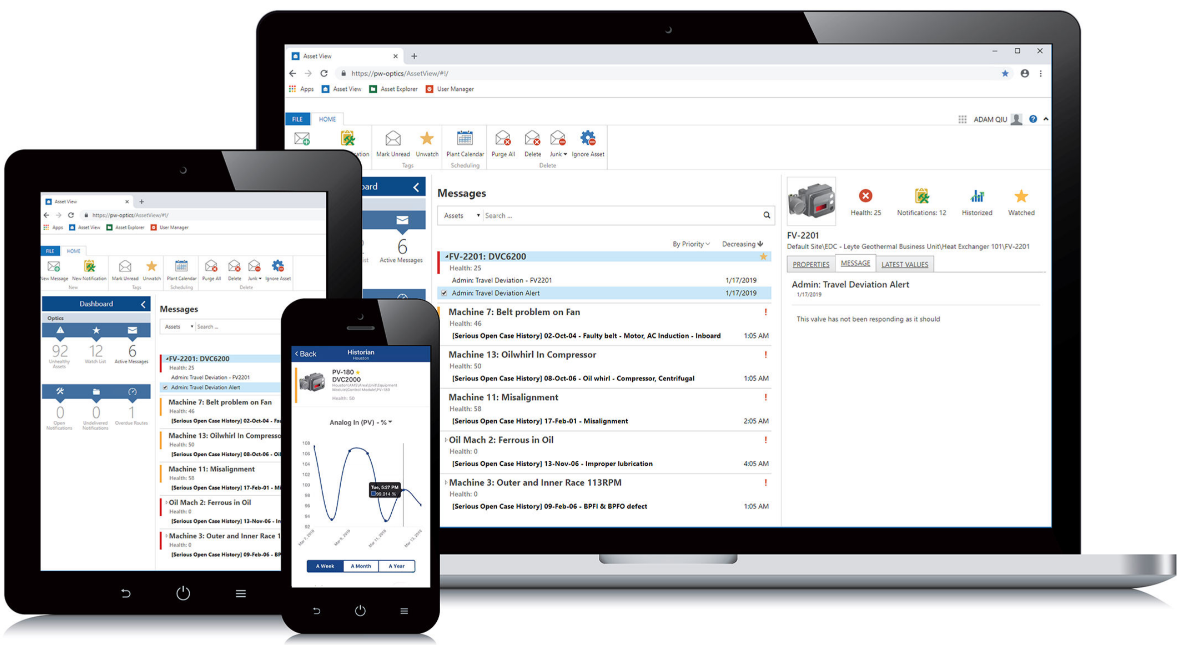
System Guide
MHM-97911, Rev 10
April 2020

Plantweb™ Optics v1.5

Plantweb™ Optics System Guide



EMERSON

Disclaimer

This manual is provided for informational purposes. EMERSON MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Emerson shall not be liable for errors, omissions, or inconsistencies that may be contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material. Information in this document is subject to change without notice and does not represent a commitment on the part of Emerson. The information in this manual is not all-inclusive and cannot cover all unique situations.

Patents

The product(s) described in this manual are covered under existing and pending patents.

Where to get help

Emerson provides a variety of ways to reach your Product Support team to get the answers you need when you need them:

Phone	Toll free 800.833.8314 (U.S. and Canada) +1.512.832.3774 (Latin America) +63.2 702.1111 (Asia Pacific, Europe, and Middle East)
Email	ap-sms@emerson.com
Web	http://www.emerson.com/en-us/contact-us

To search for documentation, visit http://www.emerson.com.

To view toll free numbers for specific countries, visit http://www.emerson.com/technicalsupport.

Contents

1 Introduction

Plantweb™ Optics

Plantweb Optics is the Emerson software application for managing asset health across the enterprise. Plantweb Optics combines the data from multiple applications into asset-centric information, then delivers persona-based alerts and Key Performance Indicators (KPIs) for improving the reliability of your rotating equipment, instruments, and valves.

The Plantweb Optics asset performance platform improves reliability and availability by enhancing the visibility to the health of your assets. Experts in your facility are always connected to assets they care about most. Through open protocols, operational data is centralized and contextualized from disparate data sources. The data is delivered to your experts with personalized content and dashboards. Plantweb Optics provides the information you need in a collaborative environment to enhance your workflow and drive corrective actions.

Plantweb Optics supports receiving data from a number of asset sources including AMS Device Manager, AMS Machinery Manager, Emerson WirelessHART gateways, and Plantweb Insight. In addition, Plantweb Optics interfaces with enterprise CMMS systems and data can be read from the system via the OPC UA server.

Configuration and interaction with Plantweb Optics happen through these utilities, which can be launched from a web browser:

- **Asset Explorer**—access and manage assets in your plant.
- **Asset View**—send, receive, and view messages in Plantweb Optics.
  You can access the same messages from a mobile device by installing the Plantweb™ Optics Mobile App.
- **User Manager**—control and monitor access to various areas of Plantweb Optics.
- **Event Viewer**—view system generated events.

About this manual

The Plantweb Optics System Guide is intended for system administrators to help plan, install, and set up the software. Emerson recommends that system administrators reference this document when setting up the Plantweb Optics system.

NOTICE

Installing AMS Machine Works? AMS Machine Works installation information has been removed from the Plantweb Optics System Guide. Please contact Emerson Product Support for details.

Other relevant documents

- Plantweb Optics Online Help—provides instructions and reference information for using Plantweb Optics after installation. This is built into the software and accessed by clicking ? in the user toolbar.
- Release Notes—contains what is new and notes pertaining to the release.

- Knowledge Base Articles—documents released to address known issues, frequently asked questions, history traces, system requirements, how-to information, and application-specific content.

2 Quick start

For an optimum system, follow this recommended installation order for a new system.

Note
Some components must be installed, and some are optional depending on the user's needs and licensing.

Prerequisites

Emerson recommends that all applications that will be connected to the system should be configured and running before starting your installation.

2.1 Preparing for installation

Procedure

1. Design and plan your system. See Planning your system.
2. Ensure all of the system requirements are met for the Plantweb Optics server, Plantweb Optics Asset Source Interface server, and any other required components. See System requirements.
3. Ensure all security requirements have been met. See Plantweb Optics security.
4. Acquire your Plantweb Optics licenses prior to installation. See Acquire licenses.

2.2 Installing Plantweb Optics

Note
These steps are required for every Plantweb Optics installation.

Procedure

1. Complete pre-installation steps required before obtaining data from other systems. See Pre-installation configurations.
2. Install Plantweb Optics Historian. Run the Plantweb Optics installer (A48OPTICS-SYSTEM0.Plantweb_Optics.1.5.X.X) on the Plantweb Optics Server. See Install the Plantweb Optics Historian.
3. Install Plantweb Optics Web Services by running the Plantweb Optics Installer (A48OPTICS-SYSTEM0.Plantweb_Optics.1.5.X.X) on the Plantweb Optics Server. See Install Plantweb Optics Web Services.
4. Register your Plantweb Optics License from the Plantweb Optics User Manager utility. See Register licenses.
5. View **License Summary** from the User Manager. See View license summary.

2.3 Installing optional services

Each of the services below are available within Plantweb Optics. Only licensed services should be installed. Licensed components are displayed in the Plantweb Optics User Manager utility under the **Licenses** tab.

Procedure

1. Register and install all licensed push model ASIs. See Installing Push Model ASIs to quickly get started. Push model ASIs include:
    - AMS Asset Monitor ASI
    - AMS Device Manager ASI
    - DeltaV Control Loop ASI
    - KNet ASI
2. Install the **Emerson Wireless Gateway ASI** on the ASI server and proceed using the default settings. See Emerson Wireless Gateway ASI.
3. Install the **Plantweb Insight ASI** on the ASI server and proceed using the default settings. See Plantweb Insight ASI.
4. Install the **AMS Machinery Manager ASI Web Service** on the ASI server. See Install AMS Machinery Manager ASI web application service.
5. Install the **AMS Machinery Manager ASI IO Service** on the AMS Machinery Manager server with default settings. During MMASI IO Services installation, when prompted for **MM Admin Password**, enter **Emerson#1** or the password set by the Administrator. See Install AMS Machinery Manager ASI IO service.
6. Install the **CMMS Interface** on the CMMS Server. See Install CMMS Interface.
7. Install the **Plantweb Optics OPC UA Server** by running the Plantweb Optics installer on the Plantweb Optics Server and selecting **Plantweb Optics OPC UA Server**. Proceed using the default settings. See Install the Plantweb Optics OPC UA Server.

2.4 Installing Push Model ASIs

Push model ASIs consist of a Data Collector, a Connector Service, and an optional Proxy to provide asset source data to Plantweb Optics.

Prerequisites

- Plantweb Optics is installed and licensed for the ASIs you want to install.

Procedure

Run registration scripts on Plantweb Optics

1. On the Plantweb Optics server, run the installer for the Data Collector you want to connect to Plantweb Optics and select the **registration** option in the installer.
2. In Plantweb Optics, verify the Data Collector folder is listed in the **Network** tab.
3. Export the Plantweb Optics self-signed security certificate bound to port 443 (configurable default) in IIS: Export a security certificate.

Install the Connector Service

4. On the server where the Connector Service will be installed, import the Plantweb Optics self-signed certificate that was previously exported: Import a security certificate. After importing a certificate, close any open browsers to ensure that the certificate is applied to your browsing session.
5. Ensure that the connection to Plantweb Optics is secure by navigating to `https://<OpticsServerMachineName>/AssetExplorer` in your web browser.
   If the connection is secure, Asset Explorer will appear – proceed to the next step. If the connection is not secure, a warning will display in your browser – complete the certificate export-import process again.
6. Install the Connector Service.
7. Ensure the Connector Service is running by navigating to `https://<ConnectorServiceMachineName>/ConnectorService` in your web browser on the Connector Service PC. A web page displaying `Connector Service` indicates the connector service is running.
8. Export the Connector Service self-signed certificate bound to port 443 (configurable default) in IIS: Export a security certificate.

(Optional) Install a Proxy and connect it to a Connector Service

9. On the server where the Proxy will be installed, import the Connector Service self-signed certificate that was previously exported: Import a security certificate. After importing a certificate, close any open browsers to ensure that the certificate is applied to your browsing session.
10. Ensure that the connection to the Connector Service is secure by navigating to `https://<ConnectorServiceMachineName>/ConnectorService` in your web browser.
    If the connection is secure, `Connector Service` will display in the top left corner of the web page – proceed to the next step. If the connection is not secure, a warning will display in your browser – complete the certificate export-import process again.
11. Install the Proxy.
12. Ensure the Proxy is running by navigating to `https://<ProxyMachineName>/Proxy` in your web browser.
    The Proxy UI will appear, indicating the Proxy is running.
13. Export the Proxy self-signed certificate bound to port 443 (configurable default) in IIS: Export a security certificate.

(Optional) Install a Proxy and connect it to another Proxy

14. On the server where the new Proxy will be installed, import the Proxy self-signed certificate that was previously exported: Import a security certificate. After importing a certificate, close any open browsers to ensure that the certificate is applied to your browsing session.
15. Ensure that the connection to the existing Proxy is secure by navigating to `https://<ExistingProxyMachineName>/Proxy` in your web browser.
    If the connection is secure, the Proxy UI will appear – proceed to the next step. If the connection is not secure, a warning will display in your browser – complete the certificate export-import process again.
16. Install the Proxy.

17. Ensure the new Proxy is running properly by navigating to `https://<NewProxyMachineName>/Proxy` in your web browser.
    The Proxy UI will appear, indicating the Proxy is running.
18. Export the Proxy self-signed certificate bound to port 443 (configurable default) in IIS: Export a security certificate.
19. Configure the new Proxy. You must change the routing table of this Proxy to route incoming requests to point to the next Proxy. In the Proxy user interface, modify the destination route to `https://<ProxyDestinationIP>/Proxy/ConnectorService/API` as described in Configure the Proxy.

Install a Data Collector and connect it to a Connector Service

Note
Multiple Data Collectors can connect to a single Connector Service

20. On the server where the Data Collector will be installed, import the Connector Service self-signed certificate that was previously exported: Import a security certificate. After importing a certificate, close any open browsers to ensure that the certificate is applied to your browsing session.
21. Ensure that the connection to the Connector Service is secure by navigating to `https://<ConnectorServiceMachineName>/ConnectorService` in your web browser.
    If the connection is secure, `Connector Service` will display in the top left corner of the web page – proceed to the next step. If the connection is not secure, a warning will display in your browser – complete the certificate export-import process again.
22. Run the Data Collector installer.

Install a Data Collector and connect it to a Proxy

23. On the server where the Data Collector will be installed, import the Proxy self-signed certificate that was previously exported: Import a security certificate. After importing a certificate, close any open browsers to ensure that the certificate is applied to your browsing session.
24. Ensure that the connection to the Proxy is secure by navigating to `https://<ProxyMachineName>/Proxy` in your web browser.
    If the connection is secure, the Proxy UI will appear – proceed to the next step. If the connection is not secure, a warning will display in your browser – complete the certificate export-import process again.
25. Run the Data Collector installer. When prompted for the Connector Service IP address or PC name, enter the IP address or PC name of the Proxy.

2.5 Completing post-installation steps

Next, complete some configuration and setup changes before wrapping up your Plantweb Optics installation.

Procedure

1. Make post-installation configuration changes. These may include:
    a) Configure Active Directory for Plantweb Optics. See Configure Active Directory for Plantweb Optics.

   b) Configure Plantweb Optics OIDC settings. See Configure Plantweb Optics OIDC settings.
   c) Configure the AMS Device Manager ASI. See Opt-In to Device Parameters.

2. Install certificates. See Install certificates.
3. Launch Asset Explorer and select **Add Emerson Wireless Gateway Asset Source** (1420 Wireless Gateway). See Launch Plantweb Optics.
4. Launch Asset Explorer and select **Add AMS Machinery Manager ASI Asset Source** to the Plantweb Optics server. See Launch Plantweb Optics.
5. Launch Asset Explorer and select **Add Plantweb Insight Asset Source** using IP Address or Machine Name. See Launch Plantweb Optics.
6. Run OPC Client (UaExpert) and select **Connect to OPC Server**. See Connect to OPC server.

Congratulations, you are now ready to start using Plantweb Optics.

3 Planning your system

Plantweb Optics is comprised of different components, and each component has its own installation that may be deployed on separate computers. Deployment depends on your network requirements and setup.

Before you install any of the system components, plan your installation using the system requirements, recommended system deployment scenarios, and the guidelines provided in this chapter.

After designing and planning your system, return to Step 1 of the *Preparing for installation* topic and continue your installation.

3.1 Guidelines for planning your system

Procedure

1. Determine the data that you want to bring into Plantweb Optics.

   Data can be brought in by the installation of asset source interfaces (ASIs). See page 18.

2. Evaluate the systems and assets that you want to integrate into Plantweb Optics.
   a) Check if these systems are compatible with Plantweb Optics. See page 217.
   b) Check the number of assets, databases, and parameters in the system. See page 37.

3. Determine your network setup.

   Your network setup affects the deployment of the Plantweb Optics components. See page 19.

4. Determine any network architecture restrictions in your network.

   Your network architecture affects whether you can receive messages outside of your plant's network or not. See page 172 and page 39.

5. Determine your database requirements.

   The Plantweb Optics database can either reside on the Plantweb Optics server (Tier-1) or on a separate server (Tier-2). See page 29.

6. Check the system requirements and system capacity recommendations. See page 31 and page 37.
7. Check IIS requirements. See page 31.
8. Plan to integrate security certificate installation with software installation. See page 42.
9. Ensure any systems you plan to interface with Plantweb Optics are ready.
   a) Before interfacing with AMS Machinery Manager databases, see page 59 for important instructions for the system administrator.

10. Determine if you need to read data from Plantweb Optics using an OPC UA client.

    There are prerequisites in Asset Explorer before installation. See page 116.

3.2 System components

Plantweb Optics must be installed on a computer with a server-class operating system. Typically, an ASI installation consists of two parts, installation of the Web Application and the Service. The Web Applications are recommended to be deployed on a separate server referred to as the ASI server station.

Client stations access Plantweb Optics utilities from a web browser. They are optionally installed with AMS Machinery Manager Launcher and AMS Device Manager Launcher.

On a mobile device, the Plantweb Optics Mobile App can be installed to enable users to send and receive alerts from a mobile device.

Plantweb Optics is comprised of many components, described in the table below.

Tip
Follow the recommended installation and setup order on page 11.

Table 3-1: System components

Component	Description
Plantweb Optics Web Services	The main software application. Plantweb Optics is always installed on the Plantweb Optics server. **Note** Install Plantweb Optics Historian and then Plantweb Optics Web Services before installing and integrating all other system components. This is a prerequisite to all other component installations.
Connector Service	Facilitates communication between Plantweb Optics and Data Collectors.
Proxy	Provides secure communication between Data Collectors and the Connector Service across an arbitrary number of networks.
Data Collector	Gathers data, such as parameter values, asset health, and events, from a configured asset source to provide to Plantweb Optics. Data Collector ASIs: • AMS Asset Monitor • AMS Device Manager • DeltaV Control Loop • KNet
Computerized Maintenance Management System (CMMS) Interface	Allows you to work with other applications, such as IBM's Maximo or SAP's Plant Maintenance Module, to keep track of assets, schedule and track maintenance tasks, and keep records of the maintenance tasks.
Plantweb Optics Historian	Allows you to view the assets' historical data so that you can analyze trends in the data.

Table 3-1: System components *(continued)*

Component	Description
Plantweb Optics OPC UA server	Allows you to read Plantweb Optics data from an OPC UA client.
Emerson Wireless Gateway ASI	Allows you to connect and display information from an Emerson Wireless Gateway and from devices on the gateway.
AMS Machinery Manager ASI	Allows you to bring AMS Machinery Manager alerts, data, KPIs, and hierarchy into Plantweb Optics. The AMS Machinery Manager ASI has two components: the Service and the Web Application (Web App).
Plantweb Insight ASI	Allows you to connect and display analytics from Plantweb Insight assets.
AMS Device Manager Launcher	Launches AMS Device Manager in context from the Asset Explorer utility when AMS Device Manager is installed on the computer. AMS Device Manager Launcher must only be installed on an AMS Device Manager client station.
AMS Machinery Manager Launcher	Launches AMS Machinery Manager in context from the Asset Explorer utility when AMS Machinery Manager is installed on the computer. AMS Machinery Manager Launcher must only be installed on a computer where an AMS Machinery Manager client is installed.
Plantweb Optics Mobile App	Allows you to display, send, and receive Plantweb Optics messages and notifications from your mobile device. Install this on your mobile device.

Important

Emerson recommends installing only the components you are licensed to use.

If you install nonessential components, it will unnecessarily use system resources.

3.3 Deployment scenarios

When determining the type of deployment, equipment, and components for your system, Emerson recommends these guidelines for performance and scalability:

- Use recommended hardware.
- Use a separate ASI server.
- Install only the components you need.
- Use server-class operating systems.

3.3.1 Scenario 1: Two-server setup deployed on four levels

Emerson recommends using a two-server setup for best system performance and high system capacity.

In this deployment, the Plantweb Optics Server is located on Level 4 and the ASI server is located on Level 3. Note that components such as SQL Server 2017 Express, OPC UA Server, NLINK Server, and Plantweb Optics Historian are co-deployed with Plantweb Optics Server. However, these components can be deployed in a separate machine depending on the overall system asset count or load. The system diagram and certificate installation notes are shown below.

Figure 3-1: Scenario 1: Two-server setup deployed on four levels

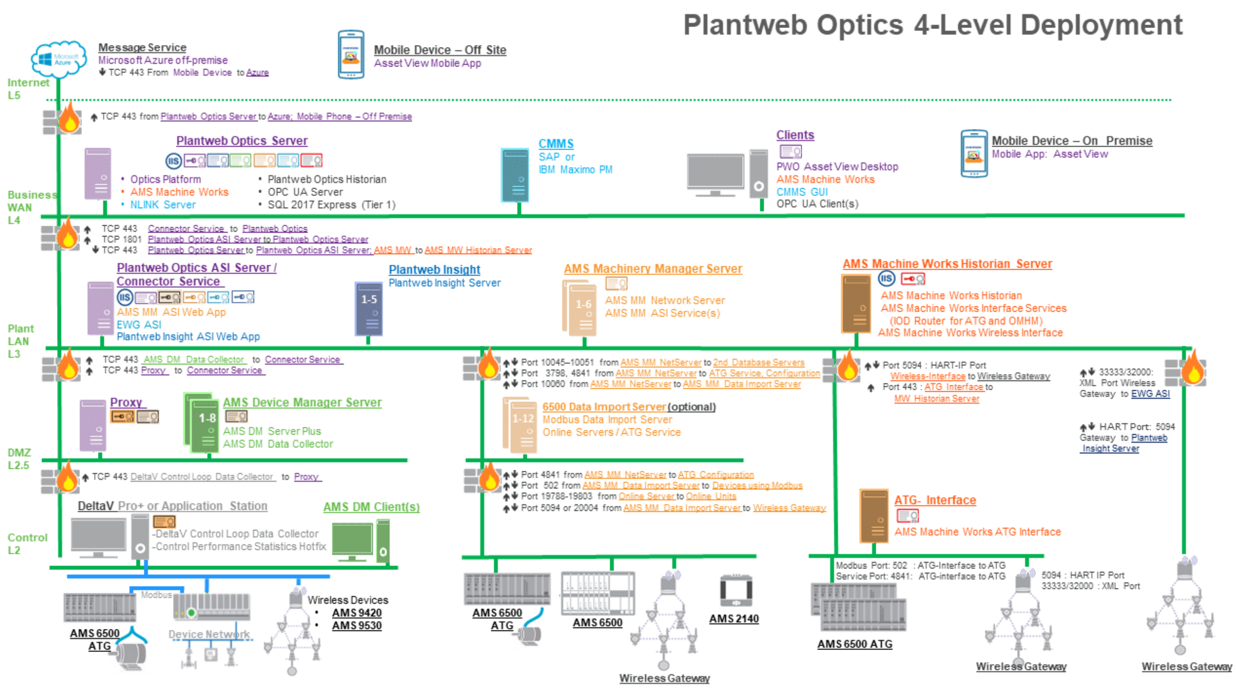


Table 3-2: Scenario 1: Two-server setup deployed on four levels

Station	Component	Certificate installation notes
Message Service	Microsoft Azure off premises	None.
Mobile Device – Off Site	Asset View Mobile Application	None. **Note** You can deploy mobile devices either on premises or off-site, but not both.
Plantweb Optics Server	Plantweb Optics AMS Machine Works NLINK Server Plantweb Optics Historian OPC UA Server SQL 2017 Express	Plantweb Optics server certificate with private key is automatically generated during software installation. Plantweb Insight ASI certificate allows communication to Plantweb Insight ASI. Install from a file. AMS Device Manager ASI certificate allows communication to AMS Device Manager ASI. Install from a file. AMS Machinery Manager ASI certificate allows communication to AMS Machinery Manager ASI. Install from a file. Emerson Wireless Gateway ASI certificate allows communication to Emerson Wireless Gateway ASI. Install from a file. AMS Machine Works certificate allows communication to AMS Machine Works. Install from a file.

Table 3-2: Scenario 1: Two-server setup deployed on four levels *(continued)*

Station	Component	Certificate installation notes
CMMS	SAP IBM Maximo PM	None.
Clients	Plantweb Optics Asset View Desktop AMS Machine Works Vibration Analyzer CMMS GUI OPC UA Client(s)	Plantweb Optics server certificate allows communication to Plantweb Optics. Install from a web browser.
Mobile Device – On Premises	Mobile Application: Asset View	None. **Note** You can deploy mobile devices either on premises or off-site, but not both.
Plantweb Optics ASI Server/ Connector Service	Connector Service AMS Machinery Manager ASI Web Application Emerson Wireless Gateway ASI Plantweb Insight ASI Web App	Plantweb Optics server certificate allows communication to Plantweb Optics. Install from a web browser. AMS Machinery Manager ASI certificate with private key is generated during ASI installation. Emerson Wireless Gateway ASI certificate with private key is generated during ASI installation. Plantweb Insight ASI certificate allows communication to Plantweb Insight ASI. Install from a file.
Plantweb Insight	Plantweb Insight	None.
AMS Machinery Manager Server	AMS Machinery Manager Network Server AMS Machinery Manager ASI Service(s)	Plantweb Optics server certificate allows communication to Plantweb Optics. Install from a web browser. AMS Machinery Manager ASI certificate allows communication to AMS Machinery Manager ASI. Install from a file.
AMS Machine Works Historian Server	AMS Machine Works Historian AMS Machine Works Interface Services (Interface Router for ATG and OMHM) AMS Machine Works Wireless Interface	None. AMS Machine Works certificate with private key is generated during ASI installation. Install from a file.
AMS Device Manager Server	AMS Device Manager AMS Device Manager Data Collector	Data Collector certificate with private key is generated during Data Collector installation. No action required. Connector Service certificate allows communication to Connector Service. Install from a file.
6500 Data Import Server (optional)	Modbus Data Import Server Online Servers/ATG Service	None.
ATG Interface	AMS Machine Works ATG Interface	AMS Machine Works certificate allows communication to AMS Machine Works. Install from a file. **Note** The ATG Interface server typically does not require the Plantweb Optics certificate since it does not communicate directly with any aspect of Plantweb Optics. However, if the ATG Machine Works Wireless Interface is on the same server, then it does require the Plantweb Optics certificate.

Table 3-2: Scenario 1: Two-server setup deployed on four levels *(continued)*

Station	Component	Certificate installation notes
AMS Device Manager Client(s)	None.	None.
DeltaV Pro+ or Application Station	DeltaV Control Loop Data Collector Control Performance Statistics Hotifx (Pro+ only)	Data Collector certificate with private key is generated during Data Collector installation. No action required. Proxy certificate allows communication to the Connector Service. Install from a file.
Proxy Server	Data Collector Proxy	Connector Service certificate allows communication to Connector Service. Install from a file.

3.3.2 Scenario 2: Two-server setup deployed on three levels

In this deployment, the Plantweb Optics Server is on network Level 4 and the ASI server is located on network Level 3. Note that components such as SQL Server 2017 Express, OPC UA Server, NLINK Server, and Plantweb Optics Historian are co-deployed with Plantweb Optics Server. However, they can be deployed in a separate machine depending on the overall system asset count or load. The system diagram and certificate installation notes are shown below.

Figure 3-2: Scenario 2: Two-server setup deployed on three levels

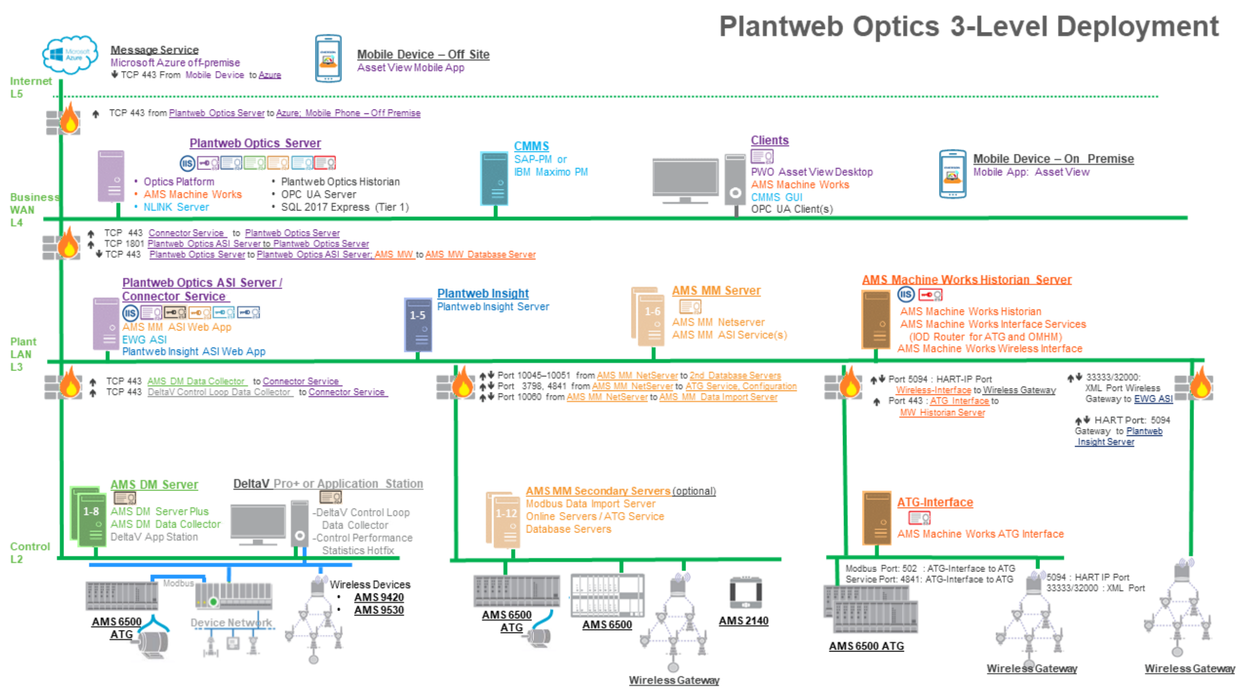


Table 3-3: Scenario 2: Two-server setup deployed on three levels

Station	Component	Certificate installation notes
Message Service	Microsoft Azure off premises	None.
Mobile Device – Off Site	Asset View Mobile Application	None. **Note** You can deploy mobile devices either on premises or off-site, but not both.
Plantweb Optics Server	Plantweb Optics AMS Machine Works NLINK Server Plantweb Optics Historian OPC UA Server SQL 2017 Express	Plantweb Optics server certificate with private key is automatically generated during software installation. Plantweb Insight ASI certificate allows communication to Plantweb Insight ASI. Install from a file. AMS Machinery Manager ASI certificate allows communication to AMS Machinery Manager ASI. Install from a file. Emerson Wireless Gateway ASI certificate allows communication to Emerson Wireless Gateway ASI. Install from a file. AMS Machine Works certificate allows communication to AMS Machine Works. Install from a file.
CMMS	SAP IBM Maximo PM	Plantweb Optics server certificate allows communication to Plantweb Optics. Install from a web browser.
Clients	Plantweb Optics Asset View Desktop AMS Machine Works Vibration Analyzer CMMS GUI OPC UA Client(s)	Plantweb Optics server certificate allows communication to Plantweb Optics. Install from a web browser.
Mobile Device – On Premises	Mobile Application: Asset View	None. **Note** You can deploy mobile devices either on premises or off-site, but not both.
Plantweb Optics ASI Server/ Connector Service	AMS Machinery Manager ASI Web Application Emerson Wireless Gateway ASI Plantweb Insight ASI Web App Connector Service	Plantweb Optics server certificate allows communication to Plantweb Optics. Install from a web browser. AMS Machinery Manager ASI certificate with private key is generated during ASI installation. Emerson Wireless Gateway ASI certificate with private key is generated during ASI installation. Plantweb Insight ASI certificate allows communication to Plantweb Insight ASI. Install from a file.
Plantweb Insight	Plantweb Insight	None.
AMS Machinery Manager Server	AMS Machinery Manager Network Server AMS Machinery Manager ASI Service(s)	None. AMS Machinery Manager ASI certificate allows communication to AMS Machinery Manager ASI. Install from a file.
AMS Machine Works Historian Server	AMS Machine Works Historian AMS Machine Works Interface Services (Interface Router for ATG and OMHM) AMS Machine Works Wireless Interface	AMS Machine Works certificate with private key is generated during ASI installation. Install from a file.

Table 3-3: Scenario 2: Two-server setup deployed on three levels *(continued)*

Station	Component	Certificate installation notes
AMS Device Manager Server	AMS Device Manager AMS Device Manager Data Collector DeltaV App Station	Data Collector certificate with private key is generated during Data Collector installation. No action required. Connector Service certificate allows communication to Connector Service. Install from a file.
AMS Machinery Manager Secondary Servers (optional)	Modbus Data Import Server Online Servers/ATG Service Database Servers	None.
ATG- Interface	AMS Machine Works ATG Interface	AMS Machine Works certificate allows communication to AMS Machine Works. Install from a file. **Note** The ATG Interface server does not require the Plantweb Optics certificate since it does not communicate directly with any aspect of Plantweb Optics. However, there is one exception to this. If the ATG Machine Works Wireless Interface is on the same server, then it does require the Plantweb Optics certificate.
DeltaV Pro+ or Application Station	DeltaV Control Loop Data Collector Control Performance Statistics Hotifx (Pro+ only)	Data Collector certificate with private key is generated during Data Collector installation. No action required. Connector Service certificate allows communication to the Connector Service. Install from a file.

3.3.3 Scenario 3: One-server setup deployed on three levels

In this deployment, Plantweb Optics and one or more ASIs are installed on one server on Level 3. When using only one server, ensure it has a server-class operating system and the recommended hardware specified in the system requirements. The system diagram and certificate installation notes are shown below.

Figure 3-3: Scenario 3: One-server setup deployed on three levels

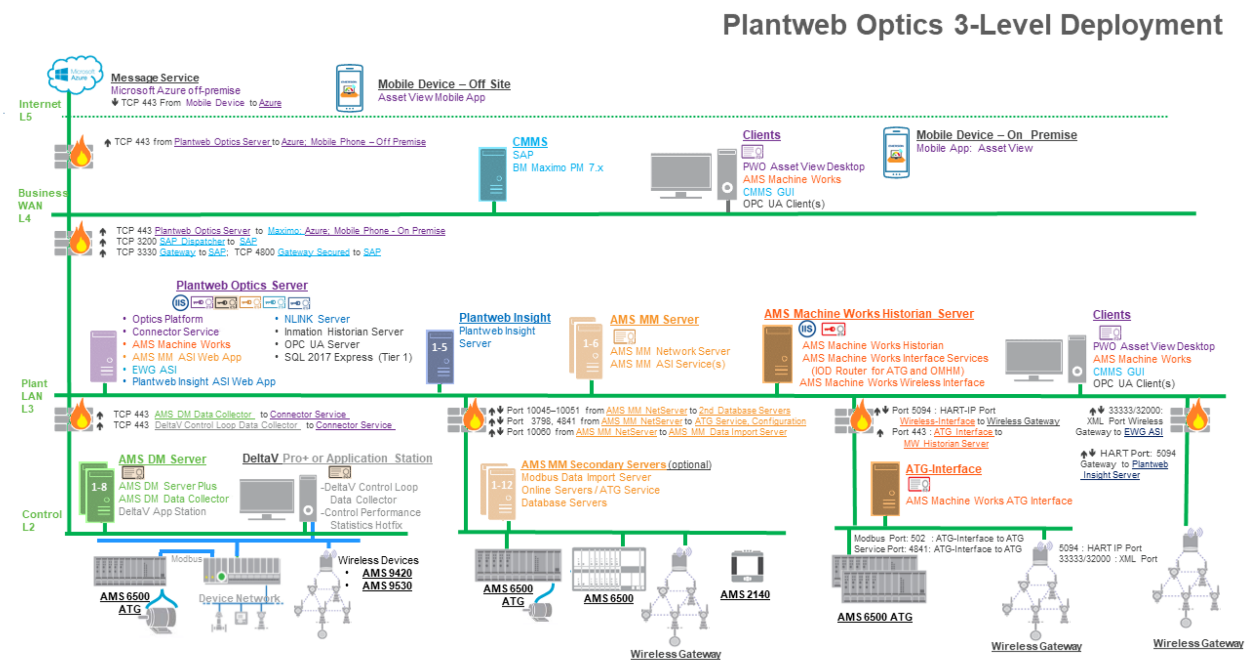


Table 3-4: Scenario 3: One-server setup deployed on three levels

Station	Component	Certificate installation notes
Message Service	Microsoft Azure off premises	None.
Mobile Device – Off Site	Asset View Mobile Application	None. **Note** You can deploy mobile devices either on premises or off-site, but not both.
CMMS	SAP IBM Maximo PM	None.
Clients	Plantweb Optics Asset View Desktop AMS Machine Works CMMS GUI OPC UA Client(s)	Plantweb Optics server certificate allows communication to Plantweb Optics. Install from a web browser.
Mobile Device – On Premises	Mobile Application: Asset View	None. **Note** You can deploy mobile devices either on premises or off-site, but not both.

Table 3-4: Scenario 3: One-server setup deployed on three levels *(continued)*

Station	Component	Certificate installation notes
Plantweb Optics Server	Plantweb Optics AMS Machine Works AMS Machinery Manager ASI Web Application Emerson Wireless Gateway ASI Plantweb Insight ASI Web App NLINK Server Inmation Historian Server OPC UA Server SQL 2017 Express Connector Service	Plantweb Optics server certificate with private key is automatically generated during software installation. AMS Machinery Manager ASI certificate allows communication to AMS Machinery Manager ASI. Install from a file. Emerson Wireless Gateway ASI certificate allows communication to Emerson Wireless Gateway ASI. Install from a file. Plantweb Insight ASI certificate allows communication to Plantweb Insight ASI. Install from a file.
Plantweb Insight	Plantweb Insight Server	None.
AMS Machinery Manager Server	AMS Machinery Manager Network Server AMS Machinery Manager ASI Service(s)	AMS Machinery Manager ASI certificate allows communication to AMS Machinery Manager ASI. Install from a file.
AMS Machine Works Historian Server	AMS Machine Works Historian AMS Machine Works Interface Services (IOD Router for ATG and OMHM) AMS Machine Works Wireless Interface	AMS Machine Works certificate with private key is generated during ASI installation. Install from a file.
Clients	Plantweb Optics Asset View Desktop AMS Machine Works CMMS GUI OPC UA Client(s)	Plantweb Optics server certificate allows communication to Plantweb Optics. Install from a web browser.
AMS Device Manager Server	AMS Device Manager Server AMS Device Manager Data Collector	Data Collector certificate with private key is generated during Data Collector installation. No action required. Connector Service certificate allows communication to the Connector Service. Install from a file.
AMS Machinery Manager Secondary (optional)	Modbus Data Import Server Online Servers/ATG Service Database Servers	None.
ATG Interface	AMS Machine Works ATG Interface	AMS Machine Works certificate allows communication to AMS Machine Works. Install from a file. **Note** The ATG Interface server does not require the Plantweb Optics certificate because it does not communicate directly with any aspect of Plantweb Optics. However, there is one exception to this. If the ATG Machine Works Wireless Interface is on the same server, then it does require the Plantweb Optics certificate.

Table 3-4: Scenario 3: One-server setup deployed on three levels *(continued)*

Station	Component	Certificate installation notes
DeltaV Pro+ or Application Station	DeltaV Control Loop Data Collector	Data Collector certificate with private key is generated during Data Collector installation. No action required.
	Control Performance Statistics Hotifx (Pro+ only)	Connector Service certificate allows communication to the Connector Service. Install from a file.

3.3.4 Scenario 4: One-server setup deployed on two levels

In this deployment, the Plantweb Optics server is installed on network Level 3 and one or more ASIs are installed on network Level 2. When using only one server, ensure it has a server-class operating system and the recommended hardware specified in the system requirements. The system diagram and certificate installation notes are shown below.

Figure 3-4: Scenario 4: One-server setup deployed on two levels

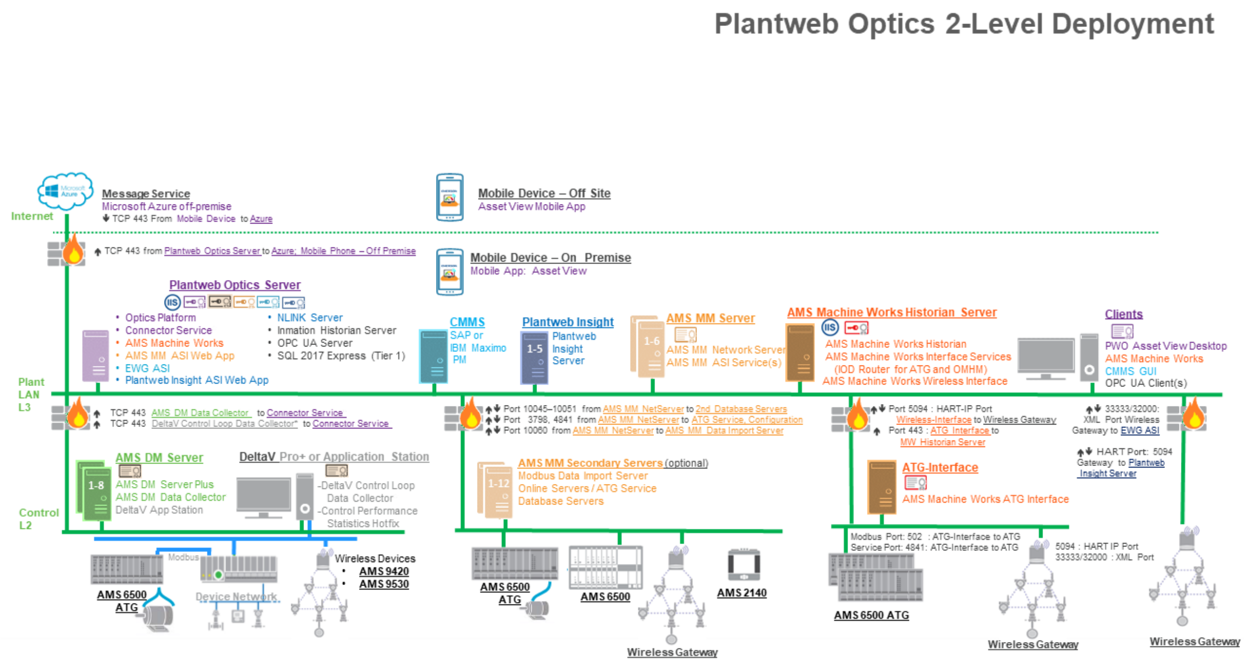


Table 3-5: Scenario 4: One-server setup deployed on two levels

Station	Component	Certificate installation notes
Message Service	Microsoft Azure off premises	None.
Mobile Device – Off Site	Asset View Mobile Application	None. **Note** You can deploy mobile devices either on premises or off-site, but not both.
CMMS	SAP IBM Maximo PM	Plantweb Optics server certificate allows communication to Plantweb Optics. Install from a web browser.
Clients	Plantweb Optics Asset View Desktop CMMS GUI OPC UA Client(s)	Plantweb Optics server certificate allows communication to Plantweb Optics. Install from a web browser.
Mobile Device – On Premises	Mobile Application: Asset View	None. **Note** You can deploy mobile devices either on premises or off-site, but not both.

Table 3-5: Scenario 4: One-server setup deployed on two levels *(continued)*

Station	Component	Certificate installation notes
Plantweb Optics Server	Plantweb Optics AMS Machine Works AMS Machinery Manager ASI Web Application Emerson Wireless Gateway ASI Plantweb Insight ASI Web App NLINK Server Inmation Historian Server OPC UA Server SQL 2017 Express Connector Service	Plantweb Optics server certificate with private key is automatically generated during software installation. AMS Device Manager ASI certificate allows communication to AMS Device Manager ASI. Install from a file. AMS Machinery Manager ASI certificate allows communication to AMS Machinery Manager ASI. Install from a file. Emerson Wireless Gateway ASI certificate allows communication to Emerson Wireless Gateway ASI. Install from a file. Plantweb Insight ASI certificate allows communication to Plantweb Insight ASI. Install from a file.
Plantweb Insight	Plantweb Insight	Plantweb Optics server certificate allows communication to Plantweb Optics. Install from a web browser. Plantweb Insight ASI certificate allows communication to Plantweb Insight ASI. Install from a file.
AMS Device Manager Server	AMS Device Manager Server AMS Device Manager Data Collector	Data Collector certificate with private key is generated during Data Collector installation. No action required. Connector Service certificate allows communication to the Connector Service. Install from a file.
AMS Machinery Manager Server	AMS Machinery Manager Network Server AMS Machinery Manager ASI Service(s)	Plantweb Optics server certificate allows communication to Plantweb Optics. Install from a web browser. AMS Machinery Manager ASI certificate allows communication to AMS Machinery Manager ASI. Install from a file.
AMS Machine Works Historian Server	AMS Machine Works Historian AMS Machine Works Interface Services AMS Machine Works Wireless Interface AMS ATG-interface	Plantweb Optics server certificate allows communication to Plantweb Optics. Install from a web browser. AMS Machine Works certificate with private key is generated during ASI installation. Install from a file.
Clients	Plantweb Optics Asset View Desktop AMS Machine Works CMMS GUI OPC UA Client(s)	Plantweb Optics server certificate allows communication to Plantweb Optics. Install from a web browser.
DeltaV Pro+ or Application Station	DeltaV Control Loop Data Collector Control Performance Statistics Hotifx	Data Collector certificate with private key is generated during Data Collector installation. No action required. Connector Service certificate allows communication to the Connector Service. Install from a file.

3.4 Database deployment

During installation, the system databases are configured and the user performing the installation is set up as the SQL database administrator.

By default, the user installing the software is set up as the SQL administrator for the EmersonCSI instance. As a best practice, immediately after installation, work with your IT department to add a second SQL administrator for the EmersonCSI instance. If there is only one administrator, and their Windows account becomes deactivated, it will not be possible to perform maintenance or make changes to the database instance.

The two database installation choices are described in the sections below.

Tier-1 installation

In a Tier 1 installation, the databases are deployed on the same server as the software and Microsoft SQL Server 2017 Express is automatically during installation. Tier-1 is the default configuration and represents the typical network server system. Automatic backup processing is available for this installation. See page 198 for more information.

- Check Windows Programs and Features to verify that Microsoft SQL Server is not currently installed. During default installation, Microsoft SQL Server 2017 Express is automatically installed and configured for Plantweb Optics.

Note
There is a 10 GB database limit on Microsoft SQL Server 2017 Express. Consider this limitation when deciding your database setup.

- The EmersonCSI named instance is automatically created with the Plantweb Optics installation when there is no existing Microsoft SQL Server installation.
- If Microsoft SQL Server is currently installed, create the EmersonCSI named instance before beginning the Plantweb Optics installation. The user installing Plantweb Optics should be a system administrator for the EmersonCSI named instance.
- The EmersonCSI named instance needs to be set up for mixed authentication—Windows and SQL accounts.
- If you are manually installing SQL Server 2017 Express, make sure the account running the SQL Server setup has rights to back up files and directories, rights to manage auditing and security log, and rights to debug programs. See Troubleshooting.

Tier-2 installation

In a Tier 2 installation, the databases are deployed on a separate server where Microsoft SQL Server 2017 is already installed. A Tier-2 installation requires specific server configuration and database management by a database administrator. Automatic backup processing is not available for this installation; the database, including backups, should be managed by a database administrator. See page 205 for more information.

- The database must be Microsoft SQL Server 2017.
- Create the EmersonCSI named instance before beginning the Plantweb Optics installation. The user installing Plantweb Optics should be a system administrator for the EmersonCSI named instance.
- The EmersonCSI named instance needs to be set up for mixed authentication—Windows and SQL accounts.
- Enable TCP/IP protocol for EmersonCSI SQL Server Network Configuration.
- Ensure the SQL Browser service is running and set it to auto-start.

3.5 Internet Information Services (IIS)

- During default installation, IIS is automatically installed and configured to use the Default Site (port 80 and 443).
- If port 80 and 443 are already in use by a previous installation of IIS, you can delete the Default Site (if unused) or configure it to use other ports. See page 199 for instructions.
- You can also use non-default ports if your existing system and network requires it. Your network administrator must configure firewall rules to allow traffic to pass through the non-default ports. It is best practice to use ports above 1024 and to use non-restricted ports.

3.6 System requirements

After ensuring that all of the following system requirements are met, return to Step 2 of the *Preparing for installation* topic and continue your installation.

Plantweb Optics server requirements

Operating system	Windows Server 2016 Datacenter Windows Server 2016 Standard Windows Server 2012 R2 Datacenter Windows Server 2012 R2 Standard
CPU architecture	64-bit
Internet Information Services (IIS)	v8.5, v10 (supplied with OS)
Microsoft SQL Server	MS SQL Server 2017 (recommended) MS SQL Server 2017 Express Edition (supported)
Browsers	Google Chrome (latest version) Internet Explorer v11 or later (supported)
Processor	3.2 GHz, 8-core processor, Intel Xeon-scalable (Gold) or faster (recommended) 2.4 GHz, 4-core processor, Intel Xeon-scalable (Gold) or faster (minimum)
Memory	32 GB (recommended) 16 GB (minimum)
Hard drive	SSD hard drive (recommended) SAS hard drive (10K RPM) (minimum)
Available disk space	100 GB (minimum)
Screen resolution	Full HD (1920 x 1080 pixels) (maximum) SXGA (1280 x 1024 pixels) (minimum)
Network	2 x 1 GB NIC (use 2 NICs to isolate Tier 3 traffic from Tier 2 traffic) (recommended) 1 x 1 GB NIC (supported)

Inmation Historian/OPC UA Server Station

Operating system	Windows Server 2016 Datacenter Windows Server 2016 Standard Windows Server 2012 R2 Datacenter Windows Server 2012 R2 Standard
CPU architecture	64-bit
Internet Information Services (IIS)	v8.5, v10 (supplied with OS)
Microsoft SQL Server	MS SQL Server 2017 Express Edition
Browsers	Google Chrome (latest version) Internet Explorer v11 or later (supported)
Processor	2.4 GHz, 4-core processor, Intel Xeon-scalable (Gold) or faster
Memory	32 GB (recommended)
Hard drive	SAS hard drive (10K RPM)
Available disk space	100 GB (minimum)
Screen resolution	Full HD (1920 x 1080 pixels) (maximum) SXGA (1280 x 1024 pixels) (minimum)
Network	2 x 1 GB NIC (use 2 NICs to isolate Tier 3 traffic from Tier 2 traffic) (recommended) 1 x 1 GB NIC (supported)

NLINK Server

Operating system	Windows 10 Pro Windows Server 2016 Datacenter Windows Server 2016 Standard Windows Server 2012 R2 Datacenter Windows Server 2012 R2 Standard
CPU architecture	64-bit
Internet Information Services (IIS)	v8.5, v10 (supplied with OS)
Microsoft SQL Server	MS SQL Server 2017 Express Edition
Browsers	Google Chrome (latest version) Internet Explorer v11 or later (supported)
Processor	2.2 GHz, 4-core processor, Intel Xeon-scalable or faster
Memory	4 GB
Hard drive	SAS hard drive (10K RPM)
Available disk space	100 GB
Screen resolution	Full HD (1920 x 1080 pixels) (maximum) SXGA (1280 x 1024 pixels) (minimum)

Network	1 x 1 GB NIC

Plantweb Optics Client Station

Operating system	Windows Server 2016 Standard Windows Server 2012 R2 Standard Windows 10 Pro
CPU architecture	64-bit
Processor	2.2 GHz, 4-core processor Intel Xeon, Intel Core i5 6th Gen (i5 6400T) or better
Memory	4 GB
Hard drive	SAS hard drive (10K RPM)
Available disk space	100 GB
Browsers	Google Chrome (latest version) Internet Explorer v11 or later (supported)
Screen resolution	4K UHD (3840 x 2160 pixels) (maximum) SXGA (1280 x 1024 pixels) (minimum)

OPC UA Client Station

Operating system	Windows Server 2016 Standard Windows Server 2012 R2 Standard Windows 10 Pro
CPU architecture	64-bit
Processor	2.2 GHz, 4-core processor Intel Xeon, Intel Core i5 6th Gen (i5 6400T) or better
Memory	4 GB
Hard drive	SAS hard drive (10K RPM)
Available disk space	100 GB
Browsers	Google Chrome (latest version) Internet Explorer v11 or later (supported)
Screen resolution	4K UHD (3840 x 2160 pixels) (maximum) SXGA (1280 x 1024 pixels) (minimum)
Third party applications	OPC UA Experts Integration Objects Prosys

Proxy or Connector Service Requirements

Operating system	Windows Server 2016 Datacenter Windows Server 2016 Standard Windows Server 2012 R2 Datacenter Windows Server 2012 R2 Standard Windows 10 Pro Windows 10 Enterprise Windows 10 IoT Enterprise 2016 LTSB (64-bit)
CPU architecture	x64
Processor	2.4 GHz, 4-core processor or faster
Memory	16 GB (recommended) 8 GB (minimum)
Hard Drive	SAS Hard Drive (10K RPM)
Available disk space	100 GB
Internet Information Services (IIS)	v8.5, v10 (supplied with OS)
Network	1 x 1GB NIC

ASI server requirements

Operating system	Windows Server 2016 Standard Windows Server 2012 R2 Standard
CPU architecture	x64
Processor	2.4 GHz, 4-core processor or faster
Memory	16 GB (recommended) 8 GB (minimum)
Available disk space	150 GB

Additional specifications

Ethernet	One or more Ethernet ports
Internet connectivity	An internet connection is required to download installations and patches, register software, and receive alerts and messages on the mobile application.
Supported virtualization	• VMware 6 • Hyper-V 2012
Software	Microsoft .NET 3.5, SP1 Microsoft .NET Framework 3.5 is required to install Plantweb Optics. See KBA NK-1600-0300 for instructions.

Supported antivirus software	• Symantec™ Endpoint Protection • McAfee™ Endpoint • Norton™ Security with Backup

Notes

Computers with Plantweb Optics components installed must have:

- system clocks synchronized.
- date/time in the same 12-hr or 24-hr format.

System clock discrepancies can block communication. (Many third-party tools are available to synchronize system clocks.) System clocks do not need to be synchronized for Mobile applications or PCs with browser-only access.

Anti-virus exclusion list

To optimize performance, it is recommended to exclude the following applications, files, and extensions in the anti-virus software.

Component	Item	Path (default locations)
Optics Web	Applications (*.exe)	C:\Windows\System32\inetsrv\w3wp.exe C:\Windows\SysWOW64\inetsrv\w3wp.exe
	Program Files	C:\EMERSONCSI* C:\Program Files (x86)\Emerson* C:\inetpub\wwwroot\EmersonCSI*
	Log files	C:\inetpub\wwwroot\EmersonCSI\Logs* C:\inetpub\wwwroot\EmersonCSI\WebLogs*
	Cachecow	C:\Windows\Temp\ARES\Cache*
SQL	Applications (*.exe)	C:\Program Files\Microsoft SQL Server \MSSQL14.EMERSONCSI\MSSQL\Binn\sqlservr.exe
	Program Files	C:\Program Files (x86)\Microsoft SQL Server* C:\Program Files\Microsoft SQL Server*
Inmation	Applications (*.exe)	C:\inmation.root\bin\inmation.exe C:\inmation.root\webapi\inmationWebAPI.exe C:\inmation.root\MongoDB\bin\mongod.exe C:\inmation.root\MongoDB\bin\mongo.exe
	Program files	C:\inmation.root*
Junot (NLINK)	Applications (*.exe)	C:\Program Files\Junot Systems\NLINK Modules\NLINK Management Module.exe C:\Program Files\Junot Systems\NLINK Server\NLINK.exe
	Program files	C:\Program Files\Junot Systems*

Component	Item	Path (default locations)
OPC UA	Applications (*.exe)	C:\Program Files (x86)\Emerson\Plantweb Optics OPC UA Server\OPCUA\Emerson.Opc.Ua.Server.exe C:\Program Files (x86)\Emerson\Plantweb Optics OPC UA Server\OPCUA\sqlite3.exe C:\Program Files (x86)\Emerson\Plantweb Optics OPC UA Server\OPCUA\Emerson.OPC.UA.Server.Tool.exe
	Program files	C:\Program Files (x86)\Emerson\Plantweb Optics OPC UA Server\
File extensions	File extensions	bak, bcp, c, cft, chk, cmtx, csv, dll, dri, edb, idx, jrs, ldf, log, mdf, ndf, obj, out, pdb, pol, prc, pre, sch, sql, sqlaudit, sdb, trc, trg, trn, xel, xem, xml
AMS MM ASI IO Interface	Applications (*.exe)	C:\RBMNET\RBMsuite\sys\ IOService\ Emerson.CSI.MMASI.IOService.exe
Windows	Windows exclusion for Windows Update	C:\Windows\SoftwareDistribution\DataStore* C:\Windows\System32\GroupPolicy\User* C:\Windows\System32\GroupPolicy\Machine*

Mobile client requirements

iOS	iOS 11.3 or later with Safari
Android	8.0 (Oreo) or later with Chrome
Memory	2 GB (minimum)
Internal memory	64 GB
Screen resolution	750 x 1334 pixels (minimum) 1440 x 2960 pixels (maximum)
Communications	WLAN—802.11 a/b/g/n/ac
Network	4G network or higher

Tablet client requirements

iOS	iOS 11.3 or later with Safari
Android	8.0 (Oreo) or later with Chrome
Memory	2 GB (minimum)
Internal memory	64 GB
Screen resolution	1668 x 2224 1536 x 2048
Communications	WLAN—802.11 a/b/g/n/ac
Network	4G network or higher

3.7 System scalability

The system is scalable, supporting up to the following maximums based on the system components, deployment type, hardware, and operating system specifications. Use the tables below as a guide to help you select the best server setup for your expected system scale.

Table 3-6: Plantweb Optics scalability

Components	Setup 1: Three-server setup recommended hardware	Setup 2: Two-server setup recommended hardware
Server specifications	Plantweb Optics server ASI server/Connector Service Plantweb Optics Historian Server, OPC UA Server	Plantweb Optics server ASI server/Connector Service
Plantweb Optics		
ASI Web	1 Emerson Wireless Gateway ASI 1 AMS Machinery Manager ASI 1 Plantweb Insight ASI	1 Emerson Wireless Gateway ASI 1 AMS Machinery Manager ASI 1 Plantweb Insight ASI
Assets	20,000	20,000
Historized assets	20,000	10,000
Configured users	25 total users	25 total users
Concurrent users	10	5
AMS Asset Monitor Data Collector		
CHARMs	3072	3072
AMS Device Manager Data Collector		
Devices	10,000	10,000
DeltaV Control Loop Data Collector		
Control Loops	5,000	5,000
KNet Data Collector		
Assets	2,000	2,000
Emerson Wireless Gateway ASI		
ASIs	1 (Up to 20 Emerson Wireless Gateways)	1 (Up to 20 Emerson Wireless Gateways)
Devices	500	500
AMS Machinery Manager ASI		
ASIs	1 (Up to 6 AMS Machinery Manager Network Servers per ASI)	1 (Up to 6 AMS Machinery Manager Network Servers per ASI)
Offline databases, machines, parameters	50 databases or 10,000 machines 1,000,000 parameters	50 databases or 10,000 machines 1,000,000 parameters

Table 3-6: Plantweb Optics scalability *(continued)*

Components	Setup 1: Three-server setup recommended hardware	Setup 2: Two-server setup recommended hardware
Online inputs, parameters	10 AMS 6500 Prediction units 50 AMS 6500 ATG units 40 AMS 9420s 15,000 total parameters	10 AMS 6500 Prediction units 50 AMS 6500 ATG units 40 AMS 9420s 15,000 total parameters
Plantweb Insight ASI		
ASIs	1 (up to 5 Plantweb Insight Servers per ASI)	1 (up to 5 Plantweb Insight Servers per ASI)
Assets	350 per asset source or 1,000 assets total	350 per asset source or 1,000 assets total
OPC UA		
OPC UA Deployment	UA Server and Plantweb Optics Server deployed separately	OPC UA Server and Plantweb Optics Server on same machine
Number of Assets	2,000 assets	1,000 Assets
Number of Total Monitored Tags	8,000 Monitored Tags	4,000 Monitored Tags
Number of Clients	5 Clients	2 Clients

Maximum concurrent users

Configured users Users configured in the User Manager utility.

Mobile device users Users issued with mobile tokens.

Plantweb Optics concurrent users Users accessing the Plantweb Optics utilities and users using the Plantweb Optics Mobile App.
Each browser session a user has open counts in the concurrent user's total.

Tip
For optimum system performance, close any unused browser sessions.

4 Plantweb Optics security

After verifying all of the security and communication requirements below are met, return to Step 3 of the *Preparing for installation* portion of the *Quick start* chapter and continue your installation.

4.1 Firewall considerations

Plantweb Optics components require firewall exceptions for a user-defined port. Port 443 is used by default.

Before installing the Plantweb Optics components, ensure you have the firewall exceptions set in place for each computer with ASI Web Applications. See Deployment scenarios to determine which servers need the firewall exceptions. Obtain the DNS names and IP addresses of the computers, and the ports that need to be open between them. Plantweb Optics requires other ports for communication. See page 39 for more information. Your IT department will determine what, if any, intermediary firewall also needs the exceptions.

Note
Before installing an ASI, you must have TCP/IP ports configured to allow communication between all ASI components in addition to opening any required firewall ports. See Ports for more information.

Firewall Considerations for Connector Service and Proxy Deployment

If any components are separated by a firewall, you must configure the firewall to allow communication on port 443 (default) or the port configured during component installation.

Firewall Considerations for Data Collector Deployments

If a Data Collector is separated by a firewall, you must configure the firewall to allow communication on port 443 (default) or the port configured during installation.

Firewall considerations for Plantweb Insight ASI deployment

If the Plantweb Insight ASI and the Plantweb Insight System are separated by a firewall, configure the firewall to allow communication on port 443. Ports 443 and 80 need to be open if the Plantweb Insight ASI and Plantweb Optics are separated by a firewall.

Firewall considerations for AMS Machinery Manager ASI deployment

If the AMS Machinery Manager ASI Service and Web App are separated by a firewall, configure the firewall to allow communication on port 443 and port 80. The same firewall ports need to be open if the AMS Machinery Manager ASI Web App and Plantweb Optics are separated by a firewall.

4.1.1 Ports

These ports must be available and need to be open through firewalls.

Below are the ports and firewall configurations that need to be configured for SQL Server, Plantweb Optics, and ASI server stations for a Tier-2 database server deployment.

Table 4-1: Ports and firewall rule on SQL Server station

Item	Direction	Firewall rule
Distributed Transaction Coordinator (RPC)	Inbound	Predefined firewall in Server 2012 R2
Distributed Transaction Coordinator (RPC-EPMAP)	Inbound	Predefined firewall in Server 2012 R2
Distributed Transaction Coordinator (TCP-In)	Inbound	Predefined firewall in Server 2012 R2
EMERSONCSI SQL instance TCP port	Inbound / Outbound	SQL
UDP Port 1434	Inbound / Outbound	SQL browser
TCP Port 1433	Inbound / Outbound	SQL

Table 4-2: Ports and firewall rule on Plantweb Optics and ASI Server stations

Item	Direction	Firewall rule
EMERSONCSI SQL instance TCP port	Inbound / Outbound	SQL
UDP Port 1434	Inbound / Outbound	SQL browser
TCP Port 1433	Inbound / Outbound	SQL

Table 4-3: Ports used by Plantweb Optics Server

Item	Direction
TCP 443 (default, configurable)	HTTPS, bidirectional
TCP 139	SQL Server
TCP 445	SQL Server—Filestream
TCP 135	Remote Procedure Call Microsoft Distributed Transaction Coordinator Microsoft Message Queue
TCP 1801	Microsoft Message Queue
TCP 4840	OPC

Table 4-4: Ports used by Connector Service

Item	Direction	Notes
TCP 443 (default, configurable)	Outbound	Connector Service to Plantweb Optics
TCP 443 (default, configurable)	Inbound	Proxy or Data Collector to Connector Service

Table 4-5: Ports used by Proxy

Item	Direction	Notes
TCP 443 (default, configurable)	Outbound	Proxy to Connector Service
TCP 443 (default, configurable)	Inbound	Data Collector/Proxy to Proxy

Table 4-6: Ports used by Emerson Wireless Gateway ASI

Item	Direction	Notes
TCP 443 (default, configurable)	Inbound	Emerson Wireless Gateway ASI to Plantweb Optics
TCP 33333	Bidirectional, secure connection	Wireless Gateways to Emerson Wireless Gateway ASI
TCP 32000	Bidirectional, default connection	Wireless Gateways to Emerson Wireless Gateway ASI

Table 4-7: Ports used by AMS Asset Monitor Data Collector, AMS Device Manager Data Collector, DeltaV Control Loop Data Collector, and KNet Data Collector

Item	Direction	Notes
TCP 443 (default, configurable)	Outbound	Data Collector to Connector Service or Proxy

Table 4-8: Ports used by AMS Machinery Manager ASI

Item	Direction	Notes
TCP 443 (default, configurable)	Inbound	AMS Machinery Manager ASI to Plantweb Optics Web Services

Table 4-9: Ports used by Plantweb Insight ASI

Item	Direction	Notes
443 (default, configurable)	Bidirectional	Plantweb Insight ASI to Plantweb Optics Web Services
443 (default, configurable)	Bidirectional	Plantweb Insight to Plantweb Insight ASI

Table 4-10: Ports used by Inmation Historian

Item	Direction	Notes
TCP 27017	Bidirectional	Mongo DB (default)
TCP 6510-6514 (default, configurable)	Bidirectional	Core Service, Connector Service, Relay Service
TCP 8002 (default, configurable)	Bidirectional	Web Service

Table 4-11: Ports used by CMMS Interface (SAP PM, IBM Maximo PM)

Item	Direction	Notes
TCP 443	Bidirectional	Plantweb Optics to NLINK (CMMS-MW)
TCP 443	Outbound	• NLINK (CMMS-MW) to CMMS (IBM Maximo PM) • CMMS GUI to CMMS (IBM Maximo PM) • NLINK Server
TCP 3200 (3200–3299)	Outbound	Dispatcher, CMMS GUI to CMMS (SAP PM)
TCP 3300 (3300–3399)	Outbound	Gateway to CMMS (SAP-PM) 1 TCP port on this range
TCP 4800 (4800–4899)	Outbound	Gateway-secured to CMMS 1 TCP port on this range
TCP 3260, 3360	Outbound	NLINK to CMMS (SAP ECC 6.0)

Table 4-12: Ports used by Plantweb Optics Mobile App (via Azure)

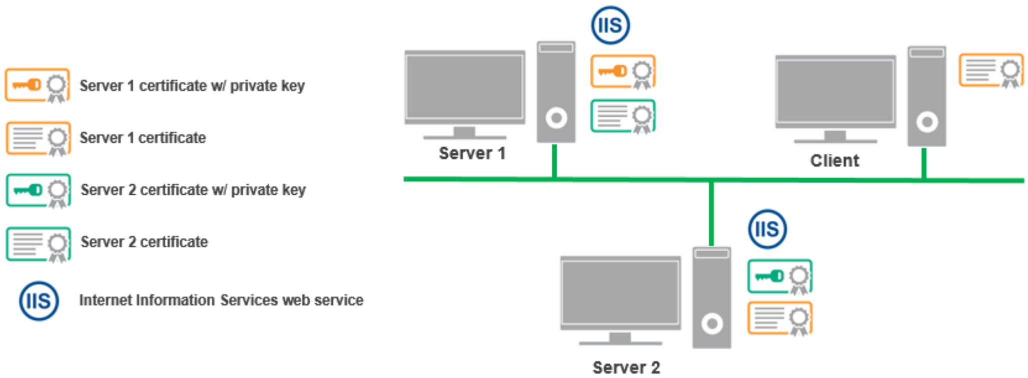
Item	Direction	Notes
TCP 443, non-configurable	Outbound	TCP 443 outbound to *.azurewebsites.net should be open to the internet for the Plantweb Optics Mobile App to work.

4.2 SSL/TLS certificates

Secure Sockets Layer (SSL)/Transport Layer Security (TLS) is required for all web communications. The following sections describe which components require certificates, examples of deployments with certificates, and basic instructions to export and import certificates. However, Emerson recommends working with qualified IT personnel to ensure your installation complies with your plant's network security policy and industry best practices.

SSL/TLS allows applications to establish a secure communication between web servers and web browsers. Figure 4-1 shows an example relationship between web servers and browsers using SSL/TLS certificates. Each server is identified by a private key. If the client has the public key, it can connect securely to the server. In the example, the servers can communicate with each other. The client is only allowed to connect to Server 1. It does not have a certificate for Server 2.

Figure 4-1: Example web servers and browsers using SSL/TLS certificates



Note

SSL/TLS requires TCP port 443.

During the Plantweb Optics installation, certificates are automatically generated and installed for components that use web applications. The certificate is unique to the server. The **private key** certificate must be kept safe on the server. **Never export (or share) the private key certificate**. Only share the **public key** with any computers in your network that need to connect to the server.

4.2.1 System components with certificates

Each computer communicating with an ASI Web Application, Connector Service, or Proxy must exchange public key certificates. The table below shows which components of Plantweb Optics have certificates. See Install certificates for certificate installation instructions.

Table 4-13: System Components with Certificates

Component	Certificate
Plantweb Optics Server	OPTICS1.5
Connector Service	ConnectorService
Proxy	Proxy
Emerson Wireless Gateway ASI	AMSEWG1.5
AMS Asset Monitor Data Collector	AMS Asset Monitor Data Collector
AMS Device Manager Data Collector	AMS Device Manager Data Collector
DeltaV Control Loop Data Collector	DeltaV Control Loop Data Collector
KNet Data Collector	KNet Data Collector
AMS Machinery Manager ASI Web Application	AMSMMASI1.5
Plantweb Insight ASI	INSIGHTASI
Inmation Historian	Not applicable.
Junot NLINK Server	Not applicable. Supports SSL certificates.

The **Certificates Deployment** table lists each security certificate and the servers where the listed certificate must be installed.

Table 4-14: Certificates Deployment

Certificate Name	Plantweb Optics PC	ASI Server	Connector Service PC	Clients	Proxy PC	Data Collector PC
OPTICS1.5	Yes	Yes	Yes	Yes	No	No
Connector Service	No	No	N/A	No	Yes*	Yes*
Proxy	No	No	No	No	Yes*	Yes*
AMSEWG1.5	Yes	Yes	No	Yes	No	No
AMSMMASI1.5	Yes	Yes	No	Yes	No	No
INSIGHTASI	Yes	Yes	No	Yes		No
AMSMWHIST1.5	Yes	Yes	No	No	No	No
AMSMWWIODI1.5	Yes	Yes	No	No	No	No
AMSMWIODR1.5	Yes	Yes	No	No	No	No

* indicates certificate installation is dependent on your network configuration. Note that:

- The Proxy requires the certificate of the component it directly sends data to. A Proxy requires either the Connector Service or Proxy certificate, depending on which component the Proxy communicates directly with.
- A Data Collector requires the certificate of the component it directly sends data to. A Data Collector requires either a Connector Service or Proxy certificate, depending on which server the Data Collector communicates directly with.

In deployments such as in the Level 4 network diagram, the Web Application is installed on a separate computer than the Service.

ASI Web Applications must have certificates to communicate with each relevant part of the system. For example, a Plantweb Optics Client computer requires the Plantweb Optics server certificate to use the Asset Explorer utility. The Plantweb Optics server certificate normally does not need the ASI server certificate, except when a new asset source is added (not required for DeltaV Control Loop ASI v1.5 and AMS Device Manager ASI v1.5.1). In the Asset Explorer utility, when you add a new asset source, the utility contacts the ASI to get information about the asset source. If you try adding an asset source, and the relevant ASI certificate is not installed, an error message lets you know there is a problem connecting to the ASI.

See Deployment scenarios for diagrams that show where the certificates must be installed based on the type of deployment.

4.2.2 Certificate installation checklist

The following tasks show the recommended order of installation on each computer in the system, with emphasis on certificate export and how it relates to installation tasks. This shows all the components, assuming each station is a separate computer, such as a four-level deployment. See Deployment scenarios for diagrams that show where the certificates must be installed based on the type of deployment.

Note
You cannot reuse a certificate from a previous installation. Perform the certificate export and installation tasks after any install, reinstall, or upgrade.

Procedure

1. On the Plantweb Optics Server:
   - ☐ Install Plantweb Optics
   - ☐ Export Plantweb Optics server certificate
2. On the ASI Server:
   - ☐ Install Plantweb Optics server certificate
   - ☐ Install Emerson Wireless Gateway ASI
   - ☐ Install Connector Service
   - ☐ Install AMS Machinery Manager ASI Web Application

- ☐ Install Plantweb Insight ASI
- ☐ Export the Emerson Wireless Gateway ASI certificate
- ☐ Export the AMS Machinery Manager ASI certificate
- ☐ Export the Plantweb Insight ASI certificate

Note
The ASIs can be installed on the ASI server in any order. However, the first ASI certificate that is installed on the ASI Server needs to be exported and installed on the Plantweb Optics Server and the Plantweb Optics client.

3. On the Plantweb Optics Server:
   - ☐ Install each of the ASI certificates
4. On the AMS Asset Monitor Server:
   - Install the AMS Asset Monitor Data Collector
5. On the AMS Device Manager Server:
   - ☐ Install AMS Device Manager Data Collector
   - ☐ Install upstream ASI component certificate (either Connector Service or Proxy)
6. On the DeltaV Server:
   - ☐ Install the DeltaV Control Loop Data Collector
   - ☐ Install upstream ASI component certificate (either Connector Service or Proxy)
7. On the KNet Server:
   - ☐ Install the KNet Data Collector
   - ☐ Install upstream ASI component certificate (either Connector Service or Proxy)
8. On the AMS Machinery Manager Network Server:
   - ☐ Install AMS Machinery Manager ASI Service
   - ☐ Install Plantweb Optics server certificate
   - ☐ Install the ASI certificate
9. On the Plantweb Optics client where users will add asset sources from ASIs:
   - ☐ Install Plantweb Optics server certificate
   - ☐ Install the certificate of the ASI needed for the asset source to be added

Note
If users will not add asset sources from this client PC, only the Plantweb Optics server certificate needs to be installed. Each time a new ASI is added to the platform, it will overwrite the current certificate with the new ASI certificate. All client PCs must then import a new certificate.

4.2.3 Install the Plantweb Optics certificate on clients and servers

You need to install the Plantweb Optics public key certificate before you can use the utilities. You can export the certificate from the server and install it on each client from a file. However, Internet Explorer allows you to easily install the Plantweb Optics public key certificate when you try to log on for the first time.

Prerequisites

- Internet Explorer is required for installing certificates from a browser.
- On a client PC, log in using an account with administrator privilege
- Port 443 must be open between the client and the server

Procedure

1. In Internet Explorer, enter the URL of a utility, such as Asset Explorer.

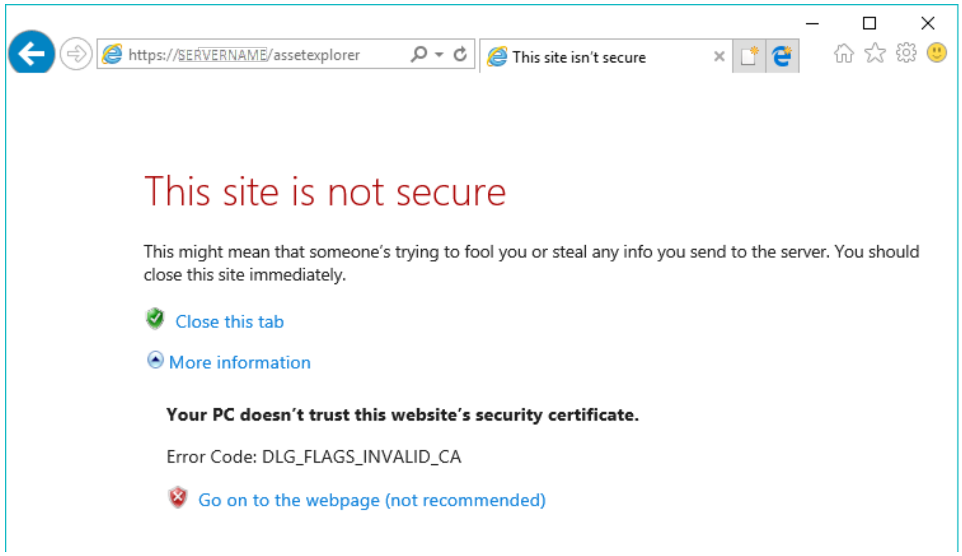
   Example

   `http://[server]/AssetExplorer`

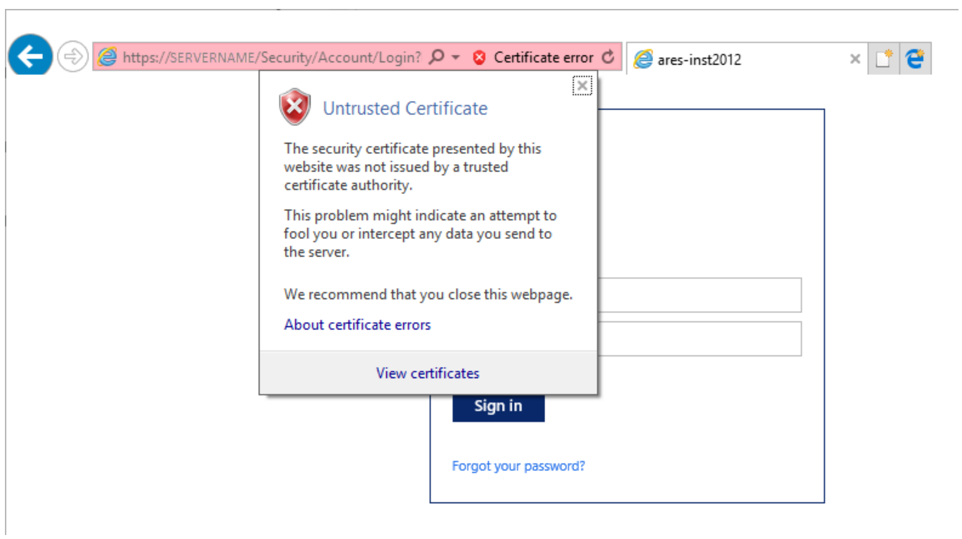
   The URL automatically redirects to use secure HTTPS. Internet Explorer displays a warning in the address bar and a message such as "This site is not secure."

2. Expand **More information**, and click **Go on to the webpage**.

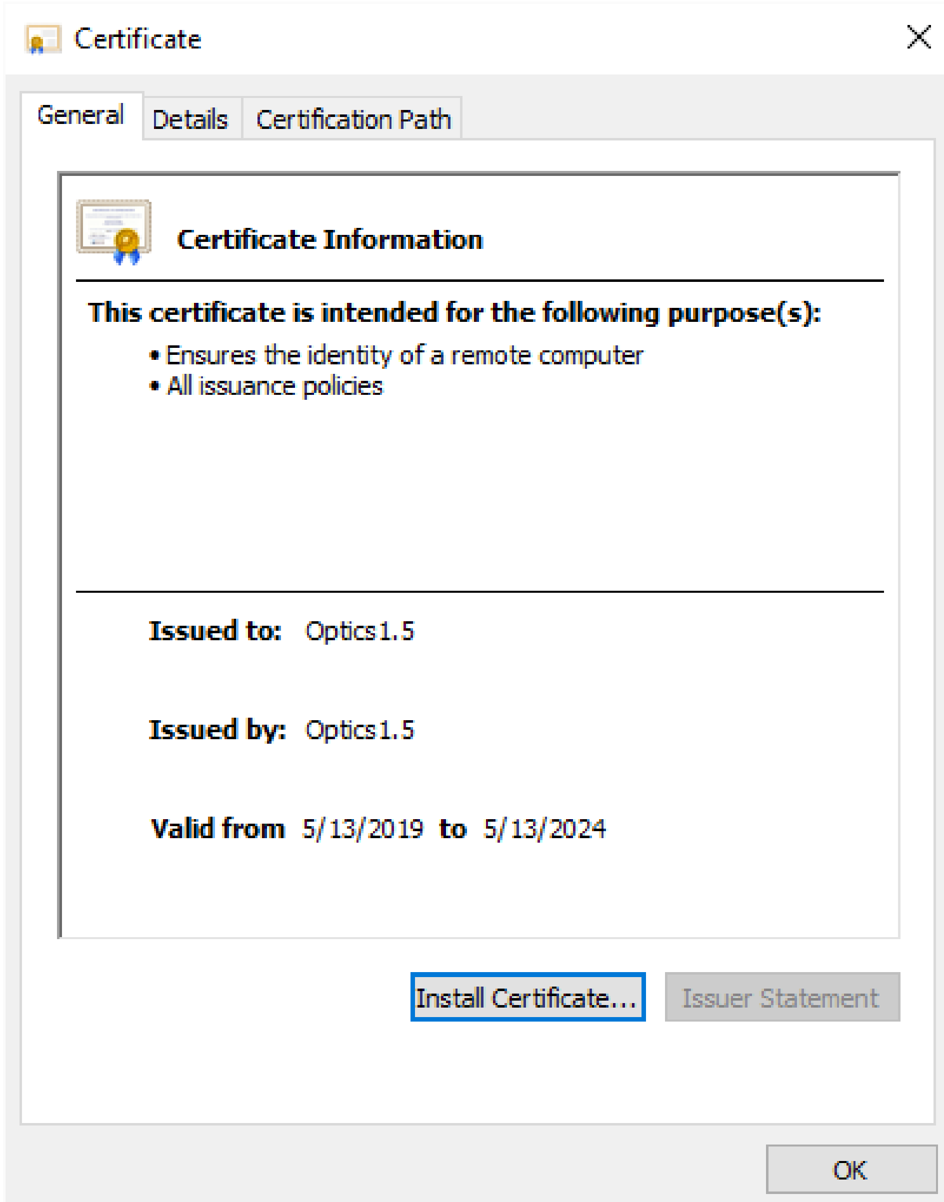
   The message may be different depending on your browser version. Select the option to continue to the website.



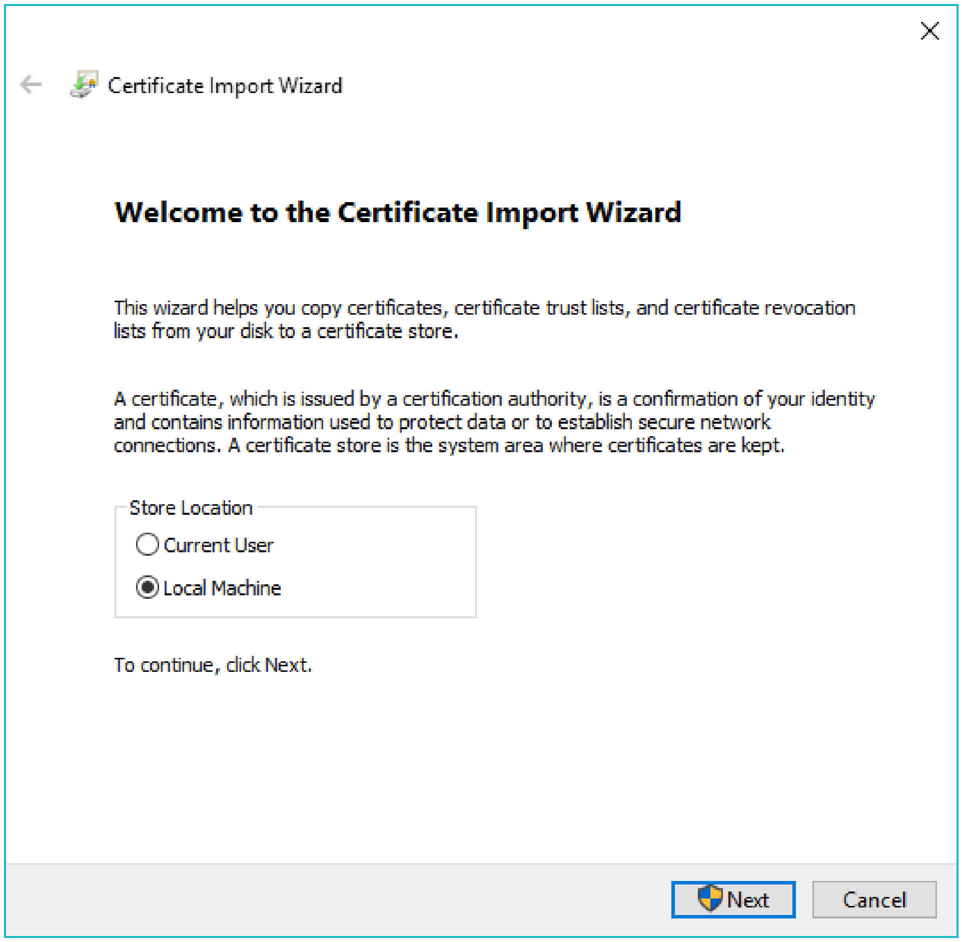
3. On the **Sign in** page, do not sign in. Click **Certificate error** in the browser's address bar.



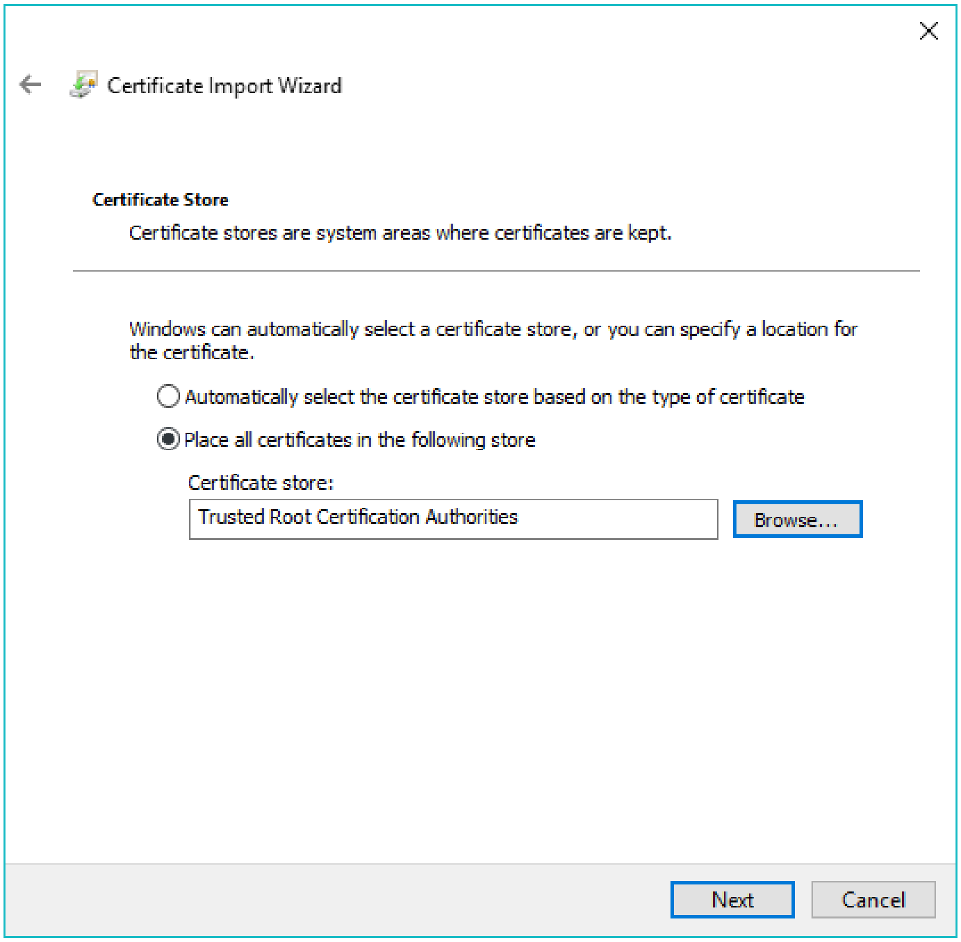
4. In the **Untrusted Certificate** dialog, click **View certificates**.



5. On the **Certificate** dialog, click **Install Certificate**.
   The **Certificate Import Wizard** displays.
6. In the **Certificate Import Wizard**, select **Local Machine**.



7. For **Certificate Store**, select **Place all certificates in the following store**, click **Browse**, and select **Trusted Root Certification Authorities**.



8. Complete the steps in the wizard.
9. Close the **Certificate** dialog.

   The **Sign in** page still shows the certificate error in the address bar.
10. Restart Internet Explorer and launch the same utility.

4.2.4 Export the public key certificate for an ASI station

If you have ASIs installed on computers other than the Plantweb Optics server, you need to export the ASI's public key certificate from that station and install it on the Plantweb Optics server and any client computers that will be accessing information provided through the ASI.

If you have multiple ASIs installed on a server, export the certificate of the ASI that was installed first. In some cases, you may need to export both certificates, such as for the AMS Machinery Manager ASI.

Note

The following instructions use Windows 10 and the `certlm.msc` utility, and are included as a guide. You can also use the `certmgr.msc` utility with the Certificates snap-in. Refer to Microsoft's documentation for more information.

Prerequisites

- On the ASI station, log in using an account with administrator privileges.
- Install the Plantweb Optics certificate on the ASI Station. To confirm, launch a Plantweb Optics utility and sign in without seeing a certificate error.

Procedure

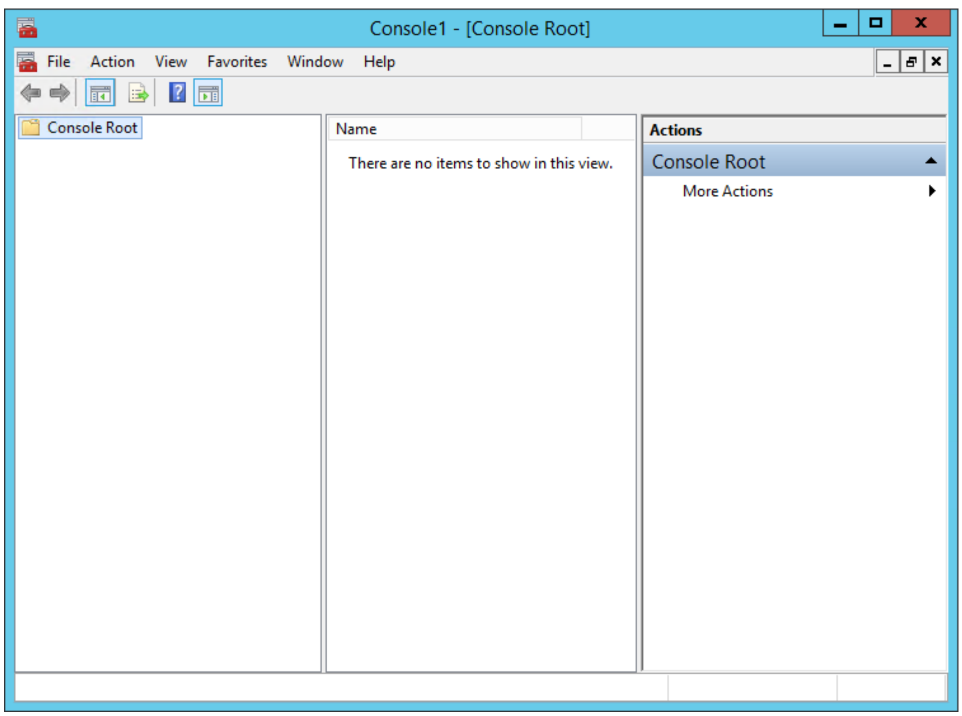
1. From the command prompt, type `MMC.exe` to launch Microsoft Management Console (MMC).

   Always refer to Microsoft's documentation for more information.

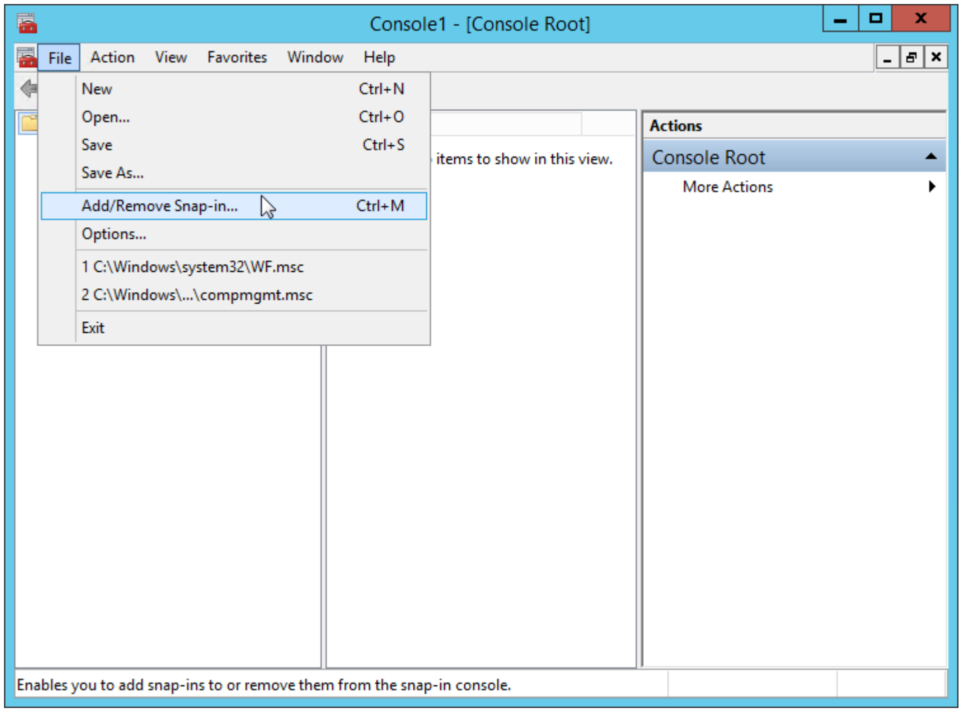
   Note
   You can type `certlm.msc` to launch Microsoft Management Console (MMC) and display the local machine level certificates. If you have `certlm.msc`, launch it and skip to Step 8.

2. In the MMC console, add the **Certificates Snap-in**.

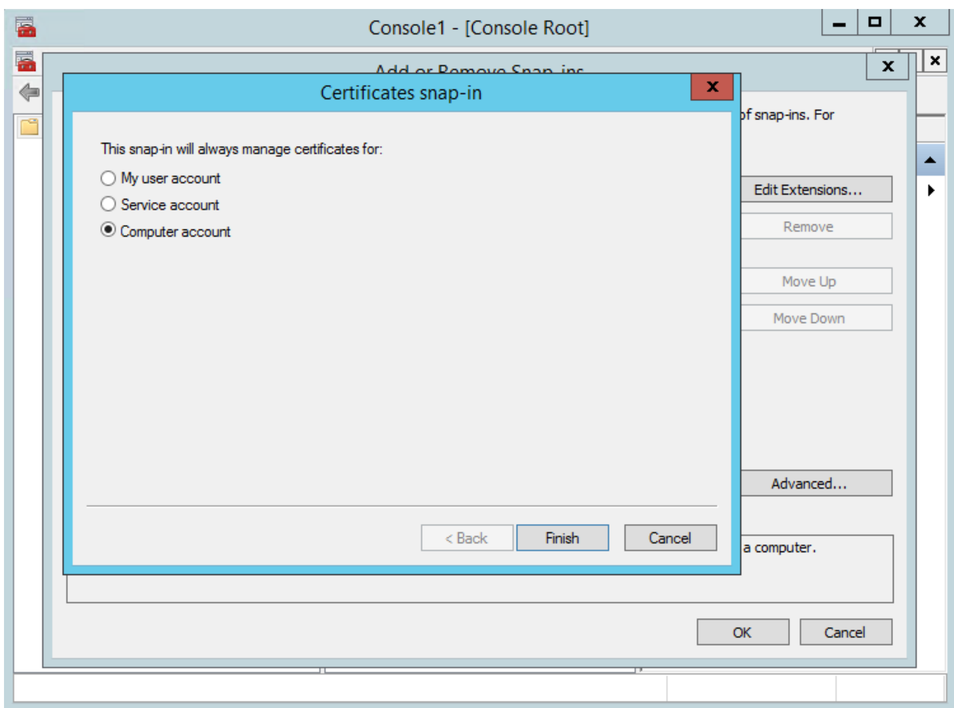
   If **Console Root** already contains the Certificates Snap-in, the **Console Root** node already contains **Certificates**. Skip to Step 8.

3. To add the Certificates Snap-in, select **File** → **Add/Remove Snap-in**.

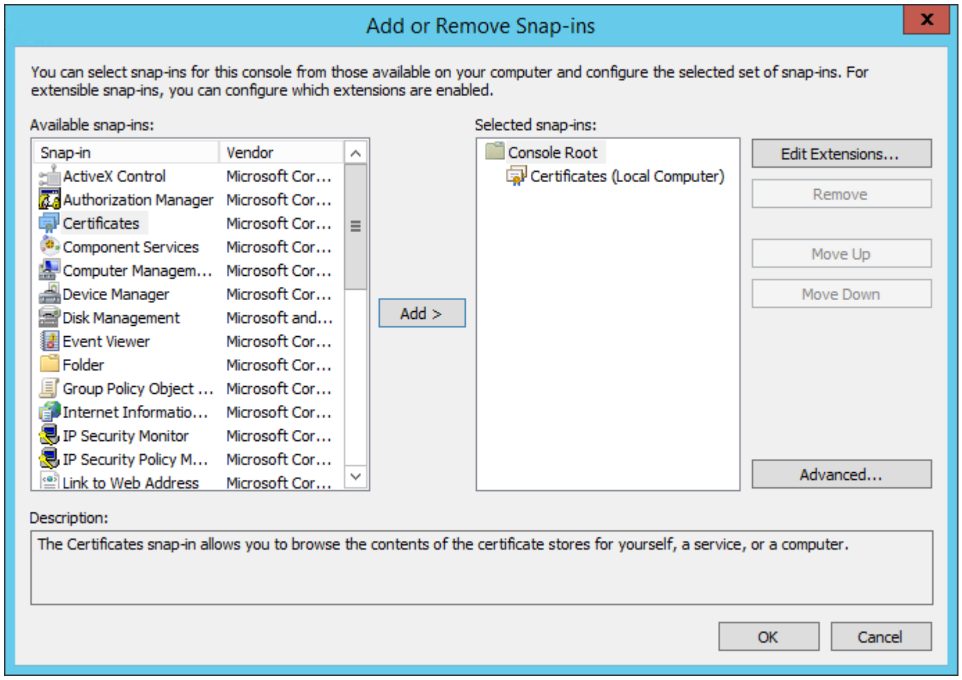


4. In the **Add or Remove Snap-ins** window, double-click **Certificates**, and click **Add**.
5. Select **Computer Account** and click **Finish**.



6. Select **Local computer** and click **Finish**.

In the **Add or Remove Snap-ins** dialog, the **Selected snap-ins** list contains **Certificates (Local Computer)**.

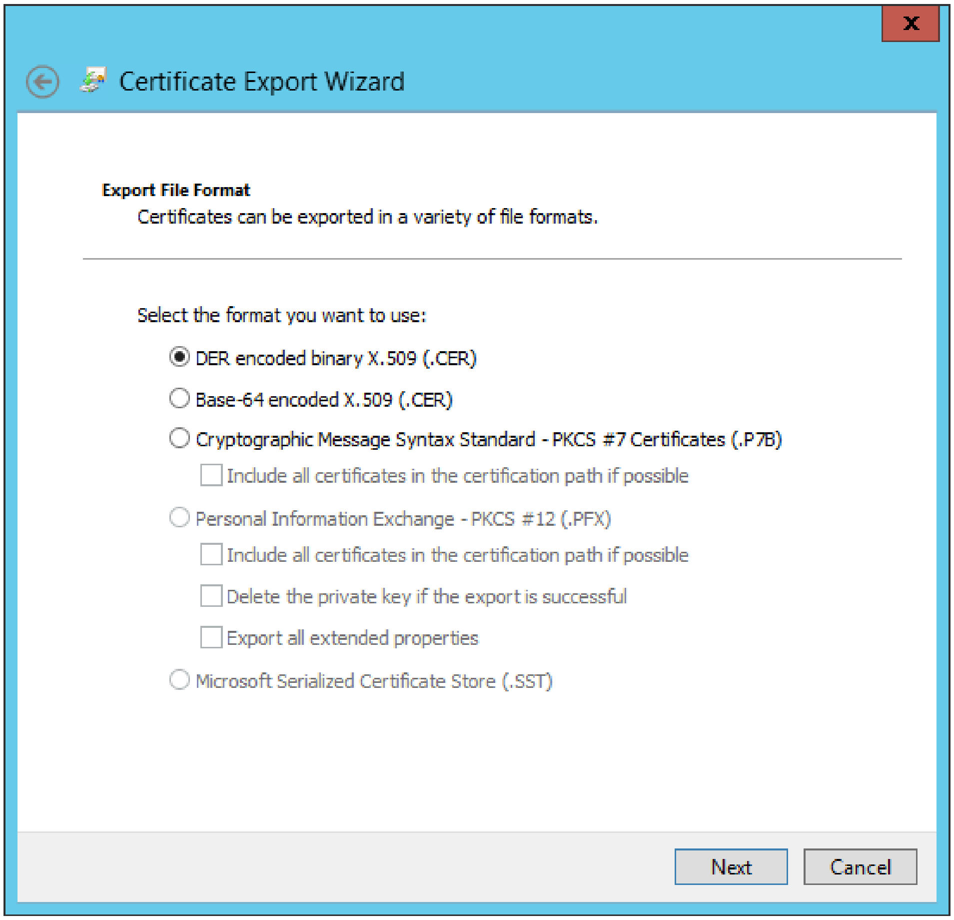


7. Click **OK** to exit the wizard.
8. In the MMC console, expand the nodes to **Certificates (Local Computer)** → **Personal** → **Certificates**.
9. Right-click the certificate to export, and select **All Tasks** → **Personal** → **Export**.
   The Certificate Export Wizard opens.
10. Select **No, do not export the private key (default).**

⚠ CAUTION

Do not export the private key file.

11. In **Export File Format**, select the default format **DER encoded binary X.509 (.CER)**, and click **Next**. (You can use another format if required.)



12. In **File to export**, specify the name and location of the file to be created, and click **Save**.
    - Browse to a secure location where you want to export the certificate as a file.
    - Enter a file name that identifies the component and the server name.

    Note

    Unique filenames can help if you need to export and install certificates for multiple servers.

13. Click **Next**, then click **Finish** to complete the export.

Copy the file to a secure location or device that you can access from the target server.

4.2.5 Install an ASI Station certificate on clients and servers

Install a certificate that has been exported to a file.

Installing the ASI station certificate is a manual process. The system administrator needs to export the certificate first and securely transfer the certificate to the client or server where it can be installed using the Windows Certificate Import Wizard.

Note
The ASIs can be installed on the ASI server in any order. However, the first ASI certificate that is installed on the ASI Server needs to be exported and installed on the Plantweb Optics and the Plantweb Optics client.

The following are some examples of where you will need to install the certificate that is manually exported from an ASI station:

- Install the ASIs according to the installation instructions. See Server installation procedures.
- On the Plantweb Optics server, install the certificate exported from the ASI station.
- On the AMS Machinery Manager station, install the AMS Machinery Manager ASI certificate.
- On the client computer where you are using the Asset Explorer utility, install the Optics1.5 and ASI certificate if you need to add a new asset source from that client.

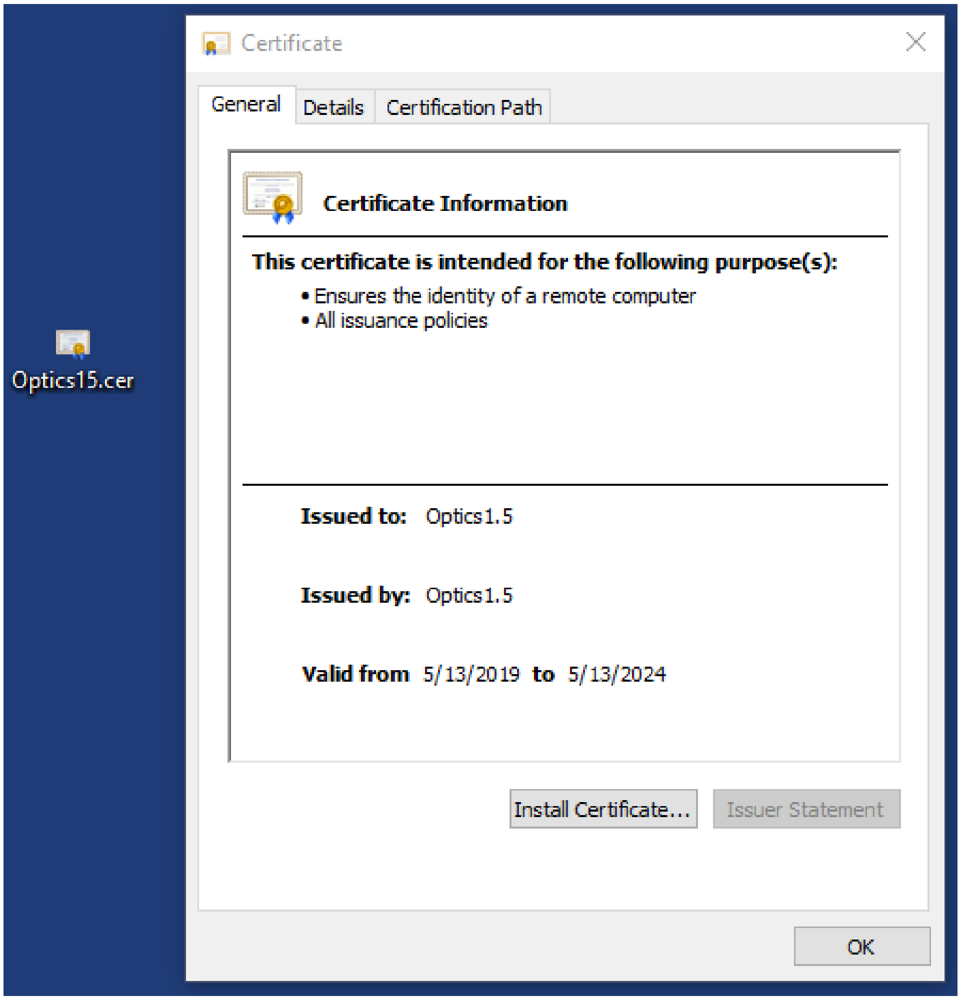
Prerequisites

- Install the Plantweb Optics certificate on the ASI Station. To confirm, launch a Plantweb Optics utility and sign in without seeing a certificate error.
- Export the public key certificate for an ASI station.
- Log in using an account with administrator privileges.

Procedure

1. Copy the certificate file to the target server. For example, copy it to the desktop.
2. Double-click the certificate.
   The **Certificate** properties dialog opens.

   Note
   The example shows the certificate for Plantweb Optics. The ASI certificate will have a different name in **Issued To** and **Issued By** that identifies the ASI.



3. Click **Install Certificate**.
   The Certificate Import Wizard opens.
4. Select **Local Machine** and click **Next**.
5. Specify the **Trusted Root Certification Authorities** store.
6. Click **Finish**.
   The certificate is installed.

4.3 Additional security considerations

Responsibilities and permissions

Assign responsibilities and permissions according to job functions. This strategy ensures that appropriate persons in the plant see relevant alarms and health changes.

Responsibilities restrict the user's view in the Asset Explorer utility according to the locations assigned to that user. Permissions assigned to the user would either enable or prevent the user from performing tasks related to assets, messages, and plant management.

User accounts

The User Manager utility controls user account security. Consider setting account lockouts, password complexity requirements, and session length before adding users in Plantweb Optics.

5 Pre-installation configurations

Other systems that interact with Plantweb Optics, such as AMS Machinery Manager and AMS Device Manager, need to be configured before joining to Plantweb Optics or before obtaining data from these systems.

After completing pre-installation configuration steps, return to Step 1 of the *Installing optional services* portion of the *Quick start* chapter and continue your installation.

5.1 Configure AMS Machinery Manager before importing databases

The following configurations in AMS Machinery Manager are prerequisites to successfully import databases into Plantweb Optics.

Prerequisites

- You must run the Database Converter Tool before you can import the AMS Machinery Manager database into Plantweb Optics or use it with AMS Machinery Manager 6.3.
- AMS Machinery Manager 6.3 or later must be installed.
- Any database you import must already be operational in AMS Machinery Manager 6.3.

Procedure

1. Do the following in AMS Machinery Manager RBMadmin:
    a) Click the **Tools** → **RBM Network Administration** to launch RBMadmin.
    b) Check that all the databases you want to import into Plantweb Optics are listed in the **Databases** pane. If the database is not listed, perform these steps:
        1. Click the **Database** menu and select **Add Database**.
        2. On the **Add Database to Master Database List** dialog, select the **Database Server** and **Data Locker** from the drop-down menus.
           See the AMS Machinery Manager Online Help for more information on data lockers.
        3. In **Database Name**, browse to the database.
           AMS Machinery Manager databases use the .rbm file extension. If the database is in a zip folder, you need to extract it first.
        4. Click **OK**.
2. Check that no data collection is currently in progress on the server and on all client machines.

   Data collection can either happen in Data Import or in the Online Configuration module. You need to stop all data collections that are in progress before importing databases into Plantweb Optics.

3. Make sure there are no changes to the database hierarchy while importing databases to Plantweb Optics.

   These activities in the AMS Machinery Manager system introduce changes to the database hierarchy:

   - Data dump from portable devices (such as from an AMS 2140, IR devices, etc.) to AMS Machinery Manager
   - Data collection from devices connected to the Data Import Server or Online Server
   - Upgrade of AMS Machinery Manager
   - Any changes to the database hierarchy through RBM Wizard, Database Setup, Online Config, and Data Import
   - Creation and update of alarm parameter (AP) sets and alarm limit (AL) sets
   - Creation and update of routes
   - Data deletion through Data Management

   Important
   If there are other users in your system, Emerson recommends you communicate your intent to import databases in advance with the date and time details before the actual database import.

4. Make sure Data Collections Sets (DCSs) are configured with Analysis Parameter (AP) sets before importing Online databases.

   Only parameters inside DCSs are imported into Plantweb Optics. See the AMS Machinery Manager Online Help for more information on data collections sets.

5. Install the latest AMS Machinery Manager patches and updates.

Postrequisites

Import AMS Machinery Manager databases into Plantweb Optics.

5.2 Configure Plantweb Insight before joining to Plantweb Optics

The following configurations in Plantweb Insight are prerequisites before joining Plantweb Insight to Plantweb Optics.

Prerequisites

Make sure your host system interface containing assets whose alerts you want to see is configured in Plantweb Insight Network Configuration.

Procedure

1. Log in to the Plantweb Insight System.
2. Select **System settings** → **Users**.
3. Select the API Keys you want to configure.

4. If no API Key is listed, click **Add API Key**. In the **Add API Keys** dialog box, enter a name for the new API Key. Click **Save** and the new API Key is displayed.
5. Note the **App Name** and the **API Key**. Enter this same information in the **Add Asset Source** dialog box in Plantweb Optics and in the Plantweb Insight ASI. The **Add Asset Source** button is only displayed if the user has MANAGEASSETSOURCE permission.

6 Server installation procedures

This chapter walks through each of the installations available for your system. Emerson recommends reviewing these procedures during the system planning stage to learn what information you must provide during each installation. Follow these procedures during installation to review notes about each installation step.

Tip

Follow the recommended installation and setup order on page 11.

Note

If a server has multiple components installed, the same user with administrator privileges must perform the installations. A different administrator user can install the components on a different server.

SQL is only available to the user who installed it even if the user who installed it is a local administrator and subsequent users are also members of the local administrator group.

6.1 Install the Plantweb Optics Historian

Plantweb Optics Historian provides the user with a way to interact with historical data associated with assets, such as health and other parameters, and allows the user to perform trend analysis on that data.

Prerequisites

- You need the `A48OPTICS-SYSTEM0.Plantweb_Optics.1.5.X.X.zip` file.
- Turn off automatic Windows updates during installation or upgrade.

Procedure

1. Extract the `A48OPTICS-SYSTEM0.Plantweb_Optics.1.5.X.X.zip` file.

   Note

   Extract the zip file on a root directory. For example, drive C.

2. Right-click **install.exe** and select **Run as administrator**.
3. Select **Install Plantweb Optics Historian** and click **Next**.
4. Read and accept the license agreement, and click **Next**.
5. On the **Plantweb Optics Historian Database** screen, enter a password for the MongoDB database.

   This account and password is only used by Plantweb Optics Historian.

   The default user account name is MongoUserAdmin.

6. Select **Install Now** to install with default options or **Customize** to change the path for installation and data.
7. On the **Installation is successful** page, click **Done**.

Return to Step 2 of the *Installing Plantweb Optics* portion of the *Quick start* chapter and continue your installation.

6.2 Install Plantweb Optics Web Services

Prerequisites

- You need the `A48OPTICS-SYSTEM0.Plantweb_Optics.1.5.X.X.zip` file.
- Turn off automatic Windows updates during installation or upgrade.
- You may need to change your computer name before installing the software. Special characters (< > ; : " * + = \ | ? , _ !), accented characters, and other multibyte characters in a computer name can cause problems and interfere with a successful installation. A valid computer name can have numbers 0-9, uppercase and lowercase letters A-Z, and the hyphen (-). Computer names cannot have only numbers, nor can they contain spaces.
- Determine if you will use the server name or IP address to launch the Plantweb Optics utilities. Emerson recommends using the server name.
  - If you use an IP address, use a static address.
  - If you use the server name, ensure the computer name is valid with no special, accented, or multibyte characters.
  - Only make changes to the IP address or server name before installing Plantweb Optics.

Procedure

1. Extract the `A48OPTICS-SYSTEM0.Plantweb_Optics.1.5.X.X.zip` file.

   Note
   Extract the zip file on a root directory. For example, drive C.

2. Right-click **install.exe** and select **Run as administrator**.
3. Select **Install Plantweb Optics Web Services** and click **Next**.

   Note
   Plantweb Optics will run a test to ensure your system is compliant with installation requirements. Any unmet minimum requirements that could impact overall system performance will be shown.

4. Read and accept the license agreement. Click **Next**.
5. Select the database setup and click **Next**:

   - Choose **Plantweb Optics and DB on the same server (Tier-1)** to install Plantweb Optics and the SQL database on the same server.
     When you choose Tier-1, you have the option to include an automated SQL maintenance task that will back up the Plantweb Optics database daily. The backup is set to simple recovery. See page 198 for more information.
     To automatically schedule daily backups of your Plantweb Optics database, ensure **Include Automated SQL Maintenance** is checked. If you uncheck this option, you can manually set up a task in Task Scheduler to automate database backups.
     If you choose Tier-1, skip to Step 7.

- Choose **Plantweb Optics and a separate DB server (Tier-2)** to install Plantweb Optics with its database on a separate SQL Server.

  Important
  In a Tier-2 installation, you need to connect to a separate SQL Server that needs preliminary setup prior to installation. See page 205 for instructions.

6. If you chose Tier-2 in the previous step, enter the following to point to the separate database server:

Server name	The computer name of the database server. **Note** All connected computers with SQL databases will show up in the list. If your database server has been set up to requirements, it will show as a computer name with \EMERSONCSI appended to it.
Authentication	Choose **Windows Authentication** or **SQL Server Authentication**. Select **Windows Authentication** to use the current Windows logged in user account for database authentication. Select **SQL Server Authentication** to use the user specifically created by the database administrator when creating the EmersonCSI named instance. If you select Windows Authentication, you will still need to use the SQL Server Authentication user name and password when accessing the database server.
User name	The user name used for database authentication.
Password	The password associated with the user name used for authentication.

7. If necessary, edit fields in the **Server and Port Binding Configuration** screen, and click **Next**:

Server Configuration	
Use Server Name	Choose **Use Server Name** if you want to access or launch Plantweb Optics using the server name. This is the default and recommended option.
Use IP Address	Choose **Use IP Address** if you want to access or launch Plantweb Optics using the server IP address.
Note The IP address column in the **Server and Port Binding Configuration** screen should be blank. The site binding does not bind to a specific IP address. **Note** Your choice becomes the only allowed setting when launching Plantweb Optics and when installing ASIs and extensions. Failure to use the same configuration when installing ASIs and extensions may cause the installation to fail and you will need to uninstall and reinstall Plantweb Optics or any associated ASIs and extensions to use the same server setting.	

Site Binding Information	
Port	The port number when accessing Plantweb Optics. Port 443 is the default port. If a port is already in use, there is a red square around the port number. You must change any port binding that is being used by another website. See page 199 to free up port 443 if it is being used by another application.

8. On the **Plantweb Optics Mobile App Settings** page, choose whether the Plantweb Optics Mobile App will use Azure Mobile services to receive messages anywhere a mobile device has an internet connection, or the on-premises solution that provides access to your plant network only. Click **Next** after selecting a mobile service.
   - (Default: Azure Mobile Services) The Plantweb Optics Mobile App can receive messages anywhere it has an internet connection. The server and mobile device require an internet connection. This option requires a license file to enable the full features of this mobile application. Click **Browse...** to navigate to your mobile license file `MobileConfig.json`. The mobile license file can be found in the Plantweb Optics license zip file (*`Serial#`*`License.zip`). If a mobile license is not available at this time, see Manually register an Optics Mobile license when using Azure Mobile Services when a mobile license file is available.
   - (On-premises Mobile Service) The mobile app can only receive messages while connected to your plant network. The server and mobile device require connection to your plant network.
9. On the **Default Install Directory** page, change the location where the product will be installed or select the default path provided. Click **Next**.
10. Select **Install Now** to install with default options or **Customize** to change the database location and database user passwords.

    If you choose **Customize**, follow these steps:

    a) Modify the password for FWK_Admin SQL Server user account and click **Next**.

    ⚠ CAUTION

    When you modify passwords, make a note of the new passwords for each user account.

    b) Modify the password for FWK_Reader SQL Server user account and click **Next**.

    c) Modify the password for FWK_Writer SQL Server user account and click **Next**.

    d) Click **Browse** and select where you want to place the database and click **Next**.
11. .Net 4.7.1 installs automatically if it is not already installed. After .Net 4.7.1 installs, the **Installation is pending** page displays.
12. On the **Installation is pending** page, click **Restart Now**.

13. After the system restarts, log in with the same user credentials that you used before. After you log in as the same user, the system installation continues automatically.
14. On the **Installation is successful** page, click **Restart Now**. After the system restarts, the Plantweb Optics installation is completed. After installation, the desktop contains shortcuts for **Asset Explorer** and **Asset View**, and the **Programs** list includes a **Plantweb Optics** folder also with the shortcuts. Access Plantweb Optics by launching the **Asset Explorer** icon on your desktop.

Return to Step 3 of the *Installing Plantweb Optics* portion of the *Quick start* chapter and continue your installation.

6.3 Acquire licenses

The machine fingerprint, or lock code, of the server where Plantweb Optics will be installed must be retrieved before a license file can be generated. The `echoid` tool found in the Plantweb Optics installation zip file is used to retrieve the machine fingerprint or lock code.

Prerequisites

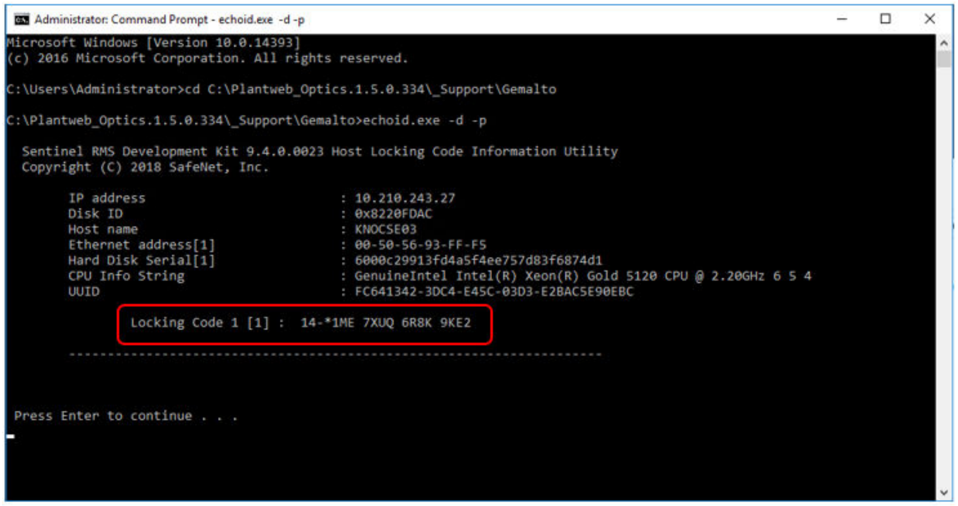
- `A48OPTICS-SYSTEM0.Plantweb_Optics.1.X.X.XXX.zip` file.

Procedure

1. Extract the `A48OPTICS-SYSTEM0.Plantweb_Optics.1.X.X.XXX.zip` file to the Plantweb Optics server.

   Note
   Extract the zip file on a root directory. For example, drive C.

2. Start a command prompt with administrator privileges.
3. Change directories to the following directory in the Plantweb Optics installer zip file: `A48OPTICS-SYSTEM0.Plantweb_Optics.1.X.X.XXX\_Support\Gemalto`
4. Run `echoid -d -p` from the command prompt window to generate your locking code:



5. Copy the 16-character locking code displayed in your command prompt starting with *. To receive your license file, send this code and your Plantweb Optics serial number to:

   wwcs.custserv@emerson.com. For a faster response, call toll-free **888.367.3774, option 2** (US and Canada) or **+63.702.1111** (rest of world).

Postrequisites

After acquiring your license file, return to Installing Plantweb Optics.

6.4 Register licenses

Plantweb Optics must be registered when it is installed.

Note

A separate license file is required for those using the Plantweb Optics Mobile App through Microsoft Azure Mobile Services. Plantweb Optics installation has an optional screen to import a separate `MobileConfig.json` license file when configuring Plantweb Optics Mobile. If a license file is not available at the time of installation, follow Manually register an Optics Mobile license when using Azure Mobile Services to manually install a mobile license file at a later time.

Follow these steps to register the product license.

Procedure

1. From your browser window, enter this URL: **https://<OPTICSservername>/usermanager**.
2. At the bottom of the screen, this message is displayed: **Please contact your local Emerson sales representative for a licensed version of the Plantweb Optics. To install license, click HERE**. Click the **HERE** prompt to register the license. The **Please Upload the License File** window displays.
3. Click **Choose File** and select the License File to activate. Plantweb Optics license files have a .lic file extension.

4. Click **Activate Product**.
5. After registering the license(s), reboot the server.

Return to Step 4 and continue your installation. If using Plantweb Optics Mobile via Azure Mobile Services and you did not register a mobile license file during initial installation, follow Manually register an Optics Mobile license when using Azure Mobile Services.

6.4.1 Manually register an Optics Mobile license when using Azure Mobile Services

A license file is required to enable the full features of the Plantweb Optics Mobile App when using Microsoft Azure Mobile Services. Follow this procedure to manually install a mobile license file if a license was not installed when configuring Plantweb Optics Mobile App Settings in Install Plantweb Optics Web Services.

Procedure

1. Unzip the file `Serial#License.zip` containing the Plantweb Optics Mobile App license file. If Plantweb Optics is licensed for Mobile, this folder will contain both a `.lic` file for Plantweb Optics and a `MobileConfig.json` Plantweb Optics Mobile App license file.
2. Copy `MobileConfig.json` to `\inetpub\wwwroot\EmersonCSI\OpticsIdSrv`
3. Restart the Plantweb Optics server.

6.5 View license summary

Check on the status of your Plantweb Optics licenses from User Manager.

Procedure

1. Using Google Chrome, enter this URL: **https://<OPTICSserverName>/usermanager**.
2. Click on the **LICENSES** tab.
3. The **LICENSES** screen displays the **Status**, **Source**, **Feature**, and expiration date for each license. You can also register other licenses from this screen.

Return to Step 5 of the *Installing Plantweb Optics* portion of the *Quick start* chapter and continue your installation.

6.6 Install the Connector Service

The Connector Service provides common functionality required by the following ASIs:

Table 6-1: ASI Compatibility

ASI	Supported ASI Versions
AMS Asset Monitor	1.5
AMS Device Manager	1.5.1

Table 6-1: ASI Compatibility *(continued)*

ASI	Supported ASI Versions
DeltaV Control Loop	1.5
KNet	1.5

The Connector Service passes information from one or multiple Data Collectors, using Microsoft Internet Information Services through HTTPS, to Plantweb Optics when an asset source is configured in each Data Collector.

The Connector Service can be installed on the same PC as the Data Collector, on a standalone PC (such as an ASI server station), or on a Plantweb Optics server. Only one Connector Service can be installed on any PC. The Connector Service can send data to only one Plantweb Optics system. Plantweb Optics can receive data from multiple Connector Services. Emerson recommends installing the Connector Service on the Plantweb Optics ASI server station.

Prerequisites

- `A48ConnectorSvc.1.5.X.X.zip` file.
- Turn off automatic Windows updates during installation or upgrade.
- The PC name or IP Address where Plantweb Optics is installed.

Procedure

1. Extract the `A48ConnectorSvc.1.5.X.X.zip` file to the computer designated for the Connector Service.

   Note
   Extract the zip file on a root directory. For example, drive C.

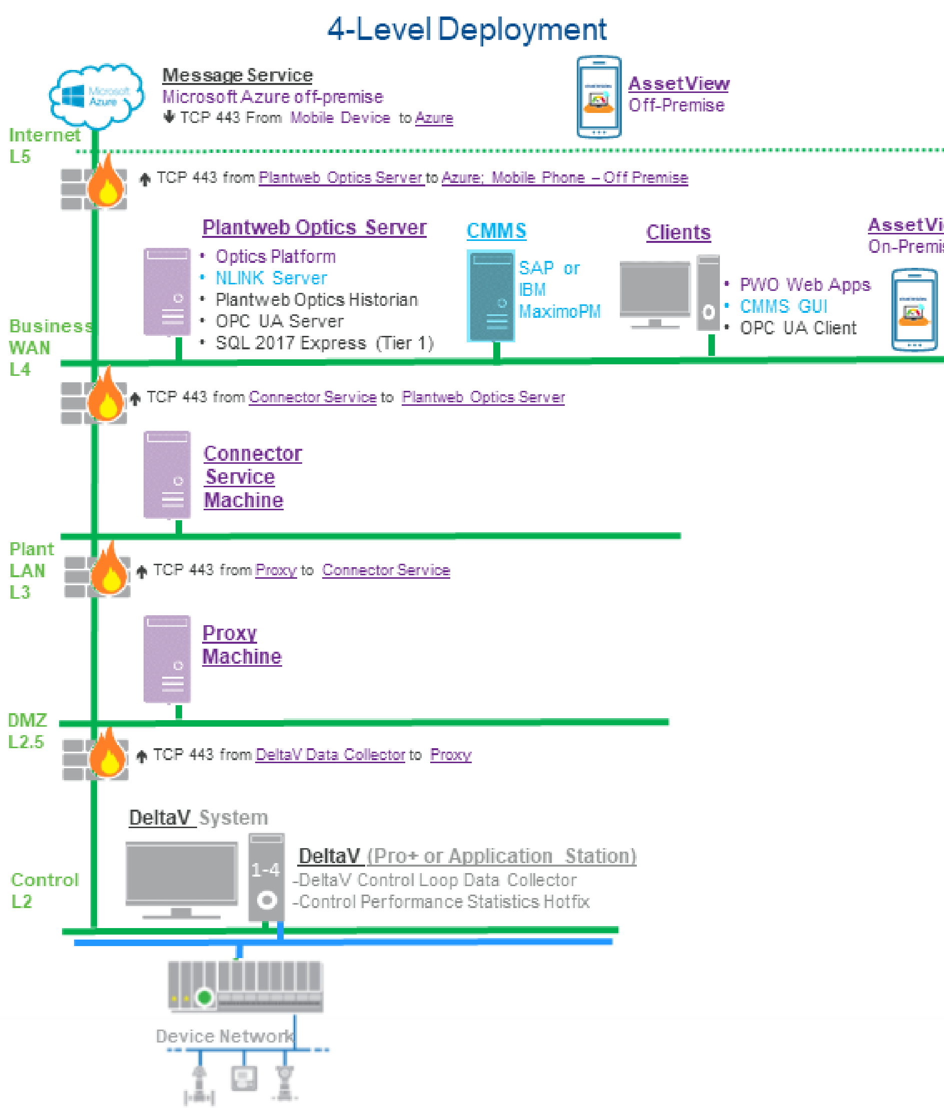
2. Right-click **ConnectorService_Setup.exe** and click **Run as administrator**.
3. Click **Next**.
4. Read the license agreement. If you accept, click **Next**.
5. Verify the installation destination folder. Click **Next**.
6. Enter the Plantweb Optics IP address/PC name and port number. The default port is 443. Click **Next**.
7. Enter the local port number the Connector Service will be bound to. The default port is 443.
8. Click **Next** to begin installation of the third-party components listed in the install dialog.
9. Click **Reboot**. Select **Yes, I want to restart my computer now** to reboot your PC and continue Connector Service installation.
10. Connector Service installation will automatically resume after your PC reboots. Click **Next** to continue installation of any remaining third-party components listed in the install dialog.
11. After installation is complete, click **Finish**.

6.7 Install the Proxy

A Proxy allows Data Collectors to send asset source data to a Connector Service across multiple network levels. Multiple Proxies can be deployed on a network, facilitating data from either Data Collectors to a Connector Service, from Proxy to Proxy, or from a Proxy to a Connector Service.

A Proxy must be deployed on each network level that exists between a Data Collector and the Connector Service it communicates with. If only one firewall exists between a Data Collector and a Connector Service, a Proxy is not required. The diagram below demonstrates deploying a Proxy to connect a DeltaV Control Loop Data Collector with a Connector Service:

Figure 6-1: Deploying a Proxy to Connect a Data Collector with a Connector Service



The Proxy is compatible with the following ASI versions:

Table 6-2: ASI Compatibility

ASI	Supported ASI Versions
AMS Asset Monitor	1.5
AMS Device Manager	1.5.1
DeltaV Control Loop	1.5
KNet	1.5

Prerequisites

- `A48PWOProxy.1.5.X.X.zip` file.
- Turn off automatic Windows updates during installation or upgrade.
- The PC name or IP address of the Proxy or Connector Service this Proxy will send data to.

Procedure

1. Extract the `A48PWOProxy.1.5.X.X.zip` file on the computer designated for the Proxy.

   Note
   Extract the zip file on a root directory. For example, drive C.

2. Right-click **Proxy_Setup.exe** and select **Run as administrator**.
3. Click **Next**.
4. Read the license agreement. If you accept, click **Next**.
5. Verify the installation destination folder.
6. Enter the PC name/IP address and port number of the Connector Service that this Proxy will send data to. Port 443 is the default port.

   Note
   If multiple Proxies are being deployed on your network, enter the PC name or IP address of the Proxy that this Proxy will send data to.

7. Enter the local port number that this Proxy will be bound to. The default port is 443.
8. Click **Next** to being installation of the third-party components listed in the install dialog.
9. On the **Installation is successful** page, click **Finish**.

Postrequisites

After installation completes, the Proxy user interface will launch in your browser. Configure the newly installed Proxy service: Configure the Proxy.

6.8 Configure the Proxy

After completing the Proxy installation process, the IP address of the Proxy or Data Collector that will send data to the newly installed Proxy must be added to the white list. This process must be completed for each Proxy intended to be used on your network.

Additionally, if multiple proxies are being deployed on your network, each Proxy that sends data directly to another Proxy must modify the destination route as outlined below.

Prerequisites

- A Proxy has been installed on the server where this process will be completed.
- The IP addresses of all servers where a Proxy will be installed.
- The IP address or PC name where the Connector Service is installed.

Procedure

1. Launch the Proxy service user interface and log in.
    a) Launch Google Chrome or Internet Explorer.
    b) Navigate to `https://`*<Proxy_PC_Name>*`/proxy`.

       If the Proxy is bound to a port other than the default port 443, navigate to `https://`*<Proxy_PC_Name>*`:`*<PortNumber>*`/proxy`.

       Replace <*PortNumber*> with the port the Data Collector is bound to and <*Proxy_PC_Name*> with the name of the PC where the Proxy is installed

    c) Log in to with your Proxy user account credentials. If a user account has not been created, you will be prompted to create a new account. The username and password are both case-sensitive.

       Note
       Proxy user accounts are bound only to the individual Proxy the account is created on. User accounts are not shared between proxies.

Add the Incoming Proxy or Data Collector IP Address to White List

2. Navigate to the **User White List** tab.
3. Click the + icon to add a new IP address.
4. Enter the IP address of the Data Collector or Proxy where the newly installed Proxy will receive data from. Click the check mark icon when finished.
5. Click **Save** to add the IP address to the white list.

Modify Destination Route If Sending Data to Another Proxy

Complete these additional steps if this Proxy will send data directly to another Proxy. This process is not necessary if this Proxy will communicate directly with a Connector Service.

6. Navigate to the **Proxy Routes** tab.
7. Click the edit icon  to edit the Proxy route sending data to another Proxy. This route is automatically added during Proxy installation.

8. Under the **Route Pattern To Destination** field, add `/proxy/` to the destination route pattern:

   Example

   ```
   https://<ProxyDestinationIP>/proxy/connectorservice/api
   ```

   Note
   It is not necessary to edit the **Route Pattern Into Proxy** field.

9. Click the check mark icon to save route changes.
10. Click **Save** to apply the configured route.

Postrequisites

Depending on your network, additional Proxies may be required to allow the Data Collector to communicate with the Connector Service. If additional Proxy servers are required, repeat the Proxy installation and setup process on each PC that will serve as a Proxy.

6.9 Install the Emerson Wireless Gateway ASI

The Emerson Wireless Gateway ASI lets you connect and display information from an Emerson Wireless Gateway and connected AMS 9420 transmitters.

There are three procedures that must be completed in order to install the Emerson Wireless Gateway ASI. These are:

1. Registering the Emerson Wireless Gateway ASI on the Plantweb Optics server.
2. Installing the Emerson Wireless Gateway ASI.
3. Enabling secure communication with an Emerson Wireless Gateway. This step is only required if you are using secure communication to the gateway. If using unsecured communication, it is not required.

After completing these procedures, return to Step 2 of the *Installing optional services* portion of the *Quick start* chapter and continue your installation.

6.9.1 Register Emerson Wireless Gateway ASI on Plantweb Optics Server

Before the Emerson Wireless Gateway ASI can be installed, you must register the ASI on the Plantweb Optics Server.

Note
The registration steps must be completed using the same user account that installed Plantweb Optics previously.

Prerequisites

- Ensure Plantweb Optics is already installed on the computer you designate as the Plantweb Optics server.

- The `A481420-DS0.EWG_ASI.1.5.X.X.zip` file is needed.
- Turn off automatic Windows updates during installation or upgrade.

Procedure

1. Copy the Emerson Wireless Gateway installer to the Plantweb Optics Server.
2. Extract `A481420-DS0.EWG_ASI.1.5.X.X.zip`.

   Note
   Extract the zip file on a root directory. For example, drive C.

3. Right-click **install.exe** and select **Run as administrator**.
4. On the **Setup** screen, select **Register Emerson Wireless Gateway ASI (on Plantweb Optics Server)**.
5. Read and accept the license agreement. Click **Next**.
6. On the **Emerson Wireless Gateway ASI Server Configuration** screen, enter the server name or IP address of the server where the ASI is installed. Click **Next**.

   Note
   Customize may be displayed as an option, but it has no effect on this registration procedure.

7. Click **Done**.

6.9.2 Install the Emerson Wireless Gateway ASI

The Emerson Wireless Gateway ASI lets you connect and display information from an Emerson Wireless Gateway and connected AMS 9420 transmitters.

Emerson Wireless Gateway ASI is recommended to be installed on a separate ASI server station.

⚠ CAUTION

When you install AMS Device Manager ASI and Emerson Wireless Gateway ASI, there is a risk of adding an Emerson Wireless Gateway that is already in Plantweb Optics. Do not connect the same Emerson Wireless Gateway to multiple AMS Device Manager systems. If this happens, duplicate devices, events, and process variables will display in Plantweb Optics.

If your system gets into this unsupported state, contact Emerson Product Support. There is no automated or user-facing methodology available to recover from this condition.

Prerequisites

- Ensure Plantweb Optics is already installed on the computer you designate as the Plantweb Optics server.
- The `A481420-DSO.EWG_ASI.1.5.X.X.zip` file is needed.
- Turn off automatic Windows updates during installation or upgrade.
- If you install this ASI on a separate server, that server must be configured to requirements before installation. The requirements vary depending on whether a Tier-1 or Tier-2 database setup is used.

Procedure

1. Extract the `A481420-DSO.EWG_ASI.1.5.X.X.zip` file on the server.

   Note
   Extract the zip file on a root directory. For example, drive C.

2. Right-click **install.exe** and select **Run as administrator**.
3. Read and accept the license agreement. Click **Next**.
4. If necessary, edit fields in the **Server and Port Binding Configuration** screen, and click **Next**.

Plantweb Optics Server	
Server Name/IP Address	Enter the Plantweb Optics server name or IP address. Be sure not to enter the ASI server.

Note
The IP address column in the **Server and Port Binding Configuration** screen should be blank. The site binding does not bind to a specific IP address.

Note
Failure to use the same configuration when installing ASIs and extensions may cause the installation to fail and you will need to uninstall and reinstall the software or any associated ASIs and extensions to use the same server setting.

Site Binding Information	
Port	The port number when accessing Plantweb Optics. Port 443 is the default port. If a port is already in use, there is a red square around the port number. You must change any port binding that is being used by another website. See page 199 to free up port 443, if it is being used by another application.

5. Select **Install Now** to install with default options.
6. On the **Installation is successful** page, click **Restart Now**. After the system restarts, the Emerson Wireless Gateway ASI installation is completed.

6.9.3 Enable secure communication with an Emerson Wireless Gateway

If the gateway is configured to use secure communication, follow this procedure to enable connections to the gateway.

Perform these steps on the Emerson Wireless Gateway ASI server only after installing the 1420 Security Setup Utility.

Prerequisites

Install the latest version of 1420 Security Setup Utility (v1.5.7 or later) on the server where the Emerson Wireless Gateway ASI is installed.

For more information on the 1420 Security Setup Utility, see the Emerson Wireless Gateway Reference Manual.

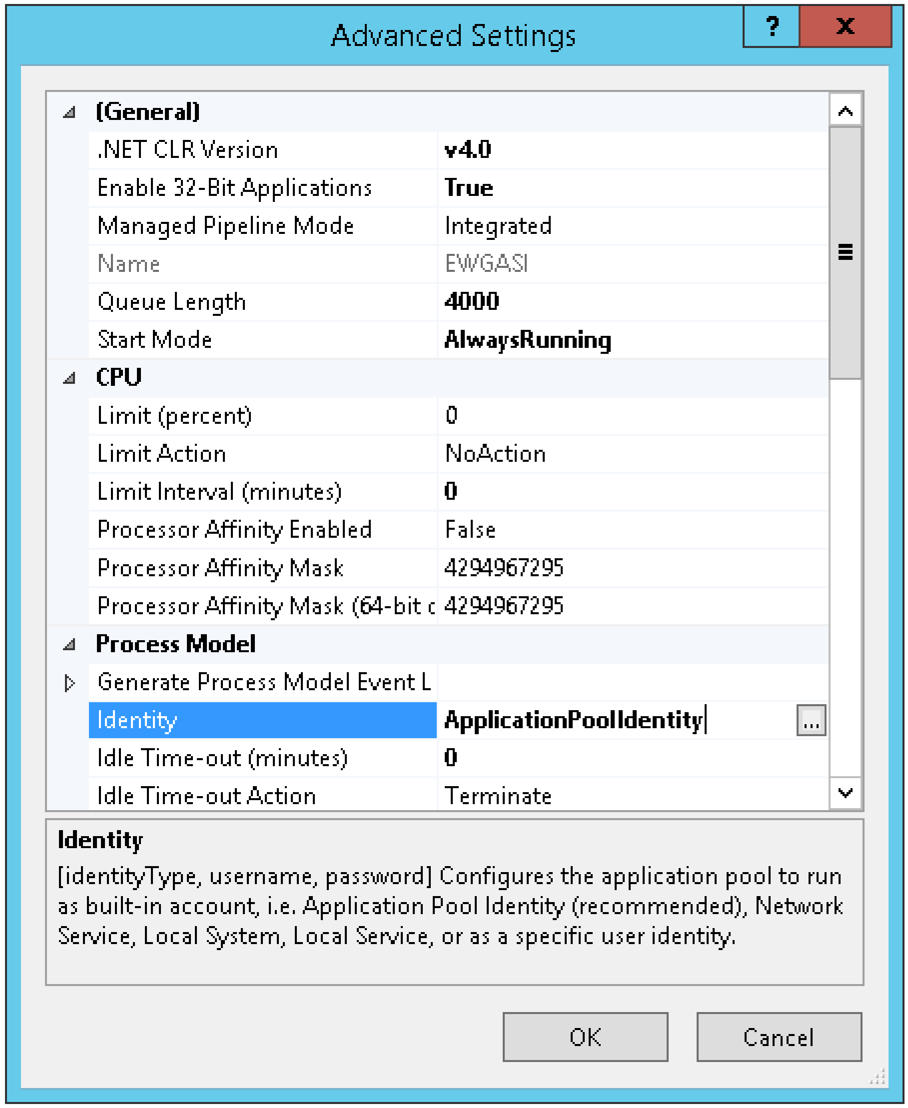
Procedure

1. Launch IIS Manager and expand the server name.
2. Click **Application Pools** and right-click **EWGASI**.
3. Select **Advanced Settings**.

   The **Advanced Settings** dialog is displayed.

4. Under the Process Model tree, select **Identity**, and click ....

Figure 6-2: Advanced Settings—Identity



5. From the Application Pool Identity dialog, select **Custom account** and click **Set**.
6. Enter the administrator username and password and click **OK**.
   The Emerson Wireless Gateway ASI is now set up to run as an administrator.
7. Click **OK** to close the dialogs.
8. From the list of Application Pools, right-click **EWGASI**, and select **Recycle**.
9. Launch the Security Setup Utility and create a new proxy:
   a) Select **Edit** → **New** → **Add AMS Access Proxy**.
   b) Right-click the new proxy and select **Properties**.
   c) Enter the IP address of your Emerson Wireless Gateway.
   d) Click **OK**.

e) Select **File** → **Save**.

f) If you are prompted for authentication, enter the admin password for the target Gateway.

g) Click **OK**.

6.10 Install the AMS Asset Monitor ASI

AMS Asset Monitor ASI Features

The AMS Asset Monitor Data Collector gathers data from AMS Asset Monitor assets and reports key information to Plantweb Optics. After an asset source is configured, information is automatically populated and updated in Plantweb Optics. You can display:

- **Asset hierarchy**—asset hierarchy as defined in AMS Asset Monitor. The physical network and machine hierarchy are displayed in Plantweb Optics Asset Explorer.
- **Asset parameters**—all asset and CHARM parameters are displayed in Plantweb Optics. Each asset may have specific parameters that are measured based on its configuration in AMS Asset Monitor. Each parameter and value displayed in AMS Asset Monitor will have a corresponding parameter and value in Plantweb Optics.
- **Asset health**—CHARM and asset health are displayed in Plantweb Optics. The Asset health score is the lowest health score of all asset parameters. Unhealthy assets (health score less than 100) are added to the unhealthy dashboard in Asset View.
- **Events and messages**—AMS Asset Monitor events and messages are displayed in Plantweb Optics. Any alert generated by AMS Asset Monitor with an Advise, Warning, or Danger state is interpreted by Plantweb Optics as a message-able event.

AMS Asset Monitor ASI Components

Three components allow the AMS Asset Monitor ASI to provide data to Plantweb Optics: the Data Collector, the Connector Service, and the (optional) Proxy. The Data Collector gathers asset source data to send to the Connector Service. The Connector Service then passes information received from the Data Collector, using Microsoft Internet Information Services through HTTPS, to Plantweb Optics. The Proxy facilitates communication between the Data Collector and Connector Service when these components are separated by multiple network levels.

Note the following regarding the Data Collector, Connector Service, and Proxy:

- The Data Collector and Connector Service can be installed on one or two PCs depending on your network requirements.
- Each Data Collector can communicate with only one Connector Service.
- A Connector Service can receive data from multiple Data Collectors. However, each Connector Service can communicate with only one Plantweb Optics system.
- There can be more than one Data Collector per Plantweb Optics server.

6.10.1 AMS Asset Monitor ASI deployment scenarios

Compatibility

The AMS Asset Monitor Data Collector can be deployed with the following AMS Asset Monitor and Plantweb Optics systems:

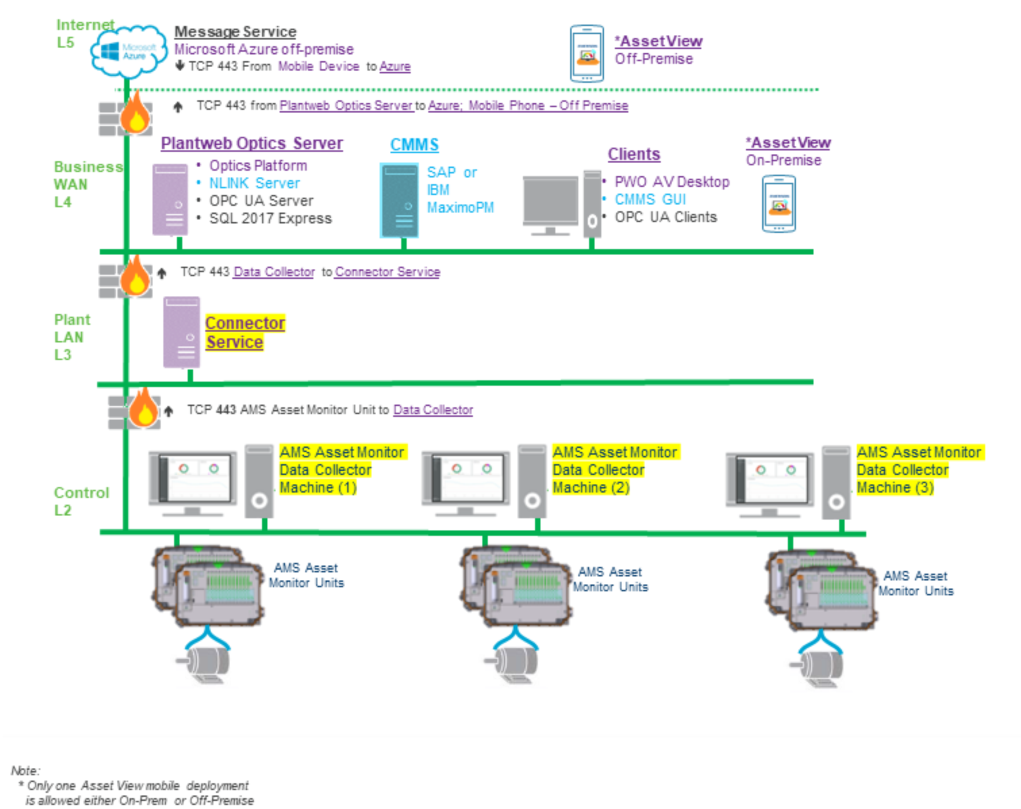
Table 6-3: AMS Asset Monitor ASI Compatibility

Data Collector Version	Plantweb Optics Version	AMS Asset Monitor Version
	1.5.1	22.18
1.5	Supported	Supported

Install AMS Asset Monitor ASI Components on Separate PCs

If Plantweb Optics and AMS Asset Monitor are on different networks, or are separated by a firewall, you must deploy the AMS Asset Monitor Data Collector and the Connector Service on different servers. The machine the Data Collector is installed on must reside on the same network level as AMS Asset Monitor. If the Data Collector and Connector Service are separated by more than one network level, a Proxy must be deployed on each network level that exists between the Connector Service and the Data Collector. The figure below demonstrates deploying the AMS Asset Monitor ASI components with three Data Collectors sending data to Plantweb Optics through a single Connector Service:

Figure 6-3: AMS Asset Monitor ASI Components



If a Connector Service is already installed and communicating with a Plantweb Optics system, the AMS Asset Monitor Data Collector can be configured during installation to communicate with the existing Connector Service.

Install AMS Asset Monitor ASI components on a single PC

For a single PC installation, install the AMS Asset Monitor Data Collector and Connector Service on the same server. The server must reside on the same network level as AMS Asset Monitor.

6.10.2 Register the AMS Asset Monitor ASI with Plantweb Optics

Before installing the AMS Asset Monitor ASI, register the AMS Asset Monitor ASI on the Plantweb Optics server. This process allows the ASI to properly create assets in Plantweb Optics.

Prerequisites

- Plantweb Optics is installed on the computer designated as the Plantweb Optics server.
- `A488500-DS0.AMS_AM_ASI.1.5.0.zip` file.

Procedure

1. Extract `A488500-DS0.AMS_AM_ASI.1.5.0.zip`.

   Note
   Extract the zip file to a root directory on the Plantweb Optics server. For example, drive C:

2. Right-click **install.exe** and select **Run as administrator**.
3. Click **Next**.
4. Read and accept the license agreement. If you accept, click **Next**.
5. Select **Registration** and click **Next**.
6. Verify the installation destination folder and click **Next**.
7. Click **Finish** to complete the registration process.

Postrequisites

After the registration process is complete, install the AMS Asset Monitor Data Collector: Install the AMS Asset Monitor Data Collector.

6.10.3 Install the AMS Asset Monitor Data Collector

Prerequisites

- `A488500-DS0.AMS_AM_ASI.1.5.0.zip` file.
- The Data Collector must be installed on a machine that resides on the same network level as AMS Asset Monitor.
- If installing on a Windows Server 2008 R2 or a Windows 7 operating system, enable Windows automatic updates.
- The PC name or IP address where the Connector Service is installed.
- If deploying the Proxy, the PC name or IP address where the Proxy is installed.
- The AMS Asset Monitor ASI registration process has been completed on the Plantweb Optics server: Register the AMS Asset Monitor ASI with Plantweb Optics.

Procedure

1. Extract the `A488500-DS0.AMS_AM_ASI.1.5.0.zip` file on the computer designated for the Data Collector.

   Note
   Extract the zip file on a root directory. For example, drive C.

2. Right-click **AMSAssetMonitorDataCollector_Setup.exe** and select **Run as administrator**.
3. Click **Next**.
4. Read the license agreement. If you accept, click **Next**.
5. Select **Data Collector** and click **Next**.
6. Verify the installation destination folder and click **Next**.

7. Enter the PC name/IP address and port number where the Connector Service is installed. Port 443 is the default port. Click **Next**.

   Note
   If using the Proxy service, enter the Proxy server PC name/IP address and port number instead.

   ---

8. Enter the local port number the Data Collector will be bound to. Port 443 is the default port.
9. Click **Next** to begin installation of any third-party components listed in the install dialog. Reboot your PC as indicated in the installer dialog. Data Collector installation resumes automatically after your PC reboots.
10. Click **Next** to continue installation of third-party components. Click **Finish** to complete the installation.

Postrequisites

After installation, the AMS Asset Monitor Data Collector user interface opens in your browser. Ensure that the Connector Service and (if applicable) Proxy security certificates are installed on the appropriate servers before adding an asset source. Additionally, the security certificate of each AMS Asset Monitor asset source must be installed on the Data Collector the asset source will communicate with: Install certificates.

6.10.4 Add an asset source to the AMS Asset Monitor Data Collector

Prerequisites

- The Connector Service is installed.
- (Optional) The Proxy is installed.
- The Connector Service and (if applicable) Proxy security certificates are installed on the appropriate servers.
- The Asset Monitor security certificate is installed on the Data Collector server where the asset source will be added.
- An asset source is not configured in the Data Collector.

Procedure

1. Launch the AMS Asset Monitor Data Collector user interface.
   a) Launch Google Chrome or Internet Explorer.
   b) Navigate to `https://`*<Data_Collector_PC_Name>*`/AMSAssetMonitorDataCollector` to launch the Data Collector user interface.

      If the Data Collector is bound to a port other than the default port 443, navigate to `https://`*<Data_Collector_PC_Name>*`:`*<PortNumber>*`/AMSAssetMonitorDataCollector`.

Replace <*PortNumber*> with the port the Data Collector is bound to and <*Data_Collector_PC_Name*> with the name of the PC where the Data Collector is installed.

2. Click the **+** icon to add a new asset source.
   The *add a new asset source* menu appears.
3. In the **Site** selection box, select the site you want associated with the new asset source.
4. Enter a **Display Name** for the new asset source. Assets will appear under this name in Plantweb Optics.
5. Enter the full **Connection URL** of your AMS Asset Monitor web interface.
6. Enter the **Username** and **Password** used to connect to your AMS Asset Monitor web interface.
7. (Optional) Enter a description for the asset source.
8. Click **Add** to begin sending asset source data to Plantweb Optics.

6.11 Install the AMS Device Manager ASI

AMS Device Manager ASI Features

The AMS Device Manager ASI allows you to gather data from AMS Device Manager and report key information to Plantweb Optics. After an asset source is configured, information is automatically populated in Plantweb Optics with automatic updates. You can display:

- **Physical networks**—all the system interfaces you configure on Server Plus and all its connected Client SCs. This includes all hardware under supported control and automation systems, multiplexers, wireless gateways, or systems that support HART, FOUNDATION™ Fieldbus or PROFIBUS DP or PA devices, as well as to a connected HART modem. Calibrators and Field Communicators are not included.
- **Asset class**—Transmitter, Final Control Element, or Industrial Interface.
- **Measurement type**—examples include temperature, pressure, and level.
- **Asset properties**—AMS Tag, as well as the following device attributes: Device Description, Manufacturer, Model, Serial Number (final assembly number), Device Revision, and Next Calibration Date.
- **SIS device attribute**—indicates whether the device is marked as a safety device.
- **Asset health**—based on NE-107 Device Alert category.
- **Device events**—device alert description, help text accompanying the Alert, and Status (whether the alert has been set or cleared). Devices must be configured in Alert Monitor. This does not include **Configuration Changed** events.
- **Device information (optional)**—device variables PV, SV, TV, and QV (not available for PROFIBUS devices), and device-specific variables for select Emerson devices.
- **Overdue calibrations**—overdue calibrations KPI is displayed in Asset View.

⚠ CAUTION

When you install AMS Device Manager ASI and Emerson Wireless Gateway ASI, there is a risk of adding an Emerson Wireless Gateway that is already in Plantweb Optics. Do not connect the same Emerson Wireless Gateway to multiple AMS Device Manager systems. If this happens, duplicate devices, events, and process variables will display in Plantweb Optics.

If your system gets into this unsupported state, contact Emerson Product Support. There is no automated or user-facing methodology available to recover from this condition.

AMS Device Manager ASI Components

There are three components that allow the AMS Device Manager ASI to provide data to Plantweb Optics: the Data Collector, the Connector Service, and the optional Proxy. The Data Collector and Connector Service components must be installed as part of the AMS Device Manager ASI. The optional Proxy facilitates communication between the Data Collector and the Connector Service when the ASI components are separated by multiple network levels. The Data Collector gathers asset source data to send to the Connector Service. The Connector Service then passes information received from the Data Collector, using Microsoft Internet Information Services through HTTPS, to Plantweb Optics.

Note the following regarding the Data Collector, Connector Service, and Proxy:

- The Data Collector and Connector Service can be installed on one or two PCs depending on your network requirements.
- Each Data Collector can communicate with only one Connector Service.
- A Connector Service can receive data from multiple Data Collectors. However, each Connector Service can communicate with only one Plantweb Optics system.
- There can be more than one Data Collector per Plantweb Optics server.

6.11.1 AMS Device Manager ASI deployment scenarios

Compatibility

The Data Collector gathers AMS Device Manager data from the AMS Device Manager database and must be installed on an AMS Device Manager station. Emerson recommends a Client SC station. The AMS Device Manager ASI can be deployed on the following AMS Device Manager and Plantweb Optics systems:

Table 6-4:

Data Collector Version	Plantweb Optics Version			AMS Device Manager Version				
	<1.5	1.5	1.5.1	<13.1.1	13.1.1	13.5	14.0	14.1.1
1.5	Not Supported	Supported	Supported	Not Supported	Not Supported	Supported	Supported	Not Supported
1.5.1	Not Supported	Supported	Supported	Not Supported	Supported	Supported	Supported	Supported

Note

The Data Collector requires a 64-bit operating system and does not support Windows Server 2008 (32-bit). Windows Server 2008 R2 is supported.

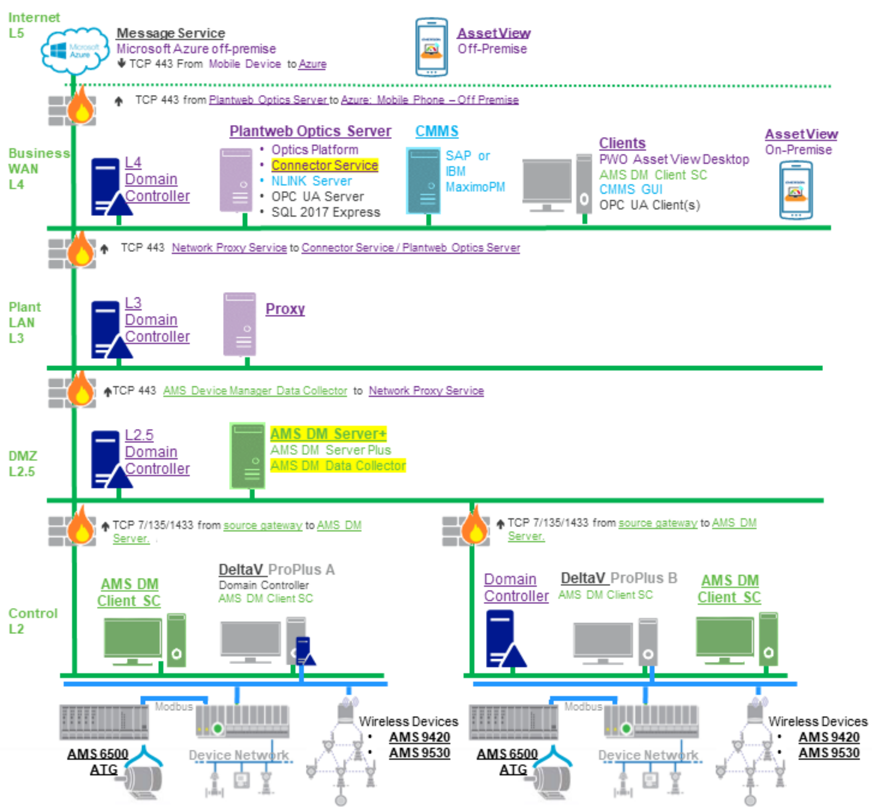
Note

Machine Works customers using Passthrough transport protocol must use AMS Device Manager ASI v1.5. Refer to the Plantweb Optics 1.5 Rev 7 System Guide for ASI v1.5 installation instructions.

Install AMS Device Manager ASI Components on Separate PCs

If the Plantweb Optics server and the AMS Device Manager PC are on different networks, or are separated by a firewall, you must deploy the AMS Device Manager Data Collector on the AMS Device Manager server station, and the Connector Service on a different server. If the Data Collector and Connector Service are separated by more than one network level, a Proxy must be deployed on each network level that exists between the Connector Service and the Data Collector. The figure below demonstrates deploying the AMS Device Manager ASI components with a Proxy facilitating communication between the Data Collector and Connector Service:

Figure 6-4: AMS Device Manager ASI Components



If a Connector Service is already installed and communicating with a Plantweb Optics system, the Data Collector can be configured to communicate with the existing Connector

Service, eliminating the need for a new Connector Service installation. Additionally, multiple AMS Device Manager versions can work with a single Connector Service to feed data to Plantweb Optics. Each AMS Device Manager must have a separate Data Collector installed.

Install AMS Device Manager ASI Components on a Single PC

For a single PC installation, install the AMS Device Manager Data Collector and Connector Service on the AMS Device Manager station.

Upgrade AMS Device Manager ASI

If you have an existing AMS Device Manager ASI installation, refer to Upgrade AMS Device Manager ASI for the AMS Device Manager ASI upgrade procedure. This process will allow you to upgrade existing AMS Device Manager ASIs while maintaining asset source data and history in Plantweb Optics.

6.11.2 Register the AMS Device Manager ASI with Plantweb Optics

Before installing the AMS Device Manager Data Collector, register the AMS Device Manager ASI on the Plantweb Optics server. This process allows the ASI to properly create assets in Plantweb Optics.

Prerequisites

- Plantweb Optics is installed on the computer you designate as the Plantweb Optics server.
- `A488000-DS0.AMS_DM_ASI.1.5.X.X.zip` file.

Procedure

1. Extract `A488000-DS0.AMS_DM_ASI.1.5.X.X.zip`.

   Note
   Extract the zip file to a root directory on the Plantweb Optics server. For example, drive C:

2. Right-click **AMSDeviceManagerDataCollector_Setup.exe** and select **Run as administrator**.
3. Click **Next**.
4. Read and accept the license agreement. If you accept, click **Next**.
5. Select **Registration** and click **Next**.
6. Verify the installation destination folder and click **Next**.
7. Click **Finish** to complete the registration process.

Postrequisites

After the registration process is complete, install the AMS Device Manager Data Collector: Install the AMS Device Manager Data Collector.

6.11.3 Install the AMS Device Manager Data Collector

Follow this procedure on the AMS Device Manager server to install the AMS Device Manager Data Collector.

Prerequisites

- `A488000-DS0.AMS_DM_ASI.1.5.X.X.zip` file.
- If installing on a Windows Server 2008 R2 or a Windows 7 operating system, Windows automatic updates must be enabled.
- The Data Collector must be installed on an AMS Device Manager Server Plus or ClientSC station, version 13.1.1, 13.5, 14, or 14.1.1.
- The PC name or IP address where the Connector Service is installed.
- If deploying the Proxy, the PC name or IP address where the Proxy is installed.
- The latest available AMS Device Manager hotfix bundle has been installed on the AMS Device Manager server.
- The AMS Device Manager ASI registration process has been completed on the Plantweb Optics server. See Register the AMS Device Manager ASI with Plantweb Optics.

⚠ CAUTION

When you install AMS Device Manager ASI and Emerson Wireless Gateway ASI, there is a risk of adding an Emerson Wireless Gateway that is already in Plantweb Optics. Do not connect the same Emerson Wireless Gateway to multiple AMS Device Manager systems. If this happens, duplicate devices, events, and process variables will display in Plantweb Optics.

If your system gets into this unsupported state, contact Emerson Product Support. There is no automated or user-facing methodology available to recover from this condition.

Procedure

1. Extract the `A488000-DS0.AMS_DM_ASI.1.5.X.X.zip` file on the computer designated for the Data Collector.

   Note
   Extract the zip file on a root directory. For example, drive C.

2. Right-click **AMSDeviceManagerDataCollector_Setup.exe** and select **Run as administrator**.
3. Click **Next**.
4. Read the license agreement. If you accept, click **Next**.
5. Select **Data Collector** and click **Next**.
6. Verify the installation destination folder and click **Next**.
7. Enter the PC name/IP address and port number where the Connector Service is installed. Port 443 is the default port. Click **Next**.

Note
If using the Proxy service, enter the Proxy server PC name/IP address and port number instead.

---

8. Enter the local port number the Data Collector will be bound to. Port 443 is the default port.
9. Click **Next** to being installation of any third-party components listed in the install dialog. Reboot your PC as indicated in the install dialog. Data Collector installation will automatically resume after your PC reboots.
10. Click **Next** to continue installation of third-party components. Click **Finish** to complete the installation.

Postrequisites

After installation, the AMS Device Manager Data Collector user interface will open in your browser. Ensure that the Connector Service and (if applicable) Proxy security certificates are installed on the appropriate servers before adding an asset source: Install certificates.

6.11.4 Add an asset source to the AMS Device Manager Data Collector

Prerequisites

- The Connector Service is installed.
- (Optional) The Proxy is installed.
- The Connector Service and (if applicable) Proxy security certificates have been installed on the appropriate servers.
- In AMS Device Manager, **Rebuild Hierarchy** has been run on the appropriate physical networks.
- In AMS Device Manager, **Scan** → **New Devices** has been run on the appropriate physical networks.
- An asset source is not currently configured. If an asset source is currently configured, it must be removed before adding a new asset source.

Procedure

1. Launch the AMS Device Manager Data Collector user interface.
    a) Launch Google Chrome or Internet Explorer.
    b) Navigate to https://*<Data_Collector_PC_Name>*/AMSDeviceManagerDataCollector.

        If the Data Collector is bound to a port other than the default port 443, navigate to https://*<Data_Collector_PC_Name>:<PortNumber>*/AMSDeviceManagerDataCollector.

        Replace <*PortNumber*> with the port the Data Collector is bound to and <*Data_Collector_PC_Name*> with the name of the PC where the Data Collector is installed.

2. Click the + icon to add a new asset source.
3. Configure the new asset source.
    a) In the **Site** selection box, select the site you want associated with the new asset source.
    b) Enter a **Name** for the new asset source. Assets will appear under this name in Plantweb Optics.
    c) (Optional) Enter a description for the asset source.
    d) (Optional) Select **Add Logical Hierarchy** to display the AMS Device Manager Plant Locations hierarchy in the Asset Explorer Location navigator.

       When not selected, the hierarchy is only displayed in the Network navigator. The asset source locations displayed in the location navigator are already bound to the corresponding devices in the Network navigator. To change this setting, you will need to remove and add the asset source again.
    e) Click **Add** to add the asset source.

Postrequisites

The Data Collector will begin sending asset source data from the locally installed AMS Device Manager to the Connector Service or Proxy IP address entered during Data Collector installation. Alert notifications and asset health will automatically be displayed in Asset Explorer.

Opt-in to process variables from HART and FOUNDATION™ Fieldbus devices. See Opt-In to Device Parameters for more information.

6.11.5 Opt-In to Device Parameters

The *AMS Device Manager Data Collector Param Read Configuration* application allows you to opt-in to device parameters from your AMS Device Manager system and pass it through to Plantweb Optics, where you can then configure and monitor those devices.

In addition to the standard data about an asset's properties, alerts, and health—included after installing the AMS Device Manager ASI and configuring it—the configuration application can help you get process variables (sometimes known as measured variables or primary variables) from all HART and FOUNDATION™ Fieldbus devices, and device specific variables from select Emerson HART and FOUNDATION™ Fieldbus devices. To do this, the Data Collector requires a .csv file with the device's AMS Tag, as well as an indication of whether that device's key process variable information and other device-specific parameters can be imported. A value of 1 indicates the column's data will be returned, 0 indicates it is not returned.

To import process and device-specific variables into Plantweb Optics, the structure of the .csv file must contain at least the following exact three column headings:

```
AMSTag,Process Variables,Device Specific Variables
```

Currently, device-specific variables can be imported for Fisher and Micro Motion devices. The device manufacturer is included below in the name of the AMSTag. In the example below, "amstag4fisher" represents a Fisher brand valve that is importing its device-specific variables, and "amstag5micromotion" is importing its process variables and device-specific variables.

```
AMSTag,Process Variables,Device Specific Variables
amstag3device,1,0
amstag4fisher,0,1
amstag5micromotion,1,1
```

Device-Specific variables

When selected in the .csv file, the following device-specific information is returned by the ASI Service.

Fisher Controls HART and FOUNDATION™ Fieldbus devices:

- Drive Signal
- In Service
- Port A Pressure
- Port B Pressure
- Relay Adjust
- Supply Pressure
- Travel
- Travel Deviation
- Cycle Count

Micro Motion HART and FOUNDATION™ Fieldbus devices:

- Mass Flow
- Live Zero
- Density
- Live Temp
- Case Temp
- Vol Flow
- Tube Freq
- Drive Gain
- LPO (filt and raw)
- RPO (filt)
- Electronics Temp
- Input Voltage
- Special Parameters (contact your Emerson Impact Partner)

⚠ CAUTION

Renaming a device tag in AMS Device Manager after the parameter opt-in process has been completed will prevent the associated device parameters from automatically updating in Plantweb Optics. If a device tag is renamed in AMS Device Manager, the parameter opt-in process must be completed again to continue receiving parameter updated in Plantweb Optics.

Get configuration data from AMS Device Manager

Prerequisites

You will need AMS Device Manager DVD2 to complete this procedure.

Procedure

1. Open AMS Device Manager. In Device Explorer, right click on the **AMS Device Manager** server.
2. Click **Export > To Generic Export File**.
3. On the **Generic Export** page, click the **Device List** checkbox. If you want a subset of all the devices in AMS Device Manager, choose **Select** next to the **Device List** checkbox, and select the devices of interest. Click **OK**. The screen displays how many devices are selected. The default is **All selected**. If you do not need to filter your list of devices by the Device Group in Alert Monitor, skip to step 14.
4. Open **AMS Device Manager Alert Monitor**, and select **Configure**.
5. In the toolbar, click **Print Preview**.
6. In the **Print Preview** toolbar, click **Export** and choose **Excel**.
7. Open the file, and filter the desired tags by **Group**.
8. Save the resulting XML file in Microsoft Excel.
9. Insert AMS Device Manager DVD2 into the DVD drive. Navigate to **Supplemental Tools > Reporting Tools** and open the file **DeviceList.xltm**.
10. Open the file in Microsoft Excel, and select **Enable Content** and **Trust Document**, if necessary.
11. Select the **LoadXML** button, and navigate to the **Device List XML** file you saved previously.
12. Rename the **AMS Tag** column to **AMSTag**.
13. Filter the devices as necessary, adding any **Group** column data from previous steps, making sure any **AMSTag** fields match.
14. In Excel, choose **File > Save As...** and select **CSV UTF-8 .csv** (comma delimited).

To import process variables and device-specific variables, see Add process variables and device-specific variables to the .csv file.

Add process variables and device-specific variables to the .csv file

No parameters or process variables will be read until this procedure is done. If you have entered AMSTag names manually, make sure they are 32 characters or less, and do not contain the following symbols: (? ' " \ * ! |). An AMSTag is not case-sensitive.

Procedure

1. In Excel, add columns with the exact names **Process Variables** and **Device Specific Variables**.
2. For each AMSTag that represents a Fisher or Micro Motion device for which you want to import process or device-specific variables, enter **1** in the cell. Entering a **0** will stop collecting the data if it has been previously collected.
3. Save the file as **UTF-8 .csv**. You can now import the .csv file using the AMS Device Manager Data Collector Param Read Configuration application.

Postrequisites

Complete Validate and import .csv file.

Validate and import .csv file

Follow these steps to validate and import the .csv file created to add process variables and device-specific variables.

Prerequisites

- The AMS Device Manager Data Collector is installed.

Procedure

1. Launch **AMS Device Manager Data Collector Param Read Configuration** from the Windows Start menu.
2. Select **Import**.
3. Select **Browse** to locate the .csv file.
4. Change the header row value to the row containing the header. The names must match exactly.
5. Select **Validate** and correct any errors in parsing the .csv file.
6. Select **Import**.
7. To view the *Device Parameter Options* report, press the button to display the list of all AMS Tags in the AMS Device Manager ASI pipeline, and whether Process Variable and Device-Specific Variables are being collected (1) or not (0).

6.12 Install the DeltaV Control Loop ASI

DeltaV Control Loop ASI Features

The DeltaV Control Loop ASI gathers control loop data from control modules configured on a DeltaV system.

DeltaV Control Loop ASI Components

Two components allow the DeltaV Control Loop ASI to provide data to Plantweb Optics: the Data Collector and the Connector Service. Both components must be installed as part of the DeltaV Control Loop ASI. The Data Collector gathers asset source data to send to the Connector Service. The Connector Service then passes information received from the Data Collector, using Microsoft Internet Information Services through HTTPS, to Plantweb Optics. An optional third component, the Proxy, allows communication between the Data Collector and the Connector Service across an arbitrary number of networks to provide network independence and security.

Note the following regarding the Data Collector, Connector Service, and Proxy:

- The Data Collector and Connector Service can be installed on one or two PCs depending on your network requirements.
- Each Data Collector can communicate with only one Connector Service.
- A Connector Service can receive data from multiple Data Collectors. However, each Connector Service can communicate with only one Plantweb Optics system.
- There can be more than one Data Collector per Plantweb Optics server.

New *ControlLoopSvc* Windows user considerations

A new Windows group Managed User Account (gMSA) *ControlLoopSvc* is created on the ProfessionalPlus server when installing the DeltaV Control Loop Data Collector. This user is also created on the Application Station depending on your deployment as outlined below. Note the following regarding the new ControlLoopSvc user:

If the PC where the Data Collector will be installed is part of a Windows domain (excluding Windows 2008 R2 and Windows 7 operating systems):

- A new user *ControlLoopSvc* is created on the ProfessionalPlus server, regardless of whether the Data Collector is installed on a ProfessionalPlus server or an Application Station.
- A new user is not created on the Application Station, regardless of where the Data Collector is installed. If the Data Collector is installed on an Application Station, the user account created on the ProfessionalPlus server will have access to the Application Station.
- Password management of the *ControlLoopSvc* user is handled automatically by the Windows domain.

If the PC where the Data Collector is installed is not part of a Windows domain, or the Data Collector is installed on a Windows 2008 R2 or Windows 7 operating system:

- A new user *ControlLoopSvc* is created on the ProfessionalPlus server, regardless of whether the Data Collector is installed on a ProfessionalPlus server or an Application Station.
- If the Data Collector is installed on an Application Station, a new Windows user *ControlLoopSvc* is created on the Application Station in addition to the user created on the ProfessionalPlus server.
- The *ControlLoopSvc* user password must be updated manually as desired or in accordance with your site's password policy. See Change the ControlLoopSvc Windows

user password to manually change the *ControlLoopSvc* user password on either the ProfessionalPlus server or the Application Station.

6.12.1 DeltaV Control Loop ASI deployment scenarios

Compatibility

The DeltaV Control Loop ASI can be deployed on the following DeltaV ProfessionalPlus and Application Station systems. The Control Performance Statistics (CPS) hotfix must be installed on the DeltaV ProfessionalPlus server prior to DeltaV Control Loop Data Collector installation:

Table 6-5: DeltaV ASI Version Compatibility

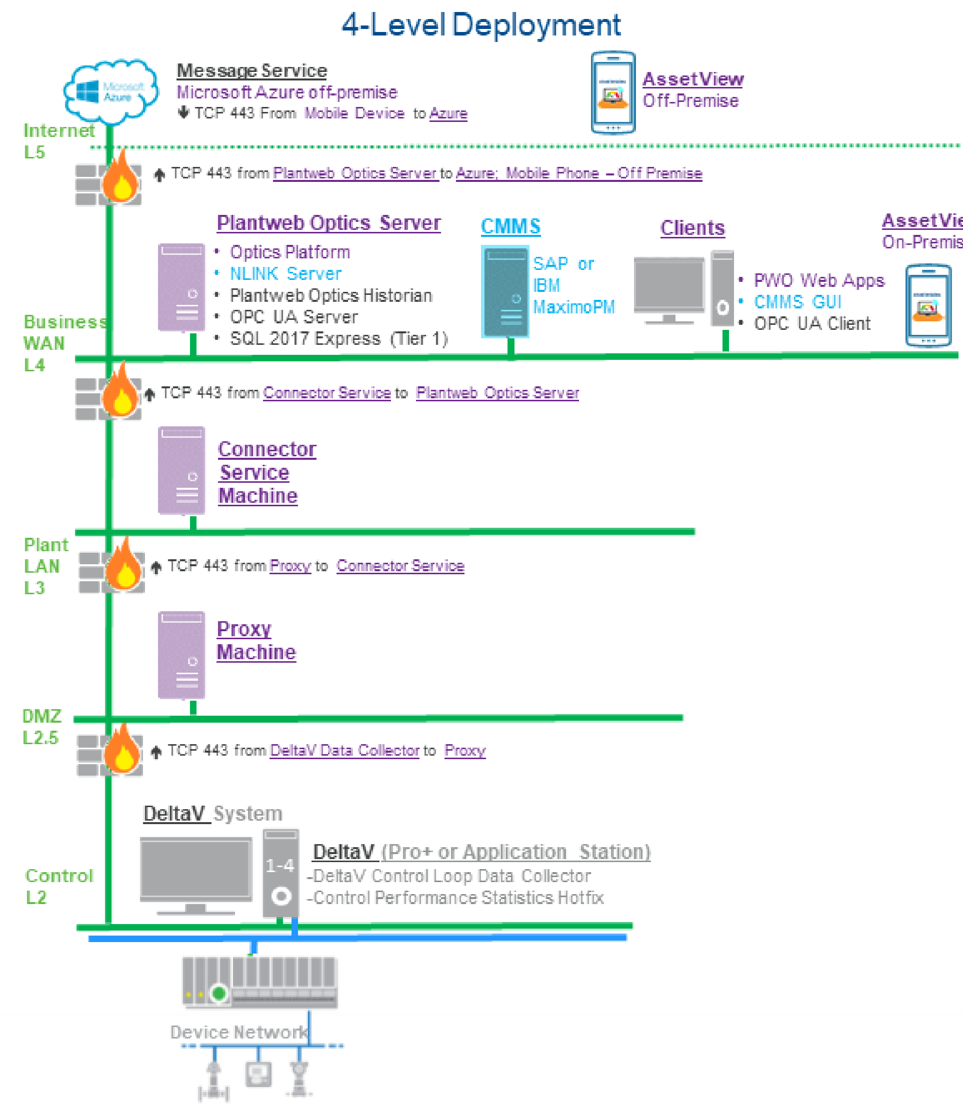
Data Collector Version	Plantweb Optics Version		DeltaV Version			
	<1.5.1	1.5.1	<12.3.1	12.3.1	13.3.1	14.3.1
1.5	Not Supported	Supported	Not Supported	Supported	Supported	Supported

Note
The Data Collector requires a 64-bit operating system and does not support Windows Server 2008 (32-bit). Windows Server 2008 R2 is supported.

Install DeltaV Control Loop ASI Components on Separate PCs

If the Plantweb Optics and the DeltaV servers are on different networks, or are separated by a firewall, you must deploy the DeltaV Data Collector on the DeltaV Control Loop server and the Connector Service on a different server. If the Data Collector and Connector Service are separated by more than one network level, a Proxy must be deployed on each network level that exists between the Connector Service and the Data Collector. The figure below demonstrates deploying the DeltaV ASI components with a Proxy facilitating communication between the Data Collector and Connector Service:

Figure 6-5: DeltaV ASI Components



If a Connector Service is already installed and communicating with a Plantweb Optics system, the DeltaV Control Loop Data Collector can be configured to communicate with the existing Connector Service, eliminating the need for a new Connector Service installation.

The DeltaV Data Collector must be deployed on either a DeltaV ProfessionalPlus or Application Station, and have access to the DeltaV-generated CPM files. By default, CPM files are placed in the `DVData` folder on the DeltaV ProfessionalPlus server. Refer to the DeltaV documentation for more information on modifying this location.

Install DeltaV Control Loop ASI components on a single PC

For a single PC installation, install the DeltaV Control Loop Data Collector and Connector Service on the DeltaV ProfessionalPlus or Application Station PC.

6.12.2 Register the DeltaV Control Loop ASI with Plantweb Optics

Before installing the DeltaV Control Loop ASI, register the DeltaV Control Loop ASI on the Plantweb Optics server. This process allows the ASI to properly create assets in Plantweb Optics.

Prerequisites

- Plantweb Optics is installed on the computer you designate as the Plantweb Optics server.
- `A48CtrlLoop-DS-0.1.5.X.X.zip` file.

Procedure

1. Extract `A48CtrlLoop-DS-0.1.5.X.X.zip`.

   Note
   Extract the zip file to a root directory on the Plantweb Optics server. For example, drive C:

2. Right-click **DeltaVControlLoopDataCollector_Setup.exe** and select **Run as administrator**.
3. Click **Next**.
4. Read and accept the license agreement. If you accept, click **Next**.
5. Select **Registration** and click **Next**.
6. Verify the installation destination folder and click **Next**.
7. Click **Finish** to complete the registration process.

Postrequisites

After the registration process is complete, install the Data Collector.

6.12.3 Install the DeltaV Control Loop Data Collector

The DeltaV Control Loop Data Collector must be installed on a DeltaV ProfessionalPLUS or Application Station. If installing the Data Collector on an Application Station, additional installation steps must be performed on the ProfessionalPLUS server to grant the Data Collector access to control loop data.

Prerequisites

- `A48CtrlLoop-DS-0.1.5.X.X.zip` file.
- If installing on a Windows Server 2008 R2 or a Windows 7 operating system, Windows automatic updates must be enabled.
- If installing in a Windows 2012 or 2016 domain environment, the user installing the Data Collector must be part of the Domain Admins (DA) group.

- The DeltaV Control Loop Data Collector must be installed on either a DeltaV ProfessionalPLUS server or Application Station, version 12.3.1, 13.3.1, or 14.3.1.
- The PC name or IP address where the Connector Service is installed.
- If deploying the Proxy, the PC name or IP address where the Proxy is installed.
- The DeltaV Control Loop ASI registration process has been completed on the Plantweb Optics server. See Register the DeltaV Control Loop ASI with Plantweb Optics.

Procedure

Application Station Deployment Pre-Installation

If installing the DeltaV Control Loop Data Collector on an Application Station, the following installation steps must be performed on the DeltaV ProfessionalPLUS server.

1. Extract the `A48CtrlLoop-DS-0.1.5.X.X.zip` file on the DeltaV ProfessionalPLUS server.

   Note
   Extract the zip file on a root directory. For example, drive C.

2. Right-click **DeltaVControlLoopDataCollector_Setup.exe** and select **Run as administrator**.
3. Click **Next**.
4. Read and accept the license agreement. If you accept, click **Next**.
5. Select **Data Collector** and click **Next**.
6. Select **Distributed Deployment**. Click **Next**.
   A notification will display informing you that the distributed deployment setup is complete on the DeltaV ProfessionalPLUS station. Proceed with installing the Data Collector on the Application Station.

Install the Data Collector

7. Extract the `A48CtrlLoop-DS-0.1.5.X.X.zip` file on the computer designated for the Data Collector.

   Note
   Extract the zip file on a root directory. For example, drive C.

8. If installing on a Windows Server 2008 R2 operating system, TLS 1.2 must be enabled. To enable TLS 1.2, right-click `Enable TLS1.2.reg`. Click **Merge**.
9. Right-click **DeltaVControlLoopDataCollector.exe** and select **Run as administrator**.
10. Click **Next**.
11. Read and accept the license agreement. Click **Next**.
12. Select **Data Collector** and click **Next**.
13. If installing the Data Collector on a ProfessionalPLUS server, select **Single Station** and click **Next**.

    Note
    If installing the Data Collector on an Application Station, this dialog will not be displayed.

14. Verify the Data Collector installation destination folder and click **Next**.
15. Enter the Connector Service PC name/IP address and port number. Port 443 is the default port assigned during Connector Service installation.

    Note
    If using the Proxy service, enter the Proxy server PC name/IP address and port number.

16. Enter the local port number that the Data Collector will be bound to and click **Next**. Port 443 is the default port.
17. Click **Next** to being installation of any third-party components listed in the install dialog. Reboot your PC as indicated in the install dialog. Data Collector installation will automatically resume after your PC reboots.
18. Click **Next** to continue installation of third-party components. Click **Finish** to complete the installation.

Postrequisites

After the system restarts, the DeltaV Control Loop Data Collector user interface will open in your browser. Ensure that the Connector Service and (if applicable) Proxy security certificates are installed on the appropriate servers before adding an asset source: Install certificates.

If using Internet Explorer, a blank screen may appear when the Data Collector user interface launches. If this occurs, continue the installation with Configure Internet Explorer for use with a Data Collector

Configure Internet Explorer for use with a Data Collector

A blank screen may occur when launching the DeltaV Control Loop Data Collector user interface in Internet Explorer. If this occurs, configure Internet Explorer with the required settings outlined below.

Procedure

1. In Internet Explorer, open **Tools** → **Internet Options**
2. Click the **Security** tab in the dialog that appears.
3. Click **Custom level...**
4. Under **Downloads**, select **Font Download** → **Enable**.
5. Under **Scripting**, select **Active Scripting** → **Enable**.
6. Click **OK**.

Postrequisites

After applying the above settings, relaunch Internet Explorer and continue with adding an asset source: Add an asset source to the DeltaV Control Loop Data Collector

6.12.4 Add an asset source to the DeltaV Control Loop Data Collector

Prerequisites

- The Connector Service is installed.
- (Optional) The Proxy is installed.
- The Connector Service and (if applicable) Proxy security certificates have been installed on the appropriate servers.
- The Control Performance Monitor (CPM) hotfix with Control Performance Statistics (CPS) has been installed on the DeltaV ProfessionalPLUS server. Refer to Knowledge Base Article NK-1900-0820 for more information.
- An asset source is not configured.

Procedure

1. Launch the DeltaV Control Loop Data Collector user interface.
   a) Launch Google Chrome or Internet Explorer.
   b) Navigate to https://*<Data_Collector_PC_Name>*/DeltaVControlLoopDataCollector to launch the Data Collector user interface.

      If the Data Collector is bound to a port other than the default port 443, navigate to https://*<Data_Collector_PC_Name>:<PortNumber>*/DeltaVControlLoopDataCollector.

      Replace *<PortNumber>* with the port the Data Collector is bound to and *<Data_Collector_PC_Name>* with the name of the PC where the Data Collector is installed.

2. Click **Add Asset Source**.
3. Configure the new asset source.
   a) In the **Site** selection box, select the site you want associated with the new asset source.
   b) Enter a **Display Name**. Assets will appear under this name in Plantweb Optics.
   c) Enter the destination folder where DeltaV Control Performance Statistics (CPS) deposits CPM files, such as `D:\DeltaV\DVData\InSight\Data`.

Postrequisites

The Data Collector will begin sending asset source data from the newest CPM file to the Proxy or Connector Service identified during Data Collector installation. Alert notifications and health data will automatically be displayed in Asset Explorer with asset data pulled from the newest CPM file.

6.12.5 Change the ControlLoopSvc Windows user password

For servers outside a Windows domain, follow this procedure to manually change the *ControlLoopSvc* user password as desired or as required by your site's password policy.

A new Windows user account *ControlLoopSvc* is created on the DeltaV ProfessionalPLUS server when installing the DeltaV Control Loop Data Collector. This user account is created on the ProfessionalPLUS server regardless of whether you choose to install the Data Collector on a ProfessionalPLUS server or an Application Station. See Install the DeltaV Control Loop ASI for more information on the *ControlLoopSvc* user created during Data Collector installation.

If the ProfessionalPLUS server (and the Application Station for distributed Data Collector deployment scenarios) is joined to a Windows domain, the *ControlLoopSvc* user password is changed automatically by the Windows domain according to your domain policy. The *ControlLoopSvc* user password should not be manually changed in this scenario.

If the ProfessionalPLUS server (and Application Station for distributed Data Collector deployment scenarios) is part of a Windows Workgroup, or is running Windows 2008 R2 or Windows 7, the *ControlLoopSvc* user password must be manually changed on the ProfessionalPLUS server as desired or in accordance with your site's password policy. If the Data Collector is installed on an Application Station, the *ControlLoopSvc* user password must be changed on both the ProfessionalPLUS server and the Application Station.

Note
If the Data Collector is installed on an Application Station, the ProfessionalPLUS *ControlLoopSvc* user password must match the Application Station *ControlLoopSvc* user password.

Procedure

Change the password on the ProfessionalPLUS server.

1. In the Windows start menu, search for **Computer Management**.
2. Expand **System Tools** → **Local Users and Groups** → **Users**.
3. Right-click **ControlLoopSvc** → **Set Password...**.
4. Click **Proceed**.
5. Enter a new password for the *ControlLoopSvc* user. Click **OK** to set the password.

Change the password on the Application Station.

6. If the Data Collector is installed on an Application Station, repeat steps 1-5 on the Application Station using the same password created in step 5.

Update the `DeltaVControlLoopDataProducer` service with the new password created in step 5. Complete these steps on the server where the Data Collector is installed (either the ProfessionalPLUS server or Application Station).

7. In the Windows start menu, search for **Services**.
8. Right-click the `DeltaVControlLoopDataProducer` service and click **Properties**.
9. Click the **Log On** tab. Ensure that **This Account** is selected.
10. Enter the *ControlLoopSvc* user password created in step 5. Click **OK**.
11. Right-click the `DeltaVControlLoopDataProducer` service and click **Restart**.

6.13 Install the KNet ASI

KNet ASI Features

The KNet ASI gathers data from KNet assets and reports key information to Plantweb Optics. After an asset source is configured, information is automatically populated and updated in Plantweb Optics. You can display:

- **Asset Hierarchy**—asset hierarchy defined in the KNet KMap module. If no hierarchy is defined, the KNet Data Collector will send a flat hierarchy to Plantweb Optics.
- **Asset properties**—all properties configured to be displayed in Plantweb Optics from KNet Objects. When a new property is added in KNet Objects and configured to be displayed in Plantweb Optics, the hierarchy and properties list displayed in Plantweb Optics is automatically updated.
- **Asset health**—asset health is calculated based on the health score parameter of a KRCA Problem block. When KRCA Problem blocks are active, the Problem block with the lowest health score will be set as the asset health score. Otherwise, the asset will be marked as healthy. The active root cause is also displayed.
- **Events**—The KNet ASI provides both system and device-specific events. KRCA Problem blocks are the main events gathered by the KNet Data Collector. When an active symptom occurs (Main Problem block), an event is tied to the object and sent to Plantweb Optics.
- **Deviating KPIs**—deviating KPI variable properties (based on the deviation status).

KNet ASI Components

Three components allow the KNet ASI to provide data to Plantweb Optics: the Data Collector, the Connector Service, and the optional Proxy. The Data Collector and Connector Service components must be installed as part of the KNet ASI. The optional Proxy facilitates communication between the Data Collector and the Connector Service when the Data Collector components are separated by multiple network levels. The Data Collector gathers asset source data to send to the Connector Service. The Connector Service then passes information received from the Data Collector, using Microsoft Internet Information Services through HTTPS, to Plantweb Optics.

Note the following regarding the Data Collector, Connector Service, and Proxy:

- The Data Collector and Connector Service can be installed on one or two PCs depending on your network requirements.
- Each Data Collector can communicate with only one Connector Service.
- A Connector Service can receive data from multiple Data Collectors. However, each Connector Service can communicate with only one Plantweb Optics system.
- There can be more than one Data Collector per Plantweb Optics server.

6.13.1 KNet ASI deployment scenarios

Compatibility

The Data Collector gathers data from the KNet asset source and must be installed on the same server where the KNet Online Server is installed. The KNet Data Collector can be deployed on the following KNet and Plantweb Optics systems:

Table 6-6: KNet ASI Compatibility

Data Collector Version	Plantweb Optics Version		KNet Online Server Version	
	<1.5.1	1.5.1	<5.1	5.1
1.5	Not Supported	Supported	Not Supported	Supported

Install KNet ASI Components on Separate PCs

If Plantweb Optics and KNet are on different networks, or are separated by a firewall, you must deploy the KNet Data Collector on the KNet Online Server, and the Connector Service on a different server. If the Data Collector and Connector Service are separated by more than one network level, a Proxy must be deployed on each network level that exists between the Connector Service and the Data Collector. The figure below demonstrates deploying the KNet ASI components with a Proxy facilitating communication between the Data Collector and Connector Service:

Figure 6-6: KNet ASI Components

Before the ASI components can communicate, security certificates must be installed. See Install certificates.

If a Connector Service is already installed and communicating with a Plantweb Optics system, the KNet Data Collector can be configured to communicate with the existing Connector Service, eliminating the need for a new Connector Service.

Install KNet ASI components on a single PC

For a single PC installation, install the KNet Data Collector and Connector Service on the KNet Online Server.

6.13.2 Register the KNet ASI with Plantweb Optics

Before installing the KNet ASI, register the KNet ASI on the Plantweb Optics server. This process allows the ASI to properly create assets in Plantweb Optics.

Prerequisites

- Plantweb Optics is installed on the computer designated as the Plantweb Optics server.
- `A48KNET-DS-0.1.5.X.X.zip` file.

Procedure

1. Extract `A48KNET-DS-0.1.5.X.X.zip`.

   Note
   Extract the zip file to a root directory on the Plantweb Optics server. For example, drive C:

2. Right-click **install.exe** and select **Run as administrator**.
3. Click **Next**.
4. Read and accept the license agreement. Click **Next**.
5. Select **Registration** and click **Next**.
6. Enter the computer name/IP address and port where Plantweb Optics is installed.

   Note
   Port 443 is the default port. If a port is already in use, a red square will surround the port entry field. You must change any port binding that is being used by another website. See page 199 to free up port 443 if it is being used by another application.

7. Click **Finish** to complete the registration process.

Postrequisites

After the registration process is complete, install the KNet Data Collector: Install the KNet Data Collector.

6.13.3 Install the KNet Data Collector

Follow this procedure on the KNet server to install the KNet Data Collector.

Prerequisites

- `A48KNET-DS-0.1.5.X.X.zip` file.
- The Data Collector must be installed on a KNet server, version 5.1
- The PC name or IP address where the Connector Service is installed.
- If deploying the Proxy, the PC name or IP address where the Proxy is installed.
- The KNet ASI registration process has been completed on the Plantweb Optics server. See Register the KNet ASI with Plantweb Optics.

Procedure

1. Extract the `A48KNET-DS-0.1.5.X.X.zip` file on the computer designated for the Data Collector.

   Note
   Extract the zip file on a root directory. For example, drive C.

2. Right-click **KNetDataCollector_Setup.exe** and select **Run as administrator**.
3. Click **Next**.
4. Read the license agreement. If you accept, click **Next**.

5. Select **Data Collector**.
6. Verify the installation destination folder and click **Next**.
7. Enter the PC name/IP address and port number where the Connector Service is installed. Port 443 is the default port. Click **Next**.

   Note
   If using the Proxy service, enter the Proxy server PC name/IP address and port number instead.

8. Enter the local port number the Data Collector will be bound to. Port 443 is the default port.
9. Click **Next** to begin installation of any third-party components listed in the install dialog. Reboot your PC as indicated in the install dialog. Data Collector installation will automatically resume after your PC reboots.
10. Click **Next** to continue installation of third-party components. Click **Finish** to complete the installation.

Postrequisites

After installation, the KNet Data Collector user interface will open in your browser. Continue the ASI installation with Add an asset source to the KNet Data Collector.

6.13.4 Add an asset source to the KNet Data Collector

Prerequisites

- The Connector Service is installed.
- (Optional) The Proxy is installed.
- The Connector Service and (if applicable) Proxy security certificates have been installed on the appropriate servers.
- An asset source is not configured.

Procedure

1. Launch the KNet Data Collector user interface.
   a) Launch Google Chrome or Internet Explorer.
   b) Navigate to `https://`*<Data_Collector_PC_Name>*`/KNetDataCollector` to launch the Data Collector user interface.

      If the Data Collector is bound to a port other than the default port 443, navigate to `https://`*<Data_Collector_PC_Name>:<PortNumber>*`/KNetDataCollector`.

      Replace <*PortNumber*> with the port the Data Collector is bound to and <*Data_Collector_PC_Name*> with the name of the PC where the Data Collector is installed.

2. Click the **+** icon to add a new asset source.
   The *add a new asset source* menu appears.

3. In the **Site** selection box, select the site you want associated with the new asset source.
4. Enter a **Name** for the new asset source. Assets will appear under this name in Plantweb Optics.
5. (Optional) Enter a description for the asset source.
6. Enter the server name, port, callback port, and user credentials that will be used when connecting to KNet.
7. Configure the assets and parameters to display in Plantweb Optics.
    a) Select a Project.
    b) Select the types of assets to send to Plantweb Optics.
    c) For each type of asset, select which parameters to send to Plantweb Optics.

    Note
    If you do not specify specific assets and parameters, all assets and all parameters will be sent to Plantweb Optics.

8. Click **Validate**.
9. (Optional) Select **Include KRCA Screenshots** to include a PDF containing KRCA screenshots when asset messages are delivered to Plantweb Optics.
10. (Optional) Select **Add Logical Hierarchy**.

    When this option is not selected, the hierarchy is only displayed in the Network navigator. The asset source locations displayed in the Location navigator are already bound to the corresponding devices in the Network navigator. To change this setting, you will need to remove and add the asset source again.
11. Click **Add** to finish adding the asset source.

6.14 Install the Plantweb Insight ASI

The Plantweb Insight ASI passes information from the Plantweb Insight System, using Microsoft Internet Information Services, through HTTPS to Plantweb Optics.

The Plantweb Insight ASI must communicate with only one Plantweb Optics installation.

The Plantweb Insight ASI can communicate with up to five Plantweb Insight Systems.

There are two procedures that must be completed in order to install the Plantweb Insight ASI. These are:

1. Registering the Plantweb Insight ASI on the Plantweb Optics server.
2. Installing the Plantweb Insight ASI.

After completing these procedures, return to Step 3 of the *Installing optional services* portion of the *Quick start* chapter and continue your installation.

6.14.1 Register AMS Plantweb Insight ASI on Plantweb Optics Server

After the AMS Plantweb Insight ASI has been installed, you must register the ASI on the Plantweb Optics Server.

Note
The registration steps must be completed using the same user account that installed Plantweb Optics previously.

Prerequisites

- Ensure Plantweb Optics is already installed on the computer you designate as the Plantweb Optics server.
- The `A48INSIGHT-DS0.Plantweb_Insight_ASI.1.5.X.X.zip` file is needed.

Procedure

1. Copy the AMS Plantweb Insight ASI installer to the Plantweb Optics Server.
2. Extract `A48INSIGHT-DS0.Plantweb_Insight_ASI.1.5.X.X.zip`.

   Note
   Extract the zip file on a root directory. For example, drive C.

3. Right-click **install.exe** and select **Run as administrator**.
4. On the **Setup** screen, select **Register AMS Plantweb Insight ASI (on Plantweb Optics Server)**.
5. Read and accept the license agreement. Click **Next**.
6. On the **AMS Plantweb Insight ASI Server Configuration** screen, enter the server name or IP address of the server where the ASI is installed. Click **Next**.

   Note
   Customize may be displayed as an option, but it has no effect on this registration procedure.

7. Click **Done**.

6.14.2 Install the Plantweb Insight ASI

Follow these steps to install the Plantweb Insight ASI.

Prerequisites

- Ensure Plantweb Optics is already installed on the computer you designate as the Plantweb Optics server.
- The `A48INSIGHT-DS0.Plantweb_Insight_ASI.1.5.X.X.zip` file is needed.
- If you install the Plantweb Insight ASI on a separate server, that server must be configured to requirements before installation. The requirements vary depending on the database setup of the Plantweb Optics server.

Procedure

1. Extract `A48INSIGHT-DSO.Plantweb_Insight_ASI.1.5.X.X.zip`.

   Note
   Extract the zip file on a root directory. For example, drive C.

2. Right-click **install.exe** and select **Run as administrator**.
3. Read and accept the license agreement. Click **Next**.
4. If necessary, edit fields in the **Server and Port Binding Configuration** screen, and click **Next**.

Plantweb Optics Server	
Server Name/IP Address	Enter the Plantweb Optics server name or IP address. Be sure not to enter the ASI server.
Note The IP address column in the **Server and Port Binding Configuration** screen should be blank. The site binding does not bind to a specific IP address. **Note** Failure to use the same configuration when installing ASIs and extensions may cause the installation to fail and you will need to uninstall and reinstall Plantweb Optics or any associated ASIs and extensions to use the same server setting.	
Site Binding Information	
Port	The port number when accessing Plantweb Optics. Port 443 is the default port. If a port is already in use, there is a red square around the port number. You must change any port binding that is being used by another website. See page 199 to free up port 443 if it is being used by another application.

5. Select **Install Now** to install with default options.
6. On the **Installation is successful** page, click **Restart Now**. After the system restarts, the AMS Plantweb Insight ASI installation is completed.

6.15 Install the AMS Machinery Manager ASI

There are two components that allow the AMS Machinery Manager ASI to provide data to Plantweb Optics: the Service and the Web Application (Web App). Both components must be installed as part of the whole AMS Machinery Manager ASI.

The Service gathers data from the AMS Machinery Manager database. The Web App passes information from the Service, using Microsoft Internet Information Services, through HTTPS, to Plantweb Optics.

The Service communicates with AMS Machinery Manager and must be installed on an AMS Machinery Manager Network Server.

The components are distributed as a single installation package, but they can be installed on one or two PCs, depending on your network requirements. Each AMS Machinery Manager ASI must communicate with only one Plantweb Optics system. Each AMS Machinery Manager ASI must communicate with only one AMS Machinery Manager.

6.15.1 Install AMS Machinery Manager ASI components on separate PCs

If the Plantweb Optics server and the AMS Machinery Manager PC are on different networks, or are separated by a firewall, you must deploy the Service with the AMS Machinery Manager Network Server, and you can deploy the Web Application, along with Microsoft Internet Information Services (IIS) or IIS Express, on different PCs.

The recommended setup is to install the Web Application on the ASI server station, along with the other ASI Web Applications and the Service on the AMS Machinery Manager Network Server. See Deployment scenarios for more information.

6.15.2 Install AMS Machinery Manager ASI components on a single PC

You can install the AMS Machinery Manager ASI (Service and Web App) on a single PC. That PC must be an AMS Machinery Manager Network Server.

The AMS Machinery Manager ASI can also communicate with Plantweb Optics from a different network. See Deployment scenarios for more information.

6.15.3 Install AMS Machinery Manager ASI web application service

There are two components that allow the AMS Machinery Manager ASI to provide data to Plantweb Optics: the Service and the Web Application. Both components must be installed as part of the whole AMS Machinery Manager ASI. See page 110 to view deployment guidelines.

Prerequisites

- Ensure Plantweb Optics is already installed on the computer you designate as the Plantweb Optics server.
- You need the `A489000-DSO.AMS_MM_ASI.1.5.X.X.zip` file.
- Turn off automatic Windows updates during installation or upgrade.
- If you install the Web App on a separate server, that server must be configured to requirements before installation. The requirements vary depending on if the system's database setup type Tier-1 or Tier-2.
- Make sure all users are logged out of the AMS Machinery Manager system and that no client application (mhm.exe) is running.

⚠ CAUTION

When you install AMS Device Manager ASI and Emerson Wireless Gateway ASI, there is a risk of adding an Emerson Wireless Gateway that is already in Plantweb Optics. Do not connect the same Emerson Wireless Gateway to multiple AMS Device Manager systems. If this happens, duplicate devices, events, and process variables will display in Plantweb Optics.

If your system gets into this unsupported state, contact Emerson Product Support. There is no automated or user-facing methodology available to recover from this condition.

Procedure

1. Extract `A489000-DS0.AMS_MM_ASI.1.5.X.X.zip`.

   Note
   Extract the zip file on a root directory. For example, drive C.

2. Right-click **install.exe** and select **Run as administrator**.
3. Select to install the AMS Machinery Manager ASI Web Application Service and click **Next**.

   Your choice must depend on your network setup and requirements. See page 109 and Deployment scenarios for more information.

4. Read and accept the license agreement. Click **Next**.
5. On the **Default Install Directory** page, change the location where the product will be installed or select the default path provided. Click **Next**.
6. Select **Install Now** to install with default options or **Customize** to change password of the account used to connect to the AMS Machinery Manager server.
   a) If you chose Customize, modify the password for the Sync_Admin user account and click **Next**.

7. Click **Done**.

Return to Step 4 of the *Installing optional services* portion of the *Quick start* chapter and continue your installation.

6.15.4 Install AMS Machinery Manager ASI IO service

There are two components that allow the AMS Machinery Manager ASI to provide data to Plantweb Optics: the Service and the Web Application. Both components must be installed as part of the whole AMS Machinery Manager ASI. See page 110 to view deployment guidelines.

Prerequisites

- Ensure Plantweb Optics is already installed on the computer you designate as the Plantweb Optics server.
- You need the `A489000-DS0.AMS_MM_ASI.1.5.X.X.zip` file.
- Turn off automatic Windows updates during installation or upgrade.

- If you install the Web App on a separate server, that server must be configured to requirements before installation. The requirements vary depending on if the system's database setup type Tier-1 or Tier-2.
- Make sure all users are logged out of the AMS Machinery Manager system and that no client application (mhm.exe) is running.
- Make sure that the AMS Machinery Manager Administrator account has completed the required change password task during first login before installing the AMS Machinery Manager ASI IO Service.

⚠ CAUTION

When you install AMS Device Manager ASI and Emerson Wireless Gateway ASI, there is a risk of adding an Emerson Wireless Gateway that is already in Plantweb Optics. Do not connect the same Emerson Wireless Gateway to multiple AMS Device Manager systems. If this happens, duplicate devices, events, and process variables will display in Plantweb Optics.

If your system gets into this unsupported state, contact Emerson Product Support. There is no automated or user-facing methodology available to recover from this condition.

Procedure

1. Extract `A489000-DS0.AMS_MM_ASI.1.5.X.X.zip`.

   Note
   Extract the zip file on a root directory. For example, drive C.

2. Right-click **install.exe** and select **Run as administrator**.
3. Select to install the AMS Machinery Manager ASI IO Service, and click **Next**.

   Your choice must depend on your network setup and requirements. See page 109 and Deployment scenarios for more information.

4. Read and accept the license agreement. Click **Next**.
5. Enter and confirm the AMS Machinery Manager ASI password.
6. If necessary, edit fields in the **Server and Port Binding Configuration** screen, and click **Next**:

Plantweb Optics Server	
Server Name/IP Address	Enter the Plantweb Optics server name or IP address. Be sure not to enter the ASI server.
Note Failure to use the same configuration when installing ASIs and extensions may cause the installation to fail and you will need to uninstall and reinstall Plantweb Optics or any associated ASIs and extensions to use the same server setting.	

Site Binding Information	
Port	The port number when accessing Plantweb Optics. Port 443 is the default port. If a port is already in use, there is a red square around the port number. You must change any port binding that is being used by another website. See page 199 to free up port 443 if it is being used by another application.

7. Select **Install Now** to install with default options or **Customize** to change password of the account used to connect to the AMS Machinery Manager server.

   If you chose Customize, modify the password for the Sync_Admin user account and click **Next**.

8. Click **Done**.

Return to Step 5 of the *Installing optional services* portion of the *Quick start* chapter and continue your installation.

6.15.5 Register AMS Machinery Manager ASI on Plantweb Optics Server

After the AMS Machinery Manager ASI Web Application Service and the AMS Machinery Manager ASI IO Service have been installed, you must register the ASI on the Plantweb Optics Server.

Note
The registration steps must be completed using the same user account that installed Plantweb Optics previously.

Prerequisites

- Ensure Plantweb Optics is already installed on the computer you designate as the Plantweb Optics server.
- The AMS Machinery Manager ASI Web Application Service and the AMS Machinery Manager ASI IO Service must be installed.
- You need the `A489000-DS0.AMS_MM_ASI.1.5.X.X.zip` file.
- Turn off automatic Windows updates during installation or upgrade.
- Make sure all users are logged out of the AMS Machinery Manager system and that no client application (mhm.exe) is running.

Procedure

1. Copy the AMS Machinery Manager installer to the Plantweb Optics Server.
2. Extract `A489000-DS0.AMS_MM_ASI.1.5.X.X.zip`.

   Note
   Extract the zip file on a root directory. For example, drive C.

3. Right-click **install.exe** and select **Run as administrator**.
4. On the **Setup** screen, select **Register AMS Machinery Manager ASI (on Plantweb Optics Server)**.
5. Read and accept the license agreement. Click **Next**.
6. On the **AMS Machinery Manager ASI Server Configuration** screen, enter the server name or IP address of the server where the ASI is installed. Click **Next**.

Note
Customize may be displayed as an option, but it has no effect on this registration procedure.

7. Click **Done**.

Note
SSL certificates are imported after all Plantweb Optics services and applications have been installed to the system. See page 119.

6.16 Install CMMS Interface

The CMMS Interface supports integration to SAP and IBM Maximo enterprise asset management systems. This installation procedure is optional and is only required if the user wants to use this functionality.

Prerequisites

- Ensure Plantweb Optics is already installed on the computer you designate as the Plantweb Optics server.
- Ensure that the Plantweb Optics certificate has been imported on the system that will host CMMS Interface.
- The `A48CMMS.CMMS_Interface.1.5.X.X.zip` file is needed.
- Turn off automatic Windows updates during installation or upgrade.

Procedure

1. Extract `A48CMMS.CMMS_Interface.1.5.X.X.zip`.

Note
Extract the zip file on a root directory. For example, drive C.

2. Right-click **install.exe** and select **Run as administrator**.
3. Read and accept the license agreement. Click **Next**.
4. Follow either step 5 (SAP installations), or step 6 (IBM Maximo installations) below.
5. If you are using SAP, select **Install Plantweb Optics CMMS - SAP** and click **Next**.
    a) Enter **SAP System Name**.
    b) Enter **SAP Server ID (ASHOST)**.
    c) Enter **SAP Client #**.

d) Click **Next**.

6. If you are using IBM Maximo, select **Install Plantweb Optics CMMS - IBM Maximo** and click **Next**.
   a) Enter **IBM Maximo Host**.
   b) Enter **Maximo Port**.
   c) Click **Next**.
7. On the **Default Install Directory** page, change the location where the product will be installed or select the default path provided. Click **Next**.
8. Select **Install Now** to install with default options or **Customize** to change the installation location.

   If you choose **Customize**, select an installation location and click **Next**.
9. On the **Installation is pending** page, click **Restart Now**.
10. On the **Installation is successful** page, click **Restart Now**. After the system restarts, the CMMS Integration installation is completed.
11. Navigate to the **NLINK Management Module**. Click **Plantweb Optics CMMS**.
12. Click **Edit** and select **Environmental Constants**.
    a) For SAP PM, on the **Environmental Constants** screen, complete these fields:
       1. **NOTIFICATION_STATUS_CANCELLED**. This value indicates the cancelled notification that is received from SAP. Enter **DLFL**.
       2. **NOTIFICATION_STATUS_CLOSED**. This value indicates the closed notification that is received from SAP. Enter **NOCO**.
       3. **ENABLE_TEST_SIMULATION**. This value is generated automatically by the system.
       4. **SIMULATION_START_NUMBER**. This value is generated automatically by the system.
       5. **SAP_LANGUAGE**. Enter **EN**.
       6. **SAP_PASSWORD**. Enter your user password.
       7. **WEB_SERVICE_PORT**. Enter the TCP/IP port to be used by the Web Services server.
       8. **SECURE_MODE**. Enter **1** for HTTPS and authenticating. Enter **0** for HTTP and no authentication.

    b) For IBM Maximo, on the **Environmental Constants** screen, complete these fields:
       1. **MAXAUTH_KEY**. This is the authenticated version of the user name and password. This is a base64 encoded string.
       2. **MAXASSET_SERVICE_URL**. The URL of the server that is hosting the CMMS software.

3. **MXWO_SERVICE_URL**. The URL of the server that is hosting the Maximo software.
4. **NOTIFICATION_STATUS_CANCELLED**. This value indicates the cancelled notification that is received from Maximo. For example, **CAN** would indicate a cancelled notification.
5. **NOTIFICATION_STATUS_CLOSED**. This value indicates the closed notification that is received from Maximo. For example, **COMP** or **CLOSE** would indicate a closed notification.
6. **WEB_SERVICE_PORT**. NLINK assigns a port that CMMS Interface uses for its connection. This port number is that NLINK port. This should be the same port as is indicated on the CMMS Service Configuration page.
7. **SECURE_MODE**. This value is set to **1** if SSL is being used. It is set to **0** if SSL is not being used.

Return to Step 6 of the *Installing optional services* portion of the *Quick start* chapter and continue your installation.

6.17 Install the Plantweb Optics OPC UA Server

Install the Plantweb Optics OPC UA Server to provide OPC UA data to OPC UA clients.

The Plantweb Optics OPC UA Server lets you read OPC UA data from OPC UA clients. It may be installed on the same server where the other components of Plantweb Optics are installed, or it may be installed on a different server.

Prerequisites

- Allow AMS Machinery Manager and AMS Device Manager hierarchies in the Asset Explorer utility to become populated with initial data before installing the Plantweb Optics OPC UA Server.
- Ensure Plantweb Optics is already installed on the computer you designate as the Plantweb Optics server.
- If you are installing the Plantweb Optics OPC UA Server on a different computer from the other components of Plantweb Optics, ensure that the Plantweb Optics server certificate has been installed on the computer where you want to install the OPC UA Server.
- The `A48OPTICS-SYSTEM0.Plantweb_Optics_Install.1.5.X.X.zip` file is needed.
- Turn off automatic Windows updates during installation or upgrade.

Procedure

1. Extract the `A48OPTICS-SYSTEM0.Plantweb_Optics_Install.1.5.X.X.zip` file.

Note
Extract the zip file on a root directory. For example, drive C.

2. Right-click **install.exe** and select **Run as administrator**.
3. Select **Install Plantweb Optics OPC UA Server**, and click **Next**.
4. Read and accept the license agreement. Click **Next**.
5. Edit fields in the **Plantweb Optics Server Configuration** screen, and click **Next**.

Server Configuration	Enter the Plantweb Optics server name or IP address. Be sure not to enter the ASI server. In the **Port** field, enter **443**.

6. Select **Install Now**.
7. Click **Done**.

Note
Building the plant hierarchy can take several minutes after installation or reboot of Plantweb Optics. Allow several minutes after installation or reboot before attempting to connect OPC UA clients.

Return to Step 7 of the *Installing optional services* portion of the *Quick start* chapter and continue your installation.

6.18 Configure Active Directory for Plantweb Optics

Before configuring Active Directory, ensure that Active Directory has been installed and that Active Directory Domain Services and Active Directory Federation Services have been set up. Then, complete the following steps to configure Active Directory Federation Services to add Plantweb Optics as an authorized client.

Procedure

1. Open **Server Manager**.
2. Click **Tools** at the top right of the screen.
3. Click **AD FS Management** in the list on the right side of the screen. The **AD FS** screen displays.
4. Right click **Application Groups** on the left side of the screen.
5. Click **Add Application Group**. The **Add Application Group Wizard** screen displays.
6. In the **Name** field, enter an Application Group name of your choosing. Click **Server Application**. Click **Next**. The **Server application** screen displays.
7. On the **Server application** screen, copy the contents of the system-generated **Client identifier** field into Notepad for use during the Configure Plantweb Optics OIDC settings procedure.
8. Under **Redirect URI**, add the following information:

For each of the three URIs, replace <HOSTNAME> with the hostname of the server where Plantweb Optics is installed, and <CALLBACK> with a user defined value. Use the same <CALLBACK> for every URI.

Note

Copy the <CALLBACK> into Notepad for use during the configuration procedure. See Configure Plantweb Optics OIDC settings.

a) https://<HOSTNAME>/opticsidsrv/<CALLBACK>

b) https://<HOSTNAME>/OnPremMobileServices/<CALLBACK>

c) https://opticsmobilesvc.azurewebsites.net/<CALLBACK>

For example, if your <HOSTNAME> is win-82phv0vjau3 and your <CALLBACK> is adfs, the three URIs would look like this:

a) https://win-82phv0vjau3/opticsidsrv/adfs

b) https://win-82phv0vjau3/OnPremMobileServices/adfs

c) https://opticsmobilesvc.azurewebsites.net/adfs

9. On the **Configure Application Credentials** screen, click the **Generate a shared secret** checkbox. The **Secret** field populates. Click **Copy to clipboard**. Click **Next**. The **Summary** screen displays.
10. Copy the new secret into Notepad for use during the Configure Plantweb Optics procedure. See Configure Plantweb Optics OIDC settings.
11. Click **Next**.
12. Continue clicking **Next** until you reach the last screen, then click **Close**.
13. The **Application Groups** screen displays showing the new Application Group.

Return to Step 1 of the *Completing post-installation steps* portion of the *Quick start* chapter and continue your installation.

6.19 Configure Plantweb Optics OIDC settings

Before configuring Plantweb Optics, ensure that Active Directory has been configured. See Configure Active Directory for Plantweb Optics. Then, complete the following steps.

Procedure

1. Log in to Plantweb Optics and open **User Manager**.
2. Click the **Settings** tab.
3. Click **OIDC Settings** on the ribbon, the **OpenID Connect Settings** screen displays.
4. On the left side of the **OpenID Connect Settings** screen, click **New OpenID Connect Provider** and enter the following values:

   a) **Claim Type**: Enter **http://schemas.xmlsoap.org/we/2005/05/identify/claims/upn** in the **Claim Type** field.

   b) **Display Name**: User defined. For example, **ADFS**.

c) **Scheme Name**: User defined. For example, **adfs**. The **Scheme Name** must be unique and cannot be the same name as another OpenID Connect Provider in Plantweb Optics.

d) **Authority**: Use this format for this field, **https://<YOUR ACTIVE DIRECTORY SERVER>/adfs/**.

e) **Callback path**: Enter the saved <CALLBACK> that you pasted into Notepad during the Configure Active Directory procedure. This is the last node of the URI address that you created. See Configure Active Directory for Plantweb Optics. For example, **/adfs**.

f) **Client ID**: Enter the saved **Client ID** that you pasted into Notepad during the Configure Active Directory procedure. See Configure Active Directory for Plantweb Optics.

g) **Enable Client Secret**: Click this checkbox.

h) **Client Secret**: Enter the displayed result that you pasted into Notepad during the Configure Active Directory procedure. See Configure Active Directory for Plantweb Optics.

5. Restart Plantweb Optics to display the changes in the login page. On the Plantweb Optics server, either restart the server or enter **iisreset** in a command prompt.
6. Login to Plantweb Optics and open User Manager. Open the list of users and select the one you want to be linked with Active Directory.
7. Click **Edit Logins** in the ribbon. The **Edit Logins** screen displays.
8. On the **Edit Logins** screen, in the **OpenID Connect Provider** field, select the OpenID Connect Provider that was created earlier in this procedure. For example, ADFS. For the **Claim Value**, enter the user's UPN (the credentials used to log in to Active Directory, usually the user's email address). Click **OK**.
9. Sign out of Plantweb Optics.
10. Log back in to Plantweb Optics by clicking a button under **External Account**. The External Account button will show the display name of the OpenID Connect Provider that was entered earlier. The Plantweb Optics sign in screen displays. The configuration is complete.

Return to Step 1 of the *Completing post-installation steps* portion of the *Quick start* chapter and continue your installation.

6.20 Install certificates

SSL certificates are imported after all web services (such as Plantweb Optics Web Service, ASI web applications or Data Collectors, and services) have been installed to the system. If you wish to manually export and install certificates instead of performing the operations described in this procedure, see Export a security certificate.

If you are installing a certificate on a Windows Server 2008 R2 machine, additional installation steps are required beyond the process described in this procedure. See Install certificates on Windows Server 2008 R2 for more information.

Perform these steps to complete SSL certification for most installation types. For more information about certificates and general procedures, refer to SSL/TLS certificates.

Note
When installing the OPC UA Server on a separate server from Plantweb Optics, you must install the Plantweb Optics Certificate before you install Plantweb Optics OPC UA Server.

When connecting an ASI to Plantweb Optics, the following certificates must be installed on the listed servers:

Table 6-7: ASI Certificates

Server	Certificate Required
Data Collector sending data to a Proxy	Proxy
Data Collector sending data directly to a Connector Service	Connector Service
Connector Service	Plantweb Optics
Proxy sending data to a Connector Service	Connector Service
Proxy sending data to another Proxy	Proxy
AMS Asset Monitor Data Collector	Asset source security certificate

When using the Proxy, the Proxy server must have either a Connector Service certificate or Proxy certificate installed depending on where the Proxy directs data. If using multiple proxies in your deployment, any Proxy that sends data to another Proxy must have a Proxy certificate installed. The Data Collector server must have either a Proxy or Connector Service certificate installed, depending on whether the Data Collector communicates directly with the Connector Service or with a Proxy.

Procedure

1. To install the Plantweb Optics certificates on an ASI server or Connector Service PC, or on a client PC, browse to the Plantweb Optics server and complete these steps:

   The Plantweb Optics certificate is required on any computer you use to access the utilities by web browser, or on any server that has web services that communicate with the Plantweb Optics Web Service.

   a) Launch Internet Explorer.

   b) Enter **https://<Optics_Server_Name>/Assetexplorer**.

   c) Click **Continue to this website**.

   d) If necessary, click **Continue to this website** again.

   e) The **Plantweb Optics Login** screen displays. A **certificate error** displays in the URL path of the browser.

   f) Click **Certificate error** in the URL path of the browser.

   g) Click **View certificates**.

   h) Click **Install certificate...** to open the **Certificate Import Wizard**.

   i) Select **Local Machine**. Click **Next**.

Note
If installing a certificate on Windows Server 2008 R2, this option is not displayed.

j) Click **Place all certificates in the following store** and click **Browse**.

k) Select **Trusted Root Certification Authorities**. Click **OK**. Click **Finish**.

2. To install the Connector Service certificate, complete these steps on the Proxy or Data Collector server:

   a) Launch Internet Explorer.

   b) Enter **https://<Connector_Service_Server_Name>/connectorservice**.

   c) Click **Continue to this website**.

   d) If necessary, click **Continue to this website** again. A **certificate error** displays in the URL path of the browser.

   e) Click **Certificate error** in the URL path of the browser.

   f) Click **View certificates**.

   g) Click **Install certificate...** to open the **Certificate Import Wizard**.

   h) Select **Local Machine**. Click **Next**.

   Note
   If installing a certificate on Windows Server 2008 R2, this option is not displayed.

   i) Click **Place all certificates in the following store** and click **Browse**.

   j) Select **Trusted Root Certification Authorities**. Click **OK**. Click **Finish**.

3. To install the Proxy certificate, complete these steps on the Proxy or Data Collector server:

   a) Launch Internet Explorer.

   b) Enter **https://<Proxy_Server_Name>/Proxy**.

   c) Click **Continue to this website**.

   d) If necessary, click **Continue to this website** again. A **certificate error** displays in the URL path of the browser.

   e) Click **Certificate error** in the URL path of the browser.

   f) Click **View certificates**.

   g) Click **Install certificate...** to open the **Certificate Import Wizard**.

   h) Select **Local Machine**. Click **Next**.

Note

If installing a certificate on Windows Server 2008 R2, this option is not displayed.

i) Click **Place all certificates in the following store** and click **Browse**.

j) Select **Trusted Root Certification Authorities**. Click **OK**. Click **Finish**.

4. To install the AMS Machinery Manager ASI certificates, navigate to the Plantweb Optics server and complete these steps **https://<ASI _Server_Name>/MMmanager**:

   a) Launch Internet Explorer.

   b) Enter **https://<ASI _Server_Name>/MMmanager**.

   c) Click **Continue to this website**.

   d) If necessary, click **Continue to this website** again. A **certificate error** displays in the URL path of the browser.

   e) Click **Certificate error** in the URL path of the browser.

   f) Click **View certificates**.

   g) Click **Install certificate...** to open the **Certificate Import Wizard**.

   h) Select **Local Machine**. Click **Next**.

   Note

   If installing a certificate on Windows Server 2008 R2, this option is not displayed.

   i) Click **Place all certificates in the following store** and click **Browse**.

   j) Select **Trusted Root Certification Authorities**. Click **OK**. Click **Finish**.

5. To install the AMS Asset Monitor asset source certificate, complete these steps on the Data Collector server the asset source is associated with:

   a) Launch Internet Explorer.

   b) Enter **https://<Asset_Monitor_asset_source_IP_Address>**.

   c) Click **Continue to this website**.

   d) If necessary, click **Continue to this website** again. A **certificate error** displays in the URL path of the browser.

   e) Click **Certificate error** in the URL path of the browser.

   f) Click **View certificates**.

   g) Click **Install certificate...** to open the **Certificate Import Wizard**.

   h) Select **Local Machine**. Click **Next**.

Note
If installing a certificate on Windows Server 2008 R2, this option is not displayed.

i) Click **Place all certificates in the following store** and click **Browse**.

j) Select **Trusted Root Certification Authorities**. Click **OK**. Click **Finish**.

If installing certificates on Windows Server 2008 R2, continue the remaining steps listed in Install certificates on Windows Server 2008 R2. Otherwise, return to Step 2 of the *Completing post-installation steps* portion of the *Quick start* chapter and continue your installation.

6.20.1 Install certificates on Windows Server 2008 R2

Additional steps are required if installing certificates on a Windows Server 2008 R2 operating system.

Procedure

Install all required certificates on your Windows Server 2008 R2 machine.

1. Complete Install certificates to install any certificates required on your Windows Server 2008 R2 machine.

   Note
   Because the Windows Server 2008 R2 certificate installation wizard does not provide an option to install certificates to the local machine (and will install certificates for the current user only), additional export and installation processes described below must be completed.

Export all required certificates to your Windows Server 2008 R2 machine.

2. On your Windows Server 2008 R2 machine, follow Export a security certificate to export the certificates installed in step 1 of this procedure to the same Windows Server 2008 R2 machine.

Import all required certificates to your Windows Server 2008 R2 machine.

3. On your Windows Server 2008 R2 machine, click **Start** and search for **mmc**.
   The Microsoft Management Console will appear.
4. Click **File** → **Add/Remove Snap-in**.
5. From the **Available snap-ins** panel, add **Certificates**.
   The **Certificates snap-in** window appears.
6. Select **Computer account** and click **Next**.
7. Ensure **Local computer** is selected and click **Finish**.
8. Click **OK** in the **Add or Remove Snap-ins** window.
   The **Certificates** folder will appear in the Microsoft Management Console under **Console Root**.
9. Expand **Console Root** → **Trusted Root Certification Authorities** → **Certificates**.
10. Right-click the **Certificates** folder.
11. Select **Folder** → **All Tasks** → **Import**.

The Certificate Import Wizard appears.

12. Click **Next**.
13. Click **Browse**. Navigate to the certificate exported in step 2 and click **Open**.
14. Click **Next**.
15. Ensure **Place all certificates in the following store: Trusted Root Certification Authorities** is selected and click **Next**.
16. Click **Finish**.
17. Repeat steps 10-16 for each certificate exported in step 2.

Postrequisites

Return to Step 2 of the *Completing post-installation steps* portion of the *Quick start* chapter and continue your installation.

6.20.2 Export a security certificate

This procedure covers manually exporting an SSL certificate and is an alternative method to Install certificates. Perform this procedure on the server containing the certificate you wish to export.

Procedure

1. On the server containing the desired SSL certificate (Plantweb Optics, Connector Service, ASI server, or Proxy), enter `certmgr.msc` on the **Start** screen. Press **Enter**.
2. Expand `Trusted Root Certification Authorities` and select **Certificates**.
3. Right-click the desired certificate and select **All Tasks** → **Export**.

   To quickly find the certificate, look for the certificate name under the **Friendly Name** column. For a list of Plantweb Optics certificates, see System components with certificates.
4. Click **Next**.
5. Select **No, do not export the private key**.
6. Click **Next**.
7. Select **DER encoded binary X.509 (.CER)**.
8. Browse to a location where you want to save the certificate and enter a file name.
9. Click **Save.**
10. Click **Next.**
11. Click **Finish.**

Postrequisites

Import the newly exported certificate to the desired server. See Import a security certificate. Or, if you are installing certificates on Windows Server 2008 R2, return to Install certificates on Windows Server 2008 R2

6.20.3 Import a security certificate

If manually installing SSL certificates, follow this procedure after exporting the desired certificate.

Procedure

1. Copy the certificate file you exported in Export a security certificate to the server you wish to install the security certificate on.
2. Double-click the certificate file.
3. Click **Install Certificate**.
4. Select **Local Machine** and click **Next**.
5. Click **Next.**
6. Select **Place all certificates in the following store**.
7. Click **Browse** and select **Trusted Root Certification Authorities**.

6.21 Connect to OPC server

Follow these instructions to run the OPC Client (UaExpert) system and connect to the OPC Server.

Procedure

1. From your Desktop, run the **UAExpert OPC Client**.
2. Add the OPC Server by clicking on the + sign.
3. Click on **<Double click to Add Server>**.
4. Before clicking **OK**, choose if you prefer to connect via username and password or by providing the OPC UA Client's Certificate. See page 177. Click **OK**.
5. Using the Server Hierarchy (on the left side of the screen), right-click on the OPTICS Server and click **Connect**.

Return to Step 6 of the *Completing post-installation steps* portion of the *Quick start* chapter and continue your installation.

6.22 Configure how emails are sent to Plantweb Optics

The SMTP configuration utility is used to configure how emails are sent in Plantweb Optics. To run the SMTP configuration utility, navigate to `C:\inetpub\wwwroot\EmersonCSI\Tools\SMTP` and open a command prompt with elevated privileges.

Table 6-8: SMTP Configuration Utility Commands

Operation	Command
Manually set the username and password used to authenticate with the SMTP server	`SMTPConfig.exe cred -u "YOUR_USERNAME" -p "YOUR_PASSWORD"`

Table 6-8: SMTP Configuration Utility Commands *(continued)*

Operation	Command
Enable (or disable) the use of default credentials instead of manually setting username and password	`SMTPConfig.exe usedefaultcreds` `SMTPConfig.exe usedefaultcreds --disable`
Set the email address and header used when sending an email	`SMTPConfig.exe from -e` *"donotreply@emerson.com"* `-h` *"Plantweb Optics"*

Configure the connection to the SMTP server	`SMTPConfig.exe connection -h` *"smtp.sendgrid.net"* `-p 25`
	`SMTPConfig.exe connection -h` *"smtp.sendgrid.net"* `-p 587 --usessl`
	`SMTPConfig.exe connection -h` *"smtp.sendgrid.net"* `-p 25 --spn` *“YOUR_SPN”* `--cdn` *“YOUR_CDN”*

Switch between using the SMTP and HTTP interfaces to deliver email	`SMTPConfig.exe usesmtp` `SMTPConfig.exe usesmtp --disable`
Display current settings	`SMTPConfig.exe getsettings`
Restore all settings to defaults	`SMTPConfig.exe reset`
Configure mail delivery settings See the table below, **Delivery Methods**, for an explanation of the delivery methods and formats	`SMTPConfig.exe delivery -m` *"network"* `-f` *"sevenbit"* `SMTPConfig.exe delivery -m` *"iis"* `-f` *"international"* `SMTPConfig.exe delivery -m` *"custom"* `-f` *"international"* `-d` *"C:\MailDirectory"*

Table 6-9: Delivery Methods

Delivery Method	Description
Network	Email is sent through the network to an SMTP server
Iis	Email is copied to the pickup directory used by a local Internet Information Services (IIS) for delivery
Custom	Email is copied to the directory specified for delivery by an external application

Table 6-10: Delivery Formats

Delivery Format	Description

Table 6-10: Delivery Formats *(continued)*

SevenBit	A delivery format using 7-bit ASCII. The traditional delivery format used in the Simple Mail Transport Protocol (SMTP) for mail messages.
International	A delivery format where non-ASCII characters in the envelope and header fields used in the Simple Mail Transport Protocol (SMTP) for mail messages are encoded with UTF-8 characters. The extensions to support international email are defined in IETF RFC 6530, 6531, and 6532.

7 Client installation procedures

On the Plantweb Optics client, you can install the following:

- AMS Device Manager Launcher
- AMS Machinery Manager Launcher

The AMS Machinery Manager Launcher can also be installed on the Plantweb Optics server.

7.1 Install the AMS Device Manager Launcher

The AMS Device Manager Launcher lets you use AMS Device Manager with Plantweb Optics, so long as AMS Device Manager is installed on the client PC. The AMS Device Manager Launcher is a client application that is recommended to be installed *only* on client machines. AMS Device Manager is available after you install the AMS Device Manager ASI.

The AMS Device Manager Launcher is different from the AMS Device Manager ASI. The AMS Device Manager Launcher lets you launch AMS Device Manager in context from the Asset Explorer or Asset View utility. The AMS Device Manager ASI extends that functionality by letting you bring AMS Device Manager alerts, device data, and hierarchy into Plantweb Optics.

Prerequisites

- Ensure Plantweb Optics is already installed on the computer you designate as the Plantweb Optics server.
- Turn off automatic Windows updates during installation or upgrade.

Procedure

1. Open a browser, type `https://[server]:[port number]/DM`.

   Where `[server]` is the computer name or IP address of the Plantweb Optics server and `[port number]`, if required, is the port number assigned for Plantweb Optics.

   Note
   Enter the server name or IP address, depending on the configuration you set during installation of Plantweb Optics.

2. On the AMS Device Manager Launcher installation page, click **Install**.
3. Run the application.
4. Click **Next**.
5. Enter the name or IP address of the Plantweb Optics server, and click **Next**.

   Note
   Use the same server setting, either IP address or server name as the Plantweb Optics configuration, when installing or upgrading components, ASIs, or extensions. For example, when you choose the **Use Server Name** option in the Server and Port Binding Configuration screen during the installation, you must enter the name of the Plantweb Optics server.

Failure to use the same configuration as Plantweb Optics when installing or upgrading components, ASIs, and extensions may cause the installation to fail and you will need to uninstall and reinstall the software to configure the same server setting.

6. Click **Install**.
7. Click **Finish** when done.

7.2 Install the AMS Machinery Manager Launcher

The AMS Machinery Manager Launcher lets you use AMS Machinery Manager with Plantweb Optics, so long as the AMS Machinery Manager client is installed on the PC. This is a Windows application that can be installed on client computers and also on the Plantweb Optics server. The AMS Machinery Manager Launcher is available after you install the AMS Machinery Manager ASI.

The AMS Machinery Manager Launcher is different from the AMS Machinery Manager ASI. The AMS Machinery Manager Launcher lets you launch AMS Machinery Manager in context from the Asset Explorer or Asset View utility. The AMS Machinery Manager ASI extends that functionality by letting you bring AMS Machinery Manager alerts, data, and hierarchy into Plantweb Optics.

Prerequisites

- Ensure Plantweb Optics is already installed on the computer you designate as the Plantweb Optics server.
- Turn off automatic Windows updates during installation or upgrade.

Procedure

1. Open a browser, type `https://[server]:[port number]/MMLauncher`.

   Where `[server]` is the computer name or IP address of the Plantweb Optics server and `[port number]`, if required, is the port number assigned for Plantweb Optics.

   Note
   Enter the server name or IP address, depending on the configuration you set during installation of Plantweb Optics.

2. On the AMS Machinery Manager Launcher installation page, click **Install**.
3. Run the application.
4. Click **Next**.
5. Enter the name/IP address and port number of the server where the AMS Machinery Manager ASI Web App is installed, and click **Next**.

   Note
   Use the same server setting, either IP address or server name as the Plantweb Optics configuration, when installing or upgrading components, ASIs, or extensions. For example, when you choose the **Use Server Name** option in the Server and Port Binding Configuration screen during the installation, you must enter the name of the Plantweb Optics server.

Failure to use the same configuration as Plantweb Optics when installing or upgrading components, ASIs, and extensions may cause the installation to fail and you will need to uninstall and reinstall the software to configure the same server setting.

6. Click **Install**.
7. Click **Finish** when done.

8 Mobile installation procedures

8.1 Install the Plantweb Optics Mobile App

The Plantweb Optics Mobile App is available for download from the Google Play™ Store or the Apple® AppStore™. This app allows you to display, send, and receive Plantweb Optics messages and notifications from your mobile device.

Procedure

1. On your mobile device, open the Google Play™ Store or the Apple® AppStore™.
2. In the search bar, type `Plantweb Optics Mobile App`.
3. Choose to install, and accept permissions.

9 Uninstall Plantweb Optics

Prerequisites

Uninstall Plantweb Optics and its components in the following order:

1. AMS Machine Works Vibration Analyzer
2. AMS Device Manager Launcher
3. AMS Machinery Manager Launcher
4. Plantweb Optics OPC UA server
5. AMS Machine Works
    - AMS Machine Works AMS 6500 ATG Interface
    - AMS Machine Works Wireless Interface
    - AMS Machine Works Interface Router
    - AMS Machine Works Historian
    - AMS Machine Works Web Services
6. Emerson Wireless Gateway ASI
7. Connector Service
8. Proxy
9. Data Collectors
10. AMS Machinery Manager ASI Service and Web App[1]
11. Plantweb Insight ASI
12. Plantweb Optics Web Services
13. Plantweb Optics Historian

Note
Steps for uninstalling the software can differ depending on your operating system.

Note
Uninstalling the application does not unregister it. For example, if you uninstall Emerson Wireless Gateway, the **Add Asset Source** button remains on the ribbon in Asset Explorer. If you then reinstall Emerson Wireless Gateway on a different server than the original, the **Add Asset Source** button will remain, but will not function properly until you once again run the Emerson Wireless Gateway registration targeting the new server.

Procedure

1. From the Control Panel, select **Add or Remove Programs**, select the component, and click **Uninstall**.

1 *Make sure all users are logged out of the AMS Machinery Manager Network Server and that the application is not running prior to uninstalling this component.*

2. The installation wizard launches.
3. On the wizard, click **Uninstall**.
4. Follow the prompts and click **Next**.
5. Restart your computer.

10 Upgrade from a previous version

Important
Back up your databases before starting the upgrade. See page 197 for more information.

Emerson recommends you complete the upgrade of the software and all its components before using the upgraded Plantweb Optics system, and that you upgrade in this order:

1. Uninstall the following ASIs prior to upgrading Plantweb Optics: AMS Device Manager ASI, Plantweb Insight ASI, and Emerson Wireless Gateway ASI.
2. Plantweb Optics

   Note
   You must upgrade Plantweb Optics before upgrading all other components.

3. AMS Machine Works

   Note
   If a user wants to upgrade to a distributed system, then it is not a direct upgrade. Those instructions are addressed in a Knowledge Base Article (KBA).

4. AMS Machinery Manager ASI
5. Emerson Wireless Gateway ASI [2]
6. AMS Device Manager ASI [3]
7. Plantweb Insight ASI [4]

   Note
   The Plantweb Insight ASI configuration file must be saved before uninstalling the Plantweb Insight ASI. Copy the asiconfig.json file from the installation location (typically C:\inetpub\wwwroot\EmersonCSI\InsightAsi)
   The configuration file will need to be copied back to the installation folder once the upgraded Plantweb Insight ASI is installed.

10.1 Plantweb Optics upgrade path

The supported upgrade paths for Plantweb Optics, ASIs, components, and complementary products are shown in the tables below.

2 *You must uninstall and reinstall this component.*
3 *You must uninstall and reinstall this component.*
4 *You must uninstall and reinstall this component.*

Table 10-1: Plantweb Optics upgrade path

Plantweb Optics Version	Upgrade to		
	Plantweb Optics 1.4 (general release)	**Plantweb Optics 1.5**	**Plantweb Optics 1.5.1**
Plantweb Optics 1.4.x (general release)	N/A	Supported	Supported
Plantweb Optics 1.5	N/A	N/A	Supported

Table 10-2: ASI upgrade path

ASI versions	Upgrade to ASI version		
	ARES 1.4 (managed release)	**Plantweb Optics 1.4 (general release)**	**Plantweb Optics 1.5**
Emerson Wireless Gateway 1.3.x	Supported	Supported	Not supported
Emerson Wireless Gateway 1.4.x (managed release)	N/A	Supported	Not supported
Emerson Wireless Gateway 1.4.x (general release)	N/A	N/A	Supported
AMS Device Manager ASI 1.4.x (managed release)	N/A	Supported	Not supported
AMS Device Manager ASI 1.4.x (general release)	N/A	N/A	Supported
AMS Machinery Manager ASI 1.4.x (general release)	N/A	N/A	Supported
Plantweb Insight ASI 1.0.x	N/A	N/A	Supported

10.2 Upgrade Plantweb Optics

Prerequisites

Important
Back up your databases before starting the upgrade. See page 197 for more information.

Note
If you are currently using Plantweb Optics version 1.4 and want to install Plantweb Optics version 1.5, use this upgrade procedure. Do not uninstall version 1.4 or you will corrupt your data.

Note
If you are using a Tier-2 system (separate MS SQL Server) then MS SQL needs to be upgraded to version 2017 and you must enable filestream before upgrading Plantweb Optics. See page 205 for more information.

- You need the `A48OPTICS-SYSTEM0.Plantweb_Optics.1.5.X.X.zip` file.
- Turn off automatic Windows updates during installation or upgrade.

Procedure

1. Extract the `A48OPTICS-SYSTEM0.Plantweb_Optics.1.5.X.X.zip` file.

   Note
   Extract the zip file on a root directory. For example, drive C.

2. Right-click **install.exe** and select **Run as administrator**.
3. Select **Install Plantweb Optics Web Services** and click **Next**.
4. Click **Upgrade**.
5. Click **Restart Now**.

10.3 Upgrade AMS Machinery Manager ASI Web Service

Follow these steps to upgrade the AMS Machinery Manager ASI Web Service.

Note
If you are currently using Plantweb Optics version 1.4 and want to install Plantweb Optics version 1.5, use this upgrade procedure. Do not uninstall version 1.4 or you will lose all of your imported databases.

Prerequisites

- You need the `A489000-DS0.AMS_MM_ASI.1.5.X.X.zip` file.
- Turn off automatic Windows updates during installation or upgrade.

Procedure

1. Extract the `A489000-DS0.AMS_MM_ASI.1.5.X.X.zip` file on a root directory. For example, drive C.
2. Right-click **install.exe** and select **Run as administrator**.
3. Select **Install AMS Machinery Manager Web Service**. Click **Next**.
4. Click **Upgrade**.
5. Click **Restart Now**.

10.4 Upgrade AMS Machinery Manager ASI IO Service

Follow these steps to upgrade the AMS Machinery Manager ASI IO Service.

Note

If you are currently using Plantweb Optics version 1.4 and want to install Plantweb Optics version 1.5, use this upgrade procedure. Do not uninstall version 1.4 or you will lose all of your imported databases.

Prerequisites

- You need the `A489000-DS0.AMS_MM_ASI.1.5.X.X.zip` file.
- Turn off automatic Windows updates during installation or upgrade.
- You must have previously upgraded AMS Machinery Manager Web Service to version 1.5.
- You must have previously upgraded AMS Machinery Manager Server to version 6.3.
- You must have changed the password of the AMS Machinery Manager Administrator account on the first login after upgrading AMS Machinery Manager from version 5.7.1 to 6.3.
- Before upgrading, force stop the AMS Machinery Manager ASI IO Service.

Procedure

1. Extract the `A489000-DS0.AMS_MM_ASI.1.5.X.X.zip` file on a root directory.
   For example, drive C.
2. Right-click **install.exe** and select **Run as administrator**.
3. Select **Install AMS Machinery Manager IO Service**. Click **Next**.
4. Click **Upgrade**.
5. Click **Restart Now**.

10.5 Execute Machinery Manager ASI Registration on Plantweb Optics Server

Follow these steps to execute the Machinery Manager ASI registration on the Plantweb Optics Server.

Note

If you are currently using Plantweb Optics version 1.4 and want to install Plantweb Optics version 1.5, use this upgrade procedure. Do not uninstall version 1.4 or you will lose all of your imported databases.

Prerequisites

- You need the `A489000-DS0.AMS_MM_ASI.1.5.X.X.zip` file.
- Turn off automatic Windows updates during installation or upgrade.

- You must have previously upgraded AMS Machinery Manager Web Service to version 1.5.

Procedure

1. Extract the `A489000-DS0.AMS_MM_ASI.1.5.X.X.zip` file on a root directory.
   For example, drive C.
2. Right-click **install.exe** and select **Run as administrator**.
3. Select **Install Register AMS Machinery Manager ASI (on Plantweb Optics Server)**. Click **Next**.
4. Click **Install**.
5. Click **Restart Now**.

10.6 Upgrade Emerson Wireless Gateway ASI

Prerequisites

- The `A481420-DS0.EWG_ASI.1.5.X.X.zip` file is needed.
- Turn off automatic Windows updates during installation or upgrade.
- Ensure Plantweb Optics is upgraded first.

Note
The **Upgrade** option in the ASI installer is not supported at this time.

Procedure

1. Uninstall the Emerson Wireless Gateway ASI.
   See page 135 for uninstall instructions.
2. Register the Emerson Wireless Gateway ASI. See page 74 for instructions.
3. Install the Emerson Wireless Gateway ASI. See page 76 for instructions.

10.7 Upgrade AMS Device Manager ASI

This process guides you through upgrading an existing AMS Device Manager ASI from version 1.5 to version 1.5.1 while maintaining asset source information including asset source configuration and device history.

Prerequisites

- The `A488000-DS0.AMS_DM_ASI.1.5.X.X.zip` file is needed.
- Turn off automatic Windows updates during installation or upgrade.
- Ensure Plantweb Optics is upgraded first.

Procedure

1. Uninstall the AMS Device Manager ASI version 1.5 Web Application and ASI Service.

Note
Uninstalling the ASI Service and Web Application will not erase asset source data or asset history.

2. Install the Connector Service. See Install the Connector Service.
3. (Optional) Install and configure the Proxy. See Install the Proxy and Configure the Proxy.
4. Register the AMS Device Manager ASI with Plantweb Optics. See Register the AMS Device Manager ASI with Plantweb Optics.
   Asset source data from the previous AMS Device Manager ASI installation will be automatically prepared for migration during this step. Each previous asset source and its history will be extracted to an `assetsources.json` file and placed in `C:\Temp\Migrations\AMSDeviceManager` on the Plantweb Optics PC. Asset source files will be transferred to the Data Collector in a later step.
5. Install the AMS Device Manager Data Collector on each AMS Device Manager asset source previously connected to Plantweb Optics. See Install the AMS Device Manager Data Collector.

   If multiple AMS Device Manager asset sources will be connected to Plantweb Optics, each asset source must have a Data Collector installed.

   Note
   Do not configure an asset source in the Data Collector. Asset source configuration will be performed automatically when the previous asset source data is migrated in the next step.

6. Copy the `assetsources.json` file generated during the registration process to `C:\inetpub\wwwroot\EmersonCSI\AMSDeviceManagerDataCollector` on the AMS Device Manager server associated with the asset source.

   Note
   If multiple asset sources were configured in Plantweb Optics prior to performing the upgrade procedure, an `assetsources.json` file will be generated for each asset source. Each `assetsources.json` must be placed on the associated AMS Device Manager server.

7. Modify the permissions of `assetsources.json`.
   a) Right-click `assetsources.json` and click **Properties**.
   b) Select the **Security** tab.
   c) Under the **Group or user names** box, click **Edit**.
   d) Click **AmsServiceUser**.
   e) Under the **Permissions for AmsServiceUser** box, check **Modify: Allow**.
   f) Click **OK**.
   g) Restart the AMS Device Manager server.
      Repeat these steps for each `assetsources.json` file copied to a Data Collector.

Postrequisites

If specific device parameters were previously opted-in to or you want to opt-in to device parameters beyond the default parameters, you will need to perform the parameter opt-in process again. See Opt-In to Device Parameters.

10.8 Upgrade Plantweb Insight ASI

Prerequisites

- The `A48INSIGHT-DS0.Plantweb_Insight_ASI.1.5.X.X.zip` file is needed.
- Turn off automatic Windows updates during installation or upgrade.
- Ensure Plantweb Optics is upgraded first.

Note
The **Upgrade** option in the ASI installer is not supported at this time.

Note
The Plantweb Insight ASI configuration file must be saved before uninstalling the Plantweb Insight ASI. Copy the asiconfig.json file from the installation location (typically C:\inetpub\wwwroot\EmersonCSI\InsightAsi)
The configuration file will need to be copied back to the installation folder once the upgraded Plantweb Insight ASI is installed.

Procedure

1. Uninstall the Plantweb Insight ASI.
   See page 135 for uninstall instructions.
2. Register the Plantweb Insight ASI. See page 108 for instructions.
3. Install the Plantweb Insight ASI. See page 108 for instructions.

Postrequisites

You must copy the asiconfig.json file (copied during the uninstallation) back into the ASI installation location (typically C:\inetpub\wwwroot\EmersonCSI\InsightAsi).

10.9 Upgrade Plantweb Optics OPC UA server

Upgrading Plantweb Optics OPC UA Server involves uninstalling and reinstalling the software.

Procedure

1. From the Windows search bar, enter **Services**.
   The Windows Services desktop application opens.
2. From the list of services, select **Plantweb Optics OPC UA Server**.
3. Right-click **Plantweb Optics OPC UA Server**, and then click **Stop**.
4. If a hotfix has been installed, uninstall it.
5. Uninstall Plantweb Optics OPC UA Server version 1.4.

6. Install Plantweb Optics OPC UA Server version 1.5.

10.10 Upgrade AMS Device Manager Launcher

To upgrade, you need to uninstall the previous version of the AMS Device Manager Launcher and install a new version from the upgraded Plantweb Optics server.

Prerequisites

Ensure Plantweb Optics is upgraded first.

Procedure

1. Uninstall the previous version of AMS Device Manager Launcher.

   See page 135 for uninstall instructions.

2. Open a browser, type `https://[server]:[port number]/DM`.

   Where `[server]` is the computer name or IP address of the Plantweb Optics server and `[port number]`, if required, is the port number assigned for Plantweb Optics.

   Note
   Enter the server name or IP address, depending on the configuration you set during installation of Plantweb Optics.

   ---

3. On the AMS Device Manager Launcher installation page, click **Install**.
4. Run the application.
5. Click **Yes** on the dialog to continue with the upgrade.
6. Click **Next**.
7. Click **Finish** when done.

11 User Manager

The User Manager function varies for administrators (those users with MANAGEUSER permission) and users. From User Manager, administrators can add users to the system, as well as edit properties, responsibilities, and settings for all currently registered users. It is also where mobile tokens can be conveniently issued and tracked. For users without administrator permissions, User Manager displays read-only information about user properties, responsibilities, and mobile tokens.

Note
Administrators are users that have been given a MANAGEUSER permission in User Manager.

Note
Options may not be available in your user account and may only be available for administrator accounts.

11.1 Add a new user

Prerequisites

- Log in to Plantweb Optics with Administrator privileges.
- Launch User Manager.

Procedure

1. Click the **USERS** tab at the bottom left side of the screen.
2. In the **HOME** ribbon, click **New User**.
3. Enter the new user account details:

Field	Description
Username	The username to access Plantweb Optics. The username must be unique to the system. Spaces are not allowed.
Email address	A valid email address to contact the user. The user receives notification emails and messages at this address, based on the user's subscription settings.
First Name	The user's first name.
Last Name	The user's last name.
Password	Password for the user when logging in to Plantweb Optics for the first time. **Note** The password must meet the complexity set in **SETTINGS** → **Password Settings**.
Confirm Password	Enter the password again to ensure that it was entered correctly.

Field	Description
User must change password on next logon	Check this checkbox if you want the user to create a new password when the user logs in for the first time.
Account is disabled	Check this checkbox if you want to set up the new user now, but want the user account to remain disabled until a later time.

4. Click **OK**. The new user is added to the **USERS** list. You can then assign responsibilities and locations, and issue mobile tokens for the user.

11.2 Delete a user

Prerequisites

- Log in to Plantweb Optics with Administrator privileges.
- Launch User Manager.

Procedure

1. Click the **USERS** tab at the bottom left side of the screen.
2. In the user hierarchy on the left side of the screen, select the user to be deleted.
3. In the ribbon, click the **Delete User** button. The user is deleted.

11.3 Change a user name

Prerequisites

- Log in to Plantweb Optics with Administrator privileges.
- Launch User Manager.

Procedure

1. Click the **USERS** tab at the bottom left side of the screen.
2. In the user hierarchy on the left side of the screen, select the user to be deleted.
3. Click **Edit** next to the user's name on the right side of the screen.
   A dialog displays that allows you to edit the user's first and last name.

11.4 Disable a user account

A disabled user account cannot login and cannot receive notifications or messages.

Prerequisites

- Log in to Plantweb Optics with Administrator privileges.
- Launch User Manager.

Procedure

1. Click the **USERS** tab at the bottom left side of the screen.
2. In the user hierarchy on the left side of the screen, select the user to be disabled.
3. In the ribbon, click the **Disable User** button. The user is disabled.

11.5 Lock a user account

A locked-out user receives notifications and email messages, but is unable to log in. If Lockout Settings are enabled, an account can also become locked after a specified number of failed login attempts.

Prerequisites

- Log in to Plantweb Optics with Administrator privileges.
- Launch User Manager.

Procedure

1. Click the **USERS** tab at the bottom left side of the screen.
2. In the user hierarchy on the left side of the screen, select the user to be disabled.
3. In the ribbon, click the **Lock User** button.
   The user account is locked.

11.6 Force a user to log out

You can force a user to log out at any time.

Prerequisites

- Log in to Plantweb Optics with Administrator privileges.
- Launch User Manager.

Procedure

1. Click the **USERS** tab at the bottom left side of the screen.
2. In the user hierarchy on the left side of the screen, select the user to be logged out.
3. In the ribbon, click the **Force Logout** button.
   The user is logged out after a slight delay. The user is then required to log in again to Plantweb Optics.

11.7 Edit user login information

Use the **Edit Logins** button to change the **OpenID Connect Provider** and the **Claim Value** for a user.

Prerequisites

- Log in to Plantweb Optics with Administrator privileges.
- Launch User Manager.

Procedure

1. Click the **USERS** tab at the bottom left side of the screen.
2. In the user hierarchy on the left side of the screen, select the user whose information requires editing.
3. In the ribbon, click the **Edit Logins** button.
4. On the **Edit Logins** screen, in the **OpenID Connect Provider** field, select the OpenID Connect Provider that was created during configuration. For the **Claim Value**, enter the claim value provided by the OpenID Connect provider.
5. Click **OK**.
   The user's login information is updated.

11.8 Reset a user password

Prerequisites

- Log in to Plantweb Optics with Administrator privileges.

  Note
  Administrator privileges are not required to reset your own password, but they are required to reset other users' passwords.

- Launch User Manager.

Procedure

1. Click the **USERS** tab at the bottom left side of the screen.
2. In the user hierarchy on the left side of the screen, select the user requiring a password reset.
3. In the ribbon, click the **Reset Password** button.
   An email is sent to the user with instructions for resetting the user's password.

11.9 Refresh the users list

After making changes to user information, it can be helpful to refresh the user list with updated information.

Prerequisites

- Log in to Plantweb Optics with Administrator privileges.
- Launch User Manager.

Procedure

1. Click the **USERS** tab at the bottom left side of the screen.
2. In the user hierarchy on the left side of the screen, select **All Users**.
3. In the ribbon, click the **Refresh Users** button. All user information is updated.
   All user information is updated.

11.10 Export the users list to a .csv file

The users list .csv file contains information about all of the users.

Prerequisites

- Log in to Plantweb Optics with Administrator privileges.
- Launch User Manager.

Procedure

1. Click the **USERS** tab at the bottom left side of the screen.
2. In the ribbon, click the **Export to CSV** button on the ribbon to download and open a .CSV file in Excel.

11.11 Assign permissions and locations to a user

User Manager provides a way to make changes to a user's permissions and the locations the user can view in Plantweb Optics.

Prerequisites

- Log in to Plantweb Optics with Administrator privileges.
- Launch User Manager.

Procedure

1. Click the **USERS** tab at the bottom left side of the screen.
2. In the user hierarchy on the left side of the screen, select the user requiring a permissions change.
3. On the right side of the screen, select the **RESPONSIBILITIES** tab.
4. Click **Edit Permissions**.
   The **Edit Permissions** screen displays.
5. Click the **Enabled** checkbox next to the permission you want to provide to this user. Descriptions of each permission are provided on the screen. There are five different permissions that can be selected.
   a) **MANAGEUSER**. This permission provides the user with administrator privileges. Specifically, it allows the user to perform the following actions in User Manager: manage users; manage templates; manage tokens; manage user, password, lockout, and OIDC settings.
   b) **HISTORIZEASSET**. This permission allows the user to enable and disable the historization of assets in Asset Explorer.
   c) **CREATEWORKNOTIFICATION**. This permission allows the user to create a work notification within Asset View (to send to the user's CMMS).
   d) **MANAGEASSETSOURCE**. This permission enables the user to add and remove asset sources in Asset Explorer under the **Network** tab. Users that do not have this permission do not see the **Add Asset Source** button (or similar buttons) in the ribbon.

   e) **MANAGESYSTEMSETTINGS**. This permission allows the user to edit various global settings in Plantweb Optics. Specifically, it allows the user to perform the following actions: edit the **System Settings** (which can be accessed in any application by clicking the **File** tab in the ribbon and clicking the **System Settings** tab); set the CMMS mapping ID within Asset Explorer; and register new licenses within User Manager.

6. Click **OK**.
7. Click **Edit Locations**.
   The **Edit Locations** screen displays.
8. Select the checkboxes for the locations the user can view in Asset Explorer.
9. Click **OK**.

Permissions and locations are assigned.

11.12 Create a user template

User Manager allows you to create a template to use when setting up new users.

Prerequisites

- Log in to Plantweb Optics with Administrator privileges.
- Launch User Manager.

Procedure

1. Click the **TEMPLATES** tab at the bottom left side of the screen.
2. In the templates hierarchy on the left side of the screen, select the folder where this new template will be placed.
3. In the ribbon, click the **New Template** button. The **New Template** screen displays.
4. In the **Name** field, enter a name for this template.
5. Click the **Enabled** checkboxes for each permission to assign to the users created with this template.
6. Click the locations checkboxes for each location the users will be able to view in Asset Explorer.
7. Click **OK**.
   The new template is created and shown in the folder selected.

11.13 Apply a user template

You can apply a template to users once they have been created. Please note that any future changes made to the template do not automatically apply to the user's information that was created using this template. The updated template would have to be applied to the users again.

Prerequisites

- Log in to Plantweb Optics with Administrator privileges.

- Launch User Manager.

Procedure

1. Click the **TEMPLATES** tab at the bottom left side of the screen.
2. In the templates hierarchy on the left side of the screen, navigate to and select the template you want to use.
3. In the ribbon, click the **Apply Template** button.
   The **Apply Template** screen displays.
4. Click the checkboxes next to the names of the users to which you want to apply this template's settings.
5. Click **OK**.
   The selected users now have the permissions and locations settings specified in the template.

11.14 Delete a user template

Prerequisites

- Log in to Plantweb Optics with Administrator privileges.
- Launch User Manager.

Procedure

1. Click the **TEMPLATES** tab at the bottom left side of the screen.
2. In the templates hierarchy on the left side of the screen, navigate to and select the template you want to delete.
3. In the ribbon, click the **Delete Template** button.
   The selected template is deleted.

11.15 Display mobile tokens for a user

User Manager allows you to view the mobile tokens issued to a user.

Prerequisites

- Log in to Plantweb Optics with Administrator or user privileges.
- Launch User Manager.

Procedure

1. Click the **USERS** tab at the bottom left side of the screen.
2. In the user hierarchy on the left side of the screen, select the user requiring a mobile token.
3. On the right side of the screen, select the **TOKENS** tab.
   The mobile tokens issued to this user are displayed.

11.16 Issue a mobile token

User Manager allows you to issue a mobile token for each user who will access the Plantweb Optics Mobile App.

Prerequisites

- Log in to Plantweb Optics with Administrator privileges.
- Launch User Manager.

Procedure

1. Click the **TOKENS** tab at the bottom left side of the screen.
2. In the hierarchy on the left side of the screen, select the user requiring a mobile token.
3. In the ribbon, click the **Issue Token** button.
   The **Issue Token** screen displays.
4. On the **Issue Token** screen, select the user from the drop-down list.
5. Select the **Application** that the user needs access to from the drop-down menu. For example, **Asset View**.
6. Click the **Send issued token notification to user** checkbox if you want to email the user that a token has been issued.
7. Click **OK**.
   The token is issued to the user.

11.17 Disable a mobile token

Prerequisites

- Log in to Plantweb Optics with Administrator or user privileges.
- Launch User Manager.

Procedure

1. Click the **TOKENS** tab at the bottom left side of the screen.
2. In the hierarchy on the left side of the screen, select the user requiring a mobile token to be disabled.
3. In the ribbon, click the **Disable Token** button.
   The token is disabled for the selected user.

11.18 Export the mobile tokens list for all users

User Manager allows you to export a list of mobile tokens for all users.

Prerequisites

- Log in to Plantweb Optics with Administrator privileges.
- Launch User Manager.

Procedure

1. Click the **TOKENS** tab at the bottom left side of the screen.
2. In the hierarchy on the left side of the screen, select the **All Tokens** folder.
3. In the ribbon, click the **Export to CSV** button to download and open a .CSV file in Excel. This file contains mobile token information for all of the users.

11.19 Register licenses

You can view the status of and register licenses from User Manager. The license applies to the entire enterprise. It does not apply to a specific user.

Note
To complete this task, you must have MANAGESYSTEMSETTINGS permission.

Prerequisites

- Log in to Plantweb Optics with Administrator privileges.
- Launch User Manager.

Procedure

1. Click the **LICENSES** tab at the bottom left side of the screen.
2. On the screen, the following information displays:
   a) **Status**: The status information indicates if the current license is **GOOD**, **FAIR**, or **POOR**. A **GOOD** license is not in any danger of running out. A **FAIR** license is getting close to running out. A **POOR** license is currently running out or is about to expire.

   b) **Source**: The source information shows the product for which the license is assigned. For example, **Plantweb Optics**.

   c) **Feature**: The feature information shows the part of the product to which this license applies. For example, **AMS_Machinery_Manager_ASI**.

   d) **Expires**: The expiration date information shows when the current license is set to expire.
3. Select the license to register from the list. Click the **Register License** button from the ribbon.
4. Click **Choose File** and browse to the license file for this feature on your PC. Typically, license files are emailed to the customer and stored in a folder of their choosing. You may need to email or call an Emerson representative to update your license. Follow the instructions on the screen.
5. Click **OK**.
   You will receive email notification that the license has been registered.

11.20 Request a license proposal

You can request a proposal for a license from Emerson directly from User Manager.

Prerequisites

- Log in to Plantweb Optics with Administrator privileges.
- Launch User Manager.

Procedure

1. Click the **LICENSES** tab at the bottom left side of the screen.
2. Click the **Request Proposal** button from the ribbon.
3. Click **Copy** to copy the machine fingerprint needed for the proposal. Email Emerson requesting a proposal and include the machine fingerprint. Follow the instructions on the screen.
4. Click **OK**.
   You will receive an email response from Emerson.

11.21 View Guardian information

The **Guardian Info** feature is used to collect information about the server that can be exported to a file and emailed to an Emerson Guardian employee for help with issues the user may be having. It is a tool used for customer support.

Prerequisites

- Log in to Plantweb Optics with Administrator privileges.
- Launch User Manager.

Procedure

1. Click the **LICENSES** tab at the bottom left side of the screen.
2. Select the license for the proposal from the list. Click the **Guardian Info** button from the ribbon.
   The **Guardian Information** screen displays.
3. Click **Export** to export the Guardian information to a .epm file.

11.22 Change user settings

Prerequisites

- Log in to Plantweb Optics with Administrator privileges.
- Launch User Manager.

Procedure

1. Click the **SETTINGS** tab at the top left side of the screen.
2. Click the **User Settings** button from the ribbon.
   The **User Settings** screen displays.
3. Click the **Require Unique Email** checkbox to prevent a single email address from having multiple accounts.

4. Click the **Allow Only Alphanumeric User Names** checkbox to prevent users from adding special characters to their user names.
5. Click **OK** to make these changes.

11.23 Change password settings

Prerequisites

- Log in to Plantweb Optics with Administrator privileges.
- Launch User Manager.

Procedure

1. Click the **SETTINGS** tab at the top left side of the screen.
2. Click the **Password Settings** button from the ribbon.
   The **Password Settings** screen displays.
3. In the **Required minimum length** field, enter a minimum length for user passwords.
4. Click the **Require special character** checkbox to require users to include at least one allowed special character in their passwords.

   The following special characters are allowed:

   Space; \ / | " * : < > ? , . ; ' " [ ] { } - _ = + ~ `
5. Click the **Require lowercase** checkbox to require users to include at least one lowercase letter in their passwords.
6. Click the **Require uppercase** checkbox to require users to include at least one uppercase letter in their passwords.
7. Click the **Require digit** checkbox to require users to include at least one numeric character in their passwords.
8. Click **OK** to make these changes.

11.24 Change lockout settings

These settings control the **Lock User** functions on the User Manager **HOME** tab.

Note

These changes are not applied until the user restarts Plantweb Optics.

Prerequisites

- Log in to Plantweb Optics with Administrator privileges.
- Launch User Manager.

Procedure

1. Click the **SETTINGS** tab at the top left side of the screen.
2. Click the **Lockout Settings** button from the ribbon.
   The **Lockout Settings** screen displays.

3. Click the **Enabled** checkbox to enable lockout settings.
4. In the **Lockout Time (in minutes)** field, enter the amount of time, in minutes, that a user is prevented from attempting to log in after the account is locked.
5. In the **Max Failed Access Attempts** field, enter the number of times a user can incorrectly enter his login credentials before the account is locked.
6. Click **OK** to make these changes.

11.25 Change OIDC settings

The OpenID Connect settings control which options appear in the login page under the section **External Account**. These external accounts allow you to log in to Plantweb Optics using your credentials from another source—for example, from your Google account, or your Microsoft account, or your Active Directory account. As long as these external providers implement OpenID Connect, a standard protocol for sharing authentication information between Web Services, they can be used to link a user in Plantweb Optics.

The OpenID Connect settings are different depending on which OpenID Connect provider you are using.

Note
These changes are not applied until the user restarts Plantweb Optics.

Prerequisites

- Log in to Plantweb Optics with Administrator privileges.
- Launch User Manager.

Procedure

1. Click the **SETTINGS** tab at the top left side of the screen.
2. Click the **OIDC Settings** button from the ribbon.
   The **OpenID Connect Settings** screen displays.
3. On the left side of the screen, select the display name whose settings you want to change. For example, AFDS.
4. In the **Claim Type** field, if you are using Active Directory/ADFS, then enter **http://schemas.xmlsoap.org/we/2005/05/identify/claims/upn**. If you are using a different provider, enter the claim type information specific to that provider. The **Claim Type** field defines which claim is used to link the user in the **Edit Logins** dialog.
5. In the **Display Name** field, enter the user defined display name. For example, **ADFS**.
6. In the **Scheme Name** field, enter the user defined scheme name. For example, **adfs**. The **Scheme Name** must be unique and cannot be the same name as another OpenID Connect Provider in Plantweb Optics.
7. In the **Authority** field, use this format for this field, if you are using Active Directory/ADFS, then enter **https://<YOUR ACTIVE DIRECTORY SERVER>/adfs/**. If you are using a different provider, enter the URL specific to that provider in the format of **https://<AUTHORITY>/.well-known/openid-configuration**. For example, **https://accounts.google.com/.well-known/openid-configuration**.

8. Enter the **Callback path** specific to the provider you are using.
9. Enter the **Client ID** specific to the provider you are using.
10. If the provider requires a client secret, check the **Enable Client Secret** checkbox and enter the secret in the **Client Secret** field.
11. Click **Add an OIDC Provider** to add a provider to Plantweb Optics.
12. Click **Delete this OIDC Provider** to remove this provider from Plantweb Optics.

11.26 Change language settings

Apply a language pack to change the Plantweb Optics language. The language pack must first be installed, then applied to Plantweb Optics. The selected language is applied only to Plantweb Optics platform applications (such as Asset View). Underlying alerts and notifications will be received in their source language. User-generated messages will also appear in their source language.

Prerequisites

- Log in to Plantweb Optics with Administrator privileges.
- Launch User Manager

Procedure

Install a Language Pack

1. Click the **SETTINGS** tab at the top left side of the screen.
2. Click the **Language Settings** button from the ribbon.
   The Language Settings screen will appear.
3. Click **Browse...** and navigate to a language pack.

   #### Example

   Note
   Language packs are included in the installation media in the `_Support\Languages` directory.

4. Click **OK** to install the language pack.
   The language pack is now installed. The page will refresh to reflect the new language pack. The language selector dropdown in the top right (flag icon) will now show the language you applied as a selectable option.

Apply a Language to Plantweb Optics

5. To apply a language to Plantweb Optics, click the language selector icon in the top right and select a language.

12 Asset Explorer

The Asset Explorer utility allows you to set up your site, create locations, add machines and devices, and arrange them according to how your plant is set up. This utility lets you centrally manage and view the health status of your plant assets. You can set persona-specific functions for user accounts by setting responsibilities and permissions in the User Manager utility. Permissions and responsibilities ensure the user has the proper access to locations and assets to which he is assigned. You can also do the following from the Asset Explorer utility:

- Specify user and system settings
- Establish connection to an Emerson Wireless Gateway
- Pull in AMS Device Manager data, alerts, and hierarchy
- Pull in AMS Machinery Manager data, alerts, and hierarchy
- Pull in Plantweb Insight data, alerts, and hierarchy
- Configure devices, machines, and assets
- Configure connected AMS 9420 transmitters
- Create Plant Calendar events
- Bind asset source locations
- Map channels to devices
- View properties and health of assets in your site
- Ignore assets or locations
- Launch AMS Device Manager in context
- Launch AMS Machinery Manager in context

12.1 Join an Emerson Wireless Gateway to Plantweb Optics

When you set up a connection to a gateway, Plantweb Optics lets you set up your system quickly by enabling quick mapping and binding. If you do not have a gateway connected, you can set up your site with locations, assets, machines, and devices prepared for mapping and binding later.

Prerequisites

- In AMS Device Manager or from a Field Communicator, enable **MHM Access Control** for each AMS 9420 device before adding the gateway. This is to make sure you can configure device settings and alert limit settings from Plantweb Optics.
  To enable this setting in AMS Device Manager for rev 4 or later devices, right-click the AMS 9420 device, and select **Configure** → **Manual Setup** → **General Settings tab** → **MHM Access Control**. To enable this setting in AMS Device Manager for rev 3 or earlier devices, right-click the AMS 9420 device, and select **Configure** → **Manual Setup** → **Device Setup tab** → **MHM Access Control**.

- Port 33333 or 32000 is open on the network and enabled in the Emerson Smart Wireless Gateway.
- The Emerson Wireless Gateway ASI is installed and reachable on the network.

Procedure

1. In the Asset Explorer utility, select the **Network** tab, and click **Emerson Wireless ASI**.
2. From the Home ribbon, select **Add Asset Source**. The **Add Asset Source** button is only displayed if the user has MANAGEASSETSOURCE permission.
3. In the dialog, enter the following:

Field	Description
Site	The site where the Gateway is housed.
Name	The name for the Gateway.
Description	The description for the Gateway.
IP Address	The Gateway IP address. **⚠ CAUTION** If the Emerson Wireless Gateway you are adding contains transmitters, ensure the same gateway is not already in Plantweb Optics through another ASI. Adding a duplicate gateway can cause duplicate devices, events, and process variables in Plantweb Optics. If your system gets into this state, contact Emerson Product Support. There is no automated or user-facing methodology available to recover from this condition.
Port Number	Use 33333 for an unsecured HART connection. Use 32000 for a secure connection. **Note** The above values are default port numbers. Check the Gateway web interface to ensure you enter the correct port number.
Enable Secure Protocol	Check the box to enable the username and password security protocols. **Note** You must also perform the following when you select this option: • Install the 1420 Security Setup Utility. • Enable secure communication for the Gateway.
User Name	The Emerson Wireless Gateway ASI server user name. This field is only available when you select the Enable Secure Protocol checkbox.

Field	Description
Password	The Emerson Wireless Gateway ASI server password. This field is only available when you select the Enable Secure Protocol checkbox.

4. Click **Create**.

The Emerson Wireless Gateway appears in the Network navigator.

12.2 Add locations to your site

Use locations to represent functional areas, floors, or sections of your site. You can nest locations within locations. You can add asset locations and asset source locations to locations. However, you cannot add locations to assets or asset source locations.

Procedure

1. In the Asset Explorer utility, select the **Location** tab, and highlight the site or a location.
2. From the **Home** ribbon, click **New Location**.
   A new location appears at the bottom of the navigator. It has a folder icon and is named **New Area**. To rename, highlight **New Area** and, in the **Home** ribbon, click **Rename**.
3. Create and name additional locations at the site level, and structure locations within the locations to represent different places in your facility.

   You can create an unlimited number of locations.

Postrequisites

Add assets and asset sources to your site.

12.3 Add assets to your site

You can add assets at the site level, in locations, or in other assets. Organize the assets in logical groups similar to how the assets are physically organized in your facility.

Procedure

1. In the Asset Explorer utility, click the **Location** tab.
2. Highlight the location where you want to add assets, or create a new location.
3. From the Home ribbon, select **New Asset**:
   a) Select **Asset (Generic)** to create a new generic asset.
   b) Select **Device** to create a new device.

   An asset or device labeled "New" appears below the location.
4. Rename the asset or device to something relevant or appropriate to your plant setup.

12.4 Add asset source locations

It is easier to add a monitoring device after it has been added to the Plantweb Optics network. However, you might need to define the network devices in your site before that device is available on your network. You can add asset source locations or placeholders for your devices to the Location navigator. These placeholders are not yet bound to a physical device on the network.

Procedure

1. In the Asset Explorer utility, select the **Location** tab.
2. Select a location where you want to add the device, and from the **Home** ribbon, click **New Asset** → **Device**.
3. In the **Add Device** dialog, locate your device by manufacturer and select from a list of available models.
4. Click **OK**.

Postrequisites

Bind the asset source locations to the actual device on the Plantweb Optics network.

12.5 Bind an asset source location to a device on the network

Binding an asset source location to a network device is used to create a logical representation of your assets in Plantweb Optics. Binding establishes a connection between the data coming into Plantweb Optics from the ASIs to the logical hierarchy you build within Plantweb Optics.

In Asset Explorer, the **Network** tab represents all of the physical device data being provided to Plantweb Optics. The **Location** tab represents all of the logical assets that you can create. Binding an asset from the **Location** tab to the **Network** tab establishes the connection required to create a logical representation of your facility.

Binding maintains a one-to-one relationship, where every asset in the **Location** tab can be bound to a single asset in the **Network** tab.

The AMS Device Manager ASI automatically completes the binding process during the installation process. When you select the **Add Logical Hierarchy in addition to Physical Hierarchy** when adding an AMS Device Manager system to Plantweb Optics, the asset source locations created in the Location navigator are already bound to the corresponding devices in Network navigator. If an asset is added to the logical hierarchy in AMS Device Manager after joining the AMS Device Manager system to Plantweb Optics, the asset needs to be manually added by rebuilding the hierarchy and it needs to be manually bound in the Asset Explorer utility Location tab.

You can choose to re-bind asset source locations from the AMS Machinery Manager hierarchy when you remove and re-import databases to Plantweb Optics.

Procedure

1. In the Asset Explorer utility, highlight an asset source location in the Location navigator.

In the Asset Explorer utility contents pane, unbound devices display with a red exclamation mark before the device icon.

2. From the Home ribbon, select **Bind**.
   The **Bind Device** dialog opens and displays only unbound asset sources of the same type as the asset source location.
3. In the **Bind Device** dialog, navigate to the asset source/device.
4. Click **Bind**.

Bind an AMS 9420 in the Location navigator to an AMS 9420 on the network.

1. In the Location navigator, right-click an unbound AMS 9420 and select **Home** → **Bind**.
2. In the **Bind Device** dialog, expand **Emerson Wireless ASI** or **AMS Device Manager ASI**, select the specific AMS 9420 on the network and click **Bind**.

   Note
   You can only select unbound AMS 9420 devices from the AMS Device Manager ASI hierarchy.

   This should typically happen if you are re-assigning AMS 9420 devices in the AMS Device Manager ASI hierarchy. Since devices in the AMS Device Manager hierarchy are automatically bound, to re-assign them you need to unbind and bind devices, and then map the channels, if necessary.

Postrequisites

Map channels to the machine if you have not already done so.

12.6 Unbind an asset source location from a device on the network

Unbinding a device removes its existing channel mapping information. Binding establishes a relationship between your logical and physical assets. Unbinding is typically required if you are making changes in your physical facility and need to make sure your Plantweb Optics system reflects these updates. You may need to unbind a device in the following scenarios:

- When you select the **Add Logical Hierarchy in addition to Physical Hierarchy** when adding an AMS Device Manager system to Plantweb Optics, devices are automatically bound to asset source locations in the Location navigator for the AMS Device Manager hierarchy. If you attempt to map channels and the channels you want to map are not displayed, the channels may already be mapped. You need to unbind the devices, bind them, and then re-map the channels to measurement locations.
- When you want to replace a device that is bound and mapped to an asset. After unbinding, you need to bind the device again to another location and redo channel mappings.

Procedure

1. In the Asset Explorer utility, highlight the device in the Location navigator.

2. From the Home ribbon, select **Unbind**.
3. Click **OK** to unbind the device and delete any channel mapping information.
   The unbound device icon displays with a red exclamation mark.

12.7 Join an AMS Machinery Manager system to Plantweb Optics

Prerequisites

- AMS Machinery Manager ASI Web App is installed and reachable on the network.
- The following services are running on the server where the AMS Machinery Manager ASI Service is installed: AMS Machinery Manager ASI IO Service, CSI Data Import Service, CSI Data Transfer Service, CSI_MhmRemote, Csi_MtdbMgr, CsiNetAdmin, and CsiO_Server.

Procedure

1. In the Asset Explorer utility, select the **Network** tab, and click the **AMS Machinery Manager ASI** folder.
2. From the Home ribbon, select **Add Asset Source**. The **Add Asset Source** button is only displayed if the user has MANAGEASSETSOURCE permission.
3. In the dialog, enter the following:

Field	Description
Site	The main site in the Location navigator. This is not editable and defaults to the name assigned to the main site.
RBM Net Admin Server Name	The computer name of the AMS Machinery Manager server where the AMS Machinery Manager ASI Service is installed.
Name	The short name of this AMS Machinery Manager system. This is the name displayed in Asset Explorer.
Description	The system description. This is the description displayed in Asset Explorer.

4. Click **Connect**.

Postrequisites

Configure AMS Machinery Manager to successfully import databases into Plantweb Optics.

12.8 Import AMS Machinery Manager databases to Plantweb Optics

Import AMS Machinery Manager databases to Plantweb Optics in the following scenarios:

- Import for the first time to display and monitor routes, equipment, and components from an AMS Machinery Manager system in Plantweb Optics.

- There are two ways to keep the database hierarchy in Plantweb Optics in sync with the AMS Machinery Manager system:
    1. Remove and re-import when there are changes to the equipment and components in the AMS Machinery Manager system, specific to the database you previously imported.
    2. Use the **Resync Hierarchy** button in Asset Explorer under the **Network** tab.
- Remove and re-import a database when there are changes to its **Unit Mode** and **System for Data Units** settings in the Database Setup tool in AMS Machinery Manager after the initial database import. This ensures the parameter values displayed in Plantweb Optics are correct. See the AMS Machinery Manager Online Help for more information on removing databases.

Prerequisites

You have previously joined the AMS Machinery Manager system to Plantweb Optics. See page 164.

You have configured AMS Machinery Manager in preparation for database import. See page 59 for instructions.

Procedure

1. In the Asset Explorer utility, select the **Network** tab and expand the **AMS Machinery Manager ASI** folder.
2. Select the AMS Machinery Manager system with the databases you want to import.
3. Click **Import Database** from the Home ribbon.
4. Select the databases you want to import and click **Import**.

    Successfully imported databases appear with a check mark.

    Note

    A warning error means the import failed and the AMS Machinery Manager ASI failed to revert all imported items. This means you need to remove and re-import the database.

    When re-importing a database, Plantweb Optics adds another folder for the same database in the Location navigator and appends a numerical number to the newly added folder. Only the newly added folder is bound to the hierarchy in the Network navigator. Equipment in the Location navigator that is not bound to the hierarchy in the Network navigator does not display health status with the health icon grayed out. You may need to manually remove the equipment and components in the Location navigator that are not bound in the Network navigator, or re-bind them when you re-import the same database to Plantweb Optics.

12.9 Join a Plantweb Insight system to Plantweb Optics

Prerequisites

- Plantweb Insight ASI System is installed and reachable on the network.
- The Plantweb Insight server station is configured in preparation for joining to Plantweb Optics. See page 60 for instructions.

Procedure

1. In the Asset Explorer utility, select the **Network** tab, and click the **Plantweb Insight ASI** folder.
2. From the Home ribbon, select **Add Asset Source**. The **Add Asset Source** button is only displayed if the user has MANAGEASSETSOURCE permission.
3. In the dialog, enter the following:

Field	Description
Site	The main site in the **LOCATION** navigator. This is not editable and defaults to the name assigned to the main site.
Name	The **Name** is the user-defined identifier for the asset source. This is the same name displayed in Asset Explorer.
Host	The IP address or system name of the Plantweb Insight System.
Port Number	The port number to use for the Plantweb Insight System. The default port is 443, but that is configurable.
App Name	A short name given to the API Key during the steps to create the API Key in Plantweb Insight.
API Key	The associated key given to the App Name when created in Plantweb Insight.
Description (optional)	This is the description displayed in Asset Explorer.

Note
Plantweb Optics only supports 64-character asset source names and asset names. If the asset names are longer that 64 characters, they will be truncated.

4. Click **Add**.

A dialog is displayed showing the status of the rebuild and shows when it has been completed.

12.10 Rebuild the Plantweb Insight hierarchy

Rebuild the hierarchy to keep it in sync with the hierarchy in the Plantweb Insight System. This is necessary when a new asset is added to AMS Device Manager.

Procedure

1. In the Asset Explorer utility, select the **NETWORK** tab.
2. Select the Plantweb Insight system with the hierarchy you want updated.
3. From the Home ribbon, select **Rebuild Hierarchy**.
   Plantweb Optics connects to the selected Plantweb Insight system and reads the information about the connected assets.

13 Launch Plantweb Optics utilities

All user interactions in the software happen through its utilities, which can be launched from a web browser. Also, on the server, you can launch the utilities through a desktop shortcut.

Prerequisites

- If Enhanced Security Configuration is enabled in Internet Explorer, add the Plantweb Optics server URL to the list of trusted sites. See page 199 for instructions.
- Determine whether the server is set up to launch by IP address or server name.
- Determine whether the server is set up to use the default port.
- Security certificates must be installed. See page 47.

Procedure

1. Open a web browser.
2. In the web browser address field, enter the URL for the utility you want to launch. Refer to the following table.

Launch	From this URL	To perform the following
User Manager	`https://[server]:[port number]/UserManager`	• Set up users • Control and monitor access to the software.
Asset Explorer	`https://[server]:[port number]/AssetExplorer`	• Set up your site • Access and manage assets in your plant
Asset View	`https://[server]:[port number]/AssetView`	• Send, receive, and view messages related to assets and health changes
Event Viewer	`https://[server]:[port number]/EventViewer`	• View events generated in the software.

Where `[server]` is the computer name or IP address of the Plantweb Optics server and `[port number]`, if required, is the port number assigned to the web site.

Asset Explorer utility from the server named OpticsServer with an IP address of 10.164.252.89 and a port number of 8080, enter `https://OpticsServer:8080/AssetExplorer` or `https://10.164.252.89:8080/AssetExplorer`.

Note
You can only use either the server name or IP address, depending on the configuration you set during installation. If you chose the **Use Server Name** option in the Server and Port Binding Configuration screen, you can only launch utilities

using the server name. If you chose the **Use IP Address** option, you can only launch utilities using the server IP address.

3. If this is the first time you have launched a utility from a client computer, do not log in when prompted.

   Install the Plantweb Optics certificate before logging in for the first time. See page 47.

4. Enter your credentials and log in.

   On first login, use the following defaults:

   - **Username**: admin
   - **Password**: Emerson#1

   Note
   After initial login, you are required to change this password. Your new password must have at least one special character, have an uppercase letter, and should be a combination of alphanumeric characters. As an administrator, you have the option to change the password complexity requirement in the User Manager utility.

Return to steps 3 through 7 of the Completing post-installation steps portion of the *Quick start* chapter and continue your installation.

14 Asset View

The Asset View utility lets you send, receive, and view messages generated in Plantweb Optics from your computer. The ability to receive and view messages is dependent on the user's responsibilities and subscriptions.

The same messages can also be sent, received, and viewed on a mobile device if the Plantweb Optics Mobile App is installed. The Plantweb Optics Mobile App is available for download from the Google Play™ store or the Apple® AppStore™. To use the mobile app, users need a mobile token associated with their account.

Messages

In Plantweb Optics, messages are tied to events and health changes. When something changes in the system, an event is created, but only some events trigger messages. When an asset's health changes, a message is generated. Messages are sent to users, depending on that users' responsibilities and subscriptions.

Like an email, a message consists of:

- Recipient
- Sender (an asset or another user)
- Subject
- Timestamp
- Body
- Attachments (optional)

Messages are generated by three sources:

Plantweb Optics	When an event is logged on an asset, the software automatically generates a message.
Asset extensions	Different situations, such as a change in asset status or health changes, can cause asset extensions or asset source interfaces to generate a message.
Users	Any user can create a message for an asset, which is distributed to users who are assigned responsibility for that asset or location.

The Asset View utility lets users send, receive, and view messages generated in Plantweb Optics from a computer. Any user can send a message but not all users can receive and view the message. Receiving of messages is dependent upon a user's responsibilities and subscriptions.

Port 443 must be open to the internet on the Plantweb Optics server to allow Plantweb Optics Mobile App messaging to work.

From the Asset View utility, users can set preferences for the messages they receive on the computer, such as tagging of junk messages, adding assets to the Watch List, and purging of all messages from their user account.

14.1 Plantweb Optics Mobile App

Mobile token

To use the Plantweb Optics Mobile App, you need a mobile token associated with your user account issued by a Plantweb Optics administrator.

You need to issue a mobile token for each user that will access the Plantweb Optics Mobile App. See page 152 for instructions. You can issue and monitor issued tokens in the User Manager utility. The token is unique to the user and is valid until it is disabled.

Internet connection/On-premises mobile service

Sending and receiving of messages can either be through an internet connection or by direct (on-premises) connection to Plantweb Optics through your plant network Wi-Fi.

Note

You need an internet connection to send and receive messages in the Plantweb Optics Mobile App if you did not choose the **On-Premises Mobile Service** option during installation. It is only during installation that you can choose from either internet connection or on-premises mobile option. The on-premises mobile option makes for a faster and more secure access to messages when inside your plant. See page 173 for more information on setting up the on-premises mobile service.

Multisite

You can display, send, and receive messages from multiple Plantweb Optics systems or sites in the Plantweb Optics Mobile App. Each site requires its own token for the user account issued by the site administrator of the specific Plantweb Optics system.

Each site in the mobile application has its own dashboard with a counter that either displays unhealthy assets or the number of messages for each site.

14.1.1 Claim a mobile token for Plantweb Optics Mobile App on your device

The first time you open the Plantweb Optics Mobile App, you will be prompted for a mobile token. A Plantweb Optics administrator can generate a mobile token and give you a join key associated with your username.

A mobile token allows you to log in to the Plantweb Optics Mobile App. The token is unique to you and the app—it identifies your username and the Plantweb Optics Mobile App. The token is valid until it is disabled by the administrator or the user.

Important

Different mobile devices require separate tokens. Different sites also require different tokens.

Prerequisites

- Download the Plantweb Optics Mobile App on your mobile device.
- Have a Plantweb Optics administrator create your username, password, and issue you a mobile token.

- Your mobile device must be connected to the internet.

Procedure

1. On your mobile device, open the Plantweb Optics Mobile App.
2. Tap **Get Started**.
3. Enter the join key and tap **OK**. Alternatively, you can scan a QR code in this step. Tap the QR code icon to display a QR scanner. Open User Manager on your desktop and select the token that has been issued to you. Scan the QR code using the scanner. The join key is entered automatically.
4. When prompted to login, enter your username and password for which the token was issued, and click **Sign in**.
   The Plantweb Optics username on the token and login must match.

You are now logged in to the Plantweb Optics Mobile App. Based on your subscriptions, you will receive Plantweb Optics notifications on the device, and you can view and send messages.

14.1.2 Set up on-premises mobile service

During installation, you can choose whether the Plantweb Optics Mobile App can receive messages anywhere it has an internet connection or only from your local wireless network, through the on-premises mobile service. When you select the on-premises mobile service, you can only receive messages on your mobile device when on the company wireless network. This happens by connecting to the Plantweb Optics server from your plant network Wi-Fi. The on-premises mobile service setup is done once. When set up, you do not need to set it up every time you log in to the Plantweb Optics Mobile App.

Prerequisites

- You must have chosen the **Enable On-Premises Mobile Services** during installation.
- Your plant network must give access to the mobile device to let it connect to the Plantweb Optics server. Contact your IT department for details.
- Connect your mobile device to your plant network Wi-Fi.

Procedure

1. On your mobile device, open the **Plantweb Optics Mobile App**.
2. Enter the join key issued by your administrator. Alternatively, you can scan a QR code in this step. Tap the QR code icon to display a QR scanner. Open User Manager on your desktop and select the token that has been issued to you. Scan the QR code using the scanner. The join key is entered automatically.
3. Tap **Advanced** and enter the following:

Field	Description
Enter Service Path	The path to the Plantweb Optics server. Type the server name and append the text `/OnPremAssetView`.

Field	Description
Enter Mobile Service Path	The path to the Plantweb Optics mobile services. Type the server name and append the text `/OnPremMobileServices`.

4. Tap **OK**.

14.1.3 Switch Plantweb Optics mobile device relay between Microsoft Azure and on-premises connection

The Plantweb Optics mobile relay configuration utility is used to switch between using the Plantweb Optics mobile device relay in Azure and the relay on premises. To run the mobile relay configuration utility, navigate to `C:\inetpub\wwwroot\EmersonCSI\Tools\MobileRelay` and open a command prompt with elevated privileges.

⚠ CAUTION

Performing a mobile relay service switch will remove all mobile tokens.

Table 14-1: Mobile Relay Configuration Utility Available Commands

Operation	Command
Switch to on-premises mode.	`MobileRelayConfig.exe onprem`
Switch to Azure mode. Requires a valid path to a `mobileconfig.json` file.	`MobileRelayConfig.exe azure -f "C:\`*`full`*`\`*`path`*`\`*`to`*`\`*`mobileconfig.json`*`"`
Displays whether the system is configured for on-premises or Azure.	`MobileRelayConfig.exe getconfig`

15 Event Viewer utility

The Event Viewer utility allows you to view system-generated events. You can choose to display events per module or view all events logged by the system.

The following modules log events:

- **AMS 9420 Device Configuration**—events relating to configuration of connected AMS 9420 devices, such as device discovery errors.
- **AMS Device Manager ASI**—events and configurations in the AMS Device Manager hierarchy, such as device alerts and asset health.
- **DeltaV Control Loop ASI**—events and configurations in the DeltaV Control Loop hierarchy, such as control loop data from control modules configured on a DeltaV system.
- **Plantweb Insight ASI**—events and configurations in the Plantweb Insight hierarchy, such as asset alerts, rebuilding hierarchies, and adding and deleting assets.
- **AMS Machinery Manager ASI**—events and configurations in the AMS Machinery Manager hierarchy. This module also logs the following: status of database import and synchronization, parameters in alarm, status of AMS Machinery Manager services, polling status, KPI summaries, route downloads, report generation, machine notes creation, and opened case histories.
- **Asset Explorer**—events and configurations in the Asset Explorer utility, such as adding, editing, and deleting assets and locations, asset binding, and all asset health changes.
- **Asset View**—events and configurations in the Asset View utility, such as creating messages and adding or removing assets from the Watch List.
- **Data Highway**—all events occurring in the Data Highway, such as parameter registration and unregistration.
- **Emerson Wireless Gateway**—all events in the Emerson Wireless Gateway, such as device alerts and device communication status.
- **Machine Configuration**—all machine configurations, such as adding, editing, and deleting components, bearings, collections, measurement definitions, alarm limits, and channel mappings.
- **User Manager**—all events in the User Manager utility, such as adding, editing, and deleting users and logging in and logging out users.

Events are displayed with the following details:

- **Date and Time**—date and time the event was recorded.
- **Event Type**—the type of event to which the ASI responds.
- **Source**—the module associated with the event.
- **Asset**—the asset associated with the event.
- **Attachments**—the attachment associated with the event. Events with attachments have a paper clip icon.

Note
The database in a Tier-1 installation, Microsoft SQL Server 2017 Express, has a size limit of 10 GB. If the databases reach this size limit, Plantweb Optics will no longer be able to store new events.

15.1 View events

Only system-generated events can be viewed in the Event Viewer utility.

Prerequisites

Launch the Event Viewer utility.

Procedure

1. On the left pane, select to view events by **Application** or by **Modules**:
   - Click **Application** to view all events logged by the system.
   - Expand the **Modules** folder and click on a module to view events recorded for the specific module.
2. Select an event from the list.

   Details display in the bottom pane. If an event has an attachment, a thumbnail of the attachment is displayed.

15.2 Archive events

Events stored in the Plantweb Optics system are archived periodically. Archived events are deleted from the database and stored in an archive file.

By default, events that are older than 180 days are archived. Event archiving automatically happens every 30 days. You can retrieve archived files in `C:\EMERSONCSI\DATA\Backups\Events`. Archive files are in .csv format with the text `OpticsEventsArchive` appended in the file name.

Note
Archived events cannot be imported and viewed in Plantweb Optics.

16 Plantweb Optics OPC UA server

OPC Unified Architecture (UA) is a communication standard used in automated systems which allows machines and devices to communicate with each other and transmit data.

When the Plantweb Optics OPC UA Server extension is installed, whether on the same server as the main components of Plantweb Optics or on another server, data from the OPC UA Server becomes available to other systems on the network that recognize OPC UA input.

The Plantweb Optics OPC UA Server extension may be installed on multiple computers. Your Plantweb Optics system may have multiple OPC UA servers. Having multiple Plantweb Optics OPC UA servers makes it more convenient to monitor different nodes.

You may use a separate OPC UA client to access data on the Plantweb Optics OPC UA Server. Then, within your application, use OPC UA to query Plantweb Optics for the data that you need.

The Plantweb Optics OPC UA Server allows you to read data via OPC UA, but you cannot write to Plantweb Optics through OPC UA.

16.1 Manage certificates

To connect an OPC UA client to the Plantweb Optics OPC UA Server, the certificates of the server and the client must first be added as trusted certificates of each other.

Prerequisites

The Plantweb Optics OPC UA Server is installed.

Procedure

1. From the OPC UA Server, add the OPC UA client certificate as a trusted certificate.
    a) Navigate to the directory where you installed the OPC UA Server. The default path is **C:\Program Files (x86)\Emerson\Plantweb Optics OPC UA Server \OPCUA**.
    b) Double-click **Emerson.OPC.UA.Server.Tool.exe**.
    c) If prompted, select **Yes** to allow the application to make changes to your device.
    d) Select **Manage Certificate Store**.
    e) Select **Trust a certificate**.
    f) Enter the file name of the certificate.
2. From the OPC UA client, add the OPC UA Server certificate as a trusted certificate.

16.2 Connect an OPC UA client

Building the plant hierarchy can take several minutes after installing the Plantweb Optics OPC UA Server and rebooting the computer. Allow several minutes after installing or rebooting before attempting to connect OPC UA clients to the Plantweb Optics OPC UA Server.

The Plantweb Optics OPC UA Server has security features that protect your connection and your data. You may configure these settings after installation and setup.

Prerequisites

The OPC UA client certificate must be a trusted certificate of the OPC UA server.

Procedure

1. From your OPC UA Client, supply the connection information of the OPC UA server.
   The OPC UA URL is **opc.tcp://[server]:4840**, where [server] is the computer name of the Plantweb Optics OPC UA server.
2. **Security Settings**—From your OPC UA client, select the security policy and message security mode that applies to your network. The Plantweb Optics OPC UA server supports these security settings:
   a) Security Policy
      - Basic128Rsa15
      - Basic256
      - Basic256Sha256

   b) Message Security Mode
      - Sign
      - Sign and Encrypt
3. **Authentication Settings**—An OPC UA client may be able to connect to the OPC UA server via a predetermined username and password, or through certificate validation. To enable an OPC UA client to connect to the server via username and password, an Administrator must add the user to the Plantweb Optics OPC UA Users Windows Group.

16.3 Security settings on an OPC UA Server

The Plantweb Optics OPC UA Server has security features that protect your connection and your data. You may configure these settings after installation and setup.

Prerequisites

The OPC UA client certificate must be a trusted certificate of the OPC UA server.

Procedure

1. **Security Settings**—From your OPC UA client, select the security policy and message security mode that applies to your network. The Plantweb Optics OPC UA server supports these security settings:
   a) Security Policy
      - Basic128Rsa15

- Basic256
- Basic256Sha256

b) Message Security Mode

- Sign
- Sign and Encrypt

2. **Authentication Settings**—An OPC UA client may be able to connect to the OPC UA server anonymously, via a predetermined username and password, or through certificate validation. To enable an OPC UA client to connect to the server via username and password, an Administrator must add the user to the Plantweb Optics OPC UA Users Windows Group.

16.4 Hierarchy filtering

This feature lets you filter nodes if you want to monitor specific nodes only. Filtering trims down the hierarchy on the address space and speeds up loading time for clients connecting with an OPC UA client. Filtering is done on the computer where the OPC UA Server is installed.

Procedure

1. From the Windows search bar, enter **Services**.
2. Open the Windows Services desktop application.
3. From the list of services, select **Plantweb Optics OPC UA Server**.
4. Right-click **Plantweb Optics OPC UA Server**, and then click **Stop**.
5. Run the Plantweb Optics OPC UA Server Tool:
   a) Go to the directory where you installed the OPC UA Server. The default path is **C:\Program Files (x86)\Emerson\Plantweb Optics OPC UA Server \OPCUA**.

   b) Double-click **Emerson.OPC.UA.Server.Tool.exe**.

   c) If prompted, select **Yes** to allow the application to make changes to your device.

   d) Select **Configure Node Filter**.

   e) Enter the path of the node that you want to monitor.

   Note
   When copying the path of the target node, exclude **Default Enterprise**.

6. Navigate back to **Services**.
7. Right-click **Plantweb Optics OPC UA Server**, and then click **Start**.

16.5 OPC tag information and data tree structure

The names of the OPC tags are usually dependent on the configuration of a system. Virtually all data acquired by Plantweb Optics is available through OPC.

In your OPC UA session, or within your OPC application, you can use an OPC browser to identify the data from an AMS 9420 sensor 1, overall. For example:

Default Enterprise → Default Site → Emerson Wireless ASI → Gateway 10.4.255.254 → Cooling Tower Mtr/Gearbox → Sensor 1 - Overall

In Plantweb Optics, the OPC tag names are created using the server name followed by each branch of the tree, then the individual parameter name; each separated by a period. Depending on the OPC browser, the parameters may or may not be listed alphabetically.

At the top level of the OPC hierarchy tree (the server name), these tags are available:

Table 16-1: OPC data tree structure

OPC path	Description
Server	Default Server name.
Server.Enterprise	Default Enterprise name.
Server.Enterprise.Site	Default Site name.
Server.Enterprise.Site.Location	Name of locations added to the site. A location can contain locations, assets, and devices.
Server.Enterprise.Site.Location.[Location|Asset|Device]	Name of a location, asset, or device.
Server.Enterprise.Site.Location.Asset	Name of an asset. An asset can contain assets, machines, and devices.
Server.Enterprise.Site.Location.Machine	A machine is a specific asset type that can contain other machines and devices.
Server.Enterprise.Site.Location.[Asset.Machine.]Device	A device contains data about the device and its measurement points.

The hardware portion of the OPC hierarchy tree is listed by Units.

Table 16-2: Device information

OPC path	Description	Data type
Server.Enterprise.Site.Location.Asset.Device. **Unitname.Status**	Status of the individual hardware device (Up, Down, Acknowledged)	String
Server.Enterprise.Site.Location.Asset.Device. **Unitname.IsOnline**	Status of the individual hardware device (On/Off)	Boolean

Table 16-3: Channel/Sensor information

OPC path	Description
Server.Device. **AI01.Description**	The hardware device name; for example, **Sensor -1** on a AMS 9420.

17 CMMS Interface

An essential part of asset reliability is the ability to identify, prioritize, and take corrective action to maintain assets. Plantweb Optics supports the ability to move asset issues, alerts, and maintenance tasks into the workflows currently in place in order to efficiently resolve problems and complete preventive maintenance tasks.

A Computerized Maintenance Management System (CMMS), such as IBM's Maximo or SAP's Plant Maintenance Module, helps plant maintenance personnel to:

- keep track of all the assets they are responsible for.
- schedule and track maintenance tasks (also called "work orders").
- keep a historical record of the work they perform.

Depending upon the type of CMMS Interface implementation, the asset may be a physical piece of equipment (listed as MTR-001, for example) or a functional location (listed as FCC-01-Reactor).

17.1 Configure CMMS Interface settings

Follow these steps to configure the CMMS Interface settings.

Prerequisites

A user requires the MANAGESYSTEMSETTINGS permission to access and configure these settings.

Procedure

1. Click the **FILE** tab at the top left side of the screen.
2. Click **System Settings** on the left side of the screen.
3. Click **CMMS Interface**. The **CMMS Interface** screen displays.
4. In the **Server** field, enter the name of the server where Plantweb Optics CMMS Interface is installed.
5. In the **Port** field, enter the port that Plantweb Optics will use to interface the Plantweb Optics Interface. For example, **8090**.
6. Plantweb Optics checks for the updated status of **Open Notifications** based on the Update Rate. In the **Update Rate** field, enter the number of minutes between polling intervals for updated health values.
7. Check **Enable Secure Connection (SSL)** if you want to use SSL (Secured Socket Layer). If this box is not checked, the **Domain**, **Username**, and **Password** fields are not displayed.
8. If you checked the **Enable Secure Connection (SSL)** checkbox, enter the following:
    a) In the **Domain** field, enter the name of the computer domain where Plantweb Optics CMMS Interface is installed.
    b) In the **Username** field, enter a valid machine user name on the machine where Plantweb CMMS Interface is installed.

c) In the **Password** field, enter a valid machine password on the machine where Plantweb CMMS Interface is installed.

9. In the **Maintenance Plant** field, enter the CMMS Maintenance Plant or Site ID.

Note
This global setting defines the context in which Plantweb Optics will interface the CMMS. Therefore, Plantweb Optics maintenance tasks shall only apply to assets in this Maintenance Plant.

10. In the **Notification Type** field, enter the type of CMMS Interface notification to be created.
11. Click **Enable Automatic Notifications** to enable or disable automatic notifications to be sent.
12. If you checked the **Enable Automatic Notifications** checkbox, in the **Asset Health Less Than or Equal** field, enter the minimum health index value that will send out an automatic work notification to CMMS Interface. For example, 25. In the **Asset Priority Greater Than or Equal** field, select **Not Set**.
13. Click **OK** to apply these changes.

17.2 Map assets to CMMS Interface individually

CMMS Interface uses an asset mapping feature to match up the assets as they are named in your SAP PM or IBM Maximo system with the naming conventions used in Plantweb Optics. The assets should be mapped by a user that has knowledge of the asset relationships between the two systems.

Complete these steps to individually map assets to CMMS Interface using Asset Explorer.

Note
In order to perform this task, the user must have MANAGESYSTEMSETTINGS permission.

Prerequisites

- Plantweb Optics is installed and licensed.
- Assets exist in CMMS Interface and in Plantweb Optics.
- Assets exist under the Location hierarchy.
- The Plantweb Optics user has permissions to map assets.

Procedure

1. Launch Plantweb Optics Asset Explorer.
2. Enter your user name and password. Click **Login**.
3. In the **Location** tab on the left side of the screen, navigate to the selected asset you want to map.
4. In the **Properties** tab on the right side of the screen, scroll to the **CMMS** heading. If you are properly licensed for CMMS Interface, you will see an **CMMS Asset ID** field listed here.
5. Enter the Plantweb **Asset ID** that you want to associate with this asset.

6. Click **Save**.

Postrequisites

An asset in SAP or Maximo has been mapped to a corresponding CMMS Interface asset ID.

17.3 Map assets to CMMS Interface in bulk

CMMS Interface uses an asset mapping feature to match up the assets as they are named in your SAP PM or IBM Maximo system with the naming conventions used in Plantweb Optics. The assets should be mapped by a user that has knowledge of the asset relationships between the two systems.

Complete these steps to map assets to CMMS Interface in bulk using a spreadsheet.

Prerequisites

- Plantweb Optics is installed and licensed.
- Assets exist in CMMS Interface and in Plantweb Optics.
- Assets exist under the **Location** hierarchy.
- The Plantweb Optics user has permissions to map assets.

Procedure

1. Launch Plantweb Optics Asset Explorer.
2. Enter your user name and password. Click **Login**.
3. Click the **Export** button on the ribbon bar to download and open a .CSV file in Excel. This file contains information about all of the assets.
4. In the **CMMS Mapping ID** column, enter the CMMS Interface Asset ID that you want to assign to each asset. Save the .CSV file.
5. Import the completed mapping spreadsheet to Plantweb Optics using Asset Explorer. Click the **Import** button on the ribbon bar. Click **Choose file** and browse to the .CSV file you updated and saved.
6. Plantweb Optics updates each asset with the appropriate CMMS Interface asset mapping.
7. In the **Location** tab on the left side of the screen, navigate to an asset to view its assigned CMMS Interface **Asset ID**.

Postrequisites

Assets have been mapped in SAP or Maximo to corresponding CMMS Interface asset IDs.

17.4 Create CMMS Interface work notifications manually

Plantweb Optics enables you to turn important asset alerts and diagnostics into work notifications that can be integrated into SAP PM or IBM Maximo. Work notifications can be created manually or automatically.

Complete these steps using Asset View to create a CMMS Interface work notification manually.

Prerequisites

- Plantweb Optics is installed and licensed.
- Assets are mapped to CMMS Interface assets.
- The Plantweb Optics user has CREATEWORKNOTIFICATION permissions.

Procedure

1. Launch Plantweb Optics Asset View.
2. Enter your user name and password. Click **Login**.
3. Select an asset from your Dashboard.
4. From the **Asset View** ribbon, click **New Notification**. The **New Work Notification** page displays.
5. On the **New Work Notification** page, complete these work notification fields.
    a) **Subject**. Enter the subject for the work notification.
    b) **Asset** and **CMMS Asset ID** fields are pre-filled.
    c) **Priority**. Set the priority of this work notification as **Low**, **Medium**, **High**, or **Very High**.
    d) **Description**. Write a short description of the problem to be addressed.
6. Click **OK**.
7. The work notification is submitted to the CMMS Interface and its status is **Pending** until confirmation is received from CMMS Interface that the notification has been created. Once the notification is created, the **Pending** status will be replaced with a numeric identifier for the notification.

17.5 Create CMMS Interface work notifications automatically

Plantweb Optics enables you to turn important asset alerts and diagnostics into work notifications that can be integrated into SAP PM or IBM Maximo. Work notifications can be created manually or automatically.

Complete these steps to create a CMMS Interface work notification automatically.

Note
In order to perform this task, the user must have CREATEWORKNOTIFICATION permission.

Prerequisites

- Plantweb Optics is installed and licensed.
- Assets are mapped to CMMS Interface assets.

Procedure

1. Click the **FILE** tab at the top left side of the screen.
2. Click **System Settings** on the left side of the screen.
3. Click **CMMS Configuration**. The **CMMS Configuration** screen displays.
4. Click **Enable Automatic Notifications** to enable or disable automatic notifications to be sent.
5. If you checked the **Enable Automatic Notifications** checkbox, in the **Asset Health Less Than or Equal** field, enter the minimum health index value that will send out an automatic work notification to CMMS Interface. For example, 25. In the **Asset Priority Greater Than or Equal** field, select **Not Set**. The **Not Set** value is the lowest **Asset Priority** value. The setting allows a user to specify that only assets with a priority setting will create an automatic notification.
6. Click **OK** to apply these changes.

17.6 View CMMS Interface work notifications

Plantweb Optics enables the user to view work notifications associated with their assets. Complete these steps using Asset View to view CMMS Interface work notifications.

Prerequisites

- Plantweb Optics is installed and licensed.
- Work notifications have been created.
- The Plantweb Optics user has permissions to view work notifications.

Procedure

1. Launch Plantweb Optics Asset View.
2. Enter your user name and password. Click **Login**.
3. On the Asset View Dashboard, click **Open Work Notifications**. A list of the open work notifications displays.
4. Select an asset from the list. It will be shown with a numeric identifier. For example, **1254: <asset name>**.
5. On the right side of the screen, this information about the work notification is displayed.
    a) **Created**. Time when the work notification was created.
    b) **CMMS Asset ID**. The CMMS Interface identifier for this asset.
    c) **Work Order ID**. The ID number for this work order.
    d) **Priority**. The priority for this work notification. For example, **Very High**.
    e) **Status**. The status of this work notification. For example, **Open**.
    f) A description of the problem.

6. Click the **Notifications** icon on the right side of the page to view tabs with information about **OPEN** notifications, **UNDELIVERED** notifications, **WORK HISTORY** associated with the notifications, and **MESSAGES** about notifications.

17.7 Manage undelivered work notifications

Plantweb Optics enables the user to view work notifications associated with their assets. However, at times due to configuration and other errors, work notifications are undeliverable.

Complete these steps using Asset View to manage these undeliverable CMMS Interface work notifications.

Prerequisites

- Plantweb Optics is installed and licensed.
- Assets are mapped to CMMS Interface assets.
- The Plantweb Optics user has permissions to create work notifications.

Procedure

1. Launch Plantweb Optics Asset View.
2. Enter your user name and password. Click **Login**.
3. On the Asset View Dashboard, click **Open Work Notifications**. A list of the open work notifications displays.
4. Click the **Notifications** icon on the right side of the page to view tabs with information about **OPEN** notifications, **UNDELIVERED** notifications, **WORK HISTORY** associated with the notifications, and **MESSAGES** about notifications.
5. Click the **UNDELIVERED** icon. The **Undelivered Notification** page displays in the center of the screen. A list of undelivered notifications is displayed.
6. Select an undelivered notification from the list. Notice the undelivered notification information that displays on the right side of the screen.
7. Click **Resend** to attempt to send the notification again, or click **Delete** to remove this notification from the system.
8. Click **Undelivered Notifications** in the Dashboard to see that this notification is no longer displayed.

18 Plantweb Optics Historian

Plantweb Optics displays the current health values for each asset. However, it is helpful to see how the health values have changed and trended over time. Plantweb Optics Historian provides you with a way to work with the assets' historical data so that you can analyze trends in the data.

Plantweb Optics Historian provides:

- health and asset parameter history trending.
- historical health value comparisons, including comparisons between assets of different types.
- event information related to historical trends.
- storage of messages and their associated images and files.
- auto archival and retrieval of data when maximum capacity is reached.

These features enable you to:

- view historical data for asset parameters.
- measure the value of investments made towards maintaining asset health.
- extract analytics from historical data and anticipate future maintenance and cost.

18.1 Plantweb Optics Historian user interface

Follow the steps below to use Plantweb Optics Historian.

Note
In order to perform this task, the user must have HISTORIZEASSET permission.

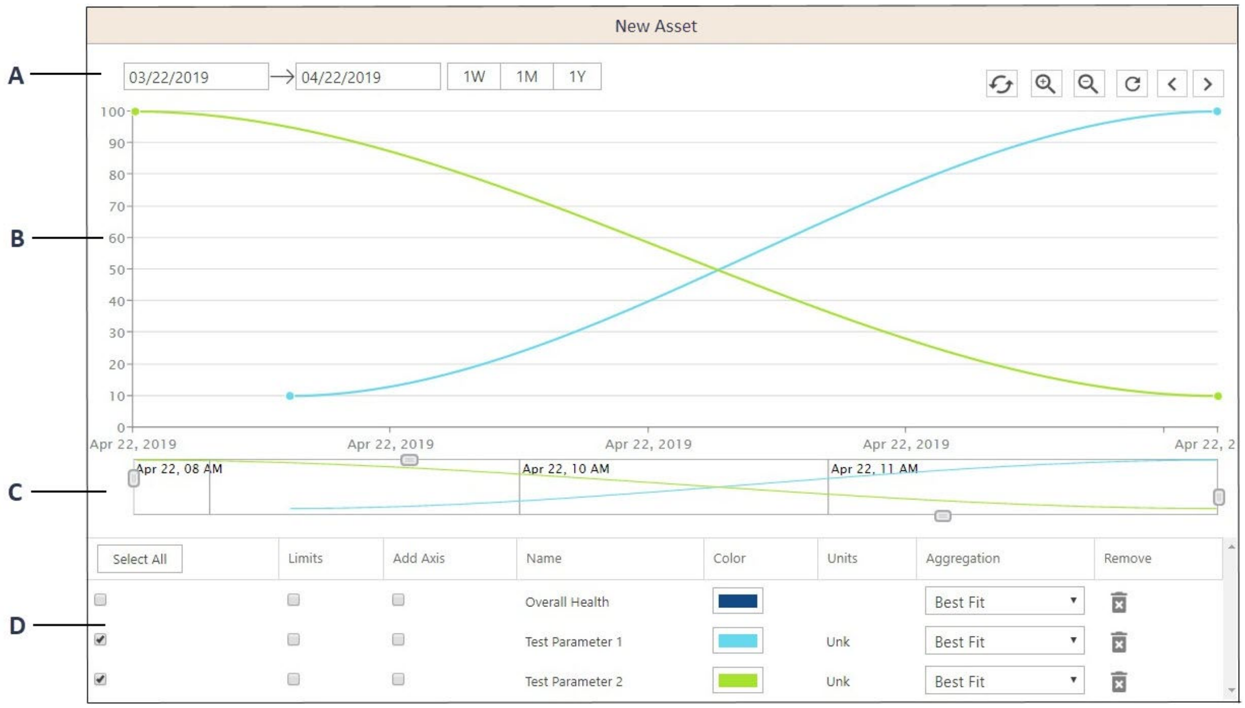
Prerequisites

- Plantweb Optics is installed and licensed.
- Assets exist in Plantweb Optics.
- Assets exist under the Location hierarchy.
- The Plantweb Optics user has permissions to use Plantweb Optics Historian.

Procedure

1. From Asset Explorer, using the **LOCATION** tab, click on an asset to select it.
2. On the right-side of the screen, click the **Historized** button. If the button shown is labelled **Unhistorized**, then click on the **Historize** button on the ribbon at the top of the screen to enable history for this asset. The trend screen for this asset displays. There are four areas of this screen.

Figure 18-1: Historian trend screen



A. ***Date range controls:*** *The top of the screen contains date fields that allow you to control the dates for the information to be displayed. The double arrow refreshes the chart data. The next buttons allow you to zoom in or zoom out. The single arrow resets the zoom to the original level. The right and left arrows allow you to move forward and backward through the data.*
B. ***Chart area****: The area of the screen where the trend chart displays.*
C. ***Ribbon****: The area that is used to select which portions of the data is displayed. Adjust sliders to change the range of data to display.*
D. ***Control panel****: The area at the bottom of the screen where you select the type of data that is displayed, its color, and the aggregation method used.*

3. In the **Date range controls** area at the top of the screen, select the date range to be displayed using any of these methods:
   a) Enter the date range for the chart in the date fields.
   b) Click 1W (one week), 1M (one month), or 1Y (one year) to display data for these lengths of time within the date range selected in the date fields.
   c) Click to refresh the chart data. Click it repeatedly to simulate a live data update.
   d) Click or to zoom in or out.
   e) Click to return the zoom to its original level.
   f) Click or to move forward or backward through the chart data in one-week increments.

4. In the **Chart area**, notice how the chart changes as you change date ranges, colors, and other selections on this screen.
5. In the **Ribbon** area just below the chart, around the edges of the ribbon there are sliders (boxes) that you can drag with your cursor to select the area of the data to display. You can also click within the selected area and drag the selected area to the left and right to view a portion of the data.
6. In the **Control Panel** area at the bottom of the screen, you can customize how you want the trend data to be displayed.
    a) You can add new parameters to the chart using a "drag and drop" function. Click on a parameter that is listed in the asset's **Latest Values** tab, then while continuing to press the left mouse button, drag and release the button in the **Control Panel** area of the chart. The new parameter is added as a selection that can be used on the chart.
    b) On the left side of the screen, click the checkboxes for the health parameters that you want displayed on the chart. The **Overall Health** information is displayed by default. Click **Select All** to check all of the boxes. Click **Select All** again to uncheck all of the boxes.
    c) In the **Limits** column, click the checkboxes to show limit lines in red on the chart. Click **Limits** to check all of the boxes. Click **Limits** again to uncheck all of the boxes.
    d) To see some of the data displayed on a different axis, click a checkbox in the **Add Axis** column to shift that selected data from the Y-axis on the left side of the chart to the Y-axis on the right side of the chart. One example of when this might be useful would be in the situation when one type of information is measured on a Fahrenheit scale and the other is on a pressure scale. Because of the different scales used to measure these two types of data, having the ability to isolate these lines will make it easier to see the relationship between the temperature and the pressure.
    e) The color selector allows you to change the colors of the lines in order to differentiate between selected trends. Click the color buttons in this column to select new colors to use. However, these color selections are not saved. Once the screen is closed, the colors revert back to their default colors.
    f) The **Agg. Method** column is used to select the aggregation method being used for the data.

Choice	Description
Best Fit	**Best Fit** is the default value. This method takes the minimum and maximum values recorded during the day and charts the middle value between these two points.
Raw	**Raw** displays every recorded data point for the day.
Average	**Average** charts an average of the data points and presents one average point per day.
Max	**Max** is the highest data point recorded during that day.

18.2 Use Latest Values for quick trend charts

Use the **Latest Values** tab to quickly display a trend chart for a single parameter.

Follow the steps below to use the **Latest Values** tab for quick trend charts.

Procedure

1. From Asset Explorer, using the **LOCATION** tab, click on an asset to select it.

   On the right-side of the screen, if the **Historized** button is displayed, then the asset is enabled for history collection.
2. Click the **LATEST VALUES** tab.
3. Click on the parameter you want to see charted.

   Note
   You can add new parameters to the chart using a "drag and drop" function. Click on a parameter that is listed in the asset's **Latest Values** tab, then while continuing to press the left mouse button, drag and release the button in the **Control Panel** area of the chart. The new parameter is added as a selection that can be used on the chart.
4. A trend chart displays for that selected parameter data.

18.3 View asset health using Health Details charts

Use the **Health** button on the right side of the screen in Asset Explorer to obtain quick health trend information.

Follow the steps below to use the **Health** button for quick health trend charts.

Procedure

1. From Asset Explorer, using the **LOCATION** tab, click on an asset to select it.
2. On the right-side of the screen, if the **Historized** button is displayed, then the asset is enabled for history collection.
3. Click the **Health** button.
4. The **Health Details** chart displays. This chart only shows information about the overall health of the asset. The overall health is calculated based on all of the parameter data combined into one value.
5. A trend chart displays for that selected parameter data.

18.4 Enable history collection for multiple assets

You can enable history collection one asset at a time, or you can enable them in bulk.

Follow the steps below to enable history collection for multiple assets at once.

Prerequisites

- Plantweb Optics is installed and licensed.

- Assets exist in Plantweb Optics.
- Assets exist under the Location hierarchy.
- The Plantweb Optics user has permissions to use Plantweb Optics Historian.

Note
The number of assets that can be historized is limited by your user license. See your Administrator regarding license changes.

Procedure

1. From Asset Explorer, click **Export Assets** in the **Bulk Edit** section of the ribbon.
   A .CSV file is exported with all of the assets listed.
2. Open the file in Microsoft Excel.
3. In the **Historized?** column, for each asset enter **true** (if you want history collected for this asset) or **false** (if you do not want history collected for this asset). Save the Excel file.
4. In Asset Explorer, click **Import** on the ribbon.
5. Click **Choose File** and browse to the Excel file you saved. Click **OK**.

A message displays showing that your import was successful, or an error is reported if the import was unsuccessful.

Postrequisites

It is a best practice to export the assets list once again and check it to ensure that the intended assets are now historized. Repeat this procedure if needed.

18.5 Disable history collection for an asset

Plantweb Optics displays the current health values for each asset that is enabled for history collection. However, you may need to disable an asset for history collection due to license or disk space limitations.

Follow the steps below to disable history collection for a specific asset.

Prerequisites

- Plantweb Optics is installed and licensed.
- Assets exist in Plantweb Optics.
- Assets exist under the Location hierarchy.
- The Plantweb Optics user has permissions to use Plantweb Optics Historian.

Procedure

1. From Asset Explorer, using the **LOCATION** tab, click on an asset to select it.
2. On the right-side of the screen, if the **Historized** button is displayed, then the asset is enabled for history collection.
3. From the ribbon at the top of the screen, click **Unhistorize** at the top of the screen to disable history collection for this asset.

18.6 Back up trend data

Use the **Optics Historian Db Admin Utility** to set up full and partial backups for the trend data.

Follow these steps to set up backups for Plantweb Optics Historian data.

Prerequisites

- Plantweb Optics Historian must be installed on the same system where the Optics Historian Db Admin Utility is run.
- The utility must be run with Administrator privileges.

Procedure

1. In the **C:\inmation.root\Plantweb Optics Historian Db Admin** folder, open a command prompt with elevated privileges.
2. Enter one of the following commands to use the functions of the Optics Historian Db Admin Utility

Command	Description
status	Retrieve the status of the system. For example, **OpticsHistorianDbAdminUtilityCommandLine.exe status**
backup	Creates a .zip file containing a backup of the Inmation img folder (the object structure) and the MongoDb data folder containing everything needed to fully restore the system. The user must select a path for the resulting file. For example, **C:\Test\fullBackup.zip**. **Note** The extension (.zip) must be part of the path. For example, **OpticsHistorianDbAdminUtilityCommandLine.exe backup –p "C:\Users\Administrator\Desktop\BR\fullbackup.zip"**
partialbackup	Similar to the full backup. However, the partial backup only backs up the data provided in a given time frame. User must select not only the output path (for example, **C:\Test\fullBackup.zip**), but also the timeframe that the user wishes to backup. For example, **OpticsHistorianDbAdminUtilityCommandLine.exe partialbackup -f "2019-03-12 12:00:00" -t "2019-03-14 12:00:00" -p "C:\Users\Administrator\Desktop\BR\partialbackup.zip"** **Note** Operations are performed only at the full hour mark. A given time of 1:35 is interpreted as 1:00.
restore	Uses the archive created during a full backup to restore the system. User must select a valid full backup archive for this to perform correctly. For example,

Command	Description
	OpticsHistorianDbAdminUtilityCommandLine.exe restore –p "C:\Users\Administrator\Desktop\BR\fullbackup.zip"
partialrestore	Uses the archive created during a full backup to restore the system. User must select a valid partial backup archive for this to perform correctly. For example, **OpticsHistorianDbAdminUtilityCommandLine.exe partialrestore -p "C:\Users\Administrator\Desktop\BR \partialbackup.zip"** **Note** Operations are performed only at the full hour mark. A given time of 1:35 is interpreted as 1:00.
purge	Deletes all data using the provided time frame. For example, **OpticsHistorianDbAdminUtilityCommandLine.exe purge -f "2019-03-12 12:00:00" -t "2019-03-14 12:00:00"** **Note** Operations are performed only at the full hour mark. A given time of 1:35 is interpreted as 1:00.
changePassword	Changes the Plantweb Optics Historian password. For example, **OpticsHistorianDbAdminUtilityCommandLine.exe changePassword -p "YOUR_NEW_PASSWORD"**

19 Databases

The software installations deploy databases into the SQL Server instance, EMERSONCSI. The sections below describe the database tables per installation.

Each database consists of several files that are created on disk in the default data directory. The location can be specified during installation. The default folder is `C:\EmersonCSI\Data`.

If the AMS Machinery Manager ASI is installed, a database named RbmSyncDb is deployed into the SQL Server instance, EMERSONCSI, on the server where the AMS Machinery Manager ASI Web App is installed.

Table 19-1: Databases

Module	Database
Plantweb Optics	EventDb
	FrameworkDb
	ImageDb
	MessageDb
	OnPremMobileServicesDb
	CMMSDb
	OpticsHistorianDb
AMS Machinery Manager ASI	RbmSyncDb
Plantweb Optics Historian	MongoDb

The recovery model can be set up differently on each database. The backup schedule for each database can be customized. However, Emerson recommends that each database is backed up with the same frequency. For instance, if a full backup is performed on each database every night, do not back up each database on a different night.

19.1 Back up and restore

Back ups

The Plantweb Optics Tier-1 and Tier-2 database options allow for two different backup strategies.

In a Tier-1 installation, automatic backup processing is available. See page 198 for more information.

A Tier-2 installation requires maintenance by a database administrator. Backups are expected to be performed by the database administrator. Please contact your database administrator or IT department for proper backup procedures as they relate to your overall backup strategy. If you do not have a database administrator or IT department, call Emerson Product Support to provide you with some basic database backup guidance.

Restore

If you need to restore any of the databases, contact your IT department or call Emerson Product Support to guide you on the proper restore procedure.

⚠ CAUTION

All Plantweb Optics databases and the AMS Machine Works database must be restored simultaneously to keep them synchronized.

19.2 Automatic backup for Tier-1 installations

Automatic backups are available for Tier-1 installations. During installation, the **Include Automated SQL Maintenance** option is selected by default when Tier-1 installation is selected. The automatic backups are triggered by scheduled tasks.

The scheduled tasks:

- are set for 2:00 AM (by default).
- run under the native "System" account.

The scheduled tasks do the following for each Plantweb Optics database:

1. Sets the Plantweb Optics databases to the simple recovery model
2. Processes a database backup
3. Shrinks the database log files

Backups are located by default under `C:\EMERSONCSI\DATA\Backups`. The two most recent backups are saved in folders named `Last` and `Prev`.

Note
Automatic backups are only available with new installations. If you upgrade from the previous version, this feature is not available.

20 Troubleshooting

Installation

<table>
<tr><th>Error</th><th>Background</th><th>Solution</th></tr>
<tr><td>The required port to install Plantweb Optics is used by another application</td><td>Port 80 and port 443 are required and used by Plantweb Optics.
If these ports are not available or used by another application, open up the ports or redirect the website using these ports.</td><td>1. Launch IIS Manager.
2. On the Connections pane, expand PC name → Sites.
3. Click Default Web Site.
4. On the Actions pane, click Bindings.
5. On the Site Bindings page, select port 80 or port 443 and click Edit.
6. On the Edit Site Binding page, enter another port number, and click OK.</td></tr>
<tr><td rowspan="5">Plantweb Optics installation failure</td><td rowspan="5">Plantweb Optics installation may fail for several reasons.</td><td>See the installation logs for additional information on the cause of the installation failure. Installation logs are in <code>C:\Users\<username>\AppData\Roaming\Emerson_ADMLogs\<random GUID folder></code>.</td></tr>
<tr><td>A probable cause of installation failure is the total length of the installation path. It should not exceed 260 characters. Shorten or change the installation path.</td></tr>
<tr><td>You may need to change your computer name before installing the software. Special characters (< > ; : " * + = \ | ? , _ !), accented characters, and other multibyte characters in a computer name can cause problems and interfere with a successful installation. A valid computer name can have numbers 0-9, uppercase and lowercase letters A-Z, and the hyphen (-). Computer names cannot have only numbers, nor can they contain spaces.</td></tr>
<tr><td>Use the same server setting, either IP address or server name as the Plantweb Optics configuration, when installing or upgrading components, ASIs, or extensions. For example, when you choose the Use Server Name option in the Server and Port Binding Configuration screen during the installation, you must enter the name of the Plantweb Optics server.
Failure to use the same configuration as Plantweb Optics when installing or upgrading components, ASIs, and extensions may cause the installation to fail and you will need to uninstall and reinstall the software to configure the same server setting.</td></tr>
<tr><td>Ensure the Windows Update service is running.
Note
Windows Update service is different from automatic updates. If you turn off automatic updates, make sure the Windows Update service is not unintentionally turned off.</td></tr>
</table>

Error	Background	Solution
		When the installer has more than one .exe included, always run **install.exe** rather than setup.exe to install Plantweb Optics and its components. Running install.exe checks that the system has necessary prerequisite software, for proper installation to continue. Some installers only have one .exe included. Always refer to the instructions for your installation.
		If you chose to have the database on a separate server from where the software is installed, you must enable TCP/IP and the SQL Server (EMERSONCSI) and SQL Server Browser services have to be running on the database server. **To enable TCP/IP:** 1. Launch SQL Server Configuration Manager. 2. On the left pane, expand the **SQL Server Network Configuration** node. 3. Select the **Protocols for EmersonCSI**. 4. On the right pane, right-click **TCP/IP** and select **Enable**. **To enable the services:** 1. Launch SQL Server Configuration Manager. 2. On the left pane, select **SQL Server Services**. 3. On the right pane, right-click **SQL Server (EMERSONCSI)** and select **Start**. 4. Right-click **SQL Server Browser** and select **Start**.
		Plantweb Optics installation will fail if there are database files from a previous installation in the EmersonCSI\Data folder. You need to remove the database files from a previous installation. See Knowledge Base Article NK-1600-0344 for a complete list of database files to be removed.

Error	Background	Solution
Error when installing SQL Server 2017	**Note** During default installation, Microsoft SQL Server 2017 Express is automatically installed and configured for Plantweb Optics. There is no need to install SQL Server 2017 if there is no SQL Server currently installed on the Plantweb Optics server. If you will manually install SQL Server 2017, make sure the account running the SQL Server setup has rights to back up files and directories, rights to manage auditing and the security log, and the right to debug programs.	1. Launch Control Panel. 2. Go to **Administrative Tools** → **Local Security Policy**. 3. Navigate to **Local Policies** → **User Rights Assignment**. 4. Double-click the **Back up files and directories** policy. 5. Check to see if the user account running the SQL Server setup is listed. If it is not, click **Add User or Group** to add it, and click **OK** to close the dialogs. 6. Double-click the **Debug programs** policy. 7. Check to see if the user account running the SQL Server setup is listed. If it is not, click **Add User or Group** to add it, and click **OK** to close the dialogs. 8. Double-click the **Manage auditing and security log** policy. 9. Check to see if the user account running the SQL Server setup is listed. If it is not, click **Add User or Group** to add it, and click **OK** to close the dialogs.
Error that ribbon bar is not updated after an ASI (or interface) registration install has been processed successfully.	This results from the Plantweb Optics cache not being updated.	Reboot the Plantweb Optics Server to correct the problem.

Launching Plantweb Optics utilities

Error	Background	Solution
Cannot launch Plantweb Optics utilities in Internet Explorer	If Enhanced Security Configuration is enabled in Internet Explorer, the Plantweb Optics server URL must be added to the list of trusted sites.	In Internet Explorer: 1. Click **Tools** → **Internet Options**. 2. Select the **Security** tab and click **Trusted sites**. 3. Click **Sites**. 4. In the **Add this website to the zone** field, enter `https://[server]`, where [server] is the computer name or IP address of the Plantweb Optics server. 5. Click **Add**.

AMS Machinery Manager ASI

Error	Background	Solution
Cannot import AMS Machinery Manager databases Cannot poll AMS Machinery Manager for updates	By default the installation creates a guest user account in the AMS Machinery Manager Network Server. This account is used for database import and data polling. When there is a guest user limit specified in the AMS Machinery Manager Network Server, you need to make sure that the number is adequate and includes the account used by the AMS Machinery Manager ASI.	1. In Windows Services, stop the **AMS Machinery Manager IO Service**. 2. In AMS Machinery Manager, do the following: • Select **Tools** and launch **RBM Network Administration** (RBMadmin). • In RBMadmin, click **File** → **Preferences**. • If the **Limit To** field is checked, make sure the number in the Guest Users box is adequate for all guest users including in the count the account used by the AMS Machinery Manager ASI. It may be necessary to increment the number in the Guest Users box by 1 to accommodate the AMS Machinery Manager ASI user account. 3. In Windows Services, start the **AMS Machinery Manager IO Service**.
	The AMS Machinery Manager IO Service needs to be running in order to add the AMS Machinery Manager ASI asset source and to import AMS Machinery Manager databases.	On the computer where the AMS Machinery Manager ASI Service is installed, do the following: • In Windows Services, right-click the **AMS Machinery Manager ASI IO Service** and select **Properties**. • On the General tab, select **Automatic** from the Startup type menu. • Click **Apply**. • Click **OK**.
	The import or polling may have communication errors during the first try.	Try reimporting the database again. If the issue persists, contact customer support.

SSL and certificates

Error	Background	Solution
Cannot add an AMS Machinery Manager Asset Source to Plantweb Optics	If the AMS Machinery Manager certificate is not installed on the AMS Machinery Manager Network Server (where the AMS Machinery Manager IO Service is installed), the Asset Explorer utility will not be able to connect to AMS Machinery Manager.	If the AMS Machinery Manager ASI Service is running, check that the certificate is installed on the AMS Machinery Manager station. An administrator can launch certlm.msc or certmgr.msc to see if the AMS Machinery Manager certificate is installed. See page 51 for instructions.

Error	Background	Solution
Cannot add a Wireless Gateway Asset Source to Plantweb Optics	A certificate must be installed on the computer where the browser resides. Often, this is the Plantweb Optics server, but it is not required to be.	Check to ensure that the certificate that is installed is the same as the certificate that is bound to the EmersonCSI website. This may be the Emerson Wireless Gateway certificate, or it could be another ASI's certificate, or it could be the platform's certificate.

Plantweb Optics OPC UA server

Error	Background	Solution
Data and hierarchy in the OPC UA client are not in sync with data and hierarchy in Plantweb Optics.	Building the plant hierarchy in the OPC UA client can take several minutes after installation or reboot of Plantweb Optics.	Allow several minutes after installation or reboot Plantweb Optics before attempting to connect OPC UA clients.
		If several minutes have passed and data in OPC UA client is still not in sync with data in Plantweb Optics, do the following: 1. In Windows Services, locate the **Plantweb Optics OPC UA Server** service. 2. Stop and then restart the service.

A Requirements for separate server (Tier-2) installations

A.1 Separate server (Tier-2) installation

A Tier-2 installation installs the system's databases on a separate SQL database server. For a Tier-2 installation, you need to set up the SQL database server and the Plantweb Optics server in a specific order.

1. Set up the separate SQL Server for a Tier-2 installation. See page 205.
2. Set up the Plantweb Optics server before a Tier-2 installation. See page 208.
3. Install Plantweb Optics on the computer you designate as the Plantweb Optics server. During installation, choose a Tier-2 installation and supply information about the database server. See page 64.

   Important
   After installation, do not start using the software or install other components until you have completely set up the system for a Tier-2 installation.

4. Finish post-installation set up on the Plantweb Optics server. See page 208.
5. Set up the ASI server before installing an ASI on a Tier-2 system. See page 211.

   Note
   This step is only required if you install the ASI on a separate server.

A.2 Set up a separate SQL server for a Tier-2 installation

Important
Complete these steps on the separate SQL server before installing Plantweb Optics on the computer you designate as the Plantweb Optics server.

Prerequisites

Plantweb Optics is NOT yet installed.

Procedure

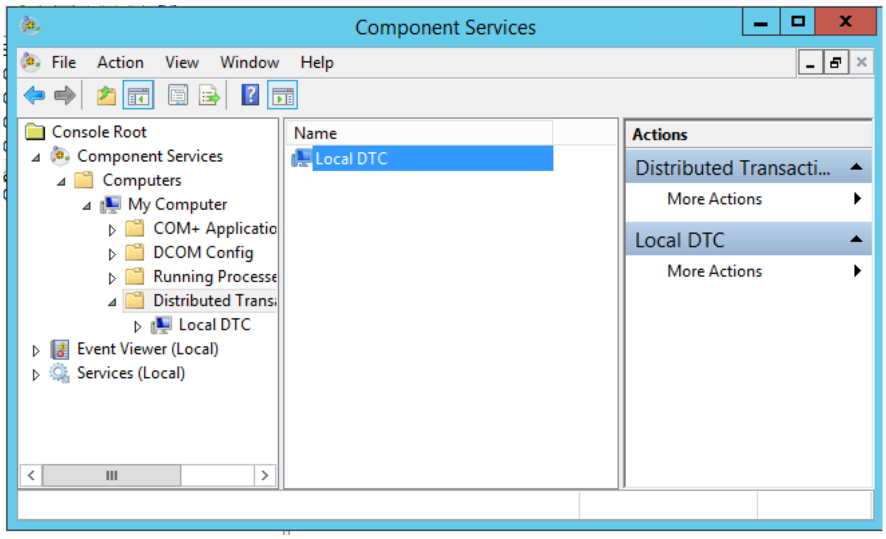
1. On the separate SQL server, ensure the server meets the following requirements to host the system's databases.
   - SQL 2017 is the minimum version supported
   - SQL Instance name must be **EMERSONCSI**
   - Remote connections must be enabled
   - Mixed authentication (Windows & SQL) must be enabled

- TCP/IP protocol must be enabled for the **EmersonCSI** SQL Server Network Configuration (SQL Server Configuration Manager)
- SQL Browser must be running and set to auto-start
- A static port for the **EMERSONCSI** SQL Instance must be set.

2. Update settings for Microsoft Distributed Transaction Coordinator (MDTC):

   a. In **Windows Component Services**, browse to **Component Services** → **Computers** → **My Computer** → **Distributed Transaction Coordinator** → **Local DTC**.

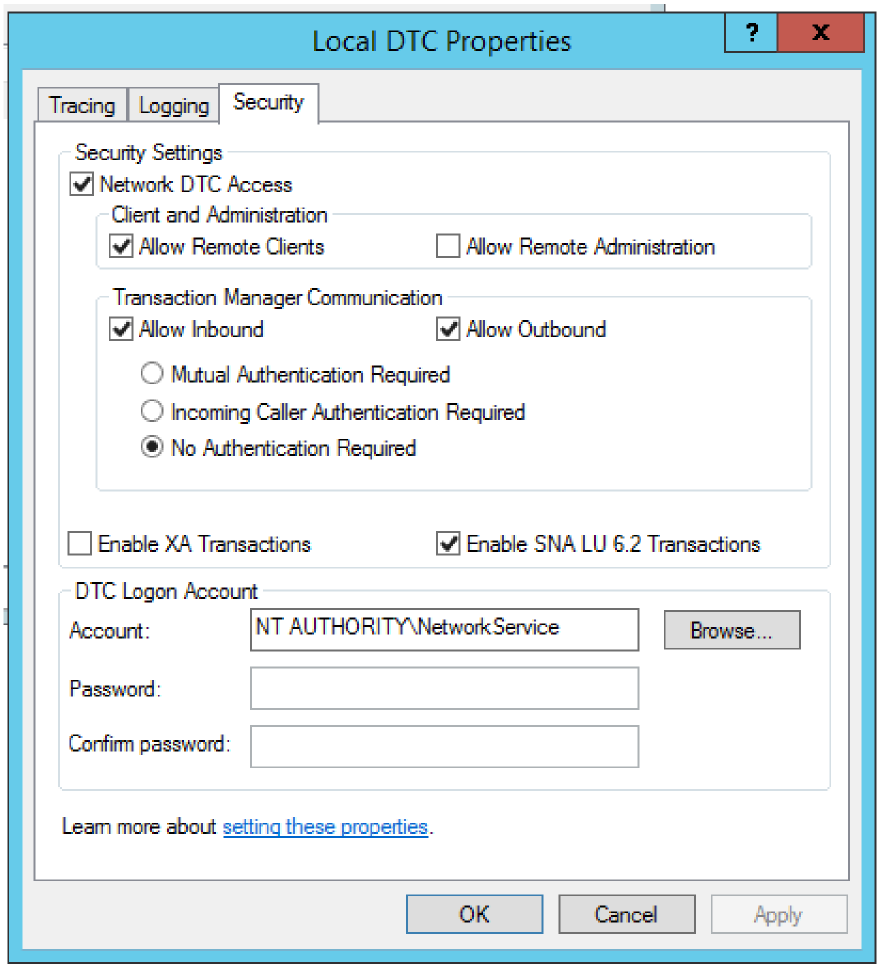
   Figure A-1: Windows Component Services expanded to Local DTC

   b. Select **More Actions** → **Properties**.

   c. In the Local DTC Properties dialog, select the Security tab and change the following settings:
      - Check **Network DTC Access**.
      - Check **Allow Remote Clients**.
      - Check **Allow Inbound**.
      - Check **Allow Outbound**.
      - Select **No Authentication Required**.
      - Check **Enable SNA LU 6.2 Transactions**.
      - The DTC Logon Account should be **NT AUTHORITY\Network Service**.

Figure A-2: Local DTC Properties dialog with required settings



3. Set communication ports and firewall rules.

Inbound communication	Firewall rule
Distributed Transaction Coordinator (RPC)	Predefined firewall rule in Server 2012 R2
Distributed Transaction Coordinator (RPC-EPMAP)	Predefined firewall rule in Server 2012 R2
Distributed Transaction Coordinator (TCP-In)	Predefined firewall rule in Server 2012 R2
UDP Port 1434	SQL Browser
TCP Port 1433	SQL
EMERSONCSI SQL instance TCP port	SQL

Outbound communication	Firewall rule
Distributed Transaction Coordinator (TCP-Out)	Predefined firewall rule in Server 2012 R2
UDP Port 1434	SQL Browser
TCP Port 1433	SQL
EMERSONCSI SQL instance TCP port	SQL

A.3 Set up the Plantweb Optics server before a Tier-2 installation

In a Tier-2 installation, when your SQL database is on a separate server, you need to change firewall settings on the Plantweb Optics server before and after installing the software, and before using the software. This section covers the settings you need to change on the Plantweb Optics server before installation.

Prerequisites

Set up the separate SQL Server for a Tier-2 installation.

Procedure

On the Plantweb Optics server, enable the ports for SQL communication to and from the server.

Inbound communication	Firewall rule
UDP Port 1434	SQL Browser
TCP Port 1433	SQL
EMERSONCSI SQL instance TCP port	SQL

Outbound communication	Firewall rule
UDP Port 1434	SQL Browser
TCP Port 1433	SQL
EMERSONCSI SQL instance TCP port	SQL

Postrequisites

Make sure you have **sa** rights on the EMERSONCSI SQL instance or know the credentials of the SQL account that has those rights before proceeding with Plantweb Optics installation.

A.4 Tier-2 post-installation setup

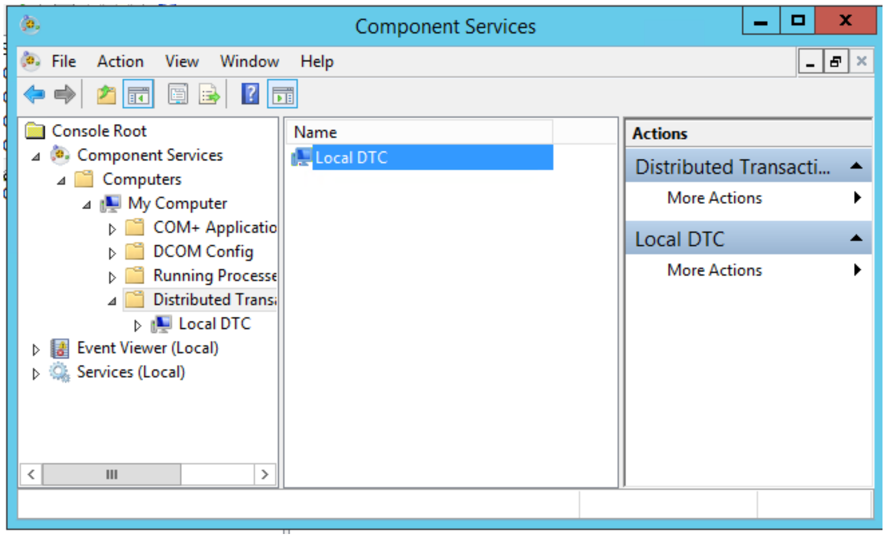
Complete this setup on the Plantweb Optics server after installing the software and before you start using it or installing other components.

Procedure

1. Update settings for Microsoft Distributed Transaction Coordinator (MDTC):

   a. In **Windows Component Services**, browse to **Component Services** → **Computers** → **My Computer** → **Distributed Transaction Coordinator** → **Local DTC**.

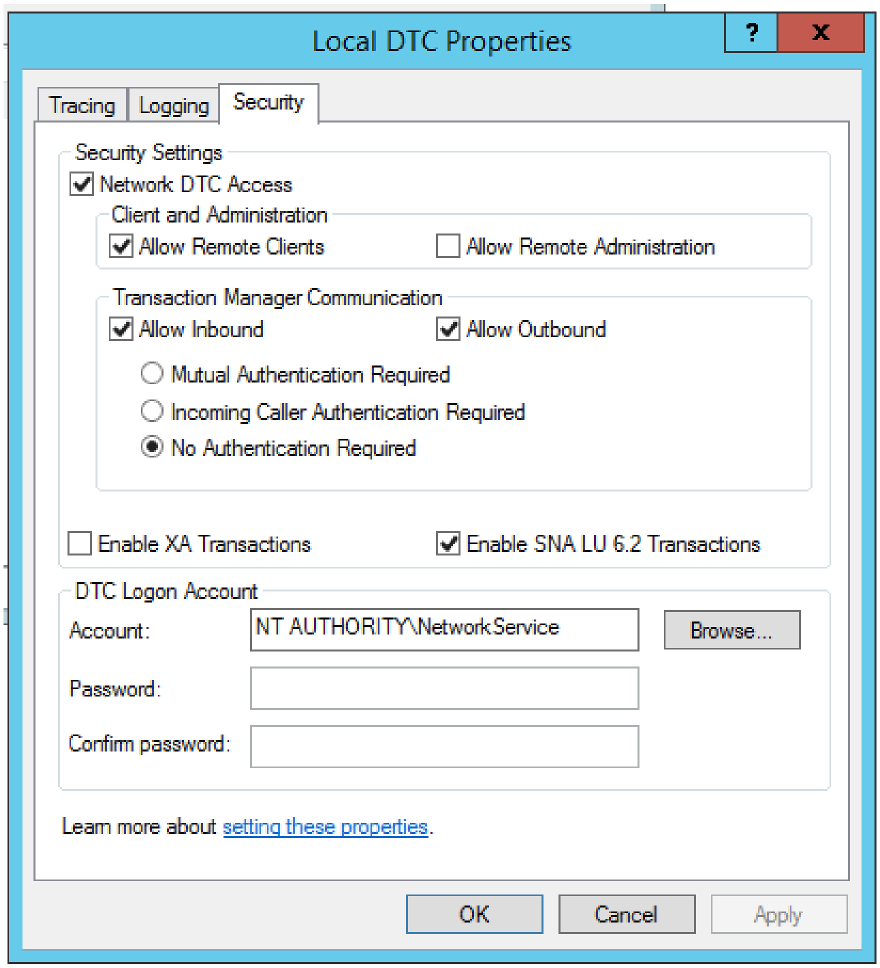
   Figure A-3: Windows Component Services expanded to Local DTC

   b. Select **More Actions** → **Properties**.

   c. In the Local DTC Properties dialog, select the Security tab and change the following settings:
      - Check **Network DTC Access**.
      - Check **Allow Remote Clients**.
      - Check **Allow Inbound**.
      - Check **Allow Outbound**.
      - Select **No Authentication Required**.
      - Check **Enable SNA LU 6.2 Transactions**.
      - The DTC Logon Account should be **NT AUTHORITY\Network Service**.

Figure A-4: Local DTC Properties dialog with required settings



2. Enable the predefined firewall rules to allow SQL communication.

Inbound communication	Firewall rule
Distributed Transaction Coordinator (RPC)	Predefined firewall rule in Server 2012 R2
Distributed Transaction Coordinator (RPC-EPMAP)	Predefined firewall rule in Server 2012 R2
Distributed Transaction Coordinator (TCP-In)	Predefined firewall rule in Server 2012 R2

Outbound communication	Firewall rule
Distributed Transaction Coordinator (TCP-Out)	Predefined firewall rule in Server 2012 R2

Note
These predefined rules are available on the Plantweb Optics server after you install the software. If the rules are not present, you may need to re-install Plantweb Optics.

Postrequisites

Install other components, as needed.

A.5 Set up the ASI server before installing the ASI on a Tier-2 system

Note
This step is only required if you install the ASI on a separate server.

This action requires connection to the SQL Server hosting the database that has rights to insert information into Plantweb Optics tables; this is known as “Action Registration." The SQL communications usually require additional access through server and network firewalls. The ASI server only needs these firewall exemptions for Action Registration during installation. If the SQL communication is not available, you will get "Action Registration" failures during the ASI installation. The firewall exceptions described here can be restored (removed) after the ASI installation is complete.

Prerequisites

- This is a Tier-2 installation. The Plantweb Optics server does not host the databases. The databases are hosted on a separate SQL server.
- Plantweb Optics installation is complete.

Procedure

- On the target server, and any intervening firewalls, enable the ports for SQL communication to the SQL database server.

Inbound communication	Firewall rule
UDP Port 1434	SQL Browser
TCP Port 1433	SQL
EMERSONCSI SQL instance TCP port (static)	SQL

Outbound communication	Firewall rule
UDP Port 1434	SQL Browser
TCP Port 1433	SQL
EMERSONCSI SQL instance TCP port (static)	SQL

Postrequisites

- Install the selected ASI on the target server.

- You can remove these exceptions on the ASI server after the ASI installation is complete.

B Internet Information Services (IIS) Reference

Note
When components are installed on separate servers, the EmersonCSI base website references the DefaultAppPool application pool.

Table B-1: IIS Module Plantweb Optics Services

Application Pool	Site
Plantweb_Optics_AssetExplorer	\AssetExplorer
Plantweb_Optics_AssetView	\AssetView
Plantweb_Optics_Apps	\DM
Plantweb_Optics_Apps	\EventViewer
Plantweb_Optics_Apps	\UserManager
Plantweb_Optics_Apps	\WirelessDeviceConfig
Plantweb_Optics_IdSrv	\OpticsIdSrv
Plantweb_Optics_LicenseMgmt	\LicenseMgmt
Plantweb_Optics_PlantImages	\PlantImages
Plantweb_Optics_PlantMgmt	\PlantMgmt
Plantweb_Optics_Security	\Security
Plantweb_Optics_Svcs	\Actions
Plantweb_Optics_Svcs	\CMMS
Plantweb_Optics_Svcs	\Help
Plantweb_Optics_Svcs	\KPIServices
Plantweb_Optics_Svcs	\MobileServices
Plantweb_Optics_Svcs	\Notifications
Plantweb_Optics_Svcs	\OnPremAssetView
Plantweb_Optics_Svcs	\OnPremMobileServices
Plantweb_Optics_Svcs	\OpticsHistorian
Plantweb_Optics_Svcs	\PlantEvents
Plantweb_Optics_Svcs	\PlantMessages
Plantweb_Optics_Svcs	\PlantStatus
Plantweb_Optics_Svcs	\PluginInfo
Plantweb_Optics_Svcs	\Reference
Plantweb_Optics_Svcs	\Resources

Table B-1: IIS Module Plantweb Optics Services *(continued)*

Application Pool	Site
Plantweb_Optics_Svcs	\RuntimeDataServices
Plantweb_Optics_Svcs	\Settings
DeviceManager	\DeviceManager

Table B-2: IIS Module Emerson Wireless Gateway ASI

Application Pool	Site
EWGASI	\EWGASI

Table B-3: IIS Module AMS Asset Monitor Data Collector

Application Pool	Site
AMSAssetMonitorDataCollector	\AMSAssetMonitorDataCollector

Table B-4: IIS Module AMS Device Manager Data Collector

Application Pool	Site
AMSDeviceManagerDataCollector	\AMSDeviceManagerDataCollector

Table B-5: IIS Module DeltaV Control Loop Data Collector

Application Pool	Site
DeltaVControlLoopDataCollector	\DeltaVControlLoopDataCollector

Table B-6: IIS Module KNet Data Collector

Application Pool	Site
KNetDataCollector	\KNetDataCollector

Table B-7: IIS Module AMS Machinery Manager ASI

Application Pool	Site
AMS_MMASI_App	\MMASI
AMS_MMASI_Svc	\MMASISvc

Table B-8: IIS Module Plantweb Insight ASI

Application Pool	Site
InsightASI	\InsightASI

C Windows services

Component	Windows service
Plantweb Optics	ARES WatchdogService
Plantweb Optics OPC UA Server	Plantweb Optics OPC UA Server
AMS Machinery Manager ASI	AMS Machinery Manager IO Service

D Device compatibility

AMS 9420 Wireless Vibration Transmitter

The following versions of the AMS 9420 are supported.

Revision	Latest version	Older versions
HART/Universal	7	7
Field device	4	3
Software	6	3 and above
Hardware	5	1, 5
DD (Device Descriptor)	7, 8	1

You can view the revision information from a Field Communicator or from AMS Device Manager. See the AMS 9420 Reference Manual for more information.

Emerson Wireless Gateway

Emerson Wireless Gateway ASI supports Emerson Wireless Gateway version 3.x.x., version 4.x.x., and later versions.

Rosemount 1420 Smart Wireless Gateway hardware versions 3.0 and 4.0 and firmware versions3.9.xx, 4.x.xx, or latest are supported.

Rosemount 1410 Smart Wireless Gateway hardware version 4.0 and firmware versions 4.6.64 or latest are supported.

AMS Device Manager

AMS Device Manager Data Collector v1.5 supports AMS Device Manager versions 13.5 and 14.0.

AMS Device Manager Data Collector v1.5.1 supports AMS Device Manager versions 13.1.1, 13.5, 14.0, and 14.1.1.

DeltaV Control Loop

DeltaV Control Loop Data Collector v1.5 supports DeltaV ProfessionalPlus and Application Station versions 12.3.1, 13.3.1, and 14.3.1. ProfessionalPlus requires the Control Performance Statistics (CPS) hotfix.

KNet

KNet Data Collector v1.5 supports KNet server version 5.1.

AMS Machinery Manager

AMS Machinery Manager ASI supports AMS Machinery Manager version 6.3 and the supported devices for v6.3.

E Component and system compatibility

This appendix shows supported software versions for system compatibility.

Table E-1: Component and system compatibility

Item	Supported versions
AMS Device Manager (*DeltaV Co-deployment with AMS Device Manager supported versions)	v13.5
	v14.0
	v14.1.1
AMS Machinery Manager	v6.3
Plantweb Insight	v1.5.022 or later
OPC UA Clients	OPC UA Expert v1.4.4 or latest
	Integration Objects
	Prosys
CMMS Interface (SAP—Plant Maintenance)	ECC 6.0 SAP R/3 4.7 ECC 5.0 S/4 HANA
CMMS Interface (Maximo— Preventive Maintenance)	MAXIMO 7.1 or higher
Inmation Historian	v1.3.2
NLINK Server	v7.0

F Security compliance

CIS Microsoft IIS benchmarks are applied to Plantweb Optics to establish Microsoft IIS security integrity. For the most current detailed information on security posture and requirements, see *AMS Product Security Documentation, AMS-SEC-PSG 001*, or contact your local Business Partner.

Index

A

B

C

D

E

H

I

K

L

M

Emerson
12001 Technology Drive
Eden Prairie, MN 55344 USA
T +1 865-675-2400
F +1 865-218-1401
www.Emerson.com

EMERSON™