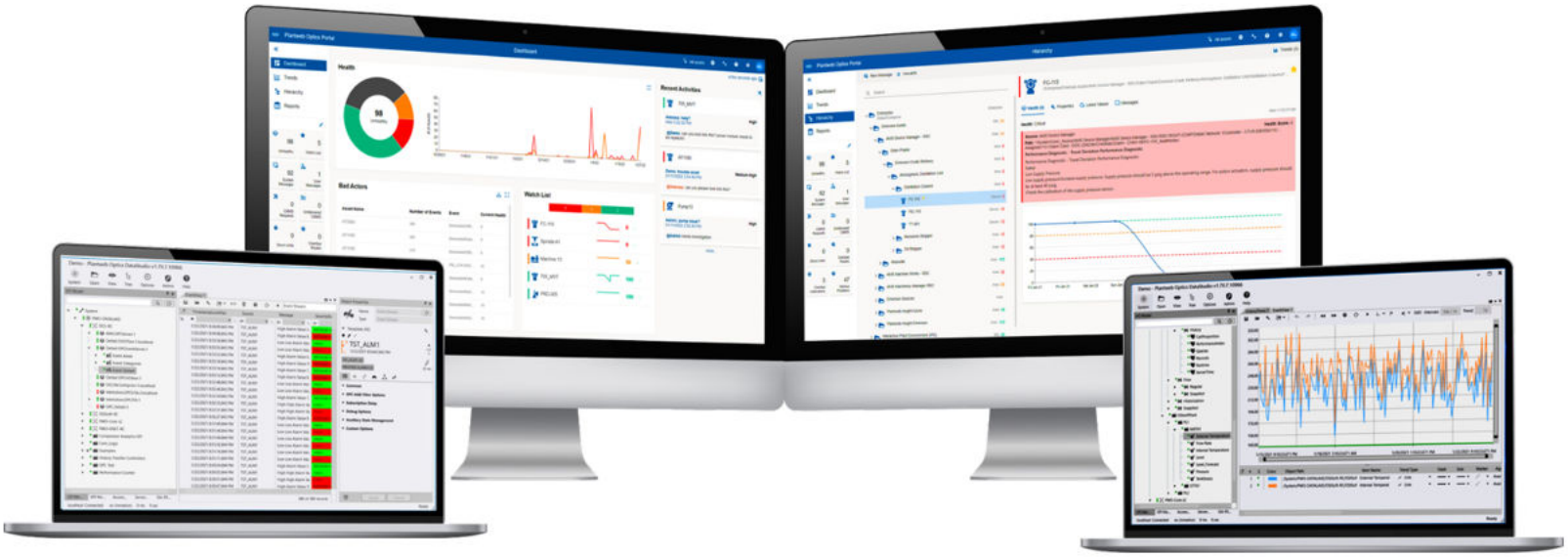
Revision 03-11-2022, Rev 01
March 2022

00_Plantweb Optics v1.8 System Guide - Chapters 1 and 3



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 document are covered under existing and pending patents.

Where to get technical support and customer service

Technical Support

Phone	Toll free 800-833-8314 (U.S. and Canada) +1 512-832-3774 (Latin America) +63 2 8702 1111 (All other locations)
Email	ap-sms@emerson.com
Internet	https://www.emerson.com/en-us/contact-us

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

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

Customer Service

Phone	Toll free 1-888-367-3774 Option 2 (U.S. and Canada) 1-888-367-3774 Option 2 (All other locations)
Email	wwcs.custserv@emerson.com
License Request	Plantweb Optics License Request Form

Trademarks and service marks

The Emerson logo is a trademark and service mark of Emerson Electric Co.

AMS, Plantweb™ and Plantweb Optics™ are marks of one of the Emerson group of companies.

Microsoft and Windows are registered trademarks of the Microsoft Corporation in the United States or other countries.

All other marks are property of their respective owners.

Contents

1 Introduction

The *Plantweb Optics System Guide* takes you through planning, securing, and installing the Plantweb Optics core services, Plantweb Optics Portal, Plantweb Optics Connector Service, and Emerson Connectors.

Note
This guide provides you links to the relevant documentation sections for *Plantweb Optics System Docs*. Using the documentation links, you can access detailed instructions to use the Plantweb Optics DataStudio client.

Emerson recommends that administrators read the first six chapters of *Plantweb Optics System Guide* before attempting to install the software and before reading the *Plantweb Optics System Docs*.

Introduction topics:

- Plantweb Optics product description
- What's in the System Guide
- Where to get help
- Plantweb Optics System Docs
- What's New in Plantweb Optics?

Other relevant documents

Other relevant documents

1.1 Plantweb Optics

Plantweb Optics provides a modern OT data connectivity, data management, and data repository solution built to accelerate your digital transformation programs. Plantweb Optics combines data from multiple applications into asset-centric information, then delivers persona-based alerts and KPIs for improving the reliability of assets throughout the facility. Eliminate OT data silos, collect and contextualize structured and unstructured data, and easily integrate OT data with IT tools and cloud applications to improve production, reliability, safety, and energy usage.

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

Configuration and interaction with Plantweb Optics happen through the following main applications:

- **Plantweb Optics Portal**–A client application accessed through modern web browsers or mobile apps for asset health management, collaboration, and workflow. This application contains a persona-based dashboard that shows automatic health scores, trends, messages, and the asset hierarchy. Plantweb Optics Portal is also used for admin functionality such as mapping users and generating mobile join keys.

- **Plantweb Optics DataStudio**–A client application that allows convenient, secure, and rapid access to your data source network. It is a fully integrated, single UI to perform system engineering tasks, object configuration, mass engineering, data analysis, and coding. Configure and manage logical assets, data sources, hierarchy of the system, and users.

For more information about Plantweb Optics and its key features, please visit `www.emerson.com/plantweboptics`.

1.2 What's in the this Guide?

The *Plantweb Optics System Guide* takes you through planning, securing, and installing the Plantweb Optics system, Plantweb Optics Portal, Plantweb Optics Connector Service, and Emerson Connectors (including Data Collectors).

If you are not installing Plantweb Optics Portal or Emerson Connectors, please refer directly to the *Plantweb Optics System Docs* for installation of Plantweb Optics system components.

If you are installing Plantweb Optics Portal or Emerson Connectors, Emerson recommends that administrators read this *Plantweb Optics System Guide* before attempting to install the software.

Other Documentation

- **Plantweb Optics System Docs**–provides an overview, installation instructions and detailed descriptions for the data management system that makes up the Plantweb Optics system and other Plantweb Optics system level components.
- **Plantweb Optics Portal Online Help**–provides instructions and reference information for using Plantweb Optics Portal after installation. This is built into the software and accessed by clicking in the user toolbar.
- **Knowledge Base Articles (KBAs)**–document product updates or configurations to address known issues, frequently asked questions, history traces, system requirements, how-to information, and application specific content.
- **Release Notes**–published as KBAs and contains what is new in this release, compatibility details, known issues, and resolved issues.
- **Plantweb Optics tutorials**–a series of short videos (how-to video playlist) 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.

Major Sections of the System Guide

1. Introduction to Plantweb Optics System Guide–***short description of each chapter***
2. Planning Your Installation–
3. Plantweb Optics Security–

4. Single server Installation–
5. Distributed server installation–
6. Post-installation Procedures–
7. Plantweb Optics DataStudio Administration–
8. Mobile Installation Procedures–
9. Uninstall Plantweb Optics Components (low-priority)–
10. Migrate Plantweb Optics Data—Accounts, Assets, and Settings, Oh My!–
11. System Image and Data Repository Procedures–
12. Troubleshooting–
13. External Interfaces–
14. Plantweb Optics Components and System Compatibility–
15. Anti-virus Exclusions–
16. Software upgrade paths–
17. Security hardening and compliance reference–

1.3 Where to get help

Technical Support

Phone	Toll free 800-833-8314 (U.S. and Canada) +1 512-832-3774 (Latin America) +63 2 8702 1111 (All other locations)
Email	ap-sms@emerson.com
Internet	https://www.emerson.com/en-us/contact-us

To search the Emerson website for product documentation, visit http://www.emerson.com.

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

Customer Service

Phone	Toll free 1-888-367-3774 Option 2 (U.S. and Canada) 1-888-367-3774 Option 2 (All other locations)
Email	wwcs.custserv@emerson.com
License Request	Plantweb Optics License Request Form

1.4 Plantweb Optics System Docs

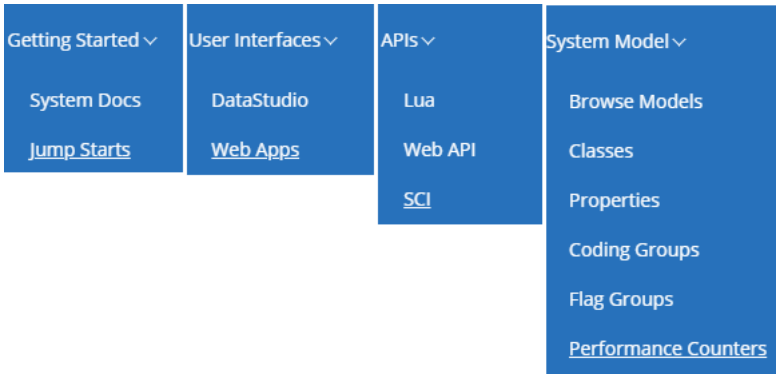
Using Guardian to reach the Plantweb Optics System Docs.

Plantweb Optics System Docs–access using the Guardian website as part of the Plantweb Optics documentation set. Once you perform the Plantweb Optics DataStudio installation, you can access the help anywhere that the DataStudio client browser runs (access Help drop-down).

1. Login to the Guardian site using the URL https://guardian.emerson.com/. Sign in with your **Email Address** and **Password**. Select preferred **Language**. Click **SIGN IN**.
2. Click **Support** (telephone icon).
3. Click **Resources** (last on the **Support** menu).
4. Under PLANTWEB OPTICS, select *Plantweb Optics DataStudio Help* to access the *Plantweb Optics System Docs*.

Tip
To quickly access other sections of the *Plantweb Optics System Docs*, use the selection menus on the top, right side of the help browser page.

Figure 1-1: Plantweb Optics System Docs - quick links



1.5 What's New in Plantweb Optics?

Plantweb Optics changes from previous versions

- **Asset (Explorer)**–configuration and set-up tasks moved to Plantweb Optics DataStudio.
- **User management tasks**–moved to Plantweb Optics DataStudio.
- **Out of Service Assets**–replaces the Plant Calendar view.

New capabilities

- **Filters**–user can now filter assets by criticality. The Filter applied to all the KPI List Views is designated with its name. User can save a maximum of 10 User Filters. Administrator can define a maximum of 10 Global Filters.
- **Messages**–two distinct presentations with the most recent messages at the start of each list. Messages include details about type, source, asset (hierarchy I/O path), and severity. Message filters on demand to provide a robust audit trail of events.
- **User Tagging**–done directly in messages for enhanced visibility. When your user login is tagged, messages are highlighted with an orange bar.
- **Join keys**–easily identify which mobile and AR join keys are disabled or assigned to users.

Security and User Permissions

- **User Permissions**–set in the Access Model for the Plantweb Optics Portal. This defines the user's realm of responsibility for portions of the plant's assets.
- **Single Sign-on access**–supports both Plantweb Optics DataStudio and Plantweb Optics Portal.
- **Data diode**–support between the AMS Device Manager Data Collector and the Proxy/ Connector Service. Future releases will provide data diode support for other connectors.

Database

Changed from a SQL database to using MongoDB (NoSQL) as the Plantweb Optics Data Repository.

Plantweb Optics includes:

Connected OT Data Infrastructure–Eliminate your data silos and manage the system centrally with support for major interfaces.

Supported Plantweb interfaces:

- OPC Data Access (DA)
- OPC Historical Data Access (HDA)
- OPC Alarms & Events (A&E)
- OPC XML Data Access (XML-DA)
- OPC Unified Architecture (UA)
- Object Linking and Embedding Database (OLE DB)
- Relational Databases (ODBC)
- Direct Programmable Logic Controller (PLC) connections
- MTQQ

Store Any Data Type–Time series, relational, pictures, documents, video, and more.

Contextualize Operational Data–Combine data from different sources into logical groups or hierarchies such as ISA-95, I/O, or physical structure, plus multiple KPI list views and reports.

Scale Easily–Every component of the Plantweb Optics can scale to support a range of design patterns from individual site deployments to an entire enterprise solution.

Use IT Visualization Tools–Can use any IT visualization tool such as Grafana, Power BI, Tableau, and Qlik for beautiful user experiences.

Manage Easily–Centrally manage an enterprise system with access to create, deploy, and delete objects. Allocate resources to match business continuity needs.

Enforce Security–Use identity and access management (IAM) model, fit for enterprise deployments.

Uses Data Repository–Enterprise scalability with MongoDB-based data repository. Scale horizontally with clusters and meet availability needs with replica sets across your global data center infrastructure.

Employs New Licensing Model–Plantweb Optics scales based on logical CPUs used, and not tags used. Pay for what you use and not how much data you store.

Automate with Powerful Logic Engine–Create rules and policies with Lua scripts. Save data scientist time by doing data transformations either at the Data Source or in the Core.

Deploy Software–Install on-premises or in cloud infrastructure in minutes. Automate administration steps using a full-featured Command Line Interface (CLI).

2

Chapter left blank - inserted later at this position.

3 Plantweb Optics security

Administrators should consider these security items for the Plantweb Optics application and its installations:

- Plantweb Optics server security
- Plantweb Optics Portal security
- Mobile application security
- Data Collector security
- Host and network firewall ports
- SSL/TLS certificates
- Miscellaneous considerations

For additional security consideration refer to the Plantweb Optics specific cybersecurity section of *AMS Product Security Documentation* (version 5).

3.1 Plantweb Optics server security

Administrators must address these security items for the Plantweb Optics Server that runs the core services:

- User identification and authentication
- Enforce user authorization
- Authorization for external connections to access Plantweb Optics
- Authorization for Profile access of models
- Administration and auditing roles
- Assign profiles for model permissions
- Manage user accounts on Plantweb Optics Server
- Secure Connector communication
- OPC UA secure communication
- Miscellaneous Optics Server recommendations

3.1.1 User identification and authentication

Identification of users is used in conjunction with authorization mechanisms to implement access control for a Plantweb Optics system. Verifying the identity of users requesting access is necessary to protect against unauthorized users from gaining access to any Plantweb Optics components.

Plantweb Optics DataStudio provides multiple methods of authentication:

- Profile Credentials
- Windows Authentication

In accordance with your security policies and procedures, Emerson strongly recommends using Windows authentication. This method of authentication provides capabilities that can uniquely identify and authenticate active users of your organization.

NOTICE

Profile objects when used to log in and access Plantweb Optics (using the Profile Credentials) can be used for user account sharing. This is because the Profile object is not mapped to any active user account in your organization. Also, the Profile object is *not subject to complying* with the organization's existing User Account Policy.

User access to Plantweb Optics Portal is also configured in Plantweb Optics DataStudio by assigning *External API* authorization. See *Authorization for external connections to access Plantweb Optics* for more details.

3.1.2 Enforce user authorization

After Plantweb Optics has verified the user's identity, Plantweb Optics must also verify that a requested operation is actually permitted, according to the defined security policies and procedures.

Plantweb Optics DataStudio provides an authorization enforcement for all authenticated users, based on their assigned responsibilities. Emerson strongly recommends you only assign the necessary permissions to qualified and authorized users.

NOTICE

In Plantweb Optics DataStudio, creating a User object below a Profile assigns that user to the Profile. This means that the User *inherits* all the permissions and privileges from that Profile. The Profile can be leveraged as a Role-based Access Control (RBAC); one that restricts access based on the roles of individual users within Plantweb Optics.

3.1.3 Authorization for external connections to access Plantweb Optics

Grants authorization to an external connection to access the Plantweb Optics site.

Name	Can access Plantweb Optics using the Plantweb Optics
DataStudio	DataStudio.
External API	Optics Portal, with just read-only access.
OPC DA Connections	Data Access client (OPC DA client).

Name	Can access Plantweb Optics using the Plantweb Optics
OPC HDA Connections	OPC Historical Data Access client (OPC HDA client).
OPC A&E Connections	OPC Alarms and Events client (OPC A&E client).
OPC UA Connections	Unified Architecture client (OPC UA client).

3.1.4 Authorization for Profile access of models

Grants authorization for a Plantweb Optics Profile to access a specific model.

Model Name	Model Description
I/O	All classes required for managing external data sources and persistent data storage including Time Series and Alarm and Event historization.
KPI	All classes which relate to key performance indicators and their organizations to other models and classes.
Access	All classes that allow for setting security permissions. It supplies the features required to create and maintain a secure Information Management System.
Server	Allows you to manage external Server Interfaces of Plantweb Optics and the assignment of other models to the namespace of other Servers.
ISA-95 Equipment	The ANSI / ISA-95 Equipment Model may be a definition of sites, areas, production units, production lines, work cells, process cells, or units.
ISA-95 Material	The ANSI / ISA-95 Material Model defines the actual materials, material definition, and information about classes of material definition.

3.1.5 Administration and auditing roles

Administrative Roles

Set the level of administrative privileges of a Plantweb Optics server profile.

Level	Administration Access Privileges
None	None
Administrator	Full
Reviewer	Read-only

Audit Trail Roles

Set roles to an Optics server Profile to manage the audit trail.

Role	Description
Administrator	Enable and disable Audit Trail, plus can update auditing strategy.
System-wide Reviewer	View Audit Trail for entire Plantweb Optics site.
Limited Reviewer	View Audit Trail for the objects that have Read access. (See Related information for details.)

3.1.6 Assign profiles model permissions

A Profile can be assigned access permissions to any level in the Model panels (for example System, Core, Connector, Node, or even an I/O item in the I/O model). Assigned permissions can then extend to any User or Group that belongs to the Profile. To assign Profile model permission, drag the Profile from the Access Model to the chosen object level in one of the Model panels. Permissions you can assign are listed in this table.

Profile Access Permission	Description of User Access Capabilities
List	When set to `True`, the object displays when listing the children of its parent. Also the ancestors of the object can be listed.
Read	All object properties (including dynamic properties) can be read by the user.
Write	The dynamic properties of the object can be written for the user.
Modify	All object properties (including dynamic properties) are writable can be written for the user.
Execute	Object methods can be called by the user.
Inheritable	The explicit permissions set for this object are inherited for all children.

NOTICE

Setting Profile access permissions can restrict users from obtaining asset information using the Plantweb Optics Portal.

The **Inheritable** permission ensures that all the children objects beneath the target object level, inherit the set permissions.

Your Plantweb Optics Administrators are responsible for configuring these permissions.

3.1.7 Manage user accounts on Plantweb Optics Server

Remove Inactive Accounts

Regularly check and remove inactive accounts. Inactive accounts are a significant security issue. Malicious users (including former employees) can use those accounts to attack your system. Emerson strongly recommends that Administrators regularly check for and remove inactive accounts.

Protect Administrator Accounts

Administrator accounts are privilege accounts that provide the ability to manage Plantweb. Emerson recommends to secure and do not share the Administrators credentials.

Refrain from using Shared Accounts

Shared accounts are accounts that multiple people use. Since many operations are logged, sharing accounts makes it difficult to determine who performed an operation by reviewing the log. Emerson strongly discourages the use of shared accounts and Profile credentials.

3.1.8 Enforce user account policies

Emerson strongly recommends using Windows Authentication. This provides the capability to enforce account and password polices. Also you can enforce account lockout policies for each user account.

For the complete list of supported Account Policies, refer to *Security Hardening and Compliance references* chapter. See the *Microsoft Windows Server Hardening* section.

NOTICE

Emerson recommends a minimum password length of ten (10) characters.

Your IT department must configure these security policies.

3.1.9 Secure Connector communication modes

Plantweb Optics Server supports secure inter-component communication. Configure the Communication Security Mode for your installation.

Mode	Description of Communication Security Mode
None	Overall strength is *none*. Uses fast proprietary obfuscation for data privacy and has no authentication. It is adequate only in a fully trusted environment.
Passphrase	Overall strength is *weak*. Uses fast proprietary data obfuscation and authenticates using a matching passphrase. It is adequate when the privacy and integrity of data is of little concern, but unauthorized access must be prevented.
TLS-SRP	Overall strength is *strong*. Uses a strong cryptographic protocol (TLS) and secure remote password authentication.
TLS-X.509	Overall strength is *strong*. Uses a strong cryptographic protocol (TLS) and X.509-certificate-based authentication (based on Microsoft Windows AD).

Emerson strongly recommends using TLS-SRP or TLS-X.509 security mode. This provides strong encryption, authentication, and authorization.

NOTICE

Combine these security modes with the connection modes:

- **Passive**–a remote component listens for incoming connection requests from the Core service.
- **Active**–a remote component actively sends connection requests to the Core service.

Your Plantweb Optics Administrators are responsible for setting up these configurations.

3.1.10 OPC UA secure communication

You can secure the communication between Plantweb Optics and a server using the external OPC UA protocol.

- **Security Modes**–The security mode `Sign` or `SignAndEncrypt` ensures that authentication at the application level is enforced. Emerson recommends using the security mode `SignAndEncrypt` because it ensures both integrity and confidentiality of data.
- **Security Policy**–Security policies determine the desired level of encryption. Emerson recommends using the most secure cryptographic algorithm supported by both OPC UA Server and the client, `Basic256SHA256`.
- **Authentication**–Emerson strongly recommends the use of credentials-based and certificate-based authentication. Avoid using an `Anonymous` connection (does not provide protection), especially for accessing critical UA server resources.

For certificate-based authentication, do not automatically allow connection to untrusted certificates. Especially, self-signed certificates without an additional verification.

3.1.11 Miscellaneous Optics Server recommendations

Emerson strongly recommends that you:

- Upgrade manually to use MongoDB 4.4.8 for existing Plantweb Optics installations. To perform the upgrade manually, visit the MongoDB website for upgrade instructions in the MongoDB documentation. Search for subjects with keywords of *Upgrade a Standalone*, *Upgrade a Replica Set*, and *Upgrade a Sharded Cluster*. See Related information for details.
- Enable MongoDB to use access control and enforce authentication by using SCRAM or x.509 authentication mechanism or integrate with existing LDAP infrastructure.
- Configure an X.509 certificate-based inter-component authentication, between Core and Connector, plus the Master Core and its Local Core.
- Configure Web API to communicate over HTTPS/Secure WebSocket (WSS).
- Manage the certificates of OPC Services using a Certificate Management dialog.

NOTICE

Except for MongoDB, configuring Web API to use HTTPS. Disable the Profile Credential login as part of your post-installation procedures.

Contact Emerson Professional Services for guidance on planning and preforming a production Plantweb Optics installation. See Related information for details.

3.2 Plantweb Optics Portal security

Security recommendations for Plantweb Optics Portal include

- Register all Optics Portal users
- Restrict your file attachment types to these files
- Keep CMMS configuration fields private.

3.2.1 Register Optics Portal users

Emerson strongly recommends that you only register users who are working directly with Plantweb Optics Portal.

All users granted an `External API` authorization in Optics DataStudio, are granted read-only access to Plantweb Optics Portal. User registration allows users to have a read and write access to the application.

NOTICE

User with administrative privileges within Optics DataStudio and registered in Plantweb Optics Portal, are treated as a Plantweb Optics Portal Administrator. A Plantweb Optics Portal Administrator can manage the **Admin Settings** (that is, Join Keys, License, Users, Language packs, and Global Filters).

Your Plantweb Optics Portal Administrator registers users that work with Plantweb Optics Portal.

3.2.2 Allowed file attachment types

Secure your Plantweb Optics system from file attachment related attacks.

- Upload scanned files only. To minimize risk, all files should be scanned for malware. Uploading of malicious files intentionally or unintentionally is strictly prohibited.
- Upload only the supported file types : that is, PDF, DOC, DOCX, PPT, PPTX, CSV. LOG, TXT, JPG, JPEG, PNG, BMP, GIF, XLS, XLSX and SVG.
- Prohibit uploading of any executable or script files.

3.2.3 CMMS Configuration

Keep the CMMS configuration fields private to avoid compromising the CMMS system. All Plantweb Optics Portal users can view the CMMS configuration settings, but only administrators can change the settings.

3.3 Mobile application security

Plantweb Optics offers a mobile application (Plantweb Optics Mobile and Augmented Reality) that can send information to your mobile devices to improve field worker productivity and safety.

Some best practices to secure your Plantweb Optics mobile apps include:

- Register mobile devices
- Use mobile application join keys (tokens)
- Install software security updates

3.3.1 Register mobile device with join key

Use mobile device registration in the **Admin Settings** of Plantweb Optics Portal, to augment security for the lifetime of your site's mobile devices.

A Plantweb Optics Administrator issues a mobile token (*join key*) to a user. to register the device. The token is unique to you and the app—it identifies your username and the Plantweb Optics Mobile App. Each mobile device requires a separate token. Different sites also require different tokens.

The administrator should only generate a mobile token for authorized users. Limiting the number of users who connect wirelessly will helps reduce the risk of an attack.

Administrators need to instruct their Plantweb Optics site users to keep their mobile tokens private.

The token (*join key*) is valid until the Plantweb Optics Administrator or the user disables it.

3.3.2 Software security updates for mobile devices

The Google App Store releases software security updates as part of it software update program.Emerson recommends that you install updates as early as possible, to ensure the integrity and security of your site.

Additionally, Emerson recommends installing IOS and Android security patches to address known mobile software vulnerabilities.

3.4 Individual data collector security

To manage asset sources, you should provide the access key required to login in to the data collector's application. The asset source administrator who installed the data collector, created the access key.

⚠ CAUTION

Emerson recommends that the asset source administrator control the access keys and keep the keys secured.

3.5 Host and network firewall ports

The Plantweb Optics components that use web API communication, need firewall exceptions for a user-defined port. The installation procedure selects port 443 as the default.

A *host-based firewall* handles incoming and outgoing network traffic for a server. It determines whether to allow data to a particular device. An example is the Microsoft firewall that comes with a Windows-based computer.

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.

Best practices include:

- Following Emerson firewall recommendations
- Using recommended port numbers for Plantweb Optics components

3.5.1 Emerson firewall recommendations

Your IT staff needs to configure firewalls, when setting up Plantweb Optics, to permit its components to communicate. Emerson recommends:

- Set up your firewall exceptions for each server before Plantweb Optics installation.
- Identify the DNS names and IP addresses of the servers. These ports must be open.
- Configure a host-based firewall for each individual server.
- Configure a network-based firewall for each network layer.
- Determine what intermediary firewalls require exceptions.

3.5.2 Plantweb Optics component port numbers

These ports must be opened to allow communication through to each component of Plantweb Optics:

- Table 3-1 - Plantweb Optics Portal Server
- Table 3-2 - Plantweb Optics Server (core)
- Table 3-3 - Plantweb Optics Database Server
- Table 3-4 - Plantweb Optics Connector Service
- Table 3-5 - Proxy
- Table 3-6 - Plantweb Optics CMMS Interface
- Table 3-7 - Plantweb Optics Mobile App
- Table 3-8 - Data Collector

Table 3-1: Ports used by Plantweb Optics Portal Server

Port	Source	Destination	Notes
TCP 443 (configurable)	Plantweb Optics Portal Client	Service	Inbound rule Allows communication with the Plantweb Optics
TCP 587 (SMTP)		**smtp.sendgrid.net**	Outbound rule to **smtp.sendgrid.net** should be open to the Internet.

Table 3-2: Ports used by Plantweb Optics Server

Port	Source	Destination	Notes
TCP 6510 – 6512, 6515	Service	Service	Plantweb Optics services ports
TCP 27017	Service	Database Server	Outbound rule MongoDB port
TCP 8002, 8003	Plantweb Optics Portal Server Connector Service	Service	Inbound rule Allows to communicate from the source

Table 3-3: Ports used by Database Server

Port	Source	Destination	Notes
TCP 27017	Plantweb Optics Data Server	Service	Inbound rule MongoDB port

Table 3-4: Ports used by Plantweb Optics Connector Service

Ports	Source	Destination	Notes
TCP 443 (configurable)	Data Collector Proxy	Service	Inbound rule Allows to receive data from the source
TCP 8002	Service	Plantweb Optics Portal Server	Outbound rule Allows to send data to the destination

Table 3-5: Ports used by Proxy

Ports	Source	Destination	Notes
TCP 443 (configurable)	Service	Plantweb Optics Connector Service	Outbound rule Allows to send data to the destination
	Data Collector Proxy from lower-level network	Service	Inbound rule Allows to receive data from the source

Table 3-6: Ports used with Plantweb Optics CMMS Interface

Ports	Source	Destination	Notes
TCP 448 (configurable)	Plantweb Optics Server CMMS (SAP / Maximo)	Plantweb Optics Server CMMS (SAP / Maximo)	Inbound and outbound rule Allows communication with Plantweb Optics and CMMS Integration (SAP or Maximo).
<CMMS Server TCP port> (configurable)	Plantweb Optics Server	Outbound	This could be SAP or Maximo server port.
TCP 3200-3299	Plantweb Optics Server	Outbound	Dispatcher, CMMS GUI to CMMS (SAP PM)
TCP 3300-3399	Plantweb Optics Server	Outbound	Gateway to CMMS (SAP-PM) One TCP port on this range
TCP 4800-4899	Plantweb Optics Server	Outbound	Gateway-secure to CMMS One TCP port on this range
TCP 3260, 3360	Plantweb Optics Server	Outbound	NLink to CMMS

Table 3-7: Ports used by Plantweb Optics Mobile App

Ports	Source	Destination	Notes
TCP 443	Plantweb Optics Portal Server	***.azurewebsites.net**	Outbound rule TCP 443 outbound to ***.azurewebsites.net** should be open to the Internet for the Plantweb Optics Mobile App.

Table 3-8: Ports used by Data Collector

Ports	Source	Destination	Notes
TCP 443 (configurable)	Service	Plantweb Optics Connector Service Proxy	Outbound rule Allows to send data to the destination
(See additional firewall consideration of each specific Data Collector on their corresponding Product Specific section)			

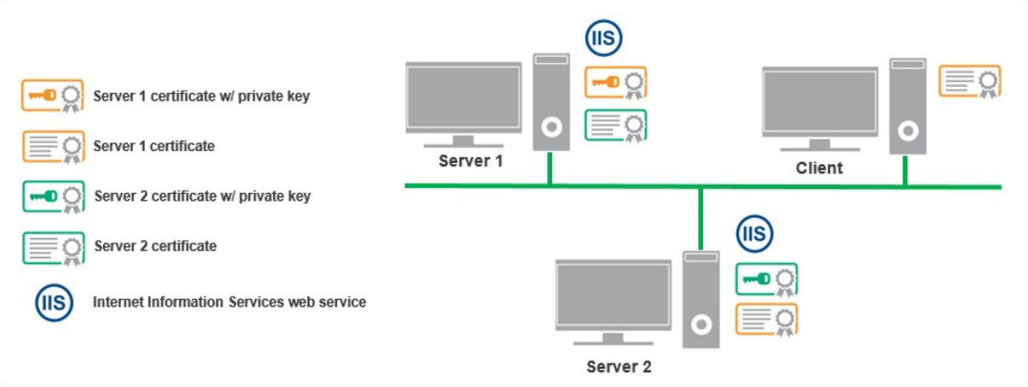
3.6 SSL and TLS certificates

Plantweb Optics requires Secure Sockets Layer (SSL) and Transport Layer Security (TLS) for all web communications. The following sections describe which components have certificates. Then, where you should install the certificates, based on a generic deployment scenario.

Emerson recommends working with qualified IT personnel to ensure your installation complies with your plant's network security policy and industry best practices.

SSL and TLS allows applications to establish secure communications between web servers and web browsers. See the following example relationship between web servers and browsers using SSL and 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 One. It does not have a certificate for Server Two.

Figure 3-1: Web servers and browsers using SSL and TLS certificates



3.6.1 Certificate names

During your Plantweb Optics installation, self-signed certificates are automatically generated and installed for components that use web applications. The certificate is unique to the server.

Component	Certificate
Plantweb Optics Portal Server	PlantwebOptics.*{Full Computer Name}*
Plantweb Optics Connector Service	PlantwebOptics.*{Full Computer Name}*
Plantweb Optics Proxy	PlantwebOptics.*{Full Computer Name}*
Plantweb Optics Data Collector	PlantwebOptics.*{Full Computer Name}*

3.6.2 Certificate deployment

Plantweb Optics components need to exchange public key certificates to successfully communicate with each other. All certificates must be installed manually.

NOTICE

Only install the certificates your Plantweb Optics components need.

⚠ CAUTION

Certificate's private keys should always be kept secure. Only the certificate's public key can be distributed to other systems that need it. If the certificate's private key is compromised, it can be used to impersonate the component it represents.

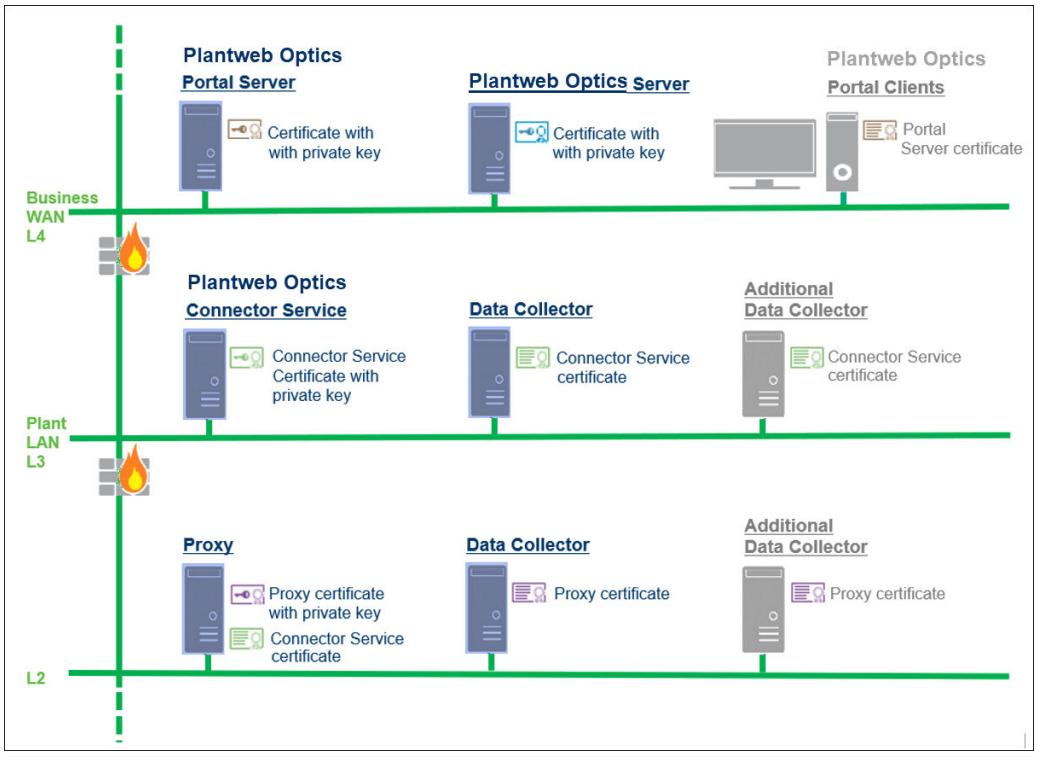
Table 3-9: Certificates deployment

System	Installed Certificate
Plantweb Optics Portal Server	None
Plantweb Optics Portal Clients	Plantweb Optics Portal Server certificate
Plantweb Optics Connector Service	None
Plantweb Optics Proxy	Connector Service certificate **Note** Install Proxy certificate instead of Plantweb Optics Connector's Service certificate if direct communication to Connector Service is not possible due to arbitrary number of networks between proxy and Connector Service.

Table 3-9: Certificates deployment *(continued)*

System	Installed Certificate
Plantweb Optics Data Collectors	Connector Service certificate **Note** Install Proxy certificate instead of Plantweb Optics Connector's Service certificate if direct communication to Connector Service is not possible due to arbitrary number of networks between proxy and Connector Service.

Figure 3-2: Certificate deployment example



3.6.3 Certificate installation checklist

These tasks show the recommended order of installation on each Plantweb Optics computer, with an emphasis on certificate export and how it relates to installation tasks.

⚠ CAUTION

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

Table 3-10: Certificate install procedure

Step	Located on the	Action
1	Connector Service machine	☐ Install the Connector Service ☐ Export the Connector Service certificate
2	Proxy machine (if used)	☐ Install the upstream component certificate (either Connector Service or Proxy) ☐ Export the Proxy certificate (if another Proxy will communicate with this Proxy)
3	AMS Device Manager Server	☐ Install the AMS Device Manager Data Collector ☐ Install the upstream component certificate (either Connector Service or Proxy)
4	AMS Machine Works Server	☐ Install the AMS Machine Works Data Collector ☐ Install the upstream component certificate (either Connector Service or Proxy)
5	AMS Machinery Manager Server	☐ Install the AMS Machinery Manager Data Collector ☐ Install the upstream component certificate (either Connector Service or Proxy)
6	DeltaV Control Loop Data Collector	☐ Install the DeltaV Control Loop Data Collector ☐ Install the upstream component certificate (either Connector Service or Proxy)
7	Optics Analytics Server	☐ Install the Optics Analytics Data Collector ☐ Install the upstream component certificate (either Connector Service or Proxy)
8	Plantweb Insight Data Collector	☐ Install the Plantweb Insight Data Collector ☐ Install the upstream component certificate (either Connector Service or Proxy)

3.7 Other 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 Plantweb Optics DataStudio Access Model 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.

Glossary

Access Model

A group of classes that defines security permissions for other Optics DataStudio models and classes. It supplies the features which are required to create and maintain a secure infrastructure. For example, a user profile can be restricted to only control assets in one branch of the asset hierarchy.

AD (Active Directory)

A directory service for Windows domain networks. The Windows Domain Controller (DC), which is the server running the AD DS role, is the software/hardware that provides the AD set of services. The primary function of a domain controller is to authenticate and authorize all users and their resources into a Windows domain network.

ADFS (Active Directory Federation Service)

An identity access solution that provides client computers (internal or external to your network) with seamless Single Sign-On (SSO) access to protected Internet-facing applications or services, even when the user accounts and applications are located in completely different networks or organizations. Active Directory is a type of directory and contains information about the properties and location of the different types of resources within the network. Using it, both users and administrators can find them easily.

alert category

A Plantweb Optics device or NAMUR NE-107 Diagnostic classification used to filter messages into Abnormal (those affecting health) or Advisory (no health impact).

Analytics Deviations

Previously known as *KNet KPI Deviations*.

asset

Any physical component (such as a device or machine) being monitored by Plantweb Optics DataStudio, or the logical representation of a physical asset. Examples include a motor, a pump, a fan, or a turbine.

asset criticality

A value representing the importance of an asset with respect to other system assets . You specify the criticality using an integer value between 1 and 100,000.

asset hierarchy

The organization of assets by location (site, area), data collector type (formerly known as ASI type), and asset source.

asset source

Anything that collects data to be associated with an asset. For example, an *AMS 9420 Wireless Vibration Transmitter*.

asset source location

A representation of the real-world, physical position of the asset source. Asset source locations help users to arrange assets and asset sources by their physical locations, in addition to their logical positions in the network. The I/O Model reflects these locations.

attachment

A document or image file linked to a specific asset. Emerson recommends that you keep file sizes less than 30 MB. For a complete list of accepted file types, refer to the *File attachments* topic in the *Plantweb Optics Portal Help* or the *Plantweb Optics System Guide*.

augmented reality (AR)

Plantweb Optics Augmented Reality overlays digital information on physical images to increase productivity, safety, and insight.

bulk edit

A Plantweb Optics DataStudio function (MassConfig) that provides users a method to change multiple objects using a spreadsheet . To use this feature, you:

1. Export a collection of assets or CMMS objects using the `.csv` (comma-separated values) file format.
2. Make all desired changes with a program that manipulates `.csv` formatted files.
3. Import the updated `.csv` file back into the data repository.

client application

A Plantweb Optics or third-party client that accesses the data repository. DataStudio is a client application that is included with Plantweb Optics. Custom client applications (Movicon.NExT) can access data from the repository (JSON) or from the Plantweb Optics Server.

CMMS work requests

A user- or system-generated request for work to be done on an asset. Work requests can be `Open` (not acted on), `Pending` (work in progress), `Closed`, or `Undelivered` (SAP or MAXIMO did not yet receive the request).

Connector

Another term for a Connector service. It retrieves data from one or multiple data sources. It integrates data from Emerson data collectors, OPC UA servers, or other sources and passes it to the Core, where it is stored in the repository. Permits the connection of multiple real-time data sources using secure, compressed single-port TCP communication with the Relay or the Core.

Core

Another term for the Core service. The central component of Plantweb Optics. The Core retrieves data from any number of Plantweb Optics Connectors, in the same network or located at remote locations. The Core processes the data, storing all information in the Data Repository. The Core also can process WebAPI and OPC requests from client applications, such as, Plantweb Optics Portal, DataStudio, and Movicon.NExT. It exposes the data to the web clients using open formats, such as, OPC UA, JSON, ODBC, CSV (spreadsheet), and so forth.

Data Access (DA)

The OPC Unified Architecture data access specification used to communicate between Plantweb Optics OPC UA server and the Movicon.NExT client project.

Data Repository

A central storehouse that stockpiles acquired data using standard formats. MongoDB is the repository; an open-source NoSQL database that can scale to work with increasing amounts of real-time data. See *MongoDB*.

data source

Data sources are also referred to as endpoints. A data source exposes information, which was retrieved using Plantweb Optics Portal. Example sources are an OPC UA server, an Emerson Connector (such as AMS Machinery Manager), or a cloud service (Azure or Amazon Web Services). A data source is connected to the Plantweb Optics Data Repository through a Connector.

DataStudio

One of many client applications used with Plantweb Optics. It is designed to be a secure and singular interface to access a data source network. DataStudio provides access to your real-time and historized data. It supports an interface and customizable tools set to provide users, power users, and administrators, the features to configure and control their workspace.

Emerson Connectors

Formerly known as an *Asset Source Interface* (ASI). Extends Plantweb Optics by adding connectivity and communications to asset sources, such as external devices or systems. Emerson Connectors allow data to be stored and accessed in the Plantweb Optics Data Repository.

events

Any occurrence in Plantweb Optics DataStudio that a service or utility wants recorded and possibly a user to react to. Certain events create a message that is delivered to users that are subscribed to receive messages for this event type. A user has access to the assets assigned by the Plantweb Optics administrator.

You can choose to receive messages for certain events, which are displayed in the Plantweb Optics. You can also choose to receive notifications on a mobile device or using email. Install the Plantweb Optics Mobile App to view and respond to messages from a mobile device.

guest account

A user account that is authenticated in Plantweb Optics Data Studio, but does not have an assigned user in Plantweb Optics Portal. A guest account has limitations. You cannot perform specific actions and you receive a message stating that, "User does not have access rights to this feature:"

- **Dashboard**–Watch List and Recent Activities
- **KPI List Views**–Watch List
- **Hierarchy** (assets)–New message and new work request
- **Settings**–Notifications and Message Filter
- **Filter panel**–Add and edit User Filters

Hierarchy

The asset and location tree that defines the customer's asset organization. You can display asset health messages, properties, latest values, messages, and KPIs associated with select assets. Displays the last seven days of health values (trend) for a selected asset. It displays the asset hierarchy that mirrors the ISA-95 model hierarchy from Plantweb Optics DataStudio. This display shows all assets for which a user has access, based on the locations and security profile applied by the administrator.

historize

Select asset parameters for trending in Plantweb Optics Portal and DataStudio.

host-based firewall

An application installed on each individual server for controlling incoming and outgoing network traffic. It also determines whether to allow data to a particular device. An example is the Microsoft firewall that comes with a Windows-based computer. Plantweb Optics recommends configuring a host-based firewall for each Plantweb Optics component server (Core, Client, Connector, Data Repository, and Data Collector.

I/O Model

Previously known as the *Network Hierarchy*. This model display's the asset's static physical devices and device parameters. The I/O Model contains such objects as Scheduler Items and Action Items. The I/O system tree comprises all classes required for managing external data sources and persistent data storage, including Time Series plus the Alarms and Events Historization. See *ISA-95 Model* for details about the asset logical view and making changes to an asset.

ignored assets

Also referred to as *out of service* assets. The **Out of Service Assets** report shows the current schedules and the out of service assets. You can also export ignored asset information as a `*.csv` file (spreadsheet).

ISA-95 Model

Previously referred to as the *Logical Hierarchy*. The model helps you to create a logically compliant hierarchical asset model for all sites, units, and modules within a plant. Use this model to make changes to the asset, while keeping the assets physical devices and measurements (parameters) static. This is the logical model you use to set specific asset properties, either manually or using the bulk edit feature (MassConfig) in Optics DataStudio. See *I/O Model* for details about the asset physical devices.

join key

Allows you to log in to the Plantweb Optics Mobile or Augmented Reality client. The join key is unique to you and the application. It identifies your username and the Plantweb Optics Mobile client. The join key is valid until it is disabled in the **Settings** > **Admin** > **Join Keys** interface by the user or a Plantweb Optics administrator.

key performance indicator (KPI)

An asset list based on criteria set in Plantweb Optics to alert users of potential problems. KPIs include **Unhealthy** (assets with low health scores), **Watch List**, **System Messages**, **User Messages**, **CMMS Requests**, **Undelivered CMMS** (work requests), **Overdue Calibration**, and so forth.

KPI Model

A collection of classes that relate to key performance indicators and their organization.

licenses

Plantweb Optics determines customer licensing using a mixture of core-based licenses (Repository, Emerson Connectors, and CMMS) and user-based licenses (mobile join key tokens and augmented reality users).

location

A logical representation of an area in a facility. You determine how to organize your facility into locations using the ISA-95 Model in Plantweb Optics DataStudio.

log files

Plantweb Optics files that record all administrative and user actions. Emerson places these logs in a known file path (folders) location to assist Product Engineering and customers with troubleshooting.

Lua script

A decision logic and calculation engine that can provide advanced asset features to users. For example, performs automatic event message spam management or designates one or more asset as *out-of-service* during a scheduled maintenance or holiday period.

MassConfig

An Plantweb Optics DataStudio feature that helps you create, change, or delete multiple objects (assets). MassConfig helps you perform bulk editing by exporting objects to Microsoft® Excel, You change object properties in Excel, and finally import the objects back into Optics DataStudio.

Reference: Optics DataStudio - MassConfig

MongoDB

The name of the open-source, NoSQL database used as the data historian to archive data for Plantweb Optics. See *Data Repository*.

MTQQ

A lightweight, publish-subscribe network protocol that transports messages between devices. The protocol usually runs over TCP/IP; however, any network protocol that provides ordered, loss-less, bi-directional connections can support MQTT. It is designed for connections with remote locations where a *small code footprint* is required or the network bandwidth is limited.

network-based firewall

An application/appliance that 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. Emerson strongly recommends configuring a network-based firewall for each network layer.

object properties

The properties of an ISA-95 equipment object (asset) or other Plantweb Optics model object that distinguishes this object from other objects.

OSI PI

A developed and supported software used to capture, process, analyze, and store any form of real-time data. The PI System is a suite of software products used for data collection, transistorizing, finding, analyzing, delivering, and visualizing.

out of service assets

Another term for an *ignored* asset. Assets set to ignore their unhealthy status and any generated system messages, for a scheduled interval. When an asset is removed from production for scheduled maintenance, planned shutdown, holidays, or variation in usage patterns, it is "out of service." This functionality helps users to avoid unnecessary system-generated messages from temporarily out-of-commission equipment (assets).

All users see the list of displayed out of service assets. An asset can be designated as out of service by any user with administrative permissions. Health roll up calculations are unaffected by out of service assets. Their health though continues to be updated. The KPI unhealthy asset list and Dashboard does not display out of service assets. Events from out of service assets are not generated. A user can still create a user message bound to an out of service asset.

Plant Calendar

A term no longer used in Plantweb Optics and replaced by the term *scheduler item*. Used to schedule plant activities and events such as required maintenance outages or holidays. Out-of-service assets can be tied to one or more reoccurring schedules, as long as the schedules do not overlap. See *scheduler item*.

Plantweb Optics Connectors

Collectively includes Emerson Connectors (previously called ASIs), plus Open Standards and Protocols through the Plantweb Optics Connector service.

Plantweb Optics Portal

One of the client applications that retrieves information from the Optics Data Repository to display asset tracking and trend information. The Asset View visualization features are now a part of the Plantweb Optics Portal client, including messaging, collaboration, dashboard displays, and KPIs.

polling rates

Durations between acquiring new information for events, hierarchy, parameters, and asset calibration.

Power Bi

A collection of Microsoft software services, apps, and connectors that work together to turn unrelated data sources into coherent, visualizations and interactive insights. The data can be an Excel spreadsheet, or a collection of cloud-based and on-premises hybrid data.

Profiles

A Plantweb Optics object used with the DataStudio authentication to access the Profile Credentials.

recurrence pattern

How often a schedule should activate, whether hourly, daily, monthly, or yearly.

Relay

Also known as the *Relay Service*. It connects the Connector and Core services over multiple logical networks. The Relay allows you to install Plantweb Optics components on different physical networks, isolating functions behind firewalls and different network levels.

Reports

A major Plantweb Optics Portal page that displays columnar reports about key problem assets. Currently there is the **Bad Actors Report** and the **Out of Service Assets Report**. Each column in the reports can be sorted in ascending or descending order. The Bad Actors Report also can be filtered based on the previous, seven, 30, 60, or 90 days. The data listed in each report can be exported to a spreadsheet formatted file.

scheduler item

A calendar event with (**a**) a start date, (**b**) an end date, and (**c**) a recurrence pattern that defines how often the scheduled event happens (for example, `Monthly`, `Yearly`, and so forth).

In Plantweb Optics DataStudio there are multiple schedules that can control one or more events. For example, a scheduler item could define the start and end dates for the winter holidays. An administrator can assign one or more assets with the **Out of Service** property (value=`true`) to this schedule. Communication from the asset changes on the start date and end date of the schedule.

security mode policy

An OPC UA security setting that defines message signing and encryption using (**a**) `none`–no message encryption or signing (**b**) `sign`–messages digitally signed to prevent manipulation, (**c**) `sign & encrypt`–messages digitally signed and encrypted.

Server

Also referred to as the *Server service*. A Server that exposes data using OPC specifications. The Plantweb Optics OPC server allows any third-party client (such as, Movicon.NExT) to connect to Plantweb Optics and access the data source network. This server is installed with the Plantweb Optics installation, as part of the Plantweb Optics core components.

Server Model

A Core service that helps you manage external Server interfaces of Plantweb Optics and the assignment of other models to the particular Servers.

sharding

The practice of distributing data across multiple machines. In the Data Repository (MongoDB) it supports instances with large data sets and needed high throughput operations. The data is distributed across all shards allowing the workload to be evenly shared.

source

A reference to the asset which generated the event notification. This would be a device tag name (for example, FIC101), when the event pertains to a tag entering the level alarm condition.

spam

A Plantweb Optics process that automatically suppresses repeated events for a given asset . The administrator defines the number of repeated events allowed from an asset. Spam settings are system-wide and managed by an administrator.

tag (*noun*)

Basic elements of dynamic information that connect to programmable logic controllers (PLC) or field devices by using communication drivers to connect to the supervision project's objects and functions. It is also possible to select the "OPC UA Browser" tab from the Tag Browser window, through which you can access the list of available OPC UA Servers. An asset identification number is used by OPC UA Browser to identify data elements to integrate into a Movicon.NExT project.

Unified Architecture (UA)

A machine-to-machine communication protocol for industrial automation developed by the OPC Foundation.

user token policy

An OPC UA security setting that defines user identity using (**a**) Anonymous or no token, (**b**) a username and password token, or (**c**) an X.509 v3 certificate. When using Anonymous, the server requires no user identification and instead uses the client application certificate.

Web API

A fast and efficient Plantweb Optics API used by Portal and DataStudio clients, to access information in the Data Repository or from an external data source.

workspace

A storage structure that contains the configurations for all items used in a DataStudio session. Whenever a user logs in to DataStudio, they must specify a workspace to use or create a new workspace. Workspaces can be saved at any time when using DataStudio as an authenticated user. When you disconnect the current session or close DataStudio, you are asked if the workspace should be saved.

Index

T

U

W

Revision 03-11-2022
Rev. 01
2022

Emerson
1100 W Louis Henna Blvd
Round Rock, TX 78681 USA
www.Emerson.com