

# Plantweb™ Optics v1.6

## Plantweb™ Optics System Guide



## Copyright

© 2021 by Emerson. All rights reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means without the written permission of 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:

<b>Phone</b>	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)
<b>Email</b>	<a href="mailto:ap-sms@emerson.com">ap-sms@emerson.com</a>
<b>Web</b>	<a href="http://www.emerson.com/en-us/contact-us">http://www.emerson.com/en-us/contact-us</a>

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

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

# Contents

<b>Chapter 1</b>	<b>Introduction.....</b>	<b>7</b>
<b>Chapter 2</b>	<b>Quick start.....</b>	<b>9</b>
	2.1 Preparing for installation.....	9
	2.2 Installing the Plantweb Optics platform.....	9
	2.3 Installing ASIs.....	9
	2.4 Installing optional services.....	13
	2.5 Completing post-installation steps.....	13
<b>Chapter 3</b>	<b>Planning your system.....</b>	<b>15</b>
	3.1 Guidelines for planning your system.....	15
	3.2 System components.....	15
	3.3 Deployment scenarios.....	17
	3.3.1 Tier 1 - single-server deployment scenarios.....	18
	3.3.2 Tier 2 - Distributed deployment scenario.....	23
	3.4 Database deployment.....	24
	3.5 Internet Information Services (IIS).....	25
	3.6 System requirements.....	25
	3.7 System scalability.....	30
<b>Chapter 4</b>	<b>Plantweb Optics security.....</b>	<b>33</b>
	4.1 Firewall considerations.....	33
	4.1.1 Ports for a host-based firewall.....	33
	4.1.2 Ports for a network-based firewall.....	37
	4.2 SSL/TLS certificates.....	38
	4.2.1 System components with certificates.....	40
	4.2.2 Certificate installation checklist.....	42
	4.3 Additional security considerations.....	44
<b>Chapter 5</b>	<b>Plantweb Optics installation procedures.....</b>	<b>45</b>
	5.1 Acquire licenses.....	45
	5.2 Install the Plantweb Optics Historian.....	46
	5.3 Install Plantweb Optics Web Services.....	47
	5.4 Register licenses.....	51
	5.4.1 Manually register a Plantweb Optics Mobile license when using Azure Mobile Services.....	51
	5.5 View license summary.....	52
	5.6 Install the Connector Service.....	53
<b>Chapter 6</b>	<b>ASI and AR installation procedures.....</b>	<b>55</b>
	6.1 Install the Proxy.....	55
	6.2 Configure the Proxy.....	57
	6.3 Install the AMS Asset Monitor ASI.....	59

6.3.1	AMS Asset Monitor ASI deployment scenarios.....	59
6.3.2	Register the AMS Asset Monitor ASI with Plantweb Optics.....	60
6.3.3	Install the AMS Asset Monitor Data Collector.....	61
6.3.4	Add an asset source to the AMS Asset Monitor Data Collector.....	62
6.4	Install the AMS Device Manager ASI.....	63
6.4.1	AMS Device Manager ASI deployment scenarios.....	64
6.4.2	Register the AMS Device Manager ASI with Plantweb Optics.....	66
6.4.3	Install the AMS Device Manager Data Collector.....	66
6.4.4	Add an asset source to the AMS Device Manager Data Collector.....	68
6.4.5	Opt-In to Device Parameters.....	70
6.5	Install the AMS Machine Works ASI.....	73
6.5.1	AMS Machine Works ASI deployment scenario.....	74
6.5.2	Register the AMS Machine Works ASI with Plantweb Optics.....	75
6.5.3	Install the AMS Machine Works Data Collector.....	76
6.5.4	Add an asset source to the AMS Machine Works Data Collector.....	77
6.6	Install the AMS Machinery Manager ASI.....	78
6.6.1	AMS Machinery Manager ASI deployment scenarios.....	79
6.6.2	Configure AMS Machinery Manager before importing databases.....	80
6.6.3	Register the AMS Machinery Manager ASI with Plantweb Optics.....	82
6.6.4	Install the AMS Machinery Manager Data Collector.....	82
6.6.5	Add an asset source to the AMS Machinery Manager Data Collector.....	84
6.7	Install the DeltaV Control Loop ASI.....	85
6.7.1	DeltaV Control Loop ASI deployment scenarios.....	86
6.7.2	Register the DeltaV Control Loop ASI with Plantweb Optics.....	87
6.7.3	Install the DeltaV Control Loop Data Collector.....	88
6.7.4	Add an asset source to the DeltaV Control Loop Data Collector.....	90
6.7.5	Change the ControlLoopSvc Windows user password.....	92
6.8	Install the Optics Analytics ASI.....	93
6.8.1	Optics Analytics ASI deployment scenarios.....	94
6.8.2	Register the Optics Analytics ASI with Plantweb Optics.....	95
6.8.3	Install the Optics Analytics Data Collector.....	96
6.8.4	Add an asset source to the Optics Analytics Data Collector.....	97
6.9	Install the Plantweb Insight ASI.....	99
6.9.1	Plantweb Insight deployment scenario.....	99
6.9.2	Register the Plantweb Insight ASI.....	101
6.9.3	Install the Plantweb Insight Data Collector.....	101
6.9.4	Add an asset source to the Plantweb Insight Data Collector.....	102
<b>Chapter 7</b>	<b>Post installation and certificate installation procedures.....</b>	<b>105</b>
7.1	Configure Active Directory for Plantweb Optics.....	105
7.2	Configure Plantweb Optics OIDC settings.....	106
7.3	Certificate installations.....	107

7.3.1	Install Plantweb Optics certificates.....	108
7.3.2	Install a Connector Service certificate.....	109
7.3.3	Install a Proxy certificate.....	109
7.3.4	Install certificates on Windows Server 2008 R2.....	110
7.3.5	Export a security certificate.....	111
7.3.6	Install a security certificate.....	112
7.4	Configure how emails are sent in Plantweb Optics.....	112
<b>Chapter 8</b>	<b>Mobile installation procedures.....</b>	<b>115</b>
8.1	Install the Plantweb Optics mobile app.....	115
8.2	Install the Plantweb Optics AR Mobile app.....	117
8.3	Set up on-premises mobile service.....	117
<b>Chapter 9</b>	<b>Uninstall Plantweb Optics, components, and Data Collectors.....</b>	<b>121</b>
<b>Chapter 10</b>	<b>Upgrade from a previous version.....</b>	<b>123</b>
<b>Chapter 11</b>	<b>Launch Plantweb Optics applications.....</b>	<b>125</b>
11.1	Data source asset screens (Launch in Context).....	126
11.2	Display data source asset screen using Asset Explorer.....	128
<b>Chapter 12</b>	<b>Databases.....</b>	<b>131</b>
12.1	Backup and restore.....	131
12.2	Automatic backup for Tier-1 installations.....	132
<b>Chapter 13</b>	<b>Troubleshooting.....</b>	<b>133</b>
<b>Appendix A</b>	<b>OPC UA and CMMS interfaces.....</b>	<b>139</b>
<b>Appendix B</b>	<b>Requirements for Tier-2, distributed deployment installations.....</b>	<b>141</b>
B.1	Tier-2 distributed deployment installation .....	141
B.2	Set up a separate SQL server for a Tier-2, distributed deployment installation.....	141
B.3	Set up the Plantweb Optics server before a Tier-2, distributed deployment installation.....	144
B.4	Tier-2 - distributed deployment post-installation setup .....	145
<b>Appendix C</b>	<b>Internet Information Services (IIS) reference and security compliance.....</b>	<b>149</b>
<b>Appendix D</b>	<b>Component and system compatibility.....</b>	<b>151</b>
<b>Index</b>	<b>.....</b>	<b>153</b>



# 1 Introduction

## Plantweb™ Optics

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 receives data from several asset sources such as external devices or systems. In addition, Plantweb Optics interfaces with enterprise Computerized Maintenance Management System (CMMS) to help plant maintenance personnel manage their assets and schedule maintenance.


Configuration and interaction with Plantweb Optics happen through the following applications, which you can launch from a web browser:

- **Asset View**—The main user interface to manage your assets with a persona-based view. This application contains a dashboard that shows automatic health scores, trends, messages, and the asset hierarchy. The Plantweb Optics mobile application provides access to this information on iOS and Android devices.
- **Asset Explorer**—Configure the platform and manage logical assets, data sources, and logical hierarchy of the system.
- **System Manager**—Manage users, licenses, mobile join keys, and permissions. View system generated events.

## About this guide

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.

## 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 pertaining to the release and is included in the installation files.
- Knowledge Base Articles (KBA)—documents released to address known issues, frequently asked questions, history traces, system requirements, how-to information, and application-specific content.
- Plantweb Optics tutorials and how-to video play-list—a series of short videos aimed at helping users understand Plantweb Optics and how to use this tool. Refer to the [Plantweb Optics Tutorial Series](#) link to access these valuable tutorials.





## 2 Quick start

This chapter contains topics on how to prepare and install Plantweb Optics, along with installing optional services and Asset Source Interfaces (ASIs). Emerson recommends that you complete each phase of the installation in the order it appears when installing 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, Connector Service, 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 the Plantweb Optics platform

Plantweb Optics Historian enables you to validate maintenance and operational responses based on past asset behaviors. The following steps are required for every Plantweb Optics installation.

### Procedure

1. Install Plantweb Optics Historian. Run the Plantweb Optics installer (A48OPTICS-SYSTEM0.Plantweb\_Optics.1.6.X.X) on the Plantweb Optics Server. See [Install the Plantweb Optics Historian](#).
2. Install Plantweb Optics Web Services by running the Plantweb Optics Installer (A48OPTICS-SYSTEM0.Plantweb\_Optics.1.6.X.X) on the Plantweb Optics Server. See [Install Plantweb Optics Web Services](#).
3. Register your Plantweb Optics License from the Plantweb Optics System Manager application. See [Register licenses](#).
4. View **License Summary** from the System Manager. See [View license summary](#).

## 2.3 Installing ASIs

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

- [AMS Asset Monitor ASI](#)
- [AMS Device Manager ASI](#)
- [AMS Machine Works ASI](#)
- [AMS Machinery Manager ASI](#)
- [DeltaV Control Loop ASI](#)
- [Optics Analytics \(KNet\) ASI](#)
- [Plantweb Insight ASI](#)

---

### Note

When navigating in your web browser, you can use either machine name or IP address of the Optics Server, Connector Service, Proxy, or Data Collectors.

### 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.  
See [System components](#) for information about the Data Collector component.
2. In Plantweb Optics, verify the Data Collector folder is listed in the **Source** tab.
3. Export the Plantweb Optics self-signed security certificate bound to port 443 (configurable default) in IIS. See [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. See [Install a security certificate](#). After importing a certificate, close any open browsers to ensure that the certificate is applied to your browsing session.

---

### Note

You can connect multiple Data Collectors to a single Connector Service.

See [System components](#) for information about the Connector Service component.

5. Ensure that the connection to Plantweb Optics is secure by navigating to `https://<OpticsServerMachineName>:<PortNumber>/AssetExplorer` in your web browser.

---

### Note

Where `https://<OpticsServerMachineName>:<PortNumber>/AssetExplorer` is the computer name where Asset Explorer is installed followed by the port number if it is different from the default port 443.

If the connection is secure, Asset Explorer appears – proceed to the next step. If the connection is not secure, a warning displays 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. See [Export a security certificate.](#)

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

---

#### **Note**

If you do not want to install a Proxy, you can proceed directly to Step 20.

---

#### **Note**

A Proxy is required when more than one level exists between a Data Collector and the Connector Service.

---

9. On the server where the Proxy will be installed, import the Connector Service self-signed certificate that was previously exported. See [Install 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>:<PortNumber>/ConnectorService` in your web browser.  
Where `https://<ConnectorServiceMachineName>:<PortNumber>/ConnectorService` is the computer name where the Connector Service is installed followed by the port number if it is different from the default port 443. 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 displays 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 appears, 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**

---

#### **Note**

If you do not want to install a Proxy and connect to another Proxy, you can proceed directly to Step 20.

---

14. On the server where the new Proxy will be installed, import the Proxy self-signed certificate that was previously exported. See [Install 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.

Where `https://<ExistingProxyMachineName>:<PortNumber>/Proxy` is the computer name where the Proxy is installed followed by the port number if it is different from the default port 443.

If the connection is secure, the Proxy UI appears – proceed to the next step. If the connection is not secure, a warning displays 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 appears, indicating the Proxy is running.
18. Export the Proxy self-signed certificate bound to port 443 (configurable default) in IIS. See [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. See [Install 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.  
Where `https://<ConnectorServiceMachineName>:<PortNumber>/ConnectorService` is the computer name where the Connector Service is installed followed by the port number if it is different from the default port 443.  
If the connection is secure, Connector Service displays in the top left corner of the web page – proceed to the next step. If the connection is not secure, a warning displays 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. See [Install 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 appears – proceed to the next step. If the connection is not secure, a warning displays 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.

## 2.4 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 System Manager application under the **Licenses** tab.

### Procedure

1. Register and install all licensed ASIs. See [Installing ASIs](#) to quickly get started.
2. Install the **CMMS Interface** on the CMMS Server. Refer to Knowledge Base Article NK-2000-0252 for more information.
3. **⚠ CAUTION**

As much as possible, you should configure the OPC UA Server and OPC Client *after* configuring the Plantweb Optics application and its Data Sources. Data or parameters updates are pushed and displayed in Plantweb Optics.

Install the **Plantweb Optics OPC UA Server**. Refer to Knowledge Base Article NK-2000-0246 for more information.

## 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 OpenID Connect (OIDC) settings. See [Configure Plantweb Optics OIDC settings](#).
  - c) Configure the AMS Device Manager ASI. See [Opt-In to Device Parameters](#).
2. Install Plantweb Optics certificates.

SSL certificates are imported after all web services (such as Plantweb Optics Web Service, Connector Service, Proxies, Data Collectors, and services) have been installed on the system. See [Certificate installations](#).

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



## 3 Planning your system

Plantweb Optics is comprised of different components, and 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.

### 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).
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 [Component and system compatibility](#).
  - b) Check the system requirements, system capacity, and system scalability recommendations to assist in determining the number of assets, databases, and parameters in the system. See [System requirements](#) and [System scalability](#).
3. Determine your network setup and architecture restrictions.  
Your network setup affects the deployment of the Plantweb Optics components. And your network architecture affects whether you can receive messages outside of your plant's network or not. For more information about deployment scenarios, see [Deployment scenarios](#).
4. 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 [Database deployment](#).
5. Check IIS requirements. See [Internet Information Services \(IIS\)](#).
6. Plan to integrate security certificate installation with software installation. See [Plantweb Optics security](#).
7. Ensure any systems you plan to interface with Plantweb Optics are ready. See [ASI and AR installation procedures](#).

### 3.2 System components

You must install the Plantweb Optics platform on a computer with a server-class operating system.

Client stations access Plantweb Optics applications from a web browser.

On a mobile device, you can install the Plantweb Optics mobile app. This app enables you to send and receive alerts from a mobile device.

See [Deployment scenarios](#) for example deployment scenarios and how the system components are configured.

**Table 3-1: System components**

Component	Description
Plantweb Optics	<p>The main software application. Plantweb Optics is always installed on the Plantweb Optics server.</p> <hr/> <p><b>Note</b> Install Plantweb Optics Historian and then Plantweb Optics before you install and integrate all other system components. This is a prerequisite to all other component installations.</p>
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 Source System	A Data Source System represents a Data Source, Data Collector, and supporting assets or devices.
Data Collector	Gathers data, such as parameter values, asset health, and events, from a configured Data Source to provide to Plantweb Optics through a Connector Service or proxy, depending on the configuration of the deployment scenario.
Data Source	<p>You can install Data Sources at different levels. Which level a Data Source is installed depends on the customer configuration and the type of Data Source. The Data Sources are the following ASIs:</p> <ul style="list-style-type: none"> <li>• AMS Asset Monitor</li> <li>• AMS Device Manager</li> <li>• AMS Machine Works</li> <li>• AMS Machinery Manager</li> <li>• DeltaV Control Loop</li> <li>• Optics Analytics (KNet)</li> <li>• Plantweb Insight</li> </ul>
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 historical parameter data so that you can analyze trends in the data.



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

Component	Description
Plantweb Optics OPC UA server	<p>Allows you to read Plantweb Optics data from an OPC UA client.</p> <hr/> <p><b>Note</b> The OPC UA server refreshes its hierarchy every 24 hours. Any changes made to an asset's properties in Plantweb Optics are displayed in the OPC UA client every 24 hours.</p>
Plantweb Optics Augmented Reality	<p>The Plantweb Optics Augmented Reality (AR) web portal works with the Augmented Reality (AR) mobile app and the Plantweb Optics platform to create, share, and use common information about plants, landmarks, AR nodes, and assets.</p>
Plantweb Optics mobile app	<p>Allows you to display, send, and receive Plantweb Optics messages and notifications from your mobile device. Install this on your iOS or Android mobile device.</p> <hr/> <p><b>Note</b> Only one Asset View mobile deployment is allowed, either On-Premise or Off-Premise.</p>

**Note**

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

Plantweb Optics utilizes a push model architecture where data flows from data sources, such as ASIs, through a data collector and/or proxy, through a connector service, and into Plantweb Optics. When determining the type of deployment, equipment, and components for your system, Emerson recommends these guidelines for performance and scalability:

- Understand the estimated total system load. The total system load is the number of assets connected to Plantweb Optics. The total system load helps you determine if you should implement a Single-server or Distributed deployment.
- Use the total system load to determine if a separate server for Connector Service server is configured or if it can be co-deployed with the Plantweb Optics server.
- Consider deploying the Connector Service on a different server other than the Plantweb Optics server for larger systems. If you connect too many components to the Connector Service, it may impact the server performance causing the system to slow down.
- You can install any Data Collector on the Connector Service server if the Data Collector has access to the data source.
- Understand the level of customer security in relation to the number of network layers between the data source and the Plantweb Optics platform to determine if you require a proxy server to communicate to the Connector Service.

- Use recommended hardware and operating systems.
- Install only the components you need.

The following sections provide examples of single-server or distributed deployment scenarios. These deployment scenario examples show the flexibility of the Plantweb Optics push model architecture and how easily it can be configured to meet customer requirements.

### 3.3.1 Tier 1 - single-server deployment scenarios

With Tier 1, single-server deployment scenarios the Plantweb Optics server is co-deployed with components like SQL Server 2019 Express, OPC UA Server, CMMS interface, and Plantweb Optics Historian. Each of these deployment scenarios highlight how you can configure Data Sources within the push model architecture. They also show how Secure Sockets Layer (SSL)/Transport Layer Security (TLS) is used to establish secure communication between system components. Refer to [Plantweb Optics security](#) for more information about system components with certificates, a list of security certificates, and where you must install the certificates.

The following list identifies supported Data Sources:

- AMS Asset Monitor
- AMS Device Manager
- AMS Machine Works
- AMS Machinery Manager
- DeltaV Control Loop
- Optics Analytics (KNet)
- Plantweb Insight

#### Tier 1 - Level 4, single-server deployment

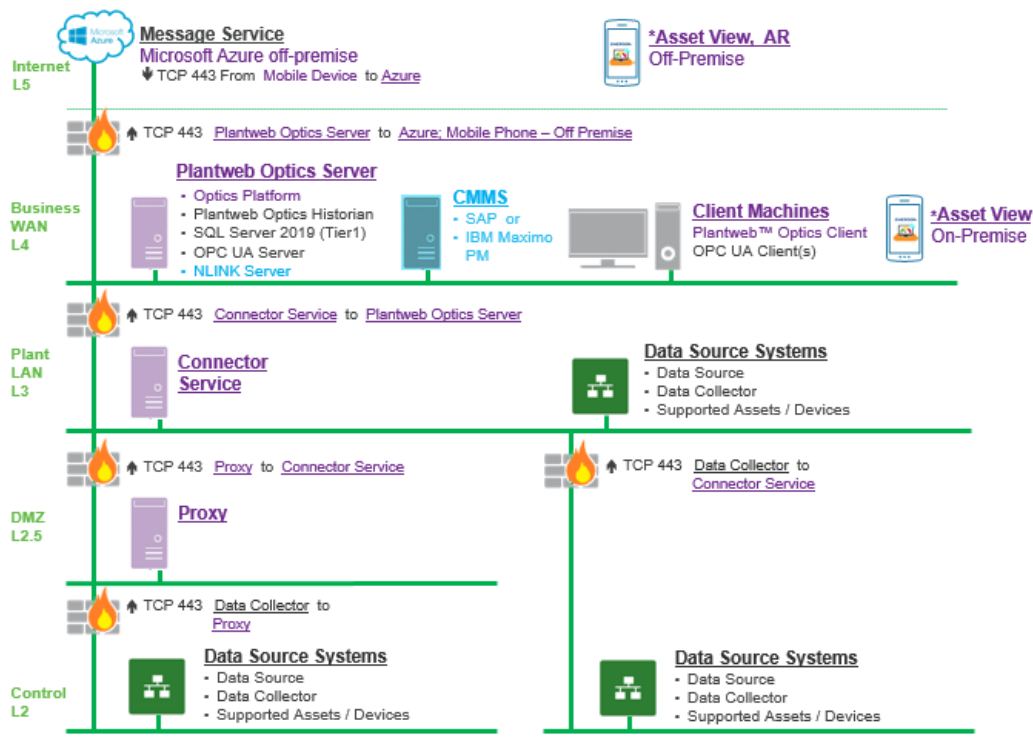
This deployment scenario shows the Plantweb Optics Server installed on Level 4. Components such as the SQL Server 2019 Express, the OPC UA Server, the CMMS interface, and the Plantweb Optics Historian are co-deployed with the Plantweb Optics Server. However, these components can be deployed in a separate server if the overall system asset count or load is high and impacting performance.

The following figure shows a standard, Tier 1, Single-server deployment with the Plantweb Optics server configured at level 4 and has the following data flow considerations when configuring your environment.

- Refer to [System components with certificates](#) for more information about system component certificates and which must be installed when deploying Plantweb Optics.
- You can install Data Source Systems at different levels. Which level you can install a Data Source depends on the Data Source type. You can install Data Source Systems at Level 2 or 3.
- Data flows from a Data Source/Data Collector to a Connector Service. You can configure data to flow from a Data Collector directly to a Connector Service, or from a Data Collector, through a proxy, and then to a Connector Service.

- Data flows from the Connector Service server to the Plantweb Optics server and then to the client machines and CMMS.

**Figure 3-1: Tier 1 - Level 4, single-server deployment**



\* Only one Asset View mobile deployment is allowed, either On-Prem or Off-Premise.

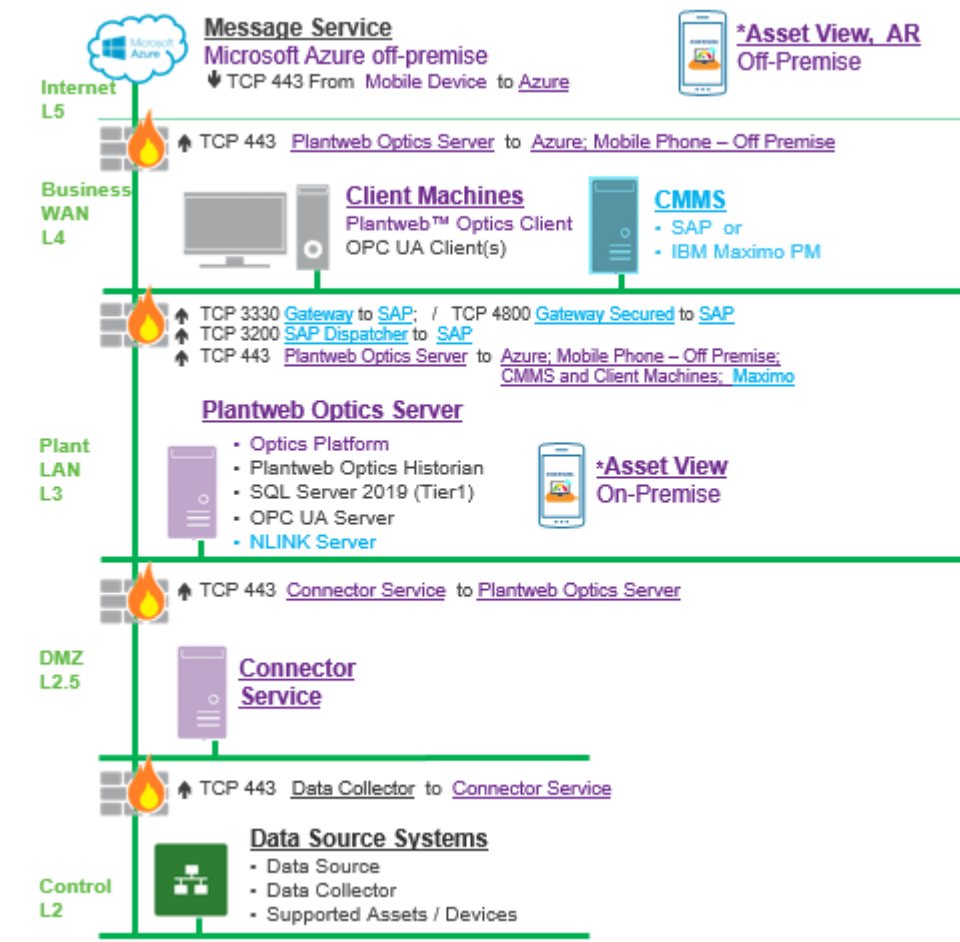
### Tier 1 - Level 3, single-server deployment

This deployment scenario shows the Plantweb Optics Server installed on Level 3 with the Connector Service server configured on Level 2.5. Components included on the Plantweb Optics server include the SQL Server 2019 Express, the OPC UA Server, the CMMS interface, and the Plantweb Optics Historian.

The following figure shows a basic, Tier 1, Single-server deployment with the Plantweb Optics server configured at level 3 and has the following data flow considerations when configuring your environment.

- Refer to [System components with certificates](#) for more information about system component certificates and which must be installed when deploying Plantweb Optics.
- The Data Source Systems are installed at Level 2, a level that offers the most security.
- Data flows from a Data Source/Data Collector to a Connector Service on Level 2.5.
- Data flows from the Connector Service server to the Plantweb Optics server and then to the client machines and CMMS.

Figure 3-2: Tier 1 - Level 3, single-server deployment



\* Only one Asset View mobile deployment is allowed, either On-Prem or Off-Premise.

### Tier 1 - Level 3, single server with separate Connector Service server

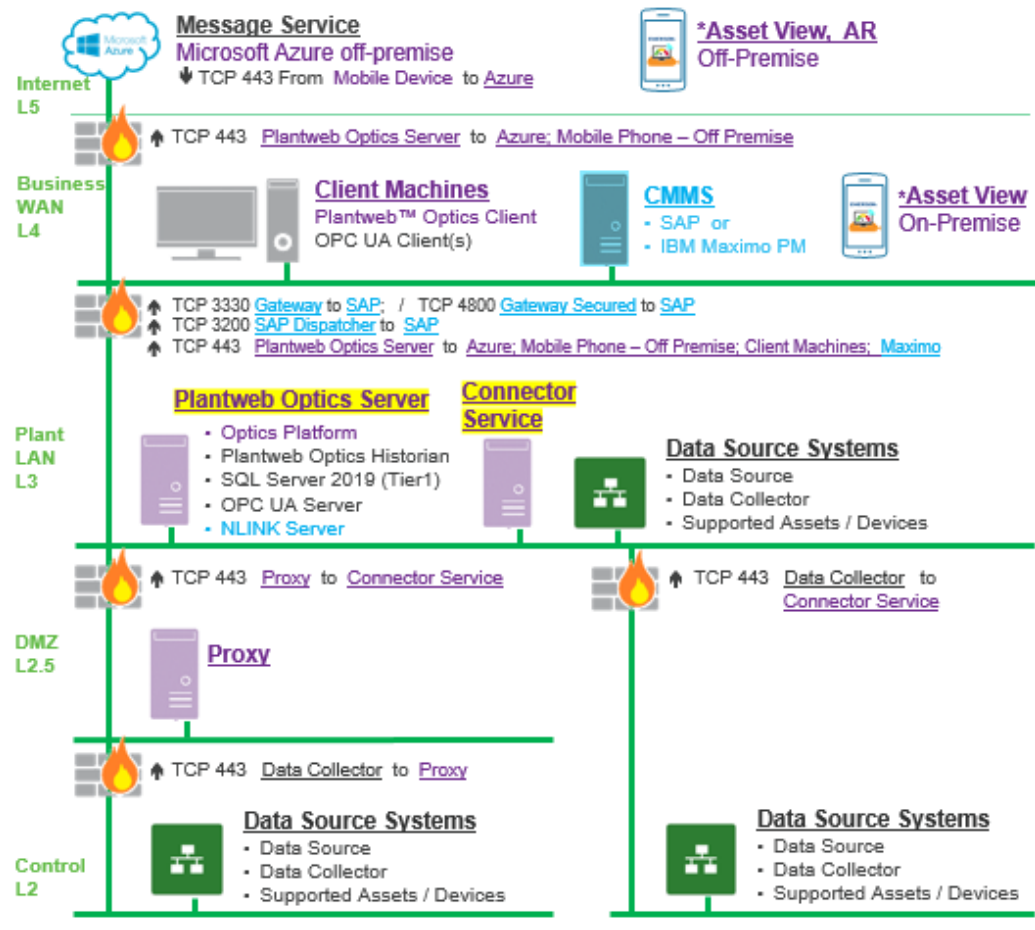
This deployment scenario shows the Plantweb Optics Server installed on Level 3 with the Connector Service server configured and installed on the same level in a separate server. Components included on the Plantweb Optics server include the SQL Server 2019 Express, the OPC UA Server, the CMMS interface, and the Plantweb Optics Historian.

The following figure shows a standard, Tier 1, single-server deployment scenario with the Plantweb Optics server configured at level 3 and has the following data flow considerations when configuring your environment.

- Refer to [System components with certificates](#) for more information about system component certificates and which must be installed when deploying Plantweb Optics.
- You can install Data Source Systems at different levels. Which level you can install a Data Source depends on the Data Source type. You can install Data Source Systems at Level 2 or 3.

- Data can flow from a Data Source/Data Collector on Level 2 or Level 3 to a Connector Service at the same level and then be passed on to the Plantweb Optics server. Or you can configure the system components to pass data from a Data Collector at Level 2, through a proxy server at Level 2.5 to the Connector Service on Level 3, and then to the Plantweb Optics server. Data then flows from the Plantweb Optics server to the client machines and CMMS.

**Figure 3-3: Tier 1 - Level 3, single-server with a separate Connector Service server deployment**



\* Only one Asset View mobile deployment is allowed, either On-Prem or Off-Premise.

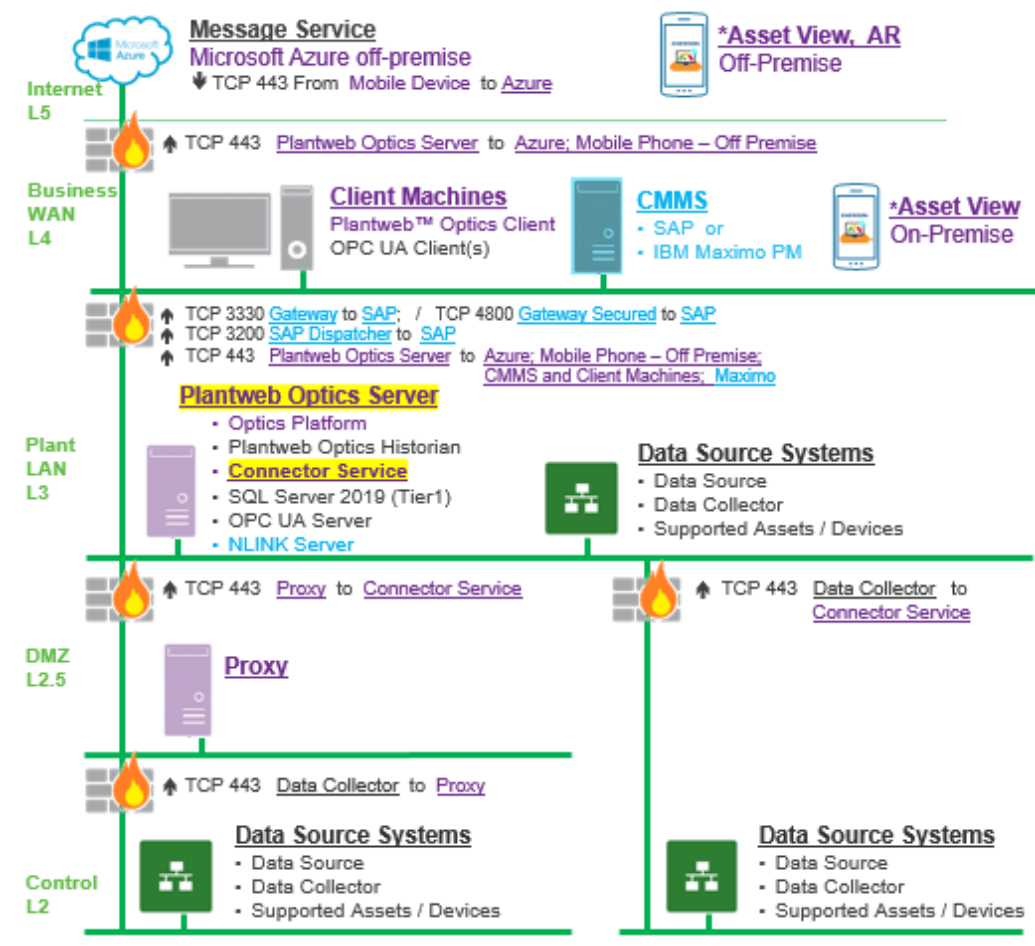
### Tier 1 - Level 3, single server with co-deployed Connector Service

This deployment scenario shows the Plantweb Optics platform and the Connector Service installed on the same server on Level 3. This scenario can work well in environments that have small asset loads. Large asset loads could impact performance in this type of deployment configuration. Other additional components included on the Plantweb Optics server include the SQL Server 2019 Express, the OPC UA Server, the CMMS interface, and the Plantweb Optics Historian.

The following figure shows a Tier 1, single-server, co-deployment of the Plantweb Optics and Connector Service on the same server. This type of configuration has the following data flow considerations.

- Refer to [System components with certificates](#) for more information about system component certificates and which must be installed when deploying Plantweb Optics.
- The Data Source Systems are installed at Level 2, a level that offers the most security.
- You can install Data Source Systems at different levels. Which level you can install a Data Source depends on the Data Source type. You can install Data Source Systems at Level 2 or 3.
- Data can flow from a Data Source/Data Collector on Level 2 or Level 3 to the Plantweb Optics server. Or you can configure Data Source Systems to pass data from a Data Collector at Level 2, through a proxy server at Level 2.5, to the Plantweb Optics server. Data then flows from the Plantweb Optics server to the client machines and CMMS.

**Figure 3-4: Tier 1 - Level 3, single-server with a co-deployed Connector Service server deployment**



\* Only one Asset View mobile deployment is allowed, either On-Prem or Off-Premise.

### 3.3.2 Tier 2 - Distributed deployment scenario

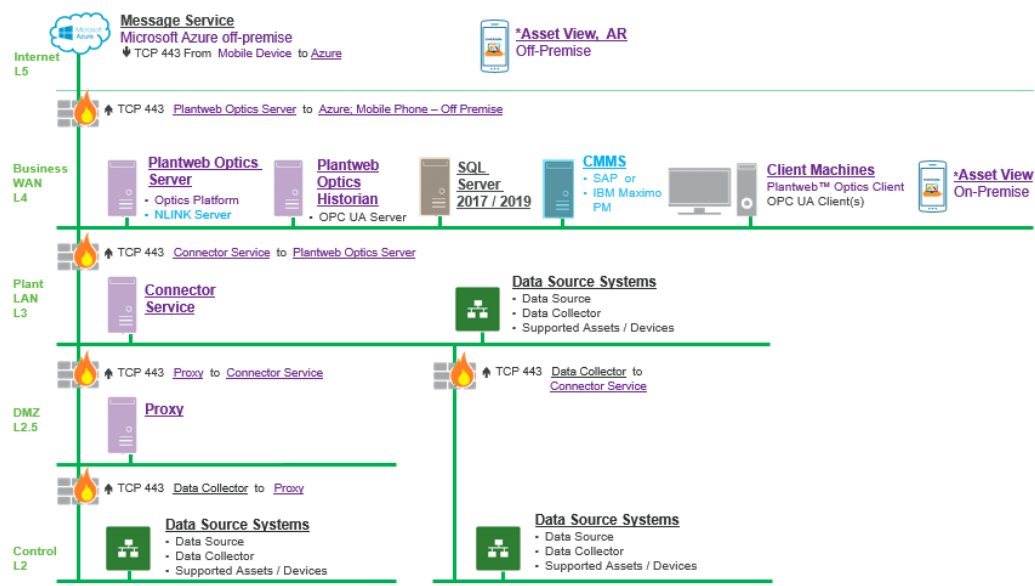
This deployment scenario is a Tier 2, distributed deployment that shows the Plantweb Optics Server installed on Level 4. In this deployment scenario the NLINK Server is co-deployed on the Plantweb Optics server. With many of the system components installed on separate servers, this deployment can support large asset loads and maintain high performance. The other additional system components are installed on standalone servers.

- SQL Server 2017/2019
- OPC UA Server and the Plantweb Optics Historian are co-deployed on a server

The following figure shows a Tier 2, distributed deployment scenario with the Plantweb Optics server configured at level 4, the Connector Service server on Level 3.

- Refer to [System components with certificates](#) for more information about system component certificates and which must be installed when deploying Plantweb Optics.
- You can install Data Source Systems at different levels. Which level you can install a Data Source depends on the Data Source type. You can install Data Source Systems at Level 2 or 3.
- Data flows from a Data Source/Data Collector to a Connector Service. You can configure data to flow from a Data Collector directly to a Connector Service, or from a Data Collector, through a proxy server, and then to a Connector Service. Data then flows to a system component or the Plantweb Optics server on Level 4.

**Figure 3-5: Tier 2 - distributed deployment on Level 4**



\* Only one Asset View mobile deployment is allowed, either On-Prem or Off-Premise.

## 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 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

During a Tier 1 installation, the databases are deployed on the same server as the software and Microsoft SQL Server 2019 Express is automatically installed. Tier-1 is the default configuration and represents the typical network server system. Automatic backup processing is available for this installation. See [Automatic backup for Tier-1 installations](#)

---

#### Note

Emerson does not support the installation of SQL Server 2017 express in a Tier1 installation.

---

- Check Windows Programs and Features to verify that Microsoft SQL Server is not currently installed. During default installation, Microsoft SQL Server 2019 Express is automatically installed and configured for Plantweb Optics.

---

#### Note

There is a 10 GB database limit on Microsoft SQL Server 2019 Express.

---

- 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 2019 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 or Microsoft SQL Server 2019 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 [Set up a separate SQL server for a Tier-2, distributed deployment installation](#).

- The database must be Microsoft SQL Server 2017 or 2019.
- 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 443).
- If port 443 is already in use by a previous installation of IIS, you can delete the Default Site (if unused) or configure it to use other ports. When other IIS applications are running use caution when specifying different ports. Refer to the **Installation** table in the [Troubleshooting](#) section 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.

## 3.6 System requirements

This chapter contains the system requirements for Plantweb Optics, Plantweb Optics Historian, the Connector Service, the Proxy, and other specifications that include browser support.

### Note

Plantweb Optics no longer supports the Internet Explorer browser. Plantweb Optics supports the current versions of Chrome and Microsoft Edge Chromium.

### Plantweb Optics server requirements

<b>Operating system</b>	Windows Server 2019 Datacenter Windows Server 2019 Standard Windows Server 2016 Datacenter Windows Server 2016 Standard
<b>CPU architecture</b>	64-bit
<b>Microsoft SQL Server</b>	MS SQL Server 2019 (recommended) MS SQL Server 2019 Express Edition (supported) MS SQL Server 2017 (supported for Tier 2 deployment) MS SQL Server 2017 Express Edition (supported for Tier 2 deployment)
<b>Processor</b>	3.2 GHz, 8-core processor, Intel Xeon-scalable or faster (recommended) 2.4 GHz, 4-core processor, Intel Xeon-scalable or faster (minimum)
<b>Memory (RAM)</b>	32 GB (recommended) 16 GB (minimum)

<b>Hard drive</b>	SSD hard drive (recommended) SAS hard drive (10K RPM) (minimum)
<b>Available disk space</b>	100 GB (minimum)

### Plantweb Optics Historian/Plantweb Optics OPC UA Server

<b>Operating system</b>	Windows Server 2019 Datacenter Windows Server 2019 Standard Windows Server 2016 Datacenter Windows Server 2016 Standard Windows Server 2012 R2 Datacenter Windows Server 2012 R2 Standard
<b>CPU architecture</b>	64-bit
<b>Processor</b>	2.4 GHz, 4-core processor, Intel Xeon-scalable or faster
<b>Memory</b>	32 GB
<b>Hard drive</b>	SAS hard drive (10K RPM)
<b>Available disk space</b>	100 GB (minimum)

### Plantweb Optics Client Station

Plantweb Optics clients can run on any computer system when it has the supported internet browsers installed and the network is connected to the Plantweb Optics server.

### Connector Service Requirements

<b>Operating system</b>	Windows 10 Pro Windows 10 Enterprise Windows 10 IoT Enterprise 2016 LTSB (64-bit) Windows Server 2019 Datacenter Windows Server 2019 Standard Windows Server 2016 Datacenter Windows Server 2016 Standard
<b>CPU architecture</b>	64-bit
<b>Processor</b>	2.4 GHz, 4-core processor, Intel Core i5, or better
<b>Memory</b>	4 GB (supported) 8 GB (recommended)
<b>Hard Drive</b>	SATA (Supported) SATA or better (Recommended)
<b>Available disk space</b>	20 GB (supported) 100 GB (recommended)
<b>Internet Information Services (IIS)</b>	v8.5, v10 (supplied with OS)
<b>Network</b>	1 x 1GB NIC

### Proxy Requirements

<b>Operating system</b>	Windows 10 Pro Windows 10 Enterprise Windows 10 IoT Enterprise 2016 LTSC (64-bit) Windows Server 2019 Datacenter Windows Server 2019 Standard Windows Server 2016 Datacenter Windows Server 2016 Standard
<b>CPU architecture</b>	64-bit
<b>Processor</b>	2.4 GHz, 2-Core processor, Intel Core i3, or better
<b>Memory</b>	2 GB RAM
<b>Hard Drive</b>	SATA (supported) SATA or better (recommended)
<b>Available disk space</b>	20 GB
<b>Internet Information Services (IIS)</b>	v8.5, v10 (supplied with OS)
<b>Network</b>	1 x 1GB NIC

### Additional specifications

<b>Browser</b>	Google Chrome v65 or later (recommended) Microsoft Edge Chromium
<b>Ethernet</b>	One or more Ethernet ports (1GB NIC)
<b>Internet connectivity</b>	A high-speed internet connection is recommended to download installations and patches, register software, and receive alerts and messages on the mobile application.
<b>Screen Resolution</b>	Minimum: SXGA (1280 x 1024 pixels)
<b>Supported antivirus software</b>	Symantec™ Endpoint Protection McAfee™ Endpoint Norton™ Security with Backup
<b>Supported virtualization</b>	VMware 6 up to 6.7 Hyper-V 2012, 2016

### 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.

**Table 3-2: Anti-virus Exclusion List**

Component	Item	Path
AMS Asset Monitor Data Collector	Data Collector executable file location	<installed drive>\PlantwebOptics\site\AMSAssetMonitorDataCollector\AMSAssetMonitorDataCollector.exe
	Data Collector Install Files	<installed drive>\PlantwebOptics\site\AMSAssetMonitorDataCollector
	Log Files	<installed drive>\PlantwebOptics\site\Logs
AMS Device Manager Data Collector	Data Collector executable file location	<installed drive>\PlantwebOptics\site\AMSDeviceManagerDataCollector\AMSDeviceManagerDataCollector.exe
	Data Collector Install Files	<installed drive>\PlantwebOptics\site\AMSDeviceManagerDataCollector
	Log Files	<installed drive>:\PlantwebOptics\site\Logs
AMS Machine Works Data Collector	Data Collector executable file location	<installed drive>\PlantwebOptics\site\AMSMachineWorksDataCollector\AMSMachineWorksDataCollector.exe
	Data Collector Install Files	<installed drive>\PlantwebOptics\site\AMSMachineWorksDataCollector
	Log Files	<installed drive>\PlantwebOptics\site\Logs
AMS Machinery Manager Data Collector	Data Collector executable file location	<installed drive>\RBMsuite\sys\DataCollector\AMSMachineryManagerDataCollector.exe
	Data Collector Install Files	<installed drive>\RBMsuite\sys\DataCollector\AMSMachineryManagerDataCollector
	Log Files	<installed drive>\RBMsuite\sys\DataCollector\AMSMachineryManagerDataCollector\Logs
DeltaV Control Loop Data Collector	Data Collector executable file location	<installed drive>\PlantwebOptics\site\DeltaVControlLoopDataCollector\DeltaVControlLoopDataCollector.exe
	Data Collector Install Files	<installed drive>\PlantwebOptics\site\DeltaVControlLoopDataCollector
	Log Files	<installed drive>\PlantwebOptics\site\Logs
	Data Producer	<installed drive>\DeltaVControlLoopDataProducer\DeltaVControlLoopDataProducer.exe
KNet Data Collector (5.2)	Data Collector executable file location	<installed drive>\PlantwebOptics\site\KNetDataCollector\KNetDataCollector.exe
	Data Collector Install Files	<installed drive>\PlantwebOptics\site\KNetDataCollector

**Table 3-2: Anti-virus Exclusion List (continued)**

Component	Item	Path
	Log Files	<installed drive>\PlantwebOptics\site\Logs
Optics Analytics Data Collector (5.3)	Data Collector executable file location	<installed drive>\PlantwebOptics\site\OpticsAnalyticsDataCollector\OpticsAnalyticsDataCollector.exe
	Data Collector Install Files	<installed drive>\PlantwebOptics\site\OpticsAnalyticsDataCollector
	Log Files	<installed drive>\PlantwebOptics\site\Logs
Plantweb Insight Data Collector	Data Collector executable file location	<installed drive>\PlantwebOptics\site\PlantwebInsightDataCollector\PlantwebInsightDataCollector.exe
	Data Collector Install Files	<installed drive>\PlantwebOptics\site\PlantwebInsightDataCollector
	Log Files	<installed drive>\PlantwebOptics\site\Logs

**Plantweb Optics Mobile and Augmented Reality (AR) requirements**

Item	Plantweb Optics Mobile	Plantweb Optics AR Mobile
Common Phone and Tablet models	iPhone 6s or later iPad Mini 4 (2015) or later	iPhone 8 or later iPad Mini (2019) or later
	Multiple Android mobile devices and tablets can support the Plantweb Optics and the Plantweb Optics AR mobile apps. For a list of the Android devices that may support both Plantweb Optics apps, go here: <a href="https://web.plantwebopticsar.com/support/android">https://web.plantwebopticsar.com/support/android</a>	
Memory (RAM)	2 GB RAM or higher	3GB or higher
Processor	Dual-core 1.84 GHz or higher	Quad-core 2.34 GHz or higher
Operating System	iOS 11.3 or later Android 9.0 or later	

**Note**

- Other mobile phone models may work if the memory, processor, and operating system requirements meet the required minimum specifications.
- Customers using both, the Plantweb Optics Mobile and the Plantweb Optics AR Mobile should use the Plantweb Optics AR Mobile specifications.

## 3.7 System scalability

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

**Table 3-3: Plantweb Optics scalability**

Components	Setup 1: Distributed deployment	Setup 2: Single-server deployment
<b>Server specifications</b>	Plantweb Optics server Plantweb Optics Historian, OPC UA Server Connector Service server	Plantweb Optics server Connector Service (separate server or co-deployed with the Plantweb Optics server)
<b>Plantweb Optics</b>		
<b>Assets</b>	30,000	10,000
<b>Total Assets</b>	Total asset count is limited by Plantweb Optics. Plantweb Optics v1.6 has a limit of 30,000 assets, which can be distributed in any way across multiple Data Collectors.	
<b>Historized assets</b>	30,000	10,000
<b>Parameters</b>	1,500,000	500,000
<b>Configured users</b>	25 total users	25 total users
<b>Concurrent users</b>	25 total users	25 total users
<b>AMS Asset Monitor Data Collector</b>		
<b>CHARMs</b>	3000	up to 3000
<b>AMS Device Manager Data Collector</b>		
<b>Devices</b>	15,000	up to 10,000
<b>AMS Machine Works Data Collector</b>		
<b>Devices</b>	4,000	4,000
<b>AMS Machinery Manager Data Collector</b>		
<b>Machine Trains</b>	10,000	10,000
<b>DeltaV Control Loop Data Collector</b>		
<b>Control Loops</b>	5,000	up to 5,000
<b>Optics Analytics (KNet) Data Collector</b>		
<b>Tags</b>	1,000	1,000
<b>Plantweb Insight Data Collector</b>		
<b>Devices</b>	1,000	1,000
<b>OPC UA</b>		
<b>OPC UA Deployment</b>	UA Server and Plantweb Optics server deployed separately	OPC UA Server and Plantweb Optics server on same machine
<b>Number of Assets</b>	2,000 assets	1,000 Assets

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

Components	Setup 1: Distributed deployment	Setup 2: Single-server deployment
<b>Number of Total Monitored Tags</b>	20,000 Monitored Tags	4,000 Monitored Tags
<b>Number of Clients</b>	5 Clients	2 Clients

**Maximum concurrent users**

<b>Configured users</b>	Users configured in the System Manager application.
<b>Mobile device users</b>	Users issued mobile join keys.
<b>Plantweb Optics concurrent users</b>	Configured 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 the security and communication requirements below are met, you are ready to begin your installation.

---

### Note

Check with your Emerson Impact Partner for the latest security information.

---

### 4.1 Firewall considerations

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

Before you install the Plantweb Optics components, ensure you have the firewall exceptions set in place for each computer with Data Collectors, Proxies, or a Connector Service. See [Deployment scenarios](#) to determine which servers need firewall exceptions. Identify 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 [Ports for a host-based firewall](#). Consult with your IT department to determine if any intermediary firewall needs exceptions set.

---

### 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 a host-based firewall](#) 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.

#### 4.1.1 Ports for a host-based firewall

A host-based firewall is installed on each individual server that controls incoming and outgoing network traffic. This firewall also determines whether to allow data to a particular device (for example, the Microsoft firewall that comes with a Windows-based computer).

The Plantweb Optics installer configures Microsoft Windows firewall during installation to allow Plantweb Optics components to communicate.

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

The following tables show the default ports that Plantweb Optics and its components use.

---

### Note

Ports tagged with asterisks (\*) need to be configured manually by your IT department.

---

**Table 4-1: Ports used by Plantweb Optics**

Port	Direction	Notes
TCP 443 (default, configurable)	Inbound	Exposed by Plantweb Optics to allow communication with the Plantweb Optics applications and Plantweb Optics web services.
TCP 15672		A local port restricted to localhost.

**Table 4-2: Ports used by Plantweb Optics OPC UA**

Port	Direction	Notes
TCP 4840	Bidirectional	Exposed by Plantweb Optics OPC UA Server to allow an OPC UA client connection.

**Table 4-3: Ports used by Plantweb Optics Client**

Port	Direction	Notes
* TCP 443	Outbound	Used by the web browser to communicate with Plantweb Optics applications.

**Table 4-4: Ports used by OPC UA Client**

Port	Direction	Notes
* TCP 4840	Bidirectional	Used by the OPC UA client to communicate with the Plantweb Optics OPC UA Server.

**Table 4-5: Ports used by Connector Service**

Port	Direction	Notes
TCP 443 (default, configurable)	Inbound	Exposed by the Connector Service to allow communication to the Connector web services.

**Table 4-6: Ports used by Proxy**

Port	Direction	Notes
TCP 443 (default, configurable)	Inbound	

**Table 4-7: Ports used by Data Collectors**

Port	Direction	Notes
TCP 443 (default, configurable)	Outbound	Used by the Data Collector to communicate with the Connector Service. Exposed by the Proxy to allow communication to the Proxy web services. If the Data Collector is unable to communicate directly to the Connector Service because of the number of arbitrary networks between them, then this becomes an outbound direction to Proxy Ports used by Data Collectors and Data Sources: <ul style="list-style-type: none"> <li>• AMS Asset Monitor</li> <li>• AMS Device Manager</li> <li>• AMS Machinery Manager</li> <li>• DeltaV Control Loop</li> <li>• Optics Analytics (KNet)</li> </ul>
Data Collector specific ports		There are additional ports needed depending on the product you want to integrate with Plantweb Optics.

**Table 4-8: Ports used by Plantweb Optics Historian**

Port	Direction	Notes
TCP 27017	Bidirectional	MongoDB (default)
TCP 6512	Bidirectional	Core Service
TCP 8002 (default, configurable)	Bidirectional	Web Service

**Table 4-9: Ports used by Plantweb Optics CMMS Integration**

Port	Direction	Notes
TCP 448 (configurable)	Bidirectional	Used for communication by Plantweb Optics and CMMS Integration (Sap or Maximo).
CMMS Server TCP port (configurable)	Outbound	This could be an SAP or a Maximo server port.
TCP 3200 (3200–3299)	Outbound	Dispatcher, CMMS User Interface to CMMS (SAP PM)

**Table 4-9: Ports used by Plantweb Optics CMMS Integration (continued)**

Port	Direction	Notes
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 4-10: Ports used by Plantweb Optics Mobile App (via Azure)**

Port	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.
* TCP 25	Outbound	TCP 25 outbound to the smtp.sendgrid.net should be open to the Internet for the Plantweb Optics Mobile App to work.

**Table 4-11: Ports used by Plantweb Optics Augmented Reality Portal and Remote Expert**

Port	Direction	Notes
TCP 443	Outbound	

The following table shows additional ports used the SQL server on a Tier 2 distributed deployment.

**Table 4-12: Ports and firewall rules by SQL Server station**

Item	Direction	Firewall rule
Distributed Transaction Coordinator (RPC)	Inbound	This is a predefined firewall and needs to be configured if SQL Server is on Tier 2 deployment.
Distributed Transaction Coordinator (RPC-EPMAP)	Inbound	This is a predefined firewall and needs to be configured if SQL Server is on Tier 2 deployment.
Distributed Transaction Coordinator (TCP-In)	Inbound	This is a predefined firewall and needs to be configured if SQL Server is on Tier 2 deployment.
EMERSONCSI SQL instance TCP port	Bidirectional	Plantweb Optics uses this port to communicate with the SQL Server.

**Table 4-12: Ports and firewall rules by SQL Server station (continued)**

Item	Direction	Firewall rule
UDP Port 1434 (SQL Server Browser service)	Bidirectional	The SQL Server Browser service listens for incoming connections to a named instance and provides the TCP port number that corresponds to that named instance to the client. The SQL Server Browser service is started when named instances of the Database Engine are used. The SQL Server Browser service does not have to be started if the client is configured to connect to the specific port of the named instance.
TCP Port 139		SQL
TCP 445		SQL Server-file stream
TCP 135		RPC

Below are additional ports used by data collectors.

**Table 4-13: Additional Ports used by AMS Asset Monitor Data Collector**

Port	Direction	Notes
TCP 443	Outbound	To allow Data Collector to communicate with the AMS Asset Monitor Unit.

**Table 4-14: Additional Ports used by Optics Analytics (KNet) Data Collector**

Port	Direction	Notes
TCP 8000	Outbound	Connect to the log service
TCP 55700	Bidirectional	Connect to the license service
TCP 55777	Bidirectional	Connect to Optics Analytics Engine or the KNet Engine
TCP 44336	Inbound	Listen to configurator service

## 4.1.2 Ports for a network-based firewall

A network-based firewall controls traffic going in and out of a network. It does this by filtering traffic based on firewall rules and allows only authorized traffic to pass through it.

### Note

Your IT personnel should configure a network-based firewall when setting up Plantweb Optics to allow its components communicate to each other.

To configure your network-based firewall, use the [Ports for a host-based firewall](#) section as a guide to determine the direction or flow of communication.

The following tables provides an example of the ports that must be available and open through network firewalls for a Level 4 deployment.

**Table 4-15:**

Ports used by L4 to L5	Source	Destination
TCP 443	Plantweb Optics Server	*.azurewebsites.net
TCP 25	Plantweb Optics Server	smtp.sendgrid.net

**Table 4-16:**

Ports used by L3 to L4	Source	Destination
TCP 443	Connector Service	Plantweb Optics Server

**Table 4-17:**

Ports used by L2.5 to L3	Source	Destination
TCP 443	Proxy	Connector Service

**Table 4-18:**

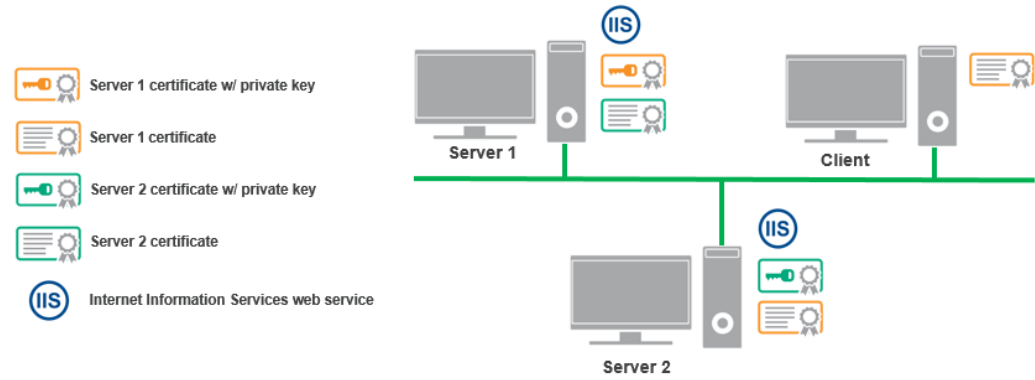
Ports used by L2 to L2.5	Source	Destination
TCP 443	All Data Collectors on level 2	Proxy

## 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 (default).

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 a Data Collector, Connector Service, or Proxy must exchange public key certificates. The table below shows which components of Plantweb Optics have certificates. See [Certificate installation checklist](#).

**Table 4-19: System Components with Certificates**

Component	Certificate
Plantweb Optics Server	PlantwebOptics.{Full Computer Name}
Connector Service	PlantwebOptics.{Full Computer Name}
Proxy	PlantwebOptics.{Full Computer Name}
AMS Asset Monitor Data Collector	PlantwebOptics.{Full Computer Name}
AMS Device Manager Data Collector	PlantwebOptics.{Full Computer Name}
AMS Machine Works Data Collector	PlantwebOptics.{Full Computer Name}
AMS Machinery Manager Data Collector	PlantwebOptics.{Full Computer Name}
DeltaV Control Loop Data Collector	PlantwebOptics.{Full Computer Name}
Optics Analytics Data Collector	PlantwebOptics.{Full Computer Name}
KNet Data Collector	PlantwebOptics.{Full Computer Name}
Plantweb Insight Data Collector	PlantwebOptics.{Full Computer Name}

The **Certificates Deployment** table lists each security certificate and the servers where the listed certificate must be installed. Only install the certificates that your Plantweb Optics system requires.

**Table 4-20: Certificates Deployment**

System	Installed Certificate
Plantweb Optics Server	None
Plantweb Optics OPC UA Server	Plantweb Optics Server certificate. This certificate allows communication to Plantweb Optics web sites. Manually install this certificate.
Plantweb Optics Clients	Plantweb Optics Server certificate. This certificate allows communication to Plantweb Optics web sites. Manually install this certificate.
Plantweb Optics OPC UA Clients	Plantweb Optics OPC UA Server certificate. This certificate allows communication to the OPC UA server. Manually install this certificate.
Connector Service	Plantweb Optics Server certificate. This certificate allows communication to Plantweb Optics web sites. Manually install this certificate.



**Table 4-20: Certificates Deployment (continued)**

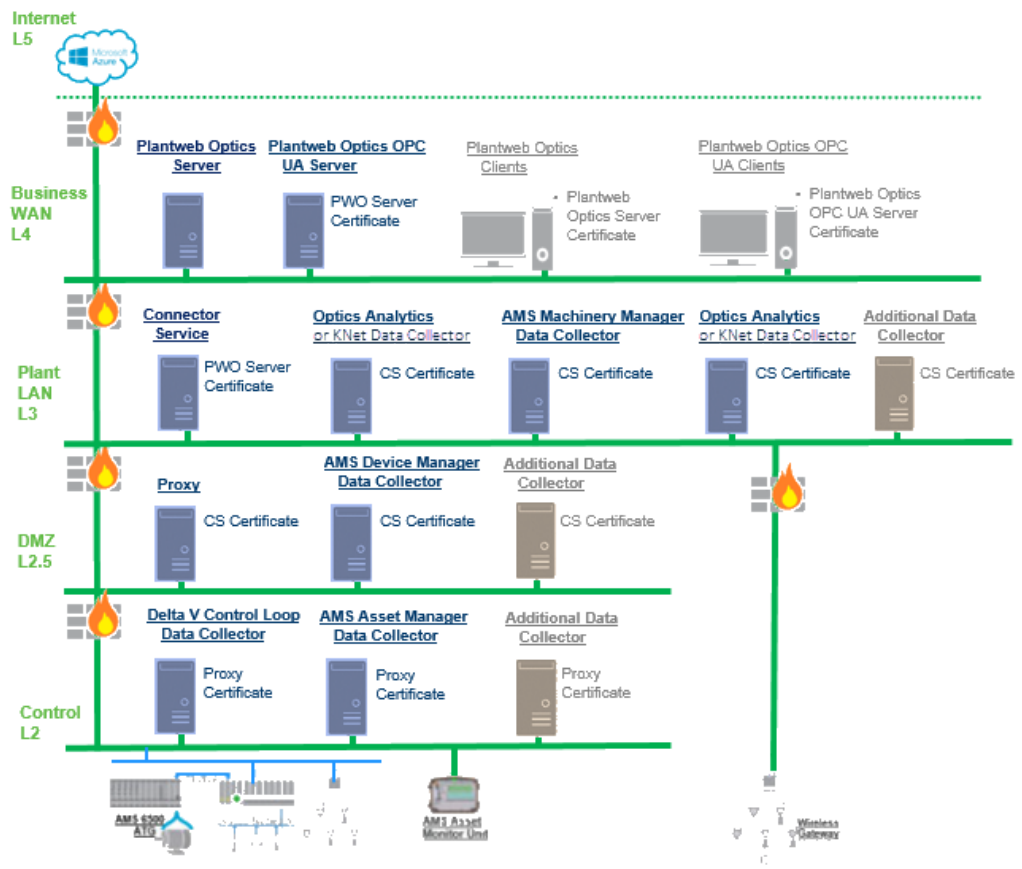
System	Installed Certificate
Proxy	<p>The Connector Service certificate. The Proxy requires the certificate of the component it directly sends data to. A Proxy requires either the Connector Service or Proxy certificate, depending on which component the Proxy communicates directly with. Manually install this certificate.</p> <p>If Proxy is unable to communicate directly to the Connector Service because of a number of arbitrary networks between them, then you should install the Proxy certificate above the Connector Service certificate.</p>
Data Collectors	<p>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. Manually install this certificate.</p> <p>The Proxy certificate is installed instead of Connector's Service certificate if direct communication to Connector Service is not possible because of an arbitrary number of networks between Data Collector and Connector Service.</p>

**Additional notes:**

ASI components including the Connector Service and Proxy must have certificates to communicate with each relevant part of the system. For example, a Connector Service computer requires the Plantweb Optics server certificate to send asset source data to Plantweb Optics. The Plantweb Optics server does not need the Data Collector certificate.

You should install the Connector Service on a separate computer other than the Data Collector. The figure below illustrates Plantweb Optics system certificate deployment. Below is an example network overview that shows how certificates are deployed.

Figure 4-2: Certificates Installed for each system component



## 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. See [Certificate installations](#) for certificate installation instructions.

### 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 the Plantweb Optics server certificate
2. On the Connector Service machine:
  - Install the Plantweb Optics server certificate

- Install the Connector Service
- Export the Connector Service certificate
- 3. On the Proxy machine (if used):
  - Install the upstream ASI component certificate (either Connector Service or Proxy)
  - Export the Proxy certificate (if another Proxy will communicate with this Proxy)
- 4. On the AMS Asset Monitor Server:
  - Install the AMS Asset Monitor Data Collector
  - Install the AMS Asset Monitor Hardware certificate
  - Install the upstream ASI component certificate (either Connector Service or Proxy)
- 5. On the AMS Device Manager Server:
  - Install the AMS Device Manager Data Collector
  - Install the upstream ASI component certificate (either Connector Service or Proxy)
- 6. On the AMS Machine Works Server:
  - a) Install the AMS Machine Works Data Collector
  - b) Install the upstream ASI component certificate (either Connector Service or Proxy)
- 7. On the AMS Machinery Manager Server:
  - Install the AMS Machinery Manager Data Collector
  - Install the upstream ASI component certificate (either Connector Service or Proxy)
- 8. On the DeltaV Server:
  - Install the DeltaV Control Loop Data Collector
  - Install the upstream ASI component certificate (either Connector Service or Proxy)
- 9. On the Optics Analytics (KNet) Data Collector:
  - Install the Optics Analytics (KNet) Data Collector
  - Install the upstream ASI component certificate (either Connector Service or Proxy)

10. On the Plantweb Insight Server.
  - a) Install the Plantweb Insight Data Collector.
  - b) Install the Plantweb Insight system certificate.
  - c) Install the upstream ASI component certificate (either Connector Service or Proxy).

## 4.3 Additional security considerations

### Permissions

Someone with administrator privileges can assign permissions according to a user's job functions. This strategy ensures that the appropriate people in the plant see relevant alarms and health changes. 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 System Manager application controls user account security. Consider setting account lockouts, password complexity requirements, and session length before adding users in Plantweb Optics.

---

### Note

Security information can be updated after a product is released. Check with your Emerson Impact Partner for the latest security information.

---

## 5 Plantweb Optics 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.

---

### Note

Follow the recommended installation and setup order defined in Chapter 2, [Quick start](#).

---

### 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.

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.

---

### 5.1 Acquire licenses

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

#### Prerequisites

- `A480PTICS-SYSTEM0.Plantweb_Optics.1.6.X.X.zip` file.

#### Procedure

1. Extract the `A480PTICS-SYSTEM0.Plantweb_Optics.1.6.X.X.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: `A480PTICS-SYSTEM0.Plantweb_Optics.1.6.X.X\Setup\_Support\_Gema1to`
4. Run `echoid.exe -d -p` from the command prompt window to generate your locking code:

```
Administrator: Command Prompt - echoid.exe -d -p
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\Plantweb_Optics.1.5.0.334\Support\Gemalto
C:\Plantweb_Optics.1.5.0.334\Support\Gemalto>echoid.exe -d -p

Sentinel RMS Development Kit 9.4.0.0023 Host Locking Code Information Utility
Copyright (c) 2018 SafeNet, Inc.

IP address           : 10.210.243.27
Disk ID              : 0x8220FDAC
Host name            : KNOCS03
Ethernet address[1]  : 00-50-56-93-FF-F5
Hard Disk Serial[1]  : 6000c29913f44a5f4ee757d83f6874d1
CPU Info String      : GenuineIntel Intel(R) Xeon(R) Gold 5120 CPU @ 2.20GHz 6 5 4
UUID                 : FC641342-3DC4-E45C-03D3-E2BAC5E90EBC

Locking Code 1 [1] : 14-*1ME 7XUQ 6R8K 9KE2

-----
Press Enter to continue . . .
```

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).

---

**Note**

License expiration starts when the license is issued. Emerson recommends you perform this step two to three days before you plan to install the product.

---

## 5.2 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 A480PTICS-SYSTEM0.Plantweb\_Optics.1.6.X.X.zip file.
- Turn off automatic Windows updates during installation or upgrade.
- You may need to change your server name before installing the software. Special characters (<>;: " \* + = \ | ? , \_ !), accented characters, and other multibyte characters in a server name can cause problems and interfere with a successful installation. A valid server name can have numbers 0-9, uppercase and lowercase letters A-Z, and the hyphen (-). Server names cannot have only numbers, nor can they contain spaces.

### Procedure

1. Extract the A480PTICS-SYSTEM0.Plantweb\_Optics.1.6.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 Software License Agreement and click **Next**.
5. Select **Install Now** to install with default options or **Customize** to change the default installation and data paths.
6. On the **Plantweb Optics Historian Database** screen, enter a password for the MongoDB database.  
  
The default user account name is **MongoUserAdmin**.  
  
This account and password are only used by Plantweb Optics Historian.
7. If you selected **Customize**, you can continue the installation with the default paths. Alternatively, you can modify the install and data paths by browsing to a new location. You can also type a new location in the **Install path** and **Data path** fields. Click **Next**.
8. On the **Installation is successful** screen, click **Done**.

## 5.3 Install Plantweb Optics Web Services

### Prerequisites

- You need the A480PTICS-SYSTEM0.Plantweb\_Optics.1.6.X.X.zip file.
- Turn off automatic Windows updates during installation or upgrade.
- You may need to change your server name before installing the software. Special characters (<>;: " \* + = \ | ? , \_ !), accented characters, and other multibyte characters in a server name can cause problems and interfere with a successful installation. A valid server name can have numbers 0-9, uppercase and lowercase letters A-Z, and the hyphen (-). Server 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 applications. Emerson recommends using the server name.
  - If you use an IP address, use a static address.
  - If you use the server name, ensure it is valid with no special, accented, or multibyte characters.
  - Only make changes to the IP address or server name before installing Plantweb Optics.

---

### Note

A server name change requires you to uninstall everything and then reinstall with the new server name.

---

### Procedure

1. Extract the A480PTICS-SYSTEM0.Plantweb\_Optics.1.6.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**.

Plantweb Optics runs a test to ensure your system is compliant with installation requirements. Unmet minimum system requirements could impact the overall system performance or halt the installation. If the installation detects unmet requirements, the **Product Setup Rules** screen appears and displays the warnings or failures. You can use the information on this screen to diagnose the issue and determine a corrective action. You can also run the checklist again or in the case of a warning, click **Next** and continue with the installation.

See [System requirements](#) for more information about minimum system requirements needed to install Plantweb Optics.

4. On the **Software License Terms** screen, read and accept the software license agreement and then click **Next**.

5. On the **Choose the installation you want** screen, click **Install Now** to install with default options or click **Customize** to change the database location and database user passwords.

- If you clicked **Install Now** skip to Step 12 for the component installation.
- If you clicked **Customize** proceed to Step 6 to set up the Plantweb Optics database.

6. On the **Plantweb Optics Database Setup** screen select one of the following database setups and then 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 [Automatic backup for Tier-1 installations](#) for more information.  
You can change the port value. The default port value is 1433.  
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 **Plantweb Optics and DB on the same server (Tier-1)**, skip to [Step 8](#).
- If you 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 [Tier-2 distributed deployment installation](#) for instructions.

---



<b>Server name</b>	The computer name of the database server.  <b>Note</b> 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.
<b>Port</b>	You can change the port value. The default port value is 1433.
<b>Authentication</b>	Choose <b>Windows Authentication</b> or <b>SQL Server Authentication</b> . Select <b>Windows Authentication</b> to use the current Windows logged in user account for database authentication. Select <b>SQL Server Authentication</b> 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 username and password when accessing the database server.
<b>Username</b>	The username used for database authentication.
<b>Password</b>	The password associated with the username used for authentication.

- From the **FWK\_Admin User Account Login** screen, you must provide a password to ensure the user account can connect to the database. Click **Next** to accept the default password or enter a new password and then click **Next**.

**⚠ CAUTION**

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

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

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

<b>Port</b>	<p>The port number when accessing Plantweb Optics. Plantweb Optics requires and uses port 80 and port 443. Port 443 is the default port.</p> <p>If a port is already in use, there is a red square around the port number. If ports 80 and 443 are not available or are being used by another application, open the ports by changing the port binding or redirecting the website using these ports.</p> <p>See <a href="#">Troubleshooting</a> to free up port 443 if it is being used by another application.</p>
-------------	---

9. On the **Plantweb Optics Historian Server Configuration** screen, enter the server name or IP address of the Plantweb Optics Historian server along with the port number, and then click **Next**.
10. On the **Plantweb Optics Mobile App Settings** screen, 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 mobile service that provides access to your plant network only. Click **Next** after you select 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 a Plantweb 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.
11. On the **Default Install Directory** screen, change the location where the product will be installed or select the default path provided. Click **Next** to start the component installation.
12. From the Plantweb Optics installation screen you can click the vertical **Components** link on the left side of the screen to view the progress of the components being installed. During the installation, the following components install automatically if they are not already installed. Each of the following components require a reboot for the installation process to continue.
  - Microsoft .NET Framework 4.8
  - Microsoft SQL Server 2019 Express (x64)
  - Microsoft SQL Server 2019 Cumulative Update

For each of the components that require you to restart the system, an **Installation is pending** screen displays.

- a) Click **Restart Now** to restart the system.
- b) After the system restarts, log in with the same user credentials that you used before. The system installation continues automatically.

13. After all components have successfully installed, the **Installation is successful** screen. Click **Restart Now**.
14. The desktop contains shortcuts for the **Asset Explorer** and the **Asset View** applications, and the **Programs** list includes a **Plantweb Optics** folder also with the shortcuts. To access Plantweb Optics, double-click the **Asset Explorer** icon on your desktop and then select your browser, making sure it's a supported browser.

## 5.4 Register licenses

You must register Plantweb Optics 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 a Plantweb 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>/SystemManager`.  
Where `https://<OpticsServerName>:<PortNumber>/SystemManager` is the computer name where System Manager is installed followed by the port number if it is different from the default port 443.  
At the bottom of the screen, this message is displayed: **Please contact your local Emerson sales representative for a license. To install license, click here.**
2. Click the **here** prompt. The **Please Upload the License File** window displays.
3. Click **Choose File** and select the License File to activate. All Plantweb Optics license files have the `.lic` file extension.
4. Click **Activate Product**.
5. After registering the license(s), reboot the server.

If using Plantweb Optics mobile with Azure Mobile Services and you did not register a mobile license file during initial installation, follow [Manually register a Plantweb Optics Mobile license when using Azure Mobile Services](#).

### 5.4.1 Manually register a Plantweb 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 `\PlantwebOptics\<INSTALLATION_DIRECTORY>\config`  
Where *INSTALLATION\_DIRECTORY* is the actual installation directory that you select. When upgrading, the location is `<ORIGINAL_INSTALLATION_DIRECTORY>\config`.
3. Restart the Plantweb Optics server.

## 5.5 View license summary

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

### Procedure

1. Using Google Chrome, enter this URL: `https://<OpticsServerName>/systemmanager`.
2. Click on the **LICENSES** tab.
3. The **Licenses** screen displays. From the Licenses screen the following information appears in the **List View**:
  - **Display Name**: Name of the license
  - **Enabled**: A check box that shows if a license is enabled
  - **Used**: A field that shows the number of licenses that are currently in use out of the total number of licenses issued
  - **Total**: Shows the total number licenses issued
  - **Expiration Date**: Shows the amount of time remaining for each license.

---

### Note

A reminder email is sent once per week for four weeks after a license expires.

---

You can select a license from the list to see more detailed information. The Details pane on the right displays detailed information about the **Feature Key** and the license **Source** in the **Details** field. You can also see if the **Status** of the license is enabled and how many licenses are in use out of the total number of licenses. Finally, you can see specific **Expiration** information that shows when a license began and when the license ends.

From the Licenses page, you can also do the following:

- Search for a license
- Register a license
- Request proposal

- View Guardian Information for an accurate inventory of all licenses

## 5.6 Install the Connector Service

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, 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.

### Prerequisites

- A48ConnectorSvc.1.6.X.X.zip file.
- The Plantweb Optics Certificate is installed. See [Install Plantweb Optics certificates](#). This certificate allows communication to Plantweb Optics web sites.
- 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.1.6.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 ASI and AR installation procedures

ASIs consist of a Data Collector and an optional Proxy that communicate to a common Connector Service to provide asset source data to Plantweb Optics. This chapter introduces each supported ASI and provides the following type or information for each ASI:

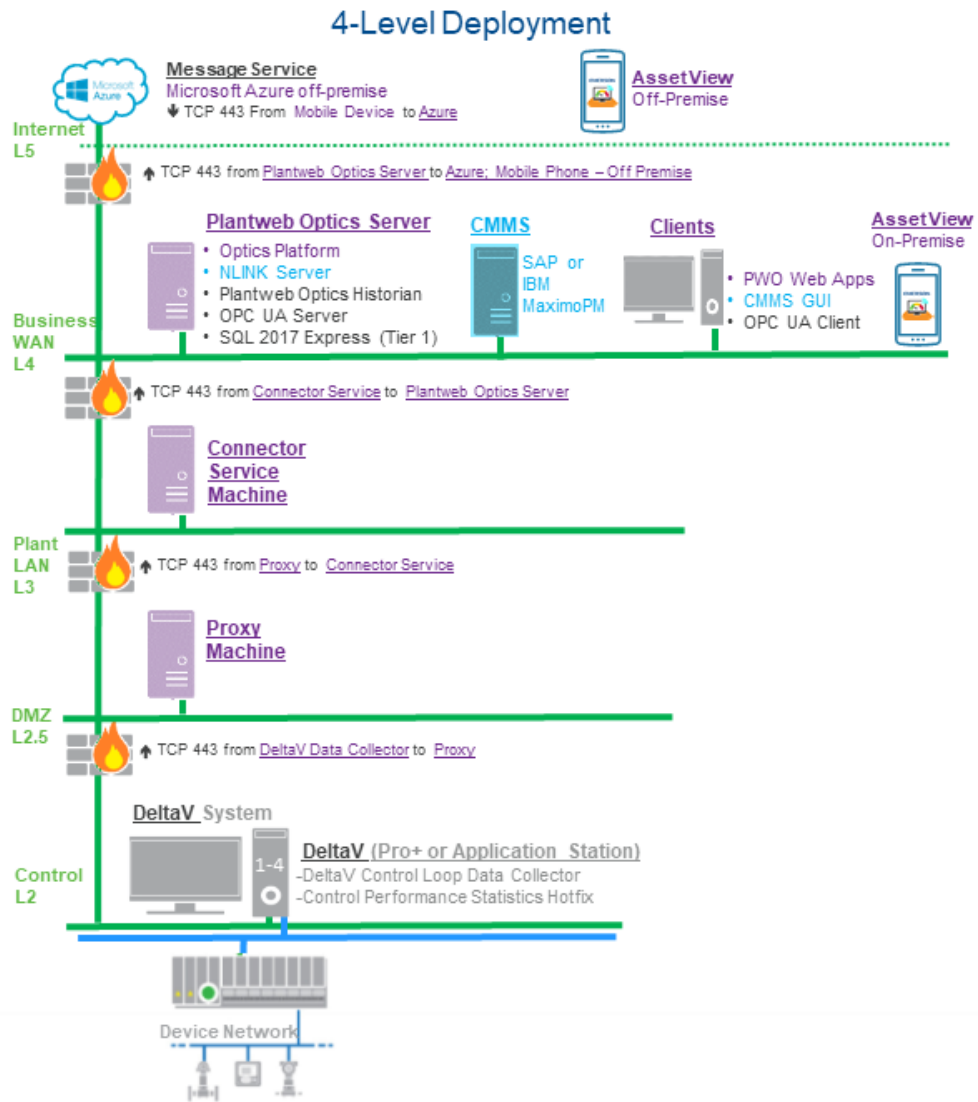
- How you can deploy an ASI along with an example deployment scenario
- How to register each ASI
- How to install each Data Collector
- How you add an asset source to the Data Collector

### 6.1 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



#### Prerequisites

- A48PWOProxy.1.6.X.X.zip file.
- The certificate from the Proxy or the Connector Service this Proxy will send data to is installed. See [Install a Connector Service certificate](#).  
A Proxy requires either the Connector Service or Proxy certificate, depending on which component the Proxy communicates directly with.
- Turn off automatic Windows updates during installation or upgrade.
- The PC name or IP address of the Proxy or Connector Service this Proxy sends data to.



### Procedure

1. Extract the A48PW0Proxy.1.6.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 begin 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 launches in your browser. Configure the newly installed Proxy service: [Configure the Proxy](#).

## 6.2 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 whitelist. 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 Microsoft Edge Chromium.
  - 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 using your Proxy access key credentials. If an access key has not been created, you will be prompted to create one. The access key is case-sensitive.

---

**Note**

Access keys are bound only to the individual Proxy or Data Collector the access key is created on. Access keys are not synchronized across services.


---

### Add the Incoming Proxy or Data Collector IP Address to Whitelist

2. Navigate to the **User Whitelist** 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 whitelist.

### 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/connector-service/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.

## 6.3 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 set or configured within Plantweb Optics. Unhealthy assets (health score less than 80) are added to the unhealthy Assets KPI in Asset View.
- **Events and messages**—AMS Asset Monitor events and messages are displayed in Plantweb Optics. Alerts generated by AMS Asset Monitor with an Advise, Warning, or Critical 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.

- You can install a Data Collector and Connector Service on one or two PCs depending on your network requirements.
- A Data Collector can communicate with only one Connector Service.
- A Connector Service can receive data from multiple Data Collectors.
- A Plantweb Optics server can communicate with multiple Data Collectors.

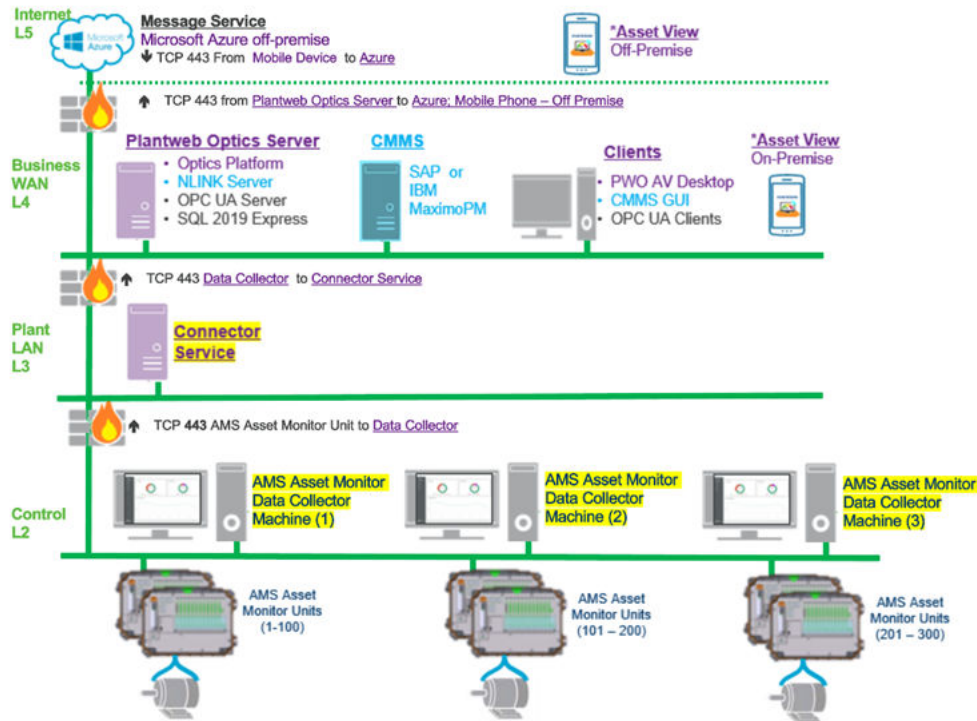
### 6.3.1 AMS Asset Monitor ASI deployment scenarios

#### 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 multiple Data Collectors sending data to Plantweb Optics through a single Connector Service:

**Figure 6-2: AMS Asset Monitor ASI Multiple Data Collector deployment scenario**



**Note:** \* Only one Asset View mobile deployment is allowed either On-Prem or Off-Premise

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.

## 6.3.2 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.
- A48AMS\_AM-DS-0.1.6.X.X.zip file.

### Procedure

1. Extract A48AMS\_AM-DS-0.1.6.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. 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](#).

## 6.3.3 Install the AMS Asset Monitor Data Collector

### Prerequisites

- A48AMS\_AM\_ASI.1.6.X.X.zip file.
- The certificate from the Proxy or the Connector Service that the Data Collector will send data to is installed. See, [Install a Proxy certificate](#) or [Install a Connector Service certificate](#).

A Data Collector requires either a Connector Service or Proxy certificate, depending on which server the Data Collector communicates directly with.

- The Data Collector must be installed on a machine that resides on the same network level as AMS Asset Monitor.
- 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 A48AMS\_AM\_ASI.1.6.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 **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: [Certificate installations](#).

## 6.3.4 Add an asset source to the AMS Asset Monitor Data Collector

**Prerequisites**

- The Connector Service is installed.
- 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.
- Install the security certificate of the device on the Asset Monitor Data Collector server.
- 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 Microsoft Edge Chromium.
  - 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.

- c) Log in using your access key credentials. If an access key has not been created, you will be prompted to create one. The access key is case-sensitive.

---

**Note**

Access keys are bound only to the individual Proxy or Data Collector the access key is created on. Access keys are not synchronized across services.

---

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** (for example, `https://<IP Address>/en`) of your AMS Asset Monitor web interface.
6. Enter the **Username** and **Password** used to connect to your AMS Asset Monitor web interface.
7. Enter a description for the asset source.
8. Click **Add** to begin sending asset source data to Plantweb Optics.

## 6.4 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. See [Opt-In to Device Parameters](#), for instructions on opt-in device-specific variables.
- **Overdue calibrations**—overdue calibrations KPI is displayed in Asset View.

### **⚠ CAUTION**

When you install the AMS Device Manager Data Collector, 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.

When the same Gateway connects through multiple Data Collectors to present different alarm and health information, it is important to configure Plantweb Optics correctly to avoid potential duplication of assets and information.

When your system gets into a state where there is duplication of information, contact Emerson Product Support for recommendations. There is no automated or available user-facing procedure to recover from this condition.

### **AMS Device Manager ASI Components**

Three components 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 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.
- Each Connector Service can receive data from multiple Data Collectors.
- Each Plantweb Optics system can communicate with multiple Connector Services.

## **6.4.1 AMS Device Manager ASI deployment scenarios**

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.



**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.

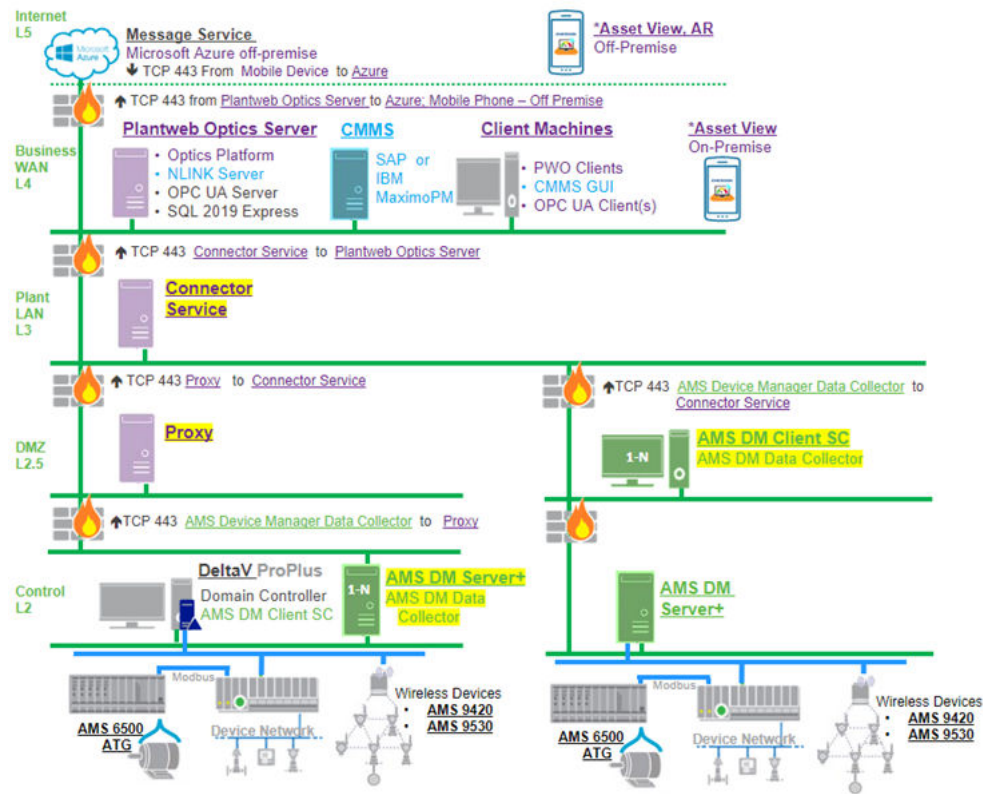
**CAUTION**

The server name for the AMS Device Manager should contain only Latin-1 (ISO-8859-1) characters. Avoid inserting localized characters. A PC name with localized characters prevents you from adding the AMS Device Manager as an asset source.

**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 multiple Data Collectors and the Connector Service:

**Figure 6-3: AMS Device Manager ASI Components for a Multiple Data Collector deployment**



**Note:** \* Only one Asset View mobile deployment is allowed either On-Prem or Off-Premise

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 Connector Service on the Plantweb Optics server and keep the AMS Device Manager Data Collector on its own server.

## 6.4.2 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.1.6.X.X.zip file.

#### Procedure

1. Extract A488000-DS0.AMS\_DM\_ASI.1.6.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](#).

## 6.4.3 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.1.6.X.X.zip file.
- The certificate from the Proxy or the Connector Service that the Data Collector will send data to is installed. See, [Install a Proxy certificate](#) or [Install a Connector Service certificate](#).  
A Data Collector requires either a Connector Service or Proxy certificate, depending on which server the Data Collector communicates directly with.
- If installing on a Windows Server 2008 R2 or a Windows 7 operating system, Windows automatic updates must be enabled.
- The TLS 1.0 protocol is not disabled on Server 2008 R2 machines, particularly if the machines are accessed through RDP or are DeltaV Workstations.
- 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 the AMS Device Manager Data Collector, 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.

When the same Gateway connects through multiple Data Collectors to present different alarm and health information, it is important to configure Plantweb Optics correctly to avoid potential duplication of assets and information.

When your system gets into a state where there is duplication of information, contact Emerson Product Support for recommendations. There is no automated or available user-facing procedure to recover from this condition.

### Procedure

1. Extract the A488000-DS0.AMS\_DM\_ASI.1.6.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 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 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: [Certificate installations](#).

## 6.4.4 Add an asset source to the AMS Device Manager Data Collector

**Prerequisites**

- The Connector Service is installed.
- 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 Microsoft Edge Chromium.
  - 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.

- c) Log in using your access key credentials. If an access key has not been created, you will be prompted to create one. The access key is case-sensitive.

---

**Note**

Access keys are bound only to the individual Proxy or Data Collector the access key is created on. Access keys are not synchronized across services.

---

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) Enter a description for the asset source.
  - d) Select **Add Location 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.

---

**Note**

You have the option to select any unbound device from the Network navigator and manually bind it to a location in the Location navigator.

---

- 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.

## 6.4.5 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

---

### Note

Leaving a field blank can cause issues. Make sure you populate all fields.

---

### 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

Use the following procedure to gather device parameters from your AMS Device Manager system and pass them through to Plantweb Optics. The Data Collector requires a .csv file with the device's AMS Tag. The following procedure shows you how to create a .csv file of selected devices of interest.

### Prerequisites

You will need the 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 select the following: 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.

- a) **Export to file:** Browse and select a location to save the file name.
  - b) **Device Parameters/Configurations:** Leave both of these options unchecked.
  - c) **Other:** Check 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 then select the devices of interest.
  - d) **Include Data:** Click the **Current** radial button.
  - e) 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. Insert AMS Device Manager DVD2 into the DVD drive. Navigate to **Supplemental Tools > Reporting Tools** and open the file **DeviceList.xltm** Microsoft Excel to enable the macros to run.
  5. Select **Enable Content** and **Trust Document**, if necessary.
  6. Click **Load XML** to import the **Device List XML** file you saved previously.
  7. Rename the **AMS Tag** column header to **AMSTag**. There should be no space between **AMS** and **Tag**.
  8. Filter the devices as necessary, adding any **Group** column data from previous steps, making sure any **AMSTag** fields match.
  9. In Excel, choose **File > Save As...** and save the file as a comma separated values (csv) file. Do not select **CSV UTF-8 .csv**.

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 two columns at the end of row 5 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 **0** stops collecting the data when it has been previously collected.

---

### Note

The more 1's you have, the longer it takes to read all the process variables.

---



3. Save the file as save the file as a comma separated values (csv) file. Do not select 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.
- An access key for the locally installed AMS Device Manager Data Collector has been created.

#### Procedure

1. From the Windows Start menu select, **AMS Device Manager Source → AMS Device Manager Data Collector Param Read Configuration**.
2. Enter the access key used to log in to the locally installed AMS Device Manager Data Collector.
3. Select **Import a comma separated file (\*.csv) to configure device/parameter group options**.
4. From the AMS Device Manager ASI Service Import Parameter Read Options window, select the following:
  - a) Select **Browse** to locate the .csv file.
  - b) Change the header row value to 5 or the row that contains the header. The names must match exactly.
  - c) Select **Validate** and correct any errors in parsing the .csv file.
5. If no errors are detected in the file, Select **Import**.
6. 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).
7. Click **Close** when complete.

## 6.5 Install the AMS Machine Works ASI

AMS Machine Works is Emerson's machinery analysis software that combines state-of-the-art technology and predictive maintenance techniques with comprehensive vibration analysis tools to provide quick and accurate assessments of machinery health in your facility. For customers who want to benefit from the features of Plantweb Optics such as Asset View, Plantweb Optics mobile, CMMS connectivity, and Plantweb Historian, they can license the AMS Machine Works ASI to connect an AMS Machine Works Data Collector to Plantweb Optics.

AMS Machine Works supports the AMS Wireless Vibration Monitor, AMS 9420, AMS 6500 ATG, and the Ovation Machinery Health Monitor Module. AMS Machine Works is installed as a standalone product and cannot co-exist on a Plantweb Optics server. AMS Machine Works connectivity to Plantweb Optics v1.6 is enabled through the AMS Machine Works ASI. The AMS Machine Works Data Collector gathers vibration and process data from AMS Machine Works and reports that information to Plantweb Optics.

AMS Machine Works provides the following types of information to Plantweb Optics.

- Machine health
- Asset and system health
- Machines that need your immediate attention
- Work recommendations and status
- Machine journal activity

## 6.5.1 AMS Machine Works ASI deployment scenario

The AMS Machine Works ASI is comprised of a AMS Machine Works Data Collector, Plantweb Optics Proxy (if one is required), and a Plantweb Optics Connector Service. You can deploy the AMS Machine Works Data Collector with:

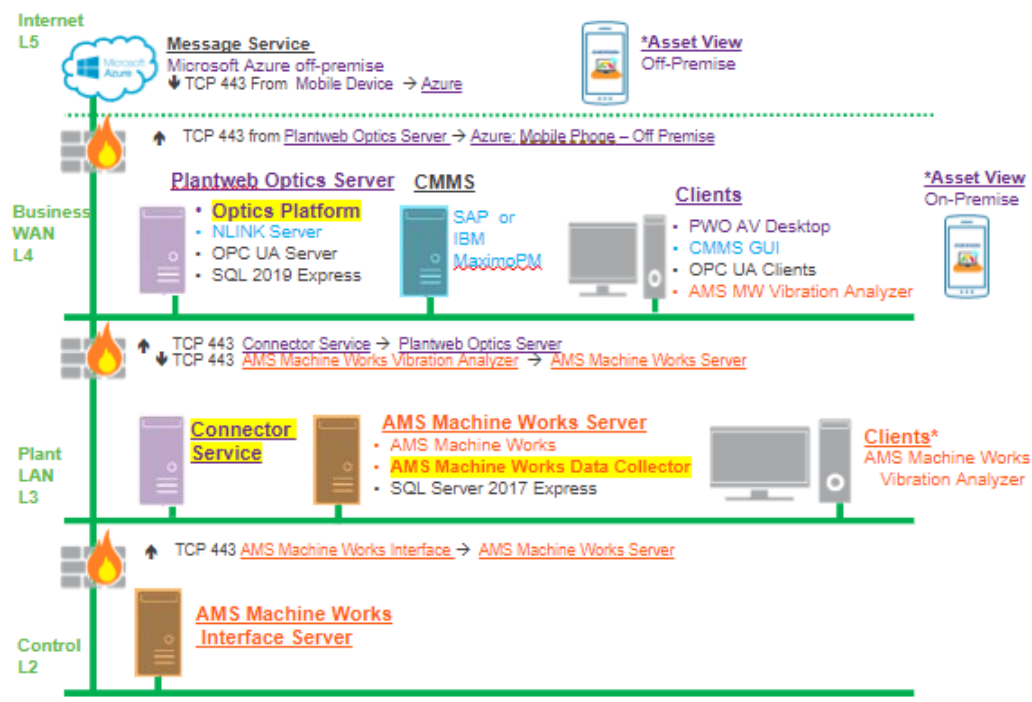
- Plantweb Optics and the Connector Service co-deployed on the same server
- Plantweb Optics with the Connector Service and a Proxy (if required) on separate servers
- AMS Machine Works on the same AMS Machine Works server

Understanding the estimated system load along with the level of security you want to achieve helps you determine the number of network layers between the data source and Plantweb Optics. It also dictates the components you need and if you need to install the Connector Service on a different server and utilize a proxy server. The following list describes deployment considerations useful when deciding which deployment scenario works best for your environment. Each of the following examples assumes the AMS Machine Works Data Collector is installed on the AMS Machine Works server.

- In a deployment with the Plantweb Optics server and the Connector Service co-existing on the same server on level 4, you can choose to configure the AMS Machine Works server on level 2 and incorporate a Proxy server on level 3, or you can deploy the AMS Machine Works server on level 3 communicating directly to the Connector Service on the Plantweb Optics server.
- In a deployment with the Plantweb Optics server and the Connector Service on separate servers on different levels, you can deploy the AMS Machine Works server on level 2 and configure a Proxy server on level 3, or you can deploy the AMS Machine Works server on the same level as the Connector Service server (level 3).
- In a deployment with multiple AMS Machine Works Data Collectors, you can configure one AMS Machine Works server on level 2 that communicates to a Connector Service server on level 3. You can also configure a second AMS Machine Works server on level 3 that communicates to a Connector Service server that is also on level 3. You can configure up to five AMS Machine Works servers on a Plantweb Optics system. You can also have one AMS Machine Works server for one Machine Works Data Collector.

The figure below demonstrates the deployment of AMS Machine Works ASI components with the Data Collector sending data to Plantweb Optics through a single Connector Service:

**Figure 6-4: AMS Machine Works Data Collector on Level 3 deployment**



## 6.5.2 Register the AMS Machine Works ASI with Plantweb Optics

Before installing the AMS Machine Works ASI, you must register it on the Plantweb Optics server. This process allows the AMS Machine Works ASI to properly create assets in Plantweb Optics.

### Prerequisites

- Plantweb Optics is installed on the computer designated as the Plantweb Optics server.
- A48AMS\_MW-DS-0.1.6.X.X.zip file.

### Procedure

1. Extract A48AMS\_MW-DS-0.1.6.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. If you accept, click **Next**.

5. Select **Registration** and then click **Next**.
6. Verify the installation destination folder and then click **Next**.
7. Click **Finish** to complete the registration process.

### Postrequisites

After the registration process is complete, install the AMS Machine Works Data Collector.

## 6.5.3 Install the AMS Machine Works Data Collector

### Prerequisites

- A48AMS\_MW\_ASI.1.6.X.X.zip
- The certificate from the Connector Service or the Proxy that the Data Collector will send data to is installed. Which server the Data Collector communicates directly with determines which certificate you must install. See, [Install the Connector Service](#) or [Install the Proxy](#).  
A Data Collector requires either a Connector Service or Proxy certificate, depending on which server the Data Collector communicates directly with.
- The Data Collector must be installed on a machine that resides on the same network level as AMS Machine Works server. The Data Collector can be installed on the AMS Machine Works server.
- 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 Machine Works ASI registration process has been completed on the Plantweb Optics server: [Register the AMS Machine Works ASI with Plantweb Optics](#)

### Procedure

1. Extract the A48AMS\_MW\_ASI.1.6.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 **AMSMachineWorksDataCollector\_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 then click **Next**.
6. Verify the installation destination folder and then click **Next**.
7. Enter the PC name/IP address and port number where the Connector Service is installed. Port 443 is the default port that the Connector Service uses. Click **Next**.

---

#### Note

If using the Proxy service, enter the Proxy server PC name/IP address and port number that the Proxy uses 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.
11. Click **Finish** to complete the installation.

#### Postrequisites

After installation, the AMS Machine Works 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.

## 6.5.4 Add an asset source to the AMS Machine Works Data Collector

#### Prerequisites

- The Connector Service is installed, and the Connector Service security certificate is installed on the appropriate servers.
- The Proxy is installed (if it is required). If a Proxy is used ensure the Proxy security certificate is installed on the appropriate server.
- Ensure the AMS Machine Works Data Collector is installed on the AMS Machine Works server.
- An asset source is not already configured in the Data Collector.

#### Procedure

1. Launch the AMS Machine Works Data Collector user interface.
  - a) Launch Google Chrome or Microsoft Edge Chromium.
  - b) Navigate to `https://<Data_Collector_PC_Name>/AMSMachineWorksDataCollector` 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>/AMSMachineWorksDataCollector`.

Replace `<Data_Collector_PC_Name>` with the name of the PC where the Data Collector is installed and `<PortNumber>` with the port the Data Collector is bound to.
  - c) From the **AMS Machine Works** → **Log In** page, enter your access key credentials and then click **Submit**. If an access key has not been created, you are prompted to create one. The access key is case-sensitive.

---

**Note**

Access keys are bound only to the individual Proxy or Data Collector the access key is created on. Access keys are not synchronized across services.

---

2. From the **Asset Sources** page, click the + icon to add a new asset source.
3. From the **Add Asset Source** dialog, select the **Site** you want associated with the asset source.
4. Enter a **Display Name** for the new asset source. Assets appear under this name in Plantweb Optics Asset Explorer.

---

**Note**

If you want to change the name of an asset after it has been created, use the **Update** feature in the user interface to update the hierarchy.

---

5. Enter a description for the asset source.
6. Enter the full **Connection URL** (`https://<machineworks [3cmachineworks] server name>`) of your AMS Machine Works web interface.
7. Optional: Select **Add Location Hierarchy** to display the AMS Machine Works 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 need to remove and add the asset source again.
8. Click **Add** to add the asset source and begin sending data to Plantweb Optics.

## 6.6 Install the AMS Machinery Manager ASI

### AMS Machinery Manager ASI Features

The AMS Machinery Manager Data Collector gathers data from AMS Machinery Manager 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 Machinery Manager. 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 Machinery Manager. Each parameter and value displayed in AMS Machinery Manager will have a corresponding parameter and value in Plantweb Optics.
- **Asset health**—Asset health is displayed in Plantweb Optics. The Asset health score (100 - Asset Severity in AMS Machinery Manager) is added to the unhealthy dashboard in Asset View.
- **Events and messages**—AMS Machinery Manager events and messages are displayed in Plantweb Optics. You can access these messages in the Asset View application, by clicking the Settings (gear) icon and selecting the AMS Machinery Manager KPIs **Routes Overdue**, **Down Units**, and **Serious Problems** to display.

### AMS Machinery Manager ASI Components

Three components allow the AMS Machinery Manager 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:

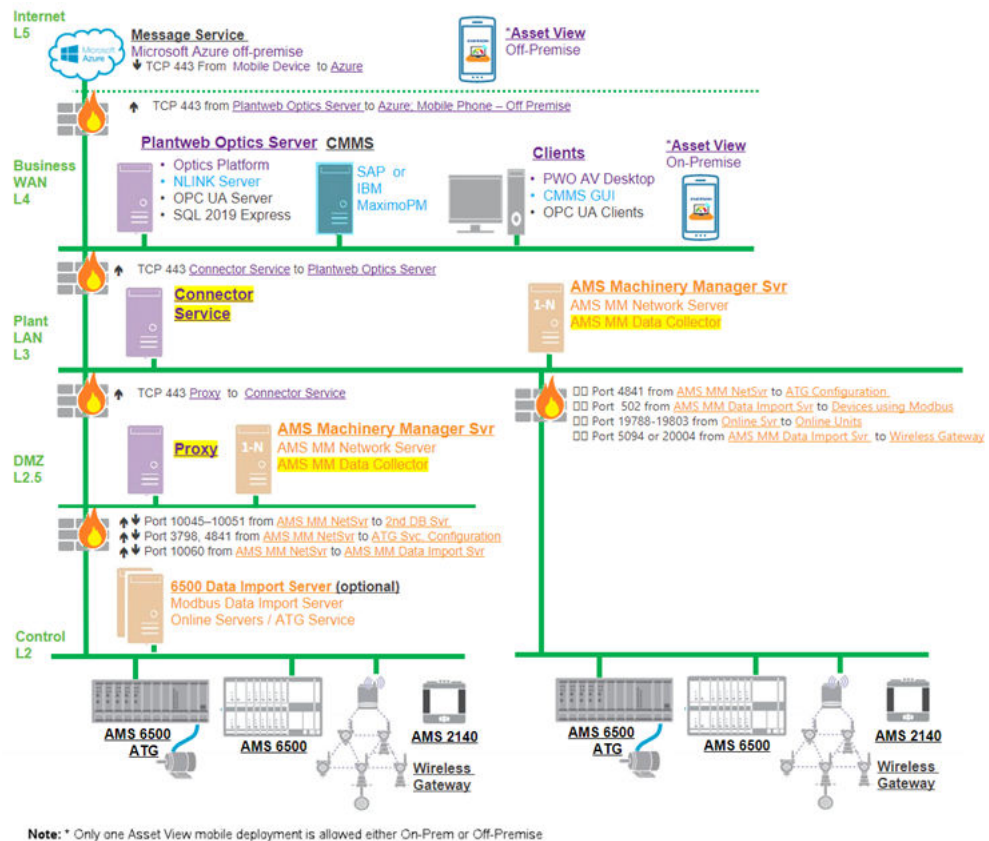
- The Data Collector and Connector Service can be installed on one or two PCs depending on your network requirements.
- Each Data Collector can communicate with only one Connector Service.
- Each Connector Service can receive data from multiple Data Collectors.
- Each Plantweb Optics system can communicate with multiple Connector Services.

## 6.6.1 AMS Machinery Manager ASI deployment scenarios

### Install AMS Machinery Manager ASI Components on Separate PCs

If Plantweb Optics and AMS Machinery Manager are on different networks, or are separated by a firewall, you must deploy the AMS Machinery Manager Data Collector and the Connector Service on different servers. 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 Machinery Manager ASI components with multiple Data Collectors sending data to Plantweb Optics through a single Connector Service:

**Figure 6-5: AMS Machinery Manager ASI Components for a Multiple Data Collector deployment**



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

### Install AMS Machinery Manager ASI components on a single PC

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

#### Note

If you install the Connector Service and Data Collector on the same PC, make sure both meet the minimum system requirements and the PC has the resources to accommodate both components.

## 6.6.2 Configure AMS Machinery Manager before importing databases

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



### Prerequisites

- Run the Database Converter Tool before importing the AMS Machinery Manager database into Plantweb Optics or use it with AMS Machinery Manager 6.31.
- Install AMS Machinery Manager 6.31 or later.
- Any database you import must already be operational in AMS Machinery Manager 6.31.

### Procedure

1. 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` filename extension. If the database is in a zip folder, you first need to extract the database.
    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.
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

---

**Note**

Emerson recommends you notify the user before importing databases.

---

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.

## 6.6.3 Register the AMS Machinery Manager ASI with Plantweb Optics

Before installing the AMS Machinery Manager ASI, register the AMS Machinery 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 designated as the Plantweb Optics server.
- A48AMS\_MM-DS-0.1.6.X.X.zip file.

**Procedure**

1. Extract A48AMS\_MM-DS-0.1.6.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. 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 Machinery Manager Data Collector: [Install the AMS Machinery Manager Data Collector](#).

## 6.6.4 Install the AMS Machinery Manager Data Collector

**Prerequisites**

- A48AMS\_MM\_ASI.1.6.X.X.zip file.

- The certificate from the Proxy or the Connector Service that the Data Collector will send data to is installed. See, [Install a Proxy certificate](#) or [Install a Connector Service certificate](#).

A Data Collector requires either a Connector Service or Proxy certificate, depending on which server the Data Collector communicates directly with.

- The Data Collector must be installed on AMS Machinery Manager.
- 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 Machinery Manager ASI registration process has been completed on the Plantweb Optics server: [Register the AMS Machinery Manager ASI with Plantweb Optics](#).

### Procedure

1. Extract the A48AMS\_MM\_ASI.1.6.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 **AMSMachineryManagerDataCollector\_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. 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.

---

7. Enter the local port number the Data Collector will be bound to. Port 443 is the default port.
8. Enter the AMS Machinery Manager Administrator account password.
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 Machinery Manager 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 Machinery Manager asset source must be installed on the Data Collector the asset source will communicate with: [Certificate installations](#).

## 6.6.5 Add an asset source to the AMS Machinery Manager Data Collector

### Prerequisites

- The Connector Service is installed.
- The Proxy is installed.
- The Connector Service and (if applicable) Proxy security certificates are installed on the appropriate servers.
- An asset source is not configured in the Data Collector.

### Procedure

1. Launch the AMS Machinery Manager Data Collector user interface.
  - a) Launch Google Chrome or Microsoft Edge Chromium.
  - b) Navigate to `https://<Data_Collector_PC_Name>/AMSMachineryManagerDataCollector` 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>/AMSMachineryManagerDataCollector`.

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.
  - c) Log in using your access key credentials. If an access key has not been created, you will be prompted to create one. The access key is case-sensitive.

---

#### Note

Access keys are bound only to the individual Proxy or Data Collector the access key is created on. Access keys are not synchronized across services.

---

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 Server Name of the AMS Machinery Manager network server.
6. Enter a description for the asset source.
7. Click **Add** to add the asset source.
8. Go to the AMS Machinery Manager Data Collector. Select the Manage Database function to add a specific Machinery Manager database to Plantweb Optics.

9. Select **Add Location Hierarchy** to display the AMS Machinery Manager hierarchy.

---

#### Need help?

If Plantweb Optics does not begin receiving Machinery Manager asset data, refer to the Troubleshooting section of the *Plantweb Optics System Guide*. Check the **AMS Machinery Manager ASI** table for problems and solutions.

---

## 6.7 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

Three components allow the DeltaV Control Loop 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.
- Each Connector Service can receive data from multiple Data Collectors.
- Each Plantweb Optics system can communicate with multiple Connector Services

### New *ControlLoopSvc* Windows user considerations

A new Windows group Managed User Account *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.

## 6.7.1 DeltaV Control Loop ASI deployment scenarios

### Compatibility

The DeltaV Control Loop ASI can be deployed on 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.

---

### Note

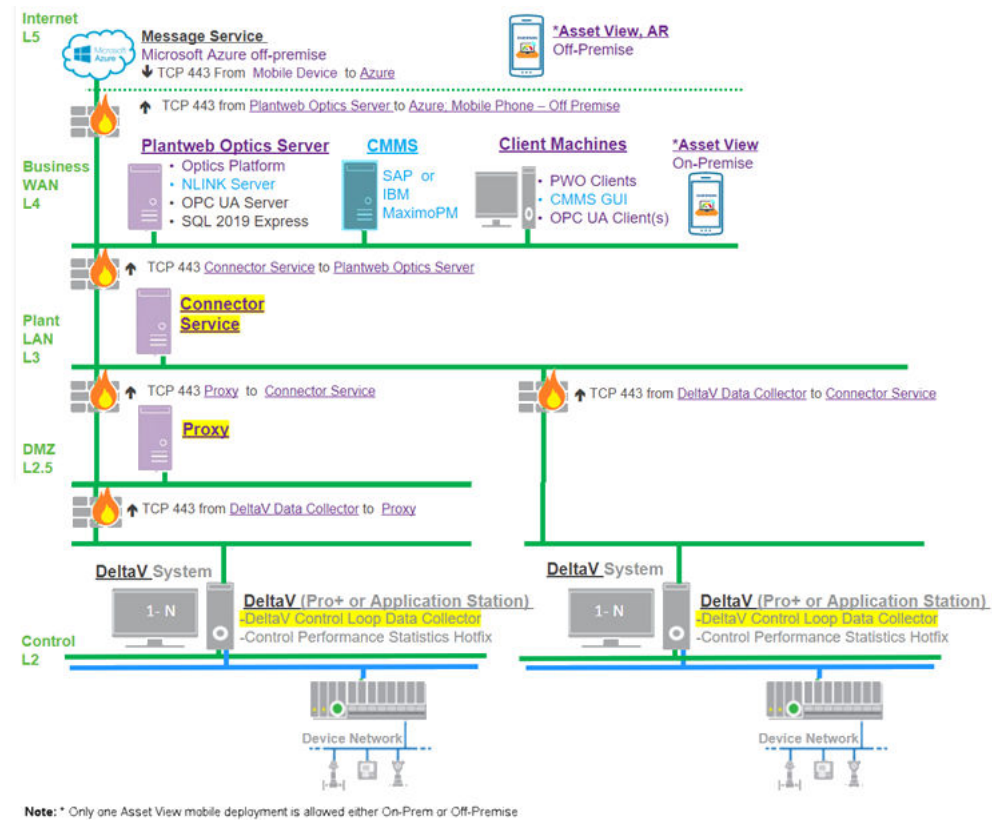
The Data Collector requires a 64-bit operating system and does not support Windows Server 2008 (32-bit). Windows Server 2008 R2 is supported.

---

### 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 multiple Data Collectors and the Connector Service:

Figure 6-6: 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.

## 6.7.2 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-0.1.6.X.X.zip file.

### Procedure

1. Extract A48CtrlLoop-DS-0.1.6.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 DeltaV Control Loop Data Collector: [Install the DeltaV Control Loop Data Collector](#).

## 6.7.3 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-0.1.6.X.X.zip file.
- The certificate from the Proxy or the Connector Service to which the Data Collector sends data is installed. See, [Install a Proxy certificate](#) or [Install a Connector Service certificate](#).  
A Data Collector requires either a Connector Service or Proxy certificate, depending on which server the Data Collector communicates directly with.
- 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, DeltaV v14.LTS (Long Term Support), or DeltaV v14.FP#.



- 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-0.1.6.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-0.1.6.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. Right-click **DeltaVControlLoopDataCollector.exe** and select **Run as administrator**.
9. Click **Next**.
10. On the **Software License Terms** screen, read and accept the software license agreement and then click **Next**.
11. Select **Data Collector** and click **Next**.
12. 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.

---

13. Verify the Data Collector installation destination folder and click **Next**.
14. 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.

---

15. Enter the local port number that the Data Collector will be bound to and click **Next**. Port 443 is the default port.
16. 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.
17. 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: [Certificate installations](#).

If using Microsoft Edge Chromium, a blank screen may appear when the Data Collector user interface launches. If this occurs, continue the installation with [Configure Microsoft Edge Chromium for use with a Data Collector](#).

## Configure Microsoft Edge Chromium for use with a Data Collector

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

**Procedure**

1. In Microsoft Edge Chromium, 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 Microsoft Edge Chromium and continue with adding an asset source: [Add an asset source to the DeltaV Control Loop Data Collector](#)

## 6.7.4 Add an asset source to the DeltaV Control Loop Data Collector

**Prerequisites**

- The Connector Service is installed.

- 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 Collector user interface.
  - a) Launch Google Chrome or Microsoft Edge Chromium.
  - 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.
  - c) Log in using your access key credentials. If an access key has not been created, you will be prompted to create one. The access key is case-sensitive.

---

#### Note

Access keys are bound only to the individual Proxy or Data Collector the access key is created on. Access keys are not synchronized across services.

---

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.

---

#### Note

If you want to change the name of an asset after it has been created, use the **Update** feature in the user interface to update the hierarchy.

---

- 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.

## 6.7.5 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*, in the Plantweb Optics System Guide 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, 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.
6. Change the password on the Application Station.

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.

7. Update the `DeltaVControlLoopDataProducer` service with the new password created in step 5.

Complete the following steps on the server where the Data Collector is installed (either the ProfessionalPLUS server or Application Station).

- a. In the Windows start menu, search for **Services**.

- b. Right-click the `DeltaVControlLoopDataProducer` service and click **Properties**.
- c. Click the **Log On** tab. Ensure that **This Account** is selected.
- d. Enter the `ControlLoopSvc` user password created in step 5. Click **OK**.
- e. Right-click the `DeltaVControlLoopDataProducer` service and click **Restart**.

## 6.8 Install the Optics Analytics ASI

---

### Note

All Optics Analytics ASI deployment, registration, and installation steps in the following topics apply directly to the KNet ASI.

---

Before you can install the Optics Analytics (KNet) Data ASI you must first install and configure Optics Analytics or KNet on a server. After it is installed and configured you can proceed with the installation of the Optics Analytics or KNet Data Collector on the same server.

See the **Optics Analytics Quick Configuration Guide** at the following location for information on how to configure Optics Analytics.

<installed drive>:\PlantwebOptics\site\OpticsAnalyticsDataCollector\Optics Analytics Quick Configuration Guide.pdf

---

### Note

For information on how to configure KNet, see the **KNet Quick Configuration Guide** at the following location.

<installed drive>:\PlantwebOptics\site\KNetDataCollector\KNet Quick Configuration Guide.pdf

---

### Optics Analytics (KNet) ASI Features

The Optics Analytics (KNet) ASI gathers data from 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 Optics Analytics Map module. If no hierarchy is defined, the Data Collector sends a flat hierarchy to Plantweb Optics.
- **Asset properties**—all properties configured to be displayed in Plantweb Optics from Optics Analytics Object. When a new property is added in Optics Analytics 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 an RCA Problem block. When RCA Problem blocks are active, the Problem block with the lowest health score is set as the asset health score. Otherwise, the asset is marked as healthy. The active root cause is also displayed.
- **Events**—The Optics Analytics ASI provides both system and device-specific events. RCA Problem blocks are the main events gathered by the 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).

### Optics Analytics (KNet) ASI Components

Three components allow the Optics Analytics 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.
- Each Connector Service can receive data from multiple Data Collectors.
- Each Plantweb Optics system can communicate with multiple Connector Services

## 6.8.1 Optics Analytics ASI deployment scenarios

### Install Optics Analytics ASI Components on Separate PCs

---

#### Note

All Optics Analytics ASI deployment information directly relates to the KNet ASI deployment information.

---

If Plantweb Optics and Optics Analytics (KNet) are on different networks, or are separated by a firewall, you must deploy the Data Collector on the Optics Analytics (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 multiple Data Collectors and the Connector Service:

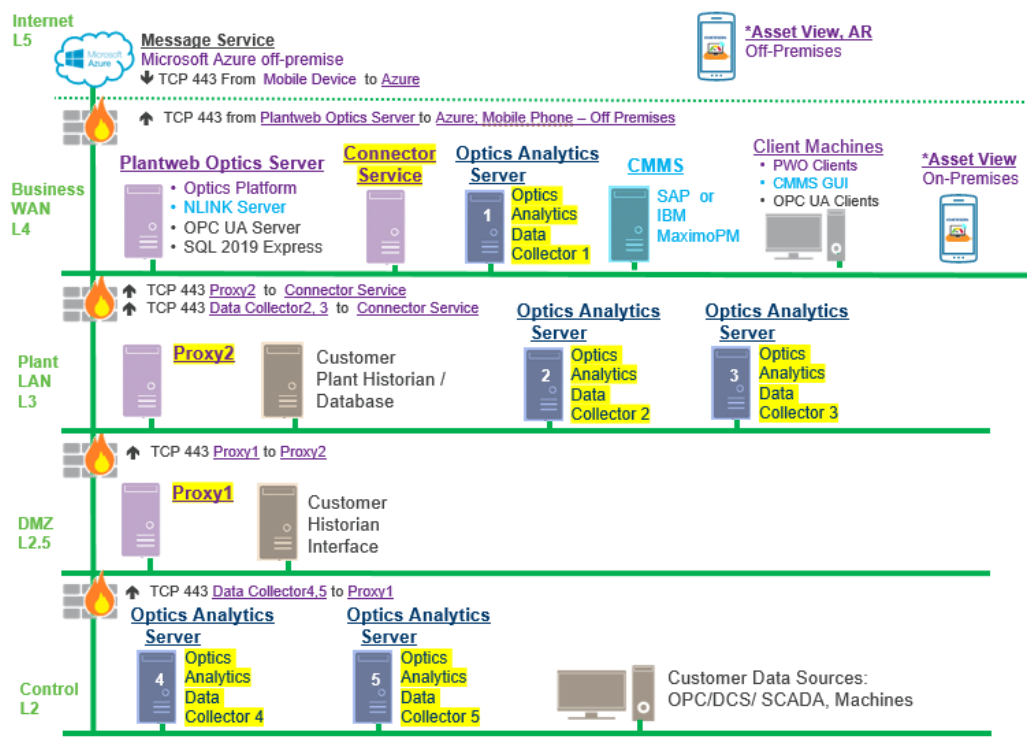
---

#### Note

The deployment scenario applies to KNet Data Collectors too.

---

**Figure 6-7: Optics Analytics ASI Components for a Multiple Data Collector deployment**



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

### Install Optics Analytics (KNet) ASI components on a single PC

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

## 6.8.2 Register the Optics Analytics ASI with Plantweb Optics

### Note

This Optics Analytics ASI registration process is the same process used for the KNet ASI.

Before installing the Optics Analytics (KNet) ASI, register the it 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-0.1.6.X.X.zip file.

### Procedure

1. Extract A48KNET-DS-0.1.6.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. On the **Software License Terms** screen, read and accept the software license agreement and then 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 133](#) 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 Optics Analytics (KNet) Data Collector.

## 6.8.3 Install the Optics Analytics Data Collector

---

**Note**

This Optics Analytics Data Collector installation process is the same process used for the KNet Data Collector.

---

Follow this procedure on the Optics Analytics (KNet) server to install the Optics Analytics Data Collector.

**Prerequisites**

- A48KNET-DS-0.1.6.X.X.zip file.
- Install Optics Analytics 5.3 on a server and then install the Data Collector on the same server.

---

**Note**

If you are installing the KNet Data Collector, you must install KNet 5.2 on a server and then you can install the Data Collector the same server.

---

- The certificate from the Proxy or the Connector Service that the Data Collector will send data to is installed. See, [Install a Proxy certificate](#) or [Install a Connector Service certificate](#).

A Data Collector requires either a Connector Service or Proxy certificate, depending on which server the Data Collector communicates directly with.

- 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 Optics Analytics ASI (or KNet ASI) registration process has been completed on the Plantweb Optics server. See [Register the Optics Analytics ASI with Plantweb Optics](#).

### Procedure

1. Extract the A48KNET-DS-0.1.6.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 **OpticsAnalyticsDataCollector\_Setup.exe** and select **Run as administrator**.

---

#### Note

If you are installing a KNet Data Collector, right-click **KNetDataCollector\_Setup.exe** and select **Run and 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 automatically resumes after your PC reboots.
10. Click **Next** to continue installation of third-party components. Click **Finish** to complete the installation.

### Postrequisites

After installation, the Optics Analytics (KNet) Data Collector user interface opens in your browser. Continue the ASI installation with [Add an asset source to the Optics Analytics Data Collector](#).

## 6.8.4 Add an asset source to the Optics Analytics Data Collector

### Prerequisites

The following procedure describes how to add an asset source to the Optics Analytics Data Collector.

- The Connector Service is installed.
- The Proxy is installed.
- The Connector Service and (if applicable) Proxy security certificates have been installed on the Optics Analytics Data Collector server.
- An asset source is not configured.

### Procedure

1. Launch the Optics Analytics Data Collector user interface.
  - a) Launch Google Chrome or Microsoft Edge Chromium.
  - b) Navigate to `https://<Data_Collector_PC_Name or IP Address>>/OpticsAnalyticsDataCollector` 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>/OpticsAnalyticsDataCollector`.

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.
  - c) Log in using your access key credentials. If an access key has not been created, you will be prompted to create one. The access key is case-sensitive.

---

#### Note

Access keys are bound only to the individual Proxy or Data Collector the access key is created on. Access keys are not synchronized across services.


---

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 display under this name in Plantweb Optics.

---

#### Note

If you want to change the name of an asset after it has been created, use the

**Update** feature in the user interface (click the **More Options** menu icon  and click **Update**) to update the hierarchy.

---

5. Enter a description for the asset source.
6. Enter the server name, server port, callback port, and user credentials used to connect to Optics Analytics.
7. Click the **Customize** button to display the Optics Analytics Engine Configuration section.
8. 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 are sent to Plantweb Optics.

---

9. Click **Done**.
10. Select **Include -RCA Screenshots** to include a PDF containing -RCA screenshots when asset messages are delivered to Plantweb Optics.
11. Select **Add Location 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 need to remove and add the asset source again.
12. Click **Add** to finish adding the asset source.

## 6.9 Install the Plantweb Insight ASI

The Plantweb Insight Asset Source Interface (ASI) brings analytics into Plantweb Optics and helps users better manage their plant assets. Plantweb Insight passes information from the Plantweb Insight System, using Microsoft Internet Information Services, through HTTPS to Plantweb Optics to notify customers of abnormal situations about their assets. Plantweb Insight works with the Plantweb Optics application to keep users informed about the health of their assets from anywhere.

The Plantweb Insight Data Collector provides results of prepackaged analytics on some of the most critical assets such as steam traps, pumps, heat exchangers, wireless pressure gauges, and pressure relief valves. Users gain real-time information about:

- Asset details including type and location
- Manufacturer and model numbers
- Asset state
- Asset health
- Energy costs
- Emission loss

The Plantweb Insight Data Collector can communicate with only one Plantweb Optics installation and up to five Plantweb Insight asset sources to provide early notifications of a failing assets. Early notifications such as these enable users to utilize the real-time information to make critical decisions and increase plant efficiency.

### 6.9.1 Plantweb Insight deployment scenario

The Plantweb Insight ASI is comprised of a Plantweb Insight Data Collector, Plantweb Optics Proxy (if one is required), and a Plantweb Optics Connector Service. You can deploy

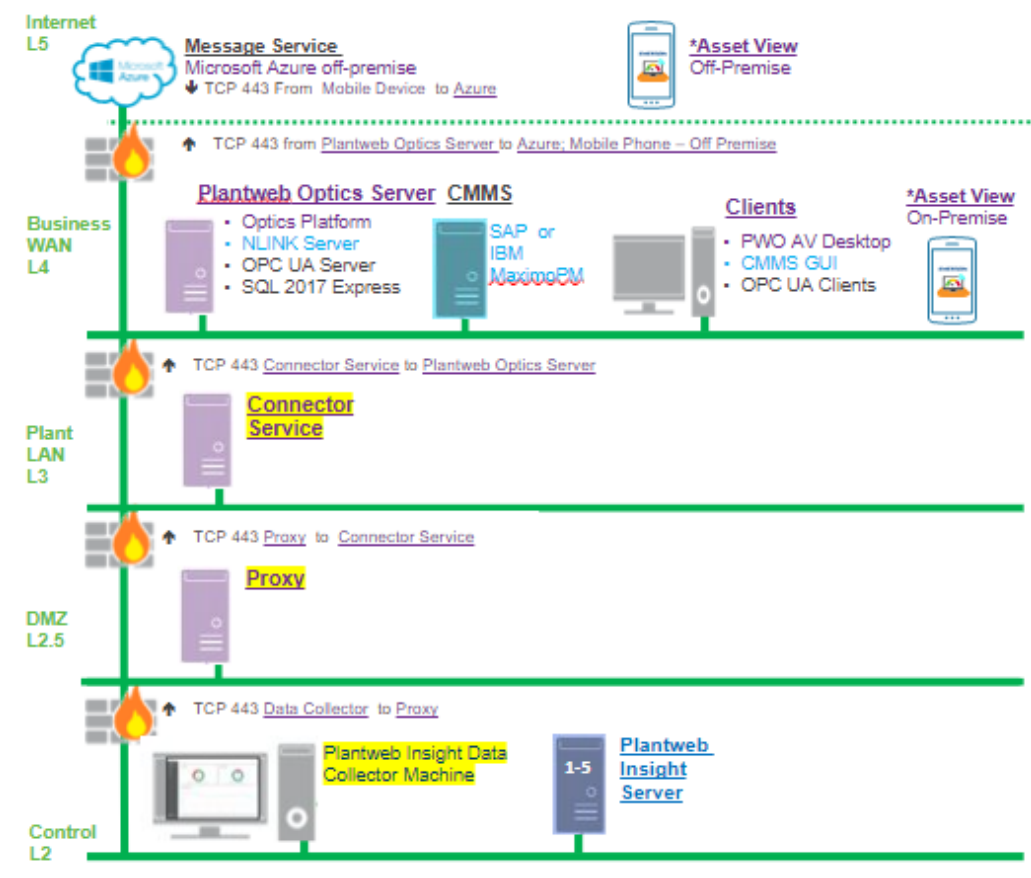
the Plantweb Insight Data Collector with multiple Data Collectors as a level-3 or level-4 deployment.

Understanding the estimated system load along with the level of security you want to achieve helps you determine the number of network layers between the data source and Plantweb Optics. It also dictates the components you need and if you need to install the Connector Service on a different server and utilize a proxy server. The following list describes deployment considerations useful when deciding which deployment scenario works best for your environment.

- If Plantweb Optics and Plantweb Insight are on different networks, or are separated by a firewall, you must deploy the Plantweb Insight Data Collector and the Connector Service on different servers.
- 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 a deployment of the Plantweb Insight ASI components with a Plantweb Insight Data Collector sending data to Plantweb Optics through a proxy and a single Connector Service:

**Figure 6-8: Plantweb Insight Data Collector deployment scenario**



## 6.9.2 Register the Plantweb Insight ASI

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

---

### Note

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

---

### Prerequisites

- Plantweb Optics is installed on the computer designated as the Plantweb Optics server.
- A48INSIGHT-DS0.Plantweb\_Insight\_ASI.1.6.X.X.zip file.

### Procedure

1. Extract the A48INSIGHT-DS0.Plantweb\_Insight\_ASI.1.6.X.X.zip file.

---

### 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. On the **Setup** screen, select **Register Plantweb Insight ASI (on Plantweb Optics Server)**.
4. Read and accept the license agreement. If you accept, click **Next**.
5. In the **AMS Plantweb Insight ASI Server Configuration** window, enter the server name or IP address of the server where the ASI is installed.
6. Click **Next**.
7. Click **Finish** to complete the registration process.

### Postrequisites

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

## 6.9.3 Install the Plantweb Insight Data Collector

### Prerequisites

- Ensure Plantweb Optics is already installed on the computer you designate as the Plantweb Optics server.
- A48INSIGHT-DS0.Plantweb\_Insight\_ASI.1.6.X.X.zip file.
- The certificate from the Proxy or the Connector Service to which this Data Collector sends data, is installed. Which server the Data Collector communicates directly with determines which certificate you must install. See [Install a Proxy certificate](#) or [Install a Connector Service certificate](#).

---

### Note

You must install the Data Collector on a server that resides on the same network level as Plantweb Insight.

---

- Know the PC name or IP address where the Connector Service is installed.
- If deploying the Proxy, know the PC name or IP address where the Proxy is installed.
- The Plantweb Insight ASI registration process has been completed on the Plantweb Optics server.

#### Procedure

1. Extract the A48OPTICS\_Plantweb\_Insight-0.1.6.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 **PlantwebInsightDataCollector\_Setup.exe** and select **Run as administrator**.
3. Click **Next**.
4. Read the license agreement. If you accept, click **Next**.
5. Select the Data Collector and then click **Next**.
6. Verify the installation destination folder and then click **Next**.
7. Enter the PC name/IP address and port number where the Connector Service is installed. Port 443 is the default port.
8. Click **Next**.
9. Select **Install Now** to install with default options.
10. On the **Installation is successful** page, click **Restart Now**. After the system restarts, the Plantweb Insight Data Collector installation is complete.

#### Postrequisites

After installation, the Plantweb Insight 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, you must install the security certificate of each Plantweb Insight asset source on the Data Collector that the asset source communicates with. Refer to [Certificate installations](#).

## 6.9.4 Add an asset source to the Plantweb Insight Data Collector

#### Prerequisites

- The Connector Service is installed.
- The Proxy (if applicable) is installed.
- The Connector Service and (if applicable) Proxy security certificates are installed on the appropriate servers.
- The Plantweb Insight security certificate is installed on the Data Collector server where the asset source is added.
- An API Key is configured in the Plantweb Insight system.

## Procedure

1. Launch the Plantweb Insight Data Collector user interface.
  - a) Launch Google Chrome or Microsoft Edge Chromium.
  - b) Navigate to `https://<Data_Collector_PC_Name>/PlantwebInsightDataCollector` 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>/PlantwebInsightDataCollector`.

Replace `<Data_Collector_PC_Name>` with the name of the PC where the Data Collector is installed and `<PortNumber>` with the port the Data Collector is bound to.
  - c) From the **Insight Data Collector** → **Log In** page, enter your Access Key credentials and then click **Submit**. If an access key has not been created, you are prompted to create one. The access key is case-sensitive.

---

### Note

Access keys are bound only to the individual Proxy or Data Collector the access key is created on. Access keys are not synchronized across services.

---

2. From the Asset Sources page, click the + icon to add a new asset source from the **Add Asset Source** menu.
3. In the **Site** drop-down field, select the site you want associated with the new asset source.
4. In the **Display Name** field, enter a name for the new asset source. This is a user-defined identifier for the asset source. This name is displayed in Asset Explorer and Asset View in Plantweb Optics.

---

### Note

If you want to change the name of an asset after it has been created, use the **Update** feature in the user interface to update the hierarchy.

---

### Note

Plantweb Optics supports asset source names and asset names that are up to 64-characters long. Asset names that are longer than 64 characters are truncated.

---

5. In the **Host** field, enter the system name or IP address of the Plantweb Insight system.
6. Enter the **Port Number** to use with the Plantweb Insight Data Collector. This is a configurable field. The default port is 443.
7. In the **App Name** field, enter the name of the API Key that exists in Plantweb Insight.
8. Enter the **API Key** to use for Plantweb Insight.
9. You can choose to enter a description of the asset source in the **Description** field. The description is displayed in Asset Explorer and Asset View.
10. Click **Add** to begin sending asset source data to Plantweb Optics.

A dialog displays showing the status of the rebuild and when it the add asset source process completes.

A Plantweb Insight Data Collector can support multiple asset sources. Repeat this procedure to add additional asset sources.



# 7 Post installation and certificate installation procedures

---

## Note

Installing and configuring Active Directory is optional. If you intend to add an identity provider or change an identity provider's settings in the Plantweb Optics, you need to configure Active Directory in the Plantweb Optics System Settings.

---

To complete your Plantweb Optics installation, complete the following post-installation configuration changes and installations.

- Configure the Active Directory for Plantweb Optics.
- Configure Plantweb Optics OpenID Connect (OIDC) settings.
- Install certificates that enable communication between the Data Collector, Proxy (if one is installed), the Connector Service, and Plantweb Optics.
- Configure how emails are sent in Plantweb Optics.

## 7.1 Configure Active Directory for Plantweb Optics

### Prerequisites

Install Windows 2016 or a later version to have access to Server Manager.

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.
7. Click **Server Application** and then click **Next**. The **Server application** screen displays.
8. 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.
9. 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 each URI.

---

**Note**

Copy the <CALLBACK> into the Notepad text editor for use during the [Configure Plantweb Optics OIDC settings](#) procedure.

---

- 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`
10. 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.
  11. Copy the new secret into Notepad editor for use during the [Configure Plantweb Optics](#) [Configure Plantweb Optics OIDC settings](#) procedure.
  12. Click **Next** to accept defaults, and then click **Close**.
  13. The **Application Groups** screen displays showing the new Application Group.

## 7.2 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 into Plantweb Optics and open **System Manager**.
2. Click **Identity Provider** in the navigation pane.
3. Click **New** on the Home ribbon.
4. On the right side of the Identity Providers page enter the following OpenID values in the **Details** pane:
  - a) **Authority:** Use this format for this field, `https://<YOUR ACTIVE DIRECTORY SERVER>/adfs/`.
  - b) **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.
  - c) **Display Name:** User defined. For example, `ADFS`.

- d) **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](#).
  - 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) **Claim:** Enter `http://schemas.xmlsoap.org/we/2005/05/identify/claims/upn` in the **Claim** field.
  - g) If the provider requires a client secret, check the **Enable Client Secret** check box and enter the secret in the **Client Secret** field. Enter the displayed result that you pasted into Notepad during the Configure Active Directory procedure. See [Configure Active Directory for Plantweb Optics](#).
  - h) Enter the secret **Client Secret:**
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.
  7. Open System Manager and then click **Users** to open the list of users and select the one you want to be linked with Active Directory.
  8. Click the **Edit** icon next to the user's name in the Details pane on the right side of the screen.
  9. In the **Logins** field, click **+ Add**.
  10. Select the OpenID Connect Provider and then enter a **Claim Value**, enter the user's email address (the credentials used by the user to log in to Active Directory), and then click the **Save** icon.
  11. Sign out of Plantweb Optics.
  12. Log back in to Plantweb Optics by clicking a button under **External Account**. The External Account button displays the name of the OpenID Connect Provider that was entered earlier. The Plantweb Optics sign in screen displays. The configuration is complete.

## 7.3 Certificate installations

You import SSL certificates after you install all web services (such as Plantweb Optics Web Service, Connector Service, Proxies, Data Collectors, and services) on the system. If you want to manually export and install certificates, 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, you must install the following certificates on the listed servers:

**Table 7-1: 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

When using a 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.

The following topics describe how to install the Plantweb Optics, Connector Service, or Proxy certificates.

- [Install Plantweb Optics certificates](#) on a Connector Service PC, or on a client PC.
- [Install a Connector Service certificate](#) on the Proxy or the Data Collector.
- [Install a Proxy certificate](#) on the Proxy or the Data Collector server.

## 7.3.1 Install Plantweb Optics certificates

Perform this procedure to install the Plantweb Optics certificates on a 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 Plantweb Optics applications by web browser, or on any server that has web services that communicate with the Plantweb Optics Web Service.

**Procedure**

1. Launch Microsoft Edge Chromium.
2. Enter **https://<Optics\_Server\_Name>/Assetexplorer**.
3. Click **Continue to this website**.
4. If necessary, click **Continue to this website** again.
5. The **Plantweb Optics Login** screen displays. A **certificate error** displays in the URL path of the browser.
6. Click **Certificate error** in the URL path of the browser.

7. In the Untrusted Certificate dialog, click **View certificates**.
8. Click **Install certificate...** to open the **Certificate Import Wizard**.
9. Select **Local Machine** and then click **Next**.

---

**Note**

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

---

10. Click **Place all certificates in the following store** and then click **Browse**.
11. Select **Trusted Root Certification Authorities**, click **OK**, and then click **Finish**.

If installing certificates on Windows Server 2008 R2, continue the remaining steps listed in [Install certificates on Windows Server 2008 R2](#).

## 7.3.2 Install a Connector Service certificate

Perform this procedure to install the Connector Service certificate on the Proxy or the Data Collector server.

### Procedure

1. Launch Microsoft Edge Chromium.
2. Enter **https://<Connector\_Service\_Server\_Name>/connectorservice**.

---

**Note**

If the Connector Service is co-deployed on the Plantweb Optics server, the certificate that shows is the Plantweb Optics v1.6 certificate and not the Connector Service certificate.

---

3. Click **Continue to this website**.
4. If necessary, click **Continue to this website** again. A **certificate error** displays in the URL path of the browser.
5. Click **Certificate error** in the URL path of the browser.
6. Click **View certificates**.
7. Click **Install certificate...** to open the **Certificate Import Wizard**.
8. Select **Local Machine** and then click **Next**.

---

**Note**

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

---

9. Click **Place all certificates in the following store** and then click **Browse**.
10. Select **Trusted Root Certification Authorities**. Click **OK** and click **Finish**.

If installing certificates on Windows Server 2008 R2, continue the remaining steps listed in [Install certificates on Windows Server 2008 R2](#).

## 7.3.3 Install a Proxy certificate

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

### Procedure

1. Launch Microsoft Edge Chromium.
2. Enter **https://<Proxy\_Server\_Name>/Proxy**.
3. Click **Continue** to this website.
4. If necessary, click **Continue** to this website again. A **certificate error** displays in the URL path of the browser.
5. Click **Certificate error** in the URL path of the browser.
6. Click **View certificates**.
7. Click **Install certificate...** to open the **Certificate Import Wizard**.
8. Select **Local Machine** and then click **Next**.

---

#### Note

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

---

9. Click **Place all certificates in the following store** and then click **Browse**.
10. Select **Trusted Root Certification Authorities**. Click **OK** and then click **Finish**.

If installing certificates on Windows Server 2008 R2, continue the remaining steps listed in [Install certificates on Windows Server 2008 R2](#).

## 7.3.4 Install certificates on Windows Server 2008 R2

Use the following procedure to install certificates on a Windows Server 2008 R2 operating system. This method of installing certificates uses the Microsoft Management Console (MMC).

### Procedure

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

1. Complete [Certificate installations](#) to install any certificates required on your Windows Server machine.

---

#### Note

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

---

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

2. On your Windows Server 2008 R2 machine, export the certificates installed in step 1 of this procedure to the same Windows Server 2008 R2 machine. You can refer to the [Export a security certificate](#) procedure for information on how to export a security certificate.

#### 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 appears.
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 then click **Next**.
  7. Ensure **Local computer** is selected and then 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 that you 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 then click **Next**.
  16. Click **Finish**.
  17. Repeat steps 10-16 for each certificate that you exported in step 2.
  18. After you have finished importing all certificates, click **File** → **Save changes**.

### 7.3.5 Export a security certificate

This procedure covers manually exporting an SSL certificate and is an alternative method to [Certificate installations](#). 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, 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 [Install a security certificate](#). Or, if you are installing certificates on Windows Server 2008 R2, return to [Install certificates on Windows Server 2008 R2](#)

## 7.3.6 Install 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**.

## 7.4 Configure how emails are sent in 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:\PlantwebOptics\Tools\SMTP and open a command prompt with elevated privileges.

**Table 7-2: SMTP Configuration Utility Commands**

Operation	Command
Manually set the username and password used to authenticate with the SMTP server	<code>Emerson.PW0.V1.EmailSettingsConfig.exe cred -u "YOUR_USERNAME" -p "YOUR_PASSWORD"</code>
Enable (or disable) the use of default credentials instead of manually setting username and password	<code>Emerson.PW0.V1.EmailSettingsConfig.exe usedefaultcreds</code> <code>Emerson.PW0.V1.EmailSettingsConfig.exe usedefaultcreds --disable</code>
Set the email address and header used when sending an email	<code>Emerson.PW0.V1.EmailSettingsConfig.exe from -e "donotreply@emerson.com" -h "Plantweb Optics"</code>



**Table 7-2: SMTP Configuration Utility Commands (continued)**

Operation	Command
Configure the connection to the SMTP server	<pre>Emerson.PW0.V1.EmailSettingsConfig.exe connection -h "smtp.sendgrid.net" -p 25</pre> <pre>Emerson.PW0.V1.EmailSettingsConfig.exe connection -h "smtp.sendgrid.net" -p 587 -- usessl</pre> <hr/> <p><b>Note</b> There may be a limitation of 30 emails per minute on secured port 587.</p> <hr/> <pre>Emerson.PW0.V1.EmailSettingsConfig.exe connection -h "smtp.sendgrid.net" -p 25 --spn "YOUR_SPN" --cdn "YOUR_CDN"</pre>
Switch between using the SMTP and HTTP interfaces to deliver email	<pre>Emerson.PW0.V1.EmailSettingsConfig.exe usesmtp</pre> <pre>Emerson.PW0.V1.EmailSettingsConfig.exe usesmtp --disable</pre>
Display current settings	<pre>Emerson.PW0.V1.EmailSettingsConfig.exe getsettings</pre>
Restore all settings to defaults	<pre>Emerson.PW0.V1.EmailSettingsConfig.exe reset</pre>
Configure mail delivery settings See the table below, <b>Delivery Methods</b> , for an explanation of the delivery methods and formats	<pre>Emerson.PW0.V1.EmailSettingsConfig.exe delivery -m "network" -f "sevenbit"</pre> <pre>Emerson.PW0.V1.EmailSettingsConfig.exe delivery -m "iis" -f "international"</pre> <pre>Emerson.PW0.V1.EmailSettingsConfig.exe delivery -m "custom" -f "international" -d "C:\MailDirectory"</pre>
Generate a test email	<pre>Emerson.PW0.V1.EmailSettingsConfig.exe test -e "&lt;some email address&gt;"</pre>
Using anonymous authentication when sending an email	<pre>Emerson.PW0.V1.EmailSettingsConfig.exe useanon</pre> <pre>Emerson.PW0.V1.EmailSettingsConfig.exe useanon -disable</pre> <hr/> <p><b>Note</b> When you enable this option, it overrides other configured authentication settings.</p>

**Table 7-3: Delivery Methods**

<b>Delivery Method</b>	<b>Description</b>
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 7-4: Delivery Formats**

<b>Delivery Format</b>	<b>Description</b>
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.

## 8 Mobile installation procedures

To use the Plantweb Optics Mobile App or the Plantweb Optics Augmented Reality (AR) Mobile App, you need a mobile join key associated with your user account issued by a Plantweb Optics administrator.

You need to issue a mobile join key for each user that will access either of the two mobile apps. You can create, issue, and monitor join keys in the System Manager application. The join key 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 a direct (on-premises) connection to Plantweb Optics through your plant network Wi-Fi.

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 an internet connection or an on-premises mobile option. The on-premises mobile option provides a faster and more secure access to messages when inside your plant. You can use the benefits that each mobile join key offers depending on your physical location.

When you enter or scan a join key, the application identifies the type of join key, a Cloud (Azure/Default) or Local (On-Premise) key.

### 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 join key 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 (health score less than 80) or the number of messages for each site.

## 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.

The first time you open the Plantweb Optics mobile app, you are prompted for a mobile join key. A Plantweb Optics administrator generates a mobile join key that is associated with your username and is unique to you and the app. The join key is valid until it is disabled by the administrator or the user.

---

### Note

Different mobile devices require separate join keys. Different sites also require different join keys.

---

### Prerequisites

- Log in to Plantweb Optics with Administrator privileges and have **Can Manage Users** permission.

- Launch the System Manager application.
- Verify that the user who needs a new join key is created.
- Create a join key (Local or Cloud) for the user who wants to access Plantweb Optics from a mobile device. Use the **System Manager** → **Join Keys** page to create a join key for the user.

You can use the following procedure to download and install Plantweb Optics mobile app to 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** to search for the Plantweb Optics mobile app.
3. Choose to install, and accept permissions.
4. From the System Manager application, click the **Join Keys** tab and then select the join key ID from the ID list pane. The join key ID and the QR code appear in the details pane on the right.
5. From your mobile device, you can manually enter the join key ID or click the scan icon and scan the QR code displayed on the **System Manager** → **Join Keys** details pane. Once you enter the join key, the app recognizes the its type. Click **OK**.

---

### Note

You can increase the size of the QR code to make it easier to scan.

---

6. Enter your Plantweb Optics username and password.
7. Answering the remaining questions so you can identify this site within your mobile app:
  - a) Enter a site name.
  - b) Enter a site address.
  - c) Enter a site description.
8. Choose the push message notification option for your key type:
  - a) Cloud—define the frequency of notifications in the **Fetch and Notification** field.
  - b) Local—set push notification to *ON* or *OFF*.
9. Click the check-mark icon in the upper right to authenticate your mobile app with Plantweb Optics.

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.

## 8.2 Install the Plantweb Optics AR Mobile app

### Prerequisites

- The Plantweb Optics software must be registered in the Augmented Reality app.
- Log in to Plantweb Optics with Administrator privileges and been assigned *Can Manage Users* permission.
- Launch the System Manager application.
- Verify that the user who needs a new Plantweb Optics Augmented Reality (AR) join key exists.
- Create an Augmented Reality join key for the user who wants to access Plantweb Optics AR from a mobile device. Use the **System Manager** → **Join Keys** page to create the join key for the user.

You can use the following procedure to download and install the Plantweb Optics AR mobile app to 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 Augmented Reality** to search for the Plantweb Optics Augmented Reality mobile app.
3. Choose to install, and accept permissions.
4. From the System Manager application, do the following.
  - a) Click the **Join Keys** tab.
  - b) Select the AR join key ID from the ID list pane that you want to issue to the user.  
Details of the AR join key ID and the QR code appear in the pane on the right.
5. On your mobile device, tap the Plantweb Optics AR app to open the mobile app.
6. On your mobile device perform the following steps to claim your Augmented Reality join key.
  - a) Manually enter the join key ID or click the scan icon and scan the QR code that is displayed in the **System Manager** → **Join Keys** details pane.  
You can increase the size of the QR code to make it easier to scan.
  - b) Click **Login**.
7. Enter your Plantweb Optics username and password.

## 8.3 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

- 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.
- Log in to Plantweb Optics with Administrator privileges and have **Can Manage Users** permission.
- Launch the System Manager application.
- Verify that the user who needs a new join key is created.
- Create a join key for the user who wants to access Plantweb Optics from a mobile device. Use the **System Manager** → **Join Keys** page to create a join key for the user.

### Procedure

1. On your mobile device, open **Plantweb Optics**.  
Perform the following steps to download **Plantweb Optics** if it is not currently installed on your mobile device.
  - a) On your mobile device, open the Google Play™ Store or the Apple® AppStore™.
  - b) In the search bar, type **Plantweb Optics** to search for the Plantweb Optics mobile app.
  - c) Choose to install, and accept permissions.
2. On your mobile device, tap the Plantweb Optics mobile app icon and then click **Local**.
3. From the System Manager application, click the **Join Keys** tab and then select the join key ID from the ID list pane. The join key ID and the QR code appear in the details pane on the right.
4. Choose **Local** for On-premise join keys. From your mobile device, on the **Add Site** screen, you can manually enter the join key ID or click the scan icon and scan the QR code displayed on the **System Manager** → **Join Keys** details pane.
5. Select **Advanced**.
  - a) Toggle to specify the Server Name or its IP Address, or specify the Service Path.
  - b) Toggle off for Server Name/IP Address—enter the server name or its IP address in the **Enter Server Name** field.
  - c) Toggle on for the Service Path:
    - Enter Plantweb Optics Service Path (path to server) using the format: *IP address/onprem/assetview*.

- Enter the Mobile Service Path (path to services) using this format: *<IP address>/onprem/mobile*.

6. Tap **Login**.

7. Perform the following steps if this is the first time you are installing the mobile app.

- a) Enter your Plantweb Optics username and password.
- b) Answering the remaining questions so you can identify this site within your mobile app:
  - Enter a site name.
  - Enter a site address.
  - Enter a site description.
  - Define the frequency (in hours) of push notifications in the **Fetch and Notification** field.
- c) Click the check-mark icon in the upper right to authenticate your mobile app with Plantweb Optics.

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.





## 9 Uninstall Plantweb Optics, components, and Data Collectors

Uninstall Plantweb Optics and its components in the following order.

1. AMS Device Manager Launcher, if previous versions exist
2. AMS Machinery Manager Launcher, if previous versions exist
3. Plantweb Optics OPC UA server
4. Connector Service
5. Proxy
6. Data Collectors
7. ASI registration components installed on the Plantweb Optics server
8. Plantweb Optics
9. Plantweb Optics Historian

---

### Note

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

---

### Procedure

1. From the Control Panel, click Programs and Features or search for Add or Remove Programs.
2. Select the component that you want to uninstall and then click **Uninstall**.
3. A confirmation dialog displays. Click **Uninstall**.
4. From the component's installation wizard, click **Uninstall**. Follow any additional prompts.
5. After the component is successfully uninstalled, the screen updates and prompts you to restart the computer. Click **Restart now** or in some cases, **Finish** to restart the server.



## 10 Upgrade from a previous version

When upgrading a Plantweb Optics system, the system can include Plantweb Optics, the Connector Service, a Proxy, and one or more configured Data Collectors. Emerson recommends you contact your Emerson Technical Support representative for assistance with the upgrade.

The supported upgrade paths for Plantweb Optics is shown in the following table.

Plantweb Optics Version	Upgrade to		
	Plantweb Optics 1.5	Plantweb Optics 1.5.1	Plantweb Optics 1.6
Plantweb Optics 1.5 (general release)	N/A	Supported	Supported
Plantweb Optics 1.5.1	Not Supported	N/A	Supported



# 11 Launch Plantweb Optics applications

All user interactions in the software happen through its applications, which can be launched from a web browser. Also, on the server, you can launch the applications through a desktop shortcut.

## Prerequisites

- If Enhanced Security Configuration is enabled in the Chromium base Edge browser, add the Plantweb Optics server URL to the list of trusted sites. See the *Launching Plantweb Optics utilities* table in the [Troubleshooting](#) chapter for instructions.

### Note

The Internet Explorer browser is no longer supported.

- 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 [Certificate installation checklist](#).

## Procedure

1. Open a supported web browser. (Google Chrome or Microsoft Edge Chromium)
2. In the web browser address field, enter the URL for the application you want to launch. Refer to the following table.

Launch	From this URL	To perform the following
<b>System Manager</b>	https://<OpticsServerName>/SystemManager or if a port is assigned to the web server then you enter the following URL: https://<OpticsServerName>:<PortNumber>/SystemManager	<ul style="list-style-type: none"> <li>• Set up users</li> <li>• Control and monitor access to the software.</li> <li>• View events generated in the software.</li> </ul>
<b>Asset Explorer</b>	https://<OpticsServerName>/AssetExplorer or if a port is assigned to the web server then you enter the following URL: https://<OpticsServerName>:<PortNumber>/AssetExplorer	<ul style="list-style-type: none"> <li>• Set up your site</li> <li>• Configure assets for access in asset view</li> </ul>
<b>Asset View</b>	https://<OpticsServerName>/AssetView or if a port is assigned to the web server then you enter the following URL: https://<OpticsServerName>:<PortNumber>/AssetView	<ul style="list-style-type: none"> <li>• Manage assets with a persona-based view</li> <li>• See the asset overall dashboard, automatic health scores, trends, messages, and asset hierarchy.</li> </ul>

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.

For example, Asset Explorer application from the server named Optics Server 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 a server name or the IP address to start utilities. You select which option during the Plantweb Optics installation's configuration:

- When selecting the **Use Server Name** option in the Server and Port Binding Configuration screen, you can only start utilities using the server name.
- When selecting the **Use IP Address** option, you can only start utilities with the server IP address.

- 
3. If this is the first time you have launched an application from a client computer, do not log in when prompted.

Install the Plantweb Optics certificate before logging in for the first time. See [Certificate installations](#).

4. Enter your credentials and log in.

On first login, use the following defaults:

- **Username:** admin
- **Password:** Emerson#123

---

**Note**


After the initial login, you must change the administration password. Your new password must include:

- a minimum of 10 characters.
- at least one special character.
- at least one uppercase letter.
- a combination of alpha and numeric characters.

As an administrator, you later can change the password complexity requirements using the System Manager application.

---

**Postrequisites**

For information on configuring your Plantweb Optics installation, refer to the Plantweb Optics Online Help. The Online Help can be launched from any Plantweb Optics application by clicking the Help  icon.

## 11.1 Data source asset screens (Launch in Context)

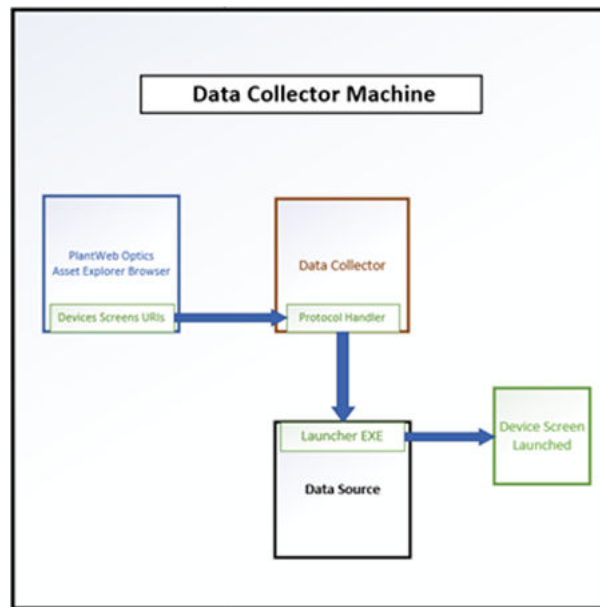
The Launch In Context feature permits the Plantweb Optics administrators to display the configured data source assets screens using the Plantweb Optics Asset Explorer.

These software elements cooperate to display the screens:

- Asset device context uniform resource identifiers (URIs)
- Protocol handler software, which is co-deployed with the data collector
- An asset source executable application to display the configured screens

The following figure shows how the Launch in Context elements work to display the screens.

**Figure 11-1: Launch in Context elements**



### Screen uniform resource identifiers

Plantweb Optics creates and attaches the device screen URIs to each device in the data collector while you build the physical hierarchy.

Some examples include:

Device Manager URI for FF 3051-15 asset Overview screen–devmgr : //localhost/?  
protocol=FF&SerialNumber=001151305114DEV000000015\_3051\_1&Screen=Overview

Device Manager URI for HART PEGW-1 asset Diagnostics screen–devmgr : //  
localhost/?  
protocol=HART&SerialNumber=793364&ManufacturerId=38&DeviceType=9806  
&DeviceRevision=5&ProtocolRevision=7&Screen=Diagnostics

### Data Collector Protocol Handler

The protocol handler is co-deployed with the data collector on the same server. The handler is installed during the data collector installation. The installer creates a sub-folder under the data collector folder to store the ProtocolHandler application and its dependencies. As part of the data collector installation, the installation software determines the file path to the protocol handler software and stores the starting command in the (HKEY\_CLASSES\_ROOT\devmgr\shell\open\command) registry key, a part of the HKEY\_CLASSES\_ROOT registry hive.

For the AMS Device Manager Data Collector, your configuration would look like:

```
ProtocolHandler folder filepath-C:\PlantwebOptics\site  
\AMSDeviceManagerDataCollector\ProtocolHandler
```

```
Protocol Handler software start command-C:\PlantwebOptics\site  
\AMSDeviceManagerDataCollector\ProtocolHandler  
\DeviceManagerProtocolHandler.exe" "%1"
```

#### **Asset screens Launcher Software**

This might be the actual data source executable or a separate executable part of the data source. For Device Manager, the assets screens software is named AMSLauncher.exe.

Once you have installed the data collector and built your asset hierarchy in Plantweb Optics, you can select an asset and display any pre-configured data source asset screens.

## 11.2 Display data source asset screen using Asset Explorer

To use the Launch in Context feature in Asset Explorer, follow these steps.

#### **Prerequisites**

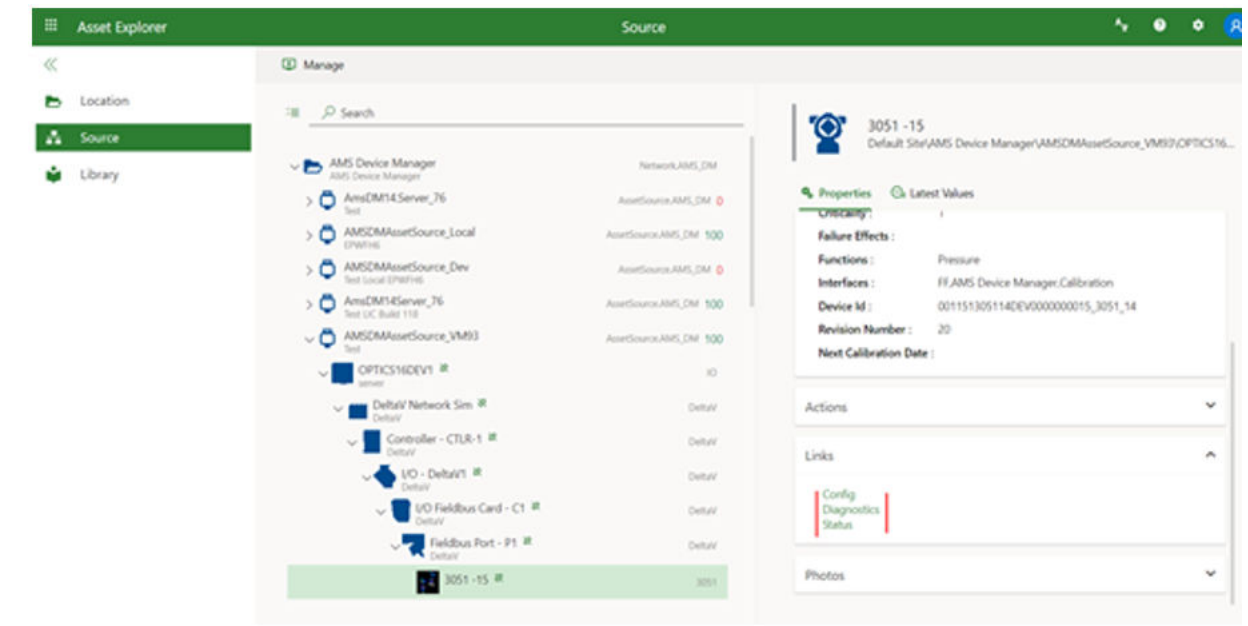
- Someone installed the data collector using the instructions found in this document.
- You have a Plantweb Optics account that permits you to change items for the asset device. For example, to display the AMS Device Manager screens, you need a Device Manager account with Change permission.
- You used the Asset Explorer to build the physical hierarchy of assets. This creates the URIs to start the display of the asset data source screens.

#### **Procedure**

1. Start the Plantweb Optics browser and go to the **Source** application.
2. Select the asset for which you intend to display the asset source screens.
3. Once you select an asset, scroll to the **Links** section of the asset **Properties** display.
4. Expand the **Links** section (highlighted in red), as shown in the following figure.

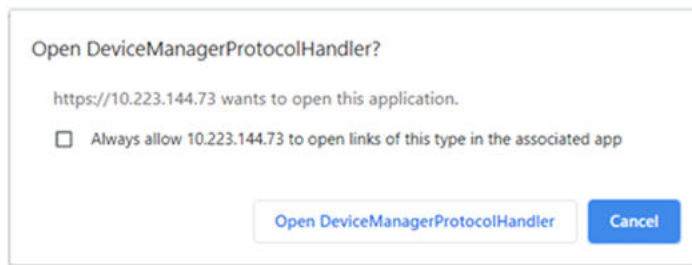


Figure 11-2: Links section highlighted for a selected asset



5. Select the link to display the protocol handler dialog box. The following figure illustrates the dialog box for the Device Manager protocol handler.

Figure 11-3: Example Device Manager Protocol Handler dialog box



6. Click the **Open data collector ProtocolHandler** button (see previous figure) to display the data source asset screen.

### Need help?

If there is an issue launching in context, please look at the data collector protocol handler log files.



# 12 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:\PlantwebOptics\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 12-1: Databases**

Module	Database
Plantweb Optics	AdminDb
	CMMSDb
	EventDb
	FrameworkDb
	ImageDb
	MessageDb
	MobileServicesDb
	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.

## 12.1 Backup 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 [Automatic backup for Tier-1 installations](#) for more information.

A Tier-2 installation requires maintenance by a database administrator. Database administrators should perform backups. Contact your database administrator or IT department for proper backup procedures. 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.

## 12.2 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:\PlantwebOptics\EMERSONCSI\DATA\Backups\PW0. 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.

---

# 13 Troubleshooting

## Installation

Error	Background	Solution
The required port to install Plantweb Optics is used by another application	Port 80 and port 443 (default) are required and used by Plantweb Optics. If these ports are not available or used by another application, open the ports or redirect the website using these ports.	<ol style="list-style-type: none"> <li>1. Launch IIS Manager.</li> <li>2. On the Connections pane, expand <b>PC name</b> → <b>Sites</b>.</li> <li>3. Click <b>Default Web Site</b>.</li> <li>4. On the Actions pane, click <b>Bindings</b>.</li> <li>5. On the Site Bindings page, select port 80 or port 443 and click <b>Edit</b>.</li> <li>6. On the Edit Site Binding page, enter another port number, and click <b>OK</b>.</li> </ol>
Plantweb Optics installation failure	Plantweb Optics installation may fail for several reasons.	See the installation logs for additional information on the cause of the installation failure. Installation logs are in <code>C:\Users\&lt;username&gt;\AppData\Roaming\Emerson\_ADMLogs\&lt;random GUID folder&gt;</code> .
		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.
		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.
		Use the same server setting, either IP address or server name as the Plantweb Optics configuration, when installing or upgrading components and ASIs. For example, when you choose the <b>Use Server Name</b> 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 and ASIs may cause the installation to fail and you will need to uninstall and reinstall the software to configure the same server setting.
		Ensure the Windows Update service is running.
		<p><b>Note</b></p> <p>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.</p>

Error	Background	Solution
		<p>When the installer has more than one .exe included, always run <b>install.exe</b> rather than setup.exe to install Plantweb Optics and its components.</p> <p>Running <b>install.exe</b> checks that the system has the necessary prerequisite software for the installation to continue.</p> <p>Some installers only have one .exe included. Always refer to the instructions for your installation.</p> <hr/> <p>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 must be running on the database server.</p> <p><b>To enable TCP/IP:</b></p> <ol style="list-style-type: none"> <li>1. Launch SQL Server Configuration Manager.</li> <li>2. On the left pane, expand the <b>SQL Server Network Configuration</b> node.</li> <li>3. Select the <b>Protocols for EmersonCSI</b>.</li> <li>4. On the right pane, right-click <b>TCP/IP</b> and select <b>Enable</b>.</li> </ol> <p><b>To enable the services:</b></p> <ol style="list-style-type: none"> <li>1. Launch SQL Server Configuration Manager.</li> <li>2. On the left pane, select <b>SQL Server Services</b>.</li> <li>3. On the right pane, right-click <b>SQL Server (EMERSONCSI)</b> and select <b>Start</b>.</li> <li>4. Right-click <b>SQL Server Browser</b> and select <b>Start</b>.</li> </ol> <hr/> <p>Plantweb Optics installations may fail if there are database files from a previous installation in the C:\PlantwebOptics\EmersonCSI\Data folder.</p> <p>See Knowledge Base Article <b>NK-1600-0344</b> for a list of database files to be removed.</p>

Error	Background	Solution
Error when installing SQL Server	<p><b>Note</b> During default installation, Microsoft SQL Server 2019 Express is automatically installed and configured for Plantweb Optics. There is no need to install SQL Server 2019 if there is no SQL Server currently installed on the Plantweb Optics server.</p> <p>If you will manually install SQL Server 2019, 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.</p>	<ol style="list-style-type: none"> <li>1. Launch Control Panel.</li> <li>2. Go to <b>Administrative Tools</b> → <b>Local Security Policy</b>.</li> <li>3. Navigate to <b>Local Policies</b> → <b>User Rights Assignment</b>.</li> <li>4. Double-click the <b>Back up files and directories</b> policy.</li> <li>5. Check to see if the user account running the SQL Server setup is listed. If it is not, click <b>Add User or Group</b> to add it, and click <b>OK</b> to close the dialogs.</li> <li>6. Double-click the <b>Debug programs</b> policy.</li> <li>7. Check to see if the user account running the SQL Server setup is listed. If it is not, click <b>Add User or Group</b> to add it, and click <b>OK</b> to close the dialogs.</li> <li>8. Double-click the <b>Manage auditing and security log</b> policy.</li> <li>9. Check to see if the user account running the SQL Server setup is listed. If it is not, click <b>Add User or Group</b> to add it, and click <b>OK</b> to close the dialogs.</li> </ol>
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.
Encountered an unsuccessful launching of a Data Collector.	The Data Collector may not be properly communicating with the Connector Service server or the Plantweb Optics Server.	<p>For a Tier 2 installation verify that:</p> <ol style="list-style-type: none"> <li>1. The proper certificates are installed and trusted between Plantweb Optics, the Connector Service, (the Proxy, if applicable), and the Data Collector.</li> <li>2. If the certificates are installed and trusted, view the Data Collector log file at C:\PlantwebOptics\site\logs, search for the keyword, <b>Error</b>, and then contact Technical Support.</li> <li>3. Under the guidance of Technical Support, reset the IIS services on the Connector Server, if necessary.</li> </ol>

Error	Background	Solution
Encountered a 505.5 error when launching a Data Collector	This error can occur if the Data Collector did not launch properly.	<p>Perform the following steps to resolve the issue.</p> <ol style="list-style-type: none"> <li>1. Check if the certificate of the Connector Service is properly imported at the Data Collector machine.</li> <li>2. Ensure communication between the Data Collector and the Connector Service or the Proxy by attempting to ping the Connector Service (or Proxy) using its IP address. Ensure that the IP Address and the Server Name is added to the server <code>host</code> file.</li> <li>3. Using a Chrome browser at the Data Collector machine, try to launch the Connector Service site or the Proxy site.</li> <li>4. Under the guidance of Technical Support, restart the IIS App pools of the Data Collector Server, if necessary.</li> </ol>

### 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.	<ol style="list-style-type: none"> <li>1. In Windows Services, stop the <b>AMS Machinery Manager IO Service</b>.</li> <li>2. In AMS Machinery Manager, do the following: <ul style="list-style-type: none"> <li>• Select <b>Tools</b> and launch <b>RBM Network Administration (RBMadmin)</b>.</li> <li>• In RBMadmin, click <b>File</b> → <b>Preferences</b>.</li> <li>• If the <b>Limit To</b> 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.</li> </ul> </li> <li>3. In Windows Services, start the <b>AMS Machinery Manager IO Service</b>.</li> </ol>
	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.	<p>On the computer where the AMS Machinery Manager ASI Service is installed, do the following:</p> <ul style="list-style-type: none"> <li>• In Windows Services, right-click the <b>AMS Machinery Manager ASI IO Service</b> and select <b>Properties</b>.</li> <li>• On the General tab, select <b>Automatic</b> from the Startup type menu.</li> <li>• On the Recovery tab, select <b>Restart the Service</b> from the First failure and Second failure drop-down fields.</li> <li>• Click <b>Apply</b>.</li> <li>• Click <b>OK</b>.</li> </ul>



Error	Background	Solution
	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 application will not be able to connect to AMS Machinery Manager.	If the AMS Machinery Manager Data Collector is running, check that all appropriate security certificates are installed. An administrator can start the <code>certlm.msc</code> or <code>certmgr.msc</code> program to see if the appropriate certificates are installed. See <a href="#">Certificate installations</a> for instructions.

### 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: <ol style="list-style-type: none"> <li>1. In Windows Services, locate the <b>Plantweb Optics OPC UA Server</b> service.</li> <li>2. Stop and then restart the service.</li> </ol>



# A OPC UA and CMMS interfaces

## CMMS

A Computerized Maintenance Management System (CMMS), such as IBM Maximo or SAP Plant Maintenance Module, helps plant maintenance personnel:

- keep track of all the assets for which they are responsible.
- schedule and track maintenance tasks (also called work orders or notifications).
- keep a historical record of work they perform.

For information on connecting Plantweb Optics to your CMMS, refer to Knowledge Base Article **NK-2000-0252**.

## OPC UA

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.

For information on installing the Plantweb Optics OPC UA Server extension, refer to Knowledge Base Article **NK-2000-0246**.



# B Requirements for Tier-2, distributed deployment installations

## B.1 Tier-2 distributed deployment installation

A Tier-2 distributed deployment installation installs the system's databases on a separate SQL database server. For a Tier 2 installation, you must configure the SQL database server and the Plantweb Optics server in a specific order.

1. Set up the separate SQL Server for a Tier-2 (distributed deployment) installation. See [page 141](#).
2. Set up the Plantweb Optics server before a Tier-2 (distributed deployment) installation. See [page 144](#).
3. Install Plantweb Optics on the computer you designate as the Plantweb Optics server. During installation, choose a Tier-2 (distributed deployment) installation and supply information about the database server. See [page 47](#).

---

### 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 (distributed deployment) installation.

---

4. Finish post-installation set up on the Plantweb Optics server. See [page 145](#).

## B.2 Set up a separate SQL server for a Tier-2, distributed deployment 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

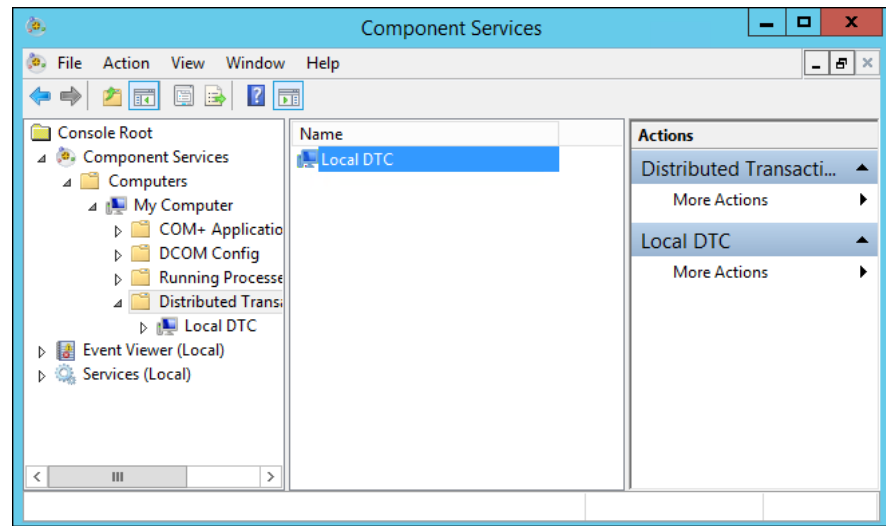
Plantweb Optics is NOT yet installed.

### 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
  - TCP/IP protocol must be enabled for the **EmersonCSI** SQL Server Network Configuration (SQL Server Configuration Manager)

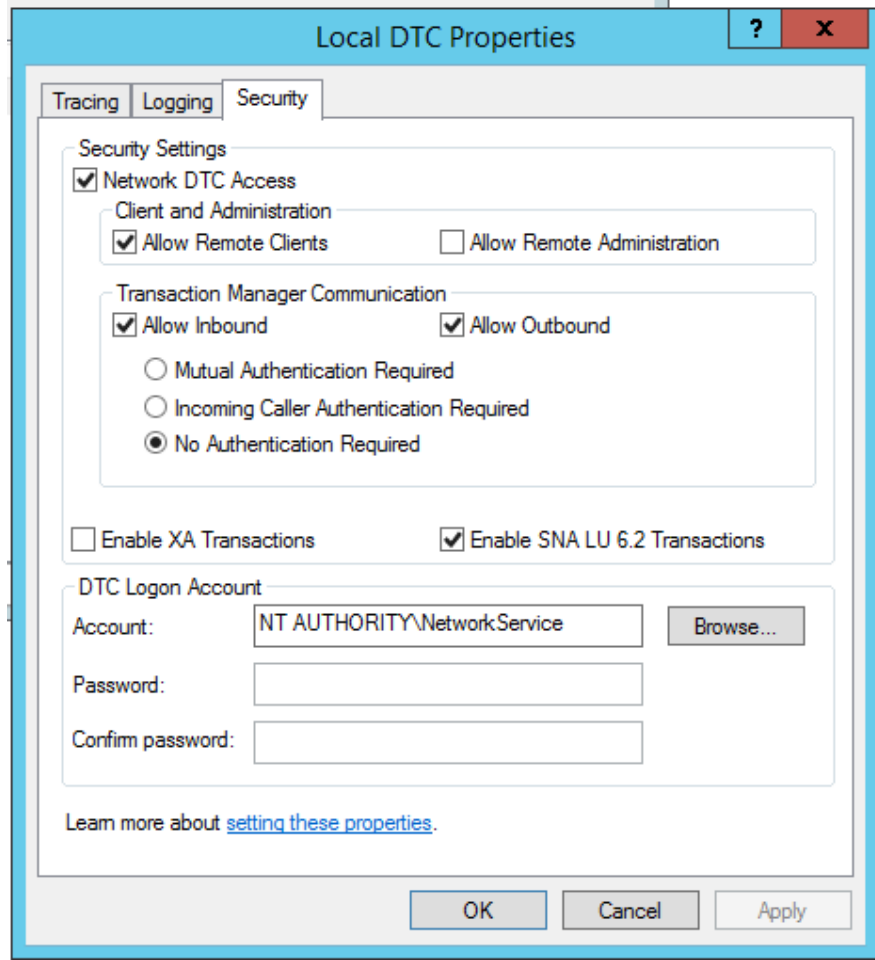
- SQL Browser must be running and set to auto-start
  - A static port for the **EMERSONCSI** SQL Instance must be set.
2. Update settings for Microsoft Distributed Transaction Coordinator (MDTC):
- a. In **Windows Component Services**, browse to **Component Services** → **Computers** → **My Computer** → **Distributed Transaction Coordinator** → **Local DTC**.

**Figure B-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 B-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 2016. This is a predefined firewall and needs to be configured if SQL Server is on Tier 2 deployment.
Distributed Transaction Coordinator (RPC-EPMAP)	Predefined firewall rule in Server 2016. This is a predefined firewall and needs to be configured if SQL Server is on Tier 2 deployment.
Distributed Transaction Coordinator (TCP-In)	Predefined firewall rule in Server 2016. This is a predefined firewall and needs to be configured if SQL Server is on Tier 2 deployment.
<b>EMERSONCSI</b> SQL instance TCP port	The port used by the Plantweb Optics to communicate with the SQL Server.

Inbound communication	Firewall rule
UDP Port 1434 (SQL Server Browser service)	SQL Browser. The SQL Server Browser service listens for incoming connections to a named instance and provides the client the TCP port number that corresponds to that named instance. Normally the SQL Server Browser service is started whenever named instances of the Database Engine are used. The SQL Server Browser service does not have to be started if the client is configured to connect to the specific port of the named instance.
TCP 139	SQL server
TCP 445	SQL server - File stream
TCP 135	RPC

Outbound communication	Firewall rule
Distributed Transaction Coordinator (TCP-Out)	Predefined firewall rule in Server 2016
UDP Port 1434	SQL Server Browser
TCP Port 1433	SQL
EMERSONCSI SQL instance TCP port	SQL

## B.3 Set up the Plantweb Optics server before a Tier-2, distributed deployment installation

In a Tier-2, distributed deployment 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, distributed deployment 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 (administrative) on the EMERSONCSI SQL instance or know the credentials of the SQL account that has those rights before proceeding with Plantweb Optics installation.

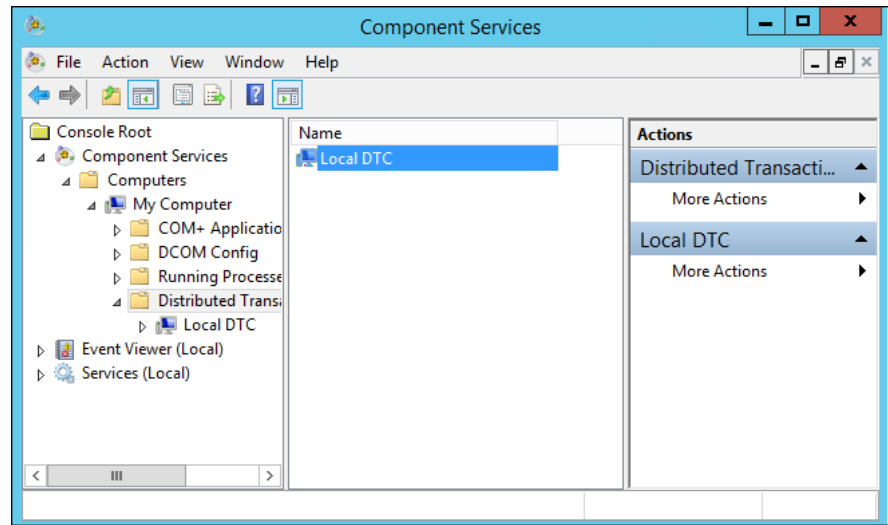
## B.4 Tier-2 - distributed deployment post-installation setup

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**.

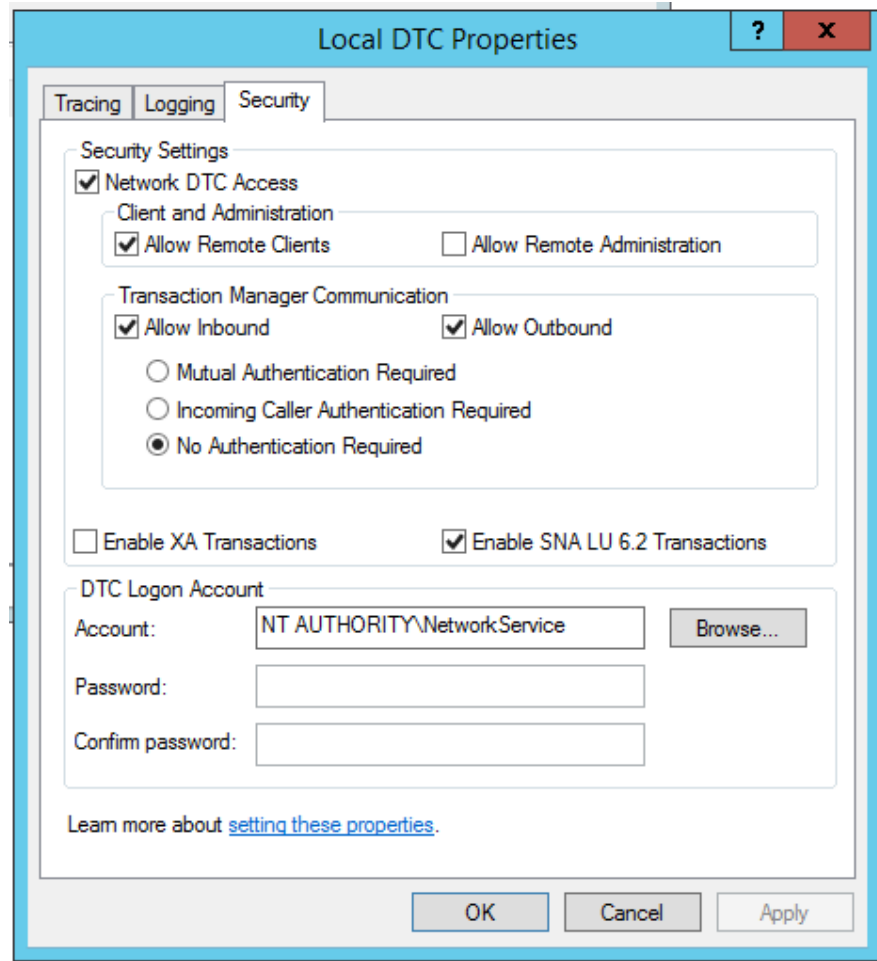
Figure B-3: Windows Component Services expanded to Local DTC



- 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 B-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 2016
Distributed Transaction Coordinator (RPC-EPMAP)	Predefined firewall rule in Server 2016

Inbound communication	Firewall rule
Distributed Transaction Coordinator (TCP-In)	Predefined firewall rule in Server 2016

Outbound communication	Firewall rule
Distributed Transaction Coordinator (TCP-Out)	Predefined firewall rule in Server 2016

---

**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.



# C Internet Information Services (IIS) reference and security compliance

## 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.

## Internet Information Services (IIS) reference

The following tables show the current IIS modules.

### Note

When components are installed on separate servers, the EmersonCSI base website references the DefaultAppPool application pool.

**Table C-1: IIS Module Plantweb Optics Services**

Application Pool	Site
AMSAssetMonitorDataCollector	\AMSAssetMonitorDataCollector
AMSDeviceManagerDataCollector	\AMSDeviceManagerDataCollector
AMSMachineWorksDataCollector	\AMSMachineWorksDataCollector
AMSMachineryManagerDataCollector	\AMSMachineryManagerDataCollector
DeltaVControlLoopDataCollector	\DeltaVControlLoopDataCollector
OpticsAnalyticsDataCollector	\OpticsAnalyticsDataCollector
KNetDataCollector	\KNetDataCollector
PlantwebInsightDataCollector	\PlantwebInsightDataCollector
ConnectorService	\ConnectorService
Proxy	\Proxy
PlantwebOptics	\Emersoncsi
PlantwebOptics_AdminServices	\AdminServices
PlantwebOptics_ASIServices	\ASIServices
PlantwebOptics_AssetExplorer	\AssetExplorer
PlantwebOptics_AssetServices	\AssetServices
PlantwebOptics_AssetView	\AssetView
PlantwebOptics_Help	\Help
PlantwebOptics_IdSrv	\OpticsIdSrv
PlantwebOptics_LicenseMgmt	\LicenseMgmt
PlantwebOptics_OnPrem	\OnPrem

**Table C-1: IIS Module Plantweb Optics Services (continued)**

Application Pool	Site
PlantwebOptics_SystemManager	\\SystemManager

**Table C-2: IIS Module AMS Asset Monitor Data Collector**

Application Pool	Site
AMSAssetMonitorDataCollector	\\AMSAssetMonitorDataCollector

**Table C-3: IIS Module AMS Device Manager Data Collector**

Application Pool	Site
AMSDeviceManagerDataCollector	\\AMSDeviceManagerDataCollector

**Table C-4: IIS Module AMS Machine Works Data Collector**

Application Pool	Site
AMSMachineWorksDataCollector	\\AMSMachineWorksDataCollector

**Table C-5: IIS Module DeltaV Control Loop Data Collector**

Application Pool	Site
DeltaVControlLoopDataCollector	\\DeltaVControlLoopDataCollector

**Table C-6: IIS Module Optics Analytics (KNet) Data Collector**

Application Pool	Site
OpticsAnalyticsDataCollector	\\OpticsAnalyticsDataCollector
KNetDataCollector	\\KNetDataCollector

**Table C-7: IIS Module AMS Machinery Manager Data Collector**

Application Pool	Site
ASMMachineryManagerDataCollector	\\ASMMachineryManagerDataCollector

**Table C-8: IIS Module Plantweb Insight Data Collector**

Application Pool	Site
PlantwebInsightDataCollector	\\PlantwebInsightDataCollector

# D Component and system compatibility

This appendix shows supported software versions for system compatibility.

**Table D-1: Component and system compatibility**

Item	Supported versions - KBA # Knowledge Base Article Title
AMS Asset Monitor	1.0.6, 1.0.7, or later
AMS Device Manager	13.1.1 - 14.1.1 (for server operating systems 2008/2016 that are 64-bit only)
AMS Machine Works	1.6
AMS Machinery Manager	6.31
DeltaV Control Loop	DeltaV 12.3.1 – NK-1400-0084 <i>DeltaV v12.3.1 Software Updates</i>
	DeltaV 13.3.1 – NK-1600-0394 <i>DeltaV v13.3.1 Software Updates</i>
	DeltaV 14.LTS – NK-1900-0840 <i>DeltaV v14.LTS (Long Term Support) / v14.3.1 Software Updates</i>
	DeltaV 14.FP# – TBD (Late May, Early June)
Optics Analytics	Optics Analytics Project Studio server 5.3
KNet	KNet online server 5.2
Plantweb Insight	2.0.x and greater
OPC UA Clients	OPC UA Expert 1.4.4 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





# Index

## A

- Add an AMS ASI asset source 68
- Add an asset source 62, 90, 97
- AMS Asset Monitor ASI
  - install 59
- AMS Asset Monitor ASI installation 61
- AMS Device Manager ASI
  - install 63
- AMS Device Manager ASI installation 66
- AMS Machinery Manager ASI
  - install 78
- AMS Machinery Manager ASI installation 82
- anonymous authentication
  - send email 112
- Asset Explorer
  - display data source asset screens 128
- Asset Monitor ASI deployment scenarios 59
- Asset Source interface and Augmented Reality installation procedures 55
- Azure Mobile Services
  - license Plantweb Optics 51

## C

- certificate
  - Connector service 109
  - install 112
  - proxy 109
- certificates
  - install Plantweb Optics 108
- compatibility
  - component support 151
- Configure a Proxy 57

## D

- data source asset screens, display with Asset Explorer 126, 128
- databases
  - backup and restore 131
  - Tier-1 automatic backup 131, 132
- DeltaV ASI deployment scenarios 86
- DeltaV Control Loop ASI
  - install 85
- DeltaV Control Loop ASI installation 88
- DeltaV ControlLoopSvc password 92

## E

- email
  - delivery methods 112

- email (*continued*)
  - formats 112
- Export a security certificate 111

## F

- formats
  - email delivery 112

## I

- Import .csv 73
- install a Connector Service certificate 109
- Install AMS Asset Monitor ASI 59
- Install AMS Device Manager ASI 63
- Install AMS Machinery Manager ASI 78
- Install DeltaV Control Loop ASI 85
- Install KNet ASI 93
- Install Optics Analytics Data Collector 96
- Install the Proxy 55
- installation
  - ASI quick start 9
  - client procedures 45
  - default 47
  - mobile procedures 115
  - overview 9
  - Tier-2 distributed deployment requirements 141
  - Tier-2 post-installation setup 145
  - Tier-2 SQL server setup 141
  - Tier-2 SQL server setup procedure 144
- Internet
  - IIS reference 149
  - system planning 25

## K

- KNet ASI
  - install 93

## L

- launch 125
- launch applications 125
- Launch in Context, display data source asset screens 126
- licensing 45

## M

- Machine fingerprint 45
- Machinery Manager ASI deployment scenarios 79
- methods

methods (*continued*)  
    email delivery 112  
Microsoft Edge Chromium configuration settings for Data Collector 90  
mobile Plantweb Optics  
    installation procedures 115  
mobile Plantweb Optics AR  
    installation procedures 115

## O

OIDC settings 106  
OPC UA and CMMS 139  
Optics Analytics ASI deployment 94

## P

param read configuration application 70  
Plantweb Optics AR Mobile app  
    install 117  
ports  
    host firewall 33  
    network firewall 37  
Proxy certificate 109

## R

Register AMS Asset Monitor 60  
Register AMS Device Manager ASI 66  
Register AMS Machinery Manager 82  
Register DeltaV ASI 87  
Register KNet 95

## S

security  
    firewall considerations 33  
    permissions 44  
    responsibilities 44  
    SSL/TLS certificates 38  
    user management 44  
SMTP configuration  
    commands 112  
system planning  
    database deployment 24  
    deployment scenarios 17  
    guidelines 15  
    Internet Information Services (IIS) 25  
    overview 15  
system requirements 25, 30  
system requirements, scalability assessment 30

## T

Tier-2  
    distributed deployment installation 141

Tier-2 (*continued*)  
    post-installation setup 145  
    SQL server setup 141  
    SQL server setup procedure 144  
troubleshooting  
    installation 133

## U

uninstall 121



**Emerson**

12001 Technology Drive  
Eden Prairie, MN 55344 USA  
[www.Emerson.com](http://www.Emerson.com)

©2021, Emerson.

The contents of this publication are presented for informational purposes only, and while every effort has been made to ensure their accuracy, they are not to be construed as warranties or guarantees, express or implied, regarding the products or services described herein or their use or applicability. All sales are governed by our terms and conditions, which are available on request. We reserve the right to modify or improve the designs or specifications of our products at any time without notice.

All rights reserved. AMS, Plantweb™, and Plantweb™ Optics are marks of one of the Emerson group of companies. The Emerson logo is a trademark and service mark of Emerson Electric Co. All other marks are the property of their respective owners.

