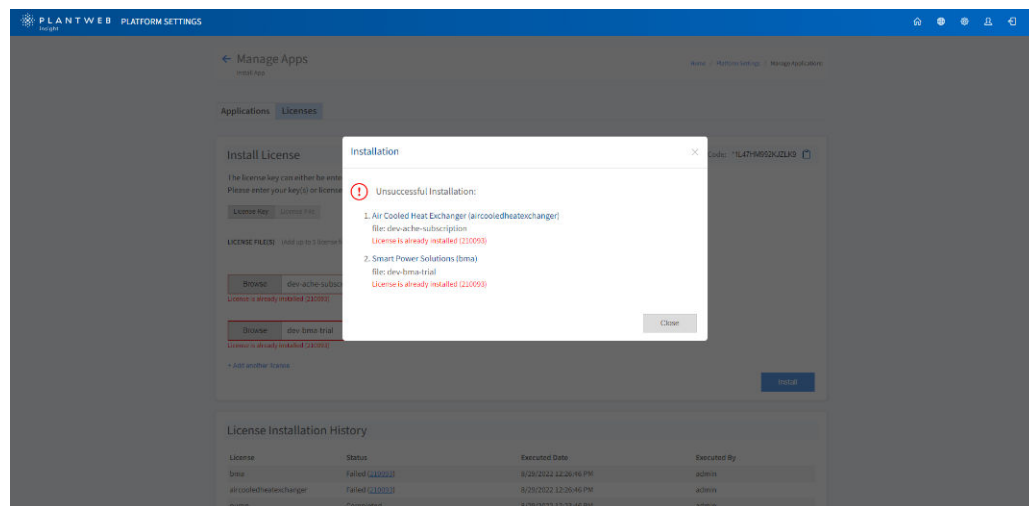


Figure D-9: Error on Licenses page

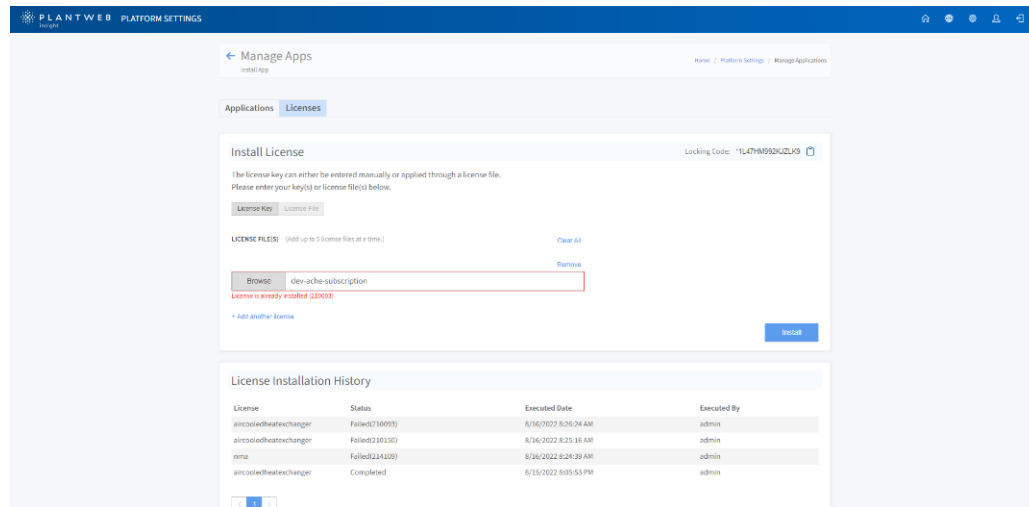


Table D-1: Common errors

Error code	Error message on user interface	Description
210150	Locking Code is invalid	The lock code used to generate the license is invalid (most likely because it does not match the lock code on the current Plantweb Insight (PWI) installation).
214109	Expired License	License is expired.
210093	License was already installed	License was already installed.

Table D-1: Common errors (continued)

Error code	Error message on user interface	Description
210188	License can only be activated on or after start date	The license start date has not been reached.

For more information: [Emerson.com](https://www.emerson.com)

©2023 Emerson. All rights reserved.

Emerson Terms and Conditions of Sale are available upon request. The Emerson logo is a trademark and service mark of Emerson Electric Co. Rosemount is a mark of one of the Emerson family of companies. All other marks are the property of their respective owners.

