



# Proficiency Plant Applications 8.2

## Web Client Installation Guide



**Proprietary Notice**

The information contained in this publication is believed to be accurate and reliable. However, General Electric Company assumes no responsibilities for any errors, omissions or inaccuracies. Information contained in the publication is subject to change without notice.

No part of this publication may be reproduced in any form, or stored in a database or retrieval system, or transmitted or distributed in any form by any means, electronic, mechanical photocopying, recording or otherwise, without the prior written permission of General Electric Company. Information contained herein is subject to change without notice.

© 2021, General Electric Company. All rights reserved.

**Trademark Notices**

GE, the GE Monogram, and Predix are either registered trademarks or trademarks of General Electric Company.

Microsoft® is a registered trademark of Microsoft Corporation, in the United States and/or other countries.

All other trademarks are the property of their respective owners.

We want to hear from you. If you have any comments, questions, or suggestions about our documentation, send them to the following email address:

[doc@ge.com](mailto:doc@ge.com)

<b>Chapter 1. Installation Overview.....</b>	<b>5</b>
Installation Overview.....	5
<b>Chapter 2. Pre-installation Configuration (Enterprise and Standard).....</b>	<b>6</b>
Configuring Apache CouchDB Settings.....	6
<b>Chapter 3. Installing Plant Applications Standard Web Client.....</b>	<b>8</b>
About Installing Standard Web Client.....	8
Standard Edition Web Client Requirements.....	8
Install Standard Web Client.....	10
About Post-Installation Tasks.....	28
Add a UAA User.....	28
Modify the Batch File to Add the User Details.....	28
Disable Discrete Applications.....	30
Enable Discrete Applications.....	31
Performance Tuning Settings.....	32
Node Application Manager Utility.....	34
Uninstall Standard Web Client.....	36
Restart Services using Tomcat Manager.....	36
<b>Chapter 4. Upgrade Plant Applications Standard Web Client.....</b>	<b>39</b>
Upgrade the Plant Applications Standard Web Client.....	39
Access Existing ThingWorx Custom Application.....	55
<b>Chapter 5. Installing Plant Applications Enterprise Web Client.....</b>	<b>56</b>
About Installing Enterprise Edition Web Client.....	56
Enterprise Edition Web Client Requirements.....	57
Files Provided by GE.....	59
Pre-Installation Checklist.....	60
Create and Configure Docker Registry.....	61
Install Enterprise Edition Web Client.....	63
Replace the SSL Certificate of Enterprise Edition Web Client.....	67
Replace the Public Keys of Remote Services.....	68
Reset Passwords and Secrets of Enterprise Edition Web Client Docker Containers.....	69
Enterprise Edition Web Client Deployment for Scalability.....	71
Disable Discrete Applications.....	74

Enable Discrete Applications.....	75
Reconfigure Enterprise Web Client after upgrading Operations Hub.....	76
Troubleshooting Enterprise Edition Web Client Installation Issues.....	76
<b>Chapter 6. Post Installation Configuration (Enterprise and Standard).....</b>	<b>78</b>
Run Message Bridge Configuration Utility.....	78
Run Operations Hub Posting Utility.....	82
Verify the Installation.....	83
Access REST APIs.....	83
Configure a GE Proficy Historian Server for the Analysis Application.....	85
Configure the Cache Settings for the Historian Tags.....	86
Configure the Cache Settings for the Plant Applications Services.....	88
Configure to Route Enable a Production Line.....	92
<b>Chapter 7. Troubleshooting.....</b>	<b>94</b>
Troubleshoot Access Issues.....	94
Renew the Docker Certificate.....	95
Access Application Log Files.....	96
Access Connection Properties.....	98
About UAA User Migration Utility.....	99
Run the Migration Utility.....	99
Export UAA Users.....	99
Import UAA Users.....	100
Map LDAP Groups with Operations Hub UAA.....	101
Swagger Url Authorization Issue.....	103
Replace the Expired Self-Signed Certificate.....	103
<b>Chapter 8. Reference.....</b>	<b>104</b>
Configure the GE Proficy Historian Server Security Settings.....	104

# Chapter 1. Installation Overview

## *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:

- [Standard Installation \(page 8\)](#): This is used to install Plant Applications Web Client for both Process and Discrete applications on a Windows machine. 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.
- [Enterprise Installation \(page 56\)](#): This is used to install Plant Applications Web Client for both Process and Discrete applications on a Linux machine. 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 \(page 94\)](#) section in this guide.

# Chapter 2. Pre-installation Configuration (Enterprise and Standard)

## *Configuring Apache CouchDB Settings*

- By default, CouchDB only runs on the local host using HTTP protocol and on port number 5984. To ensure that CouchDB runs on HTTPS, you must execute the **config\_couchDB.bat** file provided with ISO.
- Perform this step only if you are installing Plant Applications Web Client for the first time.
- CouchDB 2.3.1 must be installed on a Windows machine.

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.

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`

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/`.

### **Note:**

- By default, the CouchDB HTTPS port number is 6984.
- To configure CouchDB with SSL, use certificates issued to the CouchDB server (machine) name. Do not use Operations Hub generated certificate if Operations Hub and CouchDB are on different servers.

You must now create a CouchDB user for using it in the Plant Applications Web Client installation.

4. Access the CouchDB url in a browser `https://<host name or IP address of Apache CouchDB>:<port number>/_utils/` and create a user that can be used in the Plant Applications Web Client installation.

# Chapter 3. Installing Plant Applications Standard Web Client

## *About Installing Standard Web Client*

Installing Plant Applications Standard Web Client 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.

The following table outlines the steps that you must complete to install Plant Applications Standard Web Client for the first time. These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed. All steps are required unless otherwise noted.

Step	Task	Notes
1	Install Operations Hub 2.0	This step is required.
2	<a href="#">Configure CouchDB for HTTPS (page 6)</a>	This step is required.
3	<a href="#">Ensure that your system meets the requirements for the Standard Web Client installation. (page 8)</a>	This step is required.
4	<a href="#">Install Standard Web Client (page 10)</a>	This step is required.
5	<a href="#">After the Standard Web Client installation, ensure to run the Message Bridge Configuration utility. (page 78)</a>	This step is required.
6	<a href="#">After configuring Message Bridge, ensure to run the Operations Hub Posting utility. (page 82)</a>	This step is required.
7	<a href="#">Verify the Installation (page 83)</a>	This step is required.

## *Standard Edition Web Client Requirements*

### **Before you begin**

Ensure that you have completed following tasks :

- Installation of Plant Application Server
- Installation of Operations Hub 2.0.
- [Configure CouchDB for HTTPS \(page 6\)](#)








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

- [System requirements \(page 9\)](#)
- [Port requirements \(page 10\)](#)

## 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
Operating system	64-bit Windows 10, Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019
Couch DB server	CouchDB version 2.3.1 installed and configured on a Windows machine.   <b>Note:</b> For more information on configuring CouchDB, refer to <a href="#">Configuring Apache CouchDB Settings (page 6)</a> .
Web browsers	Chrome 85.0 or later , with minimum resolution 1366x768.  <b>Devices:</b> <ul style="list-style-type: none"> <li>• <b>iPad:</b> Safari v13.1+, Chrome 85.0 or later with resolution 2048x1536</li> <li>• <b>HP tablet:</b> Chrome 85.0 or later , with minimum resolution 1920x1280</li> </ul>  <b>Note:</b> Devices supports only Unit Operations, Work Queue, and Non Conformance applications.
OLEDB Driver	Microsoft OLE DB Driver 18 for SQL Server   <b>Note:</b> You can download the Microsoft OLE DB Driver 18 for SQL Server from the following URL: <a href="https://www.microsoft.com/en-us/download/details.aspx?id=56730">https://www.microsoft.com/en-us/download/details.aspx?id=56730</a> .
Hard drive	100 GB (minimum)
Processor	2.4 GHz clock-speed Intel Core i3, i5, or i7 CPU or equivalent AMD Phenom CPU   <b>Note:</b> For better performance, it is recommended to use a octa core (8-cores) processor.

Item	Version
Memory	32 GB (recommended)   <b>Note:</b> You must have 64 GB or more if you plan to install Web Client (Both Process and Discrete), Historian, Operations Hub, and Plant Applications 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.
8090/8091	The default port for the Tomcat server.
1433	The default port for the Microsoft SQL server.
9093	The default port for Kafka.
2185	The default port for ZooKeeper.
6984	The default port for CouchDB.
5059	The default port for Web Applications

## *Install Standard Web Client*

Perform the [preinstallation tasks \(page 8\)](#).

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 8.2** screen.

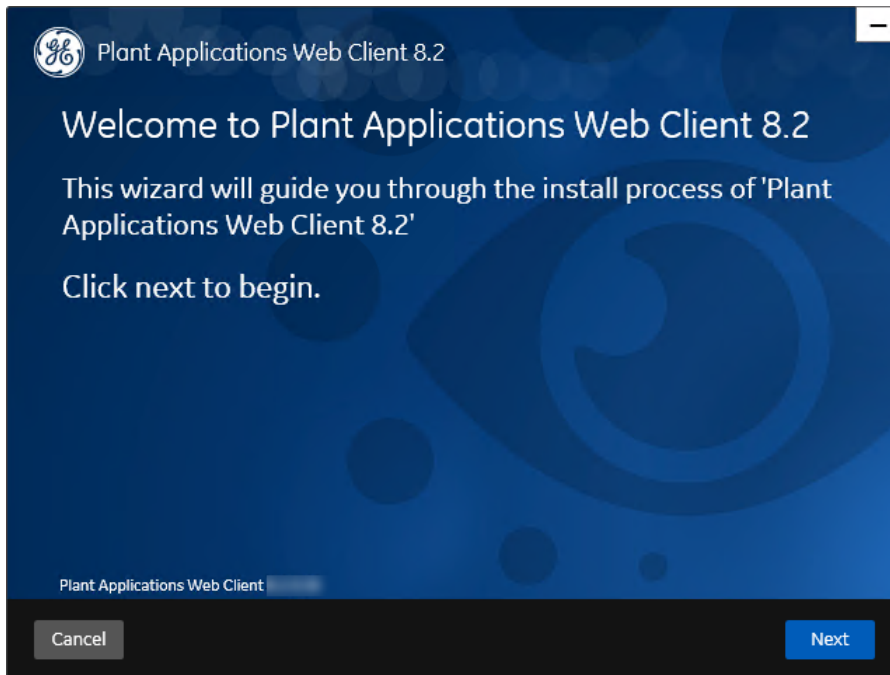


**i Tip:** You can hover over each task that appears in the installation menu to refer to the tooltip associated with that task.

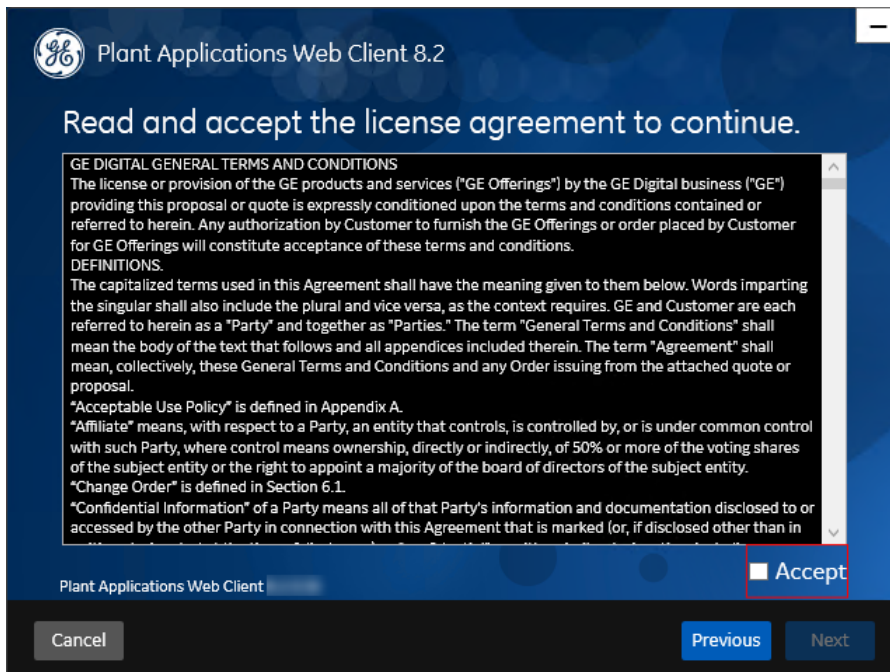
**📄 Note:** Ensure that you have installed the Microsoft Visual C++ 2015 Redistributable (64-bit) package.

### 3. Select **Plant Applications Web Client**.

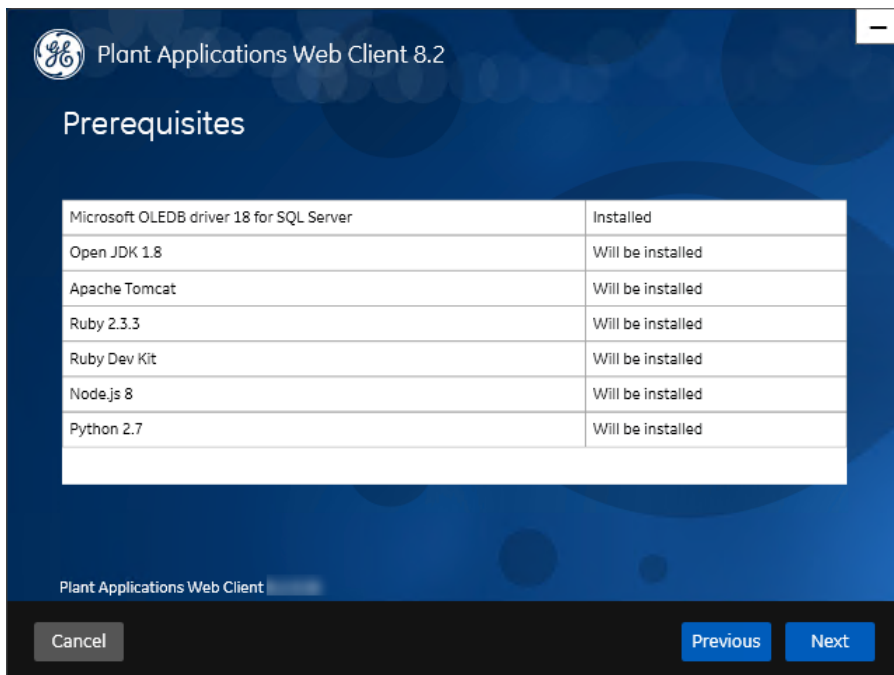
The Plant Applications Web Client installation wizard appears, displaying the **Welcome to Plant Applications Web Client 8.2** screen.



4. In the **Welcome to Plant Applications Web Client 8.2** screen, select **Next**. The **Read and accept the license agreement to continue** screen appears.



5. Read the license agreement, select **Accept**, and then select **Next** to continue the installation. The **Prerequisites** screen appears.




If any of the following required software packages are not already installed on your computer, the installer installs them automatically:

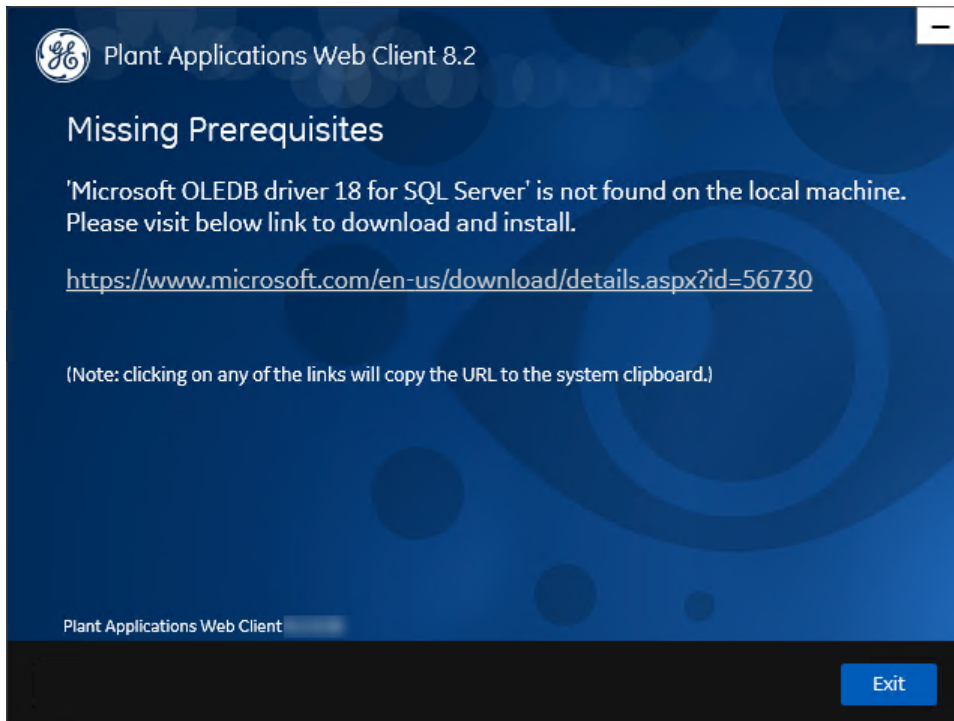
- Apache Tomcat version 9.0.35
- Ruby 2.3.3
- Ruby DevKit version 4.65.0.0

 **Note:**

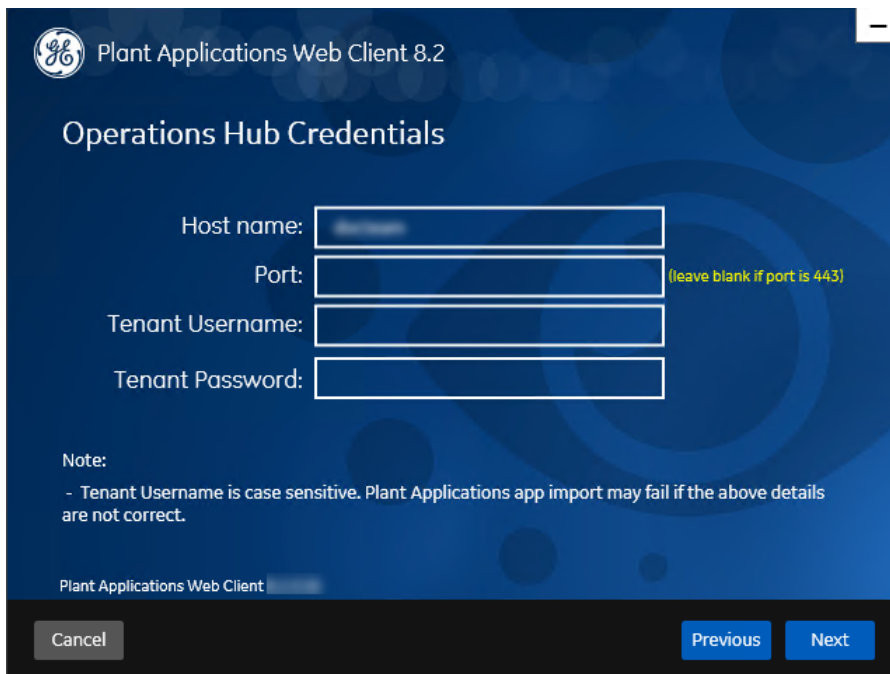
Ruby is required because the UAA Command Line Interface (UAAC) is dependent on Ruby.

- NodeJS 8.12
- Python 2.7.2
- OpenJDK 1.8


 **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.






6. In the **Prerequisites** screen, select **Next** to view all installed prerequisites and install any missing prerequisites.  
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.

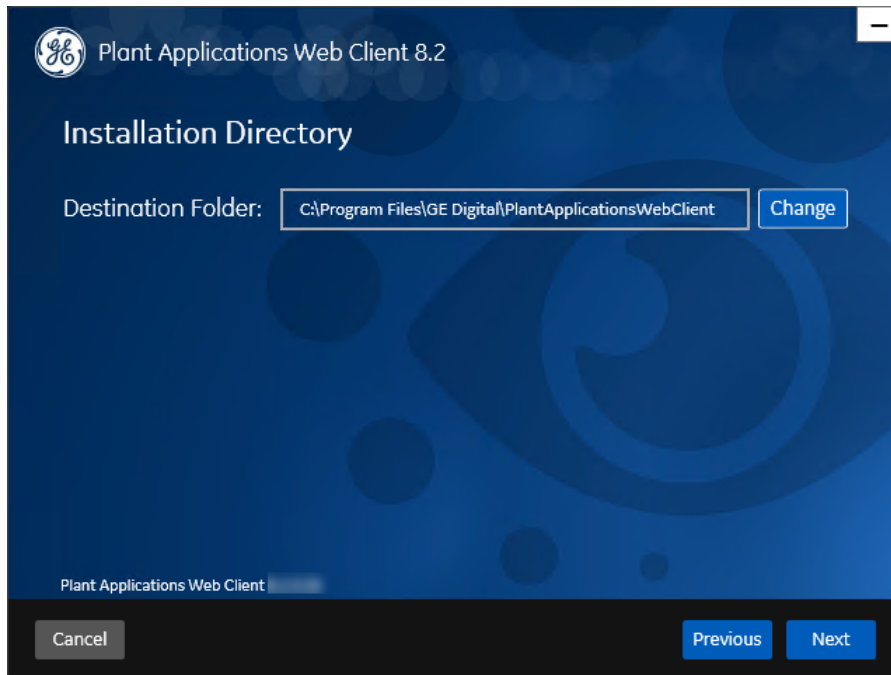
 **Note:** Ensure that you use lower case when entering the server names through out the installation.

Credential	Description
Server Name	<p>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.</p> <p> <b>Note:</b> Instead of IP address, it is recommended to use the Operations Hub host name (computer name).</p>
Port	Enter the Operations Hub port number.
Tenant Username	<p>Enter the tenant Hub username to access the Operations Hub server instance.</p> <p> <b>Note:</b> The default user name is <code>ophubAdmin</code>.</p>
Tenant Password	<p>Enter the password for the user name you entered in the <b>Tenant Username</b> box.</p> <p> <b>Note:</b> The tenant username and password must be same as the credentials that you have specified during the Operations Hub installation.</p>


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 **UAA Credentials** screen appears.



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

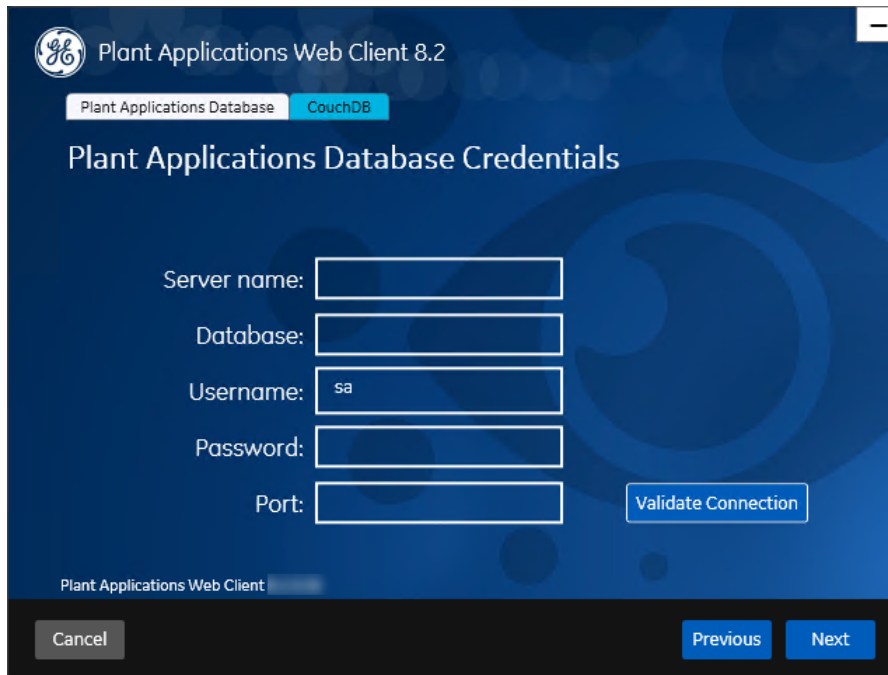
Credential	Description
Server Name	Enter the host name of the UAA server.  <b>Note:</b> Instead of IP address, it is recommended to use the UAA host name (computer name).
Port	Enter the UAA port number.  <b>Note:</b> You can leave this field blank if you are using the default port number (443).
Admin Client ID	Enter the admin Client ID to access the UAA server instance.  <b>Note:</b> The default user name is <code>admin</code> .
Admin Client Secret	Enter the Client Secret for the user name you entered in the <b>Admin Client ID</b> box.

Credential	Description								
Validate	<p>Select <b>Validate</b> to validate the UAA server connection.</p> <p> <b>Note:</b> The following table describes each icon indicating a validation status that might appear during the validation process.</p> <table border="1" data-bbox="440 396 1414 615"> <thead> <tr> <th data-bbox="440 396 927 436">Icon</th> <th data-bbox="927 396 1414 436">Description</th> </tr> </thead> <tbody> <tr> <td data-bbox="440 436 927 497"></td> <td data-bbox="927 436 1414 497">Indicates that the validation is in progress.</td> </tr> <tr> <td data-bbox="440 497 927 558"></td> <td data-bbox="927 497 1414 558">Indicates that the validation was successful.</td> </tr> <tr> <td data-bbox="440 558 927 615"></td> <td data-bbox="927 558 1414 615">Indicates that the validation was unsuccessful. In this case, make sure you enter the correct password.</td> </tr> </tbody> </table>	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.
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.

12. Select **Next**.


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






13. In the **Plant Applications Database Credentials** screen, 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 <code>HOST_NAME \INSTANCE</code> . Where <code>HOST_NAME</code> is the host name (either a fully qualified domain name or IP address, of the server) and <code>INSTANCE</code> is the instance of the server used by the database.   <b>Note:</b> If there is no instance for the server, you can enter <code>HOSTNAME</code> as the server name. <code>localhost</code> is not an acceptable value for <code>HOSTNAME</code> .
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 <b>Database</b> box. By default, the user name appears as <code>sa</code> .
Password	Enter the password for the user name you entered in the <b>Username</b> box.
Port	Optional: Enter the number of the port that the instance uses to listen for client connections.   <b>Note:</b> The default port is 1433.

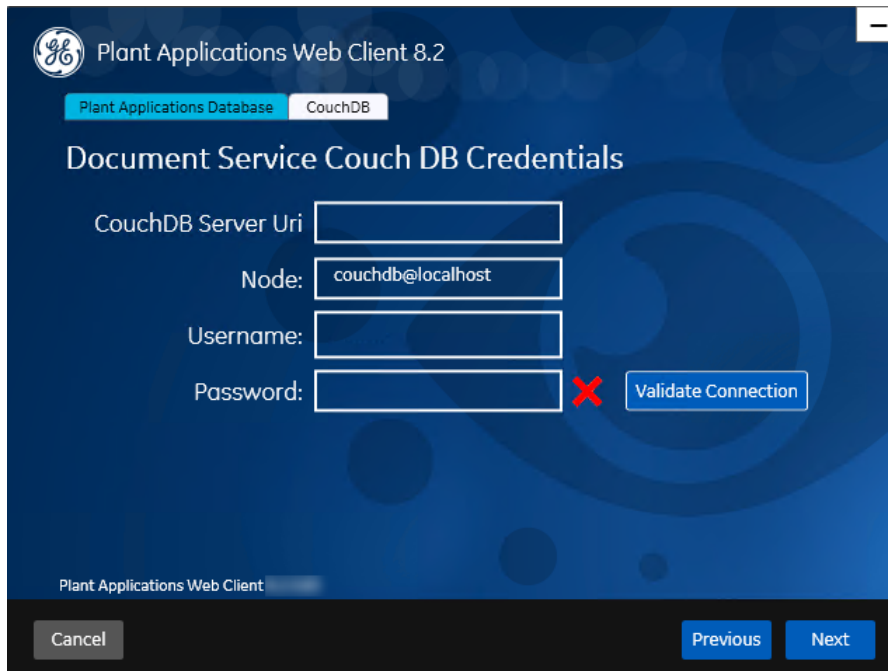
14. Select **Validate Connection** to validate the database connection.

 **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.

15. In the **Plant Applications Database Credentials** screen, select the **CouchDB** tab. The **Document Service Couch DB Credentials** section appears.



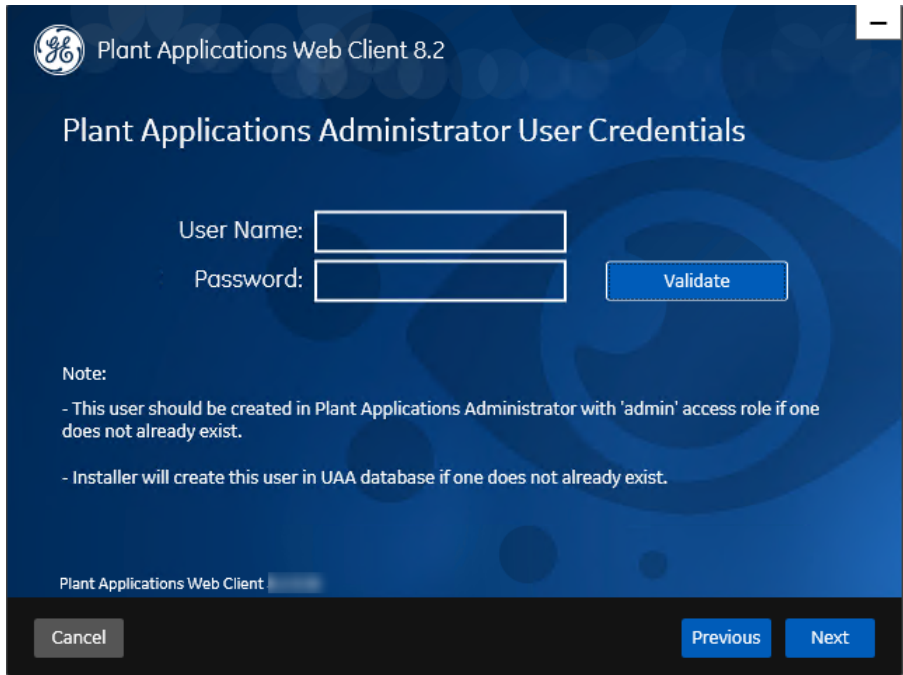
16. In the **Document Service Couch DB Credentials** section, enter the Couch DB credentials as described in the following table.

Credential	Description								
CouchDB Server Uri	Enter the fully qualified web address of Apache CouchDB in the format: <code>https://&lt;host name or IPaddress&gt;:&lt;port number&gt;</code> .								
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 <b>Database</b> box.								
Password	Enter the password for the user name you entered in the <b>Username</b> box.								
Validate	<p>Select <b>Validate Connection</b> to validate the Apache CouchDB database credentials.</p> <p> <b>Note:</b> The following table describes each icon indicating a validation status that might appear during the validation process.</p> <table border="1"> <thead> <tr> <th>Icon</th> <th>Description</th> </tr> </thead> <tbody> <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> </tbody> </table>	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.
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.











17. Select **Next**.

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



18. 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 <b>User Name</b> box.								
Validate	<p>Select <b>Validate</b> to validate the Plant Applications Administrator credentials.</p> <p> <b>Note:</b> The following table describes each icon indicating a validation status that might appear during the validation process.</p> <table border="1" data-bbox="440 1604 1414 1822"> <thead> <tr> <th data-bbox="440 1604 927 1646">Icon</th> <th data-bbox="927 1604 1414 1646">Description</th> </tr> </thead> <tbody> <tr> <td data-bbox="440 1646 927 1705"></td> <td data-bbox="927 1646 1414 1705">Indicates that the validation is in progress.</td> </tr> <tr> <td data-bbox="440 1705 927 1764"></td> <td data-bbox="927 1705 1414 1764">Indicates that the validation was successful.</td> </tr> <tr> <td data-bbox="440 1764 927 1822"></td> <td data-bbox="927 1764 1414 1822">Indicates that the validation was unsuccessful. In this case, make sure you enter the correct password.</td> </tr> </tbody> </table>	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.
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.

19. Select **Next**.




The **Tomcat Installation** screen appears.


The screenshot shows the 'Tomcat Installation' screen with the following details:

- Port: 8090
- Redirect Port: 8444
- Username: admin
- Roles: manager-gui,admin-g
- Password: (empty, highlighted with a red box)
- Re-enter Password: (empty, highlighted with a red box)

Buttons at the bottom: Cancel, Previous, Next.

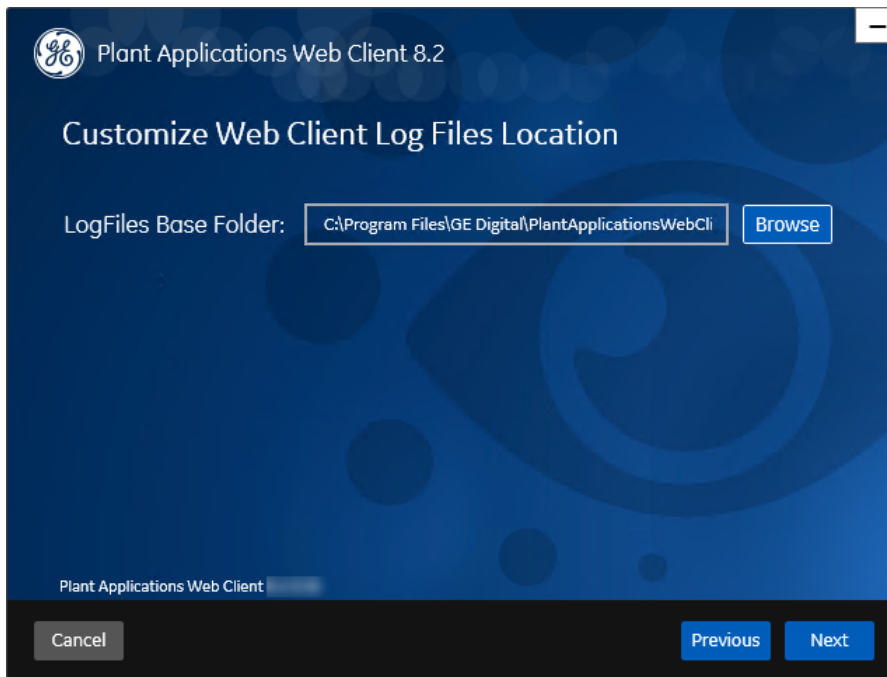
20. In the **Tomcat Installation** screen, enter the Tomcat installation details for a new or existing installation as described in the following table. The installer prompts you to enter details for an existing Tomcat if the Tomcat installation details are available in the registry settings for the 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.  <b>Note:</b> The default port is 8081.
Redirect Port	Enter the HTTPS port that Tomcat uses to redirect all HTTP requests to this port.  <b>Note:</b> The default redirect port is 8444.
Username	Enter the user name to access Tomcat.  <b>Note:</b> The default user name is <code>admin</code> .
Roles	Skip this box because it is automatically populated.

Installation Detail	Description
Password	Enter the password for the user name you entered in the <b>Username</b> box.
Re-enter Password	Reenter the password for the user name entered in the <b>Username</b> box.   <b>Note:</b> This box appears only when a new installation of Tomcat is initiated by the installer.

21. Select **Next**.

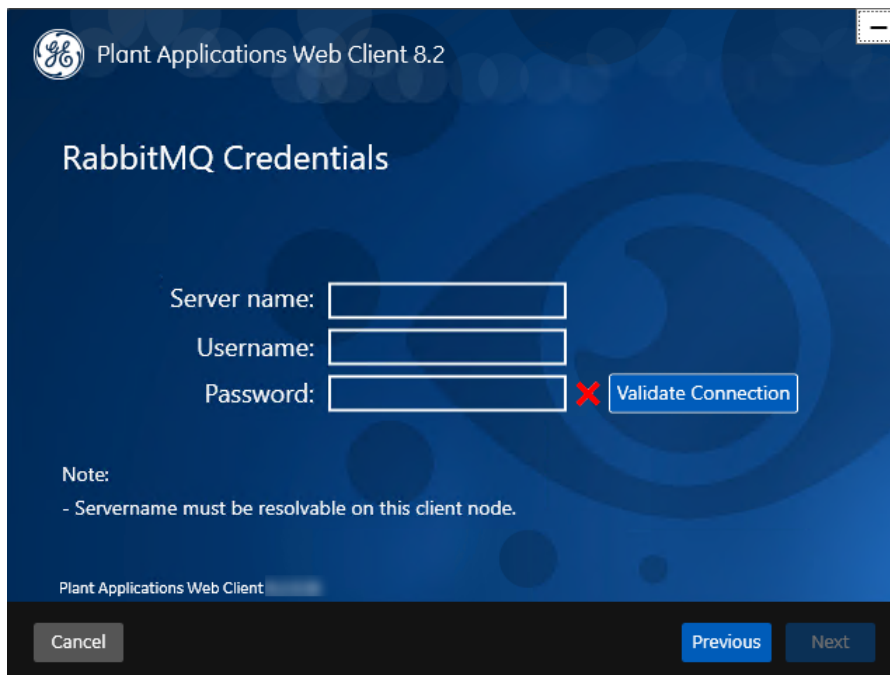
The **Customize Web Client Log Files Location** screen appears.



22. **Optional:** In the **LogFiles Base Folder** box, select **Browse** to browse and select the directory where you want to install the Plant Applications Web Client service logs.

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

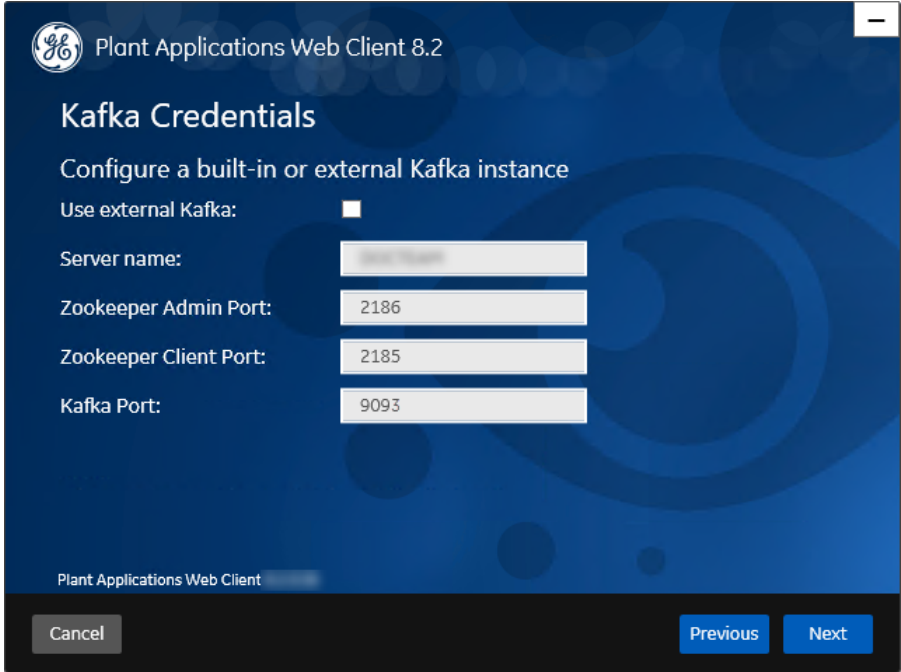
The following table describes each icon indicating a validation status that might appear during the validation process.

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. Make a note of the kafka port number that is listed for configuring Message Bridge after the Web Client installation.



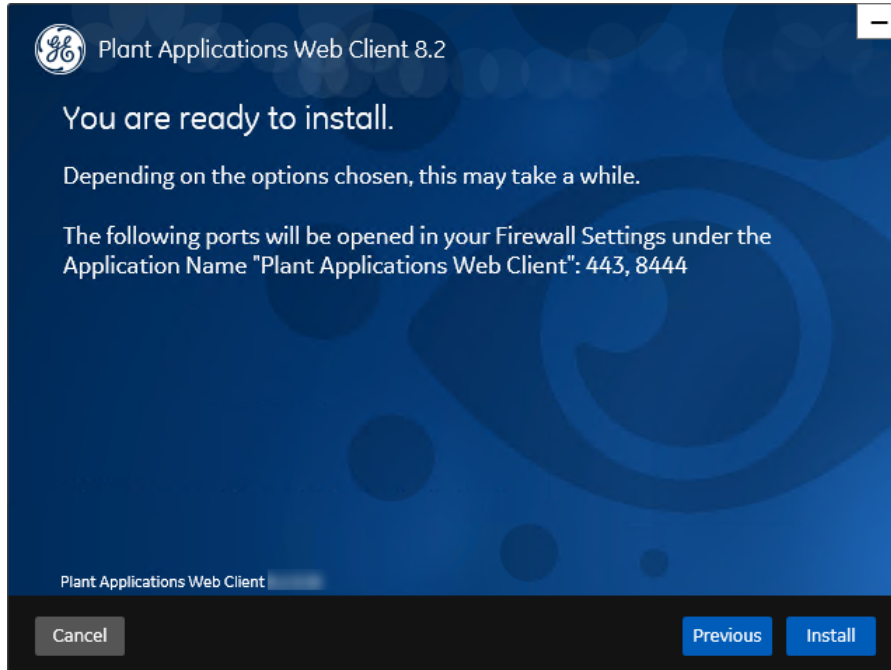
26. In the **Kafka Credentials** screen, enter the credentials to access the Kafka server as described in the following table.

Credential	Description
Use external Kafka	Select this check box if you want to configure an external Kafka instance.
Server Name	Enter the host name of the Kafka server.   <b>Note:</b> Instead of IP address, it is recommended to use the Kafka host name (computer name).
Zookeeper Admin Port	Enter the Zookeeper Admin port number.
Zookeeper Client Port	Enter the Zookeeper Client port number.   <b>Note:</b> Ensure that you have entered a valid Zookeeper port number. If you have entered an invalid port number, refer to <b>Changing the Zookeeper Port Number</b> section in <i>Getting Started Guide</i> .
Kafka Port	Enter the Kafka port number.
Zookeeper Client Port	Enter a valid Zookeeper Client port number.

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

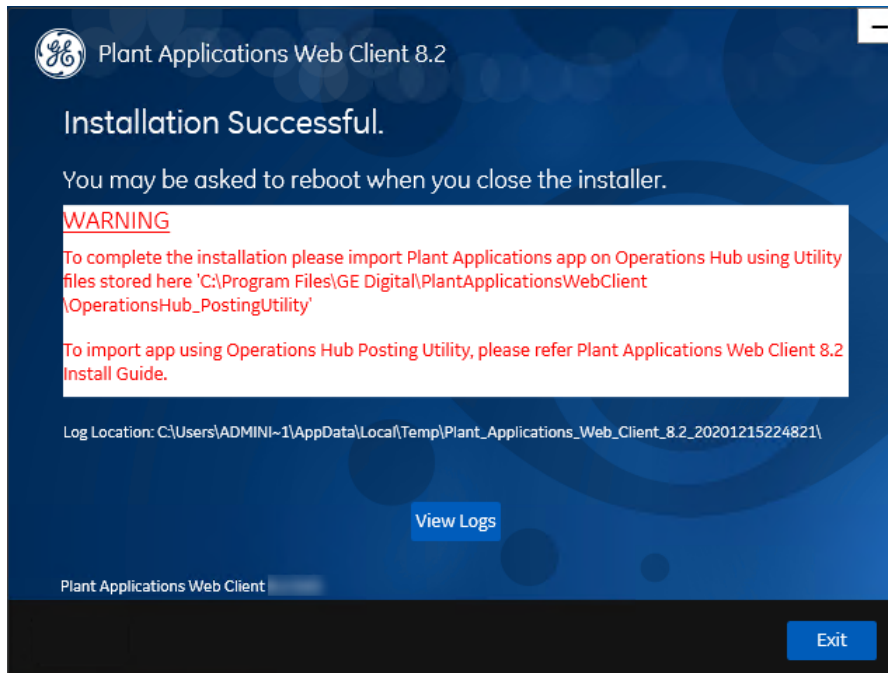
27. Select **Next**.

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 Message Bridge Configuration Utility \(page 78\)](#) on the Plant Applications Server to update the Kafka details in the Message Bridge configuration.
  32. [Run Operations Hub Posting Utility \(page 82\)](#) to import the Plant Applications into the Operations Hub.
  33. Once you have completed running Message Bridge Configuration and Operations Hub Posting utilities, [Verify the Installation \(page 83\)](#) to verify if the Plant Applications Web Client applications are up and running.
  34. [Access REST APIs \(page 83\)](#) to access the REST APIs for Plant Applications Web Client.
- Perform the [post-installation steps \(page 28\)](#).

## About Post-Installation Tasks

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

- [Add a UAA user \(page 28\)](#).
- [Configure a GE Proficy Historian Server for the Analysis application \(page 85\)](#).
- [Configure the cache settings for the Historian tags used in the Analysis application \(page 86\)](#).

### Add a UAA User

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

Ensure that you [modify the PA\\_UAA\\_Config\\_Win.bat file to add the user details \(page 28\)](#).

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.

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

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
<code>bm-operator</code>	<code>&lt;user name created during installation&gt;</code>
<code>bm-line-leader</code>	<code>bm_lineleader_1</code>

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
<code>call uaac user add &lt;user name created during installation&gt; -p test --emails &lt;user name created during installation&gt;@xx.com</code>	<code>call uaac user add john -p test --emails john@xx.com</code>
<code>call uaac member add trend_client.read &lt;user name created during installation&gt;</code>	<code>call uaac member add trend_client.read john</code>
<code>call uaac member add trend_client.write &lt;user name created during installation&gt;</code>	<code>call uaac member add trend_client.write john</code>
<code>call uaac member add bm-operator &lt;user name created during installation&gt;</code>	<code>call uaac member add bm-operator john</code>
<code>call uaac member add historian_rest_api.read &lt;user name created during installation&gt;</code>	<code>call uaac member add historian_rest_api.read john</code>
<code>call uaac member add historian_rest_api.write &lt;user name created during installation&gt;</code>	<code>call uaac member add historian_rest_api.write john</code>

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
<code>call uaac user add bm_lineleader_1 -p test --emails bm_lineleader_1@xx.com</code>	<code>call uaac user add lisa -p test --emails lisa@xx.com</code>
<code>call uaac member add bm-line-leader bm_lineleader_1</code>	<code>call uaac member add bm-line-leader lisa</code>

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

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

## *Disable Discrete Applications*

When you install Standard Plant Applications Web Client, both Process and Discrete services and applications are installed by default. However, post-installation, you can disable the Discrete applications. Disabling the Discrete applications is a two step process:

1. Disable the services from the web server
2. Hide the applications from the Operations Hub server

### *Disable the services from the web server*

1. Extract the `enable-disable-discrete-utility-master.zip` file located at the `<Installation_Directory>\GE_Digital\PlantApplicationsWebClient` directory.
2. After the zip file is extracted, open the `enable-disable-discrete-utility-master` folder.
3. In the `enable-disable-discrete-utility-master` folder, run (run as administrator) `DisableDiscrete.bat`.  
A command prompt appears for you to enter the tomcat installation location.
4. At the `Enter Tomcat Installation path` prompt, enter the path where tomcat is installed in double-quotes. For example, "`<tomcat_home>/Apache Software Foundation/Tomcat 9.0`".  
You will be prompted to enter the Web Client installation path.
5. At the `Enter Web Client Installation path` prompt, enter the path where Web Client is installed in double-quotes. For example, "`C:\Program Files\GE Digital\PlantApplicationsWebClient\OperationsHub_PostingUtility`".  
All the Discrete applications will be disabled. A **DiscreteBackUp** folder is created under the `<Installation_Directory>\GE_Digital\PlantApplicationsWebClient` path and all the Discrete services files are moved to this folder. This in turn is used in future if you want to enable the Discrete applications.

### *Hide the apps from Operations Hub*

1. Access Ophub designer with Ophub tenant user credentials :  
`https://<ophub-host>/iqp`
2. Select **Plant Applications** under Apps.

3. Select NAVIGATION located the top-left corner of the screen.

You need to delete the following Discrete Apps:

- Unit Operations
- Work Order Manager
- Route Editor
- WorkQueue
- Time Booking

4. Select the app and then select the Delete icon.

5. Repeat the same for all discrete applications.

Now, when you access the Web Client, the Discrete applications are not visible in the left panel.

## *Enable Discrete Applications*

When you install Standard Plant Applications Web Client, both Process and Discrete services and applications are installed by default. If you have disabled the Discrete Applications and want to re-enable them, perform the following two step process:

1. Run the utility to enable the services in the web server
2. Add apps in the Operations Hub

### *Enable the services in the web server*

1. Extract the `enable-disable-discrete-utility-master.zip` file located at the `<Installation_Directory>\GE Digital\PlantApplicationsWebClient` directory.
2. After the zip file is extracted, open the `enable-disable-discrete-utility-master` folder.
3. In the `enable-disable-discrete-utility-master` folder, run (run as administrator) `EnableDiscrete.bat`.  
A command prompt appears for you to enter the tomcat installation location.
4. At the `Enter Tomcat Installation path` prompt, enter the path where tomcat is installed in double-quotes. For example, "`<tomcat_home>/Apache Software Foundation/Tomcat 9.0`".  
You will be prompted to enter the Web Client installation path.
5. At the `Enter Web Client Installation path` prompt, enter the path where Web Client is installed in double-quotes. For example, "`C:\Program Files\GE Digital\PlantApplicationsWebClient\OperationsHub_PostingUtility`".

All the Discrete applications will be enabled.

## *Re-enable apps from Operations Hub*

1. Access Ophub designer with Ophub tenant user credentials :  
`https://<ophub-host>/iqp`
2. Select **Plant Applications** under Apps.
3. Select NAVIGATION located the top-left corner of the screen.
4. Select **Add new page**.
5. Select the Discrete applications and select **Add**.  
Now, you can access the Discrete applications in Web Client.

## *Performance Tuning Settings*

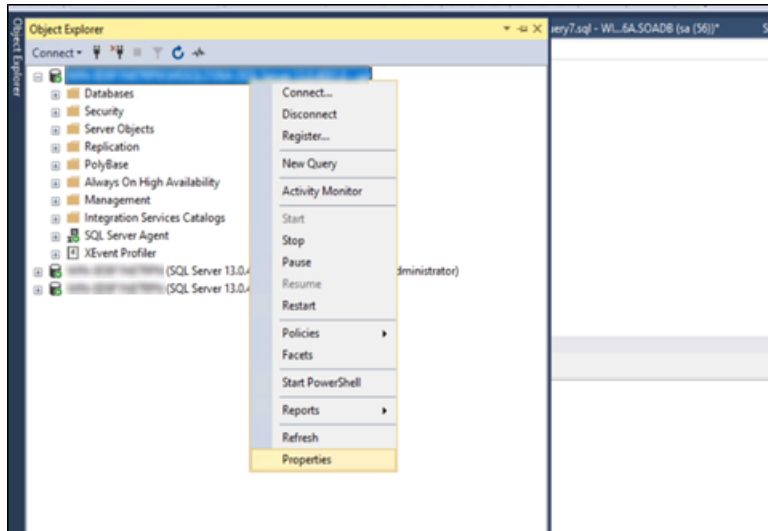
Here are the recommended performance tuning settings for your environment to achieve optimal performance.

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.

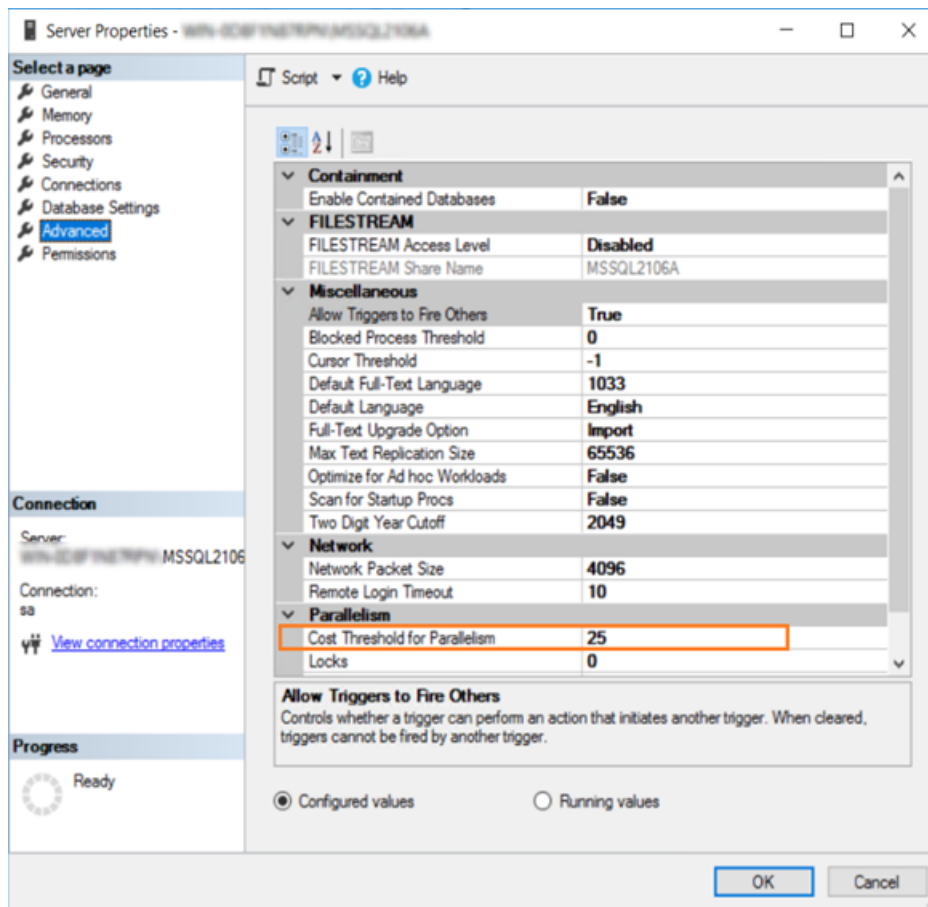


### 3. Update database settings:

- 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*

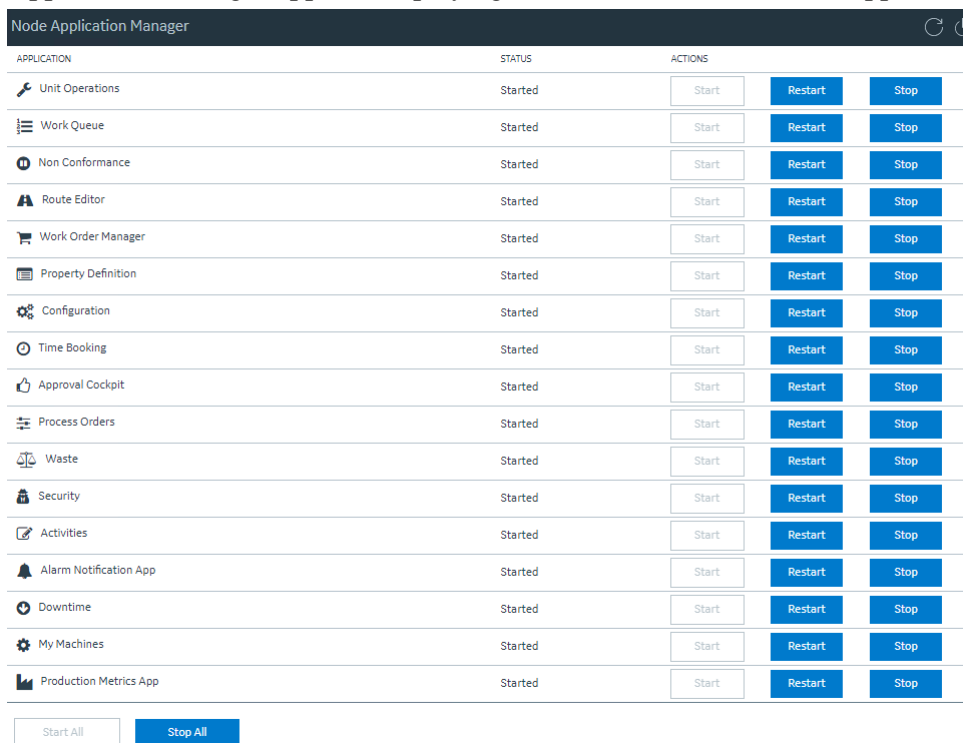
Node Application Manager is a simple utility that displays the health of the UI micro applications in a dashboard. You can use this utility to stop or restart the applications if you are not able to access them in the universal client from the browser.

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)
```

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.



APPLICATION	STATUS	ACTIONS
Unit Operations	Started	Start Restart Stop
Work Queue	Started	Start Restart Stop
Non Conformance	Started	Start Restart Stop
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.

## *Uninstall Standard Web Client*

This procedure is applicable if you want to uninstall the Plant Applications Standard Web Client and its components from your system.

1. From the Windows **Start** menu, select **Control Panel > Programs > Programs and Features**.
2. From the list of applications, uninstall Plant Application Web Client.
3. After uninstalling, you must restart your system if you choose to re-install or upgrade Plant Applications Web Client at later point of time.

## *Restart Services using Tomcat Manager*

If an application or a service encounter any errors, you can restart the services manually in the following order:

<b>Serial No</b>	<b>Service Name</b>
1	usersettingservice
2	mes
3	productservice
4	securityservice
5	accesscontrolservice
6	propertydefinitionservice
7	assignmentservice
8	laborservice
9	externalconfigservice
10	commentsservice
11	esignatureservice
12	alarm-service
13	reasonservice
14	activitieservice
15	processorderservice
16	timebookingservice
17	downtimeservice

<b>Serial No</b>	<b>Service Name</b>
18	wastemanagementservice
19	mymachinesservice
20	propertydefinitionappservice
21	segmentdefinition
22	route-service
23	mesdataservice
24	approvalcockpitservice
25	ncmservice
26	erpschedulerservice
27	documentmanagementservice
28	workorder
29	externalconfigappservice
30	processanalyzer-app-service
31	activitiesappservice
32	alarm-app-service
33	esignatureappservice
34	productionmetrics-service
35	approvalcockpitappservice
36	commentappservice
37	downtime-app-service
38	erptransformationservice
39	erpexportservice
40	erpimportservice
41	historyservice
42	plantexecutionservice
43	ncmappservice
44	pa-mymachinesservice
45	operatorappservice
46	productionmetrics-app-service
47	productionscheduleraappservice
48	rmsappservice

<b>Serial No</b>	<b>Service Name</b>
49	securityadministratorappservice
50	supervisorappservice
51	wastemanagementappservice
52	bommanagementappservice
53	receivinginspectionappservice
54	receivinginspectionsservice
55	spcappservice
56	webgenealogyappservice
57	approvalcockpitservice
58	wastemanagementservice


# Chapter 4. Upgrade Plant Applications Standard Web Client

## *Upgrade the Plant Applications Standard Web Client*

- 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.

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

 **Note:** The Plant Applications 8.2 installer is the base installer for all upgrade requirements.

1. Run the `installfrontend.exe` file as an Administrator.  
The installation menu appears, displaying the **Install Proficy Plant Applications 8.2** screen.



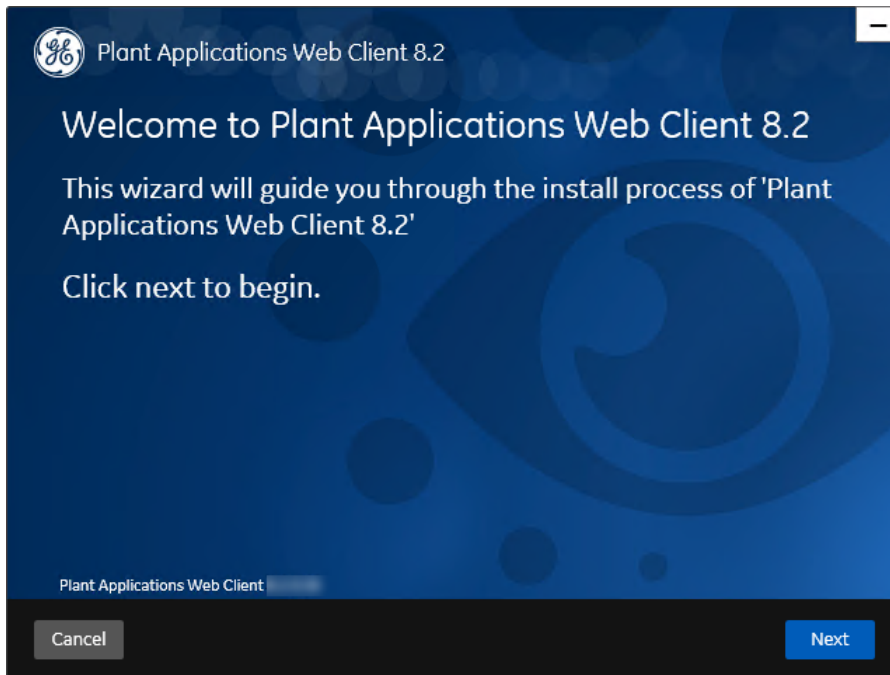
**i Tip:** You can hover over each task that appears in the installation menu to refer to the tooltip associated with that task.

## 2. Select **Plant Applications Web Client**.

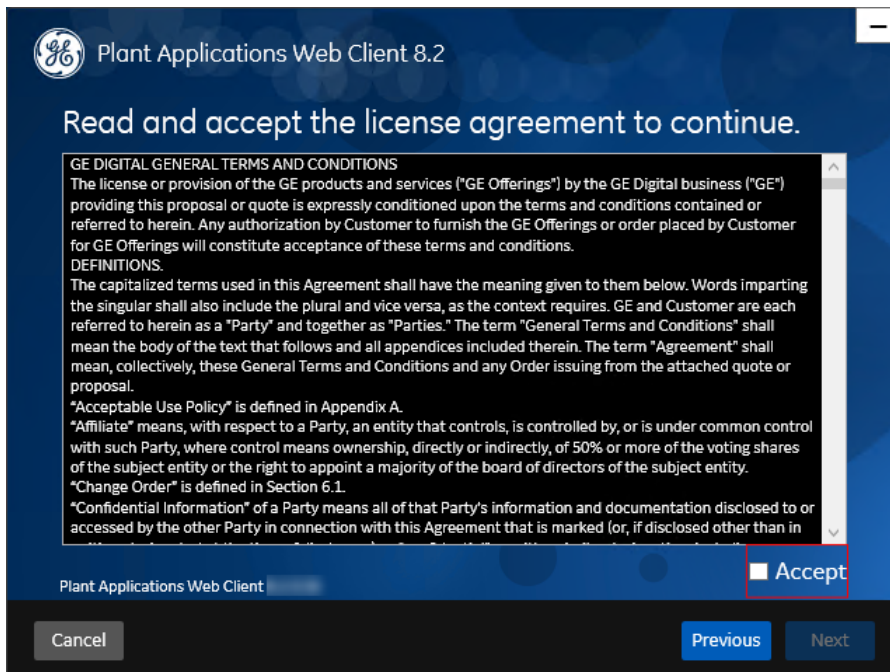
The installer gathers the current configuration and determines the required configurations that need to be updated.

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

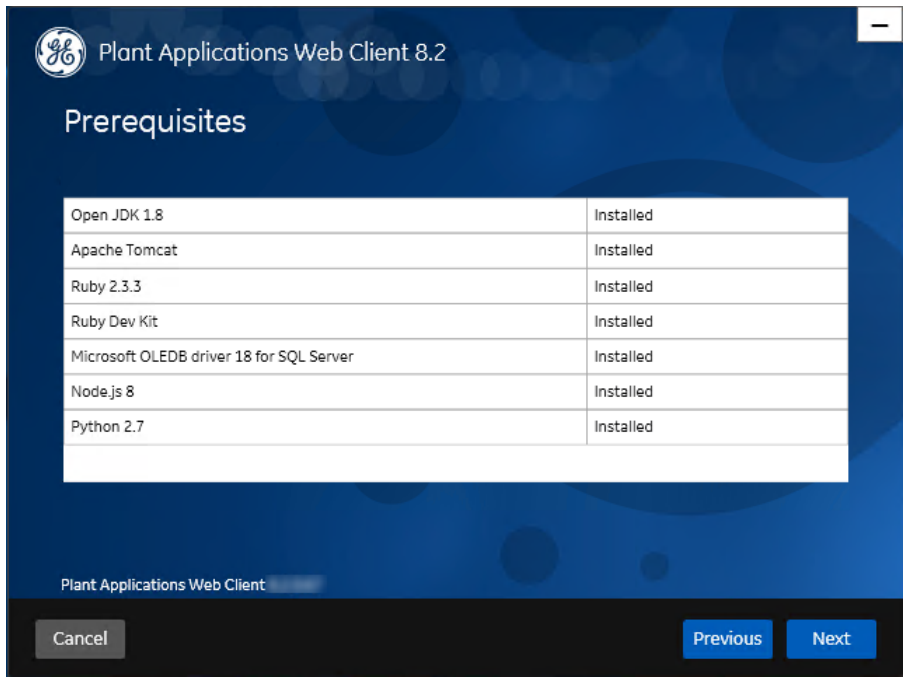




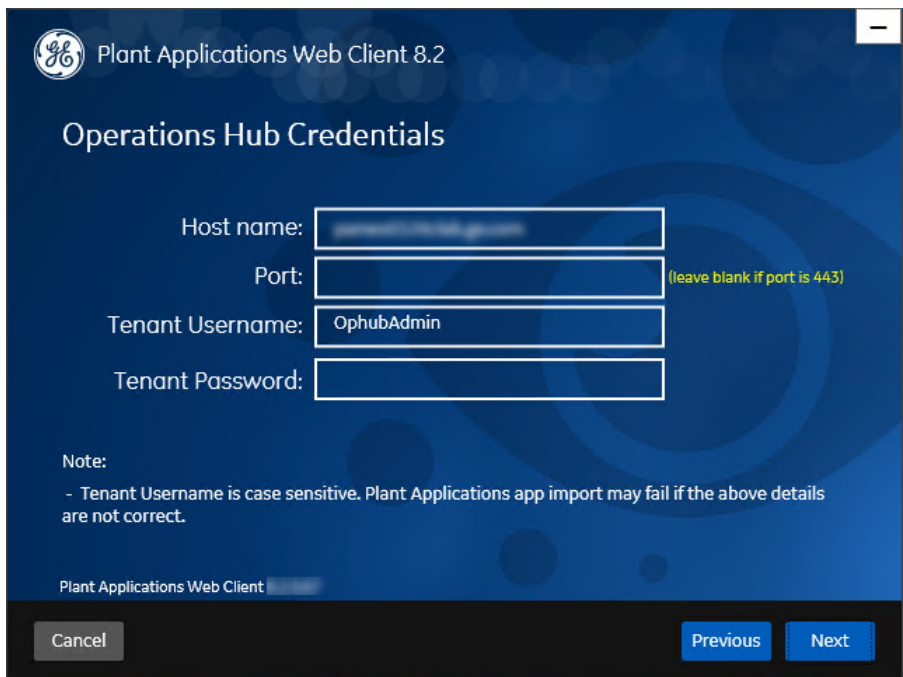
3. In the **Welcome to Plant Applications Web Client 8.2** screen, select **Next**. The **Read and accept the license agreement to continue** screen appears.






4. Read the license agreement, select **Accept**, and then select **Next** to continue the installation. The **Prerequisites** screen appears.



- In the **Prerequisites** screen, select **Next** to view all installed prerequisites and install any missing prerequisites.  
The **Operations Hub Credentials** screen appears.



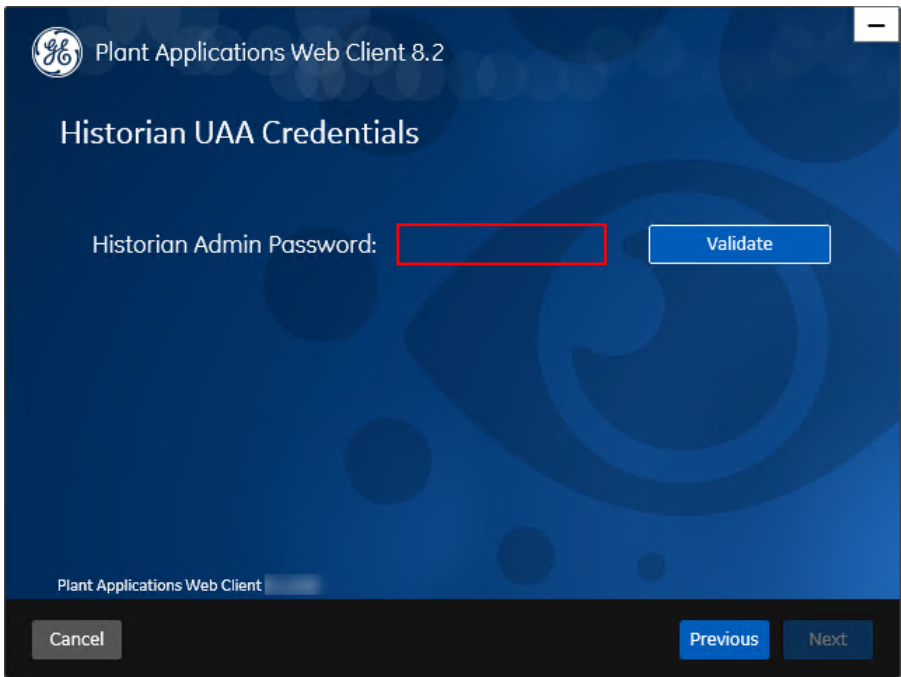
- In the **Operations Hub Credentials** screen, enter the credentials to access the Operations Hub server as described in the following table.

Credential	Description
Server Name	<p>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.</p> <p> <b>Note:</b> Instead of IP address, it is recommended to use the Operations Hub host name (computer name).</p>
Port	Enter the Operations Hub port number.
Tenant Username	<p>Enter the tenant Hub username to access the Operations Hub server instance.</p> <p> <b>Note:</b> The default user name is <code>OphubAdmin</code>.</p>
Tenant Password	<p>Enter the password for the user name you entered in the <b>Tenant Username</b> box.</p> <p> <b>Note:</b> The tenant username and password must be same as the credentials that you have specified during the Operations Hub installation.</p>

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




7. Select **Next**.

The **Historian UAA Credentials** screen appears.



8. In the **Historian UAA Credentials** screen, enter the password to access the Historian UAA server and then select **Validate**.

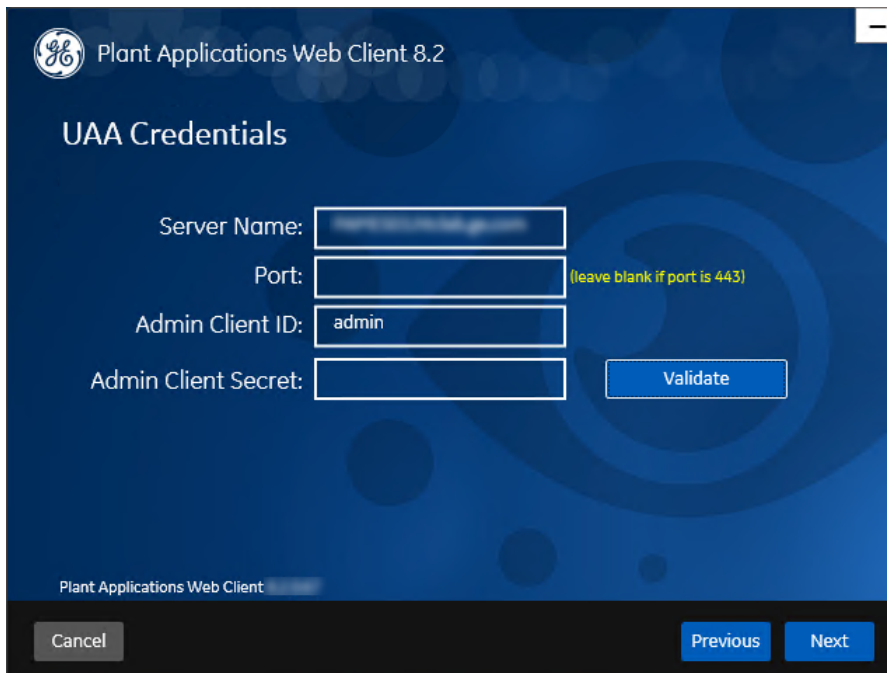
The following table describes each icon indicating a validation status that might appear during the validation process.

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.











9. Select **Next**.

The **UAA Credentials** screen appears.



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

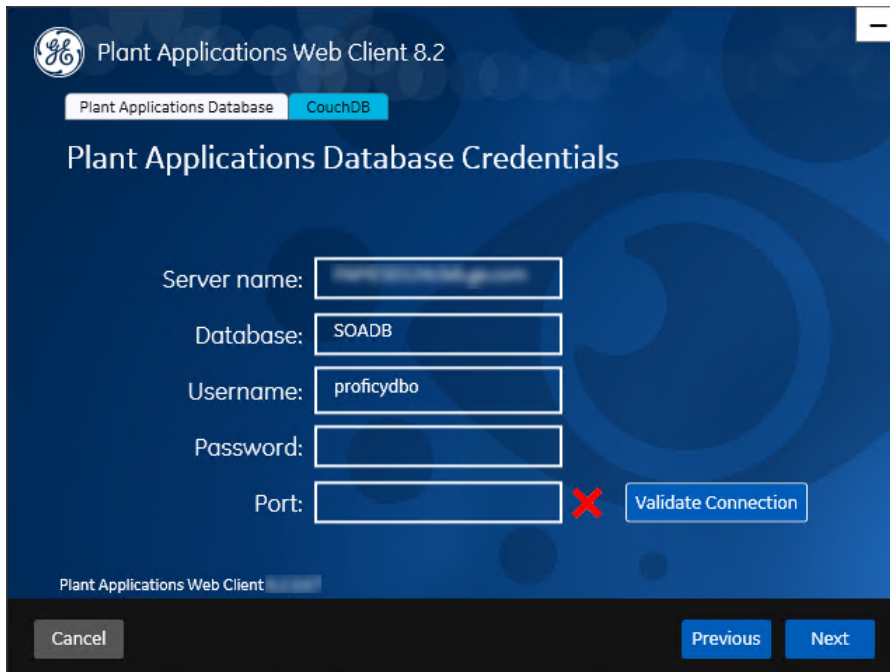
Credential	Description
Server Name	Enter the host name of the UAA server.   <b>Note:</b> Instead of IP address, it is recommended to use the UAA host name (computer name).
Port	Enter the UAA port number.
Admin Client ID	Enter the admin Client ID to access the UAA server instance.   <b>Note:</b> The default user name is <code>admin</code> .

Credential	Description								
Admin Client Secret	Enter the Client Secret for the user name you entered in the <b>Admin Client ID</b> box.								
Validate	Select <b>Validate</b> to validate the UAA server connection.								
<p> <b>Note:</b> The following table describes each icon indicating a validation status that might appear during the validation process.</p> <table border="1"> <thead> <tr> <th>Icon</th> <th>Description</th> </tr> </thead> <tbody> <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> </tbody> </table>		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.
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.

11. Select **Next**.


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






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

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

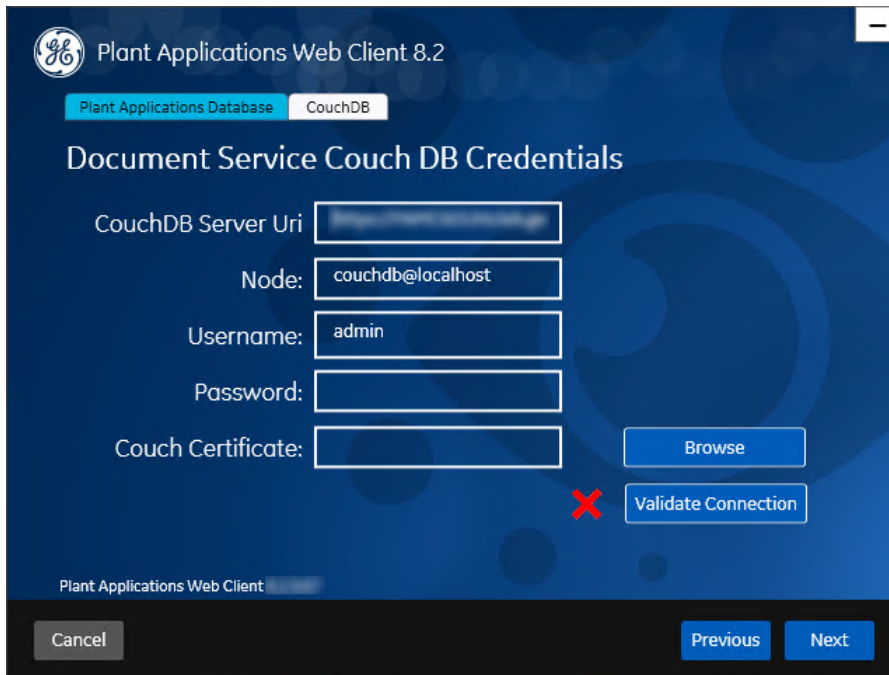
13. Select **Validate Connection** to validate the database connection.

 **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.

14. In the **Plant Applications Database Credentials** screen, select the **CouchDB** tab. The **Document Service Couch DB Credentials** section appears.



15. 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: <code>https://&lt;host name or IPaddress&gt;:&lt;port number&gt;</code> .								
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 <b>Database</b> box.								
Password	Enter the password for the user name you entered in the <b>Username</b> box.								
Couch Certificate	Select <b>Browse</b> to locate the Apache CouchDB server certificate (couch_server.crt) that you have generated and upload it.								
Validate	Select <b>Validate</b> to validate the Apache CouchDB database credentials.  <b>Note:</b> The following table describes each icon indicating a validation status that might appear during the validation process.								
<table border="1"> <thead> <tr> <th>Icon</th> <th>Description</th> </tr> </thead> <tbody> <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> </tbody> </table>		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.
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.

16. Select **Next**.











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

17. 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 to the Web Client applications.

Credential	Description
User Name	Enter the user name for an administrator account in Plant Applications.  <b>Note:</b> The default user name is <code>ophubAdmin</code> .
Password	Enter the password for the user name you entered in the <b>User Name</b> box.




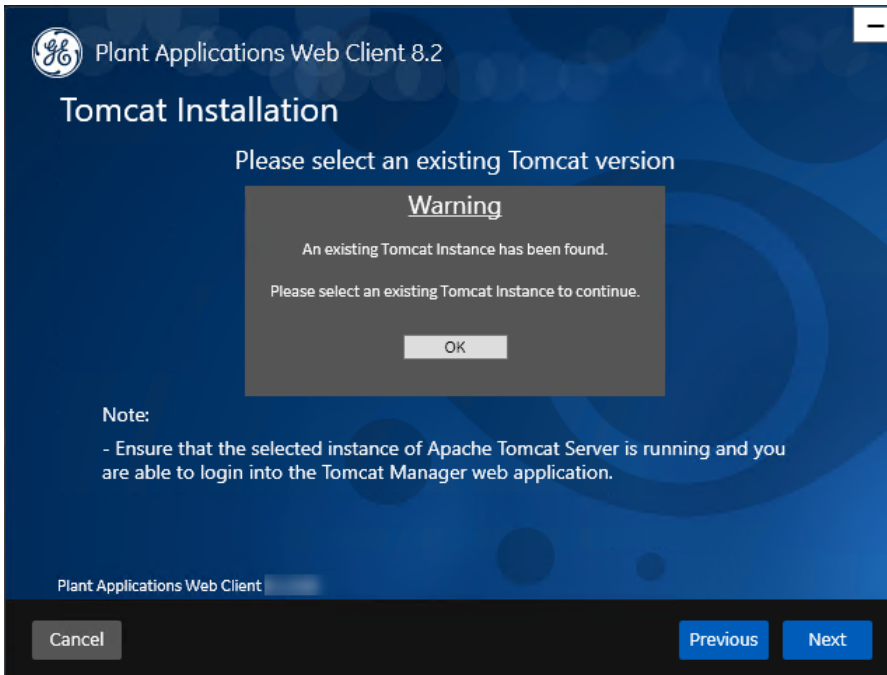
Credential	Description								
Validate	<p>Select <b>Validate</b> to validate the Plant Applications Administrator credentials.</p> <p> <b>Note:</b> The following table describes each icon indicating a validation status that might appear during the validation process.</p> <table border="1" data-bbox="440 401 1414 604"> <thead> <tr> <th data-bbox="440 401 911 432">Icon</th> <th data-bbox="911 401 1414 432">Description</th> </tr> </thead> <tbody> <tr> <td data-bbox="440 443 911 495"></td> <td data-bbox="911 443 1414 495">Indicates that the validation is in progress.</td> </tr> <tr> <td data-bbox="440 506 911 558"></td> <td data-bbox="911 506 1414 558">Indicates that the validation was successful.</td> </tr> <tr> <td data-bbox="440 569 911 621"></td> <td data-bbox="911 569 1414 621">Indicates that the validation was unsuccessful. In this case, make sure you enter the correct password.</td> </tr> </tbody> </table>	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.
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.

18. 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.



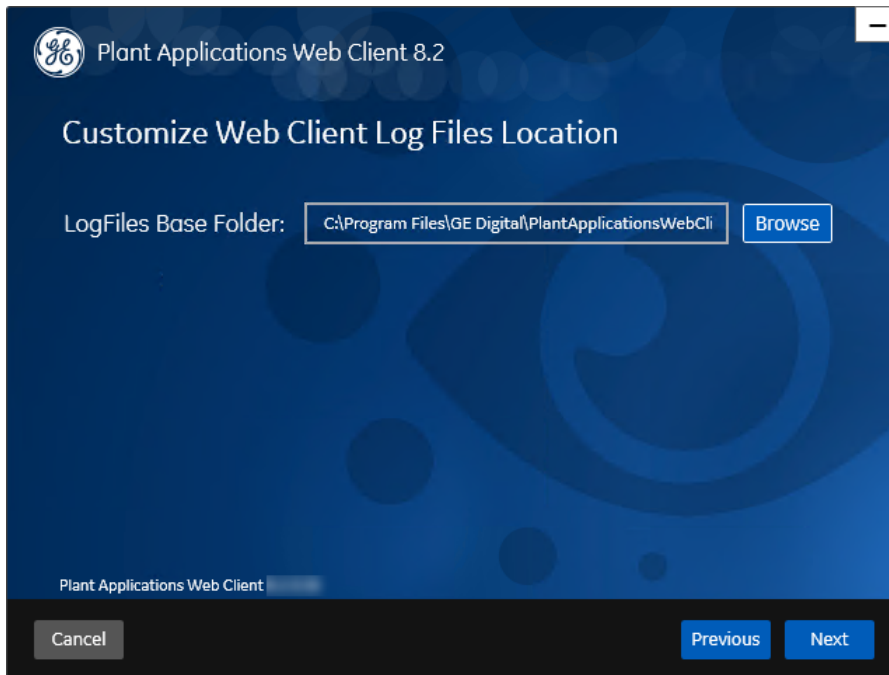
19. In the **Tomcat Installation** screen, select **OK**.

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.

20. In the **Tomcat Installation** screen, select an appropriate Tomcat instance from the drop-down list box.
21. 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.  <b>Note:</b> The default port is 8081.
Redirect Port	Enter the HTTPS port that Tomcat uses to redirect all HTTP requests to this port.  <b>Note:</b> The default redirect port is 8444.
Username	Enter the user name to access Tomcat.  <b>Note:</b> The default user name is <code>admin</code> .
Roles	Skip this box because it is automatically populated.
Password	Enter the password for the user name you entered in the <b>Username</b> box.
Re-enter Password	Reenter the password for the user name entered in the <b>Username</b> box.  <b>Note:</b> This box appears only when a new installation of Tomcat is initiated by the installer.

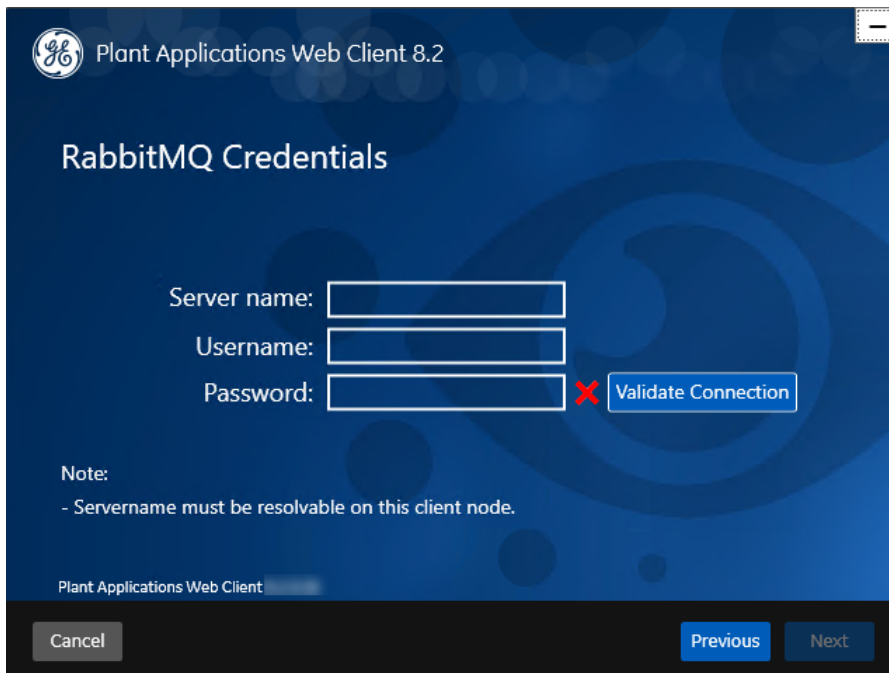
22. Select **Next**.  
The **Customize Web Client Log Files Location** screen appears.



23. **Optional:** In the **LogFiles Base Folder** box, select **Browse** to browse and select the directory where you want to install the Plant Applications Web Client service logs.

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**.

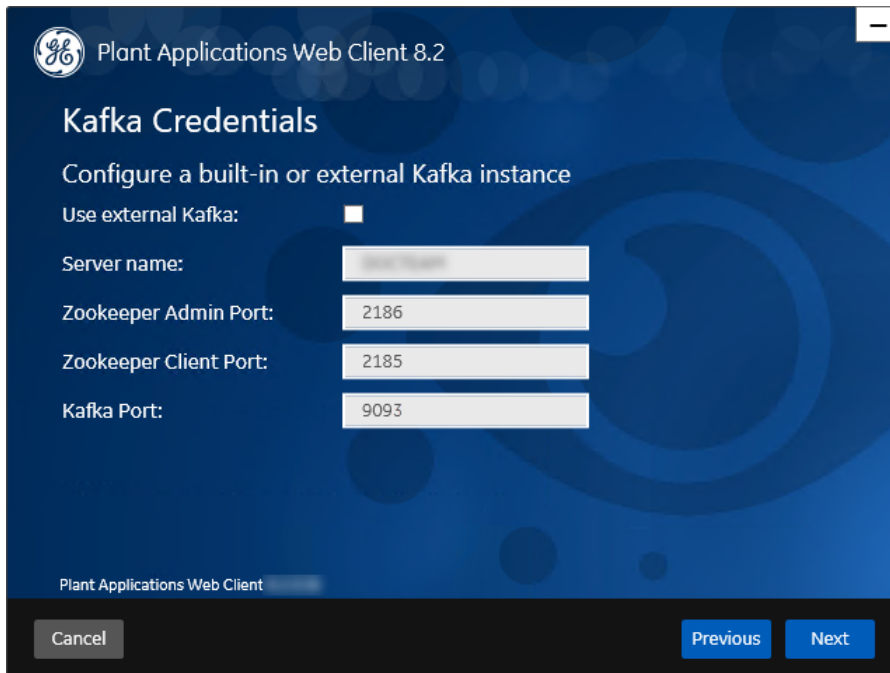
Credential	Description
<b>Server name</b>	Enter the computer name or IP address that hosts your Plant Applications Message Bridge.
<b>Username</b>	Enter the Administrator's user name that you set during Plant Applications Message Bridge installation.
<b>Password</b>	Enter the password for the Administrator's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



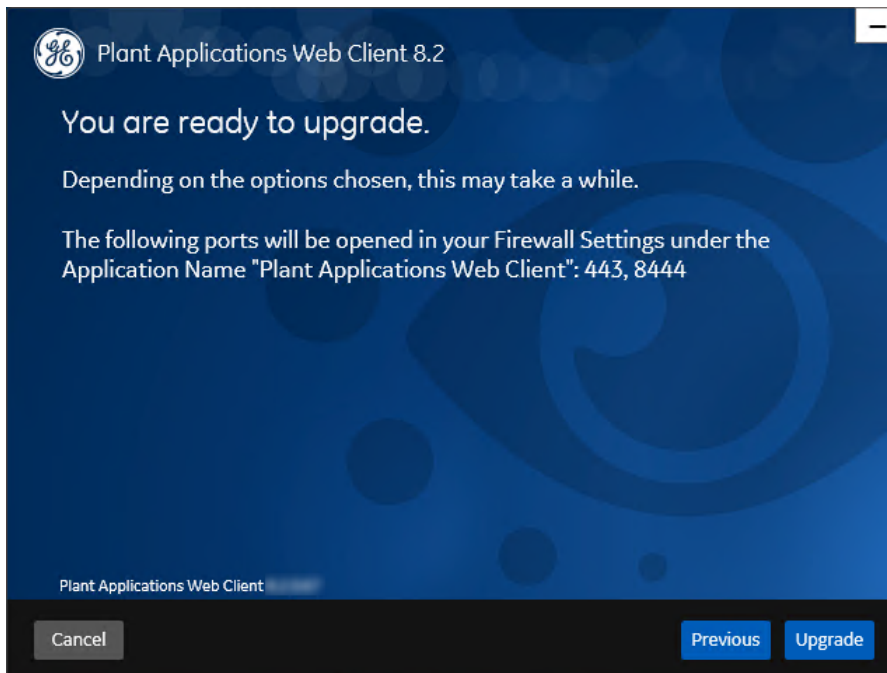
27. In the **Kafka Credentials** screen, enter the credentials to access the Kafka server as described in the following table.

Credential	Description								
Server Name	Enter the host name of the Kafka server.   <b>Note:</b> 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 <b>Validate</b> to validate the Kafka server connection.   <b>Note:</b> The following table describes each icon indicating a validation status that might appear during the validation process.								
<table border="1"> <thead> <tr> <th>Icon</th> <th>Description</th> </tr> </thead> <tbody> <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> </tbody> </table>		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.
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 Message Bridge Configuration Utility \(page 78\)](#) on the Plant Applications Server to update the Kafka details in the Message Bridge configuration.
33. [Run Operations Hub Posting Utility \(page 82\)](#) to import the Plant Applications into the Operations Hub.
34. Once you have completed running Message Bridge Configuration and Operations Hub Posting utilities, [Verify the Installation \(page 83\)](#) to verify if the Plant Applications Web Client applications are up and running.
35. [Access REST APIs \(page 83\)](#) to access the REST APIs for Plant Applications Web Client.

## *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 Enterprise Web Client

## *About Installing Enterprise Edition Web Client*

### **Before you begin**

Ensure that you have completed following tasks before you run the Plant Applications Enterprise Web Client installer:

- Installation of Plant Application Server
- Installation of Operations Hub Server
- [Configure CouchDB for HTTPS \(page 6\)](#)
- Your deployment environment must be connected to the Internet.

For more information, refer to the [Enterprise Edition Web Client Requirements \(page 57\)](#).

#### **Note:**

- Plant Applications Enterprise 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**

Plant Applications Enterprise Web Client installer is a Silent-mode installation that allows you to specify an installation configuration only once and perform the installation based on the defined configuration. The silent installer reads the settings you specified in an YAML (`silentinstaller.yml`) file before beginning the installation. This one-step installation program requires you to run a single command after defining your inputs in the `silentinstaller.yml` file.

The installer for Plant Applications Enterprise Web Client uses Docker technology. During the Plant Applications Enterprise Web Client installation process, the following tasks are performed:

- 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 Enterprise Edition Web Client server node



- Updating the Docker stack

You must enter the configuration details in the `silentinstaller.yml` file provided in the `plantapps-enterprise-webclient-<buildno>` folder. Based on the input, the corresponding Linux shell scripts are triggered to complete the tasks involved in the installation.

The installer can either install or upgrade (version 8.0 or above) Plant Applications Enterprise Web Client on a Linux environment.

The following table outlines the steps that you must complete to install Plant Applications Enterprise Web Client for the first time. These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed. All steps are required unless otherwise noted.

Step	Task	Notes
1	Install Operations Hub 2.0	This step is required.
2	<a href="#">Configure CouchDB for HTTPS (page 6)</a>	This step is required.
3	<a href="#">Ensure that your system meets the requirements for the Enterprise Edition Web Client installation. (page 57)</a>	This step is required.
4	<a href="#">Review the files provided by GE (page 59)</a>	This step is required.
5	<a href="#">Review the pre-installation checklist before installing Enterprise Edition Web Client. (page 60)</a>	This step is required.
6	<a href="#">Install Enterprise Edition Web Client (page 63)</a>	This step is required.
7	<a href="#">After the Enterprise Edition Web Client installation, ensure to run the Message Bridge Configuration utility. (page 78)</a>	This step is required.
8	<a href="#">After configuring Message Bridge, ensure to run the Operations Hub Posting utility. (page 82)</a>	This step is required.
9	<a href="#">Verify the Installation (page 83)</a>	This step is required.

## *Enterprise Edition Web Client Requirements*

### **Before you begin**


Ensure that you have completed following tasks :

- Installation of Plant Application Server
- Installation of Operations Hub 2.0.
- [Configure CouchDB for HTTPS \(page 6\)](#)

## System Requirements

Ensure that your computer meets the system requirements as described in the following table.

Item	Version
Operating system	Redhat 7.8 and 8.2 or Ubuntu 18.x  <b>Note:</b> Ubuntu is not supported in a production environment.
Docker	<ul style="list-style-type: none"> <li>• Docker Community Edition or Enterprise Edition 18.0 or 19.0</li> </ul>  <b>Note:</b> For installing Docker Engine, refer to <a href="https://docs.docker.com/engine/install/">https://docs.docker.com/engine/install/</a> . <ul style="list-style-type: none"> <li>• Docker Compose 1.25.x</li> </ul>  <b>Note:</b> For installing Docker Compose, refer to <a href="https://docs.docker.com/compose/install/">https://docs.docker.com/compose/install/</a> . <ul style="list-style-type: none"> <li>• Docker Swarm initiated as Swarm Manager</li> </ul>
Web browsers	Chrome 85.0 or later, with minimum resolution 1366x768. <b>Devices:</b> <ul style="list-style-type: none"> <li>• <b>iPad:</b> Safari v13.1+, Chrome 85.0 or later with resolution 2048x1536</li> <li>• <b>HP tablet:</b> Chrome 85.0 or later , with minimum resolution 1920x1280</li> </ul>  <b>Note:</b> Devices supports only Unit Operations, Work Queue, and Non Conformance applications.
Couch DB server	CouchDB version 2.3.1 installed and configured on a Windows machine.  <b>Note:</b> For more information on configuring CouchDB, refer to <a href="#">Configuring Apache CouchDB Settings (page 6)</a> .
Hard drive	100 GB (minimum)  <b>Note:</b> However, you may need more disk space based on your production data.

Item	Version
Processor	2.4 GHz clock-speed Intel Core i3, i5, or i7 CPU or equivalent AMD Phenom CPU  <b>Note:</b> For better performance, it is recommended to use an octa core (8-cores).
Memory	32 GB (recommended)

 **Note:**

- You can combine the Installer node, Plant Applications Web Client node, and the Local Docker Registry node into a single Linux server, especially if you want to upgrade to Plant Applications 8.2.
- If you are using controller and performing a remote upgrade of 8.0 SIM2, then you must uninstall the **docker-py** module on the Enterprise Edition Web Client node before starting the upgrade process.

## 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.
1433	The default port for the Microsoft SQL server.
9093	The default port for Kafka.
2185	The default port for ZooKeeper.
6984	The default port for CouchDB.
5059	The default port for Web Applications

## *Files Provided by GE*

The following files are provided by GE:


- `plantapps-enterprise-webclient-<buildno>`: Contains the installer and the supporting utilities.
- `plantapps-prereq.tar`: Contains the files required for installing Web Client prerequisites.

 **Note:** Ensure you copy `plantapps-prereq.tar` and `plantapps-enterprise-webclient-<buildno>` into a same folder before running the installation.

- `plantapps-webclient-docker-images.zip`: Contains the Enterprise Edition Web Client Docker Images that are used by the Web Client services. These files are Docker images of the new features.
- `DTR.zip`: Contains files required to setup local docker registry.
- `Readme.txt`: Contains a list of the defects fixed in this release and a list of new features.

## Pre-Installation Checklist

1. Ensure that you have Plant Application Server, Operations Hub Server, and CouchDB installed and running before installing Plant Applications Enterprise Web Client. For information, refer to the *Enterprise Deployment Architecture* section in the *Getting Started Guide*.
2. 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`.
3. If your installation environment runs behind a proxy, on all the three servers, set the `HTTP_PROXY` and `HTTPS_PROXY` environment variables to point to your proxy servers.

 **Note:** If you are using different nodes for docker registry and remore installation, you must set the `HTTP_PROXY` and `HTTPS_PROXY` in the respective nodes.

4. [Create and configure Docker Registry \(page 61\)](#).
5. 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>"
```

6. Access the node on which you want to install Plant Applications Enterprise Web Client.
7. Extract the contents of the `plantapps-webclient-docker-images.zip` file.
8. Extract the contents of the `plantapps-enterprise-webclient-<buildno>`.
9. Navigate to the installer folder, and run the following shell command: `~/your/path/plantapps-enterprise-webclient-<buildno> sudo chmod +x ./setup.sh`


## Create and Configure Docker Registry

If you are working on an offline system, you need to have required packages to be available. Perform the following steps to download the required packages on a machine that is connected to the internet and then manually copy the packages to the offline machine.

1. In the machine that is connected to the internet, download the docker images `registry:2.4.1` and `hyper/docker-registry-web` by using following commands.
  - a. `sudo docker pull registry:2.4.1`
  - b. `sudo docker pull hyper/docker-registry-web`
2. Create a tar file for above docker images using following commands:
  - a. `sudo docker save -o registry.tar registry:2.4.1`
  - b. `sudo docker save -o docker-registry-web.tar hyper/docker-registry-web`
3. Copy the above tar files to the offline system.
4. After copying the tar files, load the files using following commands:
  - a. `sudo docker load -i registry.tar`
  - b. `sudo docker load -i docker-registry-web.tar`

Use this section to create and configure docker registry.

1. From the Plant Applications Enterprise Web Client installation package, download the `DTR.zip` file into the machine on which you want to run Docker Registry.
2. Extract the `DTR.zip` file into a new `pa-dtr` folder by running following command: `sudo unzip <downloaded_path>/DTR.zip -d pa-dtr`. This folder stores the Docker Registry configuration files.


 **Note:** Ensure that you have enough space (minimum 20 GB) to store these extracted 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 Enterprise Web Client, enter `<host name or IP address of this local Docker Registry>:5000`.

 **Note:** Do not enter http or https.


## *Install Enterprise Edition Web Client*

Before starting the Plant Applications Enterprise Web Client installation, you must define your configuration in the **silentinstaller.yml** file. Once you are ready with the configuration you can start the installer. The **silentinstaller.yml** file can be found at: `~/your/path/plantapps-enterprise-webclient-<buildno>/silentinstaller.yml`

- During the installation, the installer displays the installation tasks on the console and in a log file at `~/your/path/wc82installer/plantapps-enterprise-webclient-<buildno>/log/ansible.log` and `~/your/path/wc82installer/plantapps-enterprise-webclient-<buildno>/log/sql_script.log`.




1. From the `~/your/path/wc82installer/plantapps-enterprise-webclient-<buildno>` directory, update the **silentinstaller.yml** file by using a text editor. For example, `$sudo nano silentinstaller.yml`

2. Using the text editor, update the following parameters in the **silentinstaller.yml** file by entering the values within the quotes ("")


 **Note:** Ensure that you:




- Do not use short names for these parameters.
- Use lower case when entering the server names.

Parameter	Description
WEBCIENT_SERVER: ""	Enter the Linux node FQDN or hostname where you are going to install Plant Applications Enterprise Web Client.  For example, <code>WEBCIENT_SERVER: "linuxnode.digital.com"</code>
WEBCIENT_SERVER_USERNAME: ""	Enter the Linux node administrator account username.  For example, <code>WEBCIENT_SERVER_USERNAME: "administrator"</code>
WEBCIENT_SERVER_PASSWORD: ""	Enter the Linux node administrator account password.

Parameter	Description
WEBCLIENT_INSTALLATION_PATH: ""	<p>Enter Web Client Installation path in which you want to install.</p> <p>For example, <code>WEBCLIENT_INSTALLATION_PATH: "/home/administrator/install/"</code></p> <p> <b>Note:</b> If you are performing an upgrade, provide the absolute path of the directory in which Enterprise Edition Web Client was installed, and press <b>Enter</b>. Unless modified, the path appears as follows: <code>&lt;buildpath&gt;/PlantApplicationsDocker</code></p> <p>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.</p>
DTR_URL: ""	<p>Enter the URL of your local Docker Registry that you created in <a href="#">Create and Configure Docker Registry (page 61)</a>.</p> <p>For example, <code>DTR_URL: "registry.gear.ge.com/dig-plantapps"</code></p> <p> <b>Note:</b> If you are performing an upgrade, provide the Docker Registry URL that was used during the previous installation in the following format: <code>&lt;IP address or hostname&gt;:&lt;port number&gt;</code>.</p>
DTR_USERNAME: ""	Enter the username that have access to the Docker Registry.
DTR_PASSWORD: ""	Enter the password to the Docker Registry.
TARFILES_FOLDER_LOCATION: ""	<p>Enter the absolute path of the directory where the <code>.tar</code> files provided by GE are located.</p> <p>For example, <code>TARFILES_FOLDER_LOCATION: "/path/to/images"</code></p>
WEBCLIENT_USERNAME: ""	<p>Enter the Plant Applications Web Client username to login into the application.</p> <p>For example, <code>WEBCLIENT_USERNAME: "admin"</code></p>
WEBCLIENT_USERPASSWORD: ""	Enter the Plant Applications Web Client password.
UAA_SERVICE_ORIGIN: ""	Enter the UAA Server hostname.
UAA_SERVICE_PORT: ""	Enter the UAA Server port number. By default, the port number is 443.
UAA_SERVICE_ADMIN_CLIENT_ID: ""	<p>Enter the admin Client ID to access the UAA server instance.</p> <p> <b>Note:</b> The default username is <b>admin</b>.</p>
UAA_SERVICE_ADMIN_CLIENT_SECRET: ""	Enter the Client Secret for the username you entered.
PLANT_APPS_DB_SERVER: ""	Enter the Plant Applications database server hostname that you want to connect with the Plant Applications Web Client.



Parameter	Description
PLANT_APPS_DB_INSTANCE: ""	<p>Enter the name of the instance of the SQL server. You can leave this parameter empty if not using an instance.</p> <p>For example, <code>PLANT_APPS_DB_INSTANCE: "sa"</code></p> <p> <b>Note:</b> Do not add a backslash (\) when entering the instance name.</p>
PLANT_APPS_DB_NAME: ""	<p>Enter the Plant Applications Database name.</p> <p>For example, <code>PLANT_APPS_DB_NAME: "SOADB"</code></p>
PLANT_APPS_DB_USERNAME: ""	<p>Enter the username that has permissions to access the database you entered.</p>
PLANT_APPS_DB_PASSWORD: ""	<p>Enter the password for the username you entered.</p>
PLANT_APPS_MB_SERVER: ""	<p>Enter the host name or IP address that hosts your Plant Applications Message Bridge.</p>
PLANT_APPS_MB_USERNAME: ""	<p>Enter the username that you set for Plant Applications Message Bridge.</p>
PLANT_APPS_MB_PASSWORD: ""	<p>Enter the password for the username you entered.</p>
COUCHDB_SERVER: ""	<p>Enter the Plant Applications CouchDB host name or IP adress.</p>
COUCHDB_DBNAME: "node@localhost"	<p>Do not change this parameter value.</p>
COUCHDB_USERNAME: ""	<p>Enter the CouchDB username.</p>
COUCHDB_PASSWORD: ""	<p>Enter the CouchDB password.</p>
OPHUB_SERVER: ""	<p>Enter the hostname of Operations HUB Server.</p>
OPHUB_SERVER_PORT: ""	<p>Enter the Operations Hub port number.</p> <p>For example, <code>OPHUB_SERVER_PORT: "443"</code></p>
OPHUB_TENANT_USERNAME: ""	<p>Enter the tenant Hub username to access the Operations Hub server instance.</p> <p>For example, <code>OPHUB_TENANT_USERNAME: "OphubAdmin"</code></p>
PASSWORDS_OR_CERTS_UPDATED : ""	<p>Default value is true. You can set this to false if you want to use OLD certificates during upgrade or apply 8.2 SIMs.</p> <p>For example, <code>PASSWORDS_OR_CERTS_UPDATED: "false"</code></p>
ENCRYPT_PASSWORDS: ""	<p>Set to true if you want to encrypt the password.</p> <p>For example, <code>ENCRYPT_PASSWORDS: "false"</code></p>

Parameter	Description
SSL_CERT_PEM_PATH: ""	<p> <b>Note:</b> Not required for Enterprise installation. Use this parameter only to replace the self-signed certificate with the trusted CA certificate.</p> <p>Enter the path to the SSL certificate.</p> <p>For example, <code>SSL_CERT_PEM_PATH: "/home/administrator/myca_certs/new_cert.pem"</code></p>
SSL_KEY_PEM_PATH: ""	<p> <b>Note:</b> Not required for Enterprise installation. Use this parameter only to replace the self-signed certificate with the trusted CA certificate.</p> <p>Enter the path where the valid CA key file is located.</p> <p>For example, <code>SSL_KEY_PEM_PATH: "/home/administrator/myca_certs/new_key.pem"</code></p>
UAA_PEM_PATH: ""	<p> <b>Note:</b> Not required for Enterprise installation. Use this parameter only to update the public keys of remote UAA services.</p> <p>Enter the path where the valid UAA public key is located.</p> <p>For example, <code>UAA_PEM_PATH: "/home/administrator/myca_certs/new_uaa_cert.pem"</code></p>

3. Save the **silentinstaller.yml** file.
4. Navigate to the installer folder and provide execute permission to the installer file by running following command.

```
$ sudo chmod +x ./ setup.sh
```

5. Depending on your deployment architecture, run one of the following commands to launch the installer:
  - If you want to run the Enterprise Edition Web Client Installer and install Enterprise Edition Web Client on a **same Linux machine**, navigate to your installer folder `~/your/path/plantapps-enterprise-webclient-<buildno>` and run the following command at the terminal:

```
$ sudo ./setup.sh
```

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

```
$ sudo ./setup.sh -r
```

The shell script `setup.sh` is launched, and Plant Application Web Client Installation console with a welcome message appears. If the installation is successful, the following message appears:


```
PLAY RECAP *****
localhost : ok=27  changed=1  unreachable=0  failed=0
Enter any key to go back to main menu
```

- 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>/plantapps-enterprise-webclient-<buildno>/log/ansible.log` of the installer directory.
  - Once the Web Client installation is complete, run the following two steps for configuring Message Bridge with Kafka details and import the Plant Applications into the Operations Hub.
6. [Run Message Bridge Configuration Utility \(page 78\)](#) on the Plant Applications Server to update the Kafka details in the Message Bridge configuration.
  7. [Run Operations Hub Posting Utility \(page 82\)](#) to import the Plant Applications into the Operations Hub.
  8. Once you have completed running Message Bridge Configuration and Operations Hub Posting utilities, [Verify the Installation \(page 83\)](#) to verify if the Plant Applications Web Client applications are up and running.
  9. [Access REST APIs \(page 83\)](#) to access the REST APIs for Plant Applications Web Client.

## *Replace the SSL Certificate of Enterprise Edition Web Client*

Install Plant Applications Enterprise Web Client.

When you install Plant Applications using Docker, a self-signed certificate for the Enterprise Edition Web Client applications is created so that you can access Enterprise Edition 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.

1. You must define your configuration in the **silentinstaller.yml** file. Update the following parameters in the **silentinstaller.yml** file:

Parameter	Description
SSL_CERT_PEM_PATH: ""	Enter the path to the SSL certificate.  For example, <code>SSL_CERT_PEM_PATH: "/home/administrator/myca_certs/new_cert.pem"</code>
SSL_KEY_PEM_PATH: ""	Enter the path to the SSL key.  For example, <code>SSL_KEY_PEM_PATH: "/home/administrator/myca_certs/new_key.pem"</code>


2. Access the `utility.sh` file in the `plantapps-enterprise-webclient-<buildno>` folder.
3. Provide execution permissions to the `utility.sh` file by running the following command:  
`sudo chmod +x <path to the installer>/plantapps-enterprise-webclient-<buildno>/utility.sh`
4. Remove the `PApaMymachinesservice` stack by running the following command: `sudo docker stack rm PApaMymachinesservice`.
5. Run the `utility.sh` file by running one of the following commands:
  - If you want to run this utility directly on the Enterprise Edition Web Client node: `<path to the installer>/plantapps-enterprise-webclient-<buildno>/sudo ./utility.sh -l -ssl reset`
  - If you want to run this utility remotely on the Enterprise Edition Web Client node: `<path to the installer>/plantapps-enterprise-webclient-<buildno>/sudo ./utility.sh -r -ssl reset`

The existing SSL certificate and key are replaced with the certificate and key that you have provided.

## *Replace the Public Keys of Remote Services*

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

 **Note:** If the certificate is signed by a Global/Public CA Certificate provider, the pem file should contain the Server Certificate. If the Certificate is signed by Enterprise CA (certificate authority), then it should contain all certificate levels: the Root CA, the Intermediate Enterprise Certificate, and the Server Certificate. After you obtain the correct certificate, use the following steps.

1. You must define your configuration in the **silentinstaller.yml** file. Update the following parameter in the **silentinstaller.yml** file:

Parameter	Description
UAA_PEM_PATH: ""	Enter the path where the valid CA key file is located.  For example, UAA_PEM_PATH: "/home/administrator/myca_certs/uaa_ca.pem"

2. Access the `utility.sh` file in the `plantapps-enterprise-webclient-<buildno>` folder.
3. Provide execution permissions to `utility.sh` file by running the following command: `sudo chmod +x your/pathto/installer/plantapps-enterprise-webclient-<buildno>/utility.sh`
4. Remove the `PAPaMymachinesservice` stack by running the following command: `sudo docker stack rm PAPaMymachinesservice`.
5. Run the `utility.sh` file by running one of the following commands:
  - If you are running this utility directly on the Enterprise Edition Web Client node: `<installer path>/plantapps-enterprise-webclient-<buildno>/sudo ./utility.sh -l -pkey reset`
  - If you are running this utility remotely on the Enterprise Edition Web Client node: `<installer path>/plantapps-enterprise-webclient-<buildno>/sudo ./utility.sh -r -pkey reset`


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 Enterprise Edition Web Client Docker Containers*

The passwords or secrets used during the installation of Enterprise Edition 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 Enterprise Edition 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.

1. You must define your configuration in the **silentinstaller.yml** file. Update the following parameter in the **silentinstaller.yml** file:

 **Note:** You must provide all the following parameter values even if there is no change in the existing passwords.

Parameter	Description
SSL_KEY_PEM_PATH: ""	Enter the path where the valid CA key file is located.  For example, <code>SSL_KEY_PEM_PATH: "/home/administrator/myca_certs/new_key.pem"</code>
PLANT_APPS_DB_SERVER: ""	Enter the Plant Applications database server hostname that you want to connect with the Plant Applications Web Client.
PLANT_APPS_DB_INSTANCE: ""	Enter the name of the instance of the SQL server. You can leave this parameter empty if not using an instance.  For example, <code>PLANT_APPS_DB_INSTANCE: "sa"</code>   <b>Note:</b> Do not add a backslash (\) when entering the instance name.
PLANT_APPS_DB_NAME: ""	Enter the Plant Applications Database name.  For example, <code>PLANT_APPS_DB_NAME: "SOADB"</code>
PLANT_APPS_DB_USERNAME: ""	Enter the username that has permissions to access the database you entered.
PLANT_APPS_DB_PASSWORD: ""	Enter the password for the username you entered.
COUCHDB_SERVER: ""	Enter the Plant Applications CouchDB host name or IP adress.
COUCHDB_DBNAME: "node@localhost"	Do not change this parameter value.
COUCHDB_USERNAME: ""	Enter the CouchDB username.
COUCHDB_PASSWORD: ""	Enter the CouchDB password.
PLANT_APPS_MB_SERVER: ""	Enter the host name or IP address that hosts your Plant Applications Message Bridge.
PLANT_APPS_MB_USERNAME: ""	Enter the username that you set for Plant Applications Message Bridge.
PLANT_APPS_MB_PASSWORD: ""	Enter the password for the username you entered.
UAA_SERVICE_ORIGIN: ""	Enter the UAA Server hostname.
UAA_SERVICE_ADMIN_CLIENT_ID: ""	Enter the admin Client ID to access the UAA server instance.
UAA_SERVICE_ADMIN_CLIENT_SECRET: ""	Enter the Client Secret for the username you entered.

2. Access the `utility.sh` file in the `plantapps-enterprise-webclient-<buildno>` folder.

3. Provide execution permissions to `utility.sh` file by running the following command: `sudo chmod +x your/pathto/installer/plantapps-enterprise-webclient-<buildno>/utility.sh`

4. Run the `utility.sh` file by running one of the following commands:

- If you are running this utility directly on the Enterprise Edition Web Client node:  
`<installer path>/plantapps-enterprise-webclient-<buildno>/sudo ./utility.sh -l -pkey -reset`
- If you are running this utility remotely on the Enterprise Edition Web Client node:  
`<installer path>/plantapps-enterprise-webclient-<buildno>/sudo ./utility.sh -r -pkey -reset`

Docker secrets are created based on the values you entered, and the Docker stacks are redeployed so that the containers use the new passwords.

## *Enterprise Edition Web Client Deployment for Scalability*

The Docker Enterprise Edition Web Client's installer has default configuration selections that are optimized for Linux machines of 32 GB RAM. In a production environment, it is recommended to choose the target Linux server with 64-GB RAM. Also, before starting the installer you must perform following task.

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_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
JAVA_OPTIONS_350=-XX:MaxRAM=350m -XX:MaxHeapSize=180m -XX:
+UnlockExperimentalVMOptions -XX:CompressedClassSpaceSize=120m
DEPLOY_RESOURCES_LIMITS_MEMORY_500=750M
DEPLOY_RESOURCES_LIMITS_MEMORY_1000=1250M
```

...with the following lines of code:

```
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
JAVA_OPTIONS_350=-XX:MaxRAM=350m -XX:MaxHeapSize=180m -XX:
+UnlockExperimentalVMOptions -XX:CompressedClassSpaceSize=120m
DEPLOY_RESOURCES_LIMITS_MEMORY_500=750M
DEPLOY_RESOURCES_LIMITS_MEMORY_1000=1250M
JAVA_OPTIONS_1600=-XX:MaxRAM=1400m -XX:MaxHeapSize=1256m -XX:
+UnlockExperimentalVMOptions -XX:CompressedClassSpaceSize=120m
```

```
DEPLOY_RESOURCES_LIMITS_MEMORY_1600=1600M
```

3. Save and close the file.
4. Access each of the following files located in the following folder: \uc-ansible-installer\roles\installer\templates\
  - activitiesappservice-yml.j2
  - downtime-app-service-yml.j2
  - pa-mymachinesservice-yml.j2
  - alarm-app-service-yml.j2
  - wastemanagementappservice-yml.j2
  - productionschedulerappservice-yml.j2
  - operatorappservice-yml.j2
  - erptransformationservice-yml.j2
  - erpimportservice-yml.j2
  - erpschedulerservice-yml.j2
  - mesdataservice-yml.j2
5. In each file, perform the following:
  - a. Search for `$JAVA_OPTIONS_350` and replace it with `$JAVA_OPTIONS_1600`
  - b. Search for `$DEPLOY_RESOURCES_LIMITS_MEMORY_500` and replace it with `$DEPLOY_RESOURCES_LIMITS_MEMORY_1600`
6. After replacing the above values in each file, save and close the file. Repeat until you finish updating all the files mentioned in Step-4.
7. Follow [Install Enterprise Edition Web Client \(page 63\)](#) version of Enterprise Edition Web Client.  
You can now use Enterprise Edition Web Client on a machine with a 64GB RAM.

## *Post-Installation Repair or Upgrade for Scalability*

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 scalability requirements, you can make the following changes to repair the installation to meet your scalability requirements to utilize RAM size of 64 GB.

1. Navigate to the `plantapps-web-docker` folder located in the Enterprise Edition 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_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
JAVA_OPTIONS_350=-XX:MaxRAM=350m -XX:MaxHeapSize=180m -XX:
+UnlockExperimentalVMOptions -XX:CompressedClassSpaceSize=120m
DEPLOY_RESOURCES_LIMITS_MEMORY_500=750M
DEPLOY_RESOURCES_LIMITS_MEMORY_1000=1250M


```

...with the following lines of code:

```

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
JAVA_OPTIONS_350=-XX:MaxRAM=350m -XX:MaxHeapSize=180m -XX:
+UnlockExperimentalVMOptions -XX:CompressedClassSpaceSize=120m
DEPLOY_RESOURCES_LIMITS_MEMORY_500=750M
DEPLOY_RESOURCES_LIMITS_MEMORY_1000=1250M
JAVA_OPTIONS_1600=-XX:MaxRAM=1400m -XX:MaxHeapSize=1256m -XX:
+UnlockExperimentalVMOptions -XX:CompressedClassSpaceSize=120m
DEPLOY_RESOURCES_LIMITS_MEMORY_1600=1600M

```

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

3. Save and close the file.
4. Access each of the following files located in the following folder: /  
 <installation\_path>/PlantApplicationsDocker/plantapps-web-docker
  - activitiesappservice-yml.j2
  - downtime-app-service-yml.j2
  - pa-mymachinesservice-yml.j2
  - alarm-app-service-yml.j2
  - wastemanagementappservice-yml.j2
  - productionschedulerappservice-yml.j2
  - operatorappservice-yml.j2
  - erptransformationservice-yml.j2
  - erpimportservice-yml.j2
  - erpschedulerservice-yml.j2
  - mesdataservice-yml.j2
5. In each file, perform the following:
  - a. Search for `$JAVA_OPTIONS_350` and replace it with `$JAVA_OPTIONS_1600`
  - b. Search for `$DEPLOY_RESOURCES_LIMITS_MEMORY_500` and replace it with `$DEPLOY_RESOURCES_LIMITS_MEMORY_1600`
6. After replacing the above values in each file, save and close the file. Repeat until you finish updating all the files mentioned in Step-4.
7. From the same folder location, run the following commands:
  - a. `$sudo chmod +x PA_Services_Deploy_Lix.sh`

b. `$sudo .\PA_Services_Deploy_Lix.sh`

 **Note:**

- If your application is not running, you might encounter errors that you can ignore.
- The above command will deploy the Enterprise Edition Web Client's services stack which will take a few minutes.

The Enterprise Edition Web Client instance will be now running with the optimally utilized system memory and will support your scalability requirements.

## *Disable Discrete Applications*

When you install Plant Applications using Docker, both Process and Discrete services and applications are installed by default. Disabling the Discrete applications is a two-step process:

1. Disable the services from the web server
2. Hide the applications from the Operations Hub server

### *Disable the services from the web server*

1. Access the `utility.sh` in the **uc-ansible-installer** folder.
2. Provide execution permissions to the `utility.sh` file by running the following command:
 

```
sudo chmod +x /uc-ansible-installer/utility.sh
```
3. Run the `utility.sh` by running one of the following commands:
  - If you want to run this utility directly on the Web Client node: `/uc-ansible-installer/sudo ./utility.sh -l -disablediscrete reset`
  - If you want to run this utility remotely on the Web Client node: `/uc-ansible-installer/sudo ./utility.sh -r -disablediscrete reset`
4. If you run this utility remotely, enter the details of the Web Client node.
5. A message appears, asking you to enter Web Client Installation Directory. Enter installation directory and then press **Enter**.

### *Hide the apps from Operations Hub*

1. Access Ophub designer with Ophub tenant user credentials :
 

```
https://<ophub-host>/iqp
```
2. Select **Plant Applications** under Apps.
3. Select NAVIGATION located at the top-left corner of the screen.

You need to delete the following Discrete Apps:

- Unit Operations
- Work Order Manager
- Route Editor
- WorkQueue
- Time Booking

4. Select the app and then select the Delete icon.

5. Repeat the same for all discrete applications.

Now, when you access the Web Client, the Discrete applications are not visible in the left panel.

## *Enable Discrete Applications*

When you install Plant Applications using Docker, both Process and Discrete services and applications are installed by default. If you have disabled the Discrete applications and want to re-enable them, perform the following two step process:

1. Run the utility to enable the services in the web server
2. Add apps in the Operations Hub

### *Enable the services in the web server*

1. Access the `utility.sh` in the **uc-ansible-installer** folder.
2. Provide execution permissions to the `utility.sh` file by running the following command:
 

```
sudo chmod +x /uc-ansible-installer/utility.sh
```
3. Run the `utility.sh` by running one of the following commands:
  - If you want to run this utility directly on the Web Client node: `/uc-ansible-installer/sudo ./utility.sh -l -enablediscrete reset`
  - If you want to run this utility remotely on the Web Client node: `/uc-ansible-installer/sudo ./utility.sh -r -enablediscrete reset`
4. If you run this utility remotely, enter the details of the Web Client node.
5. A message appears, asking you to enter Web Client Installation Directory  
Enter installation directory and then press **Enter**.

### *Re-enable apps from Operations Hub*


1. Access Ophub designer with Ophub tenant user credentials :

```
https://<ophub-host>/iqp
```

2. Select **Plant Applications** under Apps.
3. Select NAVIGATION located the top-left corner of the screen.
4. Select **Add new page**.
5. Select the Discrete applications and select **Add**.  
Now, you can access the Discrete applications in Web Client.

## *Reconfigure Enterprise Web Client after upgrading Operations Hub*

You can use the following steps to reconfigure the Enterprise Edition Web Client after upgrading Operations Hub.

 **Note:** These steps work only when Operations Hub URL and credentials are not changed. If credentials or URL are updated, Web Client must be reinstalled.

1. On the Enterprise Edition Web Client machine run below commands to restart the `uaa_uaac` service:
  - a. `$sudo docker service scale uaa_uaac=0`
  - b. `$sudo docker service scale uaa_uaac=1`
2. Copy uaa cert pem to the linux machine.
3. On Web Client machine navigate to installer folder using `$cd path/to/installer`
4. Edit the **silentinstaller.yml** file to update the `UAA_PEM_PATH` key value with uaa pem path.
5. Provide execution permissions to `utility.sh` file by running the following command: `$sudo chmod +x utility.sh`
6. Run the `utility.sh` file to update web client with latest uaa pem: `$sudo ./utility.sh -l -pkey reset.`

## *Troubleshooting Enterprise Edition Web Client Installation Issues*

Issue	Resolution
<p>Unable to access Plant Applications Enterprise Web Client.</p> <p>When you install Enterprise Edition 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 Enterprise Web Client installation with a CA certificate that is added to your trust stores across the local network, you cannot access Enterprise Edition Web Client.</p>	<ol style="list-style-type: none"> <li>1. Access the following URLs: <ul style="list-style-type: none"> <li>• https://&lt;Enterprise Edition Web Client node IP address or system name&gt;:5059/</li> <li>• https://&lt;Enterprise Edition Web Client node IP address or system name&gt;:5051/</li> </ul> <p>A message appears to accept the insecure URL to proceed. Choose to do so.</p> </li> <li>2. Select <b>Not Secure</b> in the address bar. A <b>Certificate</b> window appears.</li> <li>3. Import the certificate and add it to your trusted store.</li> <li>4. Refresh the Plant Applications Enterprise Web Client window.</li> </ol>
<p>When you run the installer (<code>setup.sh</code>) and select an option, the following error message appears: Unexpected Exception, this is probably a bug: No closing quotation</p>	<p>Access the <code>ansible.cfg</code> file, and comment out the following lines of code:</p> <pre>strategy_plugins = ./tmp/mitogen-0.2.9/ ansible_mitogen/plugins/strategy strategy = mitogen_linear</pre>
<p>Multiple container restart issue.</p>	<p>If you have multiple container restart issue, run the following command in the web client (linux server ) node:</p> <pre>docker swarm update --dispatcher-heartbeat 120s</pre>

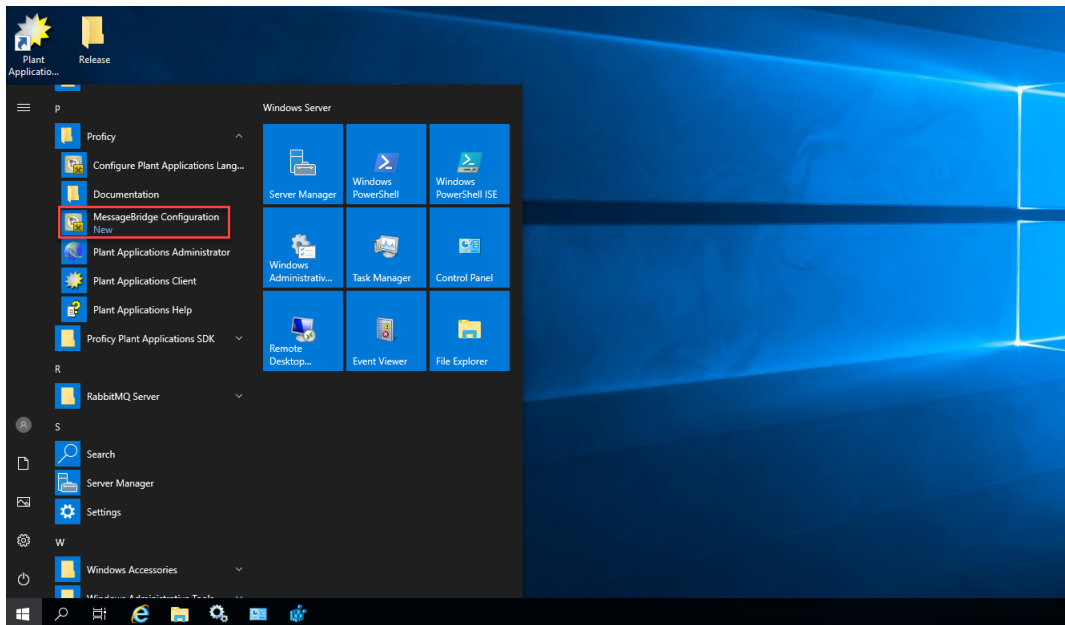
# Chapter 6. Post Installation Configuration (Enterprise and Standard)

## *Run Message Bridge Configuration Utility*

You must have installed the Plant Applications Web Client before you run the **MessageBridge Configuration** utility.


You must run the utility to update the Kafka details in the Message Bridge configuration.



1. On the Plant Applications Server node, from the Windows **Start** menu, expand **Proficy**.



2. From the list, select **Message Bridge Configuration**.  
The **Message Bridge Configuration** window appears to enter the Plant Applications Database Server details.

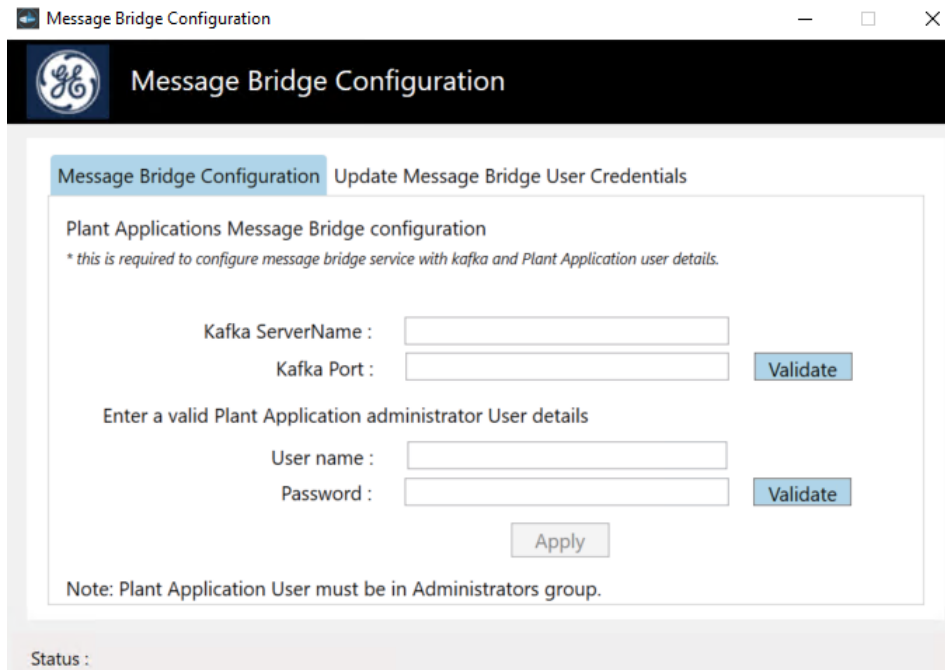
3. In the **Message Bridge Configuration** tab, enter the Plant Applications Database credentials as described in the following table.

 **Note:** The **Message Bridge Configuration** utility prompts to enter the Plant Applications Database connection details only for the first time you access the utility. Once the connection is established, the utility automatically fetches the database details for the next time you access the utility.



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

4. Select **Validate** to validate the database connection.  
If the database connection is successfully validated, the **Next** button is enabled.

5. Select **Next**.  
You will be prompted to enter the Plant Applications Message Bridge configuration details.



6. In the **Message Bridge Configuration** tab, enter the credentials to access the Kafka server as described in the following table.

Credential	Description
Kafka ServerName	Enter the host name of the Kafka server.  <b>Note:</b> Instead of IP address, it is recommended to use the Kafka host name (computer name).
Kafka Port	Enter the Kafka port number.  <b>Note:</b> The default port number is 9093. <ul style="list-style-type: none"> <li>• <b>Enterprise Installation:</b> The default port number is always 9093.</li> <li>• <b>Standard Installation:</b> The port number is available in the <code>server.properties</code> file located at <code>&lt;Installation_directory&gt;\Kafka\config</code>. For example, <code>C:\Kafka\config\server.properties</code>.</li> </ul>

7. Select **Validate** to validate the Kafka Server connection.  
If the connection is successfully validated, enter the Plant Applications Administrator User details as described in the following table.



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 <b>User Name</b> box.
Validate	Select <b>Validate</b> to validate the Plant Applications Administrator credentials.

- Once the Plant Applications Administrator User credentials are validated, select **Apply**. The entered Message Bridge configuration details are applied and the message bridge service is restarted.

## Update Message Bridge User Credentials

Use this tab only to update the Message Bridge credentials if you have modified the Plant Applications user credentials.

In the **Update Message Bridge User Credentials** tab, enter the Plant Applications Administrator user credentials for the Message Bridge service configuration as described below.


The screenshot shows a web browser window titled "Message Bridge Configuration". The main content area has a dark header with the GE logo and the text "Message Bridge Configuration". Below this, there are two tabs: "Message Bridge Configuration" and "Update Message Bridge User Credentials", with the latter being active. The main content area contains the following text: "Enter Plant Application Administrator user credentials for the Message Bridge service configuration" followed by a note: "\* use this to update message bridge credentials when a configured Plant Application user credentials are modified." Below this text are two input fields: "User name :" and "Password :". At the bottom of the input area are two buttons: "Exit" and "Update". At the very bottom of the page, there is a "Status :" label.

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 <b>User Name</b> box.
Update	Select to update the Plant Applications Administrator credentials for Message Bridge service .

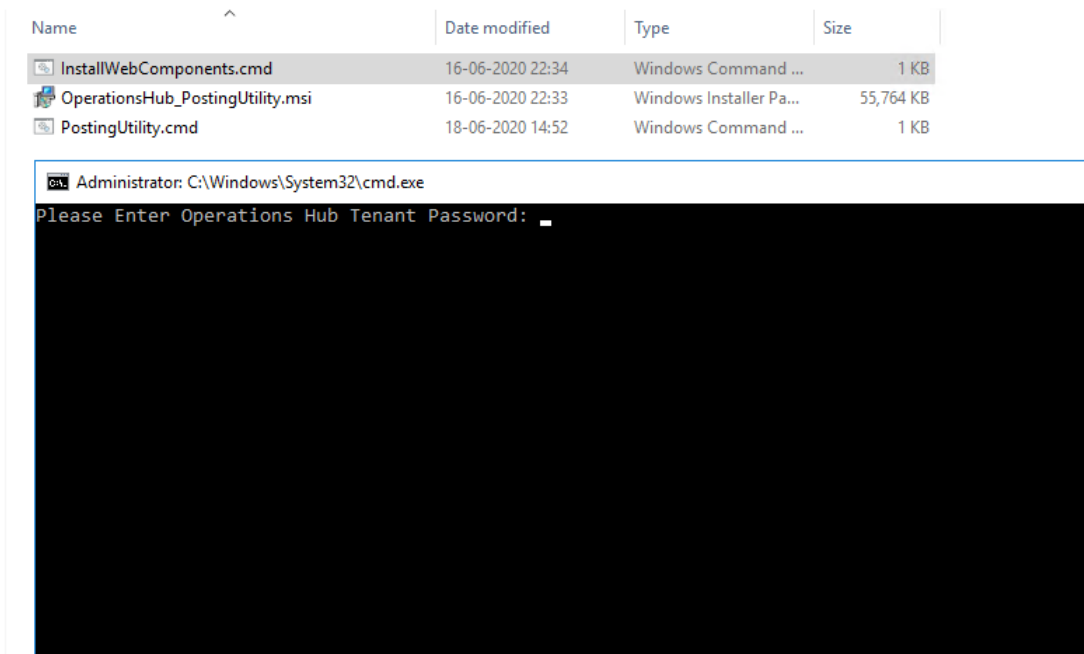
## Run Operations Hub Posting Utility

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

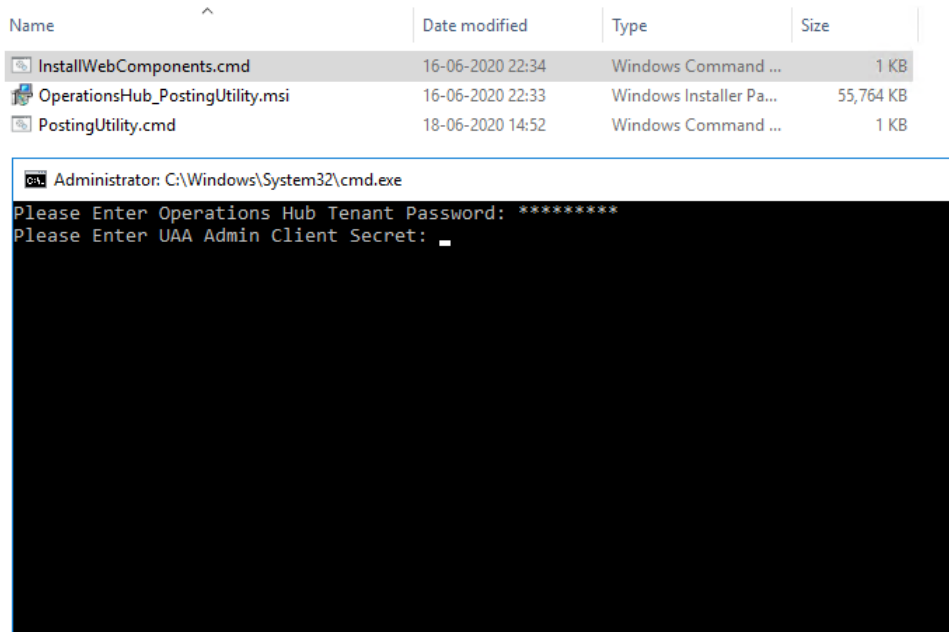
You must run the utility to import the Plant Applications into Operations Hub.

 **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.

1. **Enterprise Installation:** In the directory <Installation\_Directory>/OperationsHub\_PostingUtility, run (run as administrator) the **InstallWebComponents.cmd** file.
2. **Standard 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.



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.


## Verify the Installation

Ensure that you have cleared the browser cache before accessing the Plant Applications Web Client URL.

1. Open the Chrome browser and access the following application: `https://<OperationsHub_server_name>/run/?app_name=Plant%20Applications`
2. Login with the username and password of the Web Client you have used in the installation.  
The Plant Applications Web Client application appears. Select an application icon on the left menu to open the corresponding application.

## Access REST APIs

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.


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

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

 **Note:** You can find all the application service names in the following link: [API Endpoint Documentation](#). You can select the individual links to access detailed API documentation.

`https://webclientservername:5059/ncm-app-service/swagger-ui.html`

**For Workorder Service:** `https://webclientservername:5059/workorder-service/apidocs/index.html`

 **Note:** All the Plant Applications Web Client applications run behind reverse proxy, which uses the port number 5059.

The Swagger UI appears.

3. **Only for Work Order Service:** To access the Swagger UI for Work Order Service, you must perform following steps in the Operations Hub Server:
  - a. Go to the `C:\ProgramData\GE\Operations Hub\uaa-config` location.
  - b. Using a text editor, update the **uaa.yml** file by adding the below lines at the end of file with proper indentation.

```
cors:
  xhr:
    allowed:
      headers:
        - X-Requested-With
        - Authorization
      methods:
        - POST
```


- c. Restart the **GE Operations Hub UAA Tomcat Web Server** service.

4. Select **Authorize**.  
The **Available authorizations** window appears.

5. In the **Available authorizations** window, scroll down to the **resource\_owner (OAuth2, password)** section, enter the following values, and then select **Authorize**:

Field	Description
username	Enter the Plant Applications Server username.
password	Enter the Plant Applications Server password.

Field	Description
client_id	Enter a value in the following format: <node name of Plant Applications Web Client>_mes. For example, if the node name is wserver, enter wserver_mes.
client_secret	Enter <b>plantappssecret</b> as the client secret.

 **Note:** In any case, if you are unable to see the **username** and **password** fields, refer to [Swagger Url Authorization Issue \(page 103\)](#).


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

## Configure a GE Proficy Historian Server for the Analysis Application



The Analysis application supports plotting of Historian tags from a GE Proficy Historian Server 8.1 SIM x version only (version 9.0 is not supported). 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:

- Based on your type of installation, perform one of the below:
  - Enterprise Installation:** In the directory `<buildpath>/PlantApplicationsDocker/plantapps-web-docker/mnt/configfiles/historian-config/prod/<version>/`, access the `historian-config-prod.properties` file by using a text editor.
  - Standard Installation:** In the directory `<Installation_directory>\config-repo\historian-config\prod\<version>\`, access the `historian-config-prod.properties` file by using a text editor.
- In the `historian-config-prod.properties` file, enter the properties and their details for each GE Proficy Historian Server as described in the following table.

 **Note:** It is recommended to use the same server name format (either IP address, FQDN, or host name) in all the properties to minimize the connection issues. For example, if you have entered FQDN for the `hist<n>.service.origin` property, you must use FQDN format for the `hist<n>.service.hostname` and `hist<n>.uaa.origin` properties as well.

Property	Description
<code>hist&lt;n&gt;.service.origin</code>	Enter the IP address, FQDN, or host name of the GE Proficy Historian Server.

Property	Description
<code>hist&lt;n&gt;.service.port</code>	Enter the port number on which the GE Proficy Historian Server is installed.  <b>Tip:</b> You can leave this property blank if the GE Proficy Historian Server is installed on the default port 8443.
<code>hist&lt;n&gt;.service.hostname</code>	Enter the IP address, FQDN, or host name of the GE Proficy Historian Server as configured in the Plant Applications Administrator. For example, <code>GESERVER</code> .  <b>Note:</b> The IP address, FQDN, or host name must match with the <b>Server Name</b> configured in Historian Connections screen of the Plant Applications Administrator.
<code>hist&lt;n&gt;.service.client.id</code>	Enter the client id of the Historian Administrator. <ul style="list-style-type: none"> <li>Historian 7.0: <b>admin</b> is the default.</li> <li>Historian 8.0 or later: <b>&lt;hostname.admin&gt;</b> where the host name is the name of the server where the Historian web tools are installed.</li> </ul>
<code>hist&lt;n&gt;.service.client.secret</code>	Enter the client secret of the Historian Administrator.
<code>hist&lt;n&gt;.uaa.origin</code>	Enter the IP address, FQDN, or host name of the UAA server.
<code>hist&lt;n&gt;.uaa.port</code>	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 file.
4. Restart the `mes-dataservice-impl-0.6.7` and `processanalyzer-service-impl-0.6.7` services to apply the changes.

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

## Configure the Cache Settings for the Historian Tags

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


1. Based on your type of installation, perform one of the below:
  - **Enterprise Installation:** In the directory `<buildpath>/PlantApplicationsDocker/plantapps-web-docker/mnt/configfiles/`

mes-dataservice/prod/<version>/, access the mes-dataservice-prod.properties file by using a text editor.

- **Standard Installation:** In the directory <Installation-directory> \PlantApplicationsWebClient\config-repo\mes-dataservice\prod\<version>, access the mes-dataservice-prod.properties file by using a text editor. Where:

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: <code>historianTagMaxCacheSize=50000</code>
historianTagCacheTimeOut	Enter the duration in the format <code>duration&lt;timeformat&gt;</code> after which the cached Historian tags are cleared by the <code>mes-dataservice-impl</code> microservice. Where: <code>&lt;timeformat&gt;</code> is <code>h</code> , <code>m</code> , or <code>s</code> to indicate time in hours, minutes, or seconds, respectively. The default value is <code>6h</code> .  Example: <code>historianTagCacheTimeOut=6h</code>
<code>scheduler.tagcaching.seconds</code>	Enter the duration in seconds after which the Historian tags are cached again by the <code>mes-dataservice-impl</code> microservice. The default value is <code>21600</code> .  Example: <code>scheduler.tagcaching.seconds=21600</code>


 **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. Based on your type of installation, perform one of the below:

- **Enterprise Installation:** In the directory <buildpath>/PlantApplicationsDocker/plantapps-web-docker/mnt/configfiles/processanalyzer-app-service/prod/<version>/, access the processanalyzer-app-service.properties file by using a text editor.
- **Standard Installation:** In the directory <Installation-directory> \PlantApplicationsWebClient\config-repo\processanalyzer-app-service\prod\<version>, access the processanalyzer-app-service.properties file by using a text editor. Where:

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 the `mes-dataservice` and `processanalyzer-app-services` services.

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

## *Configure the Cache Settings for the Plant Applications Services*

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.

- Enterprise Installation:** In the directory `<Installation_Directory>/PlantApplicationsDocker/plantapps-web-docker`, access the `env.yml` file by using the vi editor.
- Standard 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.
- 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	scheduler_workorder_timer_seconds: 7200
	scheduler_mes_timer_seconds: 1800
route-service	maximumProductCacheSize: 1000
	cacheProductExpireAfterAccess: "15m"
	schedulerTime: 36000
route-app-service	maximumProductCacheSize: 1000
	schedulerTime: 36000
	cacheProductExpireAfterAccess: "15m"
supervisor-app-service	supervisor.scheduler.delay=3600000
segmentdefinitionservice	maximumCacheSize: 100
	cacheExpireAfterAccess: "50m"
operator-app-service	maximumDayCacheSize = 1000 cacheDayExpireAfterAccess = 24h maximumShiftCacheSize=100 cacheShifExpireAfterAccess=4h maximumWeekCacheSize=1000 cacheWeekExpireAfterAccess=168h
erp-import-service	maximumCacheSize: 100
	cacheExpireAfterWrite: 5m
erp-export-service	maximumCacheSize: 100
	cacheExpireAfterWrite: 5m
	cacheLaborExpireAfterAccess: 60m
process-analyzer-app-service	maximumCacheSize=100
	cacheExpireAfterAccess=20m
	tagVariableMaxCacheSize=100
	tagVariableCacheTimeOut=6h
	kpiMaxCacheSize=40
	kpiCacheTimeOut=30m
	siteParameterMaxCacheSize=20
	siteParameterCacheTimeOut=1h

Service Name	Properties
mes-data-service	historianTagMaxCacheSize=50000
	historianTagCacheTimeOut=6h
	scheduler.tagcaching.seconds=21600
alarm-app-service	maximumDayCacheSize: 100
	cacheDayExpireAfterAccess: 12h
	maximumShiftCacheSize: 100
	cacheExpireAfterShiftAccess: 8h
	maximumHourCacheSize=100
	cacheExpireAfterHourAccess=1h
productionmetrics-app-service	maximumDayCacheSize: 100
	cacheDayExpireAfterAccess: 1h
	maximumWeekCacheSize: 100
	cacheWeekExpireAfterAccess: 24h
	maximumShiftCacheSize: 1
	cacheShiftExpireAfterAccess: 10m
downtime-app-service	maximumHourCacheSize: 100
	cacheDayExpireAfterHourAccess: 1h
	maximumDayCacheSize: 100
	cacheExpireAfterDayAccess: 24h
productionschedulerappservice	maximumSize=500
	configurationCacheExpiryTime: 30m
processorderservice	maximumSize=1000
	configurationCacheExpiryTime=1m
waste-management-app-service	maximumDayCacheSize=1000
	cacheDayExpireAfterAccess=24h
	maximumWeekCacheSize=1000
	cacheWeekExpireAfterAccess=168h
	maximumShiftCacheSize=100
	cacheShiftExpireAfterAccess=4h
webgenealogy-app-service	genealogy.scheduler.timer.seconds=36000
Bom-management-app-service	maximumCacheSize=100

Service Name	Properties
	cacheExpireAfterWrite=1h
Approval-cockpit-service	NA (observed a few cache properties defined in application.properties file but they're not in use).
Approval-cockpit-app-service	NA (observed a few cache properties defined in application.properties file but they're not in use).
Receiving-inspection-app-service	maximumCacheSize=100
	cacheExpireAfterWrite=1h
Receiving-inspection-service	cacheExpireAfterWrite=1h
	maximumCacheSize=100
Time-booking-app-service	cacheExpireAfterWrite=1h
	maximumCacheSize=100
property-definition-app-service	maximumDayCacheSize = 100
	cacheDayExpireAfterAccess = 1h
	maximumShiftCacheSize=1
	cacheShifExpireAfterAccess=10min
	maximumWeekCacheSize=100
	cacheWeekExpireAfterAccess=24h
property-definition-service	maximumDayCacheSize = 100
	cacheDayExpireAfterAccess = 1h
	maximumShiftCacheSize=1
	cacheShifExpireAfterAccess=10min
	maximumWeekCacheSize=100
	cacheWeekExpireAfterAccess=24h
usersettings-service	maximumDayCacheSize = 100
	cacheDayExpireAfterAccess = 24h
activities-app-service	maximumHourCacheSize=100
	cacheDayExpireAfterHourAccess=1h
	maximum5MinCacheSize=100
	cacheExpireAfter5MinAccess=5m
	maximumShiftCacheSize=100
	cacheExpireAfterShiftAccess= <b>8h</b>
activities-service	maximum5MinCacheSize=100

Service Name	Properties
	cacheExpireAfter5MinAccess=5m
	maximumHourCacheSize=100
	cacheDayExpireAfterHourAccess=1h
	maximumDayCacheSize=100
	cacheExpireAfterDayAccess= <b>24h</b>
esignature-app-service	maximumShiftCacheSize=10
	cacheExpireAfterShiftAccess=8h
my-machines-service	maximumDayCacheSize = 100
	cacheExpireAfterAccess = <b>24h</b>

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.

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

## *Configure to Route Enable a Production Line*

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.

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

## *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.

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.

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`

## Access Application Log Files

If an application or a service encounter any errors, you can use the application log files that provide useful troubleshooting information.

### Access Standard (Windows) Web Client Logs

You can access the service logs located at `<Installation_directory>\GE Digital \PlantApplicationsWebClient\ServiceLogs`.

### Access Enterprise (Linux) Web Client Logs

You can access the service logs located at `<buildpath>\PlantApplicationsDocker\plantapps-web-docker/mnt/logs`, where `<buildpath>` is the location that you specified in the `silentinstaller.yml` file during the Enterprise Web Client installation.

### Set the size limit for Log files

By default, the maximum limit for Work Queue and Unit Operations log file size is set to 10MB. That is, if the receptive log file reaches 10MB in size, a new log file will be created. These files are retained for 14 days and the old files are archived. However, you can change these settings by modifying `maxSize` and `maxFiles` parameters in the `operator-app-prod.yml` and `workqueue-app-prod.yml` files. Follow below instructions to change these parameters in respective files:

#### Unit Operations Log Settings:


1. Based on your type of installation, perform one of the below:
  - **Enterprise Installation:** In the directory `<buildpath>/PlantApplicationsDocker/plantapps-web-docker/mnt/configfiles/operator-app/prod/<version>`, access the `operator-app-prod.yml` file by using a text editor.
  - **Standard Installation:** In the directory `<Installation_directory>\config-repo\operator-app\prod\<version>`, access the `operator-app-prod.yml` file by using a text editor.
2. In the `operator-app-prod.yml` file, search and update the following `loggerSettings` with required values:

```
"maxSize": "10000000"
"maxFiles": "14d"
```



For example:

```
"maxSize" : "5000000"
"maxFiles" : "7d"
```

 **Note:** It is recommended to use the file size range from 5MB (5000000) to 20MB (20000000).

3. After making the modifications, save the file and then restart the operator- app.

### Work Queue Log Settings:

1. Based on your type of installation, perform one of the below:


- **Enterprise Installation:** In the directory <buildpath>/PlantApplicationsDocker/plantapps-web-docker/mnt/configfiles/workqueue-app/prod/<version>, access the workqueue-app-prod.yml file by using a text editor.
- **Standard Installation:** In the directory <Installation\_directory>\config-repo\workqueue-app\prod\<version>, access the workqueue-app-prod.yml file by using a text editor.

2. In the workqueue-app-prod.yml file, search and update the following **loggerSettings** with required values:

```
"maxSize" : "10000000"
"maxFiles" : "14d"
```

For example:

```
"maxSize" : "5000000"
"maxFiles" : "7d"
```

 **Note:** It is recommended to use the file size range from 5MB (5000000) to 20MB (20000000).

3. After making the modifications, save the file and then restart the work queue app service.

### Log Levels

By default, the log files are populated with the warning messages only. However, to change what type of messages needs to be populated in the service log files, you can set the logging levels to debug more detail logs. The log levels helps you to identify and troubleshoot any errors that you may encounter. Below are the properties that you can set either in the **portainer** or in the common-service-prod.properties file.

1. Based on your type of installation, perform one of the below:

- **Enterprise Installation:** In the directory <buildpath>/PlantApplicationsDocker/plantapps-web-docker/mnt/

configfiles/common-service/prod/1.0.1/, access the common-service-prod.properties file by using a text editor. For example, `$sudo nano common-service-prod.properties`

- **Standard Installation:** In the directory <Installation\_directory>\config-repo\common-service\prod\1.0.1, access the common-service-prod.properties file by using a text editor.
2. In the common-service-prod.properties file, search and update the following properties as follows:
    - logging.level.root=DEBUG
    - logging.level.com.ge.bm=DEBUG
    - logging.level.com.ge.digital=DEBUG
  3. For **work-order-service**, search and update the following properties as follows:
    - Logging.LogLevel.Microsoft=Information
    - Logging.LogLevel.Default=Information
    - Logging.LogLevel.GE=Information
    - Logging.LogLevel.Microsoft.EntityFrameworkCore=Information
  4. After making the modifications, save the file and then restart the specific service that you want to debug.

## *Access Connection Properties*

You can use the common-service-prod.properties file to access the connection details of Database, UAA, CouchDB, and RabbitMQ Message properties.

To configure or modify one or more connection properties for the Plant Applications, follow these steps:

1. Based on your type of installation, perform one of the below:
  - **Enterprise Installation:** In the directory <buildpath>/PlantApplicationsDocker/plantapps-web-docker/mnt/configfiles/historian-config/prod/1.0.1/, access the common-service-prod.properties file by using a text editor.
  - **Standard Installation:** In the directory <Installation\_directory>\config-repo\common-service\prod\1.0.1, access the common-service-prod.properties file by using a text editor.
2. In the common-service-prod.properties file you can modify required Database, UAA, CouchDB, and RabbitMQ Message properties and save the file.
3. To take effect for any modifications to this file, you must restart the respective services.

## 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.

### Run the Migration Utility

1. Download this utility (**uaa-users-migration-utility.zip**) from this link: [Download uaa-users-migration-utility.zip](#).
2. Unzip the `uaa-users-migration-utility.zip` file.
3. Select the `runutility.bat` file.

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

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

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

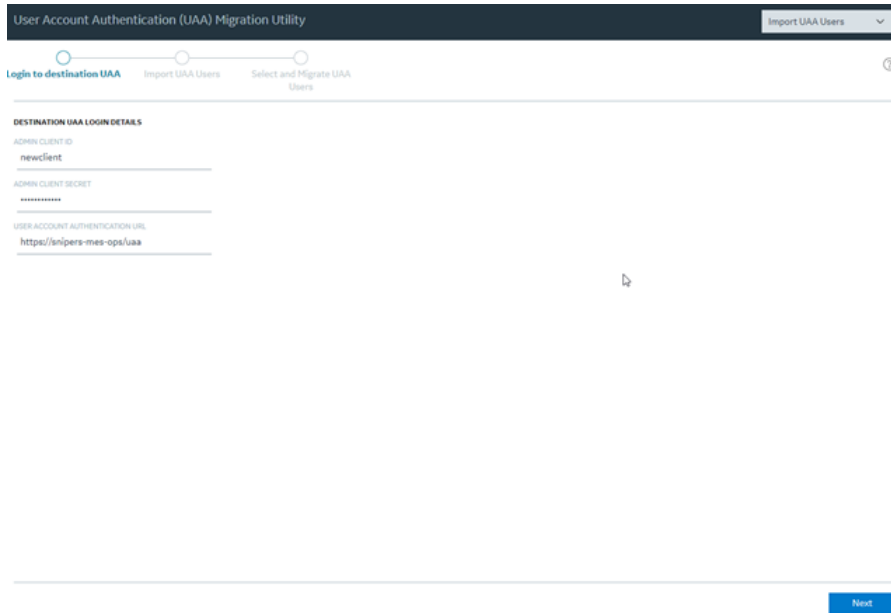
2. Select **Next**.  
The details of the user in the UAA system is displayed.
3. Select the users that you want to migrate.
  - To migrate individual users, select the check box next to the respective username.
  - To migrate all the users listed in the table, select the **User Name** check box.
4. Select **Export to CSV**.

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

 **Note:** This file is not encrypted.

## Import UAA Users

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**.

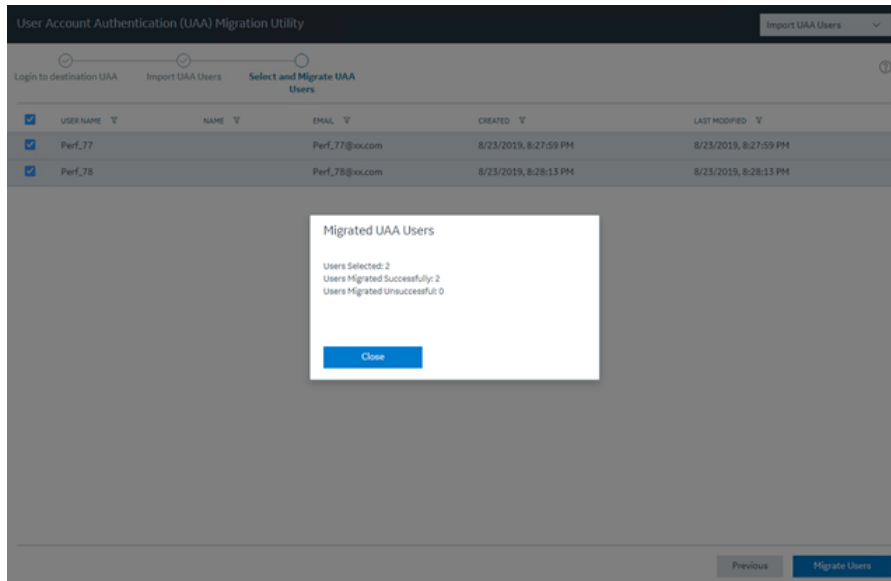
Option	Description
<b>Field</b>	<b>Description</b>
<b>ADMIN CLIENT ID</b>	A unique string representing the registration information provided by the client.
<b>ADMIN CLIENT SECRET</b>	The secret passphrase configured for the OAuth client.
<b>USER ACCOUNT AUTHENTICATION URL</b>	URL of the server to which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

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*

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.


There are two methods to map LDAP groups with Operations Hub UAA groups:

1. **Using the UAA/LDAP Connectivity tool directly:** In this method, you map the Operations Hub UAA group for each application with an appropriate LDAP group.

**Important:** If you want to use discrete applications, you cannot use this method.

2. **Using the Security application in Web Client:** In this method, you create a group in the Security application, add all the applications to this group, and then map this group with the appropriate LDAP group using the UAA/LDAP Connectivity tool.

This topic describes these two methods.

 **Note:** You cannot view more than 100 UAA groups using the UAA/LDAP Connectivity tool.

[Import UAA users \(page 100\)](#).

1. If you want to use the UAA/LDAP Connectivity tool directly, map the Operations Hub UAA group for each application with an appropriate LDAP group. For instructions, refer to [https://www.ge.com/digital/documentation/opshub/windows/windows/t\\_uaa\\_map\\_ldap\\_groups\\_with\\_oh\\_uaa.html?hl=ldap](https://www.ge.com/digital/documentation/opshub/windows/windows/t_uaa_map_ldap_groups_with_oh_uaa.html?hl=ldap).

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

2. If you want to use the Security application in Web Client:
  - a. Access Security.
  - b. Create a group (*page*      ).
  - c. Add applications (*page*      ) to the group that you have created.

- d. Using the UAA/LDAP Connectivity tool, map the group that you have created with the appropriate LDAP group. For instructions, refer to [https://www.ge.com/digital/documentation/opshub/windows/windows/t\\_uaa\\_map\\_ldap\\_groups\\_with\\_oh\\_uaa.html](https://www.ge.com/digital/documentation/opshub/windows/windows/t_uaa_map_ldap_groups_with_oh_uaa.html).

## Swagger Url Authorization Issue

Use this section, if you are unable to see the **username** and **password** fields in the **Available authorizations** window. Enter the following

1. In the **Available authorizations** window, scroll down to the **resource\_owner (OAuth2, password)** section, enter the following values, and then select **Authorize**:

Field	Description
client_id	Enter a value in the following format: <node name of Plant Applications Web Client>_mes. For example, if the node name is wserver, enter wserver_mes.
client_secret	Enter <b>plantappssecret</b> as the client secret.

The UAA login page appears.

2. In the UAA login page, enter the UAA credentials and then select **Login**.  
Once the credentials are validated, you will be redirected back to the **Available authorizations** window.

## Replace the Expired Self-Signed Certificate

You can use this section to replace the expired self-signed certificates with new self-signed/signed certificate. This procedure includes using the self-signed Operations Hub certificate.

1. Stop the **GE.PlantApps.Httpd** service.
2. From the <Webclient\_Installation\_path>\Service-Httpd\conf\cert location, delete the public.pem and key.pem files.
3. Navigate to the C:\Program Files\GE\Operations Hub\httpd\conf\cert location.
4. Copy the server.crt and the server.pem files to the <Webclient\_Installation\_path>\Service-Httpd\conf\cert location.
5. Rename server.crt to public.pem and server.pem to key.pem.
6. Start the **GE.PlantApps.Httpd** service.

# Chapter 8. Reference

## *Configure the GE Proficy Historian Server Security Settings*

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.

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.





