Web Client Installation Guide

Version 8.1.

Contents

Chapter 6: Post Installation Configuration (Docker and Non-docker) 68

Chapter 7: Troubleshooting 78

Chapter 8: Reference 82

Copyright GE Digital

© 2020 General Electric Company.

GE, the GE Monogram, and Predix are either registered trademarks or trademarks of General Electric Company. All other trademarks are the property of their respective owners.

This document may contain Confidential/Proprietary information of General Electric Company and/or its suppliers or vendors. Distribution or reproduction is prohibited without permission.

THIS DOCUMENT AND ITS CONTENTS ARE PROVIDED "AS IS," WITH NO REPRESENTATION OR WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO WARRANTIES OF DESIGN, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. ALL OTHER LIABILITY ARISING FROM RELIANCE UPON ANY INFORMATION CONTAINED HEREIN IS EXPRESSLY DISCLAIMED.

Access to and use of the software described in this document is conditioned on acceptance of the End User License Agreement and compliance with its terms.

Chapter

1

Installation Overview

Topics:

-

Installation Overview

Plant Applications Web Client contains two types of applications:

- Process: Contains the applications that are used in a process or continuous manufacturing model (for example, bottle or paper manufacturing).
- Discrete: Contains the applications that are used in a discrete manufacturing model (for example, motor or bike manufacturing).

The following methods of installation are available:

- Without using a Docker container: This is used to install Plant Applications Web Client for either Process, Discrete, or both applications. You can choose this method of installation if you want to perform a first-time installation to upgrade from a previous version of Plant Applications Web Client.
- Using a Docker container: This is used to install Plant Applications Web Client for both process and discrete applications. You can choose this method only for a first-time installation of Plant Applications.

To troubleshoot any issues during the installation or upgrade process, refer to the Troubleshooting section in this guide.

Chapter

2

Pre-installation Configuration (Docker and Non-docker)

Topics:

Configuring Apache CouchDB Settings

Before You Begin

- By default, CouchDB only runs on the local host using HTTP protocol. To ensure that CouchDB runs on HTTPS, you must execute the **config_couchDB.bat** file provided with ISO.
- Perform this step only for a fresh installation of Plant Applications Web Client version 8.1.
- CouchDB 2.3.1 must be installed on a Windows machine.

About This Task

Apache CouchDB is a document storage application that stores the documents used in discrete applications. Perform steps below to automate the configuration of CouchDB settings to work with Plant Applications. You can skip this procedure if you have already performed it.

Procedure

1. In a machine where CouchDB is installed, mount the ISO file for the Plant Applications Web Client or load the DVD if you created one from the ISO file for Plant Applications.
2. From the ISO root folder, run the **config_couchDB.bat** file using the System Administrator credentials. The command prompt window appears and prompts you for inputs.
3. Provide details for the following:

   - Path of the certificate file. For example, `C:\certs\server.crt`
   - Path of the key file. For example, `C:\certs\server.key`
   - Path where the CouchDB is installed. For example, `C:\CouchDB`

Results

If no error messages appear and when the command prompt window closes, that is an indication that Apache CouchDB settings are configured. You can view all the changes that you have made by accessing `https://<host name or IP address of Apache CouchDB>:<port number>/_utils/`

Chapter

3

Installing Plant Applications Web Client Without Using Docker

Topics:

About Installing Plant Applications Web Client Without Using Docker

Installing Plant Applications Web Client without using a docker container installs both the process and discrete applications. You must perform this type of installation if you want to upgrade from a previous version of Plant Applications. You can choose this method for a first-time installation as well.

About Preinstallation Requirements

Review the following preinstallation requirements before you run the Plant Applications Web Client installer:

- System requirements
- Port requirements
- Software requirements
- Plant Applications Server Requirements
- Plant Applications Message Bridge Requirements

System Requirements

Ensure that your computer meets the system requirements as described in the following table. For more information, refer to the System Requirements section in the *Plant Applications Getting Started Guide* document for the latest Plant Applications release.

Item	Version
GE Operations Hub 1.7	Operations Hub 1.7 **Note:** You can select an external UAA application while installing Operations Hub. However, if you do not select the external UAA, by default, Operations Hub installs UAA.
Web browsers	Chrome 80.0 or later , with minimum resolution 1366x768. **Devices**: • **iPad**: Safari v13.1+, Chrome 80.0 or later with resolution 2048x1536 • **HP tablet**: Chrome 80.0 or later , with minimum resolution 1920x1280 **Note:** Devices supports only Unit Operations,Work Queue, and Non Conformance applications. .
Operating system	64-bit Windows 10, Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019
Microsoft Visual C++	Microsoft Visual C++ 2015 Redistributable packages to be installed on the Web Client node.
Framework	Microsoft[®] .NET Framework 4.7 or later

Item	Version
SQL server	SQL server 2016 (64-bit), 2017 (64-bit), or 2019 (64-bit and with mandate Cumulative Update 4 installed)
	Note: Ensure that you have configured the SQL server database as the Plant Applications database. For more information, refer to the *Plant Applications Getting Started Guide* for the latest release.
Couch DB server	CouchDB version 2.3.1 installed and configured on a Windows machine.
	Note: For more information on configuring CouchDB, refer to Configuring Apache CouchDB Settings on page 4.
Hard drive	100 GB (minimum)
Processor	2.4 GHz clock-speed Intel Core i3, i5, or i7 CPU or equivalent AMD Phenom CPU with 16 GB RAM
	Note: For better performance, it is recommended to use a quad core (4-cores) processor for Process applications and octa core (8-cores) for Discrete or both applications.
Memory	16 GB (recommended)
	Note: You must have 32 GB or more if you plan to install Web Client (Both Process and Discrete), Historian, Operations Hub, Plant Applications, Message Bridge on the same node. However, it is recommended to install them in a distributed environment.

Port Requirements

Ensure that the ports described in the following table are opened before you install Plant Applications Web Client.

Port	Description
15672	The default port for the RabbitMQ Message bridge required to communicate with the Plant Applications server for retrieving data updates.
8444	The default port for the Tomcat server.
1433	The default port for the Microsoft SQL server.
9095	The default port for Kafka.
2185	The default port for ZooKeeper.

Software Requirements

The installer identifies all available and missing software packages required before installing the Plant Applications Web Client.

You must install the following software packages before you run the installer:

• Microsoft OLE DB Driver 18 for SQL Server

Note: You can download the Microsoft OLE DB Driver 18 for SQL Server from the following URL: https://www.microsoft.com/en-us/download/details.aspx?id=56730.

If you do not install Microsoft OLE DB Driver 18 for SQL Server, the following screen appears, and the installation is stopped.
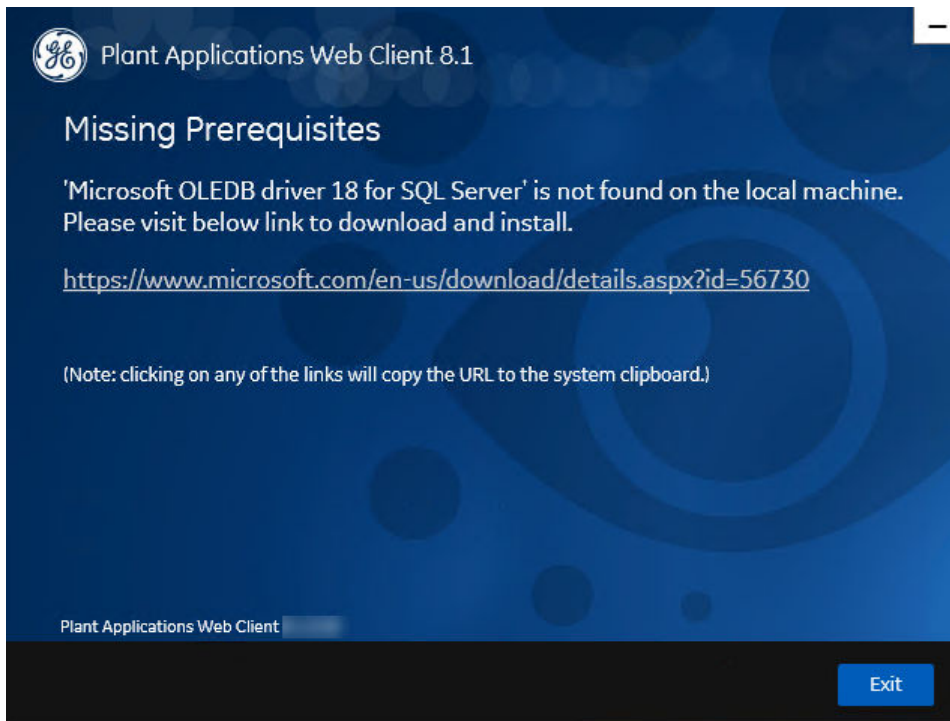
If any of the following required software packages are not already installed on your computer, the installer installs them automatically:

- Apache Tomcat version 9.0.35
- Ruby 2.3.3
- Ruby DevKit version 4.65.0.0

   Note:

   Ruby is required because the UAA Command Line Interface (UAAC) is dependent on Ruby.
- NodeJS 8.12
- Python 2.7.2
- OpenJDK 1.8

Plant Applications Server Requirements

Ensure that the Plant Applications Server 8.1 is installed. For more information, refer to the *Plant Applications Getting Started Guide* for the latest release.

Install Operations Hub

For instructions, refer to the Operations Hub installation Guide provided along with the Operations Hub installation package.

Plant Applications Message Bridge Requirements

GE recommends that you configure the RabbitMQ Message Bridge in the Plant Applications server before installing the Plant Applications Web Client. For more information, refer to the Installing the Plant Applications Message Bridge section in the *Plant Applications Getting Started Guide*.

Install the Plant Applications Web Client Without Using Docker

About This Task
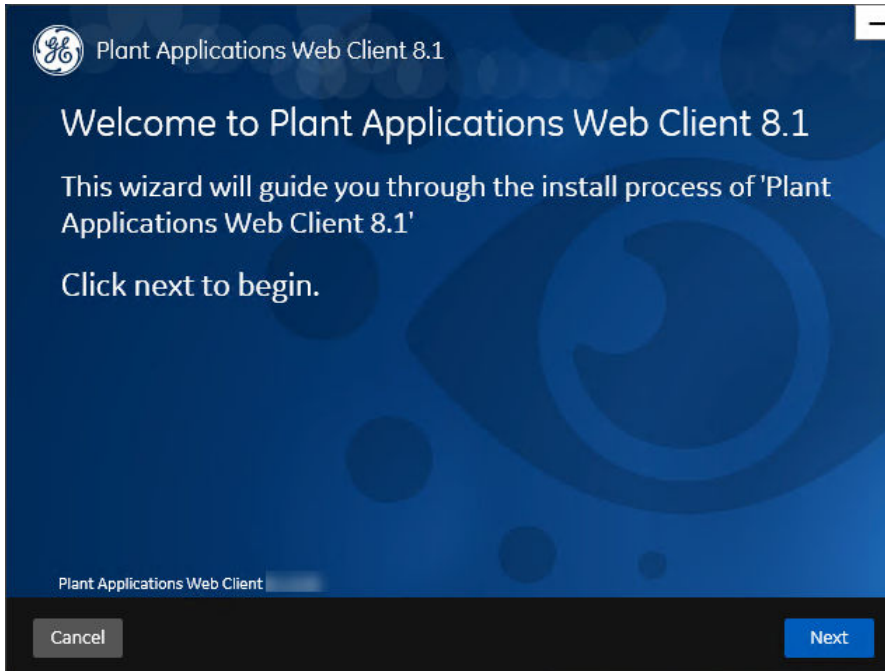
Perform the preinstallation tasks.

Procedure

1. Mount the ISO file for the Plant Applications Web Client or load the DVD if you created one from the ISO file on the application server for Plant Applications.
2. Run the `installfrontend.exe` file as an Administrator.
   The installation menu appears, displaying the **Install Proficy Plant Applications 8.1** screen.
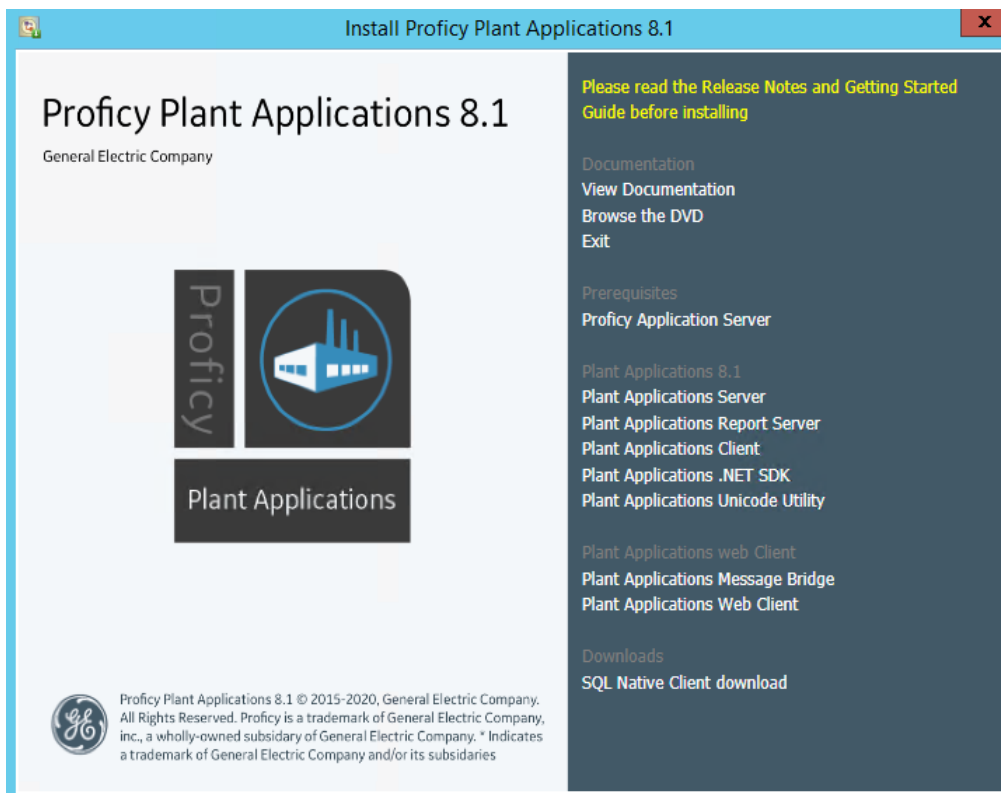
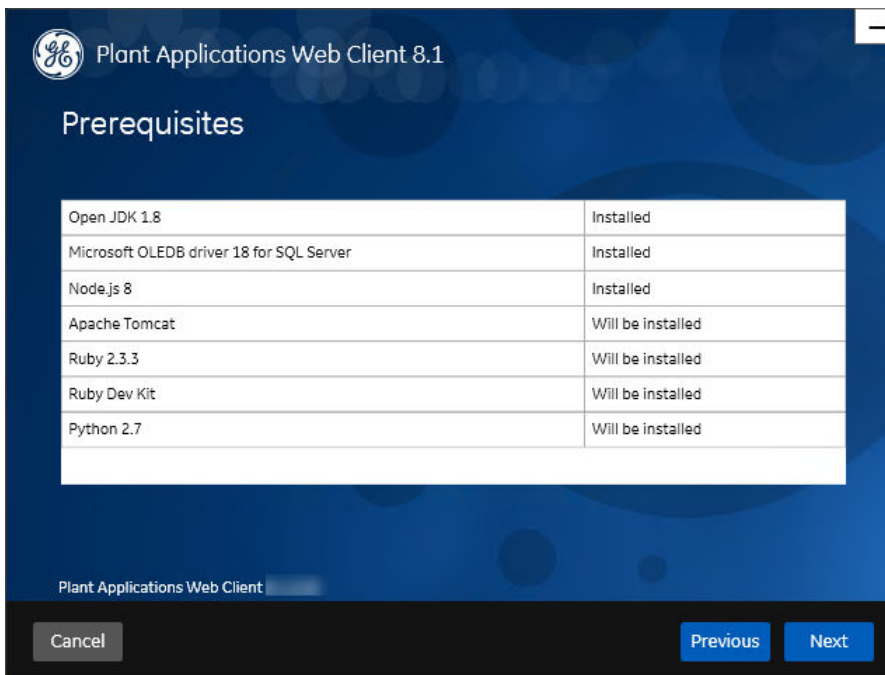> **Tip:** You can hover over each task that appears in the installation menu to refer to the tooltip associated with that task.

> **Note:** Ensure that you have installed the Microsoft Visual C++ 2015 Redistributable (64-bit) package.

3. Select **Plant Applications Web Client 8.1**.
   The Plant Applications Web Client installation wizard appears, displaying the **Welcome to Plant Applications Web Client 8.1** screen.

4. In the **Welcome to Plant Applications Web Client 8.1** screen, select **Next**.
   The **Prerequisites** screen appears.

Open JDK 1.8	Installed
Microsoft OLEDB driver 18 for SQL Server	Installed
Node.js 8	Installed
Apache Tomcat	Will be installed
Ruby 2.3.3	Will be installed
Ruby Dev Kit	Will be installed
Python 2.7	Will be installed

Note: If Microsoft OLE DB Driver 18 for SQL Server or later is not installed, the **Missing Prerequisites** screen appears informing you to install the required version of the missing software before you run the installer. You must exit the installation, and first install the required software.

5. In the **Prerequisites** screen, select **Next** to view all installed prerequisites and install any missing prerequisites.
   The **Read and accept the license agreement to continue** screen appears.
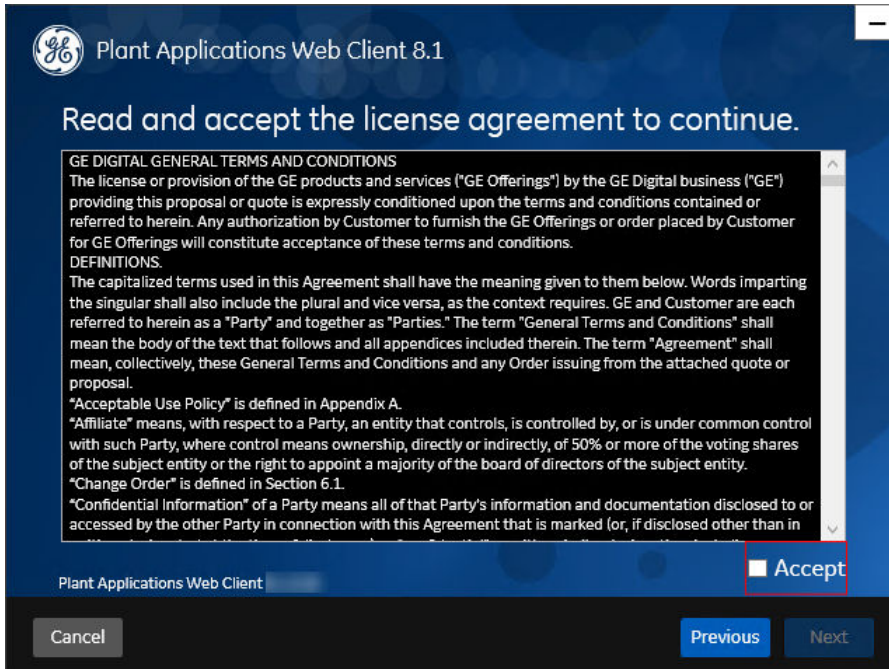
6. Read the license agreement, select **Accept**, and then select **Next** to continue the installation. The **Operations Hub Credentials** screen appears.


7. In the **Operations Hub Credentials** screen, enter the credentials to access the Operations Hub server as described in the following table.

| Credential	Description
Server Name	This field is automatically populated with the local host name, fully qualified host name, or IP address, based on the configuration in Operations Hub. You can edit the host name of the Operations Hub server based on requirement.
	Note: Instead of IP address, it is recommended to use the Operations Hub host name (computer name).
Port	Enter the Operations Hub port number.
Tenant Username	Enter the tenant Hub username to access the Operations Hub server instance.
	Note: The default user name is `OphubAdmin`.
Tenant Password	Enter the password for the user name you entered in the **Tenant Username** box.
	Note: The tenant username and password must be same as the credentials that you have specified during the Operations Hub installation.

If all the options are entered correctly, the **Next** button is enabled.

8. Select **Next** to continue with the installation.
   The **Installation Directory** screen appears with the default installation directory selected as `C:\Program Files\GE Digital\PlantApplicationsWebClient`.
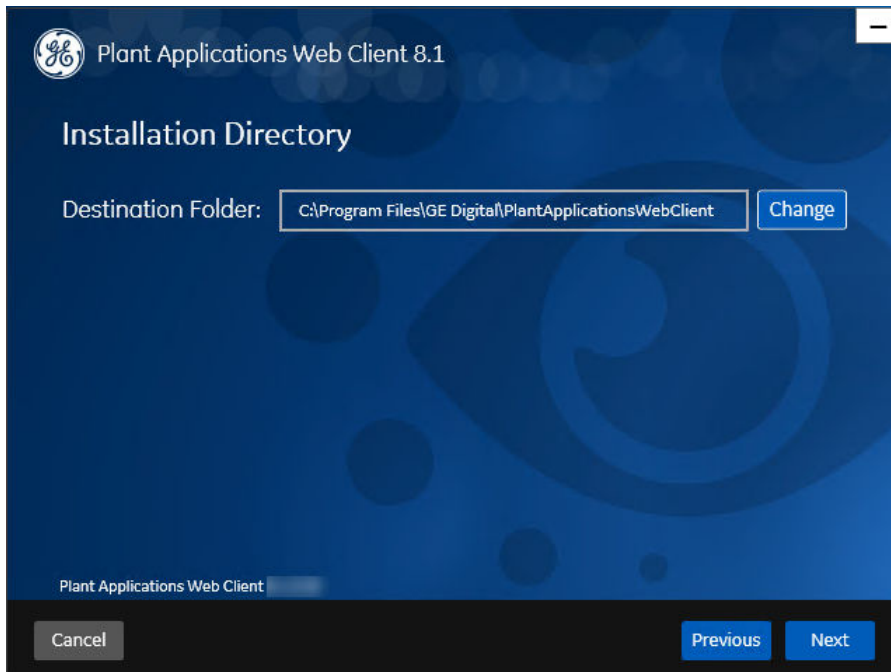
9. **Optional:** In the **Destination Folder** box, select **Change** to browse and select the directory where you want to install the Plant Applications Web Client.

   Note: Do not use the user profile folder for installation.
10. In the **Installation Directory** screen, select **Next**.
    The **Install Model Selection** screen appears.
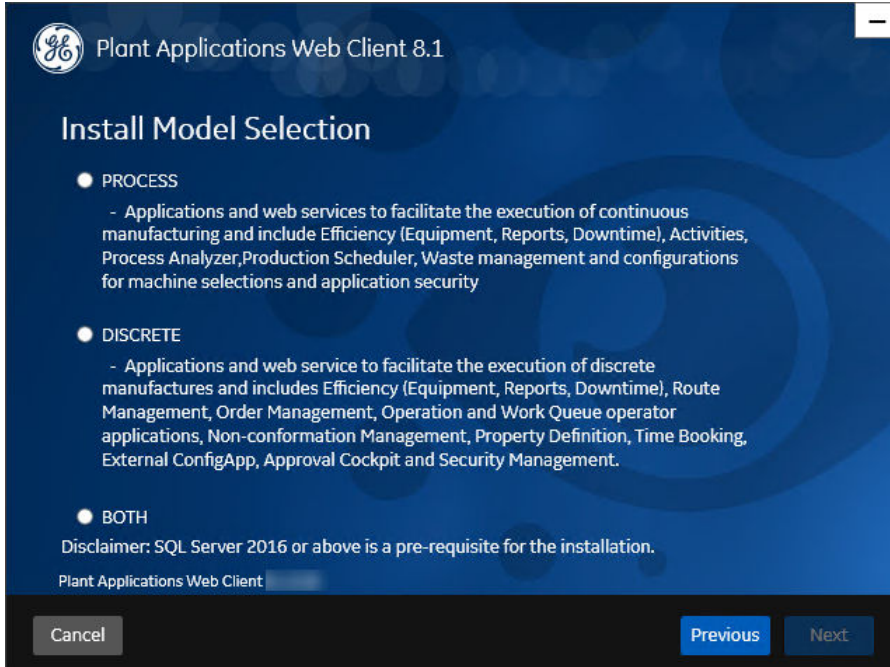
11. In the **Install Model Selection** screen, select any of the following options based on the requirement.
    - PROCESS: Installs only the Process applications along with the web services.
    - DISCRETE: Installs only the Discrete applications along with the web services.
    - BOTH: Installs both the Process and Discrete applications.

12. Select **Next**.
    The **UAA Credentials** screen appears.

13. In the **UAA Credentials** screen, enter the credentials to access the UAA server as described in the following table.

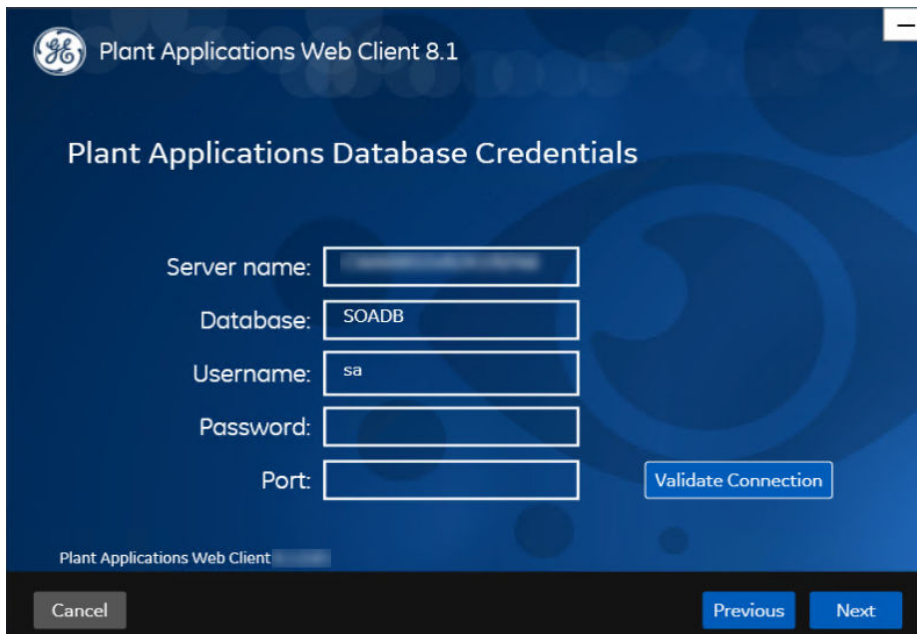| Credential	Description
Server Name	Enter the host name of the UAA server. **Note:** Instead of IP address, it is recommended to use the UAA host name (computer name).
Port	Enter the UAA port number.
Admin Client ID	Enter the admin Client ID to access the UAA server instance. **Note:** The default user name is `admin`.
Admin Client Secret	Enter the Client Secret for the user name you entered in the **Admin Client ID** box.
Validate	Select **Validate** to validate the UAA server connection. **Note:** The following table describes each icon indicating a validation status that might appear during the validation process.

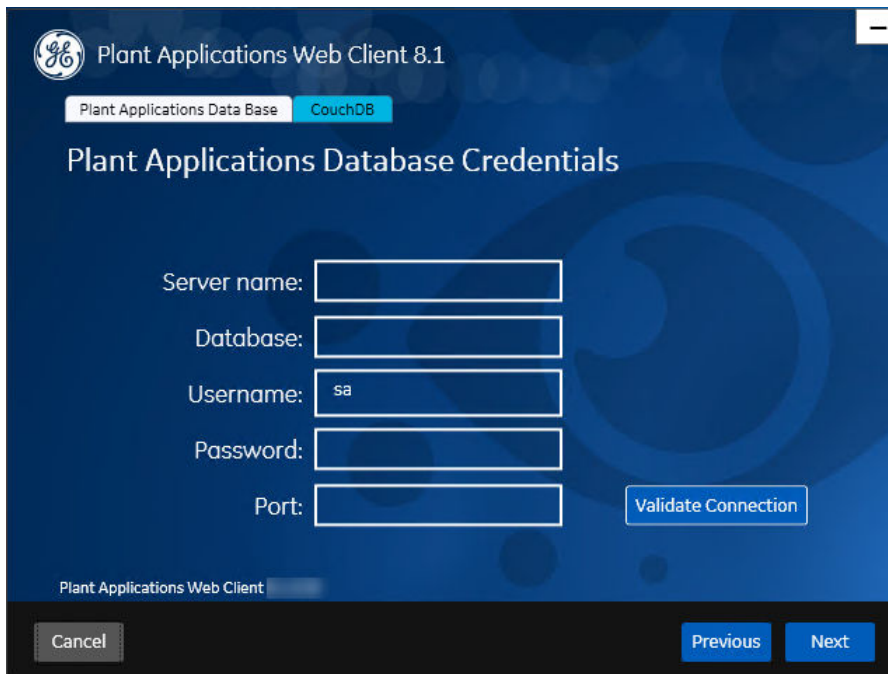| Icon	Description
⚙	Indicates that the validation is in progress.
✔	Indicates that the validation was successful.
✖	Indicates that the validation was unsuccessful. In this case, make sure you enter the correct password.

If all the options are entered correctly, the **Next** button is enabled.

14. Select **Next**.

The **Plant Applications Database Credentials** screen appears.

Note: If you have selected either DISCRETE or BOTH in the **Install Model Selection** screen, the following screen appears that allows you to enter the Couch DB details.

15. In the **Plant Applications Database Credentials** screen, in the Plant Applications Data Base section, enter the Plant Applications database credentials as described in the following table.

Credential	Description
Server name	Enter the server name where the Plant Applications database is installed in the format $HOST\_NAME \backslash INSTANCE$. Where $HOST\_NAME$ is the host name (either a fully qualified domain name or IP address, of the server) and $INSTANCE$ is the instance of the server used by the database. **Note:** If there is no instance for the server, you can enter $HOSTNAME$ as the server name. $Localhost$ is not an acceptable value for $HOSTNAME$.
Database	Enter the name of the Plant Applications database that you want to connect with the Plant Applications Web Client.
Username	Enter the user name that has permissions to access the database you entered in the **Database** box. By default, the user name appears as sa.
Password	Enter the password for the user name you entered in the **Username** box.
Port	Optional: Enter the number of the port that the instance uses to listen for client connections. **Note:** The default port is 1433.

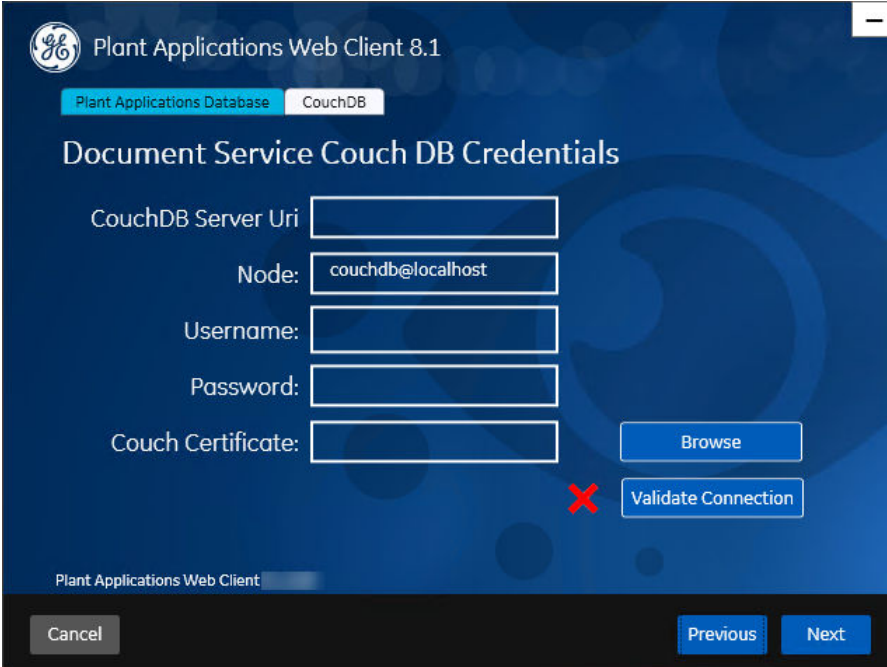16. Select **Validate Connection** to validate the database connection.

Note: The validation process takes some time to check whether a compatible version of the Plant Applications server is installed.

The following table describes each icon indicating a validation status that might appear during the validation process.

Icon	Description
⚙	Indicates that the validation is in progress.
✅	Indicates that the validation was successful.
❌	Indicates that the validation was unsuccessful. In this case, make sure you enter the correct password.

If you have selected PROCESS in the **Install Model Selection** screen and the database connection is successfully validated, the **Next** button is enabled. Skip to **Step 19**.

17. If you have selected either DISCRETE or BOTH in the **Install Model Selection** screen, in the **Plant Applications Database Credentials** screen, select the **CouchDB** tab.
The **Document Service Couch DB Credentials** screen appears.

18. In the **Document Service Couch DB Credentials** screen, enter the Couch DB credentials as described in the following table.

Credential	Description
CouchDB Server Uri	Enter the fully qualified web address of Apache CouchDB in the format: `https://<host name or IPaddress>:<port number>`.
Node	Enter the name of the node where Apache CouchDB is running. By default, the node value appears.
Username	Enter the user name of the administrator that has permissions to access the database you entered in the **Database** box.
Password	Enter the password for the user name you entered in the **Username** box.

Credential	Description
Couch Certificate	Select **Browse** to locate the Apache CouchDB server certificate (couch_server.crt) that you have generated and upload it.
Validate	Select **Validate** to validate the Apache CouchDB database credentials. **Note:** The following table describes each icon indicating a validation status that might appear during the validation process.

Icon	Description
⚙	Indicates that the validation is in progress.
✅	Indicates that the validation was successful.
❌	Indicates that the validation was unsuccessful. In this case, make sure you enter the correct password.

If the Apache CouchDB database connection is successfully validated, the **Next** button is enabled.

19. Select **Next**.

The **Plant Applications Administrator User Credentials** screen appears.

20. In the **Plant Applications Administrator User Credentials** screen, enter the Plant Applications Administrator credentials as described in the following table.
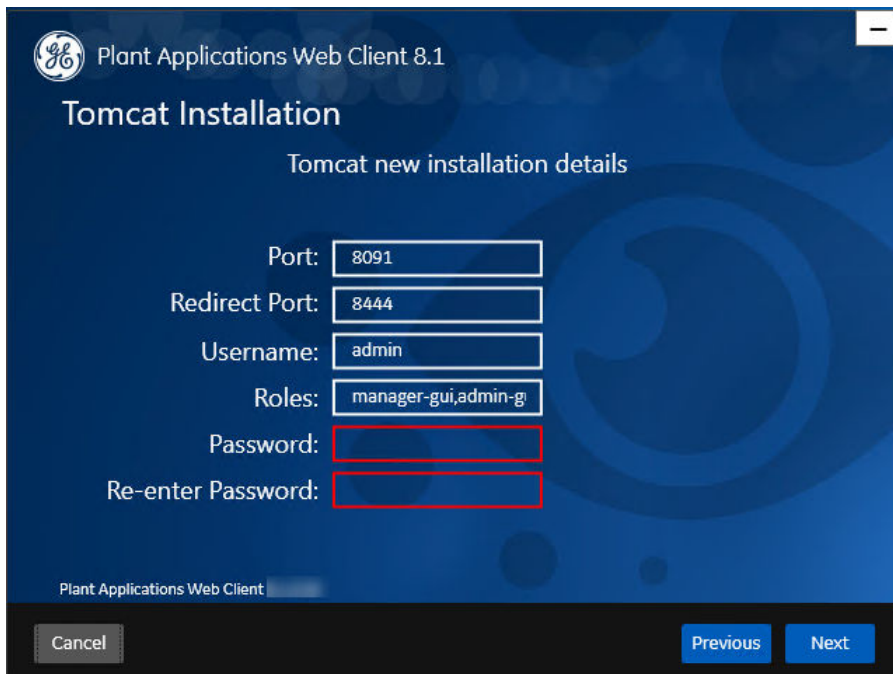
Note: Ensure that the user credentials entered here must exist in Plant Applications Server with an administrator role defined and you must use the same credentials to login into the Web Client applications.

Credential	Description
User Name	Enter the user name for an administrator account in Plant Applications.
Password	Enter the password for the user name you entered in the **User Name** box.
Validate	Select **Validate** to validate the Plant Applications Administrator credentials. **Note:** The following table describes each icon indicating a validation status that might appear during the validation process.

Icon	Description
⚙	Indicates that the validation is in progress.
✔	Indicates that the validation was successful.
✖	Indicates that the validation was unsuccessful. In this case, make sure you enter the correct password.

If the Plant Applications Administrator connection is successfully validated, the **Next** button is enabled.

21. Select **Next**.
    The **Tomcat Installation** screen appears.

22. In the **Tomcat Installation** screen, enter the Tomcat installation details for a new or existing installation as described in the following table. The installer prompts you to enter details for an existing Tomcat if the Tomcat installation details are available in the registry settings for the Plant Applications Web Client on your computer. Else, the installer prompts you to enter details for a new installation of Tomcat.

Installation Detail	Description
Port	Enter the HTTP port that Tomcat uses to listen for client connections. **Note:** The default port is 8081.
Redirect Port	Enter the HTTPS port that Tomcat uses to redirect all HTTP requests to this port. **Note:** The default redirect port is 8444.
Username	Enter the user name to access Tomcat. **Note:** The default user name is admin.
Roles	Skip this box because it is automatically populated.
Password	Enter the password for the user name you entered in the **Username** box.
Re-enter Password	Reenter the password for the user name entered in the **Username** box. **Note:** This box appears only when a new installation of Tomcat is initiated by the installer.

23. Select **Next**.
    The **RabbitMQ Credentials** screen appears.

24. In the **RabbitMQ Credentials** screen, perform one of the following steps:

    • Enter the RabbitMQ credentials for the machine that hosts your Plant Applications message bridge as described in the following table, and then select **Validate Connection**.

Credential	Description
Server name	Enter the computer name or IP address that hosts your Plant Applications Message Bridge.
Username	Enter the Administrator's user name that you set during Plant Applications Message Bridge installation.
Password	Enter the password for the Administrator's user name you entered in the **Username** box.

The following table describes each icon indicating a validation status that might appear during the validation process.

Icon	Description
⚙	Indicates that the validation is in progress.
✔	Indicates that the validation was successful.
✖	Indicates that the validation was unsuccessful. In this case, make sure you enter the correct password.

25. Select **Next**.
The **Kafka Credentials** screen appears.

Note: You must provide the Kafka and Zookeeper details that were defined during the Message Bridge installaton.

26. In the **Kafka Credentials** screen, enter the credentials to access the Kafka server as described in the following table.

Credential	Description
Server Name	Enter the host name of the Kafka server.
	Note: Instead of IP address, it is recommended to use the Kafka host name (computer name).
Kafka Port	Enter the Kafka port number.
Validate	Select **Validate** to validate the Kafka server connection.
	Note: The following table describes each icon indicating a validation status that might appear during the validation process.

Icon	Description
⚙	Indicates that the validation is in progress.
✅	Indicates that the validation was successful.
❌	Indicates that the validation was unsuccessful. In this case, make sure you enter the correct password.

Credential	Description
Zookeeper Client Port	Enter a valid Zookeeper Client port number.

If all the options are entered correctly, the **Next** button is enabled.

27. Select **Next**.

The **You are ready to install** screen appears.
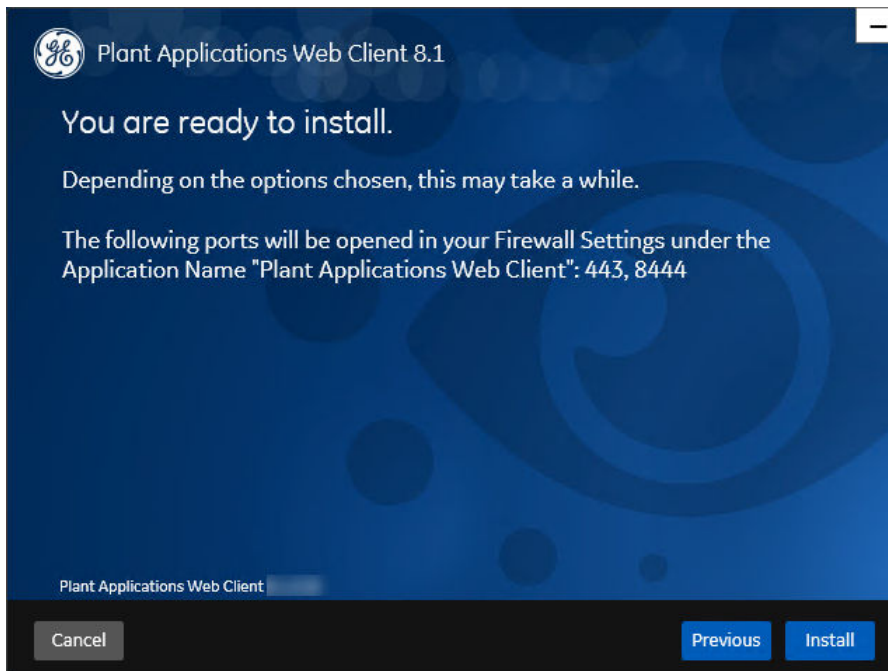
28. Select **Install**, and then wait for the installation to complete.

Depending on the options selected, the installation process may take some time. On successful installation, the **Installation Successful** screen appears.
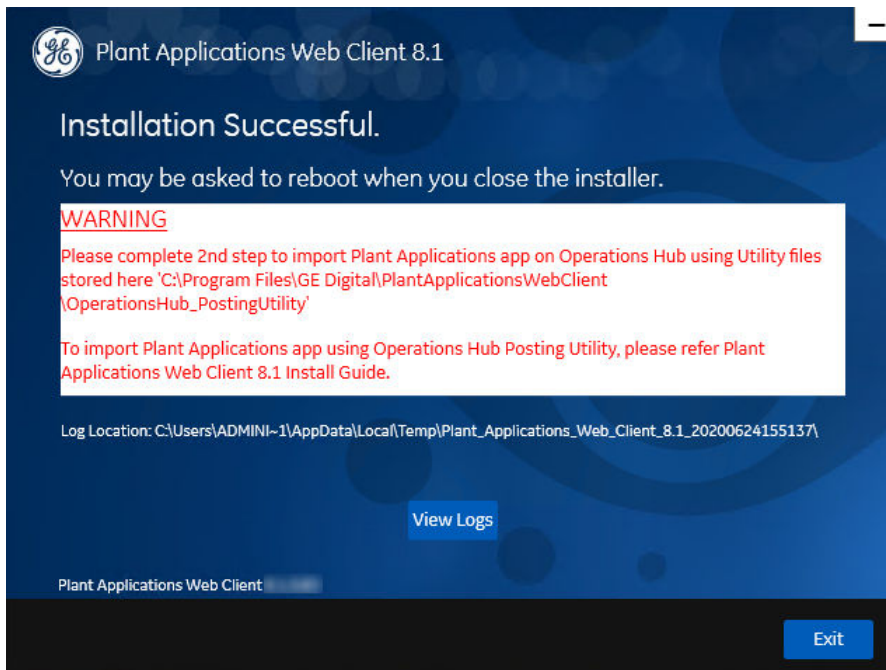
29. **Optional:** Select **View Logs** to see the installation details.
30. In the **Installation Successful** screen, select **Exit** to close the wizard.
    The Plant Applications Web Client is successfully installed on your computer.

    Remember: If you upgrade JAVA later, it might create some issues in using the Plant Applications Web Client. To resolve this issue, refer to the Community article 000020691 in the support site http://support.ge-ip.com.
31. Run Operations Hub Posting Utility on page 69 to import the Plant Applications into the Operations Hub.

Next Steps

Perform the post-installation steps.

About Post-Installation Tasks

Based on your requirements, perform the following post-installation tasks:

- Add a UAA user.
- Configure a GE Proficy Historian Server for the Analysis application.
- Configure the cache settings for the Historian tags used in the Analysis application.

Add a UAA User

About This Task

You must add User Authentication Service (UAA) users to access the Plant Applications Web Client.

Before You Begin

Ensure that you modify the `PA_UAA_Config_Win.bat` file to add the user details.

Procedure

1. Log in to the computer where you installed the Plant Applications Web Client.
2. Select **Start**, and then search for the Command Prompt application.
3. In the search results, right-click **Command Prompt**, and then select **Run as administrator**.
4. In the command prompt, modify the directory path to the path where the `PA_UAA_Config_Win.bat` file is located.

    Note: By default, the `PA_UAA_Config_Win.bat` file is located in the Plant Applications Web Client installation directory.

5. In the command prompt, enter `PA_UAA_Config_Win.bat`.
6. Press Enter to run the `PA_UAA_Config_Win.bat` file.

Results

The user is added as a UAA user to the Operations Hub UAA with an access level you set for the user in the `PA_UAA_Config_Win.bat` file.

Modify the Batch File to Add the User Details

About This Task

You can use the `PA_UAA_Config_Win.bat` file located in the Plant Applications Web Client installation directory to add a Web Client user as a User Authentication Service (UAA) user and set the access level as `bm-line-leader` or `bm-operator`. The access levels `bm-line-leader` and `bm-operator` are defined in the Plant Applications Administrator. The `PA_UAA_Config_Win.bat` file associates a user for the access levels as described in the following table.

Access Levels	Default User
`bm-operator`	`<user name created during installation>`
`bm-line-leader`	`bm_lineleader_1`

Procedure

1. In the Plant Applications Web Client installation directory, open the `PA_UAA_Config_Win.bat` file using a text editor.
2. Depending on the access level, identify each instance of the default user, and then replace the default user with the required user name.

    For example, if the user name is `john` and you want to define `bm_operator` as the access level, replace the instances of `<user name created during installation>` with `john` as shown in the following table.

Original Code Snippet	Modified Code Snippet
`call uaac user add <user name created during installation> -p test --emails <user name created during installation>@xx.com`	`call uaac user add john -p test --emails john@xx.com`
`call uaac member add trend_client.read <user name created during installation>`	`call uaac member add trend_client.read john`
`call uaac member add trend_client.write <user name created during installation>`	`call uaac member add trend_client.write john`
`call uaac member add bm-operator <user name created during installation>`	`call uaac member add bm-operator john`
`call uaac member add historian_rest_api.read <user name created during installation>`	`call uaac member add historian_rest_api.read john`
`call uaac member add historian_rest_api.write <user name created during installation>`	`call uaac member add historian_rest_api.write john`

Similarly, if the user name is `lisa` and you want to define `bm_lineleader` as the access level, replace the instances of `bm_lineleader_1` with `lisa` as shown in the following table.

Original Code Snippet	Modified Code Snippet
`call uaac user add bm_lineleader_1 -p test --emails bm_lineleader_1@xx.com`	`call uaac user add lisa -p test --emails lisa@xx.com`
`call uaac member add bm-line-leader bm_lineleader_1`	`call uaac member add bm-line-leader lisa`

3. Save your changes to the `PA_UAA_Config_Win.bat` file.

Results

The `PA_UAA_Config_Win.bat` file is modified with the required user details.

Configure a GE Proficy Historian Server for the Analysis Application

About This Task

The Analysis application supports plotting of Historian tags from a GE Proficy Historian Server SP5 or later versions only. You can configure a maximum of 10 remote or native GE Proficy Historian Servers in the `application.properties` file for the Analysis application.

To configure one or more GE Proficy Historian Servers for the Analysis application, follow these steps:

Procedure

1. In the directory *<tomcat_home>*`/Apache Software Foundation/Tomcat 9.0/webapps/ mes-dataservice-impl-`*<version>*`/WEB-INF/classes,` access the `application. properties` file by using a text editor. Where:

   - *<tomcat_home>*: Is the directory where you installed Apache Tomcat. For example, `C:/Program Files`.
   - *<version>*: Is the version of the `mes-dataservice-impl` microservice created during the installation of the Plant Applications Web Client. For example, `0.6.7`.

2. Enter the properties and their details for each GE Proficy Historian Server as described in the following table.

Property	Description
`hist`*<n>*`.service.origin`	Enter the IP address of the GE Proficy Historian Server. For example, `10.181.213.204`.
`hist`*<n>*`.service.port`	Enter the port number on which the GE Proficy Historian Server is installed.
	Tip: You can leave this property blank if the GE Proficy Historian Server is installed on the default port 8443.
`hist`*<n>*`.service.hostname`	Enter the host name of the GE Proficy Historian Server as configured in the Plant Applications Administrator. For example, `GESERVER`.
`hist`*<n>*`.service.client_id`	Enter the client id of the Historian Administrator.
	- Historian 7.0: **admin** is the default.
	- Historian 8.0 or later: **<hostname.admin>** where the host name is the name of the server where the Historian web tools are installed.
`hist`*<n>*`.service.client_secret`	Enter the client secret of the Historian Administrator.
`hist`*<n>*`.uaa.origin`	Enter the IP address of the UAA server.
`hist`*<n>*`.uaa.port`	Enter the port number on which the UAA server is installed.

Note: In the **Property** column, in each entered property, *<n>* represents a numeric value between 1 and 10 indicating the count of the Historian Server configured in the file. For example, `hist1.service.origin`, `hist2.service.origin`, and so on.

3. Save changes to the `application.properties` file.
4. Restart `mes-dataservice-impl-0.6.7` and `processanalyzer-service-impl-0.6.7` to apply the changes.

Results

The configured GE Proficy Historian Servers appear in the Analysis application.

Configure the Cache Settings for the Historian Tags

About This Task

The Analysis application supports the caching and refreshing of the cached Historian tags after certain time interval. You configure the duration of the saved cached Historian tags in the `application.`

properties file of the `mes-dataservice-impl` and `processanalyzer-service-impl` microservices for the Analysis application. After the set duration, the Historian tags are cached again.

Procedure

1. In the directory `<tomcat_home>/Apache Software Foundation/Tomcat 9.0/webapps/mes-dataservice-impl-<version>/WEB-INF/classes`, access the `application.properties` file by using a text editor. Where:

   - *<tomcat_home>*: Is the directory where you installed Apache Tomcat. For example, `C:/Program Files`.
   - *<version>*: Is the version of the `mes-dataservice-impl` microservice created during the installation of the Plant Applications Web Client. For example, `0.6.2`.

2. Enter the properties and their details as described in the following table.

Property	Description
`historianTagMaxCacheSize`	Enter the maximum cache size in KB. The default value is `50000`. Example: `historianTagMaxCacheSize=50000`
`historianTagCacheTimeOut`	Enter the duration in the format `duration<timeformat>` after which the cached Historian tags are cleared by the `mes-dataservice-impl` microservice. Where: `<timeformat>` is h, m, or s to indicate time in hours, minutes, or seconds, respectively. The default value is `6h`. Example: `historianTagCacheTimeOut=6h`
`scheduler.tagcaching.seconds`	Enter the duration in seconds after which the Historian tags are cached again by the `mes-dataservice-impl` microservice. The default value is `21600`. Example: `scheduler.tagcaching.seconds=21600`

Note: The value you enter for the `historianTagCacheTimeOut` and `scheduler.tagcaching.seconds` properties must of the same duration you enter for the `tagVariableCacheTimeOut` property in the `processanalyzer-service-impl` microservice.

3. Save the changes to your file.
4. In the directory `<tomcat_home>/Apache Software Foundation/Tomcat 9.0/webapps/processanalyzer-service-impl-<version>/WEB-INF/classes`, access the `application.properties` file by using a text editor. Where:

   - *<tomcat_home>*: Is the directory where you installed Apache Tomcat. For example, `C:/Program Files`.
   - *<version>*: Is the version of the `processanalyzer-service-impl` microservice created during the installation of the Plant Applications Web Client. For example, `0.6.2`.

5. For the `tagVariableCacheTimeOut` property, enter the duration in the format `duration<timeformat>` after which the tags are cached again. Where: `<timeformat>` is h, m, or s to indicate time in hours, minutes, or seconds, respectively. The default value is `6h`. Example: `tagVariableCacheTimeOut=6h`

Note: The value you enter for the `tagVariableCacheTimeOut` property must be of the same duration you enter for the `historianTagCacheTimeOut` and `scheduler.tagcaching.seconds` properties in the `mes-dataservice-impl` microservice.

6. Save the changes to your file.
7. Restart Tomcat to apply the changes.

Results

The cached tags are refreshed after the duration you set in the `application.properties` file of the `mes-dataservice-impl` and `processanalyzer-service-impl` microservices for the Analysis application.

Performance Tuning Settings

About This Task

Here are the recommended performance tuning settings for your environment to achieve optimal performance.

Procedure

1. Update Tomcat default threads.

   a) Navigate to **C:\Program Files\Apache Software Foundation\Tomcat 9.0\conf**
   b) Open the **Server.xml** file in Notepad. In **Server.xml**, search for the line **102** or **<Connector protocol="org.apache.coyote.http11.Http11NioProtocol" maxThreads="150"**
   c) Change the max thread count to **800** (maxThreads="800").
   d) **Save** the file.

2. Update JVM memory settings.

   a) Navigate to **C:\Program Files\Apache Software Foundation\Tomcat 9.0\bin** and then run **Tomcat8w.exe**.
   b) Select the **Java** tab.
   c) Enter the following recommended values:

      • **Initial memory pool:** 4096 MB
      • **Maximum memory pool:** 4096 MB
      • **Thread stack size:** Leave this field empty

   d) Select **OK**.
   e) **Stop** and **Start** Tomcat.

3. Update database settings:

   a) Update the **Cost Threshold for Parallelism** value:

      i. Open SSMS connect to the instance, where SOA db is deployed.
      ii. Select the instance. Now, right-click on the instance and then select **Properties**.
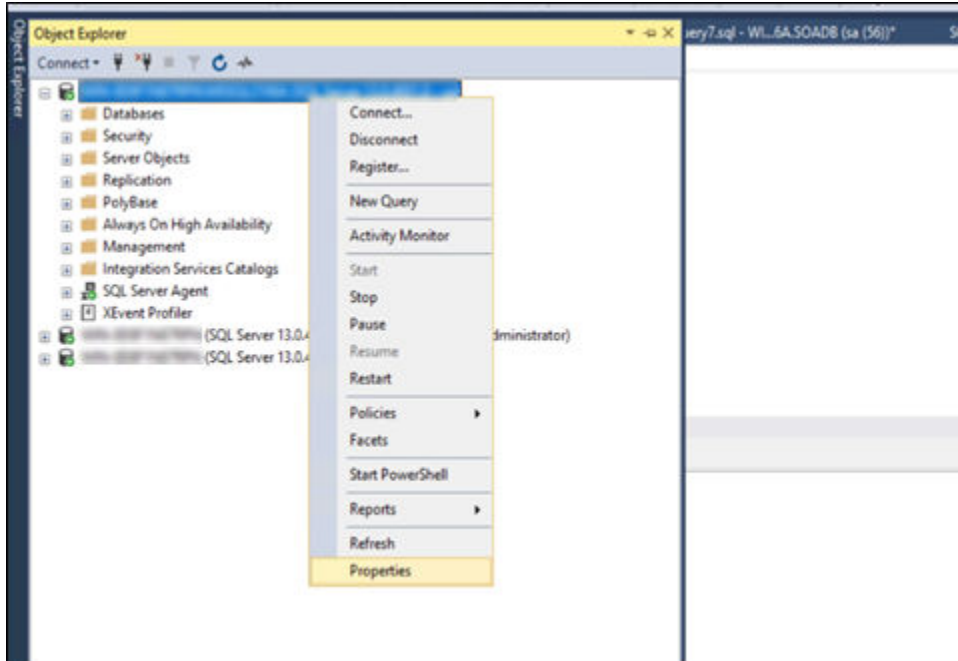
iii. Select the **Advanced** tab. In the **Parallelism** section, in the **Cost Threshold for Parallelism** box, change the default value from **5** to **25**.
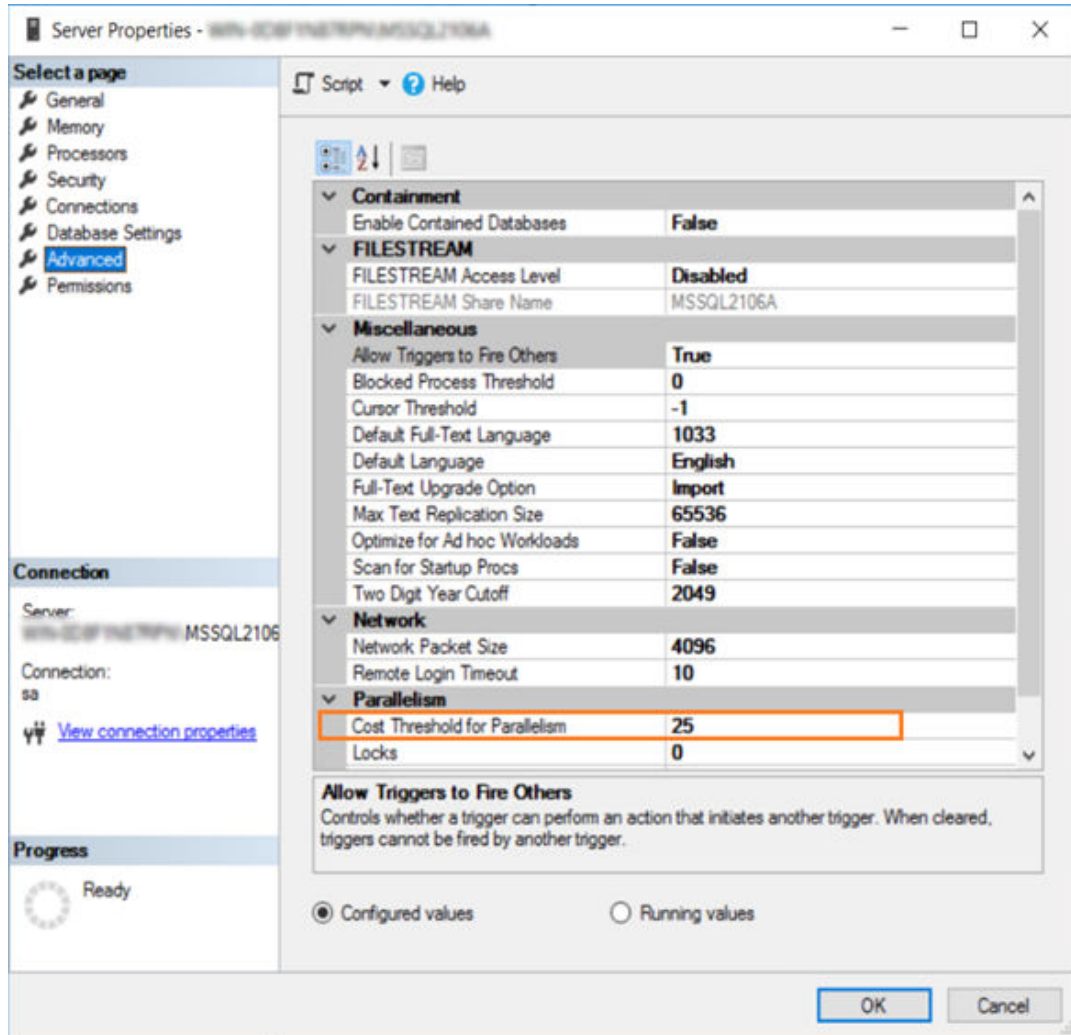
b) Ensure that statistics (sp_updatestats) is updated in the database.

c) It is recommended to move the transaction logs to a different drive to optimize disk I/O performance.

Node Application Manager Utility

About This Task

Node Application Manager is a simple utility that displays the health of the UI micro applications in a dashboard. You can use this utility to stop or restart the applications if you are not able to access them in the universal client from the browser.
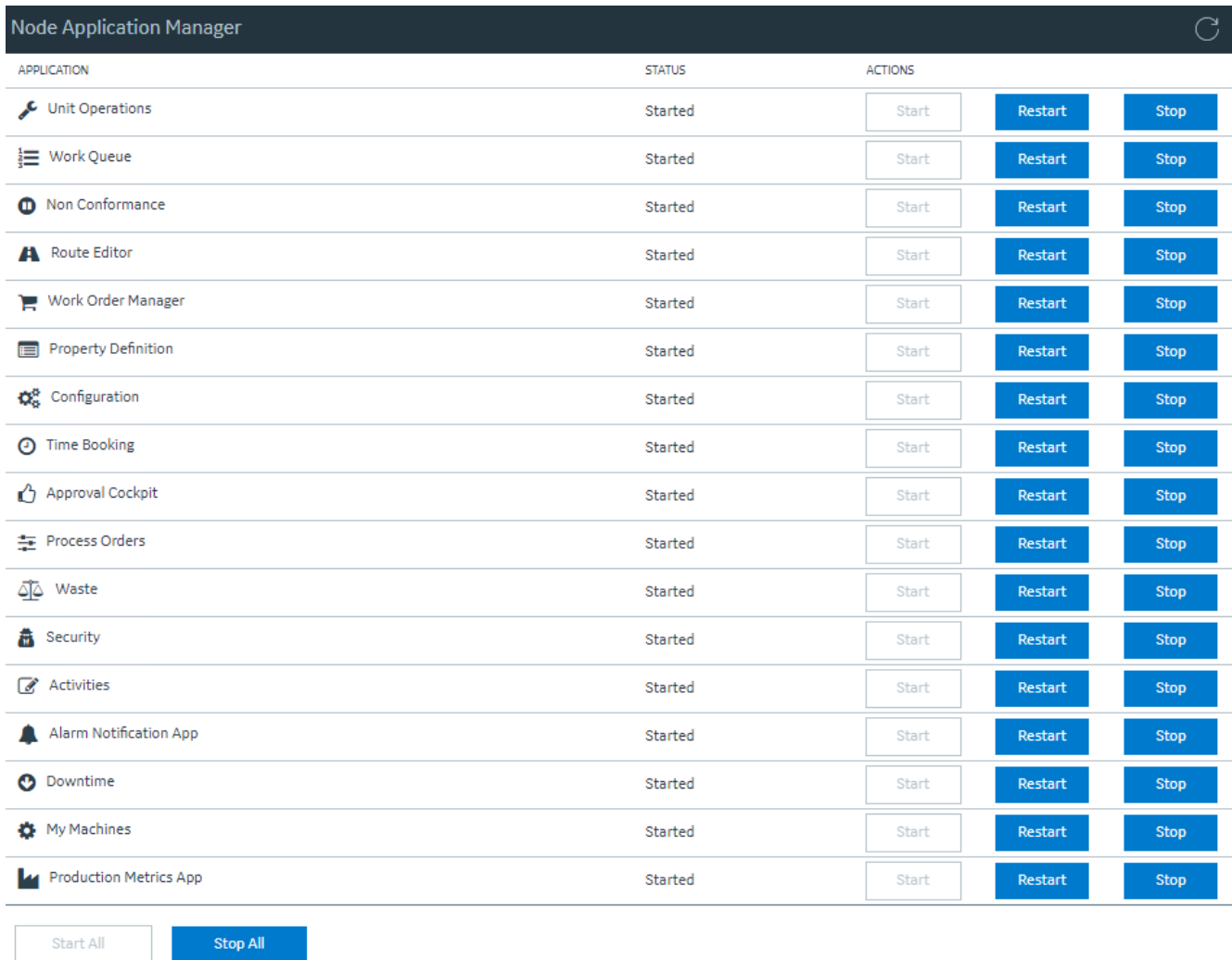
The properties of Node Application Manager is updated to accommodate for new applications.

```
jsapps.name[index]=plantAppsContainer (Node JS APplication name)
jsapps.port[6]=3000 (Port number)
jsapps.path[6]="C:\\Program Files\\GE Digital\
\PlantApplicationsUniversalClient\\plantapps-container" (path where
the application is installed)
```

```
jsapps.displayName[6]=PlantAppsContainer (Display name)
jsapps.displayIcon[6]=fa fa-home (icon)
```

Procedure

1. Launch this utility using the desktop shortcut icon where you have installed the Plant Applications Universal Client. Alternatively, you can also launch this by directly entering the following URL in the browser from any computer that has access to the Plant Application.

   `https://<PlantAppComputerHostname>:<TomcatPortNo>/node-manager-app`

2. Enter the credentials that has the **manager-ui** role of Tomcat assigned to log in. The Node Application Manager appears displaying the health of the individual applications in a dashboard.

Node Application Manager						
APPLICATION		STATUS	ACTIONS			
🔧	Unit Operations	Started	Start	Restart	Stop	
☰	Work Queue	Started	Start	Restart	Stop	
ⓞ	Non Conformance	Started	Start	Restart	Stop	
A	Route Editor	Started	Start	Restart	Stop	
🛒	Work Order Manager	Started	Start	Restart	Stop	
🖽	Property Definition	Started	Start	Restart	Stop	
⚙	Configuration	Started	Start	Restart	Stop	
⏱	Time Booking	Started	Start	Restart	Stop	
👍	Approval Cockpit	Started	Start	Restart	Stop	
⇅	Process Orders	Started	Start	Restart	Stop	
⚖	Waste	Started	Start	Restart	Stop	
🔒	Security	Started	Start	Restart	Stop	
📝	Activities	Started	Start	Restart	Stop	
🔔	Alarm Notification App	Started	Start	Restart	Stop	
⏺	Downtime	Started	Start	Restart	Stop	
⚙	My Machines	Started	Start	Restart	Stop	
📊	Production Metrics App	Started	Start	Restart	Stop	

Start All   Stop All

3. You can either **Start**, **Stop**, or **Restart** an individual application by selecting corresponding button. You can also use **Start All** or **Stop All** buttons either to start or stop all applications respectively.

4. You can select ↻ to reload the dashboard or refresh the browser.

5. You can select ⏻ to logout from Node Application Manager.

Chapter

4

Upgrade Plant Applications Web Client Without Using Docker

Topics:

Upgrade the Plant Applications Web Client Without Using Docker

Before You Begin

- Ensure that you complete the following procedure specific to the Plant Applications Message Bridge:

    1. Uninstall the earlier version of the Plant Applications Message Bridge.
       The Proficy Server Message Bridge service is disabled.
    2. Delete the directory - `C:\Program Files (x86)\Proficy\Proficy Server \RabbitMQMessageBridgeService`.
    3. Restart your computer.
    4. Install the version of the Plant Applications Message Bridge included in the Plant Applications installer.
    5. Restart the Proficy Server Manager service.
       The Proficy Server Message Bridge service is automatically restarted.

- Ensure that you create a backup copy of the text file that includes the user-specific settings. The file is created in the directory `<tomcat_home>/Apache Software Foundation/Tomcat 9.0/ users/<user>`, where:

    ◦ *<tomcat_home>* is the directory where you installed Apache Tomcat. For example, `C:/Program Files`.
    ◦ *<user>* is the name of a logged-in user.

    After you upgrade, you can copy-paste the file to the same location to replicate the user-specific settings. For more information, refer to the Plant Applications Web Client Help.

About This Task

You can upgrade any earlier service pack (SP) version of Plant Applications Web Client 7.0 to 8.1.

Note: The Plant Applications 8.1 installer is the base installer for all upgrade requirements.

Procedure

1. Run the `installfrontend.exe` file as an Administrator.
   The installation menu appears, displaying the **Install Proficy Plant Applications 8.1** screen.
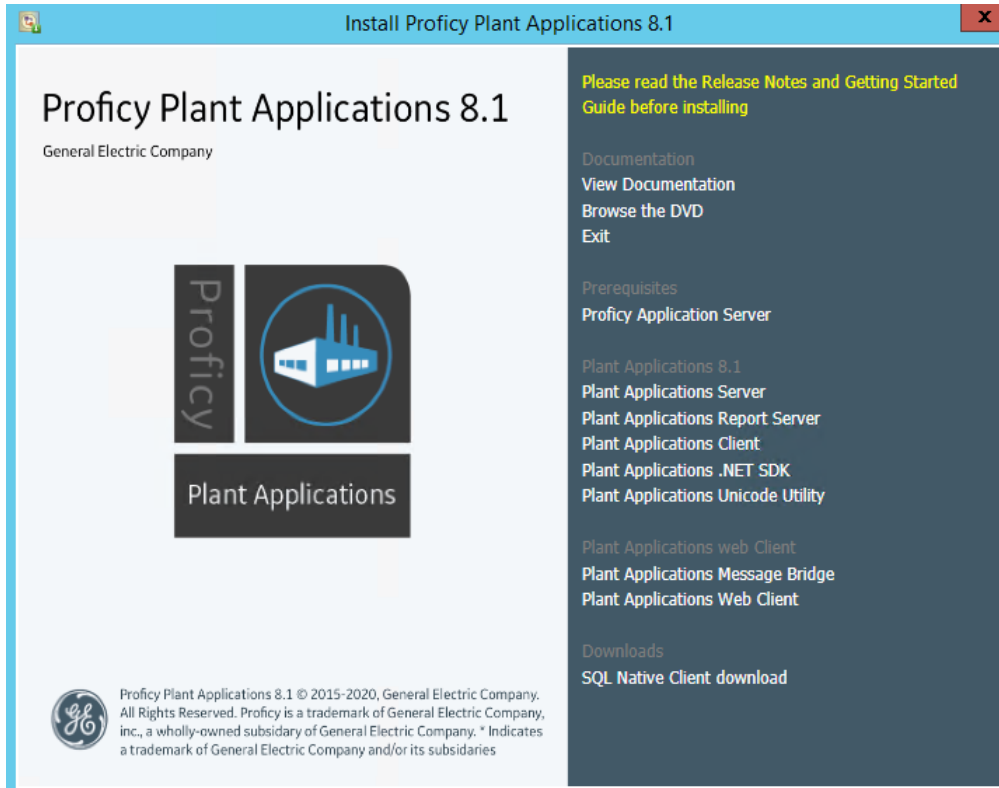
Tip: You can hover over each task that appears in the installation menu to refer to the tooltip associated with that task.

2. Select **Plant Applications Web Client**.
   The installer gathers the current configuration and determines the required configurations that need to be updated.

   Then the upgrade wizard appears, displaying the **Welcome to Plant Applications Web Client** screen.

3. In the **Welcome to Plant Applications Web Client 8.1** screen, select **Next**.
The **Read and accept the license agreement to continue** screen appears.
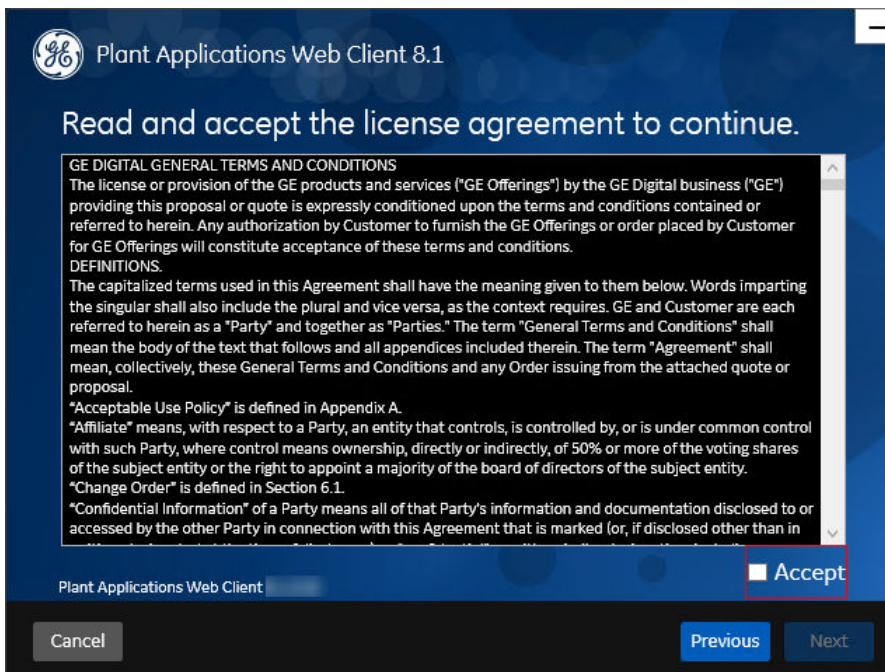
4. Read the license agreement, select **Accept**, and then select **Next** to continue the installation.
The **Prerequisites** screen appears.
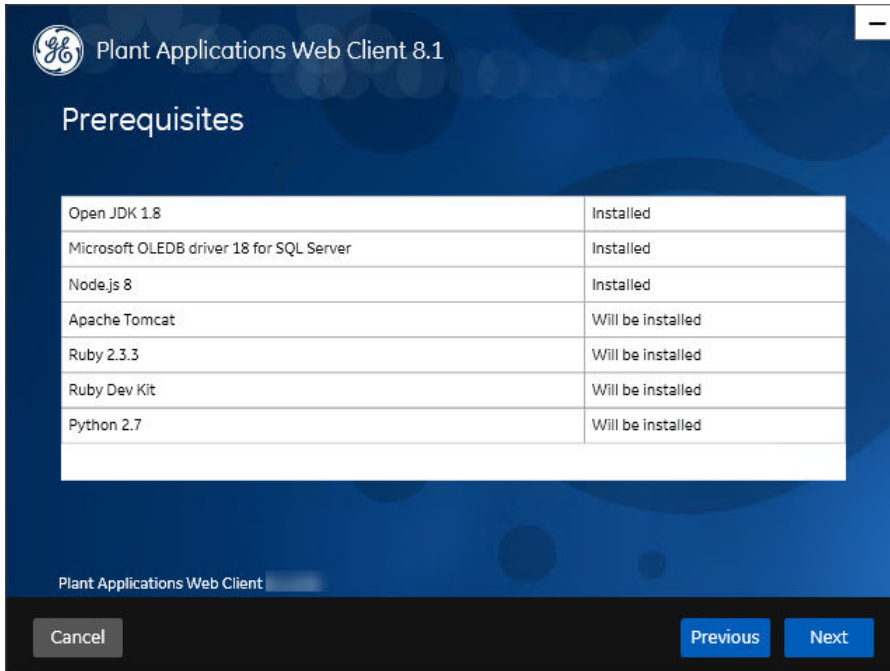
5. In the **Prerequisites** screen, select **Next** to view all installed prerequisites and install any missing prerequisites.
The **Operations Hub Credentials** screen appears.

6. In the **Operations Hub Credentials** screen, enter the credentials to access the Operations Hub server as described in the following table.

Credential	Description
Server Name	This field is automatically populated with the local host name, fully qualified host name, or IP address, based on the configuration in Operations Hub. You can edit the host name of the Operations Hub server based on requirement. **Note:** Instead of IP address, it is recommended to use the Operations Hub host name (computer name).
Port	Enter the Operations Hub port number.
Tenant Username	Enter the tenant Hub username to access the Operations Hub server instance. **Note:** The default user name is `OphubAdmin`.
Tenant Password	Enter the password for the user name you entered in the **Tenant Username** box. **Note:** The tenant username and password must be same as the credentials that you have specified during the Operations Hub installation.

If all the options are entered correctly, the **Next** button is enabled.

7. Select **Next** to continue with the installation.
   The **Install Model Selection** screen appears.
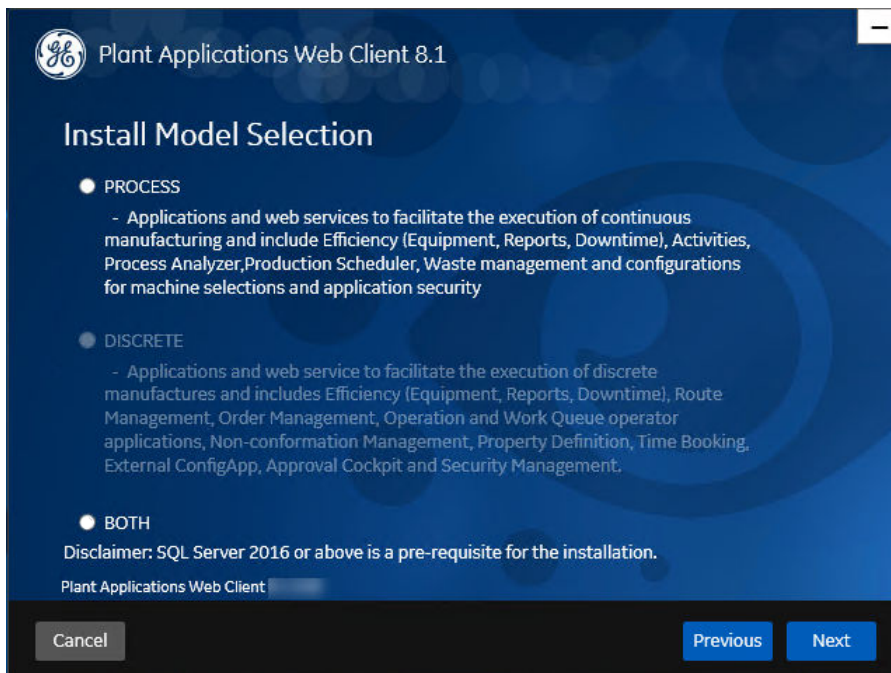
8. In the **Install Model Selection** screen, select any of the following options based on the requirement.

   - PROCESS: Installs only the Process applications along with the web services.
   - BOTH: Installs both the Process and Discrete applications.

   Note: When upgrading, you can either select PROCESS or BOTH only.

9. Select **Next**.
   The **Historian UAA Credentials** screen appears.
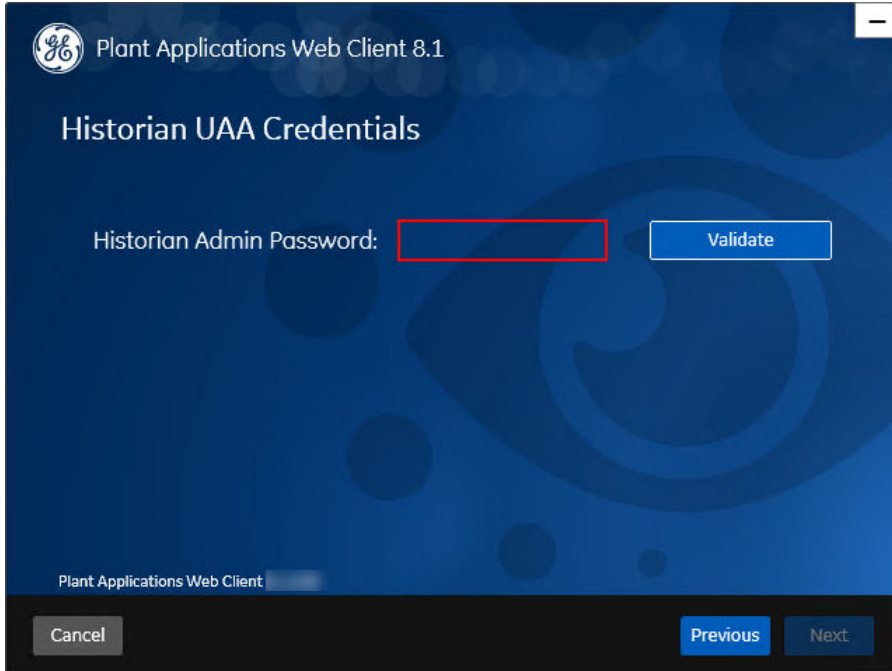
10. In the **Historian UAA Credentials** screen, enter the password to access the Historian UAA server and then select **Validate**.
    The following table describes each icon indicating a validation status that might appear during the validation process.

Icon	Description
⚙	Indicates that the validation is in progress.
✅	Indicates that the validation was successful.
❌	Indicates that the validation was unsuccessful. In this case, make sure you enter the correct password.

If the Historian UAA server connection is successfully validated, the **Next** button is enabled.

11. Select **Next**.
    The **UAA Credentials** screen appears.

12. In the **UAA Credentials** screen, enter the credentials to access the UAA server as described in the following table.

Credential	Description
Server Name	Enter the host name of the UAA server.
	Note: Instead of IP address, it is recommended to use the UAA host name (computer name).
Port	Enter the UAA port number.
Admin Client ID	Enter the admin Client ID to access the UAA server instance.
	Note: The default user name is `admin`.
Admin Client Secret	Enter the Client Secret for the user name you entered in the **Admin Client ID** box.
Validate	Select **Validate** to validate the UAA server connection.
	Note: The following table describes each icon indicating a validation status that might appear during the validation process.
	<table><tr><th>Icon</th><th>Description</th></tr><tr><td>⚙</td><td>Indicates that the validation is in progress.</td></tr><tr><td>✔</td><td>Indicates that the validation was successful.</td></tr><tr><td>✖</td><td>Indicates that the validation was unsuccessful. In this case, make sure you enter the correct password.</td></tr></table>

If all the options are entered correctly, the **Next** button is enabled.

13. Select **Next**.

The **Plant Applications Database Credentials** screen appears.

Note: If you have selected **BOTH** in the **Install Model Selection** screen, the following screen appears that allows you to enter the Couch DB details.

14. In the **Plant Applications Database Credentials** screen, in the Plant Applications Data Base section, enter the Plant Applications database credentials as described in the following table.

Credential	Description
Server name	Enter the server name where the Plant Applications database is installed in the format `HOST_NAME\INSTANCE`. Where `HOST_NAME` is the host name (either a fully qualified domain name or IP address, of the server) and `INSTANCE` is the instance of the server used by the database. **Note:** If there is no instance for the server, you can enter `HOSTNAME` as the server name. `Localhost` is not an acceptable value for `HOSTNAME`.
Database	Enter the name of the Plant Applications database that you want to connect with the Plant Applications Web Client.
Username	Enter the user name that has permissions to access the database you entered in the **Database** box. By default, the user name appears as `sa`.
Password	Enter the password for the user name you entered in the **Username** box.
Port	Optional: Enter the number of the port that the instance uses to listen for client connections. **Note:** The default port is 1433.

15. Select **Validate Connection** to validate the database connection.

    Note: The validation process takes some time to check whether a compatible version of the Plant Applications server is installed.

    The following table describes each icon indicating a validation status that might appear during the validation process.

Icon	Description
	Indicates that the validation is in progress.
	Indicates that the validation was successful.
	Indicates that the validation was unsuccessful. In this case, make sure you enter the correct password.

    If you have selected PROCESS in the **Install Model Selection** screen and the database connection is successfully validated, the **Next** button is enabled. Skip to **Step 19**.

16. If you have selected **BOTH** in the **Install Model Selection** screen, in the **Plant Applications Database Credentials** screen, select the **CouchDB** tab.
    The **Document Service Couch DB Credentials** screen appears.

17. In the **Document Service Couch DB Credentials** screen, enter the Couch DB credentials as described in the following table.

Credential	Description
CouchDB Server Uri	Enter the fully qualified web address of Apache CouchDB in the format: `https://<host name or IPaddress>:<port number>`.
Node	Enter the name of the node where Apache CouchDB is running. By default, the node value appears.
Username	Enter the user name of the administrator that has permissions to access the database you entered in the **Database** box.
Password	Enter the password for the user name you entered in the **Username** box.

Credential	Description
Couch Certificate	Select **Browse** to locate the Apache CouchDB server certificate (couch_server.crt) that you have generated and upload it.
Validate	Select **Validate** to validate the Apache CouchDB database credentials. **Note:** The following table describes each icon indicating a validation status that might appear during the validation process.

Icon	Description
⚙	Indicates that the validation is in progress.
✅	Indicates that the validation was successful.
❌	Indicates that the validation was unsuccessful. In this case, make sure you enter the correct password.

If the Apache CouchDB database connection is successfully validated, the **Next** button is enabled.

18. Select **Next**.
The **Plant Applications Administrator User Credentials** screen appears.

19. In the **Plant Applications Administrator User Credentials** screen, enter the Plant Applications Administrator credentials as described in the following table.

Note: Ensure that the user credentials entered here must exist in Plant Applications Server with an administrator role defined and you must use the same credentials to login into the Web Client applications.

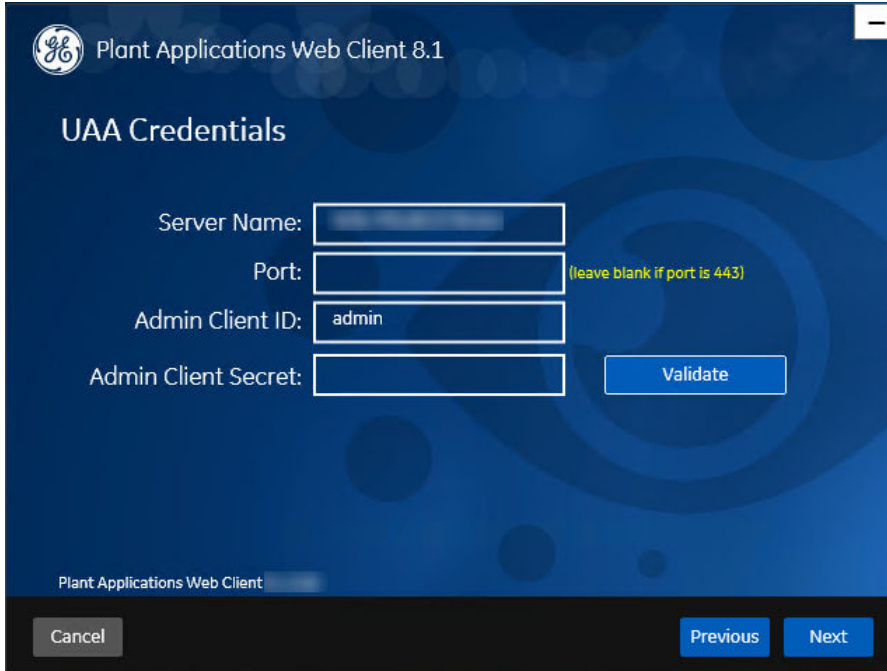| Credential	Description
User Name	Enter the user name for an administrator account in Plant Applications. **Note:** The default user name is `OphubAdmin`.
Password	Enter the password for the user name you entered in the **User Name** box.
Validate	Select **Validate** to validate the Plant Applications Administrator credentials. **Note:** The following table describes each icon indicating a validation status that might appear during the validation process. **table below**

Icon	Description
⚙	Indicates that the validation is in progress.
✅	Indicates that the validation was successful.
❌	Indicates that the validation was unsuccessful. In this case, make sure you enter the correct password.

If the Plant Applications Administrator connection is successfully validated, the **Next** button is enabled.

20. Select **Next**.
The **Tomcat Installation** screen appears.
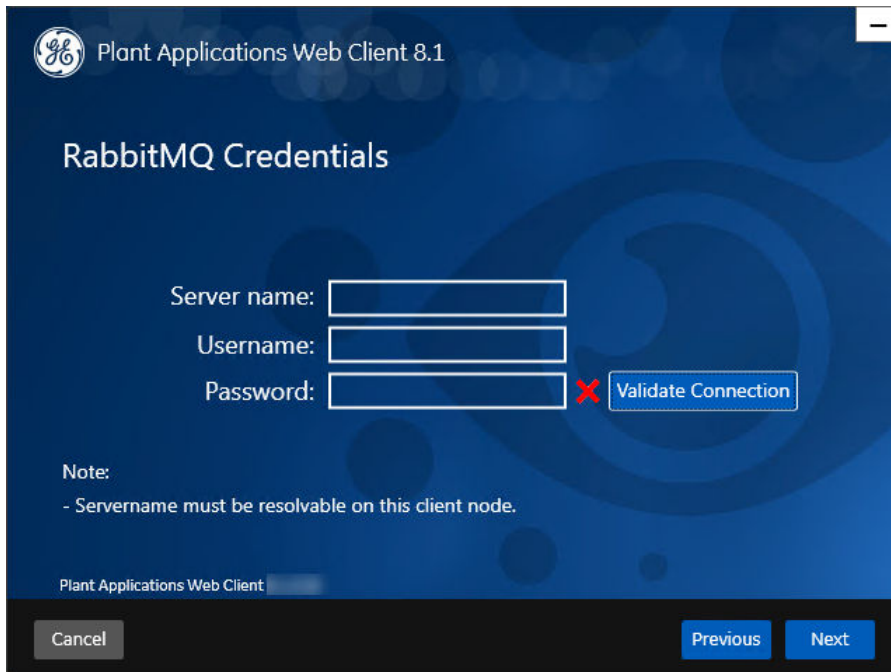
Note: If you already have a Tomcat instance running, a message stating that the Tomcat instance has been found appears in the Tomcat Installation screen informing you to select the existing Tomcat instance.
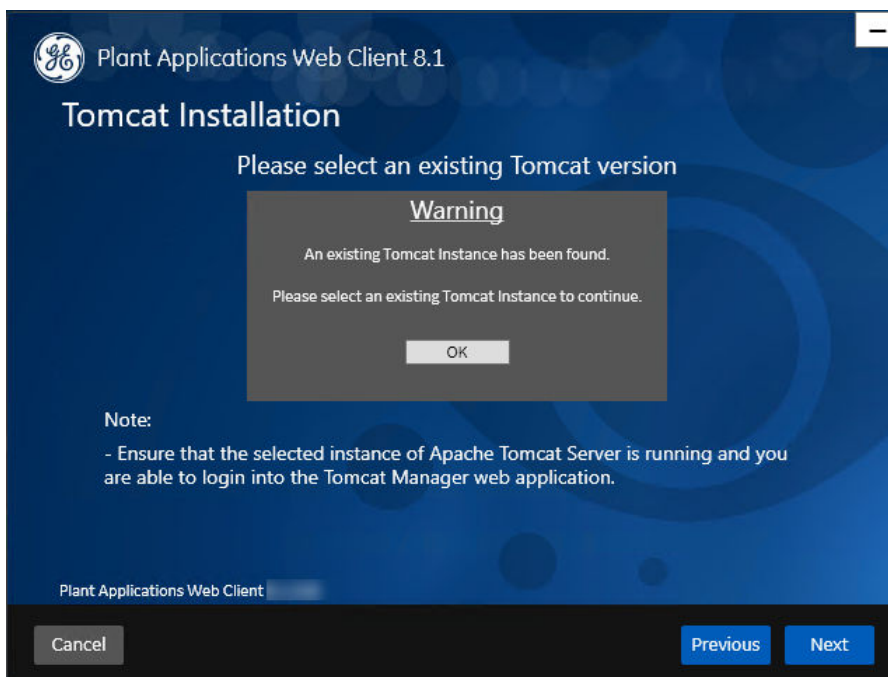
21. In the **Tomcat Installation** screen, select **OK**.
    The installer prompts you to select an existing Tomcat instance if the Tomcat installation details are available in the registry settings for the Plant Applications Web Client on your computer.
22. In the **Tomcat Installation** screen, select an appropriate Tomcat instance from the drop-down list box.
23. In the **Tomcat Installation** screen, enter the Tomcat installation details for a new or existing installation as described in the following table. The installer prompts you to enter details for an existing Tomcat if the Tomcat installation details are available in the registry settings for the Plant Applications Web Client on your computer. Else, the installer prompts you to enter details for a new installation of Tomcat.

Installation Detail	Description
Port	Enter the HTTP port that Tomcat uses to listen for client connections.
	Note: The default port is 8081.
Redirect Port	Enter the HTTPS port that Tomcat uses to redirect all HTTP requests to this port.
	Note: The default redirect port is 8444.
Username	Enter the user name to access Tomcat.
	Note: The default user name is `admin`.
Roles	Skip this box because it is automatically populated.
Password	Enter the password for the user name you entered in the **Username** box.
Re-enter Password	Reenter the password for the user name entered in the **Username** box.
	Note: This box appears only when a new installation of Tomcat is initiated by the installer.

24. Select **Next**.
    The **RabbitMQ Credentials** screen appears.

25. In the **RabbitMQ Credentials** screen, perform one of the following steps:

- Enter the RabbitMQ credentials for the machine that hosts your Plant Applications message bridge as described in the following table, and then select **Validate Connection**.

Credential	Description
Server name	Enter the computer name or IP address that hosts your Plant Applications Message Bridge.
Username	Enter the Administrator's user name that you set during Plant Applications Message Bridge installation.
Password	Enter the password for the Administrator's user name you entered in the **Username** box.

The following table describes each icon indicating a validation status that might appear during the validation process.

Icon	Description
⚙	Indicates that the validation is in progress.
✅	Indicates that the validation was successful.
❌	Indicates that the validation was unsuccessful. In this case, make sure you enter the correct password.

26. Select **Next**.
The **Kafka Credentials** screen appears.

27. In the **Kafka Credentials** screen, enter the credentials to access the Kafka server as described in the following table.

Credential	Description
Server Name	Enter the host name of the Kafka server.
	Note: Instead of IP address, it is recommended to use the Kafka host name (computer name).
Kafka Port	Enter the Kafka port number.
Zookeeper Client Port	Enter the Zookeeper Client port number.
Validate	Select **Validate** to validate the Kafka server connection.
	Note: The following table describes each icon indicating a validation status that might appear during the validation process.

Icon	Description
	Indicates that the validation is in progress.
	Indicates that the validation was successful.
	Indicates that the validation was unsuccessful. In this case, make sure you enter the correct password.

If all the options are entered correctly, the **Next** button is enabled.

28. Select **Next**.

The **You are ready to upgrade** screen appears.
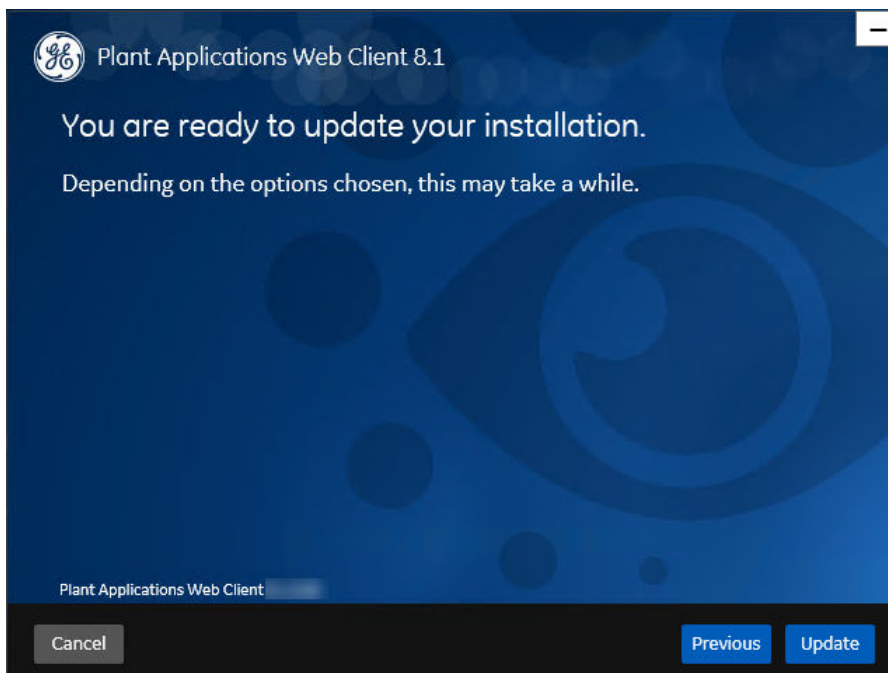
29. Select **Upgrade**, and then wait for the upgrade process to complete.

Depending on the contents to be upgraded, the upgrade process might take some time. A message appears in the wizard, indicating whether the upgrade was successful or not.
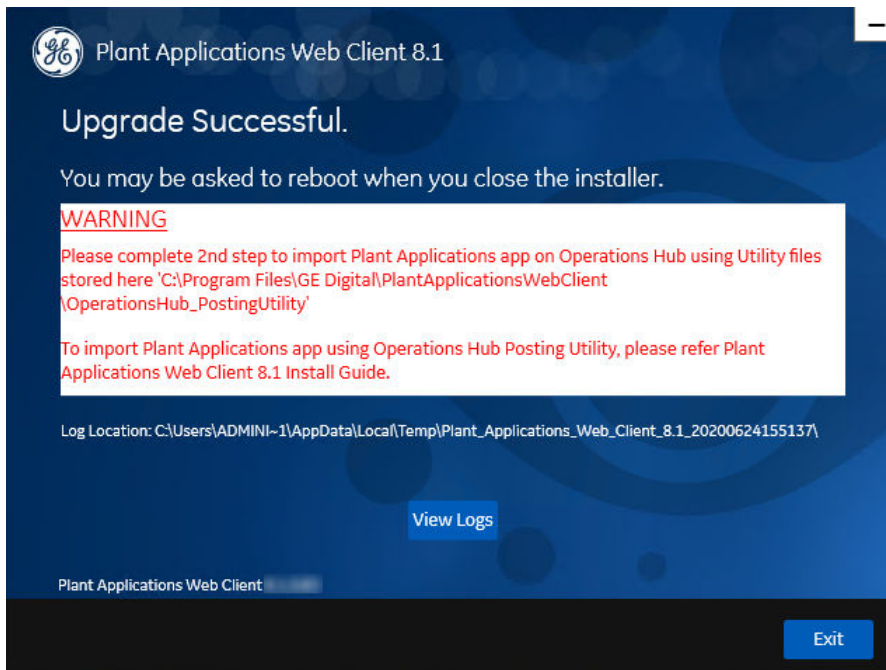
30. **Optional:** Select **View Logs** to see the upgrade details.
31. In the **Upgrade Successful** screen, select **Exit** to close the upgrade wizard.
    Plant Applications Web Client has been upgraded to the latest version.
32. Run Operations Hub Posting Utility on page 69 to import the Plant Applications into the Operations Hub.

Access Existing ThingWorx Custom Application

You can access custom applications created in ThingWorx up to Plant Applications Universal Client 7.0 SP5 using following URL.

```
https://<host name>:<Tomcat redirect port number>/Thingworx/Composer/
index.html
```

Chapter

5

Installing Plant Applications Web Client Using Docker

Topics:

-

About Installing Plant Applications Web Client Using Docker

Before you begin

Ensure that you have completed all the pre-requisite software installation and configuration. For more information, refer to the pre-installation requirements.

Note:

- Docker Web Client installation supports only the fully-qualified domain environment. Therefore, to avoid any potential issues, you must use the fully-qualified domain names for the remote server.
- Ensure that during Operations Hub installation, you provide the fully-qualified domain name (FQDN) for primary host name.

Introduction

The installer for Plant Applications Web Client using Docker automates the following tasks that are required to install a fresh copy of Plant Applications Web Client version 8.1 or upgrade from Plant Applications Web Client version 8.0 SIM2 to version 8.1:

- Transforming the raw .tar files related to the new features
- Updating the Docker images
- Pushing the Docker images to the local docker registry
- Pulling the Docker images on to the Web Client server node
- Updating the Docker stack

This Ansible-based installer is a Client Line Interface (CLI) driven tool. You must enter the configuration details when prompted. Based on the input, the corresponding Linux shell scripts or Ansible playbooks are triggered to complete the tasks involved in the installation.

The installer can either install Plant Applications Web Client on a Linux server with Docker installed or perform an upgrade from Plant Applications Web Client version 8.0 to version 8.1. In both the cases, the CLI-based navigation remains the same.

Deployment Architecture

The following diagram shows the recommended deployment architecture. In this diagram, the numbering of the servers suggests the order of installation of the various software packages on their respective servers. We recommend that you follow the same order.
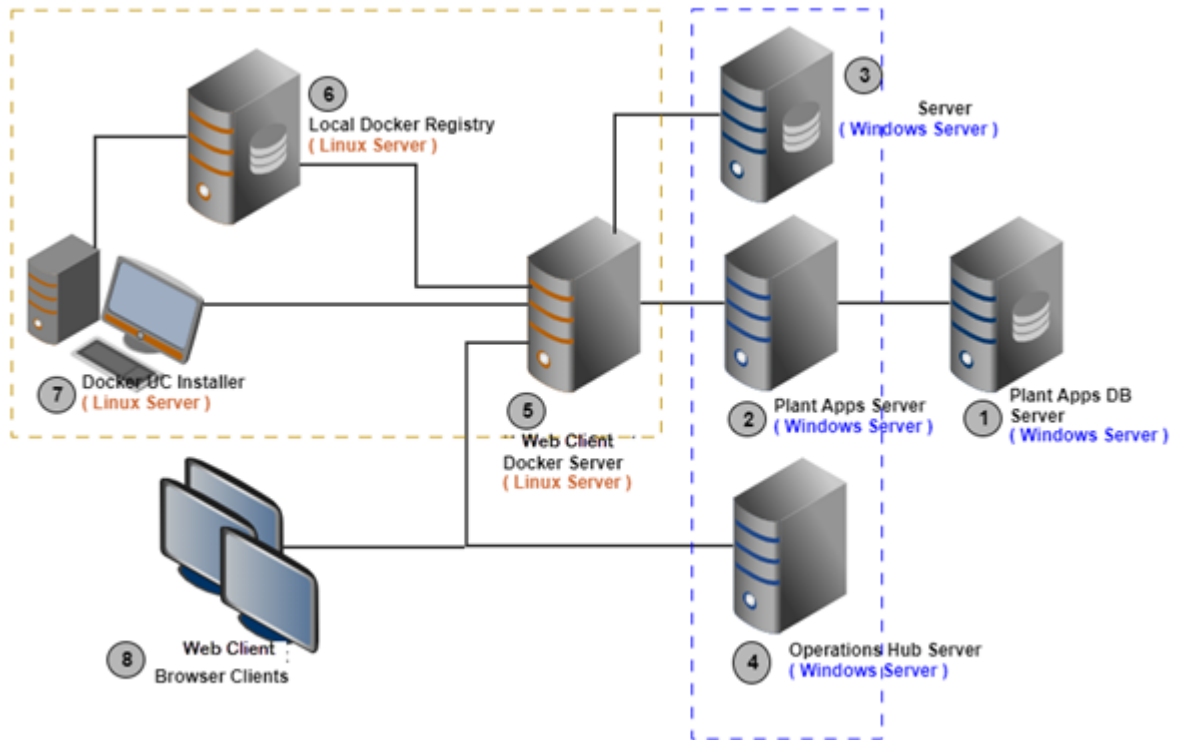
Depending on your data storage and the number of concurrent client requirements, you can choose to set up nodes 2, 3, and 4 on a Windows machine and nodes 5, 6, and 7 on a Linux machine. If, however, you choose the minimum-number-of-servers configuration for the deployment, resolve the following possible port conflicts:

- **Operations Hub and Plant Applications Web Reports:** Operations Hub uses 443 as the port number for https binding. Therefore, use a different port for the Web Reports server.
- **Operations Hub IQP and Apache CouchDB:** Both these applications use 5986 as the port number. Therefore, modify the `default.ini` file of Apache CouchDB to set the port number under httpd to 5987.

About Preinstallation Requirements

Important: To proceed with the installation or upgrade of Plant Applications Web Client, your deployment environment must be connected to the Internet.

Following are the details of the nodes and the pre-requisite software:

Node	Description	Requirements
1. Plant Applications database server	This node will contain the Plant Applications database.	• 64-bit Windows 10, Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019 • SQL server 2016 (64-bit), 2017 (64-bit), or 2019 (64-bit and with mandate Cumulative Update 4 installed) For hardware requirements, refer to Getting Started Guide.
2. Plant Applications server	This node will contain the Plant Applications server (that is, Plant Applications core, Message Bridge, and RabbitMQ)	Refer to Getting Started Guide.
3. Apache CouchDB	This node will contain Apache CochDB, which is the document management store that is used by the Route Editor application to store documents. **Note:** For more information on configuring CouchDB, refer to Configuring Apache CouchDB Settings on page 4.	• 64-bit Windows 10, Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019 • Apache CouchDB 2.3.1
4. Operations Hub	This node will contain the Operations Hub container running server. Beginning in Plant Applications v8.1, Web Client applications are hosted in an Operations Hub container.	• 64-bit Windows 10, Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019 • Operations Hub • Operations Hub UAA

5. Web Client	This node will contain the linux server on which you install or upgrade the Docker images for Web Client.	• Ubuntu 18.x
		• Minimum 32GB of RAM
		  Note: If you want to use a 64GB RAM, modify the .env file after installing Web Client.
		• An 8-core processor
		• A free disk space of 100GB
		  Note: However, you may need more disk space based on your production data.
		• Docker Community Edition or Enterprise Edition 18.0 or later
		• Docker Compose 1.25.x
		• Docker Swarm initiated as Swarm Manager
		• Public Docker Images:
		  ◦ confluentinc/cp-kafka:5.1.2
		  ◦ confluentinc/cp-zookeeper:5.1.2
		  ◦ thomsch98/kafdrop:latest
		  ◦ confluentinc/cp-schema-registry:5.1.2
		  ◦ redis:5.0.7
		  ◦ eventuateio/eventuate-tram-cdc-mysql-service:0.21.3.RELEASE
		  ◦ haproxy:1.8

Node	Description	Requirements
6. Local Docker Registry	This node will contain Docker Images provided by GE. You will store and maintain the Docker Images so that the required images can be used on the node on which you want to install Web Client Docker containers.	- Ubuntu 18.x - Docker Community Edition or Enterprise Edition 18.0 or later - Ensure that Docker Registry is running with volume mounting completed and the registry service's URL is accessible from any node in the network. For information, refer to Create and Configure Docker Registry on page 55. - Public Docker Images: - hyper/docker-registry-web:latest - registry:2.4.1
7. Installer Node	This node will contain the Ansible-based installer. You can also run the installer on the Web Client node.	- Ubuntu 18.x - Docker Community Edition or Enterprise Edition 18.0 or later - Ensure that PIP is installed and accessible to sudo user. - Ansible v2.9.10 (recommended). For more information, refer to the *Upgrade to Ansible 2.9* section below.
8. Browser-Based clients	This node will contain browser-based clients to access Web Client.	- Google Chrome 80.0 or later - Ensure that this node is on the same network as the remaining ones.

Note:

- You can combine the Installer node, Plant Applications Web Client node, and the Local Docker Registry node in to a single Linux server, especially if you want to upgrade to Plant Applications 8.1.
- Except the proxy settings, all the shell commands that are required to install the pre-requisite software (including Ansible) are included in the Plant Applications Web Client installer. However, ensure you have Docker and Python Package installer (pip) installed on the Ansible node.
- If you are using controller and performing a remote upgrade of 8.0 SIM2, then you must uninstall the **docker-py** module on the Web Client node before starting the upgrade process.
- If your deployment environment is not connected to the Internet, you must have the necessary arrangement for installing the aforementioned components offline. For more information, refer to Install Web Client on Offline Systems on page 60.

Upgrade to Ansible 2.9

Perform below steps to upgrade to Ansible 2.9:

1. Append below line to `/etc/apt/sources.list` file and save it.`deb http://ppa.launchpad.net/ansible/ansible-2.9/ubuntu bionic main`
2. Run the command `sudo apt-get update`.

   Note: You may run into an error if the NO_PUBKEY 93C4A3FD7BB9C367 public key is not available. In such case, run the following command:

   `sudo curl -sL "http://keyserver.ubuntu.com/pks/lookup?op=get&search=0x93C4A3FD7BB9C367" | sudo apt-key add`
3. Now run the installer, it will install latest version of ansible

Files Provided by GE

The following files and folders are provided by GE:

- `PA8.1PAcoreBuild`: Contains the latest build of Plant Applications v8.1.
- `PA8.1 wc-anisble-installer`: Contains the version 8.1 installer, which includes:
  - SQL scripts
  - Linux shell scripts
  - Ansible playbooks (.yml, .j2, .sh, .sql, and other plain text files)
  - `UAAC.tar`
  - `OperationsHub_PostingUtility.msi`
- `PA8.1_WC_TARFILES.ZIP`: Contains the Web Client Docker Images (not the public images) in a .tar format. These files are Docker images of the new features.
- `Readme.txt`: Contains a list of the defects fixed in this release and a list of new features.

Pre-Installation Steps

Before You Begin

- Ensure that you have all the nodes required to install Plant Applications Web Client. For information, refer to Deployment Architecture on page 50 and About Preinstallation Requirements on page 51.
- If you are using a UAA service other than Operations Hub UAA, migrate your UAA data to Operations Hub UAA using `uaa-users-migration-utility`.
- During installation, you will be required to enter the following details at different steps. Therefore, make a note of these details.
  - The location of the tar files provided by GE.
  - URL of the local Docker Registry
  - Credentials to access the local Docker Registry (required if authentication is enabled).
  - Host name, username, and password to access the remote server (if you want to install Web Client on a remote server)
  - Name of the Plant Applications database server
  - Instance name of the Plant Applications database server (required only if the database has an instance)
  - Name of the Plant Applications server
  - Credentials to access RabbitMQ
  - Credentials of the username and password of the Plant Applications Admin user who will be added to the UAA service
  - Name of the Apache CouchDB server and access credentials
  - Node name of the Apache CouchDB server (the node name used during the CouchDB configuration. For example: couchdb@localhost)
  - Server name of Operations Hub
  - Admin client ID and secret of Operations Hub UAA
  - Tenant username and password of Operations Hub

Procedure

1. If your installation environment runs behind a proxy, on all the three servers (nodes 5, 6, and 7 in the deployment architecture), set the HTTP_PROXY and HTTPS_PROXY environment variables to point to your proxy servers.

2. Create and configure Docker Registry.

3. Set the NO_PROXY environment variable to the IP addresses or host names of the local Docker Registry, Plant Applications database, Plant Applications, Apache CouchDB, and Operations Hub servers. To do so:

    a) Run the following command: `sudo nano /etc/environment`

    b) Add the following line in the environment file, and save the file:

    `no_proxy="127.0.0.1, <IP address or hostname of the UAA server>, <IP address or hostname of soadb>, <IP address or hostname of RabbitMQ>, <IP address or hostname of the Docker Registry>"`

4. Access the node on which you want to install Plant Applications Web Client.

5. Create a folder named `wc81tars`.

6. Extract the contents of the `PA Web Client 8.1_Tarfiles.zip` file, and copy the contents into the `wc81tars` folder.

7. Create another folder named `wc81installer`.

8. Extract the contents of the `PA8.1_uc-ansible-installer`, and copy the contents into the `wc81installer` folder.

9. Navigate to the installer folder, and run the following shell command: `~/your/path/wc81installer/wc_ansible_install/ sudo chmod +x ./wcinstall.sh`

Create and Configure Docker Registry

Procedure

1. From the Plant Applications Web Client installation package, download the `DTR.zip` file into the machine on which you want to run Docker Registry.

2. Create a folder named `pa-dtr` by running the following command: `sudo mkdir -p <folder path>/pa-dtr`. This folder stores the Docker Registry configuration files.

3. Create another folder named `docker.service.d` in the `/etc/systemd/system` folder by running the following command: `sudo mkdir -p /etc/systemd/system/docker.service.d`

4. In the `docker.service.d` folder that you have created, create a file named `http-proxy.conf` by running the following command: `sudo nano /etc/systemd/system/docker.service.d/http-proxy.conf`

5. Copy the following lines of code into the `http-proxy.conf` file, replacing the text in the angular brackets with the appropriate values:

```
[Service]
Environment="HTTP_PROXY=<proxy URL>:<port number of the proxy
server>/""NO_PROXY=localhost,127.0.0.1,<IP address of the Docker
Registry node>,<host name of the Docker Registry node>"
```

6. Save the file and close it.

    Note: To save and close the file, enter ctrl+o and ctrl+x, respectively.

7. Create a file named `daemon.json` in the following folder: `/etc/docker`

8. Add the following lines of code in the `daemon.json` file:

```
{
"insecure-registries" : ["<IP address of the Docker Registry
node>:5000","<host name of the Docker Registry node>:5000"]
}
```

9. Run the following commands to verify that the proxy details that you have entered are correct:

```
sudo systemctl daemon-reload
                    sudo systemctl restart docker
                    systemctl show --property=Environment
docker
```

10. Using terminal, navigate to the `pa-dtr` folder.
11. Access the .env file, and update the following parameters with the correct absolute path.

    • REGISTRY_WEB_CONFIG_VOLUME_PATH=/<absolute path>/pa-dtr/conf/registry-web
    • REGISTRY_WEB_DB_VOLUME_PATH=/<absolute path>/pa-dtr/conf/registry-web/db
    • REGISTRY_CONFIG_VOLUME_PATH=/<absolute path>/pa-dtr /pa-dtr/conf/registry
    • REGISTRY_DATA_VOLUME_PATH=/<absolute path>/pa-dtr/data

12. In the `pa-dtr` folder, change the permission of the `PA_DTR_Start_Lix.sh` file to 775 by running the following command: `sudo chmod 775 ./PA_DTR_Start_Lix.sh`
13. Access the `PA_DTR_Start_Lix.sh` file, and run the Shell script with sudo privileges: `sudo ./PA_DTR_Start_Lix.sh`. This is necessary to create and access the Docker registry.
14. Go to the following locations to check if the Docker registry is created successfully:

    • **Registry-url:** http://<host name or IP address>:5000/v2/_catalog to verify that the registry is up and running.
    • **Registry-web-url:** http://<host name or IP address>:8080 to verify the docker images.

    Docker Registry is created. When prompted for the DTR URL during the installation of Plant Applications Web Client, enter <host name of IP address of this local Docker Registry>:5000.

    Note: Do not enter http or https.

Install Plant Applications Web Client Using Docker

About This Task

• During the installation, the installer displays the installation tasks on the console and in a log file at `$~/your/path/wc81Installer/wc_ansible_install/log/ansible.log` and `$~/your/path/wc81Installer/wc_ansible_install/log/sql_script.log`.
• The steps in this topic are applicable to both first-time installation and upgrade.

    Note: If you are using a controller and performing a remote upgrade of 8.0 SIM2, you must uninstall the **docker-py** module on the Web Client node before starting the upgrade process.

    1. On the Web Client node, run: `$sudo pip uninstall docker-py` to uninstall the **docker-py** python module.
    2. After uninstalling the **docker-py** python module, run: `$sudo pip install docker` to install the **docker** python module.
    3. Run the installer.

Procedure

1. Depending on your deployment architecture, run one of the following commands to launch the installer:

   - If you want to install Web Client Installer and Web Client on a single Linux machine, navigate to your installer folder `~/your/path/wc81Installer/wc_ansible_install/` and run the following command at the terminal:

     `$ sudo ./wcinstall.sh -l target`

     or

     `$ sudo ./wcinstall.sh`

   - If you want to install Web Client on a remote machine, run the following command at the terminal:

     `$ sudo ./wcinstall.sh -r target`

   The shell script `wcinstall.sh` is launched, and a welcome message appears.

2. Press any key to proceed further.

3. Press any key to display the license agreement.
   At the end of the license agreement, you will be prompted to agree or reject it.

4. Enter Y to proceed.
   The installer displays the sequence of installation steps. Read through the steps and follow the exact sequence when installing.

Note: It is recommended to execute steps from 1 to 3 continuously. However, you can execute these steps in intervals. For example, after executing Step-1, you can choose to exit and come back to execute Step-2 by running the installer again.

Next Steps

Perform following sequence of steps:

1. **Step -1**: Add Docker Images to Your Local Docker Registry on page 57
2. **Step -2**: Update Docker Swarm with Web Client Containers on page 58
3. **Step -3**: Post Plant Applications Web Client Configuration to Operations Hub on page 60
4. **Step -4**: Exit

Add Docker Images to Your Local Docker Registry

Procedure

1. Enter 1 to add the Web Client Docker images to your local Docker Registry.

2. Provide the URL of your local Docker Registry. If you are performing an upgrade, provide the Docker Registry URL that was used during the previous installation in the following format: <IP address or host name>:<port number>

   Note: Do not include the protocol (http or https) but specify the port. Unless modified, the port number is 5000.

   - **Username and Password:** Provide the user credentials that have access to the Docker Registry. If you have not used a secure Docker Registry, skip these inputs by pressing Enter.
   - **Path of tar files:** Provide the absolute path of the directory where the .tar files provided by GE are located. For example, `/home/administrator/`.

3. Provide the path, and press Enter.
   The installer reads the `.tar` files, converts them to Docker images, and then pushes the images to the Docker Registry. The status of the tasks is displayed.

   Note: If the installer encounters issues in executing a task, the console displays the task and the issue, along with the description. If the count of failed issues is zero, it indicates that all the tasks are executed successfully.

Update Docker Swarm with Web Client Containers

Procedure

1. After performing Step-1, on the main menu, enter 2.
   You will be prompted for inputs in series. To minimize time duration and avoid wrong entries, it is recommended to keep the notes handy as suggested in the *Pre-Installation Steps* section.

   Note: If the following messages appear, ignore them:


```
TASK [dtr : set_fact] ****************************************************************
skipping: [localhost]

TASK [dtr : Tagging Service Images] *************************************************
skipping: [localhost]

TASK [dtr : Loading Service Images from package folder and Pushing into the DTR] ***
skipping: [localhost]

TASK [dtr : Tagging UI-App images] *************************************************
skipping: [localhost]

TASK [dtr : Tagging Analysis-App images] ******************************************
skipping: [localhost]

TASK [dtr : Loading UI-App Images from package folder and Pushing into the DTR] ****
skipping: [localhost]

TASK [dtr : Loading Analysis-App Images from package folder and Pushing into the DTR] ***
skipping: [localhost]
```

2. Enter values for each prompt specified below from the information that you have already noted.

   Note:

   - If you have chosen to install Web Client on a remote node, you will be prompted to enter the host name, username, and password to access the remote node.
   - If you are performing an upgrade, provide the absolute path of the directory in which Web Client was installed, and press Enter. Unless modified, the path appears as follows: `/<build path>/PlantApplicationsDocker`.
   - If you are performing a first-time installation, provide the absolute path of the directory in which you want to install. For example: `/home/administrator/webclient81`.

Note: The path that you provide must be a valid one. The installer will not create the directories in the given path if they do not exist.

```
Enter host name for Web Client installation (press enter to accept
default value) :
Enter Username (press enter to accept default value) :
Enter password:
Enter Web Client installation Directory :
Enter Docker Registry URL, without mentioning the protocol, ex.
xx.xx.xx.xx:5000
Enter Docker Registry access user name - -you can skip if default
value is correct -[admin]:
Enter Docker Registry access user password - (output is hidden)
Enter UAA User name ( This user has to be Plant Applications user
with 'admin' role.)
Enter UAA User Password (output is hidden):
Enter SQL Server name -:
Enter SQL DB name -:
Enter SQL Database Username:
Enter SQL Database User Password:
Enter Plant Apps MessageBridge Server name:
Enter RabbitMessageQueue admin user name:
Enter RabbitMessageQueue admin user password:
Enter CouchDB Server host name:
Enter the node name in CouchDB:
Enter CouchDB user name:
Enter CouchDB password:
```

- If you are performing an upgrade, the installer checks the configuration of the existing installation, and asks you if you want to modify the settings. Except for passwords, you can choose to use the existing settings.
- If you are performing a first-time installation, a new folder named `PlantApplicationsDocker` is created. All the files and folders required for installation are placed in this folder.

If the installation is successful, the following message appears:

Results

- If the failed count is zero, the installation is successful and after few minutes, PAServices and PAContainer stacks are operational.
- If the installer encounters any errors, the installation process stops at the failed task and details of the process are displayed both on the screen and in the log file at `<installation path>/8.1Installer/uc-ansible-installer/log/ansible.log` of the installer directory.

Post Plant Applications Web Client Configuration to Operations Hub

Procedure

1. After performing Step-2, from the main menu, select **3** to post the Plant Applications Web Client installation configuration parameters (which are the result of updating Docker Swarm to Plant Applications 8.1) to Operations Hub.
2. Enter values for each prompt as specified in the following table.

Prompt	Description
Enter Operations Hub server name	Enter the host name or the IP address of the Operations Hub server.
Enter Operations Hub Tenant User	Enter the UAA tenant username of Operations Hub.
Enter UAA Admin ClientID	Enter the UAA admin client ID.
Enter UAA Admin Client Secret	Enter the UAA admin client secret.

   A folder named `OperationsHub_Post` is created in the installation folder. If the failed count is 0, the installation is successful.
3. Enter 4 to exit the installer.
4. Copy the `OperationsHub_Post` folder to a folder in the Operations Hub (Windows) server.
5. Access the folder in the Operations Hub server, and run the `InstallWebComponents.cmd` file as an administrator.
   The Web Client plug-ins are placed in the Operations Hub server.

Verify the Installation

Procedure

1. Access the following application: `https://<OperationsHub_server_name>/iqp`
2. Log in with the username and password of the UAA user that you created in
   The Operations Hub application appears, displaying the **Designer** page.
3. In the **APPS** page, select **ALL APPS**.
   Plant Applications appears in the list of applications.
4. Access **Plant Applications**.
   Plant Applications Web Client appears.

   Note: The applications appear on the left menu. Select a button to open the corresponding application.

Install Web Client on Offline Systems

Before You Begin

Even though you want to install Web Client on an offline machine, you need to have required packages to be available. For this, you need to perform from Step-1 through Step-8 to download these required

packages on a machine that is connected to the internet and then manually copy the packages to the offline machine.

About This Task

Use this method of installation if you want to install Plant Applications Web Client in an offline mode.

Procedure

1. Ensure that you are connected to the internet until Step-5. Create a **requirements.txt** file.
2. Open the **requirements.txt** file and copy below 3 lines (no line spaces in between) into the file and save it.

   pymssql==2.1.4

   ansible==2.9.0

   Jinja2==2.10
3. Run the command `mkdir offlinepackages && pip download -r requirements.txt -d offlinepackages` to download the offline packages dependencies.
   Once the command is executed the **offlinepackages** directory is created.
4. Copy the **requirements.txt** file into the **offlinepackages** directory.
5. Run the `tar -zcf offlinepackages.tar.gz offlinepackages` command.
6. Uninstall pymssql, ansible, and jinja2.
7. Create a new directory **offline_rpms** using the `mkdir offline_rpms` command.
8. Run the following commands to download the **freetds** rpm packages to the **offline_rpms** folder.

   a. `sudo wget http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm`
   b. `sudo rpm -ivh epel-release-6-8.noarch.rpm`
   c. `sudo yum install --downloadonly --downloaddir=offline_rpms freetds freetds-devel`

   Once the above commands are executed, you can see the below rpm packages downloaded to the **offline_rpms** folder.

   * `freetds-1.1.20-1.el7.x86_64.rpm`
   * `freetds-devel-1.1.20-1.el7.x86_64.rpm`
   * `freetds-libs-1.1.20-1.el7.x86_64.rpm`

   Perform Step-9 through Step-15 on a offline machine where you want to install Plant Applications Web Client.
9. Copy the **offline_rpms** folder and the **offlinepackages.tar.gz** file to any selected path on the target machine.
10. Navigate to the **offline_rpms** folder.
11. From the **offline_rpms** folder, run the following commands to install the rpm packages locally.

    a. `sudo yum localinstall freetds-1.1.20-1.el7.x86_64.rpm`
    b. `sudo yum localinstall freetds-devel-1.1.20-1.el7.x86_64.rpm`
    c. `sudo yum localinstall freetds-libs-1.1.20-1.el7.x86_64.rpm`
12. Navigate to the folder where the **offlinepackages.tar.gz** file was copied.
13. To extract the file, run `tar -zxf offlinepackages.tar.gz`.
14. Run `pip install -r offlinepackages/requirements.txt --no-index --find-links offlinepackages` to install the libs and their dependencies.
15. Perform the installation.

Access REST APIs

Before You Begin

Install Plant Applications Web Client.

Note: The list of REST APIs that you can access depends on the roles and assignments assigned to the UAA user group to which you belong.

About This Task

This topic describes how to access the REST APIs for Web Client.

Procedure

1. Access a node on which Web Client has been installed.
2. Access the following URL: https://<server name of web client>:<port number>/<application service name>/swagger-ui/index.html
   https://webclientservername:5051/ncm-app-service/swagger-ui/index.html

   Note: All the Web Client applications run behind reverse proxy, which uses the port number 5051.

   The Swagger UI appears.
3. Select **Authorize**.
   You will be prompted to enter the client ID and client secret.
4. Enter the following values, and select **Authorize**:

Field	Description
client_id	Enter a value in the following format: <node name of Web Client>mes. For example, if the node name is wcserver, enter wcservermes.
client_secret	Leave it blank.

You can now access the REST APIs for the application that you have entered in the URL.

Replace the SSL Certificate of Web Client

Before You Begin

Install Plant Applications Web Client.

About This Task

When you install Plant Applications using Docker, a self-signed certificate for the Web Client applications is created so that you can access Web Client using HTTPS. For better security, we recommend that you replace this self-signed certificate with one issued by a trusted CA authority.

Note: Only **.pem** (with certificate and private key included) files are supported.

Procedure

1. Access the `wcrepair.sh` file in the `uc-ansible-installer` folder.

2. Provide execution permissions to the `wcrepair.sh` file by running the following command: `sudo chmod +x <path to the installer>/uc-ansible-installer/wcrepair.sh`
3. Run the `wcrepair.sh` file by running one of the following commands:

    - If you want to run this utility directly on the Web Client node: `<path to the installer>/uc-ansible-installer/sudo ./wcrepair.sh -l -ssl reset`
    - If you want to run this utility remotely on the Web Client node: `<path to the installer>/uc-ansible-installer/sudo ./wcrepair.sh -r -ssl reset`
4. If you run this utility remotely, enter the details of the Web Client node.
   A message appears, asking you to enter the path of the new SSL certificate.
5. Enter the path of the new SSL certificate.
   `/home/administrator/myca_certs/new_cert.pem`
   The existing SSL certificate is replaced with the certificate that you have provided.

Replace the Public Keys of Remote Services

About This Task

During the installation of Web Client, the installer uses the public keys of remote services such as Apache CouchDB and UAA. This allows HTTPS communication between Web Client applications and these remote services.

If you change the SSL certificate of these remote services, the communication fails. This topic describes how to resolve this issue.

Procedure

1. Access the `wcrepair.sh` file in the `uc-ansible-installer` folder.
2. Provide execution permissions to `wcrepair.sh` file by running the following command: `sudo chmod +x your/pathto/installer/uc-ansible-installer/wcrepair.sh`
3. Run the `wcrepair.sh` file by running one of the following commands:

    - If you are running this utility directly on the Web Client node: `<installer path>/uc-ansible-installer/sudo ./wcrepair.sh -l -pkey reset`
    - If you are running this utility remotely on the Web Client node: `<installer path>/uc-ansible-installer/sudo ./wcrepair.sh -r -pkey reset`
4. At the **Enter the Web Client Installation Directory** prompt, enter the location where the Web Client is installed.
5. At the **Enter the ROOT CA path (incuding the file name)** prompt, provide the valid Certificate Authority (CA) certificate including the file name in the **.pem** format.
6. If you run this utility remotely, enter the details of the Web Client node.
   The installer reads the existing installation configuration, and updates it with the new public keys of Apache CouchDB and UAA.

Reset Passwords and Secrets of Web Client Docker Containers

About This Task

The passwords or secrets used during the installation of Web Client are converted into Docker secrets. These Docker secrets are used by the containers for communicating with remote systems such as the Plant Applications database, Apache CouchDB, RabbitMQ, and UAA.

After Web Client installation, over a period of time, if the passwords / secrets used during the installation time become are changed or reset at the source, you can update the Docker containers with the new passwords or secrets.

Procedure

1. Access the `wcrepair.sh` file in the `uc-ansible-installer` folder.
2. Provide execution permissions to `wcrepair.sh` file by running the following command: `sudo chmod +x your/pathto/installer/uc-ansible-installer/wcrepair.sh`
3. Run the `wcrepair.sh` file by running one of the following commands:
   - If you are running this utility directly on the Web Client node: `<installer path>/uc-ansible-installer/sudo ./wcrepair.sh -l -pkey -reset`
   - If you are running this utility remotely on the Web Client node: `<installer path>/uc-ansible-installer/sudo ./wcrepair.sh -r -pkey -reset`
4. If you run this utility remotely, enter the details of the Web Client node.
   The server name, database name, and database username of the Plant Applications SQL database appear. A message appears, asking you to enter the new password.
5. If you want to reset the Plant Applications database password, enter the new password. If not, press Enter.
   The host name, database name, node name, and username of Apache CouchDB appear. A message appears, asking you to enter the new password.
6. If you want to reset the Apache CouchDB password, enter the new password. If not, press Enter.
   The Message Bridge server name and RabbitMQ username appear. A message appears, asking you to enter the new password for RabbitMQ.
7. If you want to reset the RabbitMQ password, enter the new password. If not, press Enter.
   The host name and username of the UAA service appears. A message appears, asking you to enter the new password.
8. If you want to reset the UAA password, enter the new password. If not, press Enter.
   Docker secrets are created based on the values you entered, and the Docker stacks are redeployed so that the containers use the new passwords.

Docker Web Client Deployment for Scalability

About This Task

The Docker Web Client's installer has default configuration selections that are optimized for Linux machines of 32 GB RAM. With the default installation, the maximum number of concurrent clients / scalability will be limited to 10 or 12. If your scalability requirements are high and need to support over 100 concurrent client sessions, you must choose the target Linux server with 64-GB RAM. Also, before starting the installer you must perform following task.

Procedure

1. Access the `plantapps-web-docker.j2` file located in the installer folder path: `\uc-ansible-installer\roles\installer\templates\`
2. Locate and replace the below lines of code...

```
JAVA_OPTIONS_1000=-XX:MaxRAM=1000m -XX:MaxHeapSize=720m -
XX:+UnlockExperimentalVMOptions -XX:CompressedClassSpaceSize=120m
JAVA_OPTIONS_350=-XX:MaxRAM=350m -XX:MaxHeapSize=180m -
XX:+UnlockExperimentalVMOptions -XX:CompressedClassSpaceSize=120m
```

```
JAVA_OPTIONS_256=-XX:MaxRAM=350m -XX:MaxHeapSize=180m -
XX:+UnlockExperimentalVMOptions -XX:CompressedClassSpaceSize=120m
JAVA_OPTIONS_1024=-XX:MaxRAM=1024m -XX:MaxHeapSize=720m -
XX:+UnlockExperimentalVMOptions -XX:CompressedClassSpaceSize=120m
JAVA_OPTIONS_512=-XX:MaxRAM=512m -XX:MaxHeapSize=320m
XX:+UnlockExperimentalVMOptions -XX:CompressedClassSpaceSize=120m
```

...with the following lines of code:

```
JAVA_OPTIONS_1000=-XX:MaxRAM=1000m -XX:MaxHeapSize=720m -
XX:+UnlockExperimentalVMOptions -XX:CompressedClassSpaceSize=250m
JAVA_OPTIONS_350=-XX:MaxRAM=650m -XX:MaxHeapSize=500m -
XX:+UnlockExperimentalVMOptions -XX:CompressedClassSpaceSize=250m
JAVA_OPTIONS_256=-XX:MaxRAM=650m -XX:MaxHeapSize=500m -
XX:+UnlockExperimentalVMOptions -XX:CompressedClassSpaceSize=250m
JAVA_OPTIONS_1024=-XX:MaxRAM=1024m -XX:MaxHeapSize=720m -
XX:+UnlockExperimentalVMOptions -XX:CompressedClassSpaceSize=250m
JAVA_OPTIONS_512=-XX:MaxRAM=650m -XX:MaxHeapSize=500m -
XX:+UnlockExperimentalVMOptions -XX:CompressedClassSpaceSize=250m
```

3. Save and close the file.
4. Access the `plantapps-web-docker-yml.j2` file located in the following folder: `\uc-ansible-installer\roles\installer\templates\`
5. Perform the following:

    a. Search for `memory:  350M` and replace it with `memory:  650M`
    b. Search for `memory:  256M` and replace it with `memory:  650M`
    c. Search for `memory:  512M` and replace it with `memory:  650M`

6. Save and close the file.
7. Follow Install Plant Applications Web Client Using Docker on page 56 version of Web Client.
   You can now use Web Client on a machine with a 64GB RAM.

Post-Installation Repair or Upgrade for Scalability

About This Task

For some reasons, if you have performed the installation with the default settings, that is, without making any changes to the `plantapps-web-docker.j2` file as stated above and realized that the default installation is not supporting your scalibillity requirements , you can make the following changes to repair the installation to meet your scalability requirements to utilize RAM size of 64 GB.

Procedure

1. Navigate to the `plantapps-web-docker` folder located in the Web Client installation path: `/<installation_path>/PlantApplicationsDocker/plantapps-web-docker`
2. Open the **.env** file in a text editor. Locate and replace the below lines of code...

```
JAVA_OPTIONS_1000=-XX:MaxRAM=1000m -XX:MaxHeapSize=720m -
XX:+UnlockExperimentalVMOptions -XX:CompressedClassSpaceSize=120m
JAVA_OPTIONS_350=-XX:MaxRAM=350m -XX:MaxHeapSize=180m -
XX:+UnlockExperimentalVMOptions -XX:CompressedClassSpaceSize=120m
JAVA_OPTIONS_256=-XX:MaxRAM=350m -XX:MaxHeapSize=180m -
XX:+UnlockExperimentalVMOptions -XX:CompressedClassSpaceSize=120m
JAVA_OPTIONS_1024=-XX:MaxRAM=1024m -XX:MaxHeapSize=720m -
XX:+UnlockExperimentalVMOptions -XX:CompressedClassSpaceSize=120m
```

```
JAVA_OPTIONS_512=-XX:MaxRAM=512m -XX:MaxHeapSize=320m
XX:+UnlockExperimentalVMOptions -XX:CompressedClassSpaceSize=120m
```

...with the following lines of code:

```
JAVA_OPTIONS_1000=-XX:MaxRAM=1000m -XX:MaxHeapSize=720m -
XX:+UnlockExperimentalVMOptions -XX:CompressedClassSpaceSize=250m
JAVA_OPTIONS_350=-XX:MaxRAM=650m -XX:MaxHeapSize=500m -
XX:+UnlockExperimentalVMOptions -XX:CompressedClassSpaceSize=250m
JAVA_OPTIONS_256=-XX:MaxRAM=650m -XX:MaxHeapSize=500m -
XX:+UnlockExperimentalVMOptions -XX:CompressedClassSpaceSize=250m
JAVA_OPTIONS_1024=-XX:MaxRAM=1024m -XX:MaxHeapSize=720m -
XX:+UnlockExperimentalVMOptions -XX:CompressedClassSpaceSize=250m
JAVA_OPTIONS_512=-XX:MaxRAM=650m -XX:MaxHeapSize=500m -
XX:+UnlockExperimentalVMOptions -XX:CompressedClassSpaceSize=250m
```

Note: Ensure that the spaces left in the original content/lines are not changed.

3. Save and close the file.
4. In the same folder location, open the **env.yml** file in a text editor.
5. Perform the following:

   a. Search for `memory: 350M` and replace it with `memory: 650M`
   b. Search for `memory: 256M` and replace it with `memory: 650M`
   c. Search for `memory: 512M` and replace it with `memory: 650M`

   Note: Ensure that the spaces left in the original content/lines are not changed.

6. Save and close the file.
   You can now use Web Client on a machine with a 64GB RAM.
7. From the same folder location, run the following commands:

   a. `$sudo docker stack rm PAServices`
   b. `$sudo docker stack rm PAContainer`

   Note: If your application is not running, you might encounter errors that you can ignore.

   c. `$sudo docker-compose -f env.yml config > PAServices.yml`
   d. `$sudo docker stack deploy -c PAServices.yml PAServices`

   Note: The above command with deploy the Web Client's services stack which will take few minutes.

   e. `$sudo docker-compose -f env.yml config > PAContainer.yml`
   f. `$sudo docker stack deploy -c PAContainer.yml PAContainer`

   Note: The above command will deploy the Web Client's UI Applications stack that will take few minutes.

The Web Client instance will be now running with the optimally utilized system memory and will support your scalability requirements up to 150 concurrent client sessions.

Troubleshooting Web Client Installation Issues

Issue	Resolution

Unable to access Plant Applications Web Client.
 	
When you install Web Client for the first time, a self-signed certificate for the applications and services to support HTTPS is created, by default. If you have not changed or reconfigured the Plant Applications Web Client installation with a CA certificate that is added to your trust stores across the local network, you cannot access Web Client.
	1. Access the following URLs:
	  • https://<Web Client node IP address or system name>:5059/
	  • https://<Web Client node IP address or system name>:5051/
	A message appears to accept the insecure URL to proceed. Choose to do so.
	2. Select **Not Secure** in the address bar. A **Certificate** window appears.
	3. Import the certificate and add it to your trusted store.
	4. Refresh the Plant Applications Web Client window.

When you run the installer (`install.sh`) and select an option, the following error message appears: Unexpected Exception, this is probably a bug: No closing quotation	Access the `ansible.cfg` file, and comment out the following lines of code:
	<pre>strategy_plugins = ./tmp/
	mitogen-0.2.9/ansible_mitogen/
	plugins/strategy
	strategy = mitogen_linear</pre>

Multiple container restart issue.	If you have multiple container restart issue, run the following command in the web client (linux server) node:
	<pre>docker swarm update --dispatcher-
	heartbeat 120s</pre>

Chapter

6

Post Installation Configuration (Docker and Non-docker)

Topics:

Run Operations Hub Posting Utility

Before You Begin

You must have installed the Plant Applications Web Client before you run the Operations Hub Posting utility.

About This Task

You must run the utility to import the Plant Applications into Operations Hub.

Note: If Operations Hub is installed on a remote node, you must manually copy the **OperationsHub_PostingUtility** folder from the Web Client node to the Operations Hub node and then run (run as administrator) the **InstallWebComponents.cmd** file.

Procedure

1. **Docker Installation:** In the directory `<Installation_Directory>/OperationsHub_PostingUtility`, run (run as administrator) the **InstallWebComponents.cmd** file.
2. **Non-Docker Installation:** Run (run as administrator) the **InstallWebComponents.cmd** from the Web Client installation path. For example: `C:\Program Files\GE Digital \PlantApplicationsWebClient\OperationsHub_PostingUtility`.
   A console appears with a prompt to enter the Operations Hub tenant password.
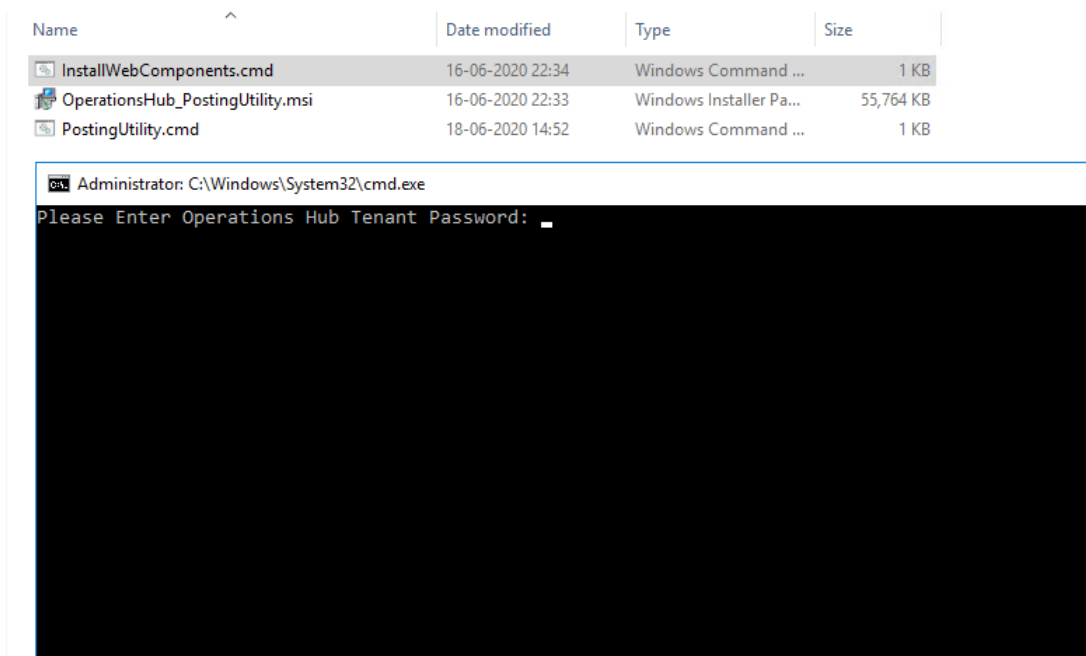
3. Enter the Operations Hub tenant password and then press **Enter**.
   You are prompted to enter the UAA Admin Client Secret.

Name	Date modified	Type	Size
InstallWebComponents.cmd	16-06-2020 22:34	Windows Command ...	1 KB
OperationsHub_PostingUtility.msi	16-06-2020 22:33	Windows Installer Pa...	55,764 KB
PostingUtility.cmd	18-06-2020 14:52	Windows Command ...	1 KB

```
Administrator: C:\Windows\System32\cmd.exe
Please Enter Operations Hub Tenant Password: *********
Please Enter UAA Admin Client Secret: _
```
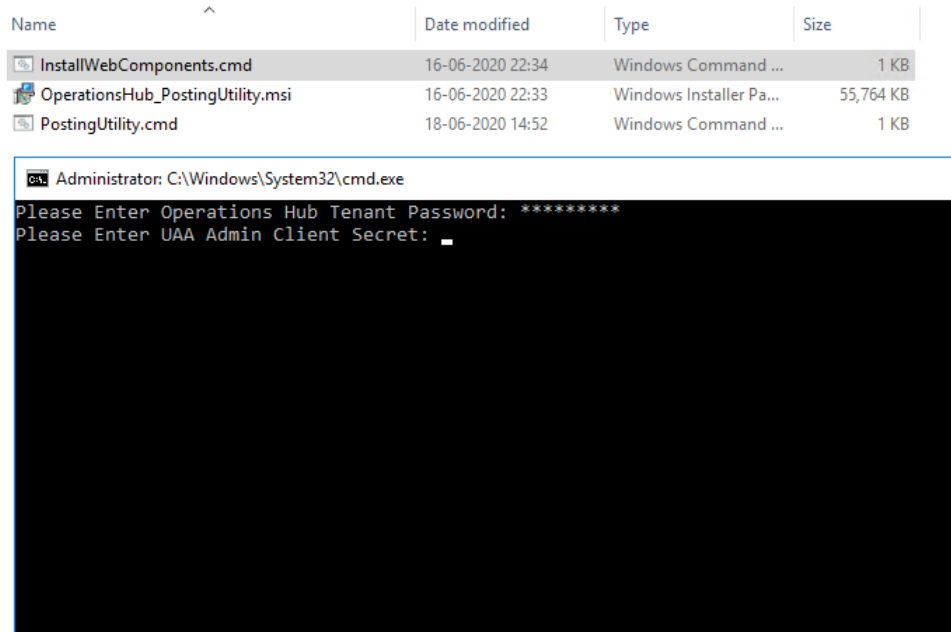
4. Enter the Client Secret to access the UAA server instance.
   The process may take some time to complete importing the Plant Applications into Operations Hub.

About UAA User Migration Utility

The UAA User Migration Utility migrates the existing set of users from the current User Account Authentication (UAA) system, such as Historian UAA, Predix, or Operations Hub to the latest version of Operations Hub UAA. Note:Only an administrator can perform this operation.

Pre-requisites

You must have one of the following applications installed on the machine on which you are performing this operation:

- Plant Applications Web Client version 8.1
- Node.js version 8 or higher

Run the Migration Utility

Procedure

1. Navigate to the folder where the utility is installed. By default, the utility is available in the following location: `C:\Program Files\GE Digital\PlantApplicationsWebClient\uaa-users-migration-utility.zip`.
2. Unzip the `uaa-users-migration-utility.zip` file.
3. Select the `runutility.bat` file.

Results

The utility launches in Google Chrome and node `app.js` command window runs in the background.

Note: Do not close the node `app.js` command window until the migration task is complete

Export UAA Users

Procedure

1. In the **SOURCE UAA LOGIN DETAILS** section, provide values as specified in the following table.

Field	Description
ADMIN CLIENT ID	The secret passphrase configured for the OAuth client.
ADMIN CLIENTSECRET	The secret passphrase configured for the OAuth client.
USER ACCOUNT AUTHENTICATION URL	URL of the server where the information is available.

2. Select **Next**.
   The details of the user in the UAA system is displayed.
3. Select the users that you want to migrate.

   - To migrate individual users, select the check box next to the respective username.
   - To migrate all the users listed in the table, select the **User Name** check box.
4. Select **Export to CSV**.

Results

A CSV file is created with details of the users and saved on your computer.

Note: This file is not encrypted.

Import UAA Users

Procedure

1. Select **Import UAA Users** from the drop-down list box of the User Account Authentication (UAA) Migration Utility.

The **DESTINATION USS LOGIN DETAILS** section appears.

2. Provide values as specified in the following table and select **Next**.

Option	
Field	**Description**
ADMIN CLIENT ID	A unique string representing the registration information provided by the client.
ADMIN CLIENT SECRET	The secret passphrase configured for the OAuth client.
USER ACCOUNT AUTHENTICATION URL	URL of the server to which the users must be migrated.

3. Drag and drop the CSV file that contains details of the users or select **Choose File** to browse and attach the CSV file.
4. Select **Next**.
   The exported details of the UAA users are displayed in a table.
5. Select the users that you want to migrate.

   • To migrate individual users, select the check box next to the respective username.
   • To migrate all the users listed in the table, select the **User Name** check box.

6. Select **Migrate Users**.

Results

The Migrated UAA Users window appears, displaying the total number of users that were migrated and errors, if any.

Note: The default password of the user after migration is the username of the user. For example, if the username is bm_operator_1, the password is bm_operator_1.

Map LDAP Groups with Operations Hub UAA

About This Task

If you want LDAP users to access Web Client and individual applications, you must map the corresponding Operations Hub UAA groups with the appropriate LDAP groups.

Before You Begin

Import UAA users.

Procedure

1. Map the iqp.user group with an appropriate LDAP group. This is required to log in to Web Client. For instructions, refer to https://www.ge.com/digital/documentation/opshub/windows/windows/t_map_ldap_groups_with_oh_uaa.html.
2. Map the Operations Hub UAA group for each application with an appropriate LDAP group. This is required to access the individual applications in Web Client.

   The following table provides a list of Operations Hub UAA groups that you map to access each application in Web Client.

Operations Hub UAA Group	Application
mes.equipment.user	OEE Dashboard
mes.reports.user	Reports
mes.downtime.user	Downtime
mes.alarms.user	Alarm Notifications
mes.security_management.user	Security
mes.activities.user	Activities
mes.my_machines.user	My Machines
mes.process_orders.user	Process Orders
mes.waste.user	Waste
mes.operations.user	Unit Operations
mes.work_queue.user	Work Queue
mes.ncm_management.user	Non Conformance
mes.order_management.user	Work Order Manager
mes.route_management.user	Route Editor
mes.property_definition.user	Property Definition
mes.configuration_management.user	Configuration
mes.time_booking.user	Time Booking
mes.approval_cockpit.user Approval	Approval Cockpit
mes.receiving_inspection.user	Receiving Inspection
mes.analysis.user	Analysis

Access Log File

The log file is located at `<utility_root_directory>/uaalog.log`.

Configure the Cache Settings for the Plant Applications Services

About This Task

The Plant Applications supports the caching and refreshing of the cached Plant Applications services after a certain time interval. You can configure the duration of the saved cached services in the `application.properties` file of the respective Plant Applications services. After the set duration, the services are cached again.

Note: Perform this task only if you want to get the updated information from the Plant Applications Server before the cache expiry time.

Procedure

1. **Docker Installation:** In the directory `<Installation_Directory>/PlantApplicationsDocker/plantapps-web-docker`, access the `env.yml` file by using the vi editor.

2. **Non-Docker Installation:** In the directory `<tomcat_home>/Apache Software Foundation/Tomcat 9.0/webapps/<service_name><version>/WEB-INF/classes`, access the `application.properties` file by using a text editor. Where:
   - *<tomcat_home>*: Is the directory where you installed Apache Tomcat. For example, `C:/Program Files`.
   - *<service_name>*: Is the service for which you want to modify the default cache properties.
   - *<version>*: Is the version of the microservice created during the installation of the Plant Applications Web Client.
3. Below is the list of cache properties with default values pertaining to the individual Plant Applications services. You can modify these default cache properties for a service based on your requirement.

Service Name	Properties
plantexecutionservice	spring_redis_timeout: 5000
	spring_redis_ttl_seconds: 300
	spring_cache_redis_use-key-prefix: "false"
	scheduler_workorder_timer_seconds: 7200
	scheduler_mes_timer_seconds: 1800
route-service	maximumProductCacheSize: 1000
	cacheProductExpireAfterAccess: "50m"
	schedulerTime: 600
route-app-service	maximumProductCacheSize: 1000
	schedulerTime: 36000
	cacheProductExpireAfterAccess: "15m"
segmentdefinitionservice	maximumCacheSize: 100
	cacheExpireAfterAccess: "50m"
operatorappservice	cacheDayExpireAfterAccess: 15m
	schedulerTime: 3600
erptransformationservice	maximumCacheSize: 100
	cacheExpireAfterWrite: 60m
alarm-app-service	maximumDayCacheSize: 100
	cacheDayExpireAfterAccess: 12h
	maximumShiftCacheSize: 100
	cacheExpireAfterShiftAccess: 8h
productionmetrics-app-service	maximumDayCacheSize: 100
	cacheDayExpireAfterAccess: 1h
	maximumWeekCacheSize: 100
	cacheWeekExpireAfterAccess: 24h
	maximumShiftCacheSize: 1
	cacheShiftExpireAfterAccess: 10m

Service Name	Properties
downtime-app-service	maximum5MinCacheSize: 100
	cacheExpireAfter5MinAccess: 5m
	maximumHourCacheSize: 100
	cacheDayExpireAfterHourAccess: 1h
	maximumDayCacheSize: 100
	cacheExpireAfterDayAccess: 24h
	maximumShiftCacheSize: 100
	cacheExpireAfterShiftAccess: 8h
processanalyzer-app-service	maximumCacheSize: 100
	cacheExpireAfterAccess: 20m
	tagVariableMaxCacheSize: 100
	tagVariableCacheTimeOut: 6h
	kpiMaxCacheSize: 40
	kpiCacheTimeOut: 30m
	siteParameterMaxCacheSize: 20
	siteParameterCacheTimeOut: 1h
productionschedulerappservice	configurationCacheExpiryTime: 30m
processorderservice	configurationCacheExpiryTime: 30m
erpexportservice	maximumCacheSize: 100
	cacheExpireAfterAccess: 5m
	cacheLaborExpireAfterAccess: 60m
	erp_export_scheduler_service_enableCleanup: "true"
	erp.export.scheduler.service.cleanupIntervalInMilliseconds: 3600000
	erp.export.scheduler.service.PublishedMessageRetentionInHours: 96
timebookingservice	maximumWeekCacheSize: 100
	cacheWeekExpireAfterAccess: 24h
	maximumShiftCacheSize: 1
	cacheShiftExpireAfterAccess: 10m
	cacheExpireAfterWrite: 1h
	maximumCacheSize: 100
erpschedulerservice	erp_scheduler_service_retrylimit: 3
	erp_scheduler_service_importJobPoll_milliseconds: 30000
	erp_scheduler_service_importJobStatusPoll_milliseconds: 30000

4. Save the changes to the `application.properties` file for the respective services that you have modified.
5. Restart the respective services in Tomcat to apply the changes.

Results

The cached services are refreshed after the duration you set in the `application.properties` file.

Configure to Route Enable a Production Line

About This Task

Only if a production line is route-enabled, you can use it in the discrete applications. This topic describes how to route-enable a production line and use it in the discrete applications.

Procedure

1. To use a production line in discrete applications, route-enable each production line that you want to use by right-clicking the production line, and selecting **Route enabled <name of the production line>**. For more information, refer to the *About Enabling a Production Line for Using a Route* topic in the Plant Applications Administrator Help.

2. To import route-enabled production lines from one Plant Applications server to another, perform the following steps:

   a. Export the production lines and related data from the source server.
   b. In the destination server, create a sample production line, and add a sample unit.
   c. Right-click the production line that you have created, and select **Route enabled <name of the production line>**.
   d. Import the production lines and related data to the destination server.
   e. Right-click each production line that you have imported, and then select **Route enabled <name of the production line>**.

      You can now use the production lines in discrete applications using the destination Plant Applications server.

Chapter

7

Troubleshooting

Topics:

Frequently Asked Questions (Non-Docker only)

- Can I access the log files created after the Plant Applications Web Client installation or upgrade process?

  Yes. You can access the log files created during the installation process from the following directory: `%USERPROFILE%\APPDATA\Local\Temp`. The log files are available in the format `Plant_Applications_Universal_Client_yyddmmhhmmss`.

- What happens if I upgrade JAVA after installing the Plant Applications Web Client?

  If you upgrade JAVA later, it might create some issues in using the Plant Applications Web Client, and Tomcat might stop. To resolve this issue, refer to the Community article 000020691 in the support site http://support.ge-ip.com.

- What should I do if the installation of GE Proficy Historian Server fails?

  If Transport Layer Security (TLS) 1.1 or 1.2, or the security policy for using the FIPS compliant algorithms is enabled, the Historian installation process fails. To install Historian successfully, you must temporarily disable the required feature, and then after successful Historian installation enable the feature again.

Troubleshoot the Tomcat Error

About This Task

The following **Tomcat** screen appears when you try to upgrade the Plant Applications Web Client and there is an issue with the Tomcat service.
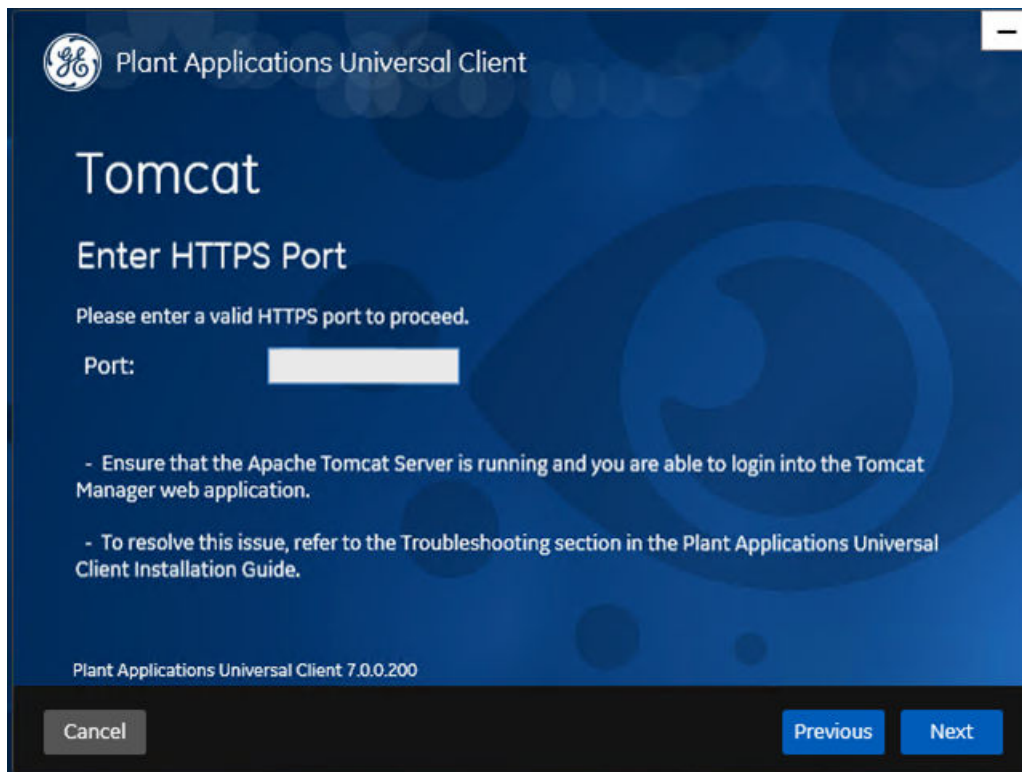
To troubleshoot the Tomcat service error, perform the following steps:

Procedure

1. In the **Tomcat** window, ensure that you have entered the correct **HTTPS** port to continue with the installation.

2. Ensure that the Tomcat service is running.

   a. Log in to the computer where you installed the Plant Applications Web Client.

   b. Select **Start**, and then search for the Services application.

   c. In the command prompt, enter `services.msc`.

   The **User Account Control** window appears.

   d. Select **Yes**.

   The **Services** window appears.

   e. Verify that the **Status** of the Tomcat service configured during the Plant Applications Web Client installation appears as **Running**. If not, start the service.
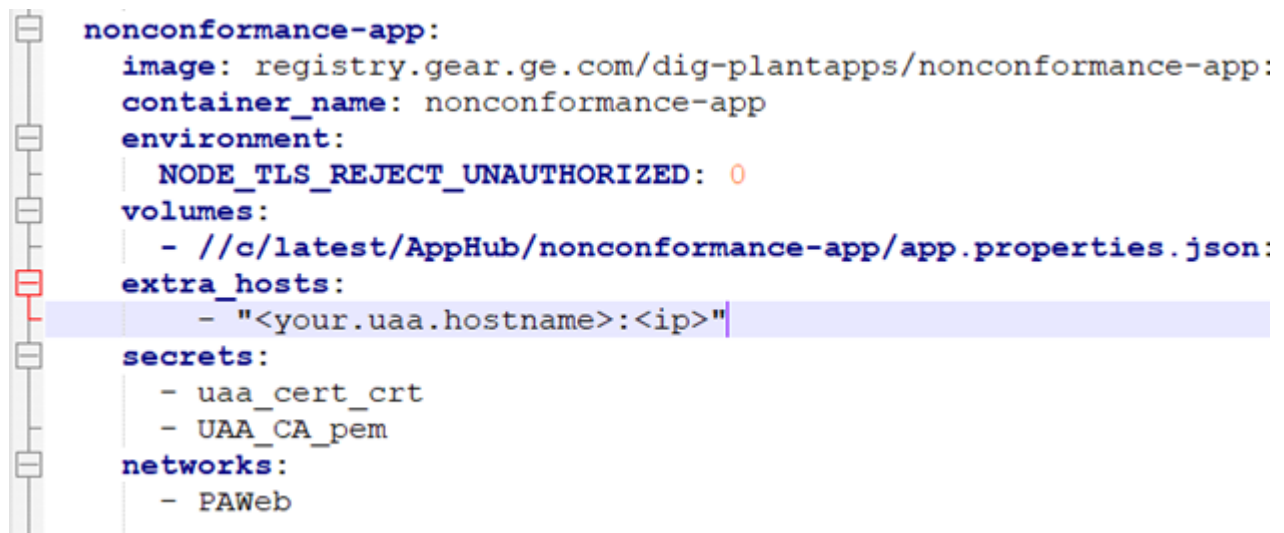
Troubleshoot Access Issues

This topic describes how to troubleshoot issues when you cannot access Operations Hub UAA, Apache CouchDB, or the Plant Applications database using the host name from the machine on which Docker has been installed. This is applicable only if you have installed Plant Applications Web Client using Docker.

Procedure

1. If the Operations Hub UAA server is not accessible using the host name from the machine on which Docker has been installed, perform the following steps:

   a) For each application that will be deployed in Plant Applications Web Client, add the following line in the `plantapps-web-docker/env.yml` and `plantapps-universal-client/env.yml` files:

   ```
   extra_hosts:
        - "<host name of the UAA server>:<IP address of the UAA
   server>"
   ```

   ```
   nonconformance-app:
       image: registry.gear.ge.com/dig-plantapps/nonconformance-app:
       container_name: nonconformance-app
       environment:
         NODE_TLS_REJECT_UNAUTHORIZED: 0
       volumes:
         - //c/latest/AppHub/nonconformance-app/app.properties.json:
       extra_hosts:
           - "<your.uaa.hostname>:<ip>"
       secrets:
         - uaa_cert_crt
         - UAA_CA_pem
       networks:
         - PAWeb
   ```

   b) Using the Command Prompt, change the directory to `plantapps-web-docker`, and run the following command: `./PA_Services_Start_Lix.sh`

c) Using the Command Prompt, change the directory to `plantapps-universal-client`, and then run the following command: `./PA_Apps_Start_Lix.sh`

2. If the Apache CouchDB UAA server is not accessible using the host name from the machine on which Docker has been installed, perform the following steps:

a) For each application that will be deployed in Plant Applications Web Client, add the following line in the `plantapps-web-docker/env.yml` and `plantapps-universal-client/env.yml` files:

```
extra_hosts:
    - "<host name of the UAA server>:<IP address of the UAA
server>"
```

b) Using the Command Prompt, change the directory to `plantapps-web-docker`, and run the following command: `./PA_Services_Start_Lix.sh`

c) Using the Command Prompt, change the directory to `plantapps-universal-client`, and then run the following command: `./PA_Apps_Start_Lix.sh`

3. If the Plant Applications Web Client server is not accessible using the host name from the machine on which Docker has been installed, perform the following steps:

a) For each application that will be deployed in Plant Applications Web Client, add the following line in the `plantapps-web-docker/env.yml` and `plantapps-universal-client/env.yml` files:

```
extra_hosts:
    - "<host name of the UAA server>:<IP address of the UAA
server>"
```

b) Using the Command Prompt, change the directory to `plantapps-web-docker`, and run the following command: `./PA_Services_Start_Lix.sh`

c) Using the Command Prompt, change the directory to `plantapps-universal-client`, and then run the following command: `./PA_Apps_Start_Lix.sh`

Renew the Docker Certificate

If Docker-based Plant Applications Universal Client machine is shut down during the 90-day interval period, Docker swarm stops working due to certificate expiry. This is a workaround to renew the expired swarm certificates.

Procedure

1. Stop the Docker service using the following command: `sudo service docker stop`
2. Modify the system date to a previous date (that is, a date before the certificate expired) using the following command: `sudo date -s "04 Feb 2020 11:00:00"`
3. Start the Docker service using the following command: `sudo service docker start`
4. Generate new certificates using the following command: `sudo docker swarm ca -rotate`
5. Stop the Docker service using the following command: `sudo service docker stop`
6. Set the system date to current time using the following command: `sudo date -s "04 Feb 2020 11:00:00"`
7. Start the Docker service using the following command: `sudo service docker start`

Chapter

8

Reference

Topics:

- Configure the GE Proficy
  Historian Server Security
  Settings

Configure the GE Proficy Historian Server Security Settings

About This Task

Configure the security settings in the GE Proficy Historian Server to enable the Plant Applications Web Client to use the GE Proficy Historian Server as the User Account and Authentication (UAA) server.

Procedure

1. Log in to the Proficy Historian Administrator.
2. Select **DataStores**.
3. Select the **Security** tab.
4. In the **Enforce Strict Client Authentication** row, select **Disabled**.
5. In the **Enforce Strict Collector Authentication** row, select **Disabled**.
6. Select **Update**.
   The GE Proficy Historian Server is now configured for the Plant Applications Web Client. You can now install the Plant Applications Web Client on the same computer as the GE Proficy Historian Server.