Proficy Plant Applications 2022

Web Client Installation Guide

Copyright GE Digital

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

Chapter 1. Installation Overview

Installation Overview

The Plant Applications Web Client provides the following methods of installation:

- **Standard Installation**: This is used to install Plant Applications Web Client for both Process and Discrete applications on a Windows machine. See About Installing Standard Web Client *(page 19)*.
- **Enterprise Installation**: This is used to install Plant Applications Web Client for both Process and Discrete applications on a Linux machine. See About Installing Enterprise Edition Web Client *(page 71)*.

Chapter 2. System Requirements (Standard and Enterprise)

Standard Edition Web Client Requirements

Before you begin

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

- System requirements *(page 7)*
- Port requirements *(page 8)*

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.

The Plant Application Server and Web Client servers can be hosted in the AWS/Azure Cloud. Ensure that when they are hosted in Cloud they meet the Plant Application and Web Client Server system requirements.

Item	Version
Operating system	64-bit Windows 10, Windows Server 2022, Windows Server 2016, or Windows Server 2022
Couch DB server	CouchDB version 2.3.1 installed and configured on a Windows machine. **Note:** For more information on downloading, installing, and configuring CouchDB, refer to Install and Configure Apache CouchDB *(page 13)*.
Operations Hub	2.1 with SIM3 and later **Important:** If using Operations Hub 2022, be aware that after you install Operations Hub you must restart your computer before installing the Plant Applications Web Client.

Item	Version
Web browsers	Chrome 92 and later. **Devices**: • **iPad**: Safari v13.1+, Chrome 92 and later **Note:** To view the application content, you must select the desktop site option from the Chrome browser settings menu. • **HP tablet**: Chrome 92 and later **Note:** Devices supports only Unit Operations,Work Queue, and Non Conformance applications. • **Android 10-inch Tablet**: Chrome 92 and later. **Note:** To view the application content, you must select the desktop site option from the Chrome browser settings menu.
OLEDB Driver	Microsoft OLE DB Driver 18 for SQL Server **Note:** You can download the Microsoft OLE DB Driver 18 for SQL Server from the following URL: https://www.microsoft.com/en-us/download/details.aspx?id=56730.
Hard drive	100 GB (minimum recommended)
Processor	2.4 GHz clock-speed Intel Core i3, i5, or i7 CPU or equivalent AMD Phenom CPU **Note:** For better performance, we recommend to use a octa core (8-cores) processor.
Memory	32 GB (minimum recommended) **Note:** You must have minimum 64 GB or more if you plan to install Web Client, 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 https port for CouchDB.
443/5059	The default port for Web Applications

What to do next: Complete the pre-installation configuration, and then proceed to install the Plant Applications Standard Edition Web Client. See About Installing Standard Web Client *(page 19)*.

Enterprise Edition Web Client Requirements

Before you begin

Ensure that you have completed the following tasks:

- Installation of Plant Application Server
- Installation of Operations Hub 2.1 with SIM3 and later

  ❗ **Important:** If using Operations Hub 2022, be aware that after you install Operations Hub you must restart your computer before installing the Plant Applications Web Client.

- Installation and Configuration of CouchDB for HTTPS

System Requirements

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

The Plant Application Server and Web Client servers can be hosted in the AWS/Azure Cloud. Ensure that when they are hosted in Cloud they meet the Plant Application and Web Client Server system requirements.

Item	Version
Operating system	RedHat 7.8 and 8.2 or Ubuntu 18.x **Note:** Ubuntu is not supported in a production environment.
Docker	• Docker Community Edition or Enterprise Edition 19.0 or 20.0 **Note:** For installing Docker Engine, refer to https://docs.docker.com/engine/install/. • For RedHat environment, we recommend to use Docker 20.x • Docker Compose 1.25.x **Note:** For installing Docker Compose, refer to https://docs.docker.com/compose/install/. • Docker Swarm initiated as Swarm Manager
Web browsers	Chrome 92 and later. **Devices**: • **iPad**: Safari v13.1+, Chrome 92 and later **Note:** To view the application content, you must select the desktop site option from the Chrome browser settings menu. • **HP tablet**: Chrome 92 and later, with minimum resolution 1920x1280 **Note:** Devices supports only Unit Operations, Work Queue, and Non Conformance applications. • **Android 10-inch Tablet**: Chrome 92 and later **Note:** To view the application content, you must select the desktop site option from the Chrome browser settings menu.
Couch DB server	CouchDB version 2.3.1 installed and configured on a Windows machine. **Note:** For more information on downloading, installing, configuring CouchDB, and binding the certificates, refer to Install and Configure Apache CouchDB *(page 13)* and Bind the Certificates to Apache CouchDB *(page 17)*.

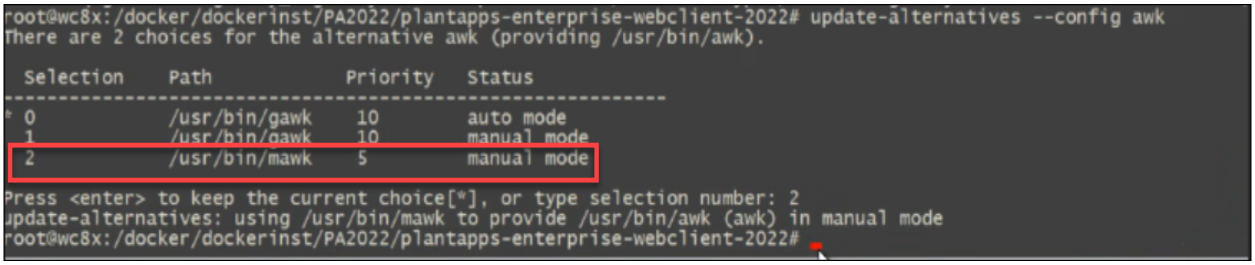
Item	Version
Hard drive	100 GB (minimum) **Note:** However, you may need more disk space based on your production data.
Processor	2.4 GHz clock-speed Intel Core i3, i5, or i7 CPU or equivalent AMD Phenom CPU **Note:** For better performance, it is recommended to use an octa core (8-cores).
Memory	32 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.
- 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.

Note:

If the Linux machine has multiple **awk** versions available, then switch to **mawk** by typing the following command: `sudo update-alternatives --config awk`. This command lists the available **awk** versions and you must select the **mawk** version.



```
root@wc8x:/docker/dockerinst/PA2022/plantapps-enterprise-webclient-2022# update-alternatives --config awk
There are 2 choices for the alternative awk (providing /usr/bin/awk).

  Selection    Path             Priority   Status
------------------------------------------------------------
* 0            /usr/bin/gawk     10        auto mode
  1            /usr/bin/gawk     10        manual mode
  2            /usr/bin/mawk     5         manual mode

Press <enter> to keep the current choice[*], or type selection number: 2
update-alternatives: using /usr/bin/mawk to provide /usr/bin/awk (awk) in manual mode
root@wc8x:/docker/dockerinst/PA2022/plantapps-enterprise-webclient-2022#
```

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.

Port	Description
9093	The default port for Kafka.
2185	The default port for ZooKeeper.
6984	The default https port for CouchDB.
443/5059	The default port for Web Applications

What to do next: Complete the pre-installation configuration, and then proceed to install the Plant Applications Enterprise Edition Web Client. See About Installing Enterprise Edition Web Client *(page 71)*.

Chapter 3. Pre-installation Configuration (Enterprise and Standard)

Install and Configure Apache CouchDB

Apache CouchDB is a document storage application that stores the documents used in discrete applications.

Plant Applications support Apache CouchDB 2.3.1.

To install Apache CouchDB, download CouchDB for Windows at http://archive.apache.org/dist/couchdb/binary/win/2.3.1/.

Note: If you experience problems while downloading the files from the Apache CouchDB website, then click here to download the files.

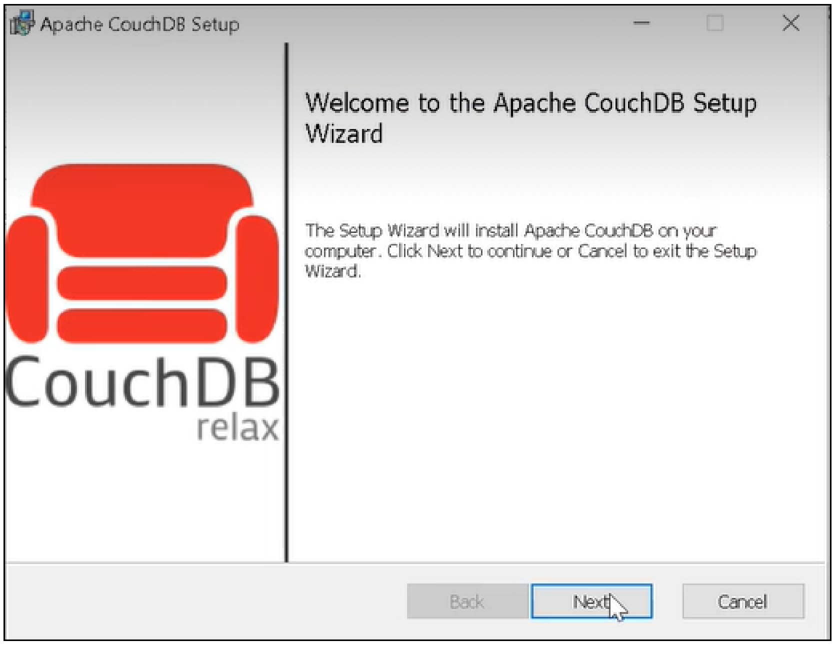
Use this procedure to install and configure ApacheCouchDB.

We recommend to install Apache CouchDB on the following nodes:

- In Standard Edition Plant Applications, install Apache CouchDB on the Plant Applications Web Client node.
- In Enterprise Edition Plant Applications, install Apache CouchDB on the Operations Hub node.

1. Right-click `apache-couchdb`, and then select **Install**.

   The **Apache CouchDB Setup** page appears.

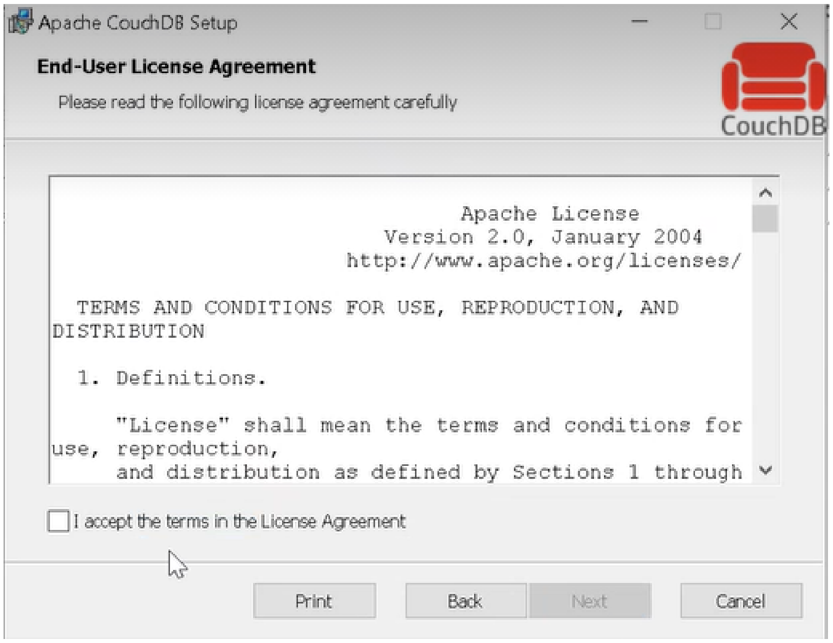


Welcome to the Apache CouchDB Setup Wizard

The Setup Wizard will install Apache CouchDB on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

2. Select **Next**.

   The **License Agreement** page appears.



End-User License Agreement

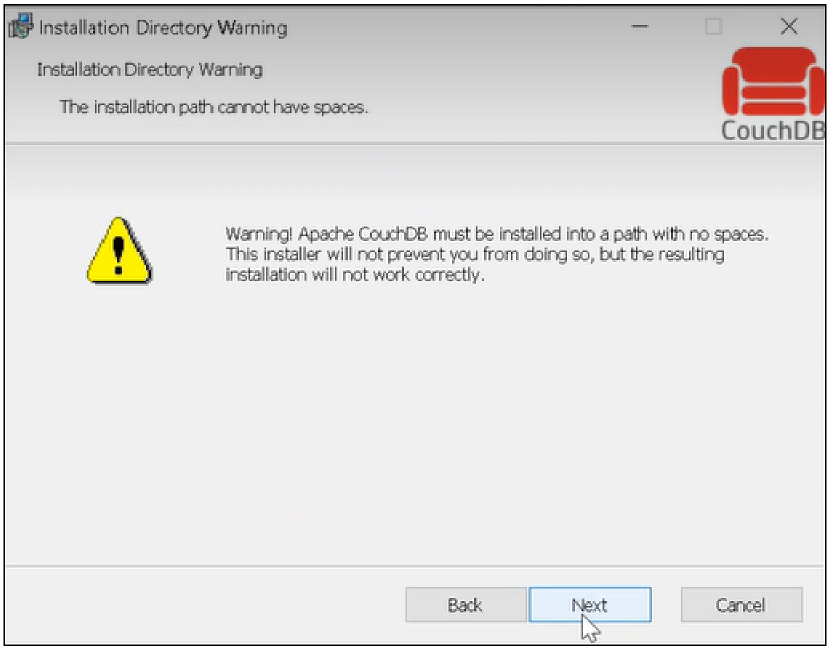
Please read the following license agreement carefully

```
                                 Apache License
                           Version 2.0, January 2004
                        http://www.apache.org/licenses/

    TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND
DISTRIBUTION

    1. Definitions.

       "License" shall mean the terms and conditions for
use, reproduction,
       and distribution as defined by Sections 1 through
```

□ I accept the terms in the License Agreement

3. Select the **I accept the terms in the License Agreement** checkbox, then select **Next**.

   The **Installation Directory Warning** page appears.



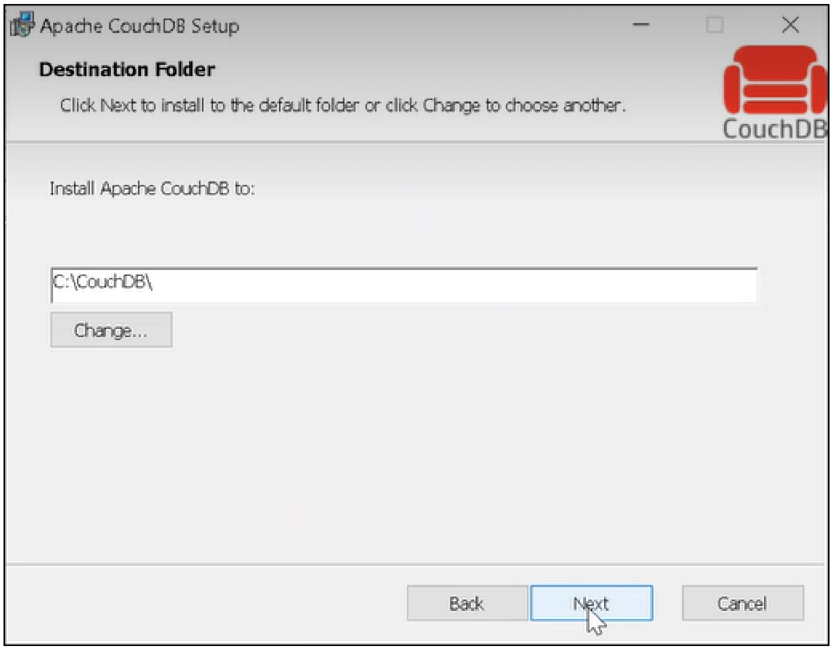
Installation Directory Warning

The installation path cannot have spaces.

Warning! Apache CouchDB must be installed into a path with no spaces. This installer will not prevent you from doing so, but the resulting installation will not work correctly.

4. Select **Next**.

   The **Destination Folder** page appears.



Destination Folder

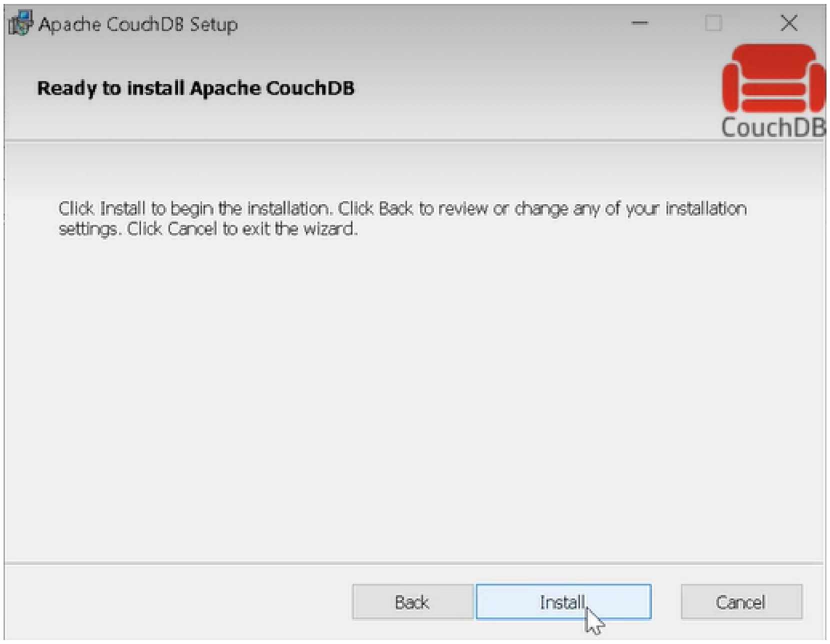
Click Next to install to the default folder or click Change to choose another.

Install Apache CouchDB to:

C:\CouchDB\

5. Select **Next** to install Apache CouchDB to the default folder or select **Change** to select a different location in the **Destination Folder** window.

   The **Ready to install Apache CouchDB** page appears.



Ready to install Apache CouchDB

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

6. Select **Install**.

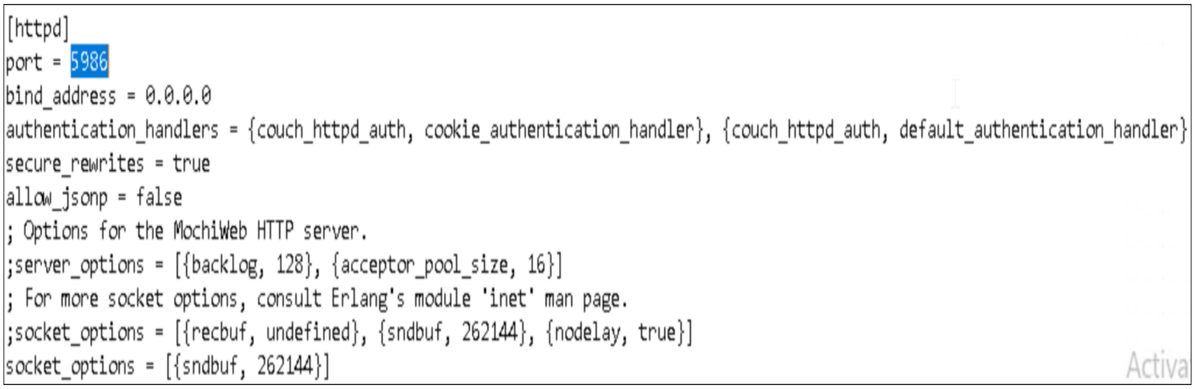
   The **Installing CouchDB** page appears and displays the progress bar.

   When installation is complete, the **Completed the Apache CouchDB Setup Wizard** appears.

7. Select **Finish** to close the setup wizard.

   Note:

   CouchDB uses 5986 for internal communications. If you are not able to access CouchDB, then verify if port 5986 is used by any other applications (for example, Azure Resource Manager uses port 5986). If it is used by other application then change the httpd port number from 5986 to 5987 in the `default.ini` file located under `CouchDB/etc`, then start the CouchDB service.



```
[httpd]
port = 5986
bind_address = 0.0.0.0
authentication_handlers = {couch_httpd_auth, cookie_authentication_handler}, {couch_httpd_auth, default_authentication_handler}
secure_rewrites = true
allow_jsonp = false
; Options for the MochiWeb HTTP server.
;server_options = [{backlog, 128}, {acceptor_pool_size, 16}]
; For more socket options, consult Erlang's module 'inet' man page.
;socket_options = [{recbuf, undefined}, {sndbuf, 262144}, {nodelay, true}]
socket_options = [{sndbuf, 262144}]
```

Apply Certificates to Apache CouchDB

Create a folder named `cert` where Apache CouchDB is installed.

Use this procedure to apply certificate to Apache CouchDB. If you do not have the signed certificate, then you can use the self-signed certificate provided along with the Operations Hub Installer.

1. Navigate to `C:\Program Files\GE\Operations Hub\httpd\conf\cert` folder in Operations Hub machine, then double-click the `cert` folder.

   The `cert` folder displays a list of certificates.

2. Copy the `server.crt` and `server.key` certificates, and then paste them to the `Apache CouchDB` folder on the machine where CouchDB is installed.

Bind the Certificates to Apache CouchDB

- Verify that you have installed Apache CouchDB on a Windows machine.
- Verify that you have copied the `server.crt` and `server.key` certificates to the `Apache CouchDB` folder. See Apply Certificates to Apache CouchDB *(page 17)*.

By default CouchDB runs on HTTP, you must configure the settings to run CouchDB on HTTPS. To configure the HTTPS, use the self-signed or signed certificates and perform the following steps:

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, right-click the `config_couchDB.bat` file, and then select **Run as administrator**.

   The command prompt window appears and prompts you for inputs.

3. Enter details for the following:
   - Path of the certificate file where Apache CouchDB is installed. For example, `C:\Program Files\CouchDB\certs\server.crt`.
   - Path of the key file Apache CouchDB is installed. For example, `C:\Program Files\CouchDB\certs\server.key`.
   - Path where the Apache CouchDB is installed. For example, `C:\Program Files\CouchDB`.

The Apache CouchDB settings are successfully configured, when the system does not display any error message and the command prompt window closes.

Note:

- To configure CouchDB with SSL, use certificates issued to the CouchDB server (machine) name.

4. To verify that CouchDB runs on HTTPS and port number 6984, in a compatible web browser, type `https://<host name or IP address of Apache CouchDB>:<port number>/_utils/`. For example, `https://host name or IP address of CouchDB:6984/_utils/`. Ensure that you use the fully qualified domain name or the IP address.

Add a User to Apache CouchDB

1. In a compatible web browser, type `https://<host name or IP address of Apache CouchDB>:<port number>/_utils/`, where the port number is 6984.

   The Apache CouchDB dashboard appears.

2. In the left navigation pane, select **User**.

   The **Create Admins** page appears.

3. Enter the user name and password.
   These are the credentials the user will use to log in to Apache CouchDB.

4. Select **Create Admins**.

   The **Log in** page appears.

5. Enter the user name and password, then select **Log in**.

Proceed to install the Plant Applications Standard Edition Web Client (See About Installing Standard Web Client *(page 19)*) or the Plant Applications Enterprise Edition Web Client (See About Installing Enterprise Edition Web Client *(page 71)*)

Chapter 4. Install Plant Applications Standard Web Client

About Installing Standard Web Client

Installing Plant Applications Standard Edition 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.

With the release of Plant Applications 2022 and later, you can now perform a silent installation of Plant Applications Standard Edition Web Client for Windows.

The following table outlines the steps that you must complete to install Plant Applications Standard Edition 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 Workflow 2.6 SP1	This step is required.
2	Install Plant Applications Server	This step is required.
3	Install Operations Hub 2.1 with SIM3 and later ❗ **Important:** If using Operations Hub 2022, be aware that after you install Operations Hub you must restart your computer before installing the Plant Applications Web Client.	This step is required.
4	Install and Configure Apache CouchDB *(page 13)*	This step is required.
5	Ensure that your system meets the requirements for the Standard Web Client installation. *(page 7)*	This step is required.
6	• Install Standard Web Client Using GUI *(page 20)* OR • Install Plant Applications Standard Web Client in Silent Mode *(page 39)*	This step is required.
7	After the Standard Web Client installation, ensure to run the Message Bridge Configuration utility. *(page 90)*	This step is required.
8	Verify the Installation *(page 95)*	This step is required.

Pre-Installation Checklist

1. Ensure that your system meets the requirements for installing Plant Applications Standard Web Client on Windows machine.
2. Ensure that you have Workflow, Plant Applications Server, Plant Applications Client, Operations Hub, and CouchDB installed and running before installing Plant Applications Standard Web Client. For information, refer to the Standard Deployment Architecture section in the *Getting Started Guide*.
3. Install Apache CouchDB, and then do this:
    a. Apply Certificates to Apache CouchDB *(page 17)*
    b. Add a User to Apache CouchDB *(page 18)*
4. Install Standard Web Client Using GUI *(page 20)* or Install Plant Applications Standard Web Client in Silent Mode *(page 39)*
5. Run the Message Bridge Configuration Utility *(page 90)*

Plant Applications Standard Web Client Installation Options

You can use any of the following installation methods to install Plant Applications Standard Web Client:

- **Graphical User Interface (GUI)-based installation**: The GUI-based installation wizard prompts for sequence of dialog boxes, guides you through the installation process, and summarizes the results when complete. This is the default installation approach. See Install Standard Web Client Using GUI *(page 20)*.
- **Unattended installation**: The unattended installation (Command Line Installation) allows you to run the standard installation settings through a command line interface without the need of a graphical user interface. See Install Plant Applications Standard Web Client in Silent Mode *(page 39)*.

Install Standard Web Client Using GUI

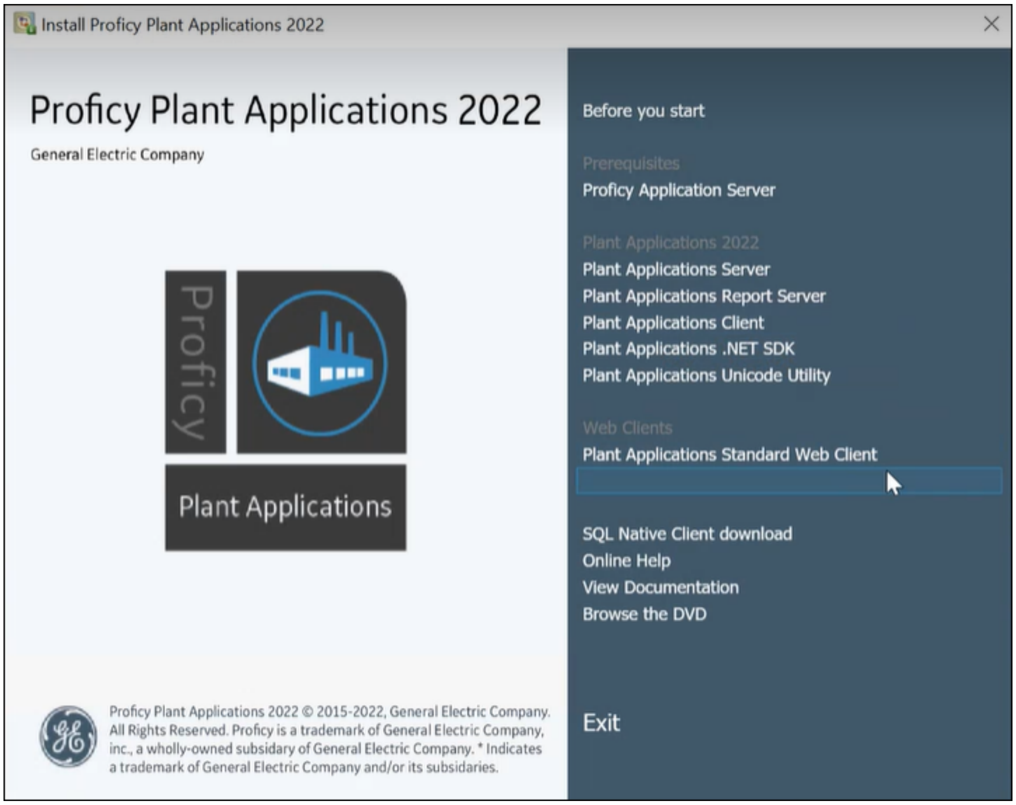
Note:

- Before installing the Standard Edition Web Client, ensure that you first perform the preinstallation tasks *(page 7)*.
- We recommend to use the signed certificates. The self-signed certificate which is provided during the Plant Applications Webclient installation expires on February 8, 2024.

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. Right-click the `installfrontend.exe` file, and then select **Run as an Administrator**.

   The **Install Proficy Plant Applications 2022** page appears and displays the installation menu.

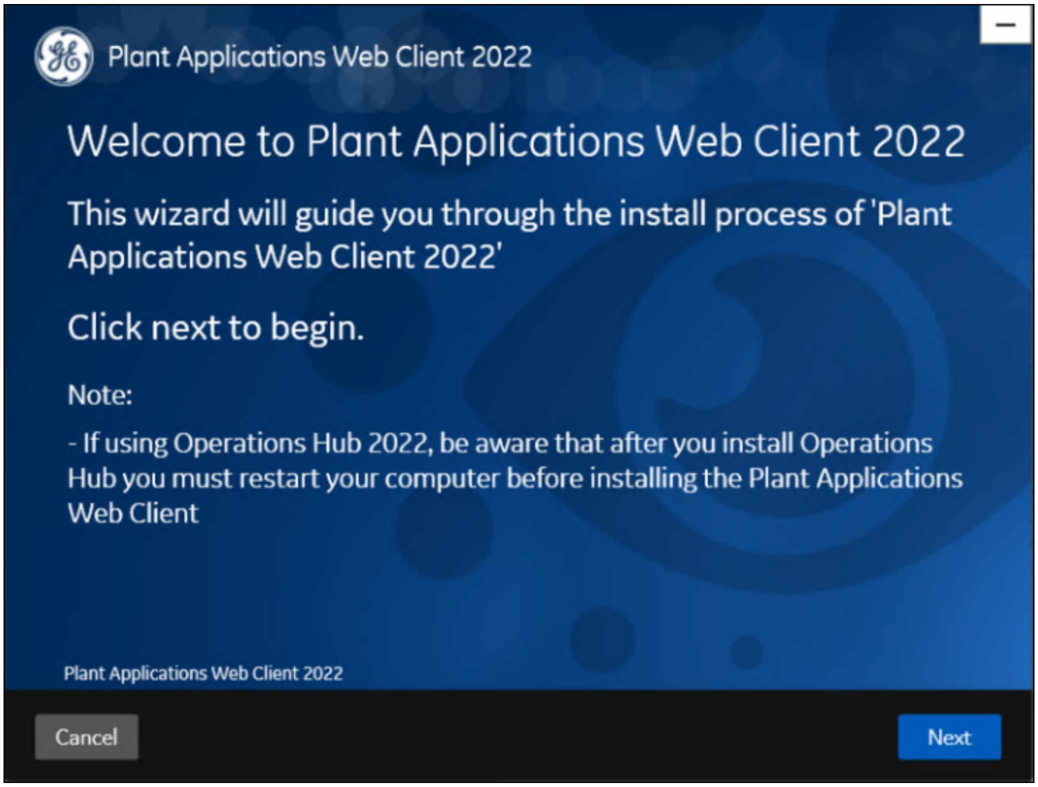

Install Proficy Plant Applications 2022
Proficy Plant Applications 2022
General Electric Company
Proficy
Plant Applications
Before you start
Prerequisites
Proficy Application Server
Plant Applications 2022
Plant Applications Server
Plant Applications Report Server
Plant Applications Client
Plant Applications .NET SDK
Plant Applications Unicode Utility
Web Clients
Plant Applications Standard Web Client
SQL Native Client download
Online Help
View Documentation
Browse the DVD
Exit

Proficy Plant Applications 2022 © 2015-2022, General Electric Company. All Rights Reserved. Proficy is a trademark of General Electric Company, inc., a wholly-owned subsidary of General Electric Company. * Indicates a trademark of General Electric Company and/or its subsidaries.

   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 2022** page.



Plant Applications Web Client 2022

Welcome to Plant Applications Web Client 2022

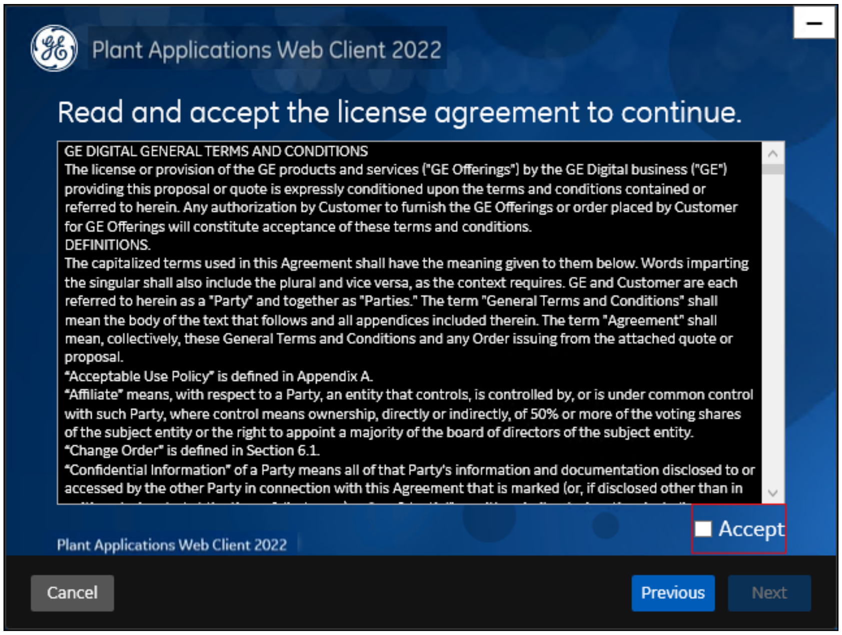
This wizard will guide you through the install process of 'Plant Applications Web Client 2022'

Click next to begin.

Note:

- If using Operations Hub 2022, be aware that after you install Operations Hub you must restart your computer before installing the Plant Applications Web Client

4. In the **Welcome to Plant Applications Web Client 2022** page, select **Next**.
   The **Read and accept the license agreement to continue** page appears.



Plant Applications Web Client 2022

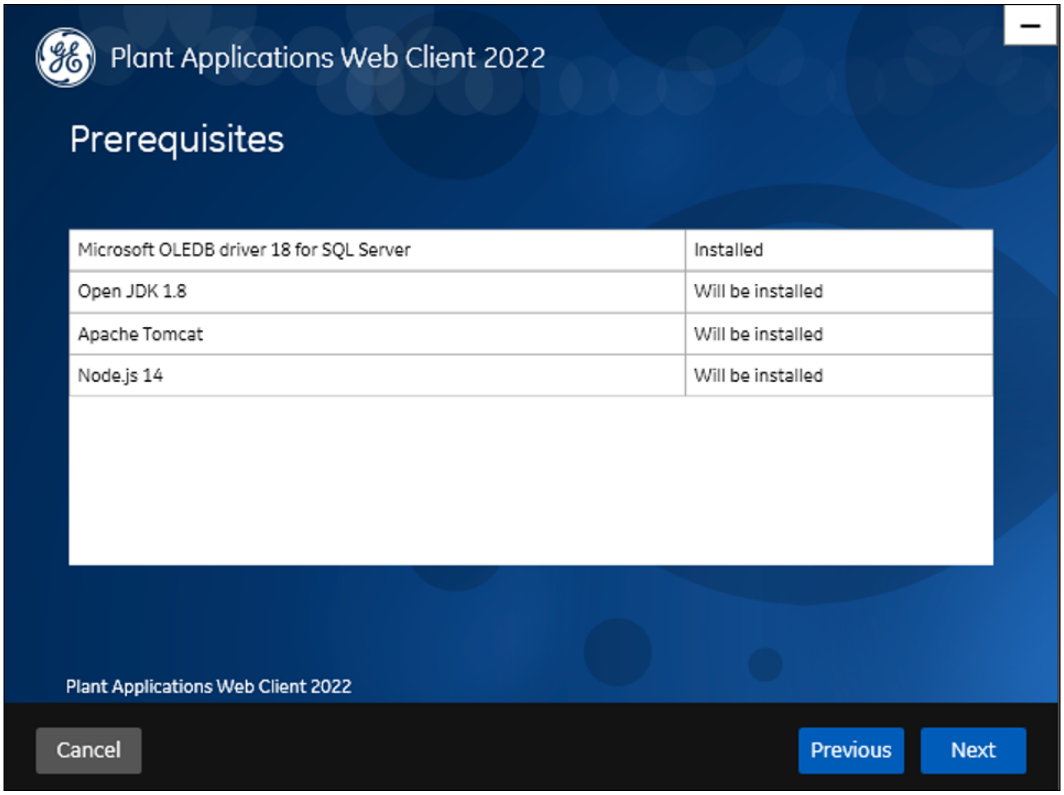
Read and accept the license agreement to continue.

GE DIGITAL GENERAL TERMS AND CONDITIONS
The license or provision of the GE products and services ("GE Offerings") by the GE Digital business ("GE") providing this proposal or quote is expressly conditioned upon the terms and conditions contained or referred to herein. Any authorization by Customer to furnish the GE Offerings or order placed by Customer for GE Offerings will constitute acceptance of these terms and conditions.
DEFINITIONS.
The capitalized terms used in this Agreement shall have the meaning given to them below. Words imparting the singular shall also include the plural and vice versa, as the context requires. GE and Customer are each referred to herein as a "Party" and together as "Parties." The term "General Terms and Conditions" shall mean the body of the text that follows and all appendices included therein. The term "Agreement" shall mean, collectively, these General Terms and Conditions and any Order issuing from the attached quote or proposal.
"Acceptable Use Policy" is defined in Appendix A.
"Affiliate" means, with respect to a Party, an entity that controls, is controlled by, or is under common control with such Party, where control means ownership, directly or indirectly, of 50% or more of the voting shares of the subject entity or the right to appoint a majority of the board of directors of the subject entity.
"Change Order" is defined in Section 6.1.
"Confidential Information" of a Party means all of that Party's information and documentation disclosed to or accessed by the other Party in connection with this Agreement that is marked (or, if disclosed other than in

□ Accept

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

The **Prerequisites** page appears.

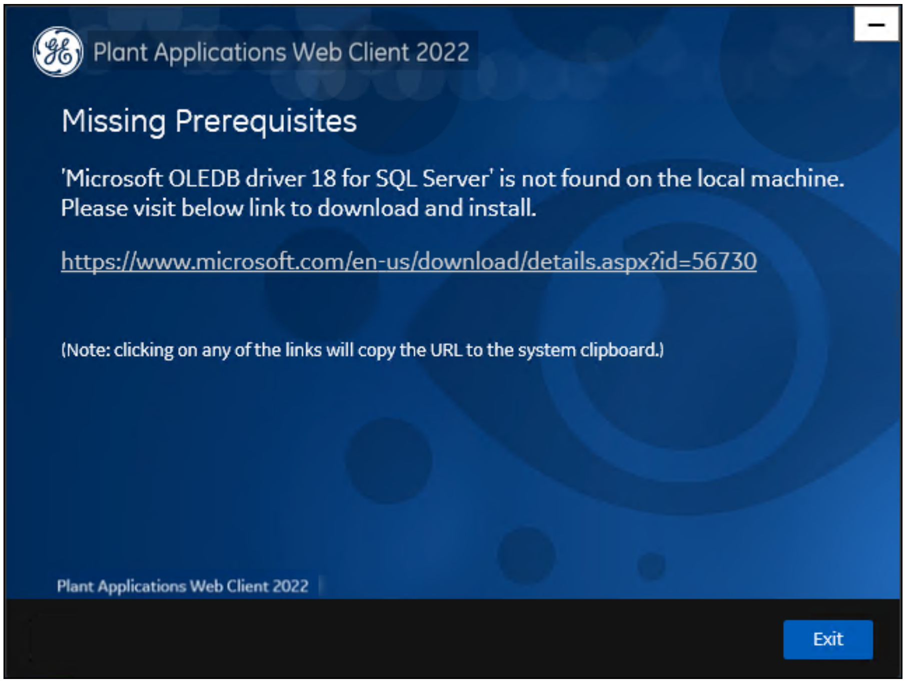

Plant Applications Web Client 2022
Prerequisites

Microsoft OLEDB driver 18 for SQL Server	Installed
Open JDK 1.8	Will be installed
Apache Tomcat	Will be installed
Node.js 14	Will be installed

Plant Applications Web Client 2022
Cancel
Previous
Next

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

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.



Plant Applications Web Client 2022

Missing Prerequisites

'Microsoft OLEDB driver 18 for SQL Server' is not found on the local machine. Please visit below link to download and install.

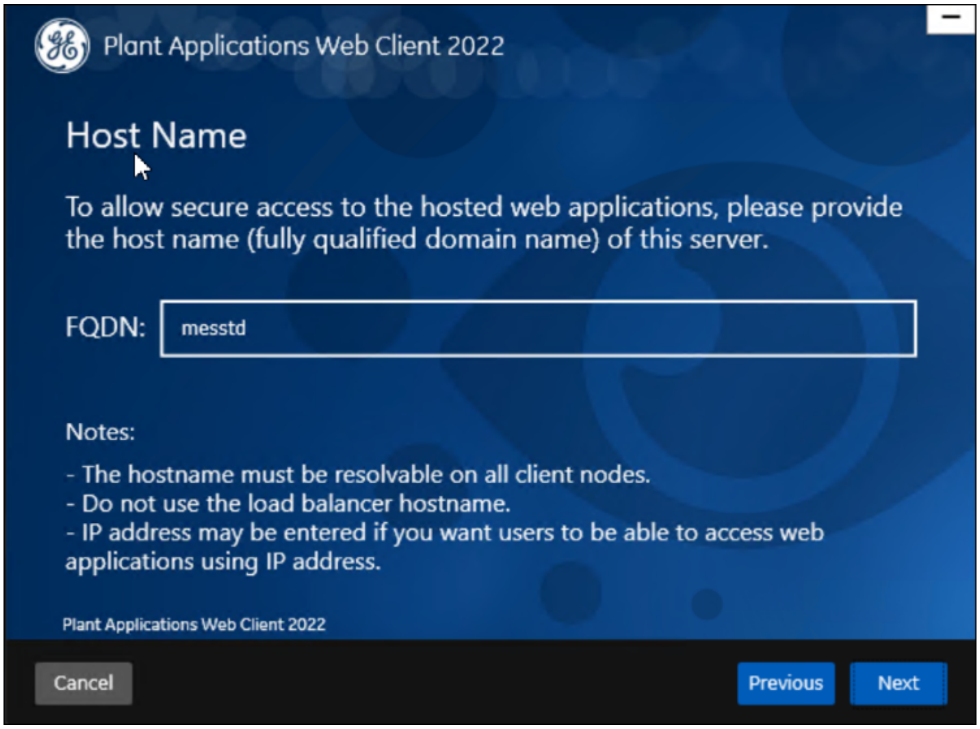
https://www.microsoft.com/en-us/download/details.aspx?id=56730

(Note: clicking on any of the links will copy the URL to the system clipboard.)

Plant Applications Web Client 2022
Exit

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

   The **Host Name** page appears.



Plant Applications Web Client 2022

Host Name

To allow secure access to the hosted web applications, please provide the host name (fully qualified domain name) of this server.

FQDN: messtd

Notes:

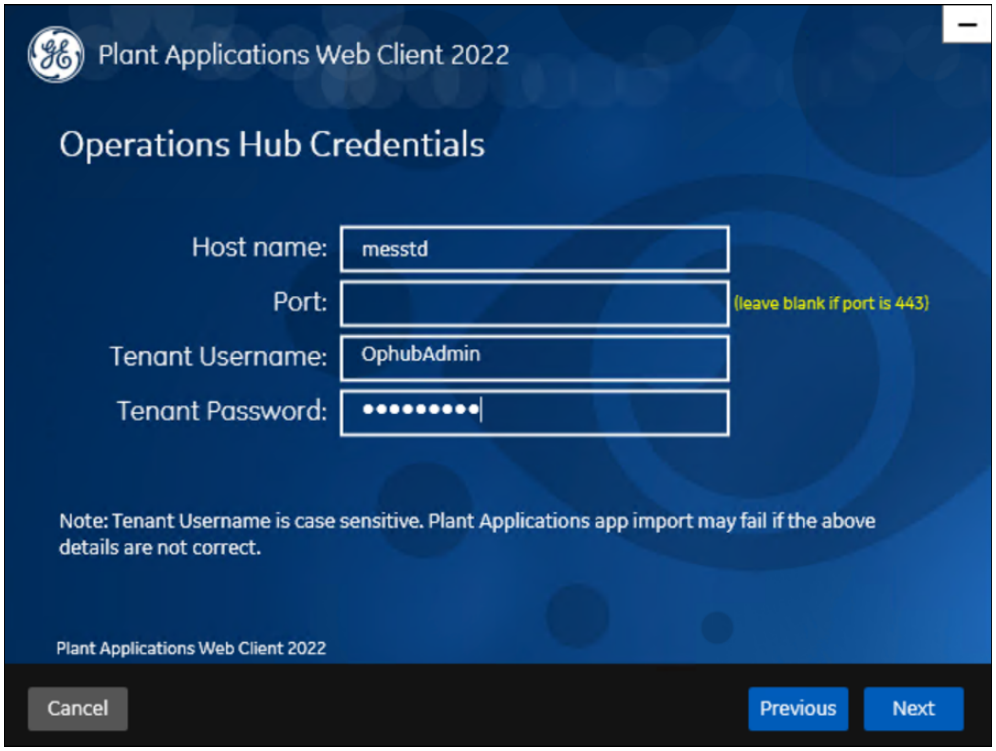
- The hostname must be resolvable on all client nodes.
- Do not use the load balancer hostname.
- IP address may be entered if you want users to be able to access web applications using IP address.

Plant Applications Web Client 2022
Cancel
Previous
Next

7. Enter the fully qualified domain name where you want to install the Plant Applications Web Client, then select **Next**.

   Note: Do not use the Load Balancer URL in the **FQDN** field. If you want to configure the Load Balancer URL, then you must perform it post installation.

   The **Operations Hub Credentials** page appears.



Plant Applications Web Client 2022

Operations Hub Credentials

Host name: messtd

Port: (leave blank if port is 443)

Tenant Username: OphubAdmin

Tenant Password: ••••••••••

Note: Tenant Username is case sensitive. Plant Applications app import may fail if the above details are not correct.

Plant Applications Web Client 2022

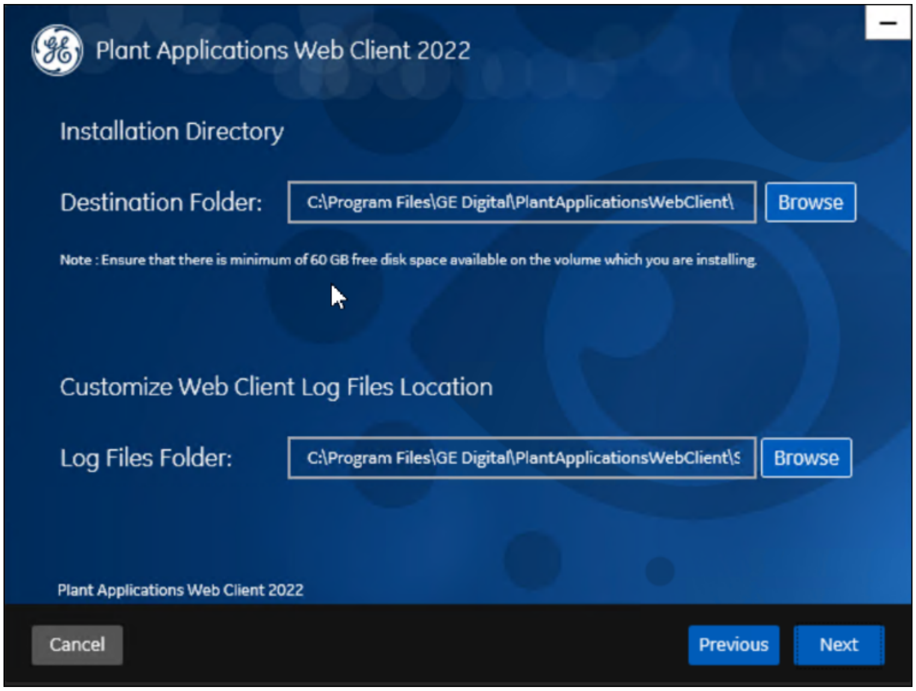
8. In the **Operations Hub Credentials** page, enter the following required credentials to access the Operations Hub server.

Field	Description
Host Name	This field is automatically populated with the local host name, fully qualified host name, or IP address, based on the configuration in Operations Hub. You can edit the host name of the Operations Hub server based on requirement. **Note:** Instead of IP address, we recommend to use the Operations Hub host name (computer name).
Port	Enter the Operations Hub port number, if it is other than 443.
Tenant Username	Enter the tenant username to access the Operations Hub server instance. **Note:** The default user name is `OphubAdmin`.

Field	Description
Tenant Password	Enter the password. **Note:** The tenant username and password must be same as the credentials that you have specified during the Operations Hub installation.

When all the options are entered correctly, the **Next** option is enabled.

The **Installation Directory and Customize Web Client Log Files Location** page appears with the default installation directory selected as `C:\Program Files\GE Digital\PlantApplicationsWebClient`.



Plant Applications Web Client 2022

Installation Directory

Destination Folder: C:\Program Files\GE Digital\PlantApplicationsWebClient\

Note : Ensure that there is minimum of 60 GB free disk space available on the volume which you are installing.

Customize Web Client Log Files Location

Log Files Folder: C:\Program Files\GE Digital\PlantApplicationsWebClient\S

Plant Applications Web Client 2022

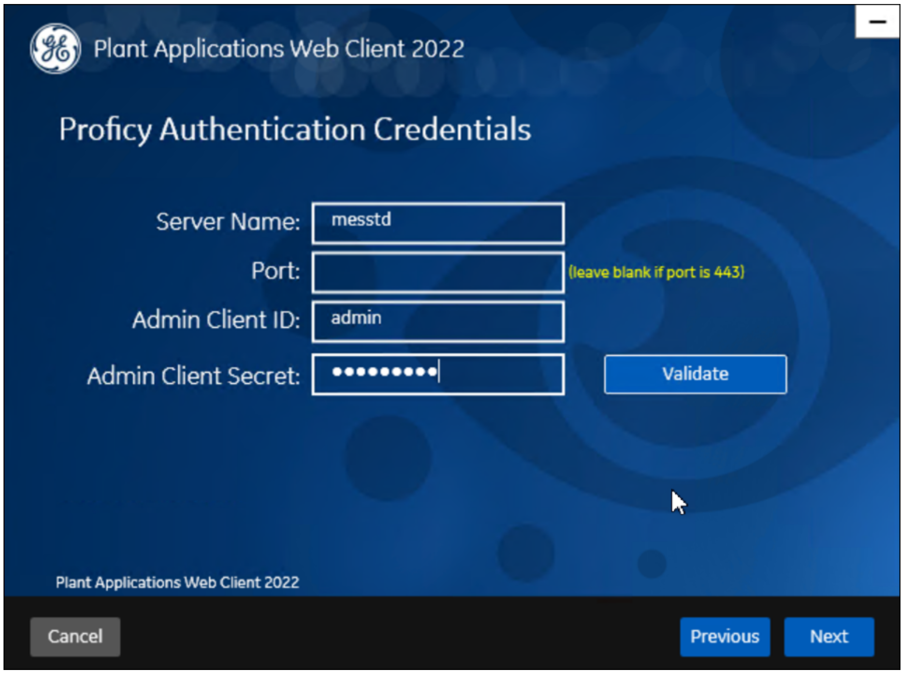
9. Do the following:
   a. In the **Destination Folder** field, select **Browse** to select the directory where you want to install the Plant Applications Web Client.

      Note:
      - Ensure that a minimum of 60 GB free disk space is available on the volume which you are installing.
      - Do not use the user profile folder for installation.

   b. In the **Log Files Folder** field, select **Browse** to select the directory where you want to install the Plant Applications Web Client service logs.

10. Select **Next**.

    The **Proficy Authentication Credentials** page appears.


Plant Applications Web Client 2022
Proficy Authentication Credentials

Server Name: messtd
Port: (leave blank if port is 443)
Admin Client ID: admin
Admin Client Secret: ••••••••••

Validate
Plant Applications Web Client 2022
Cancel
Previous
Next

11. Enter the following credentials to access the Proficy Authentication (UAA) server.

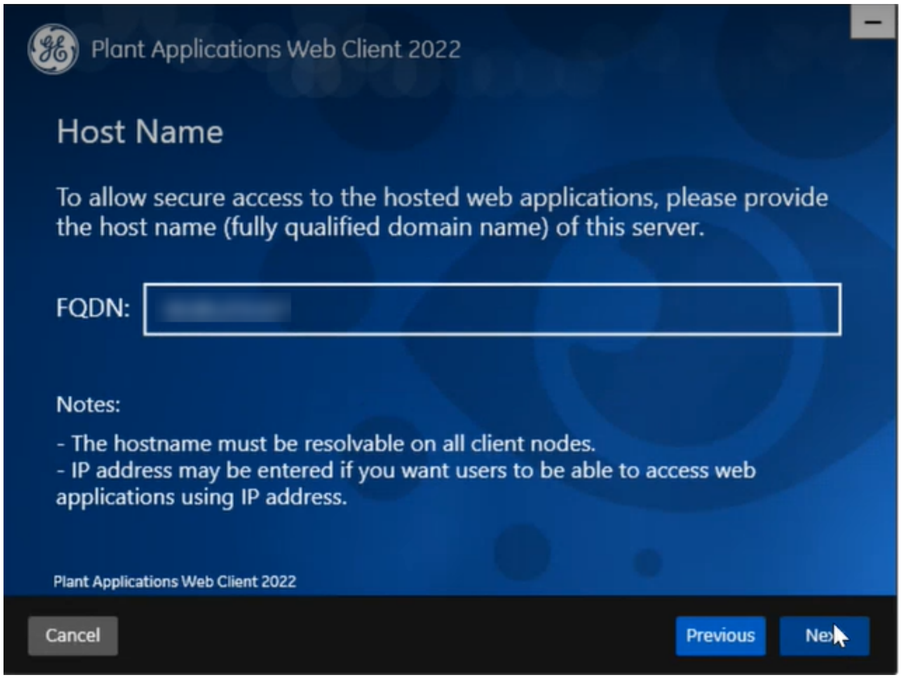
Field	Description
Server Name	Enter the host name of the Proficy Authentication (UAA) server. This is the server name where Operations Hub is installed. When you install Proficy Authentication (UAA) on a different node, then you must provide the Proficy Authentication (UAA) host name. **Note:** Instead of IP address, we recommend to use the Proficy Authentication (UAA) host name (computer name).
Port	Enter the Proficy Authentication (UAA) port number. **Note:** 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 Proficy Authentication (UAA) server instance. **Note:** The default user name is **admin**.
Admin Client Secret	Enter the password.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td><b>Validate</b></td><td>Validate the Proficy Authentication (UAA) server connection.
<b>Note:</b> The following table describes each icon indicating a validation status that might appear during the validation process.
<table>
<tr><th>Icon</th><th>Description</th></tr>
<tr><td>⚙</td><td>Indicates that the validation is in progress.</td></tr>
<tr><td>✓</td><td>Indicates that the validation was successful.</td></tr>
<tr><td>✗</td><td>Indicates that the validation was unsuccessful. In this case, make sure you enter the correct password.</td></tr>
</table>
</td></tr>
</table>

When all the options are entered correctly, the **Next** option is enabled.

12. Select **Next**.

    The **Host Name** page appears.



Plant Applications Web Client 2022

Host Name

To allow secure access to the hosted web applications, please provide the host name (fully qualified domain name) of this server.

FQDN: [redacted]

Notes:

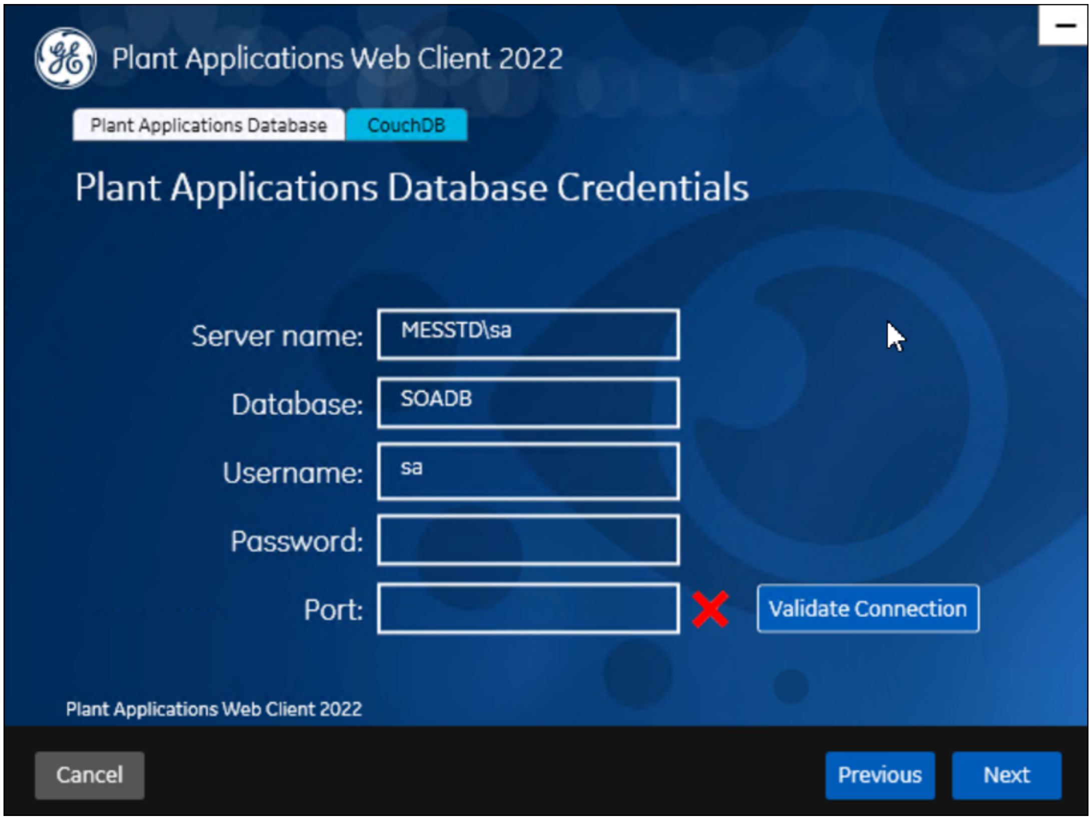
- The hostname must be resolvable on all client nodes.
- IP address may be entered if you want users to be able to access web applications using IP address.

Plant Applications Web Client 2022

13. Enter the fully qualified domain name where you want to install the Plant Applications Web Client, then select **Next**.

    Note: Do not use the Load Balancer url in the **FQDN** field. If you want to configure the Load Balancer url, then you must perform it post installation.

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


Plant Applications Web Client 2022
Plant Applications Database
CouchDB

Plant Applications Database Credentials

Server name: MESSTD\sa

Database: SOADB

Username: sa

Password:

Port:

Validate Connection
Plant Applications Web Client 2022
Cancel
Previous
Next

14. Enter the Plant Applications database credentials.

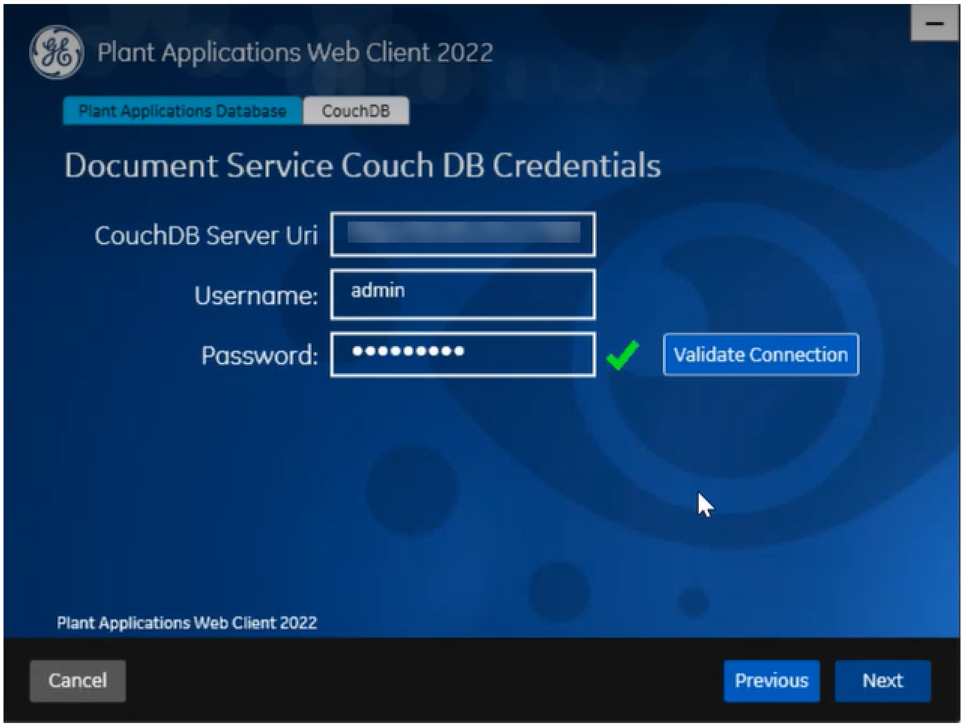
Field	Description
Server name	Enter the server name where the Plant Applications database is installed in the format `HOST_NAME\INSTANCE`. Where `HOST_NAME` is the host name (either a fully qualified domain name or IP address, of the server) and `INSTANCE` is the instance of the server used by the database.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

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

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

16. In the **Plant Applications Database Credentials** page, select the **CouchDB** tab.

    The **Document Service Couch DB Credentials** page appears.



Plant Applications Web Client 2022
Plant Applications Database
CouchDB
Validate Connection
Plant Applications Web Client 2022
Cancel
Previous
Next

Document Service Couch DB Credentials

CouchDB Server Uri [redacted]

Username: admin

Password: ••••••••••

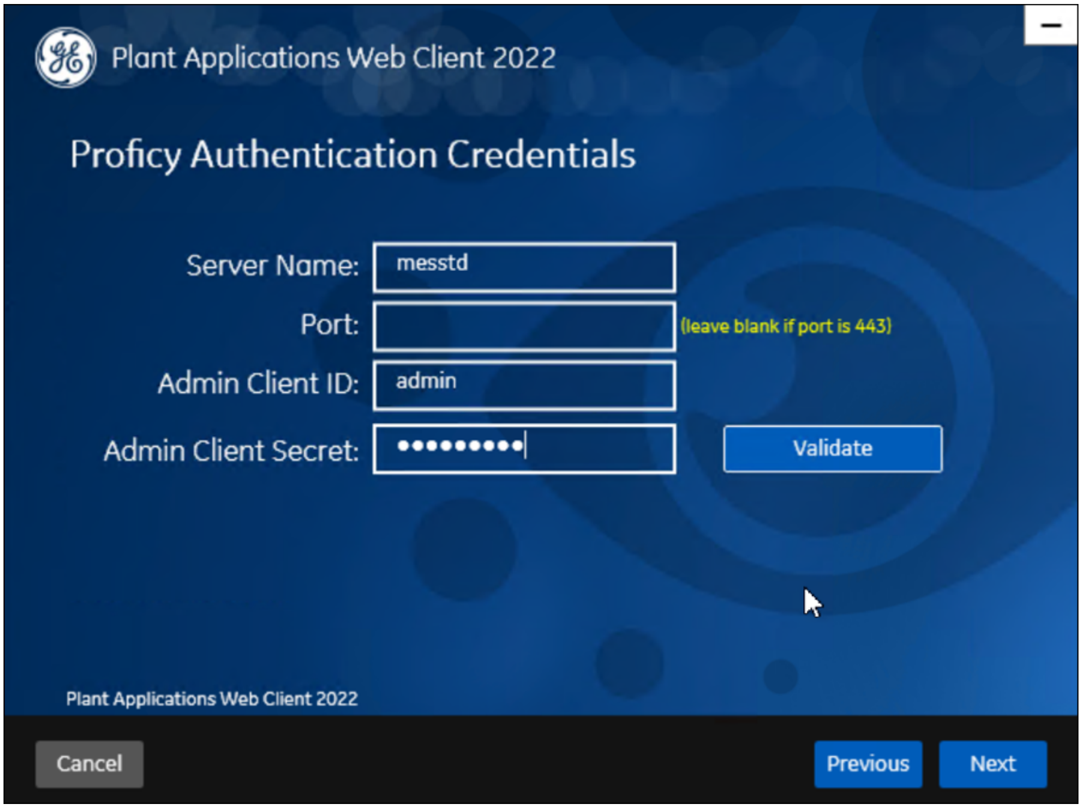
17. Enter the following Couch DB credentials.

Field	Description
CouchDB Server Uri	Enter the fully qualified web address of Apache CouchDB in the format: `https://<host name or IPaddress>:<port number>`. For example, `https://testmachine:6984`.
Username	Enter the CouchDB user name.
Password	Enter the CouchDB password.
Validate Connection	Select the option to validate the Apache CouchDB database credentials.

When the Apache CouchDB database connection is successfully validated, the **Next** option is enabled.

18. Select **Next**.

    The **Proficy Authentication Credentials** page appears.



Plant Applications Web Client 2022

Proficy Authentication Credentials

Server Name: messtd

Port: (leave blank if port is 443)

Admin Client ID: admin

Admin Client Secret: ••••••••••

19. Enter the following credentials to access the Proficy Authentication (UAA) server.

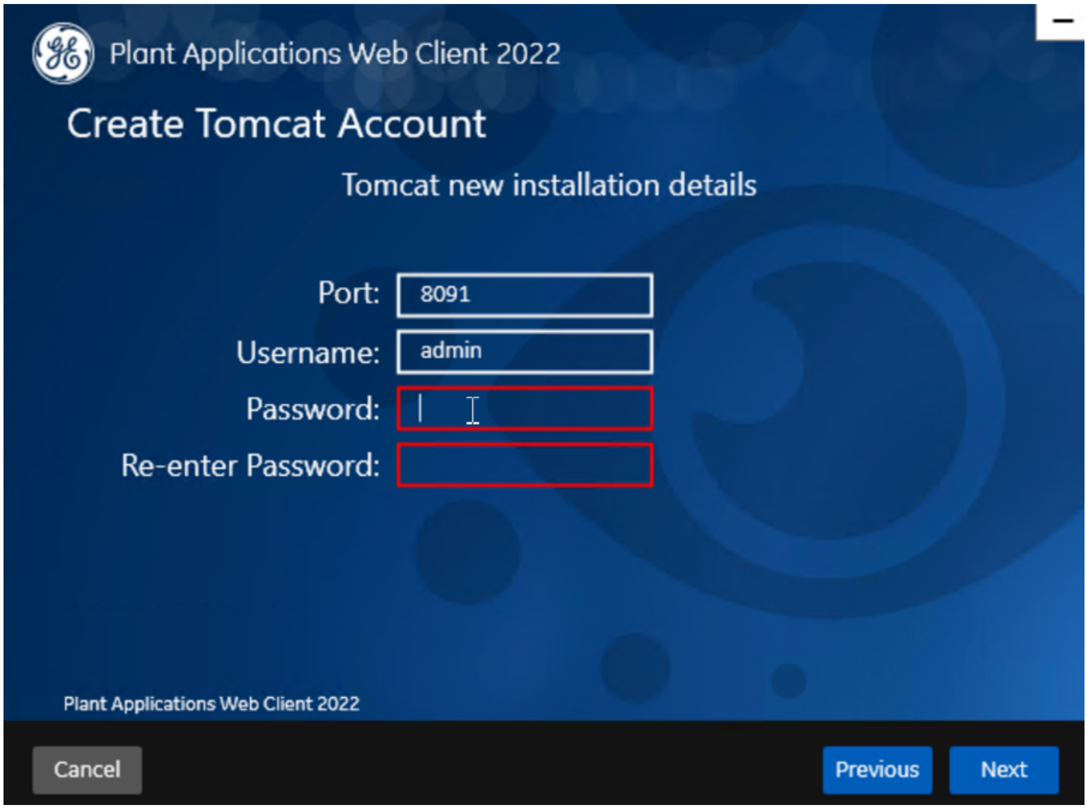
Field	Description
Server Name	Enter the host name of the Proficy Authentication (UAA) server. This is the server name where Operations Hub is installed. When you install Proficy Authentication (UAA) on a different node, then you must provide the Proficy Authentication (UAA) host name. **Note:** Instead of IP address, we recommend to use the Proficy Authentication (UAA) host name (computer name).
Port	Enter the Proficy Authentication (UAA) port number. **Note:** 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 Proficy Authentication (UAA) server instance. **Note:** The default user name is **admin**.
Admin Client Secret	Enter the password.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td><b>Validate</b></td><td>Validate the Proficy Authentication (UAA) server connection.
<b>Note:</b> The following table describes each icon indicating a validation status that might appear during the validation process.
<table>
<tr><th>Icon</th><th>Description</th></tr>
<tr><td>⚙</td><td>Indicates that the validation is in progress.</td></tr>
<tr><td>✓</td><td>Indicates that the validation was successful.</td></tr>
<tr><td>✗</td><td>Indicates that the validation was unsuccessful. In this case, make sure you enter the correct password.</td></tr>
</table>
</td></tr>
</table>

When all the options are entered correctly, the **Next** option is enabled.

20. Select **Next**.

    The **Create Tomcat Account** page appears.



Plant Applications Web Client 2022
Create Tomcat Account
Tomcat new installation details

Port: 8091

Username: admin

Password:

Re-enter Password:

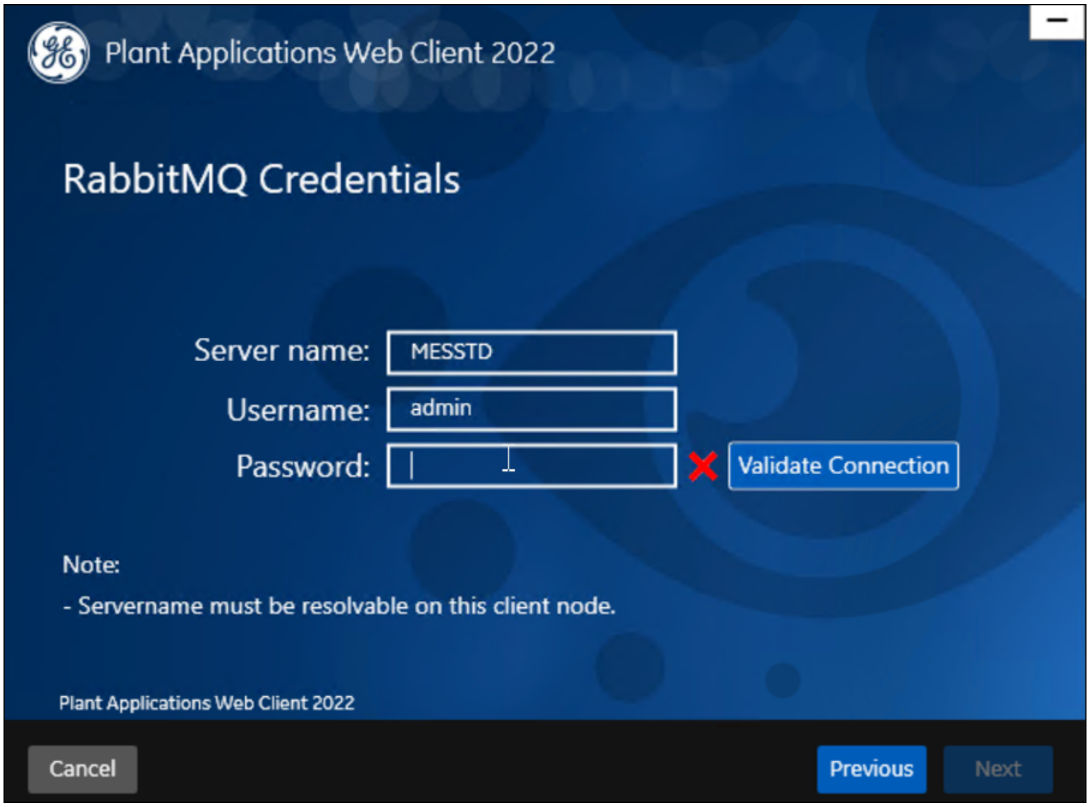
Plant Applications Web Client 2022
Cancel
Previous
Next

21. In the **Create Tomcat Account** page, enter the Tomcat installation details for a new or existing installation. 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.

Field	Description
Port	Enter the HTTP port that Tomcat uses to listen for client connections. **Note:** The default port is 8090 and when upgrading the Plant Applications Web Client, the default port is 8091.
Username	Enter the user name to access Tomcat. **Note:** The default user name is **admin**.
Password	Enter the password.
Re-enter Password	Reenter the password to confirm the value you entered in the **Password** field. **Note:** This field appears only when a new installation of Tomcat is initiated by the installer.

22. Select **Next**.

    The **RabbitMQ Credentials** page appears.


Plant Applications Web Client 2022
Validate Connection
Plant Applications Web Client 2022
Cancel
Previous
Next

RabbitMQ Credentials

Server name: MESSTD

Username: admin

Password:

Note:

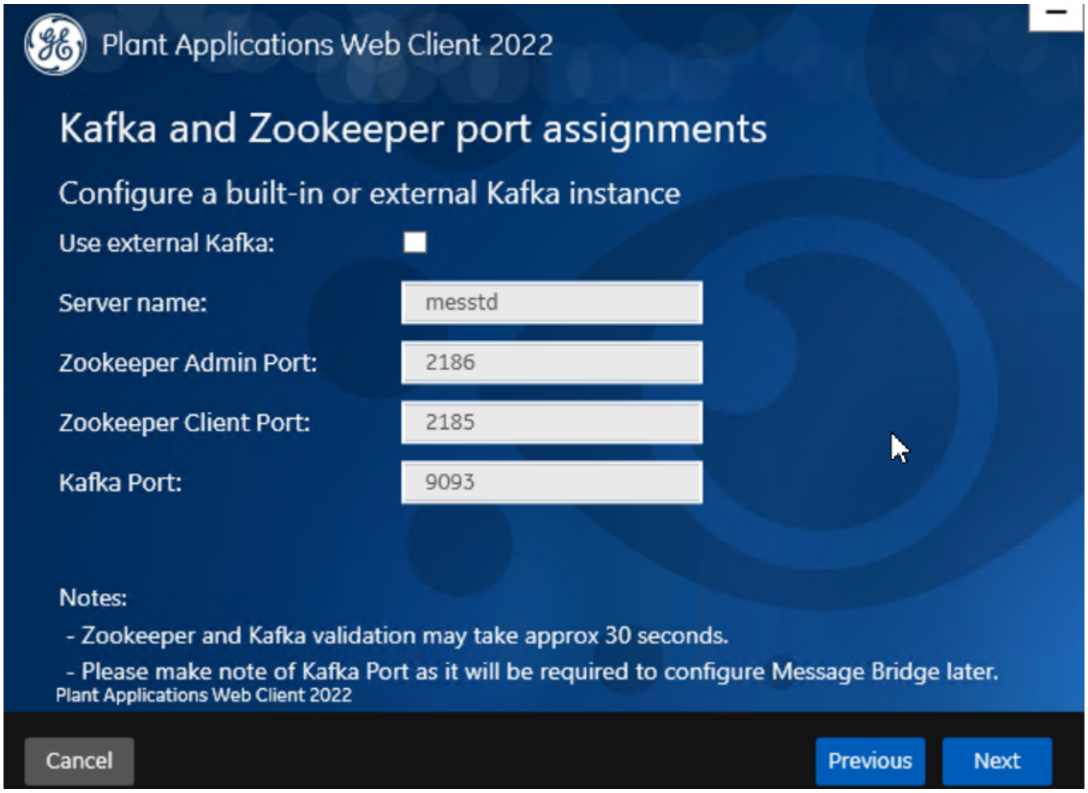
- Servername must be resolvable on this client node.

23. RabbitMQ is installed by default as part of the Plant Application Server. Enter the RabbitMQ login details to proceed with the installation, and then select **Validate Connection**.

Field	Description
Server name	Enter the computer name or IP address that hosts the Plant Applications server.
Username	Enter the Administrator's user name that you set during Plant Applications server installation. The default username is **admin**.
Password	Enter the password.

24. Select **Next**.

    The **Kafka and Zookeeper port assignments** page appears. Make a note of the kafka port number that is listed for configuring Message Bridge after the Web Client installation.



Plant Applications Web Client 2022

Kafka and Zookeeper port assignments

Configure a built-in or external Kafka instance

Use external Kafka: □

Server name: messtd

Zookeeper Admin Port: 2186

Zookeeper Client Port: 2185

Kafka Port: 9093

Notes:

- Zookeeper and Kafka validation may take approx 30 seconds.
- Please make note of Kafka Port as it will be required to configure Message Bridge later.

Plant Applications Web Client 2022

25. Select **Next**.

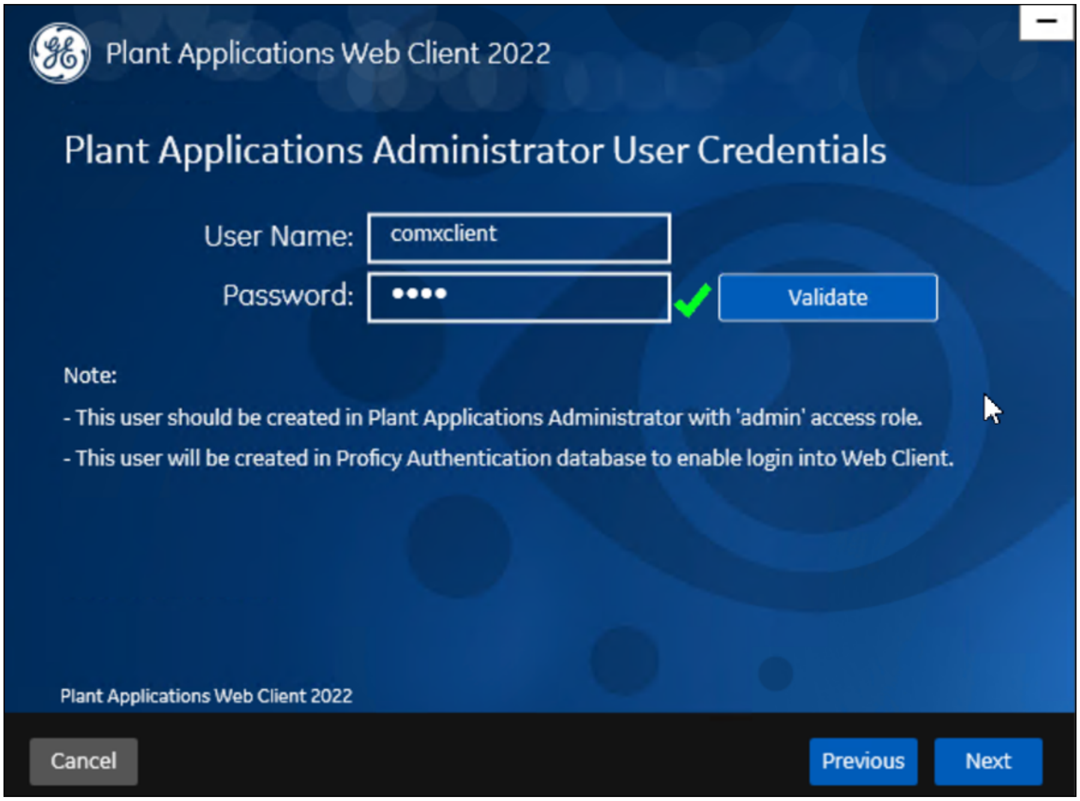
26. Enter the following credentials to access the Kafka server.

Field	Description
Use external Kafka	Select this check box if you want to configure an external Kafka instance.

Field	Description
Server Name	Enter the host name of the Kafka server. By default, it is the Plant Applications Web Client server name.
Zookeeper Admin Port	Accept the default port number. To change the default port number, enter a new Zookeeper Admin port number. By default, Kafka and Zookeeper will be installed along with Plant Applications Web Client. If you are not using any external Kafka server, then you can use Plant Applications Web Client server name.
Zookeeper Client Port	Accept the default port number. To change the default port number, enter a new Zookeeper Client port number. **Note:** Ensure that you have entered a valid Zookeeper port number. If you have entered an invalid port number, refer to **Changing the Zookeeper Port Number** section in *Getting Started Guide*.
Kafka Port	Accept the default port number. The default port number is 9093. To change the default port number, enter a new Kafka port number.

When all the options are entered correctly, the **Next** option is enabled.

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


Plant Applications Web Client 2022

Plant Applications Administrator User Credentials

User Name: comxclient

Password: ••••

Note:

- This user should be created in Plant Applications Administrator with 'admin' access role.
- This user will be created in Proficy Authentication database to enable login into Web Client.

Plant Applications Web Client 2022
Cancel
Previous
Next

27. Enter the following Plant Applications administrator credentials.

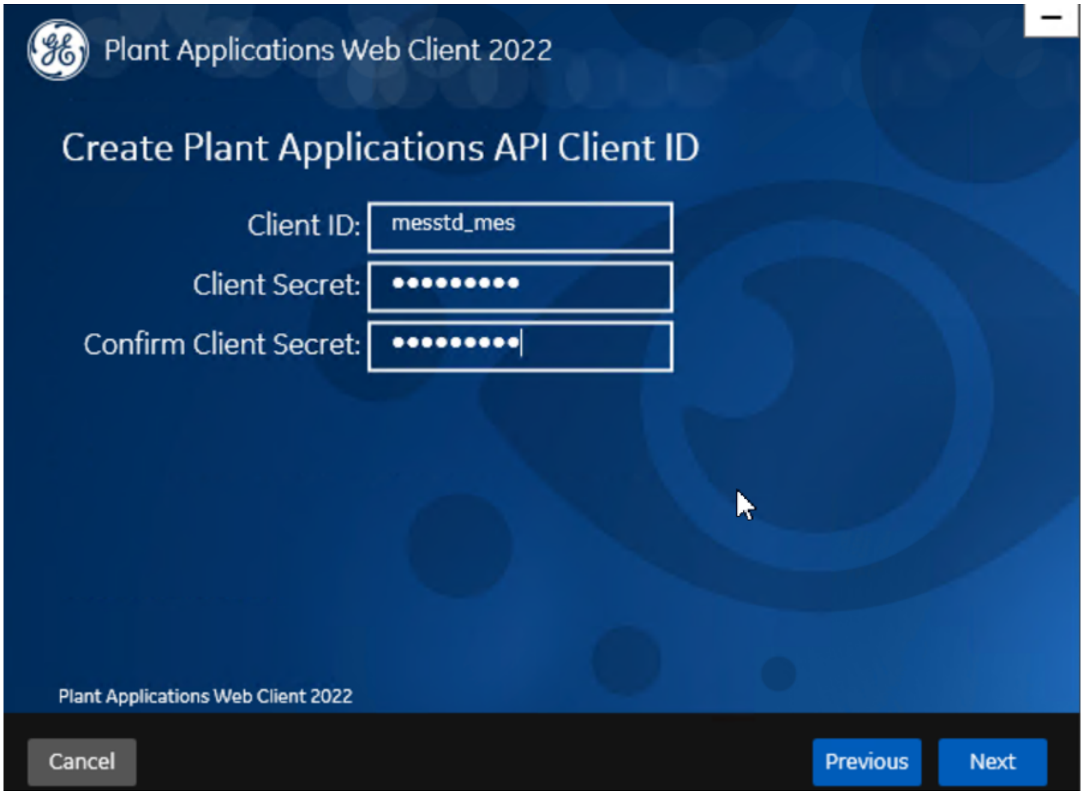
Note: Ensure that the user credentials entered here must exist in Plant Applications Server with an administrator role defined and you must use the same credentials to login into the Web Client applications.

Field	Description
User Name	Enter the user name for an administrator account in Plant Applications.
Password	Enter the password.

28. Select **Validate** to validate the Plant Applications administrator credentials.
When the Plant Applications administrator connection is successfully validated, the **Next** option is enabled.

29. Select **Next**.

The **Create Plant Applications API Client ID** page appears. The Client ID and Client Secret is useful for accessing the Plant Applications APIs/Swagger URLs.



Plant Applications Web Client 2022

Create Plant Applications API Client ID

Client ID: messtd_mes

Client Secret: ••••••••••

Confirm Client Secret: ••••••••••

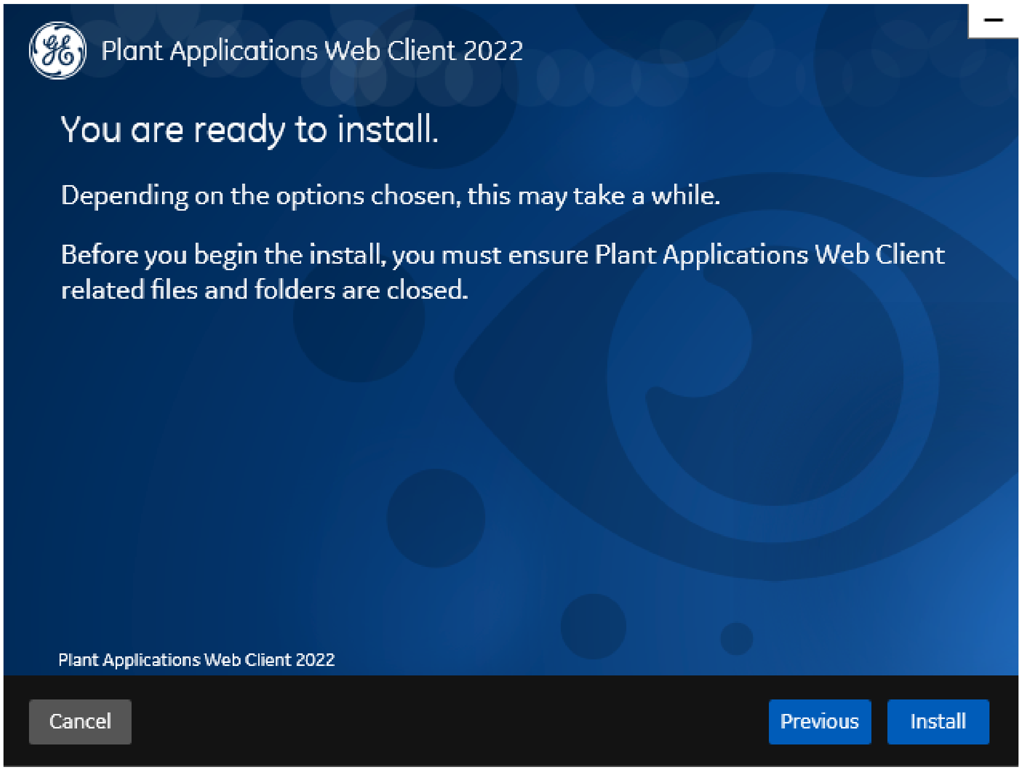
30. Enter the required information in the following fields.

Field	Description
Client ID	Enter the username. The default username is hostname_mes, you can enter the user name of your choice.

Field	Description
Client Secret	Enter the password.
Confirm Client Secret	Enter the password to confirm the value in the **Confirm Client Secret** field.

31. Select **Next**.

    The **You are ready to install** screen appears.



Plant Applications Web Client 2022

You are ready to install.

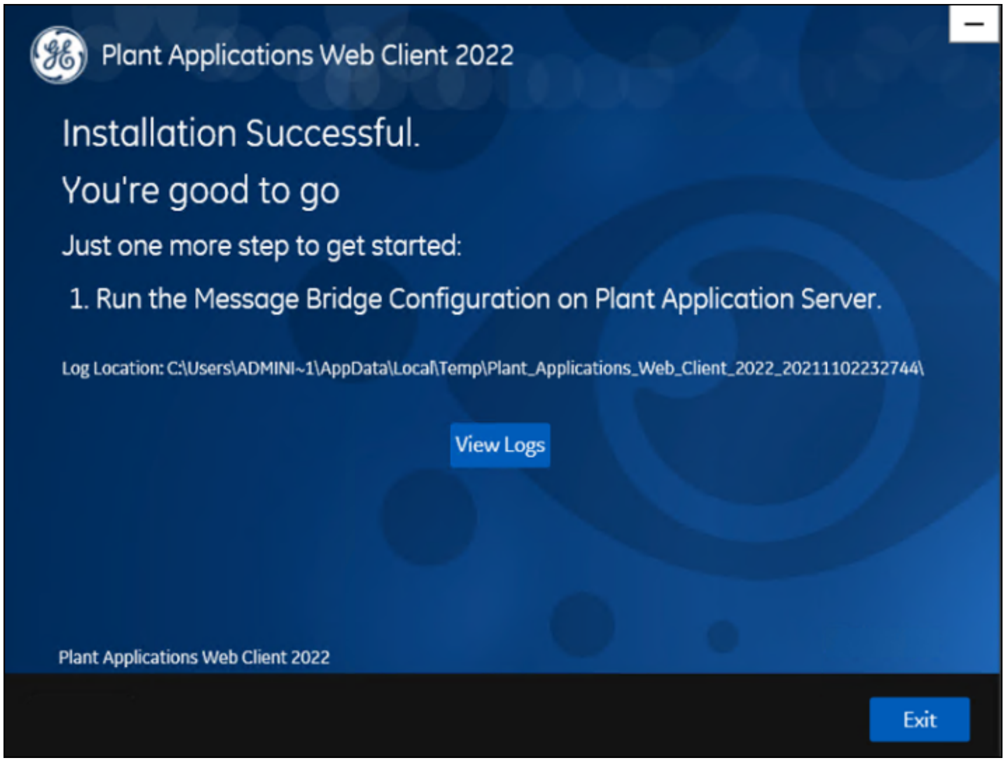
Depending on the options chosen, this may take a while.

Before you begin the install, you must ensure Plant Applications Web Client related files and folders are closed.

Plant Applications Web Client 2022

32. Select **Install**, and then wait for the installation to complete.

    The installation process might take around 20 minutes. On successful installation, the **Installation Successful** page appears.



Plant Applications Web Client 2022

Installation Successful.

You're good to go

Just one more step to get started:

1. Run the Message Bridge Configuration on Plant Application Server.

Log Location: C:\Users\ADMINI~1\AppData\Local\Temp\Plant_Applications_Web_Client_2022_20211102232744\

Note: Before you log into the Plant Applications Web Client, ensure to complete the configuration of the Message Bridge Utility.

33. **Optional:** Select **View Logs** to see the installation details.
34. In the **Installation Successful** page, select **Exit** to close the wizard.
    The Plant Applications Web Client is successfully installed on your computer.

    After the installation is complete, Run the Message Bridge Configuration Utility *(page 90)*. This is a mandatory step that you must complete before using the Plant Applications Web Client.

    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.

35. When you have completed running Message Bridge Configuration, Verify the Installation *(page 95)* if the Plant Applications Web Client applications are up and running.
36. Access the Plant Applications REST APIs *(page 95)* to access the REST APIs for Plant Applications Web Client.

37. When installation is successful but posting apps into Operations Hub fail, then you must post the apps using utility. See Post Applications into Operations Hub Manually *(page 128)*.

38. After the installation is complete, if you want to find the port details or swagger URL information, refer the `WebClient-Ports.txt` located in `C:\Program Files\GE Digital\PlantApplicationsWebClient\WebClient-Ports.txt`.

    Note: When you complete the installation of Web Client, you must configure the SQL "Always On" server setup. For more information, see Configure Web Client to Support SQL "AlwaysOn" Setup *(page 46)*.

Perform the post-installation steps *(page 41)*.

Install Plant Applications Standard Web Client in Silent Mode

Note: Before installing the Plant Applications Standard Edition Web Client, ensure that you first perform the preinstallation tasks *(page 7)*.

The silent installation consists of configuring settings in a configuration file. Use the configuration file `configuration.ini` to configure same settings that you configure during interactive installation.

1. Mount the ISO, and then navigate to the `E:\Install\WebClient` directory, and then open the `configuration.ini` file using any text editor, for example, Notepad or Notepad++.

    Note:

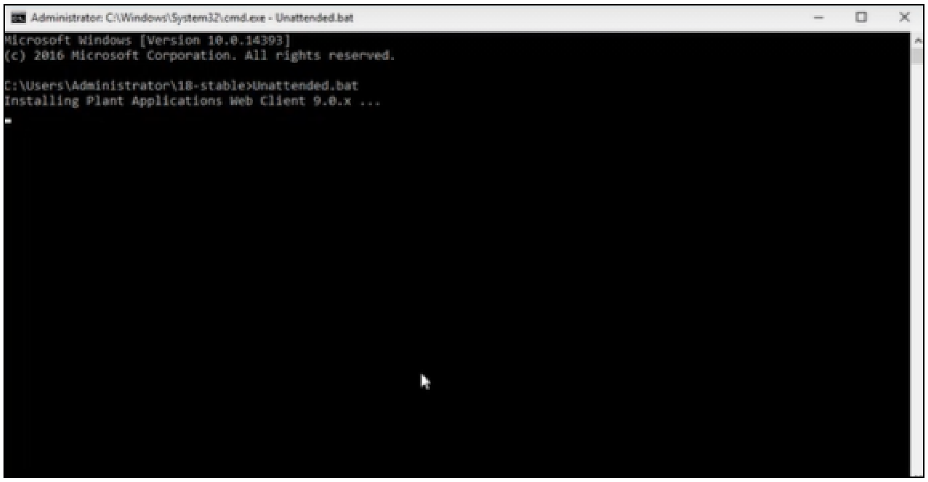
    To edit the configuration file `configuration.ini`, copy the `.ini` file to a location on your machine. For example, `C:\New folder`.

2. In the configuration file, enter details for the following:
    - Operations Hub credentials
    - Fully Qualified Domain Name (FQDN)
    - Installation Directory
    - Proficy Authentication (UAA) credentials
    - Plant Applications Web Client API Login details
    - Plant Applications Database credentials
    - Plant Applications CouchDB credentials
    - Plant Applications Administrator User credentials
    - Tomcat credentials
    - Log file location

- RabbitMQ credentials
- Kafka and Zookeeper credentials

3. Save the `configuration.ini` file.

4. Open the command prompt in the administrator mode, and then navigate to the path `E:\Install\WebClient` where the `Unattended.bat` file resides. The `E:\` is the drive where the ISO has been mounted. Then run this command: `Unattended.bat “<absolute path of configuration.ini file>”`.

   Administrator: C:\Windows\System32\cmd.exe - Unattended.bat

   ```
   Microsoft Windows [Version 10.0.14393]
   (c) 2016 Microsoft Corporation. All rights reserved.

   C:\Users\Administrator\18-stable>Unattended.bat
   Installing Plant Applications Web Client 9.0.x ...
   ```

   The Plant Applications Standard Web Client installation starts. A progress bar appears and displays the installation progress.

   Note: The installation takes about 20 minutes to complete and might take longer based on system resources.

   Note: Before you log into the Plant Applications Web Client, ensure to complete the configuration of the Message Bridge Utility.

5. To see the installation details, you can access the log file here: `C:\ProgramData\Proficy\Logs\webclientinstaller\`. To see the application details, you can access the log file here: `C:\Program Files\GE Digital\PlantApplicationsWebClient\ServiceLogs`.
   When the installation is complete, Run the Message Bridge Configuration Utility *(page 90)*. This is mandatory step to be completed before using the Web Client.

   Note: If the installation fails, then the system displays an error code: `Failure.exit code is 3010`. Check the log file to view the error and the description for the problem.

6. When you have completed running Message Bridge Configuration, Verify the Installation *(page 95)* if the Plant Applications Web Client applications are up and running.

7. Access the Plant Applications REST APIs *(page 95)* to access the REST APIs for Plant Applications Web Client.

8. When installation is successful but posting applications into Operations Hub fail, then you must post the applications using utility. See Post Applications into Operations Hub Manually *(page 128)*.

9. After the installation is complete, if you want to find the port details or swagger URL information, refer the `WebClient-Ports.txt` located in `C:\Program Files\GE Digital\PlantApplicationsWebClient\WebClient-Ports.txt`.

Perform the post-installation steps *(page 41)*.

About Post-Installation Tasks

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

- Configure a Proficy Historian for the Analysis application *(page 99)*.
- Configure the cache settings for the Historian tags used in the Analysis application *(page 100)*.

Disable Discrete Applications

When you install Plant Applications Standard Edition 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
   - Work Queue
   - 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 Standard Edition 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

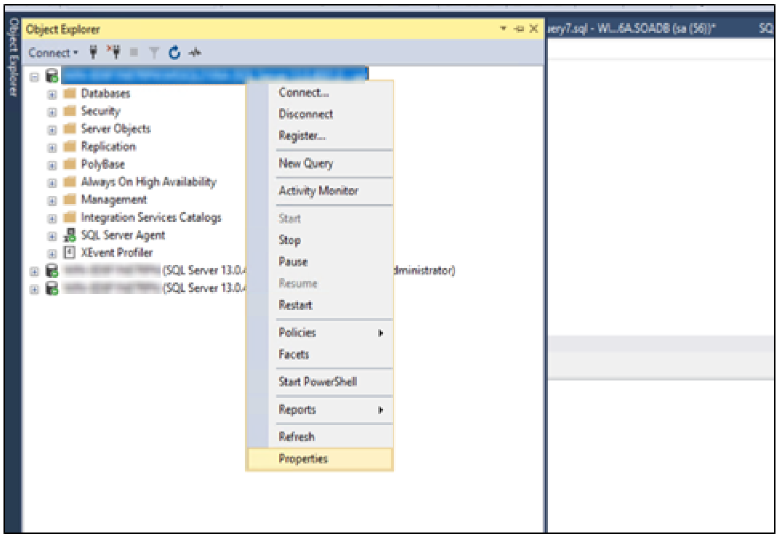
These are the recommended performance tuning settings for your environment to achieve optimal performance.

Update database settings:

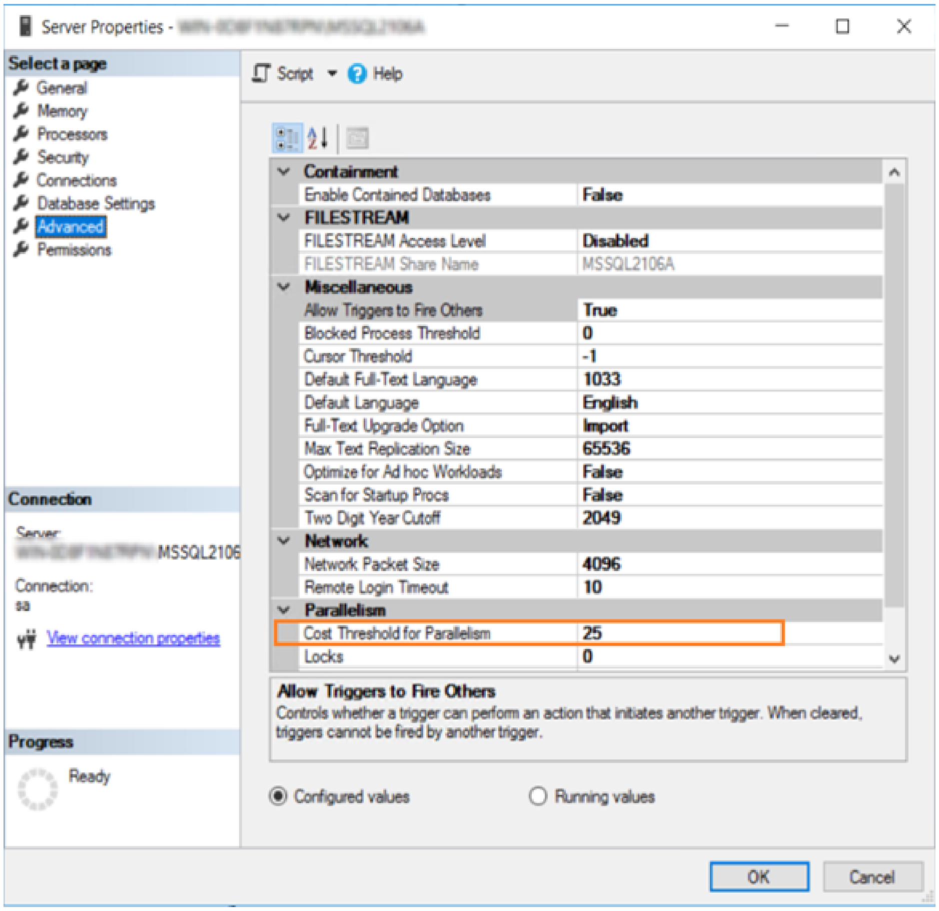
a. Update the **Cost Threshold for Parallelism** value:

   i. Open SSMS connect to the instance, where SOA db is deployed.

   ii. Select the instance, and then right-click, 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.



Server Properties - [redacted]

Containment	
Enable Contained Databases	False
FILESTREAM	
FILESTREAM Access Level	Disabled
FILESTREAM Share Name	MSSQL2106A
Miscellaneous	
Allow Triggers to Fire Others	True
Blocked Process Threshold	0
Cursor Threshold	-1
Default Full-Text Language	1033
Default Language	English
Full-Text Upgrade Option	Import
Max Text Replication Size	65536
Optimize for Ad hoc Workloads	False
Scan for Startup Procs	False
Two Digit Year Cutoff	2049
Network	
Network Packet Size	4096
Remote Login Timeout	10
Parallelism	
Cost Threshold for Parallelism	25
Locks	0

Allow Triggers to Fire Others
Controls whether a trigger can perform an action that initiates another trigger. When cleared, triggers cannot be fired by another trigger.

Connection
Server:
[redacted]MSSQL2106
Connection:
sa

● Configured values ○ Running values

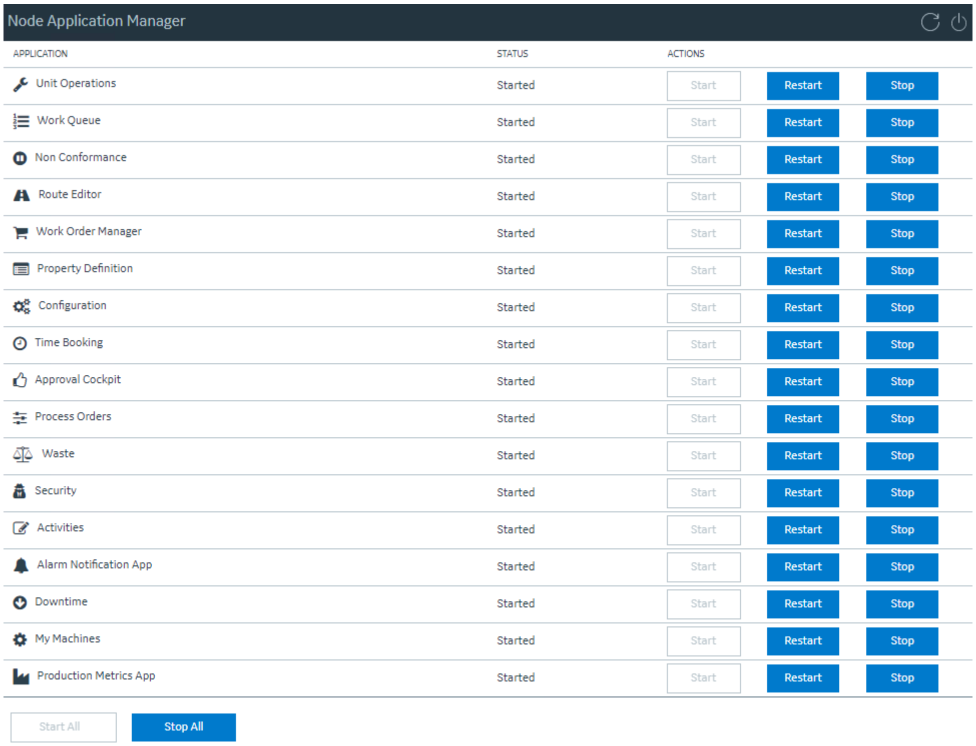
b. Ensure that statistics (sp_updatestats) is updated in the database.

c. We recommend 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.

1. Launch this utility by entering the following URL: `http://<webclient hostname>:<TomcatPortNo>/node-manager-app` in the browser from any computer that has access to the Plant Applications.
2. Enter the credentials that has the **manager-ui** role of Tomcat assigned to log in. The Node Application Manager appears and displays the health of the individual applications in a dashboard.



Node Application Manager

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

- You can either **Start**, **Stop**, or **Restart** an individual application by selecting corresponding options . You can also use **Start All** or **Stop All** either to start or stop all applications respectively.
- You can select the **Refresh** icon (⟳) to reload the dashboard or refresh the browser.
- You can select ⏻ to logout from Node Application Manager.

Configure Web Client to Support SQL "AlwaysOn" Setup

Be sure to follow the steps below to enable SQL "**AlwaysOn**" support. Even if not setup across multiple subnets, you still should configure the SQL **Always On** option. With this setup, the **MultiSubnetFailover** parameter should always be set to `Yes`. If the DNS returns multiple names, without this option configured, you might run into issues.

1. Navigate to the installation directory, and then go to the `Configuration` folder:`<installation-path>/plantapps-web-docker/mnt/configfiles/work-order-service/prod/2.2.2/`.
2. Update this file `work-order-service-prod.properties` for the following:
   ```
   ConnectionStrings.PlantAppsConnection=Server=
   ${plant.apps.db.dotnet.server};Database=${plant.apps.db.name};User Id=
   ${plant.apps.db.username};Password=
   ${plant.apps.db.username.password};connect timeout=100
   ```

```
ConnectionStrings.WorkOrderConnection=Server=
${plant.apps.db.dotnet.server};Database=${plant.apps.db.name};User Id=
${plant.apps.db.username};Password=
${plant.apps.db.username.password};connect timeout=100
```

3. Replace with the following:

```
ConnectionStrings.PlantAppsConnection=Server=
${plant.apps.db.dotnet.server};Database=${plant.apps.db.name};User Id=
${plant.apps.db.username};Password=
${plant.apps.db.username.password};connect
timeout=100;MultiSubnetFailover=Yes
ConnectionStrings.WorkOrderConnection=Server=
${plant.apps.db.dotnet.server};Database=${plant.apps.db.name};User Id=
${plant.apps.db.username};Password=
${plant.apps.db.username.password};connect
timeout=100;MultiSubnetFailover=Yes
```

4. Enter the following commands to Restart Work order services:

```
sudo docker service scale PAworkorder_workorder=0
sudo docker service scale PAworkorder_workorder=1
```

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 the Plant Applications 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

1. To log into the Tomcat Manager, type `http://<webclient hostname>:8090/manager/html` in a compatible web browser.

   Note: If Tomcat Manager does not run on port 8090, then to find the port details, refer the `WebClient-Ports.txt` located in `C:\Program Files\GE Digital\PlantApplicationsWebClient\WebClient-Ports.txt`.

2. Enter the username and password.

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

Serial No	Service Name
1	usersettingsservice
2	mes
3	productservice
4	securityservice
5	accesscontrolservice
6	propertydefinitionservice
7	assignmentservice
8	laborservice
9	externalconfigservice
10	commentservice
11	esignatureservice
12	alarm-service
13	reasonservice
14	activitiesservice
15	processorderservice
16	timebookingservice
17	downtimeservice
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

Serial No	Service Name
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	productionschedulerappservice
48	rmsappservice
49	securityadministratorappservice
50	supervisorappservice
51	wastemanagementappservice
52	bommanagementappservice
53	receivinginspectionappservice
54	receivinginspectionservice
55	spcappservice
56	webgenealogyappservice
57	approvalcockpitservice
58	wastemanagementservice

Resolve Apache CouchDb Certificate Error

When the Couchdb certificate is changed or renewed, then document-management-service reports PKIX path error. To resolve the certificate error, you must re-import the certificate to tomcat jre keystore.

1. Note the location of the working `couchdb public certificate (.crt)` file.
2. Navigate to the Web Client installation folder. The default installation path is `C:\Program Files\GE Digital\PlantApplicationsWebClient`.
3. Access this file using an editor such as Notepad++ `webclient install path>\ConfigurationFiles\import_cert_couchDB.ps1`.
4. Replace `C:\Program Files\GE Digital\PlantApplicationsWebClient\CouchdbExportedCertificate-1.crt` with path of new `couchdb crt` file, and then save it.
5. Open the command prompt in an administrator's mode, and then navigate to the folder: `webclient install path>\ConfigurationFiles`.
6. Run the below command:

   ```
   import_cert.bat import_cert_couchDB.ps1
   ```

Chapter 5. Upgrade Plant Applications Standard Web Client

Upgrade the Plant Applications Standard Edition 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.
- Ensure that you configure the database credentials in the Configure Database Utility when the SQL password is updated before upgrading to Plant Applications 2022.

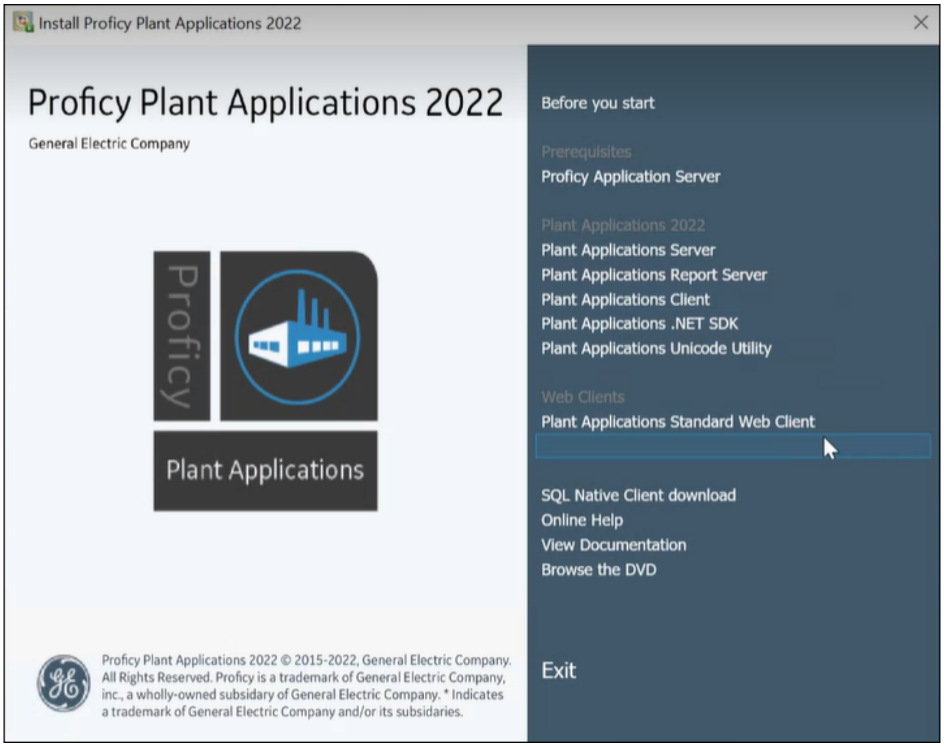
After you upgrade, you can copy-paste the file to the same location to replicate the user-specific settings. For more information, refer to the Plant Applications Web Client Help.

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

Note: The Plant Applications 2022 installer is the base installer for all upgrade requirements.

Note: During upgrade, the installer replaces the existing certificates with the new self-signed certificates.

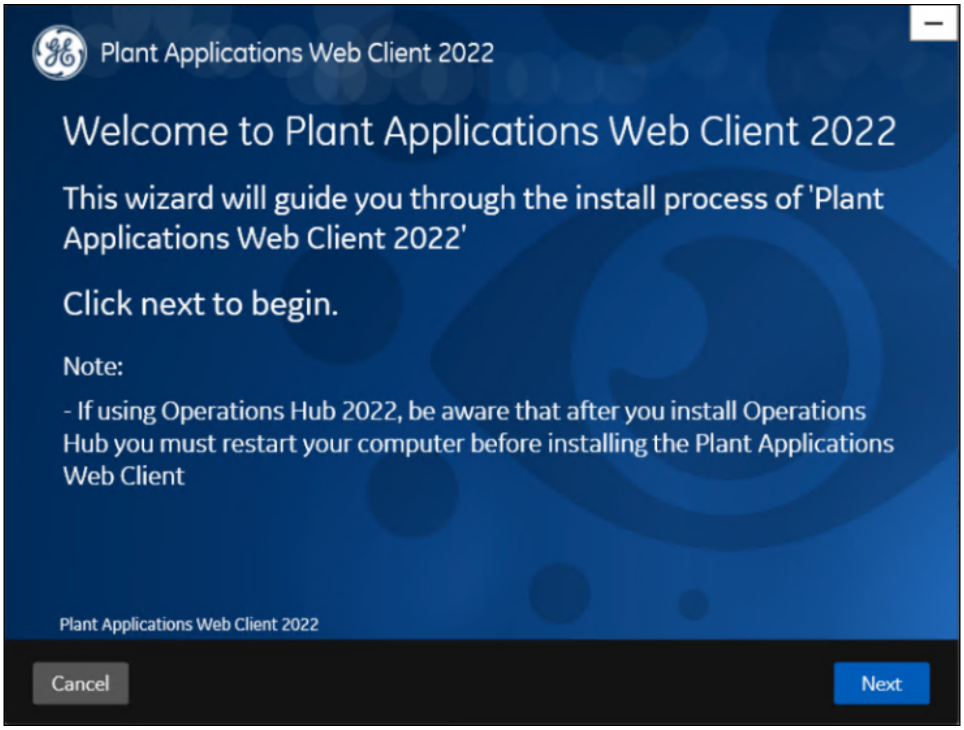
1. Run the `installfrontend.exe` file as an Administrator.
   The installation menu appears, displaying the **Install Proficy Plant Applications 2022** page.


Install Proficy Plant Applications 2022
Proficy Plant Applications 2022
General Electric Company
Proficy
Plant Applications
Proficy Plant Applications 2022 © 2015-2022, General Electric Company. All Rights Reserved. Proficy is a trademark of General Electric Company, inc., a wholly-owned subsidary of General Electric Company. * Indicates a trademark of General Electric Company and/or its subsidaries.
Before you start
Prerequisites
Proficy Application Server
Plant Applications 2022
Plant Applications Server
Plant Applications Report Server
Plant Applications Client
Plant Applications .NET SDK
Plant Applications Unicode Utility
Web Clients
Plant Applications Standard Web Client
SQL Native Client download
Online Help
View Documentation
Browse the DVD
Exit

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 2022** page.



Plant Applications Web Client 2022

Welcome to Plant Applications Web Client 2022

This wizard will guide you through the install process of 'Plant Applications Web Client 2022'

Click next to begin.

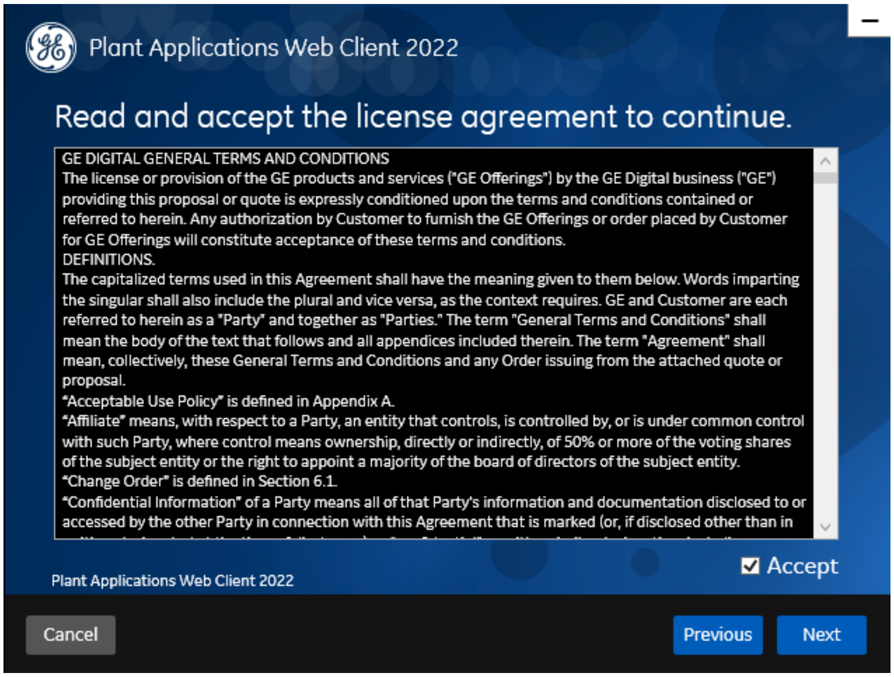
Note:

- If using Operations Hub 2022, be aware that after you install Operations Hub you must restart your computer before installing the Plant Applications Web Client

Plant Applications Web Client 2022
Cancel
Next

3. Select **Next**.

   The **Read and accept the license agreement to continue** page appears.



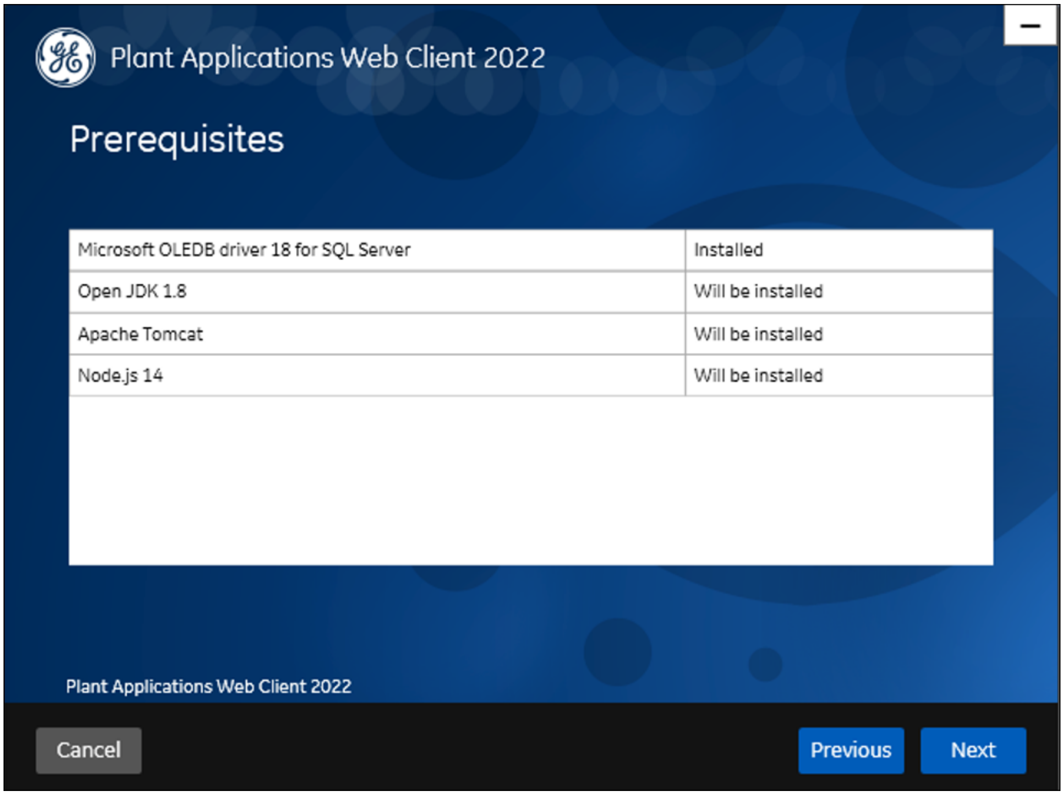
Read and accept the license agreement to continue.

GE DIGITAL GENERAL TERMS AND CONDITIONS
The license or provision of the GE products and services ("GE Offerings") by the GE Digital business ("GE") providing this proposal or quote is expressly conditioned upon the terms and conditions contained or referred to herein. Any authorization by Customer to furnish the GE Offerings or order placed by Customer for GE Offerings will constitute acceptance of these terms and conditions.
DEFINITIONS.
The capitalized terms used in this Agreement shall have the meaning given to them below. Words imparting the singular shall also include the plural and vice versa, as the context requires. GE and Customer are each referred to herein as a "Party" and together as "Parties." The term "General Terms and Conditions" shall mean the body of the text that follows and all appendices included therein. The term "Agreement" shall mean, collectively, these General Terms and Conditions and any Order issuing from the attached quote or proposal.
“Acceptable Use Policy” is defined in Appendix A.
“Affiliate” means, with respect to a Party, an entity that controls, is controlled by, or is under common control with such Party, where control means ownership, directly or indirectly, of 50% or more of the voting shares of the subject entity or the right to appoint a majority of the board of directors of the subject entity.
“Change Order” is defined in Section 6.1.
“Confidential Information” of a Party means all of that Party’s information and documentation disclosed to or accessed by the other Party in connection with this Agreement that is marked (or, if disclosed other than in

☑ Accept

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

The **Prerequisites** page appears.



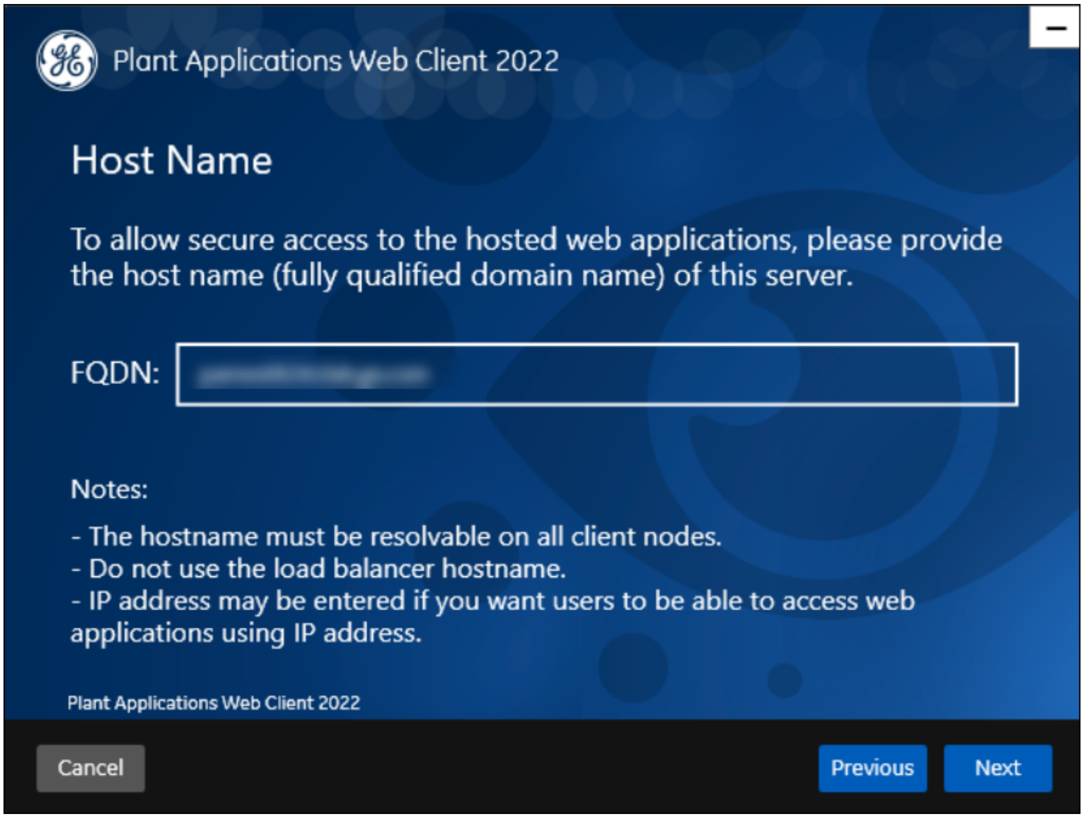
Plant Applications Web Client 2022
Prerequisites

Microsoft OLEDB driver 18 for SQL Server	Installed
Open JDK 1.8	Will be installed
Apache Tomcat	Will be installed
Node.js 14	Will be installed

Plant Applications Web Client 2022
Cancel
Previous
Next

5. Select **Next** to view all installed prerequisites and install any missing prerequisites.

   The **Host Name** page appears.



Host Name

To allow secure access to the hosted web applications, please provide the host name (fully qualified domain name) of this server.

FQDN: [redacted]

Notes:

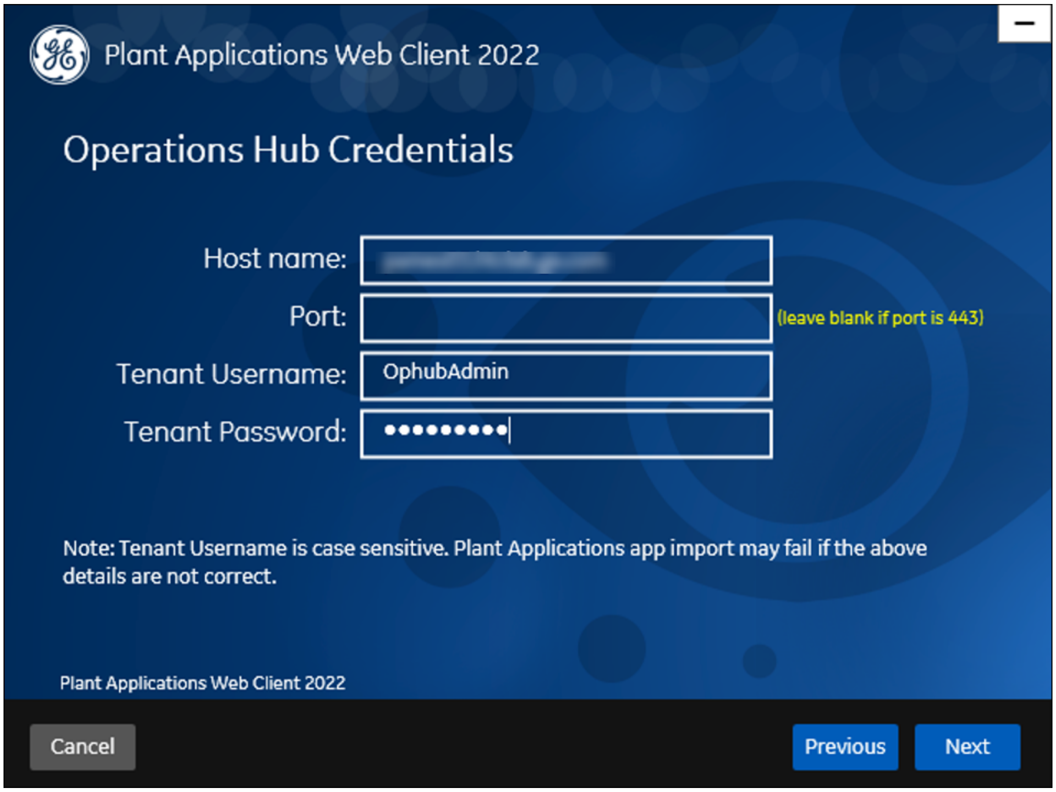
- The hostname must be resolvable on all client nodes.
- Do not use the load balancer hostname.
- IP address may be entered if you want users to be able to access web applications using IP address.

Plant Applications Web Client 2022

6. Enter the fully qualified domain name where you want to install the Plant Applications Web Client, then select **Next**.

   Note: Do not use the Load Balancer URL in the **FQDN** field. If you want to configure the Load Balancer URL, then you must perform it post installation.

   The **Operations Hub Credentials** page appears.



Operations Hub Credentials

Host name: [redacted]

Port: (leave blank if port is 443)

Tenant Username: OphubAdmin

Tenant Password: •••••••••

Note: Tenant Username is case sensitive. Plant Applications app import may fail if the above details are not correct.

Plant Applications Web Client 2022

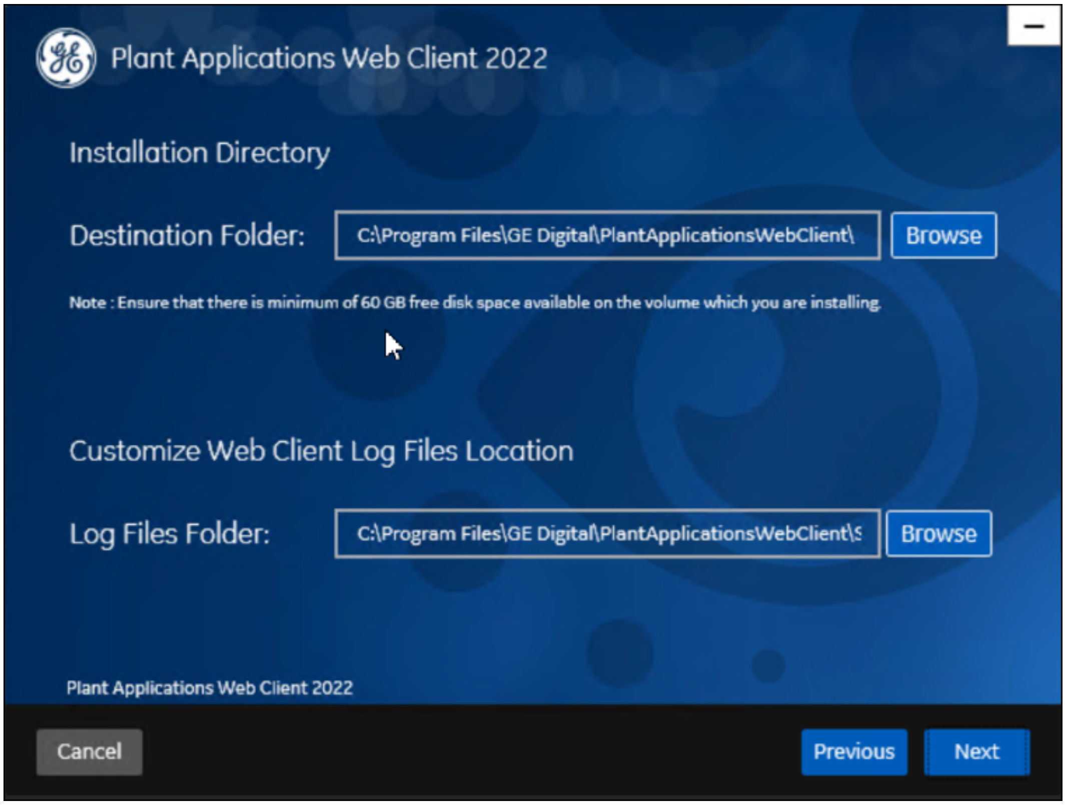
7. In the **Operations Hub Credentials** page, enter the credentials to access the Operations Hub server as described in the following table.

Field	Description
Host Name	This field is automatically populated with the local host name, fully qualified host name, or IP address, based on the configuration in Operations Hub. You can edit the host name of the Operations Hub server based on requirement. **Note:** Instead of IP address, we recommend to use the Operations Hub host name (computer name).
Port	Enter the Operations Hub port number if it is other than 443.
Tenant Username	Enter the tenant Hub username to access the Operations Hub server instance. **Note:** The default user name is `OphubAdmin`.
Tenant Password	Enter the password. **Note:** The tenant username and password must be same as the credentials that you have specified during the Operations Hub installation.

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

8. Select **Next**.

   The **Installation Directory and Customize Web Client Log Files Location** page appears.



Plant Applications Web Client 2022

Installation Directory

Destination Folder: C:\Program Files\GE Digital\PlantApplicationsWebClient\

Note : Ensure that there is minimum of 60 GB free disk space available on the volume which you are installing

Customize Web Client Log Files Location

Log Files Folder: C:\Program Files\GE Digital\PlantApplicationsWebClient\S

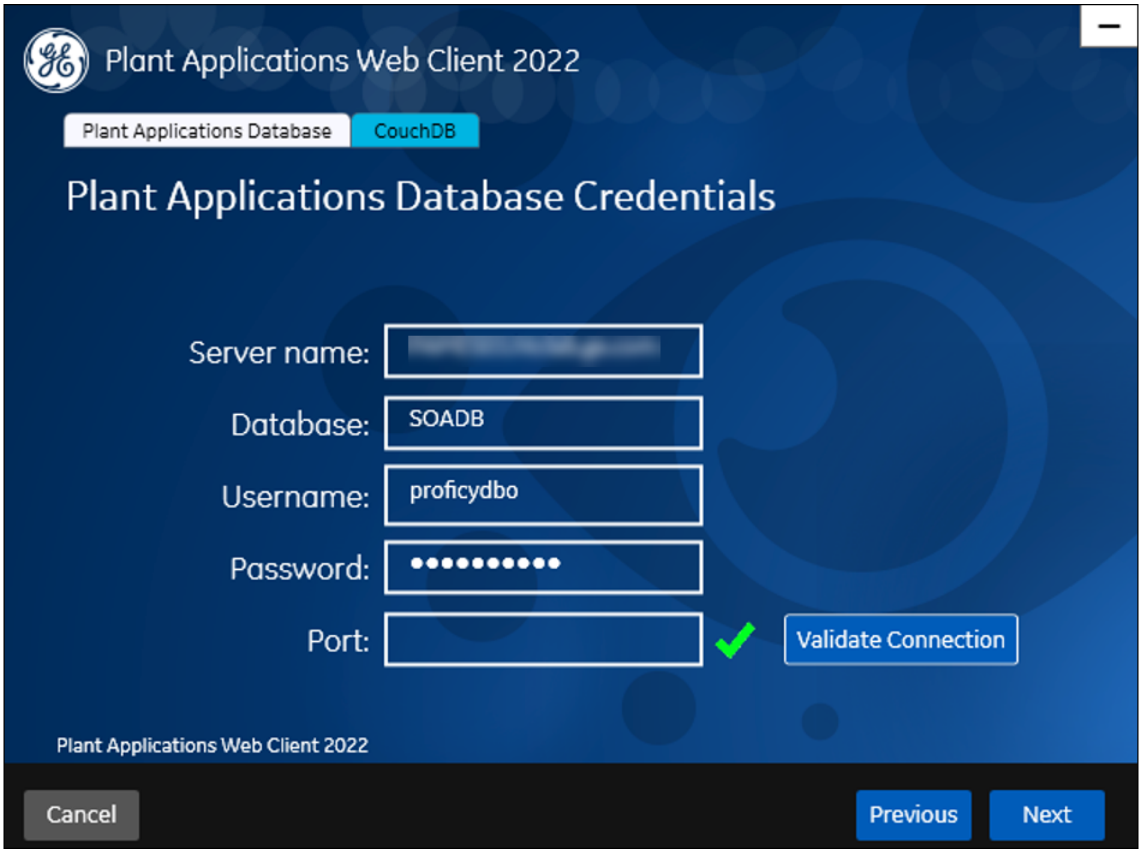
Plant Applications Web Client 2022

9. Do the following:
   a. In the **Destination Folder** field, select **Browse** to select the directory where you want to install the Plant Applications Web Client.

      Note:
      - Ensure that a minimum of 60 GB free disk space is available on the volume which you are installing.
      - Do not use the user profile folder for installation.

   b. In the **Log Files Folder** field, select **Browse** to select the directory where you want to install the Plant Applications Web Client service logs.

10. Select **Next**.
    The **Plant Applications Database Credentials** page appears.


Plant Applications Web Client 2022
Plant Applications Database
CouchDB
Validate Connection
Plant Applications Web Client 2022
Cancel
Previous
Next

Plant Applications Database Credentials

Server name: [redacted]

Database: SOADB

Username: proficydbo

Password: ●●●●●●●●●●

Port:

11. 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.

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

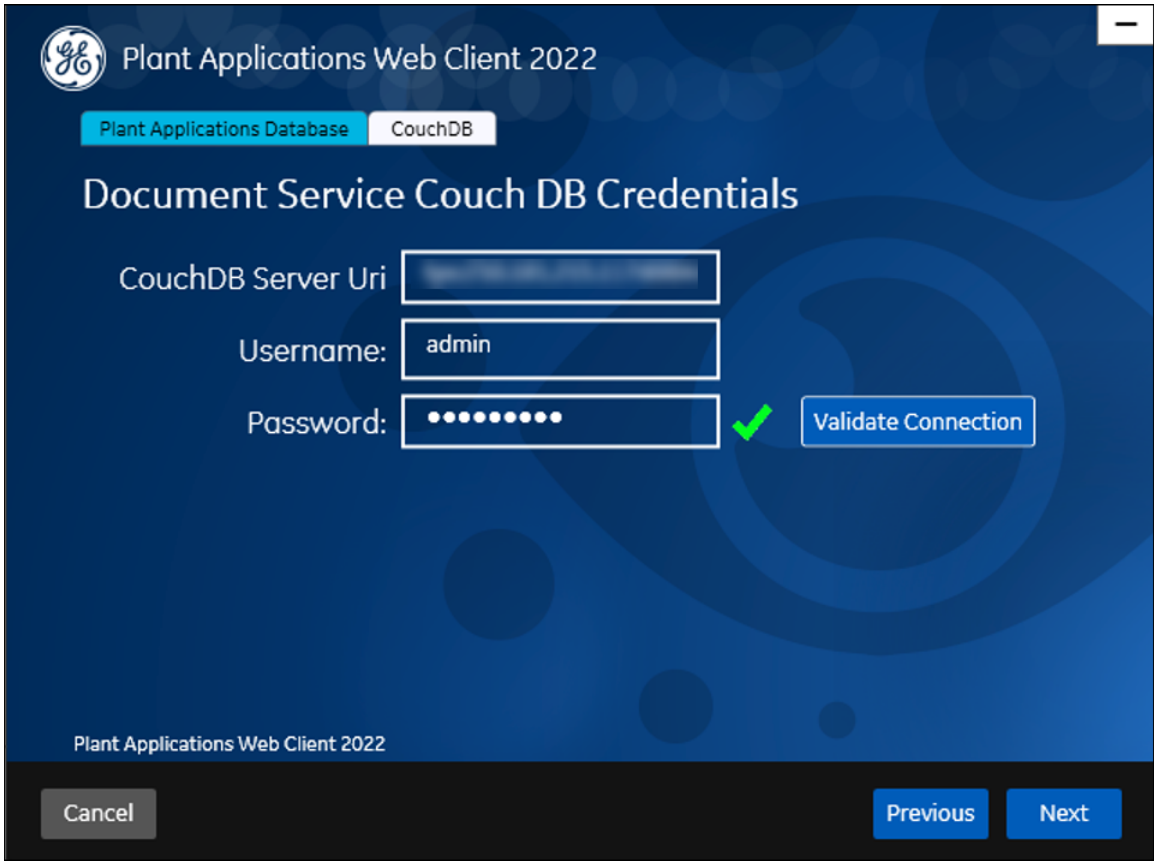
Field	Description
Port	Enter the number of the port that the instance uses to listen for client connections. This field is optional. **Note:** The default port is 1433.

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

    When the Plant Applications Database credentials are successfully validated, the **Next** button is enabled.

13. In the **Plant Applications Database Credentials** page, select the **CouchDB** tab.

    The **Document Service Couch DB Credentials** section appears.



Plant Applications Web Client 2022

Document Service Couch DB Credentials

CouchDB Server Uri [redacted]

Username: admin

Password: ●●●●●●●●●● ✓

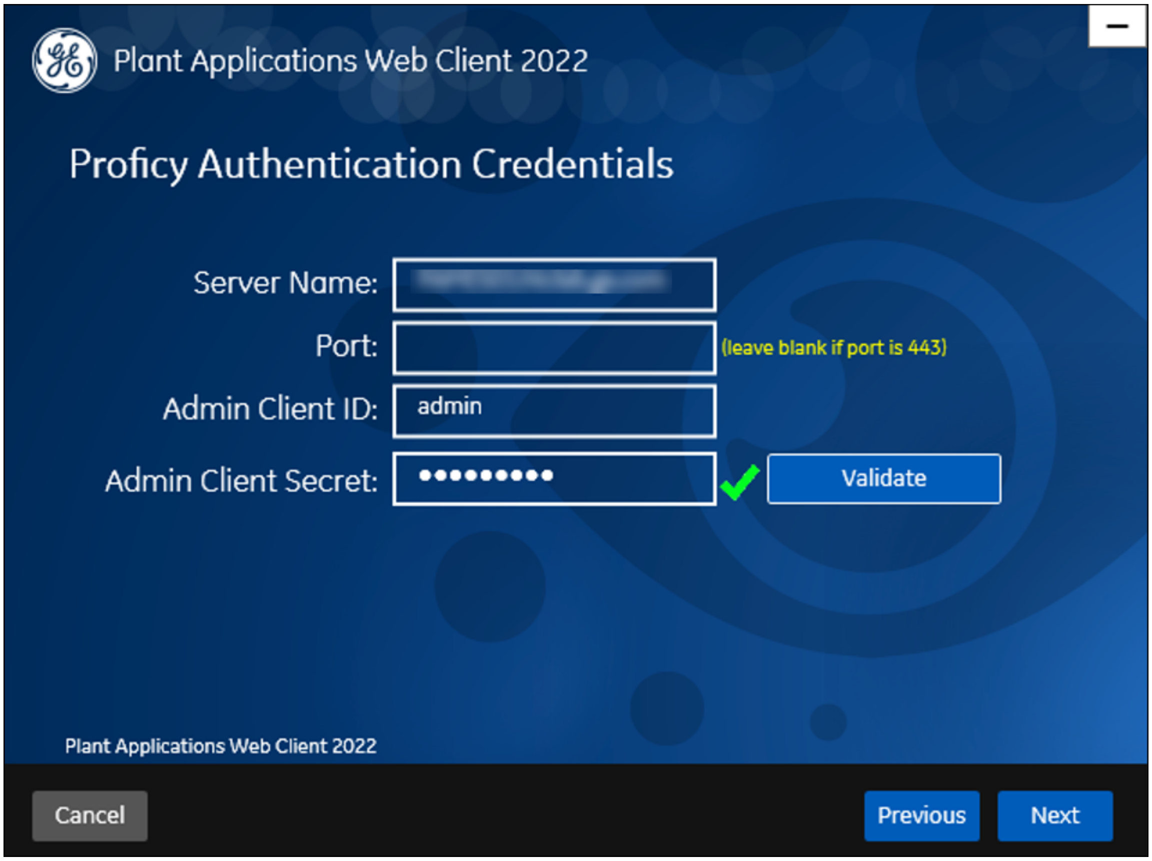
Plant Applications Database
CouchDB
Validate Connection
Plant Applications Web Client 2022
Cancel
Previous
Next

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

Field	Description
CouchDB Server Uri	Enter the fully qualified web address of Apache CouchDB in the format: `https://<host name or IPaddress>:<port number>`. For example, https://testmachine:6984.
Username	Enter the user name of the administrator that has permissions to access the database you entered in the **Database** field.
Password	Enter the password.

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

15. Select **Next**.
The **Proficy Authentication Credentials** page appears.



Plant Applications Web Client 2022

Proficy Authentication Credentials

Server Name: [redacted]
Port: (leave blank if port is 443)
Admin Client ID: admin
Admin Client Secret: ●●●●●●●●● ✓

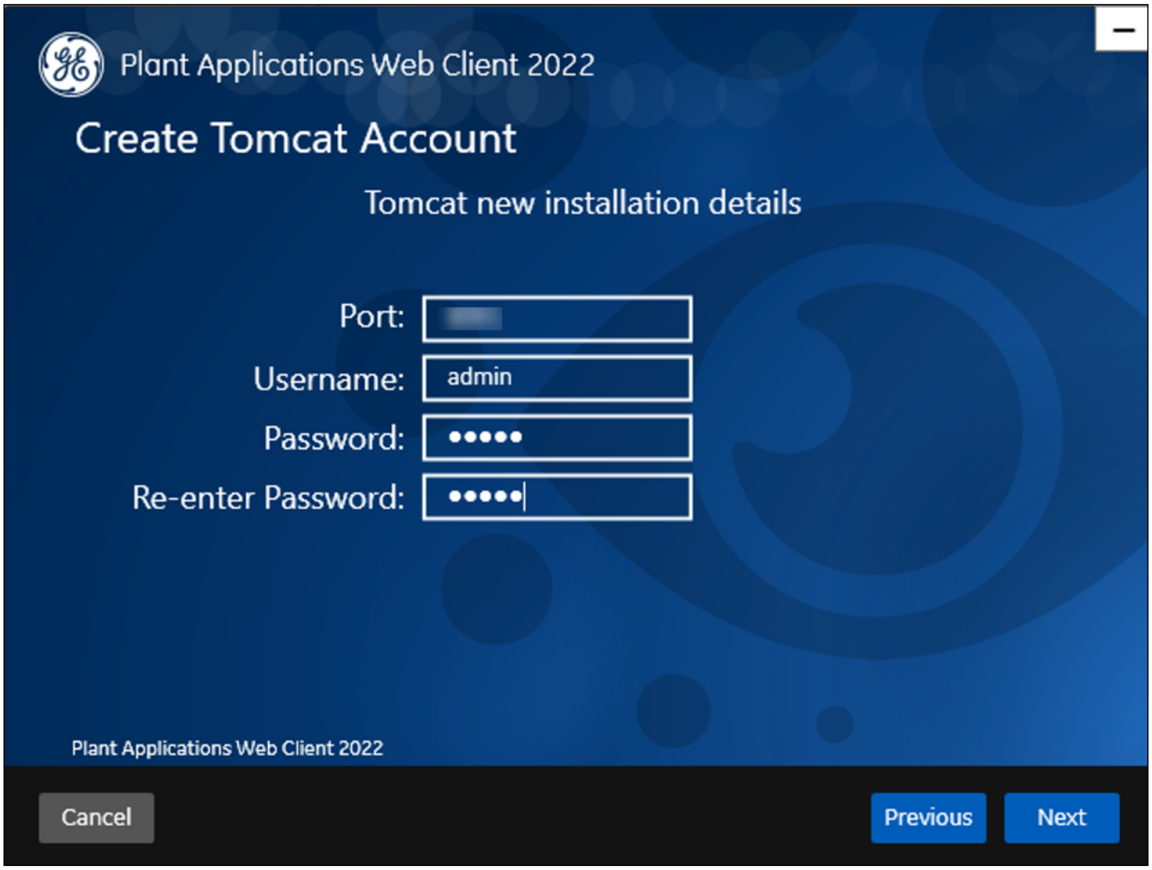
Validate
Plant Applications Web Client 2022
Cancel
Previous
Next

16. Enter the credentials to access the Proficy Authentication server as described in the following table.

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

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

The **Create Tomcat Account** page appears.



Plant Applications Web Client 2022

Create Tomcat Account

Tomcat new installation details

Port: [redacted]

Username: admin

Password: ●●●●●

Re-enter Password: ●●●●●

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.

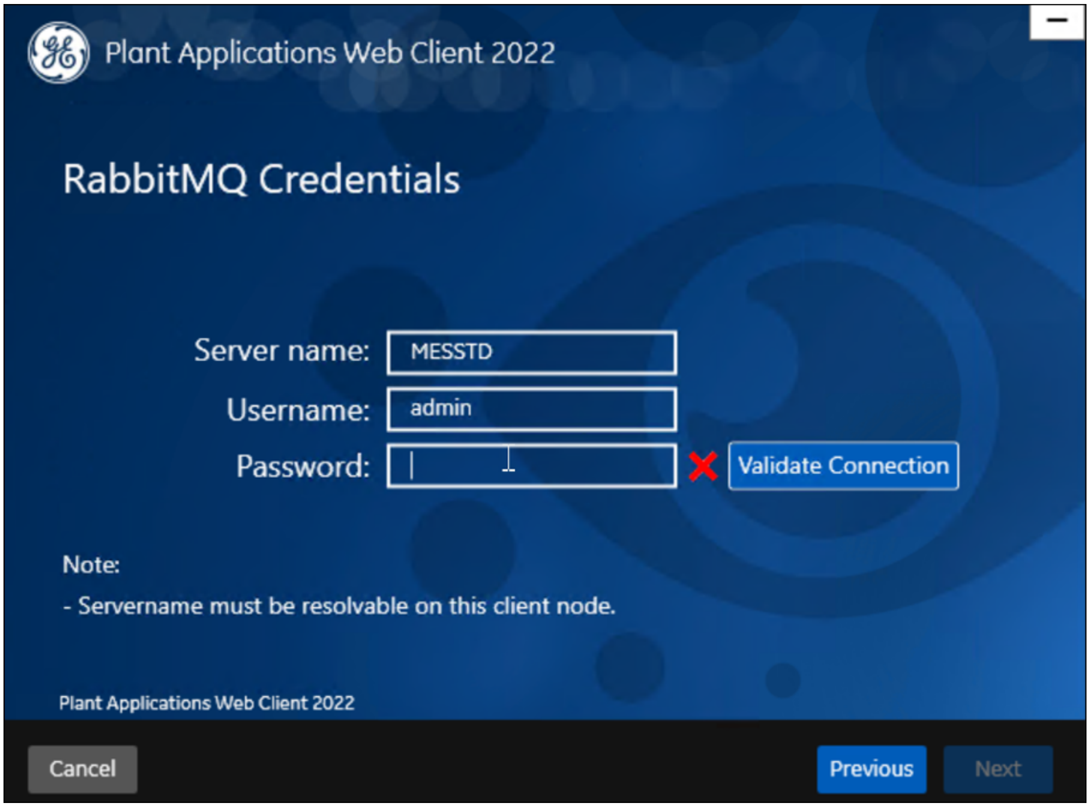
17. Enter the Tomcat installation details for a new or existing installation as described in the following table. The installer prompts you to enter details for an existing Tomcat if the Tomcat installation details are available in the registry settings for the Plant Applications Web Client on your computer.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

Field	Description
Port	Enter the HTTP port that Tomcat uses to listen for client connections. **Note:** The default port is 8091.
Username	Enter the user name to access Tomcat. **Note:** The default user name is `admin`.
Password	Enter the password for the user name you entered in the **Username** field.

Field	Description
Re-enter Password	Re-enter the password for the user name entered in the **Username** field. **Note:** This box appears only when a new installation of Tomcat is initiated by the installer.

18. Select **Next**.

    The **RabbitMQ Credentials** page appears.



Plant Applications Web Client 2022

RabbitMQ Credentials

Server name: MESSTD

Username: admin

Password:

Note:

- Servername must be resolvable on this client node.

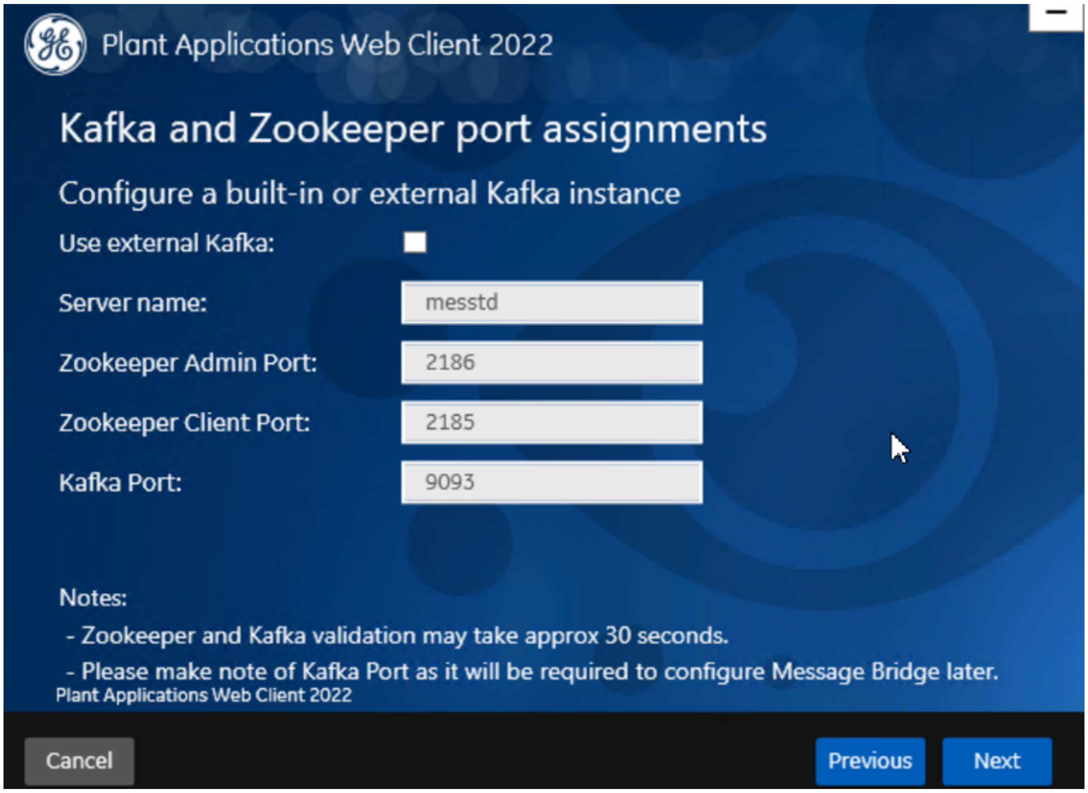
Plant Applications Web Client 2022

RabbitMQ is by default installed as part of the Plant Application Server. Enter the RabbitMQ login details to proceed with the installation.

19. Enter the required information in the following fields, and then select **Next**.

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

The **Kafka and Zookeeper port assignments** page appears.



Plant Applications Web Client 2022

Kafka and Zookeeper port assignments

Configure a built-in or external Kafka instance

Use external Kafka: □

Server name: messtd

Zookeeper Admin Port: 2186

Zookeeper Client Port: 2185

Kafka Port: 9093

Notes:

- Zookeeper and Kafka validation may take approx 30 seconds.
- Please make note of Kafka Port as it will be required to configure Message Bridge later.

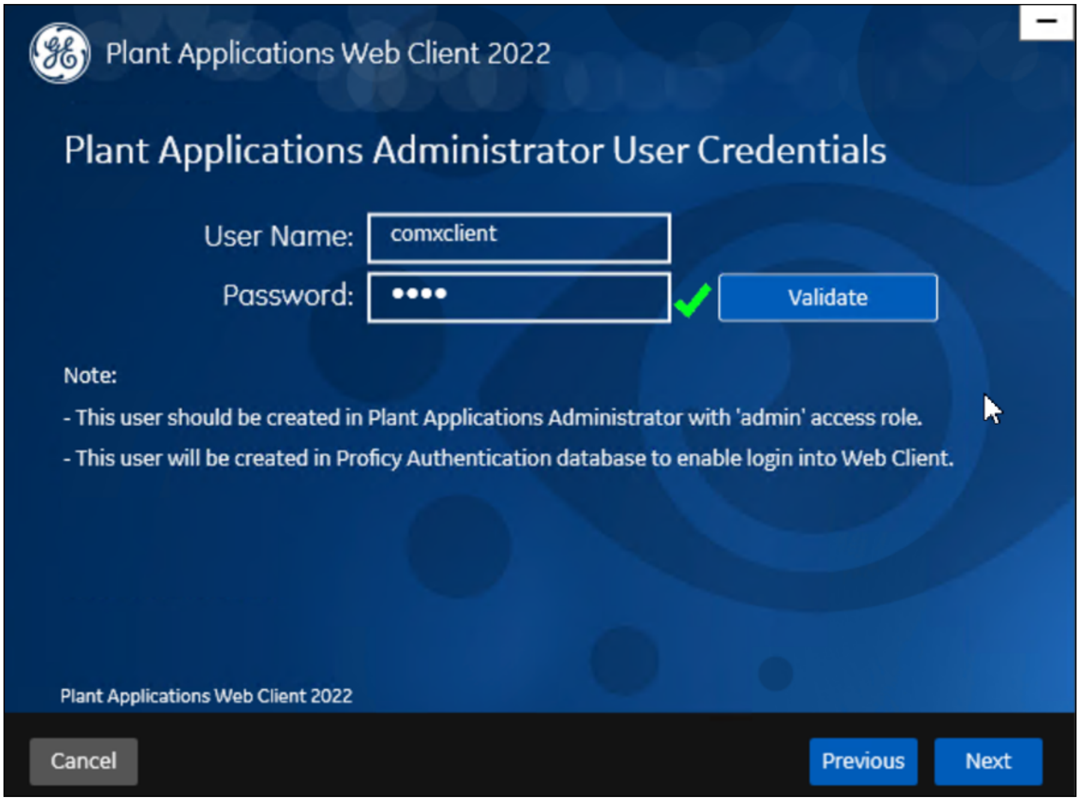
Plant Applications Web Client 2022
Cancel
Previous
Next

20. Enter the credentials to access the Kafka server as described in the following table.

Field	Description
Server Name	Enter the host name of the Kafka server. By default, it is the Plant Applications Web Client server name.
Zookeeper Admin Port	Accept the default port number. To change the default port number, enter a new Zookeeper Admin port number. By default, Kafka and Zookeeper will be installed along with Plant Applications Web Client. If you are not using any external Kafka server, then you can use Plant Applications Web Client server name.
Zookeeper Client Port	Accept the default port number. To change the default port number, enter a new Zookeeper Client port number. **Note:** Ensure that you have entered a valid Zookeeper port number. If you have entered an invalid port number, refer to **Changing the Zookeeper Port Number** section in *Getting Started Guide*.
Kafka Port	Accept the default port number. The default port number is 9093. To change the default port number, enter a new Kafka port number.

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

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



Plant Applications Web Client 2022

Plant Applications Administrator User Credentials

User Name: comxclient

Password: ••••

Note:

- This user should be created in Plant Applications Administrator with 'admin' access role.
- This user will be created in Proficy Authentication database to enable login into Web Client.

Plant Applications Web Client 2022

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

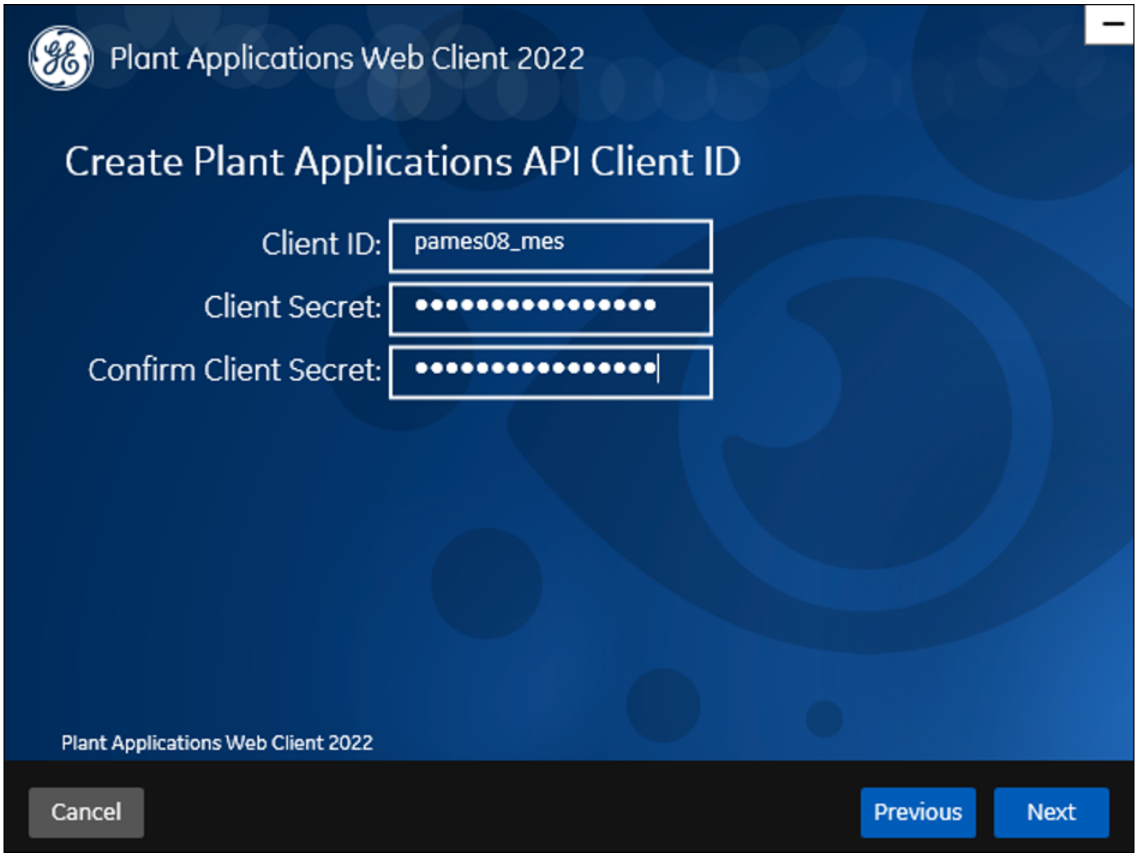
Note: Ensure that the user credentials entered here must exist in Plant Applications Server with an administrator role defined and you must use the same credentials to login to the Web Client applications.

Credential	Description
User Name	Enter the user name for an administrator account in Plant Applications. **Note:** The default user name is `OphubAdmin`.
Password	Enter the password for the user name you entered in the **User Name** box.
Validate	Validate the Plant Applications Administrator credentials.

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

23. Select **Next**.

The **Create Plant Applications API Client ID** page appears.



Plant Applications Web Client 2022

Create Plant Applications API Client ID

Client ID: pames08_mes

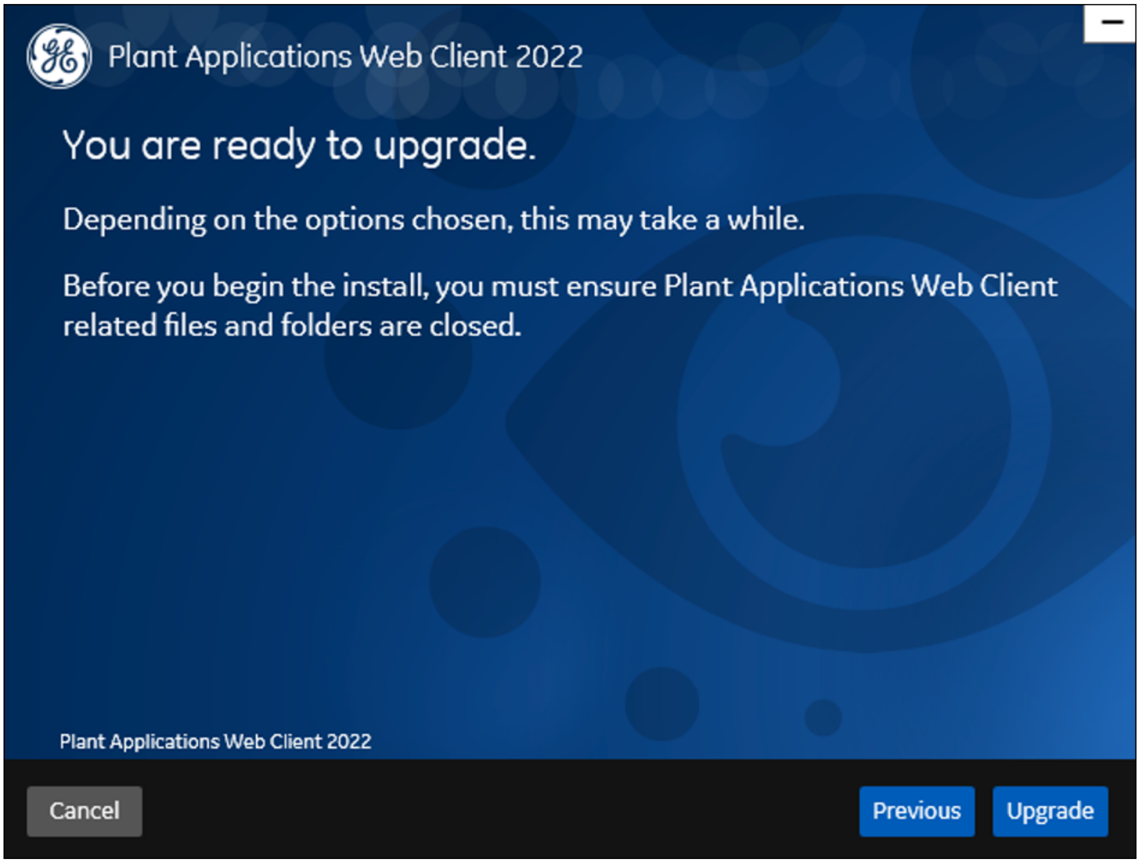
Client Secret: ●●●●●●●●●●●●●●●●

Confirm Client Secret: ●●●●●●●●●●●●●●●●

24. Enter the required information in the following fields, and then select **Next**.

Field	Description
Client ID	Enter the user name. The default username is `hostname_mes`, you can enter the user name of your choice.
Client Secret	Enter the password.
Confirm Client Secret	Enter the password to confirm the value in the **Client Secret** field.

25. Select **Next**.
    The **You are ready to upgrade** page appears.



Plant Applications Web Client 2022

You are ready to upgrade.

Depending on the options chosen, this may take a while.

Before you begin the install, you must ensure Plant Applications Web Client related files and folders are closed.

Plant Applications Web Client 2022

26. 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.

27. **Optional:** Select **View Logs** to see the upgrade details.

28. In the **Upgrade Successful** screen, select **Exit** to close the upgrade wizard.
    Plant Applications Web Client has been upgraded to the latest version.

29. Run the Message Bridge Configuration Utility *(page 90)* on the Plant Applications Server to update the Kafka details in the Message Bridge configuration.

    Note: If you are using signed certificates, then you must re-import the signed certificates using Configuration Manager utility after the upgrade is completed.

30. Once you have completed running Message Bridge Configuration and Operations Hub Posting utilities, Verify the Installation *(page 95)* to verify if the Plant Applications Web Client applications are up and running.

31. Access the Plant Applications REST APIs *(page 95)* to access the REST APIs for Plant Applications Web Client.
32. When upgrade is successful but posting apps into Operations Hub fail, then you must post the apps using utility. See Post Applications into Operations Hub Manually *(page 128)*.

Upgrade Plant Applications Web Client in Silent Mode

The silent upgrade consists of configuring settings in a configuration file. Use the configuration file `configuration.ini` to configure same settings that you configure during interactive installation.

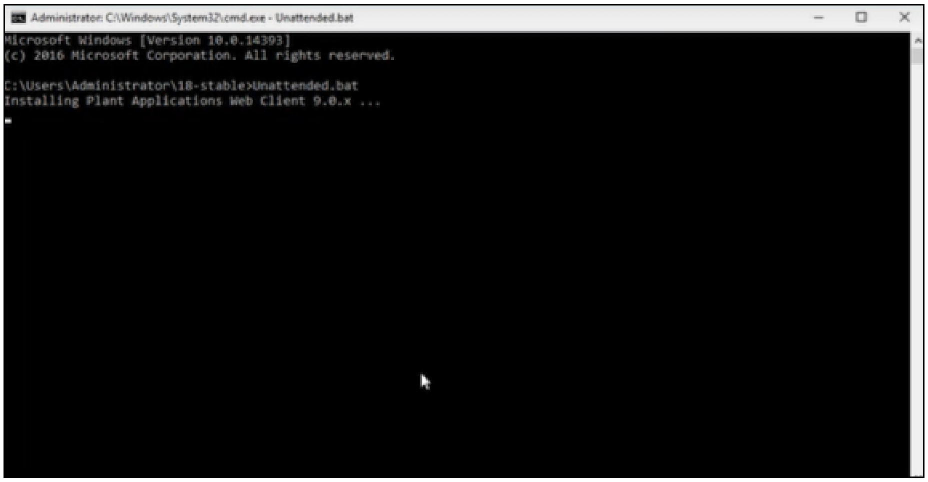
The silent mode of upgrade for Standard Web Client is applicable to only the **Standard** method.

1. Mount the ISO, and then navigate to the `E:\Install\WebClient` directory, and then open the `configuration.ini` file using any text editor, for example, Notepad or Notepad++.

   Note:

   To edit the configuration file `configuration.ini`, copy the `.ini` file to a location on your machine. For example, `C:\New folder`.

2. In the configuration file, enter details for the following:
   - Operations Hub credentials
   - Fully Qualified Domain Name (FQDN)
   - Installation Directory
   - Proficy Authentication (UAA) credentials
   - Plant Applications Web Client API Login details
   - Plant Applications Database credentials
   - Plant Applications CouchDB credentials
   - Plant Applications Administrator User credentials
   - Tomcat credentials
   - Log file location
   - RabbitMQ credentials
   - Kafka and Zookeeper credentials
3. Save the `configuration.ini` file.
4. Open the command prompt in the administrator mode, and then navigate to the path `E:\Install\WebClient` where the `Unattended.bat` file resides. The `E:\` is the drive where the ISO has been mounted. Then run this command: `Unattended.bat "<absolute path of configuration.ini file>"`.



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\18-stable>Unattended.bat
Installing Plant Applications Web Client 9.0.x ...
```

The Plant Applications Standard Web Client upgrade starts. A progress bar appears and displays the upgrade progress.

Note: The installation takes about 20 minutes to complete and might take longer based on system resources.

Note: Before you log into the Plant Applications Web Client, ensure to complete the configuration of the Message Bridge Utility.

5. To see the installation details, you can access the log file here: `C:\ProgramData\Proficy\Logs\webclientinstaller\`. To see the application details, you can access the log file here: `C:\Program Files\GE Digital\PlantApplicationsWebClient\ServiceLogs`.
   When the upgrade is complete, Run the Message Bridge Configuration Utility *(page 90)*.
   This is mandatory step to be completed before using the Web Client.

   Note: If the upgrade fails, then the system displays an error code: `Failure.exit code is 3010`. Check the log file to view the error and the description for the problem.

6. When you have completed running Message Bridge Configuration, Verify the Installation *(page 95)* if the Plant Applications Web Client applications are up and running.

   Note: If you are using signed certificates, then you must re-import the signed certificates using Configuration Manager utility after the upgrade is completed.

7. Access the Plant Applications REST APIs *(page 95)* to access the REST APIs for Plant Applications Web Client.

8. When upgrade is successful but posting applications into Operations Hub fail, then you must post the applications using utility. See Post Applications into Operations Hub Manually *(page 128)*.
9. After the upgrade is complete, if you want to find the port details or swagger URL information, refer the `WebClient-Ports.txt` located in `C:\Program Files\GE Digital \PlantApplicationsWebClient\WebClient-Ports.txt`.

Perform the post-installation steps *(page 41)*.

Chapter 6. Installing Plant Applications Enterprise Web Client

About Installing Enterprise Edition Web Client

Plant Applications Enterprise Edition 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 YML (`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 Edition Web Client uses Docker technology. During the Plant Applications Enterprise Edition 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-2022` 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 Edition Web Client on a Linux environment.

Note:

- Plant Applications Enterprise Edition 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.

The following table outlines the steps that you must complete to install Plant Applications Enterprise Edition 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 Workflow 2.6 SP1	This step is required.
2	Install Plant Applications Server	This step is required.
3	Install Operations Hub 2.1 with SIM3 and later ❗ **Important:** If using Operations Hub 2022, be aware that after you install Operations Hub you must restart your computer before installing the Plant Applications Web Client.	This step is required.
4	Install and Configure CouchDB for HTTPS *(page 17)*	This step is required.
5	Ensure that your system meets the requirements for the Enterprise Edition Web Client installation. *(page 9)*	This step is required.
6	Review the files provided by GE *(page 72)*	This step is required.
7	Review the pre-installation checklist before installing Enterprise Edition Web Client. *(page 73)*	This step is required.
8	Install Enterprise Edition Web Client *(page 75)*	This step is required.
9	After the Enterprise Edition Web Client installation, ensure to run the Message Bridge Configuration utility. *(page 90)*	This step is required.
10	Verify the Installation *(page 95)*	This step is required.

Files Provided by GE

The following files are provided by GE:

- `plantapps-enterprise-webclient-2022`: Contains the installer and the supporting utilities.
- `plantapps-prereq.tar`: Contains the files required for installing Web Client pre-requisites.

  Note: Ensure you copy `plantapps-prereq.tar` and `plantapps-enterprise-webclient-2022` into a same folder before running the installation.

- `plantapps-images.tar`: 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`: Used to create and configure Docker Registry.

Pre-Installation Checklist

1. Ensure that you have Plant Applications Server, Operations Hub Server, and CouchDB installed and running before installing Plant Applications Enterprise Edition Web Client. For information, refer to the *Enterprise Deployment Architecture* section in the *Getting Started Guide*.
2. If you are using a Proficy Authentication (UAA) service other than Operations Hub UAA, migrate your Proficy Authentication (UAA) data to Operations Hub UAA.
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 remote installation, you must set the HTTP_PROXY and HTTPS_PROXY in the respective nodes.

4. Create and configure Docker Registry *(page 73)*.
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 Edition Web Client.
7. Extract the contents of the `plantapps-enterprise-webclient-<buildno>`.
8. 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

Use this section to create and configure docker registry.

1. From the Plant Applications Enterprise Edition 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 50 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\u0002proxy.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 restart the docker:

```
sudo systemctl restart docker
```

10. Using terminal, navigate to the `pa-dtr` folder.

11. 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`

12. 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.

13. 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 Edition Web Client, enter <host name of IP address of this local Docker Registry>:5000.

    Note: Do not enter http or https.

Install Enterprise Edition Web Client

Note: Before installing the Plant Applications Enterprise Edition Web Client, ensure that you first perform the preinstallation tasks *(page 7)* and then 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 `~/<Install file path>/plantapps-enterprise-webclient-<buildno>/log/ansible.log` and `~/<Install file path>/plantapps-enterprise-webclient-<buildno>/log/sql_script.log`.

1. From the `~/<Install file path>/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
WEBCLIENT_SERVER: ""	Enter the Linux node FQDN or hostname where you are going to install Plant Applications Enterprise Edition Web Client. For example, `WEBCLIENT_SERVER: "linuxnode.digital.com"`

Parameter	Description
WEBCLIENT_SERVER_USERNAME: ""	Enter the Linux node administrator account username. For example, `WEBCLIENT_SERVER_USERNAME: "administrator"` **Note:** Enter the Web Client Server user name. This field is required only during remote installation.
WEBCLIENT_SERVER_PASSWORD: ""	Enter the Linux node administrator account password. **Note:** Enter the Web Client Server password. This field is required only during remote installation.

WEBCLIENT_INSTALLATION_PATH: ""	Enter Web Client Installation path in which you want to install.
	For example,
	`WEBCLIENT_INSTALLATION_PATH: "/home/administrator/install/"`
	Note: If you are performing an upgrade, provide the absolute path of the directory in which Enterprise Edition Web Client was installed, and press **Enter**. Unless modified, the path appears as follows:
	`/<buildpath>/PlantApplicationsDocker`
	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.

DTR_URL: ""	Enter the URL of your local Docker Registry that you created in Create and Configure Docker Registry *(page 73)*. For example, `DTR_URL:<IP address or hostname>:<port number>`, where the default port number is 5000. For example, if you are using the GE repository, `"registry.gear.ge.com/dig-plantapps"`. **Note:** If you are performing an upgrade, provide the Docker Registry URL that was used during the previous installation in the following format: `<IP address or hostname>:<port number>`.
DTR_USERNAME: ""	Enter the username that have access to the Docker Registry. **Note:** Enter none if using insecure registry.
DTR_PASSWORD: ""	Enter the password to the Docker Registry. **Note:** Enter none if using insecure registry.

Parameter	Description
TARFILES_FOLDER_LOCATION: ""	Enter the absolute path of the directory where the **.tar** files provided by GE are located. For example, `TARFILES_FOLDER_LOCATION: "/plantapps-enterprise"` If the `.tar` file located in a build folder under administrative account, then the path will be `"administrator/build"`.
WEBCLIENT_USERNAME: ""	Enter the Plant Applications Web Client username to login into the application. For example, `WEBCLIENT_USERNAME: "comxclient"`
WEBCLIENT_USERPASSWORD: ""	Enter the Plant Applications Web Client password.
PROFICY_AUTHENTICATION_SERVICE_ORIGIN: ""	Enter the Proficy Authentication Server (UAA) hostname.
PROFICY_AUTHENTICATION_SERVICE_PORT: ""	Enter the Proficy Authentication Server port number. By default, the port number is 443.
PROFICY_AUTHENTICATION_SERVICE_ ADMIN_CLIENT_ID: ""	Enter the admin Client ID to access the Proficy Authentication server instance. **Note:** The default username is **admin**.
PROFICY_AUTHENTICATION_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.
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, `PLANT_APPS_DB_INSTANCE: "sa"` **Note:** Do not add a backslash (\) when entering the instance name.
PLANT_APPS_DB_NAME: ""	Enter the Plant Applications Database name. For example, `PLANT_APPS_DB_NAME: "SOADB"`
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.
PLANT_APPS_MB_SERVER: ""	Enter the host name or IP address of the Plant Applications Server.
PLANT_APPS_MB_USERNAME: ""	Enter the username that you set for Plant Applications Message Bridge during the Plant Applications Server installation.

Parameter	Description
PLANT_APPS_MB_PASSWORD: ""	Enter the password for the username you entered.
COUCHDB_SERVER: ""	Enter the Plant Applications CouchDB host name or IP address.
COUCHDB_USERNAME: ""	Enter the CouchDB username.
COUCHDB_PASSWORD: ""	Enter the CouchDB password.
PLANT_APPS_API_CLIENT_ID	Enter the user name that you want to use for accessing Plant Applications APIs. **Note:** It can be used to login to Swagger APIs. Default is `'hostname_mes'`.
PLANT_APPS_API_CLIENT_SECRET	Enter the password.
OPHUB_SERVER: ""	Enter the hostname of Operations Hub server.
OPHUB_SERVER_PORT: ""	Enter the Operations Hub port number. For example, `OPHUB_SERVER_PORT: "443"`
OPHUB_TENANT_USERNAME: ""	Enter the tenant Hub username to access the Operations Hub server instance. For example, `OPHUB_TENANT_USERNAME: "OphubAdmin"`. **Note:** The OPHUB_TENANT_USERNAME field is case sensitive. You must always enter the user name as OphubAdmin.
PASSWORDS_OR_CERTS_UPDATED : ""	Default value is true. You can set this to false if you want to use OLD certificates during upgrade. For example, `PASSWORDS_OR_CERTS_UPDATED: "false"`
ENCRYPT_PASSWORDS: ""	Set to true if you want to encrypt the password. For example, `ENCRYPT_PASSWORDS: "false"`
SSL_CERT_PEM_PATH: ""	Enter the path to the SSL certificate. For example, `SSL_CERT_PEM_PATH: " /home/administrator/myca_certs/new_cert.pem"` **Note:** Not required for Enterprise installation but is required only when applying the certificates using the `utility.sh`. Use this parameter only to replace the self-signed certificate with the trusted CA certificate.

Parameter	Description
SSL_KEY_PEM_PATH: ""	Enter the path where the valid CA key file is located. For example, `SSL_KEY_PEM_PATH: "/home/administrator/myca_certs/new_key.pem"` **Note:** Not required for Enterprise installation but is required only when applying the certificates using the `utility.sh`. Use this parameter only to replace the self-signed certificate with the trusted CA certificate.
UAA_PEM_PATH: ""	Enter the path where the valid UAA public key is located. For example, `UAA_PEM_PATH: "/ home/administrator/myca_certs/new_uaa_cert.pem"` **Note:** Not required for Enterprise installation but is required only when applying the certificates using the `utility.sh`. Use this parameter only to update the public keys of remote UAA services.

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
   ```

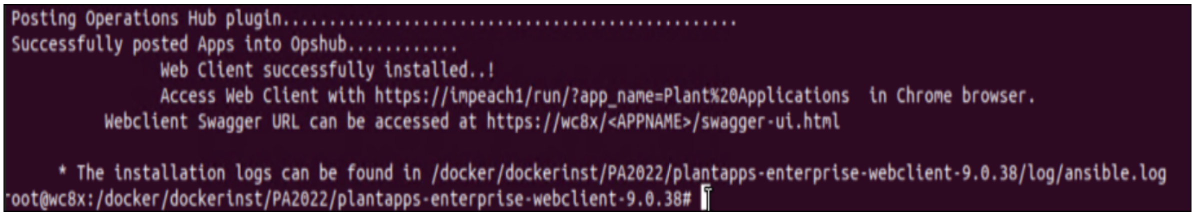
5. Depending on your deployment architecture, run one of the following commands to launch the installer:
   - If you want to run the Enterprise Edition Web Client Installer and install Enterprise Edition Web Client on a **same Linux machine**, navigate to your installer folder `~/your/path/plantapps-enterprise-webclient-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



```
Posting Operations Hub plugin...............................................
Successfully posted Apps into Opshub............
                Web Client successfully installed..!
                Access Web Client with https://impeach1/run/?app_name=Plant%20Applications  in Chrome browser.
          Webclient Swagger URL can be accessed at https://wc8x/<APPNAME>/swagger-ui.html

     * The installation logs can be found in /docker/dockerinst/PA2022/plantapps-enterprise-webclient-9.0.38/log/ansible.log
root@wc8x:/docker/dockerinst/PA2022/plantapps-enterprise-webclient-9.0.38#
```

- 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 the Message Bridge Configuration Utility *(page 90)* on the Plant Applications Server to update the Kafka details in the Message Bridge configuration.

7. Once you have completed running Message Bridge Configuration, Verify the Installation *(page 95)* if the Plant Applications Web Client applications are up and running.

8. Access the Plant Applications REST APIs *(page 95)* to access the REST APIs for Plant Applications Web Client.

9. When installation is successful but posting apps into Operations Hub fail, then you must post the apps using utility. See Post Applications into Operations Hub Manually *(page 128)*.

Replace the SSL Certificate of Enterprise Edition Web Client

Install Plant Applications Enterprise Edition 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 the Enterprise Edition Web Client using HTTPS. For better security, we recommend replacing this self-signed certificate with one issued by a trusted CA authority.

Note: We recommend to use the signed certificates. The self-signed certificate which is provided during the installation is valid for 2 years from the date of installation of the Enterprise Edition Web Client.

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, `SSL_CERT_PEM_PATH: " /home/administrator/myca_certs/new_cert.pem"`
SSL_KEY_PEM_PATH: ""	Enter the path to the SSL key. For example, `SSL_KEY_PEM_PATH: "/home/administrator/myca_certs/new_key.pem"`

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. 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 Proficy Authentication (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 the Root CA and the Intermediate Enterprise 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
PROFICY_AUTHENTICATION_PEM_PATH: ""	Enter the path where the valid CA key file is located. For example, `PROFICY_AUTHENTICATION_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. 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 Proficy Authentication (UAA).

Reset Passwords 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.

Based on the requirement, you can update the following in the `silentinstaller.yml` file:

- SQL credentials. See Reset SQL Credentials *(page 82)*
- Message Bridge credentials. See Reset Message Bridge Credentials *(page 83)*
- CouchDB credentials. See Reset CouchDB Credentials *(page 84)*

Reset SQL Credentials

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

Parameter	Description
WEBCLIENT_INSTALLATION_PATH: ""	Enter the Web Client Installation path in which you want to install. For example, `WEBCLIENT_INSTALLATION_PATH: "/ home/ administrator/install/"`
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, `PLANT_APPS_DB_INSTANCE:"sa"` **Note:** Do not add a backslash (\) when entering the instance name.
PLANT_APPS_DB_NAME: ""	Enter the Plant Applications Database name. For example, `PLANT_APPS_DB_NAME:"SOADB"`
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.
PLANT_APPS_DB_PORT: ""	Enter the SQL Server port.

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 -sql 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 -sql reset`

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

Reset Message Bridge Credentials

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

Parameter	Description
WEBCLIENT_INSTALLATION_PATH: ""	Enter Web Client Installation path in which you want to install. For example, `WEBCLIENT_INSTALLATION_PATH: "/home/ administrator/install/"`
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.

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 -mb 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 -mb reset`

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

Reset CouchDB Credentials

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

Parameter	Description
WEBCLIENT_INSTALLATION_PATH: ""	Enter the Web Client Installation path in which you want to install. For example, `WEBCLIENT_INSTALLATION_PATH: "/home/ administrator/install/"`
COUCHDB_SERVER: ""	Enter the Plant Applications CouchDB host name or IP address.
COUCHDB_USERNAME: ""	Enter the CouchDB username.
COUCHDB_PASSWORD: ""	Enter the CouchDB password.

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 -couch 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 -couch reset`

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

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 the top-left corner of the screen.
   You need to delete the following Discrete Apps:
   - Unit Operations
   - Work Order Manager
   - Route Editor
   - Work Queue
   - 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 in 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 works only when Operations Hub URL and credentials are not changed. If credentials or URL are updated, the Web Client must be reinstalled.

1. On the Enterprise Edition Web Client machine, navigate to this directory `{{Installer directory}}/ OpshubPost/`.
2. Update the `application.properties` file.
3. To give executable permissions, run `sudo chmod +x ./Linux_UpdateScopesAndPostPlugins.sh`.
4. Run `sudo ./Linux_UpdateScopesAndPostPlugins.sh`
5. Copy uaa cert pem to the linux machine.
6. On the Web Client machine navigate to installer folder using `$cd path/to/installer`
7. Edit the `silentinstaller.yml` file to update the UAA_PEM_PATH key value with uaa pem path.
8. Provide execution permissions to `utility.sh` file by running the following command: `$sudo chmod +x utility.sh`
9. 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
Unable to access Plant Applications Enterprise Edition Web Client. 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 Edition 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.	1. Access the following URLs: • https://<Enterprise Edition Web Client node IP address or system name>:5059/443 • https://<Enterprise Edition Web Client node IP address or system name>:5051/ A message appears to accept the insecure URL to proceed. Choose to do so. 2. Select **Not Secure** in the address bar. A **Certificate** window appears. 3. Import the certificate and add it to your trusted store. 4. Refresh the Plant Applications Enterprise Edition Web Client window.

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

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

Unable to access the Enterprise Edition Web Client after successful installation, and Haproxy service logs displays the following errors:
[NOTICE] (6) : haproxy version is 2.5.1-86b093a
[NOTICE] (6) : path to executable is /usr/local/sbin/haproxy
[**ALERT**] (6) : [haproxy.main()] Cannot raise FD limit to 8251, limit is 1024
Note: This issue is specific to the Web Client that runs on Amazon Linux OS.
	1. Modify `/etc/sysconfig/docker`
	`OPTIONS=”--default-ulimit nofile=1024:4096”`
	Replace with
	`OPTIONS=”--default-ulimit nofile=10000:15000”`
	2. Restart the docker.

Issue	Resolution
While installing the Enterprise Web Client, the system did not display the progress of the installation and displayed the following errors: `awk: options '-W interactive' unrecognized, ignored` `awk: options '-W interactive' unrecognized, ignored` `awk: options '-W interactive' unrecognized, ignored`	If the Linux machine has multiple **awk** versions available, then switch to **mawk** by typing the following command: `sudo update-alternatives --config awk.`. This command lists the available **awk** versions, and you must select the **mawk** version only. **Note:** If the installer does not show any progress, then open another console and navigate to the `plantapps-enterprise-webclient-2022` directory and refer to the log by typing the following command in the installer path: `tail -f log/ansible.log`.

Restart Services for Enterprise Edition Plant Applications Web Client

When an application or a service encounters an error, you can stop and restart by running the commands.

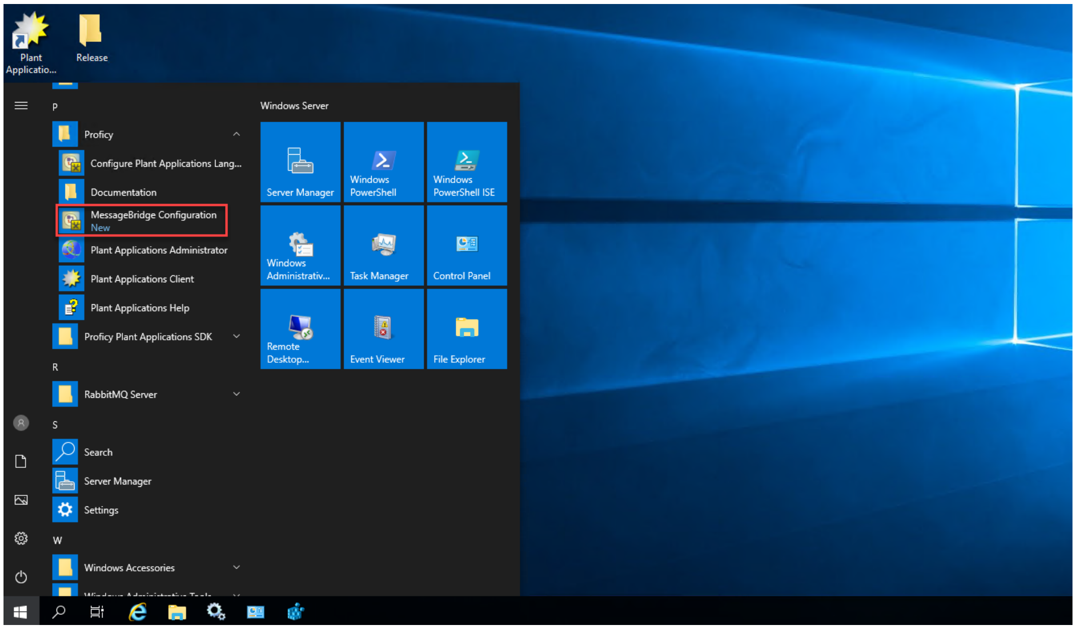
1. Log in to the system where the Plant Applications Web Client is installed.
2. To stop a particular service, type the following command: `$ docker service scale <Service Name> = 0`. For example, to stop the work order service, the command is `$ docker service scale PAworkorder_workorder=0`.
3. To restart a particular service, type the following command: `$ docker service scale <Service Name> = 1`. For example, to restart the work order service, the command is `$ docker service scale PAworkorder_workorder=1`.
   For more information, see https://docs.docker.com/engine/reference/commandline/service_scale/.

Chapter 7. Post Installation Configuration (Enterprise and Standard)

Run the Message Bridge Configuration Utility

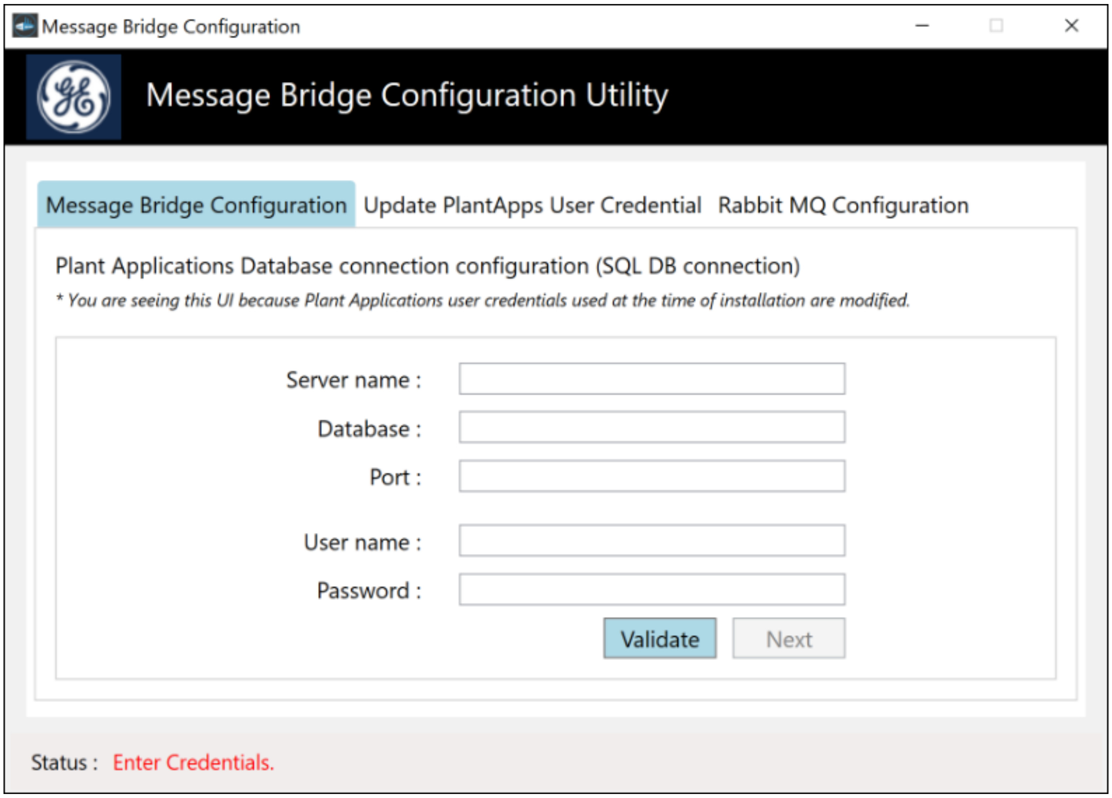
The Message Bridge Configuration Utility bridges the Plant Applications Server and the Plant Applications Web Client with the Kafka server details.

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



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

   The Plant Applications Database Credentials page appears only when you are accessing the utility for the first time.


Message Bridge Configuration
Message Bridge Configuration Utility
Message Bridge Configuration
Update PlantApps User Credential
Rabbit MQ Configuration
Server name :
Database :
Port :
User name :
Password :
Validate
Next

Plant Applications Database connection configuration (SQL DB connection)

** You are seeing this UI because Plant Applications user credentials used at the time of installation are modified.*

Status : Enter Credentials.

3. Select the **Message Bridge Configuration** tab, and then 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.

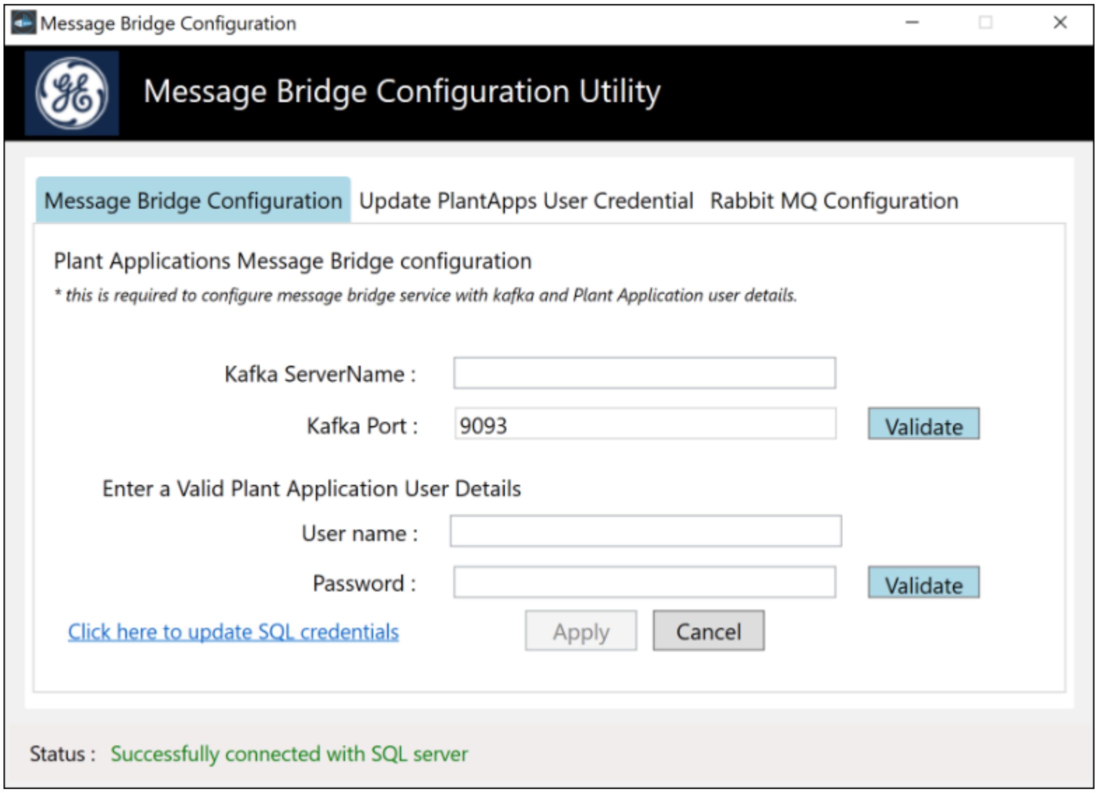
Credential	Description
Server name	Enter the server name where the SQL database is installed.
Database	Enter the name of the Plant Applications database that you want to connect with the Plant Applications Web Client.
Port	Enter the number of the port that the instance uses to listen for client connections. This field is optional. **Note:** The default port is 1433.
Username	Enter the user name that has permissions to access the database you entered in the **Database** field.
Password	Enter the password.

4. Select **Validate** to validate the database connection.

When the database connection is successfully validated, the Message Bridge Configuration Utility displays the message: `Successfully authenticated` and the **Next** button is enabled.

5. Select **Next**.

   You will be prompted to enter the Plant Applications Message Bridge configuration details.


Message Bridge Configuration
Message Bridge Configuration Utility
Message Bridge Configuration
Update PlantApps User Credential
Rabbit MQ Configuration
Validate
Validate
Click here to update SQL credentials
Apply
Cancel

Plant Applications Message Bridge configuration

* this is required to configure message bridge service with kafka and Plant Application user details.

Kafka ServerName :

Kafka Port : 9093

Enter a Valid Plant Application User Details

User name :

Password :

Status : Successfully connected with SQL server

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 server name where the Plant Applications Web Client is installed.
Kafka Port	Enter the Kafka port number. **Note:** The default port number is 9093. • **Enterprise Installation**: The default port number is always 9093. • **Standard Installation**: The port number is available in the `server.properties` file located at `<Installation_directory>\Kafka\config`. For example, `C:\Kafka\config\server.properties`.

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.

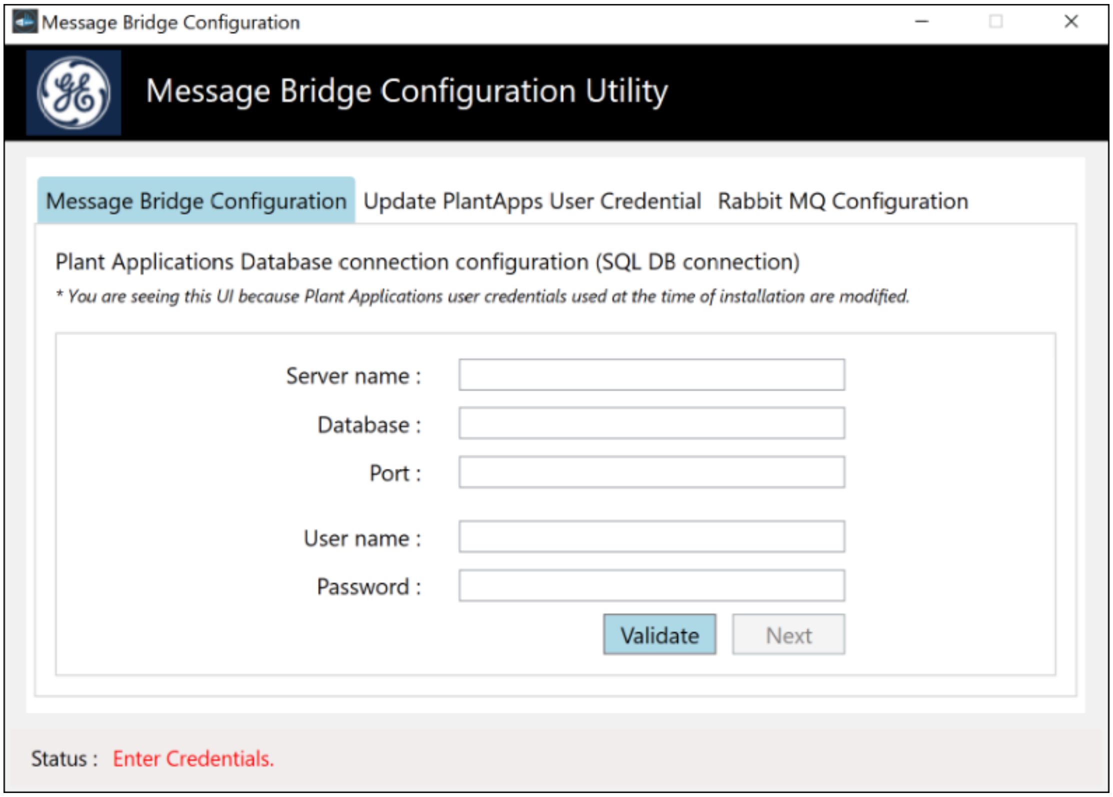
Credential	Description
User Name	Enter the Plant Applications login user name.
Password	Enter the password.
Validate	Select to validate the Plant Applications Administrator credentials.

8. When 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.



Message Bridge Configuration

Message Bridge Configuration Utility

Message Bridge Configuration
Update PlantApps User Credential
Rabbit MQ Configuration

Plant Applications Database connection configuration (SQL DB connection)

** You are seeing this UI because Plant Applications user credentials used at the time of installation are modified.*

Server name :

Database :

Port :

User name :

Password :

Status : Enter Credentials.

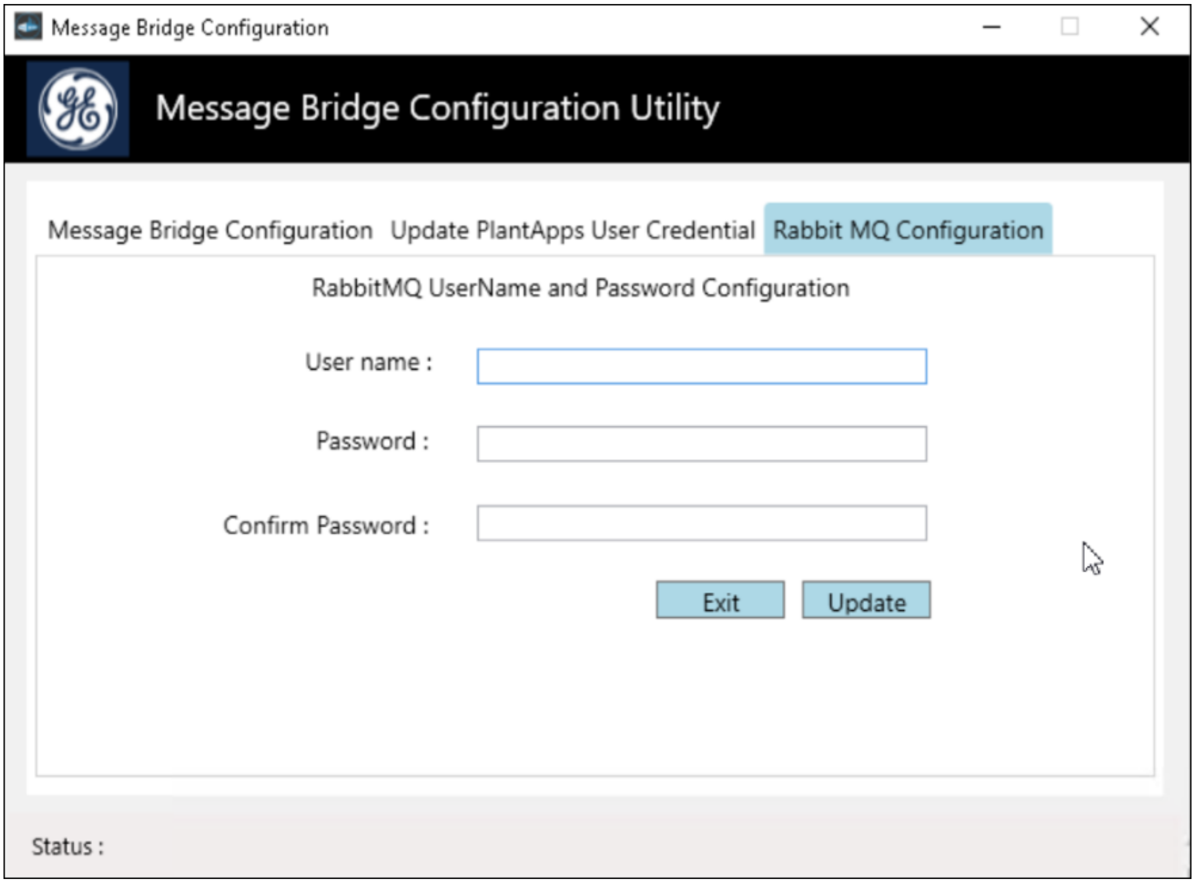
Credential	Description
User Name	Enter the user name for an administrator account in Plant Applications.
Password	Enter the password.

Credential	Description
Update	Select to update the Plant Applications Administrator credentials for Message Bridge service.

Update Rabbit MQ Credentials

Use this tab only to update the Rabbit MQ credentials if you have modified the Rabbit MQ credentials.

1. In the **Update Rabbit MQ Credentials** tab, enter the Rabbit MQ credentials as described below.


Message Bridge Configuration
Message Bridge Configuration Utility
Message Bridge Configuration
Update PlantApps User Credential
Rabbit MQ Configuration
RabbitMQ UserName and Password Configuration
User name :
Password :
Confirm Password :
Exit
Update
Status :

Credential	Description
User name	Enter the Administrator's user name that you set during Plant Applications server installation.
Password	Enter the password.
Confirm Password	The password that the user must enter to confirm the value in the **Password** field.

2. Select **Update** to update the Rabbit MQ credentials.

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 the Plant Applications REST APIs

The Plant Applications Web Client provides a Swagger-based UI to view and run the Representational State Transfer (REST) APIs.

You can access the UI from the list of supported Web browsers by entering a URL in the following format: `https://<server_name>:<port_number>/<micro_service_name>/swagger-ui.html`.

Where:

- `<server_name>`: Represents the name of the server on which the Plant Applications Web Client is installed.
- `<port_number>`: Represents the network port used by the Plant Applications Web Client.

  Note:

  By default the Web Client installs on port 443. When port 443 is not available, then the Web Client tries to install on port 5059.

  If the Web Client is running on 443, then you do not need to specifically provide the port number in the URL. For example, `https://<server_name>/<micro_service_name>/swagger-ui.html`.

  If the Web client is running on 5059, then you must provide the port number in the URL. For example, `https://<server_name>:5059/<micro_service_name>/swagger-ui.html`.

- `<micro_service_name>`: Represents the name of the microservice for which you want to run the REST APIs. The microservice and the corresponding applications where you can run the microservice are listed in the following table.

Microservice
`access-control-service`
`activities-app-service`
`activities-service`
`alarm-app-service`
`alarm-service`
`analysis-uapp`
`approval-cockpit-app-service`
`approval-cockpit-service`
`assignment-service`
`bom-management-app-service`
`comment-app-service`
`comment-service`
`document-management-service`
`downtime-app-service`
`downtime-service`
`erp-export-service`
`erp-import-service`
`erp-scheduler-service`
`erp-transformation-service`
`esignature-app-service`
`esignature-service`
`external-config-app-service`
`external-config-service`
`gateway-service`
`labor-service`
`mes-dataservice`
`mes-service`
`mymachines-service`

Microservice
`nonconformance-app-service`
`nonconformance-service`
`operator-app-service`
`pa-mymachines-service`
`plant-execution-service`
`process-order-service`
`processanalyzer-app-service`
`product-service`
`productionmetrics-app-service`
`productionmetrics-service`
`productionscheduler-app-service`
`property-definition-app-service`
`property-definition-service`
`reasons-service`
`receiving-inspection-app-service`
`receiving-inspection-service`
`route-app-service`
`route-service`
`security-administration-app-service`
`security-service`
`segments-definition-service`
`spc-app-service`
`supervisor-app-service`
`time-booking-app-service`
`usersettings-service`
`waste-management-app-service`
`waste-management-service`
`webgenealogy-app-service`
`work-order-history-service`
`work-order-service`

1. Access the following URL: `https://<server name of web client>:<port number>/<application service name>/swagger-ui.html`
   - **For Workorder Service**: `https://webclientservername:5059/workorder-service/apidocs/index.html`
   - **For Esignature-app-service Service**: `https:// webclientservername:<port>/esignature-app-service/swagger-ui/`

   The Swagger UI appears.

2. **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.

3. Select **Authorize**.
   You will be prompted to enter the client ID and client secret.

4. Enter the following values, and select **Authorize**:

Field	Description
User Name	Enter the Plant Applications login user name.
Password	Enter the Plant Applications login password.
client_id	Enter a client id value that was used during the installation. By default <node name of Plant Applications Web Client>_mes.
client_secret	Enter the password. This password is set during the Web Client installation.

Note: If you are not able to see the username and password fields, refer to Swagger URL Authorization Issue.

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

Important:

The following REST API microservices are deprecated. These REST API microservices will be permanently removed in the future release.

- In `mes-service`:
    - `GET /downtime/v1/downtimeRecords`
    - `GET /downtime/v1/downtimeRecords/{id}`
    - `GET /downtime/v1/downtimeStatistics`
    - `GET /downtime/v1/faults`
    - `GET /downtime/v1/faults/{id}`

Configure a Proficy Historian Server for the Analysis Application

This topic describes how to configure Proficy Historian servers for the Analysis application so that you can plot Historian tags. The Analysis application supports plotting of Historian tags from Proficy Historian versions 8.1 SIM 1, SIM2, SIM3, and 9.1.

Note: The Analysis application does not support plotting of Historian tags from Proficy Historian 9.0 version.

You can configure a maximum of 10 remote or native Historian servers in the `application.properties` file for the Analysis application.

1. Based on your type of installation, perform one of the following steps:
    - **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.

2. In the `historian-config-prod.properties` file, enter the properties and their details for each Proficy Historian 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 connection issues. For example, if you have entered FQDN for the `hist<n>.service.origin` property, use the FQDN format for the `hist<n>.service.hostname` and `hist<n>.uaa.origin` properties as well.

Property	Description
`hist<n>.service.origin`	Enter the IP address, FQDN, or host name of the Proficy Historian server.
`hist<n>.service.port`	Enter the port number on which the Proficy Historian server is installed. **Tip:** You can leave this property blank if the Proficy Historian server is installed on the default port 8443.
`hist<n>.service.hostname`	Enter the IP address, FQDN, or host name of the Proficy Historian server as configured in Plant Applications Administrator. For example, `GESERVER`. **Note:** The IP address, FQDN, or host name must match with the **Server Name** configured in the **Historian Connections** page of Plant Applications Administrator.
`hist<n>.service.client_id`	Enter the client id of the Historian Administrator. • Historian 7.0: **admin** is the default value. • Historian 8.0 or later: **<hostname>.admin** is the default value, where the host name is the server's name where Historian Web-based Clients are installed.
`hist<n>.service.client_secret`	Enter the client secret of Historian Administrator.
`hist<n>.uaa.origin`	Enter the IP address, FQDN, or host name of the UAA server.
`hist<n>.uaa.port`	Enter the port number on which the UAA server is installed.

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

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

3. Save the changes to your file.

4. 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-service` 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.

1. **Enterprise Installation:** In the directory `<Installation_Directory>/PlantApplicationsDocker/plantapps-web-docker`, access the `env.yml` file by using the vi editor.
2. **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.
3. Below is the list of cache properties with default values pertaining to the individual Plant Applications services. You can modify these default cache properties for a service based on your requirement.

Service Name	Properties
plantexecutionservice	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=**8h**
activities-service	maximum5MinCacheSize=100

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

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.

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.

For configuring LDAP or non LDAP users to Plant Applications Web Client, see Add a New User to the Plant Applications Web Client *(page 111)*.

Map LDAP Groups With Proficy Authentication

If you want LDAP users to use Proficy Authentication, you must map the corresponding LDAP groups with UAA group created during the Proficy product installation.

1. From your desktop, launch the Proficy Authentication application.
   The shortcut icon on your desktop is created after you install Proficy Authentication.
2. Select the **Identity Providers** tab.
   The **UAA/LDAP/SAML Connectivity Tool** appears.
3. Select the **Map Existing LDAP Groups** check box.
4. In the **UAA Connection** section, provide values as specified in the following table.

   ! **Important:** The values that you provide in this step must match the values that you provided while installing your Proficy product. These values are required to connect to Proficy Authentication. Proficy Authentication works only with a single instance of UAA, which is specified during Proficy Authentication installation. After installation, you cannot change the instance of UAA that Proficy Authentication will use.

Field	Description
URL	This information is read-only. The authorization server URL of the Proficy Authentication server is populated by default. This is the **UAA Base URL** that you specified during installation .
Client ID	Enter the client ID of the Proficy Authentication server that you specified for **Admin Client ID** during installation.
Client Secret	Enter the client secret configured for the OAuth client that you specified for **Admin Client Secret** during installation.

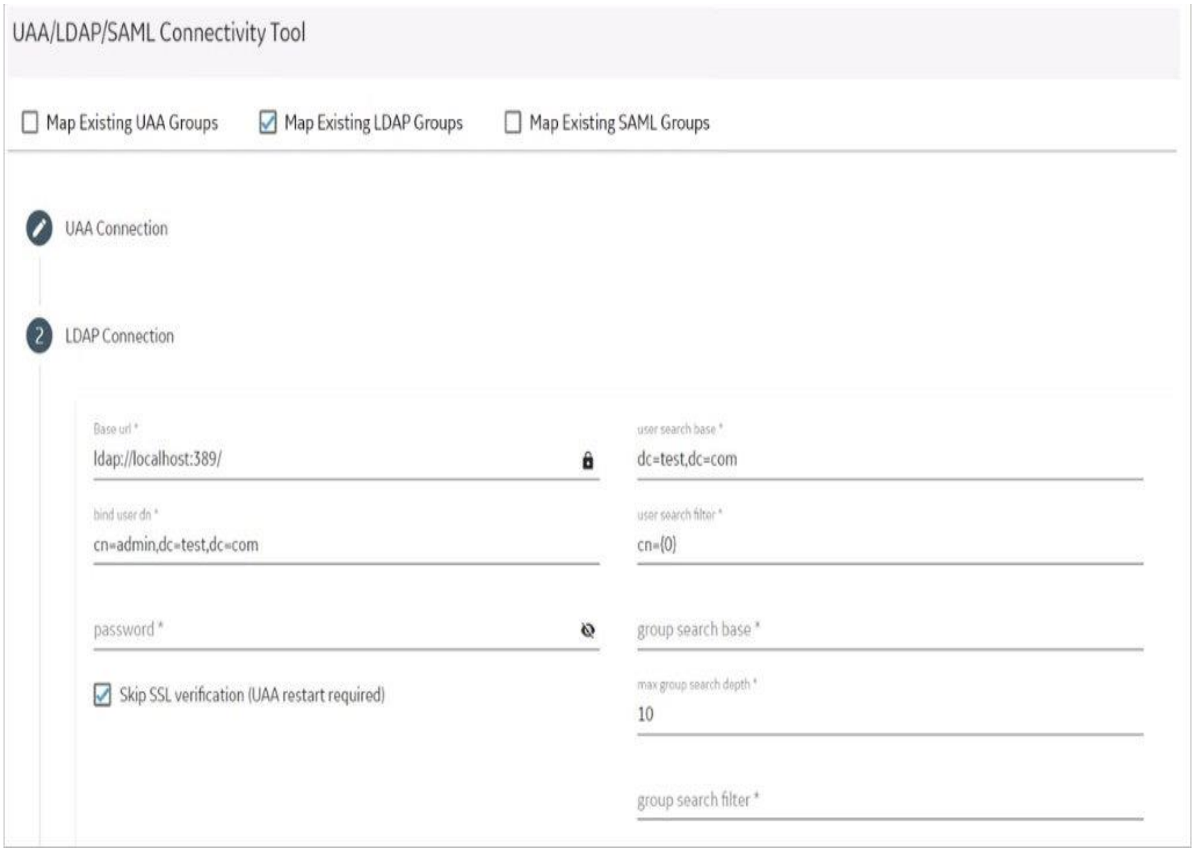
5. Select **Test**.

If connection to the Proficy Authentication server is established, a message appears, confirming the same.

Note: Currently, the **Test** button displays a successful connection for LDAP even when no security certificate, or a bad certificate is found.

6. In the **LDAP Connection** section, provide values as specified in the following table.

Field	Description
URL	Enter the base URL of the LDAP server (for example, https://localhost).
Bind User DN	Enter the distinguished name of the bind user (for example, cn=admin, ou=Users, dc=test, dc=com).
Password	Enter the password for the LDAP user ID that searches the LDAP tree for user information.
Skip SSL Verification (UAA restart required)	Select this check box if you do not have the certificate to access the LDAP server. Messages are still encrypted, but the certificate is not verified for correctness. Do not select this option if you are not confident of the direct connection to the LDAP server; it could result in redirected traffic outside of your controlled network.
User Search Filter	Enter the subdirectories to include in the search (for example, cn={0}).
User Search Base	Enter the starting point for the LDAP user search in the directory tree (for example, dc=developers,dc=com).
Group Search Base	Enter the starting point for the LDAP group search in the directory tree (for example, ou=scopes, dc=developers, dc=com).
Max Group Search Depth	Enter a value to define the maximum depth for searching LDAP groups. (This may impact performance for very large systems.) By default this value is 10.
Group Search Filter	Enter the subdirectories to include in the search (for example, member={0}).



UAA/LDAP/SAML Connectivity Tool

☐ Map Existing UAA Groups ☑ Map Existing LDAP Groups ☐ Map Existing SAML Groups

UAA Connection

2 LDAP Connection

Base url *: ldap://localhost:389/

user search base *: dc=test,dc=com

bind user dn *: cn=admin,dc=test,dc=com

user search filter *: cn={0}

password *

group search base *

☑ Skip SSL verification (UAA restart required)

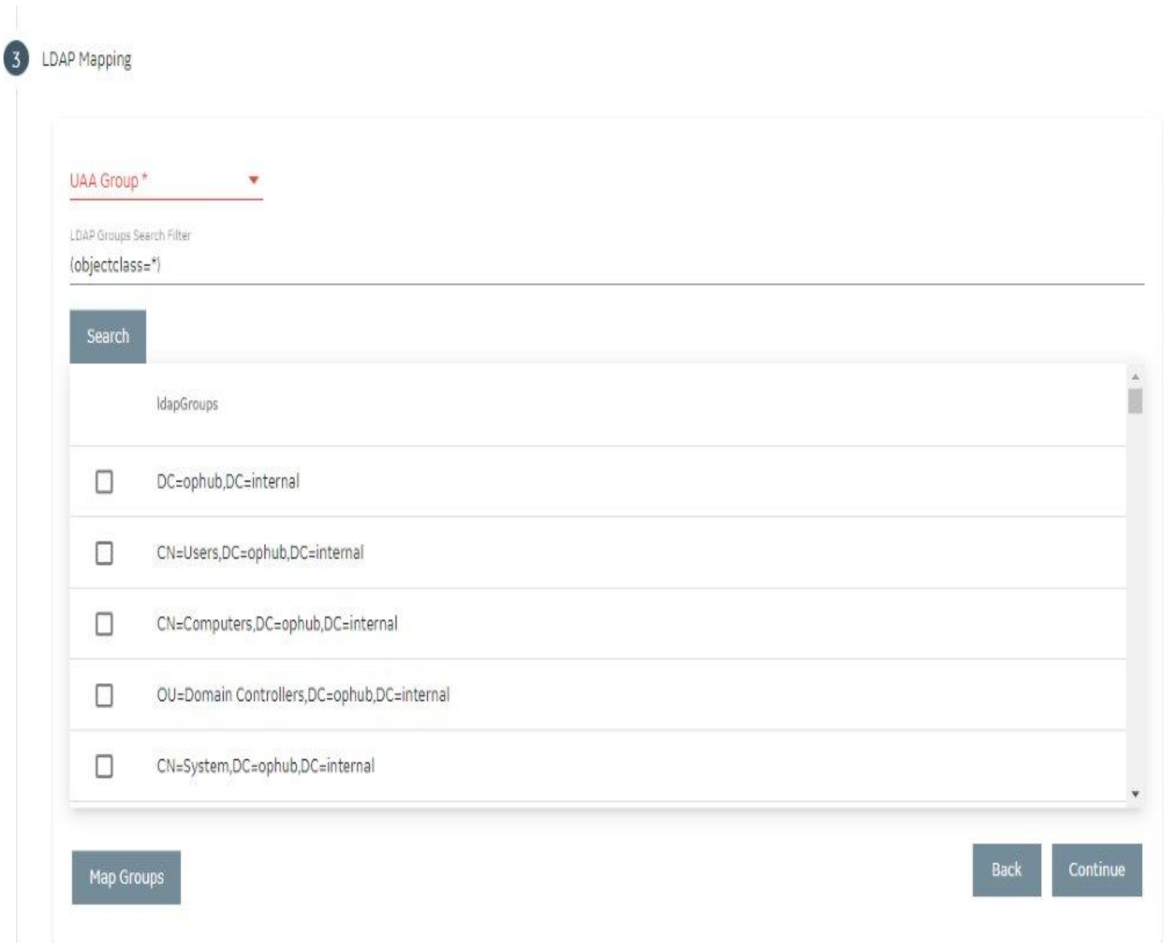
max group search depth *: 10

group search filter *

7. Select **Test**, and then select **Submit**.
   If connection to the LDAP server is established, a message appears, confirming the same.

8. Select **Test** again, and then select **Continue**.
   In the **LDAP Mapping** section, the drop-down list box contains a list of groups in Proficy Authentication.

9. In the drop-down list box, select the Proficy Authentication group to which you want to map LDAP groups. You can also search for a group in the **LDAP Groups Search Filter** box. When searching, be sure to use the standard LDAP query language for your search.



LDAP Groups Search Filter: (objectclass=*)

	ldapGroups
□	DC=ophub,DC=internal
□	CN=Users,DC=ophub,DC=internal
□	CN=Computers,DC=ophub,DC=internal
□	OU=Domain Controllers,DC=ophub,DC=internal
□	CN=System,DC=ophub,DC=internal

Note: If a group is already mapped to the Proficy Authentication group that you have selected, the check box is already selected.

10. Select **Map Groups**.
    A message appears, confirming that the LDAP groups are mapped to the Proficy Authentication group.
11. Repeat steps 8-10 for all the Proficy Authentication groups that you want to map.

The LDAP groups are mapped with the Proficy Authentication (UAA) groups.

Warning: Any change in the configured details for LDAP impacts its connectivity. Make sure to update the connectivity screens to reflect the changes.

Add a New User to the Plant Applications Web Client

Previously, when a user logged into the Web Client for the first time, the user was not added to Plant Applications Administrator automatically. Now, when a new user who is part of a UAA group and has access to Plant Application Web Client applications will be automatically created in Plant Applications. For providing access to a Plant Application Web Client Application, see Add or Delete Applications from Groups *(page 116)*. However, a Role-based user is created by default with timestamp as password. Hence, the user cannot be added to any group and is not able to login into Plant Applications Administrator or Plant Applications Thick Client.

Use this procedure to create a user and provide access to the Plant Applications Web Client.

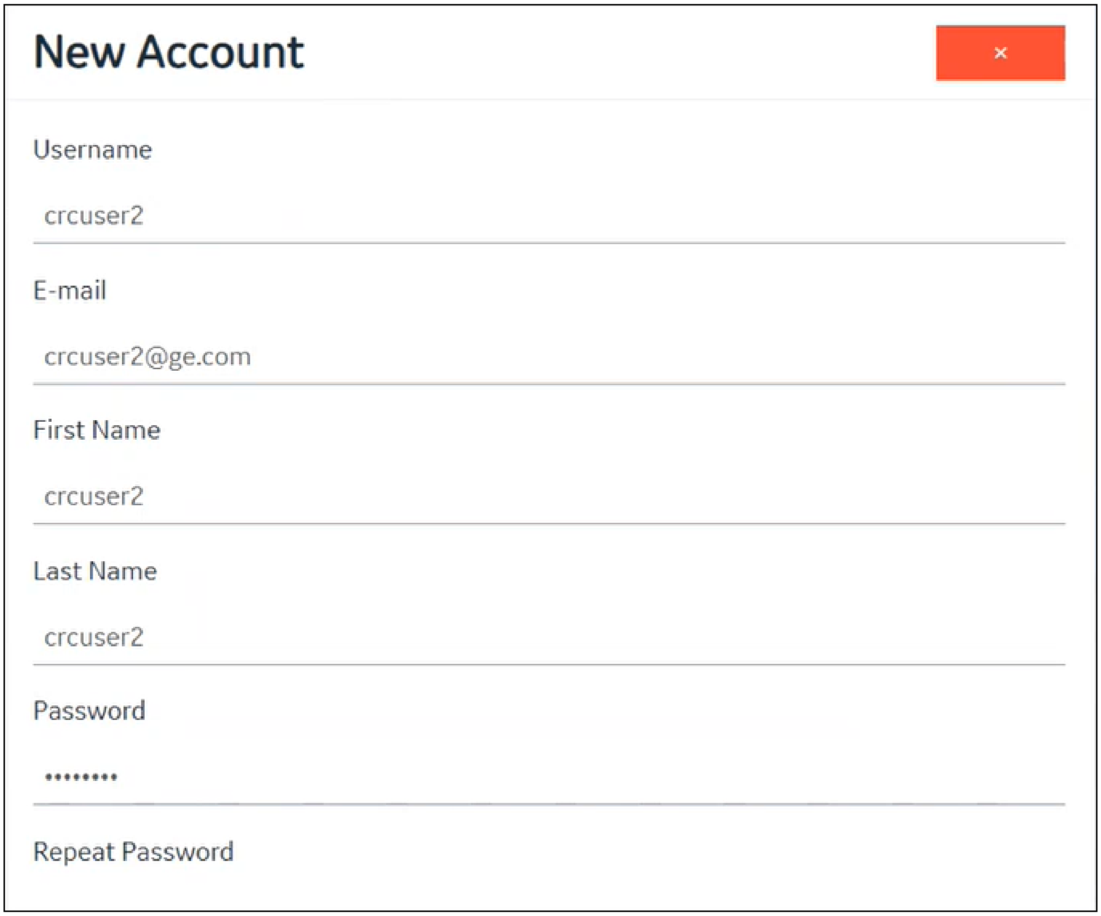
User required to login to Plant Applications can be a part of an LDAP server group or a UAA group (non-LDAP user). The mapping management of LDAP and non LDAP users can be done using the UAA/LDAP/SAML Connectivity Tool.

For LDAP user, see Map LDAP Groups With Proficy Authentication *(page 107)*.

When a new user (non-LDAP) logs into the application for the first time, the user credentials are created in the Plant Applications Administrator. However, you must update user properties in the **Edit User** page.

1. Log in to `https://OpshubHostname/iqp` or the Operations Hub designer page using Operations Hub Admin credentials.
2. From the main navigation menu, select **Manage**, and then select **App users**.

   The **New Account** page appears.



New Account

Username

crcuser2

E-mail

crcuser2@ge.com

First Name

crcuser2

Last Name

crcuser2

Password

••••••••

Repeat Password

3. Enter the required information in the following fields.

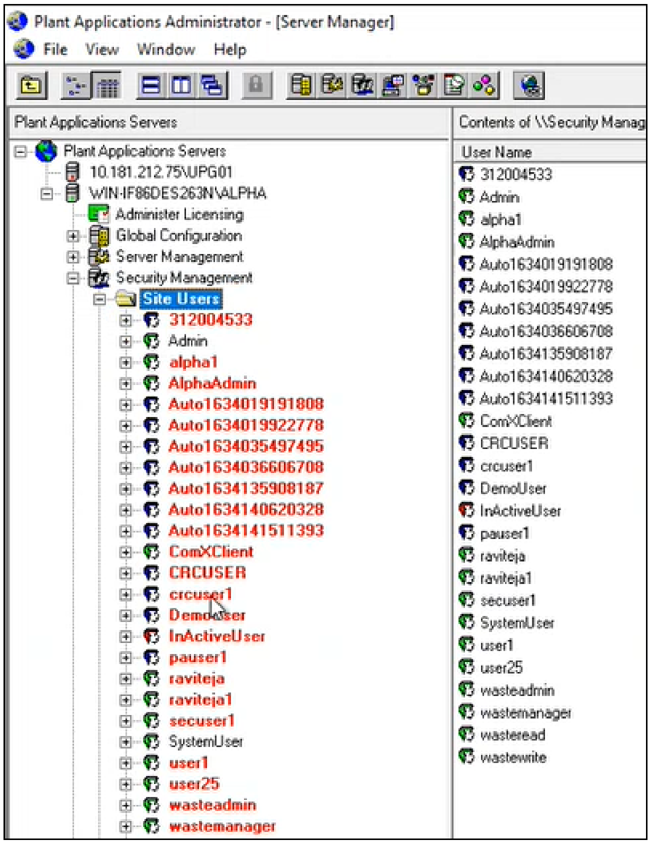
Field	Description
Username	Enter the user name the user will use to log in to Operations Hub. The value must be unique.
E-mail	Enter the email ID of the user. The value must be unique.
First Name	Enter the first name.
Last Name	Enter the last name.
Password	Enter a password that the user will use to log in to Operations Hub.
Repeat Password	Enter the password to confirm.
Groups	Select the UAA group that you want to assign to this user. Select **iqp.user**.
Apps	Select **Plant Applications** and other applications you want the user to have access to.

4. Select **Create**.

5. Log in to the Plant Application Web Client with the newly created user.

   Note: At this point, this user in Plant Applications Web Client is created automatically in Plant Applications but as a role-based user. Hence, the user cannot log in to Plant Applications Thick Client. To allow this user to log in successfully to Plant Applications Thick Client, you must follow additional steps.

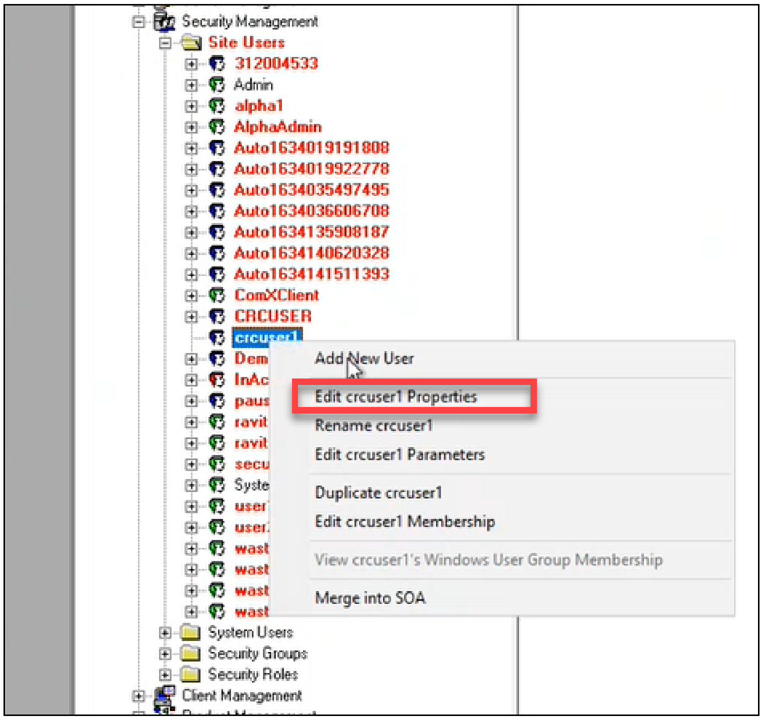
6. Log in to the **Plant Applications Administrator - [Server Manager]**.


Plant Applications Administrator - [Server Manager]
File
View
Window
Help
Plant Applications Servers
Contents of \\Security Manag
User Name

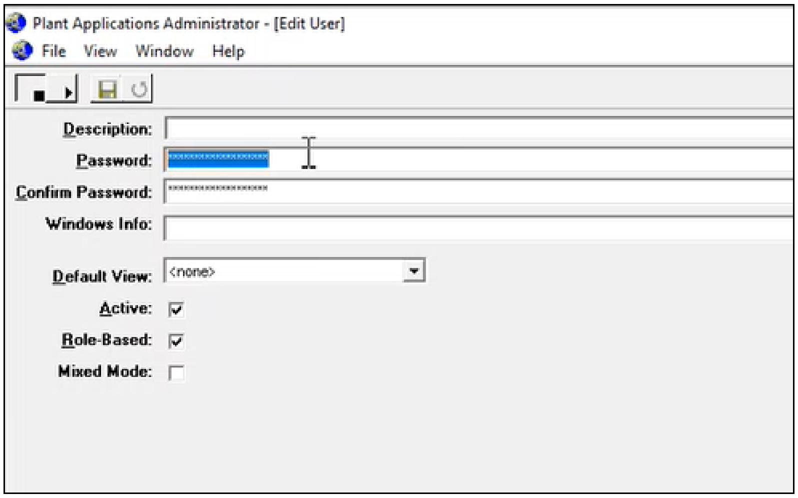
- Plant Applications Servers
  - 10.181.212.75\UPG01
  - WIN-IF86DES263N\ALPHA
    - Administer Licensing
    - Global Configuration
    - Server Management
    - Security Management
      - Site Users
        - 312004533
        - Admin
        - alpha1
        - AlphaAdmin
        - Auto1634019191808
        - Auto1634019922778
        - Auto1634035497495
        - Auto1634036606708
        - Auto1634135908187
        - Auto1634140620328
        - Auto1634141511393
        - ComXClient
        - CRCUSER
        - crcuser1
        - DemoUser
        - InActiveUser
        - pauser1
        - raviteja
        - raviteja1
        - secuser1
        - SystemUser
        - user1
        - user25
        - wasteadmin
        - wastemanager

User Name
312004533
Admin
alpha1
AlphaAdmin
Auto1634019191808
Auto1634019922778
Auto1634035497495
Auto1634036606708
Auto1634135908187
Auto1634140620328
Auto1634141511393
ComXClient
CRCUSER
crcuser1
DemoUser
InActiveUser
pauser1
raviteja
raviteja1
secuser1
SystemUser
user1
user25
wasteadmin
wastemanager
wasteread
wastewrite

7. Under **Security Management**, from the list of users, select the user you created in Operations Hub, and then right-click, and select **Edit <user name> Properties**.



The **Edit <user name> Properties** page appears.



Description:

Password: ******************

Confirm Password: ******************

Windows Info:

Default View: <none>

Active: ☑

Role-Based: ☑

Mixed Mode: □

8. Do the following:
   a. In the **Password** field, update the password. By default, the password is displayed in the timestamp format.
   b. Clear the **Role-Based** checkbox.

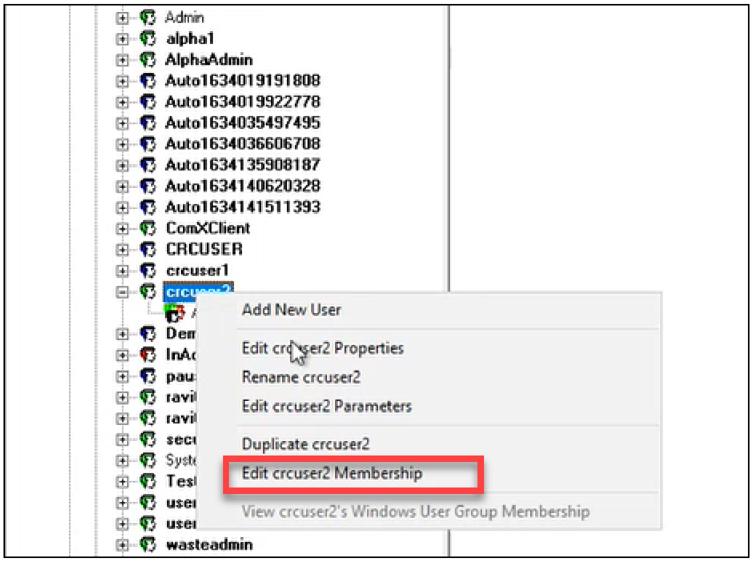
Note: For LDAP users, you must update the **WindowsUser Info** field in **Users_Base** column in SQL directly. For example, update **Users_Base** for the following details: `SET WindowsUserInfo = ‘xyzdomain.com\pa22user1’`, where Username = ‘pa22user1’

Note: For the first-time login, the LDAP user must log in to the Plant Applications Thick Client first and then log in to the Plant Applications Web Client.

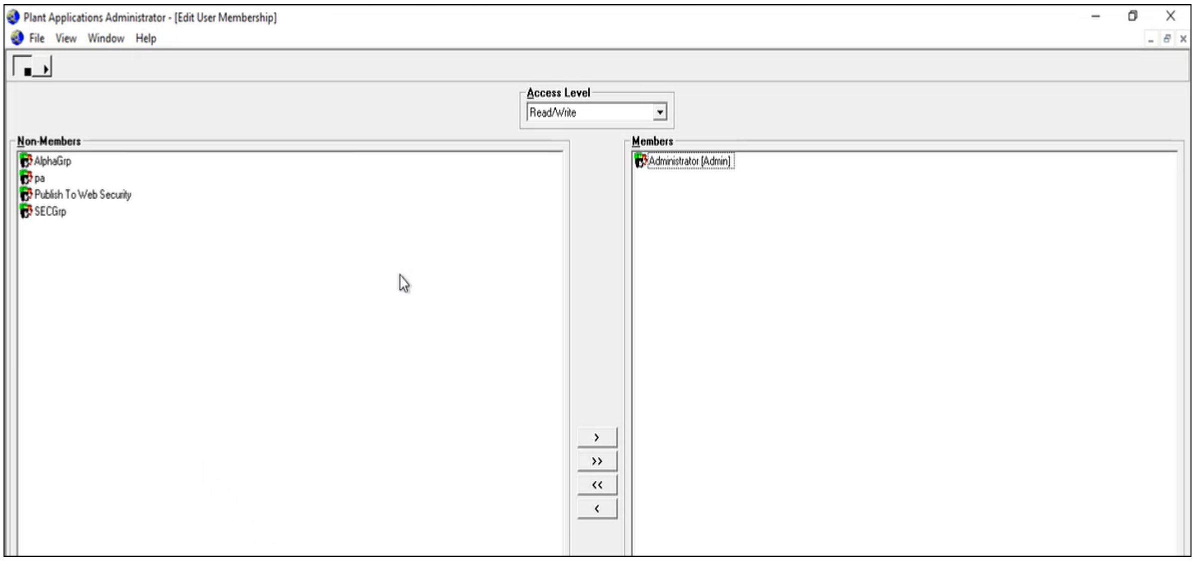
9. Select **Save**.

Note: From Step 9 onwards, the procedure is specific only to the security configuration.

10. Right-click on the user again, and then select **Edit <user name> Membership**.



11. Select the Security Groups you want the user to belong to, and then from the **Access Level** list, select the appropriate access level, for example, **Admin**, then select the right arrow to populate the **Member** column.


Plant Applications Administrator - [Edit User Membership]

Access Level: Read/Write

Non-Members: AlphaGrp, pa, Publish To Web Security, SECGrp

Members: Administrator [Admin]

12. Close the window.

Note: **Save** operation is not required.

Add or Delete Applications from Groups

When an application is added to the group, the users in the group can access the application.

1. Select **Groups**.
   The **Groups** page appears displaying the list of groups.

2. Select ✎ in the row containing the group you want to modify.
   The **Members** page appears, displaying the members added to the group.

3. Select **Applications**.

4. To add applications to the group perform the following steps:

   a. Select the applications you want to add to the group from the **Search for Applications to add them to this group** drop-down list box.

      Note: You can select multiple applications.

   b. Select +.

   The applications are added to the group. The count of total applications of the group is updated.

5. To delete applications from the group, select × in the row containing the group you want to delete.
   The applications are deleted from the group. The count of the total applications of the group is updated.

Chapter 8. Configuration Manager for Plant Applications Web Client

Configuration Manager for Plant Applications Web Client

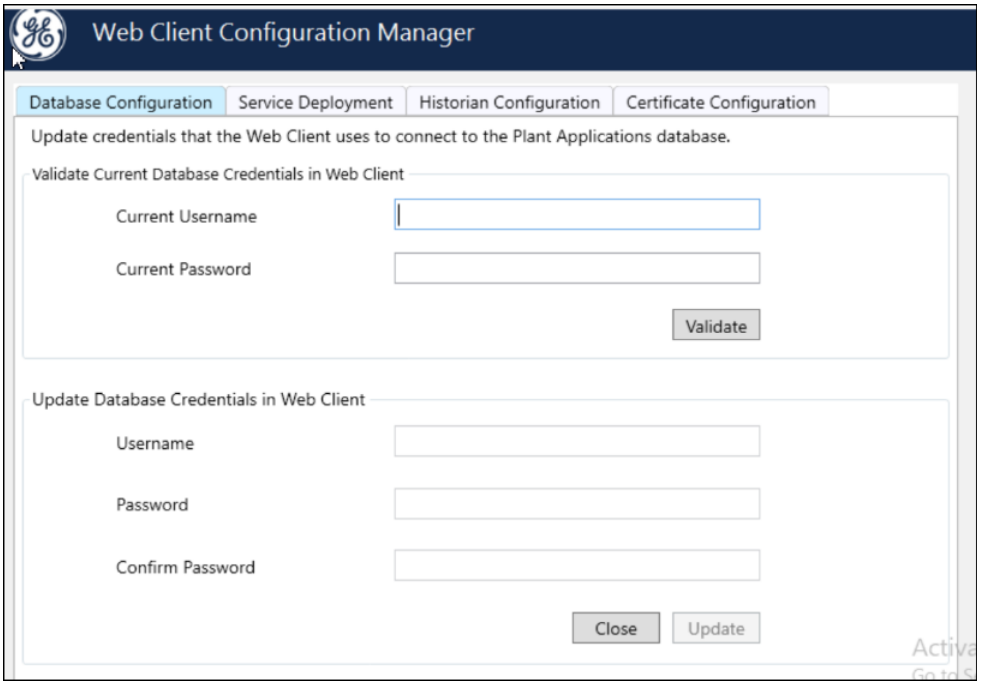
Use the Configuration Manager to update the following:

- Database passwords. See Update or Validate the Database Password *(page 117)*
- Service deployments. See Deploy and Configure .War Files *(page 118)*
- Historian configuration. See Update Historian Administrator Client Credentials *(page 119)*
- Certificate configuration. See Import Certificates *(page 121)*

Update or Validate the Database Password

This tab allows you to update the database password the Web Client uses to connect to the Plant Applications databases. You can also use this tab to validate the current database password.

You can validate or update the database credentials in the Web Client.



Update credentials that the Web Client uses to connect to the Plant Applications database.

Web Client Configuration Manager
Database Configuration
Service Deployment
Historian Configuration
Certificate Configuration
Validate Current Database Credentials in Web Client
Current Username
Current Password
Validate
Update Database Credentials in Web Client
Username
Password
Confirm Password
Close
Update

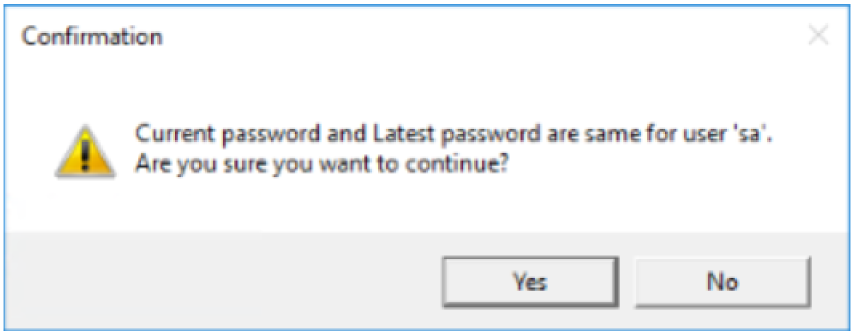
1. To validate the current credentials in the Web Client, do this:
    a. Enter the **Current Username** and **Current Password** in the respective fields.

b. Select **Validate**.

If the details provided are valid, a `Successfully Validated` message appears.

2. To update the database credentials in the Web Client, do this:
   a. In the **Update Database Credentials in Web Client** section, enter the required information in the **Username**, **Password**, and **Confirm Password** fields.
   b. Select **Update**.

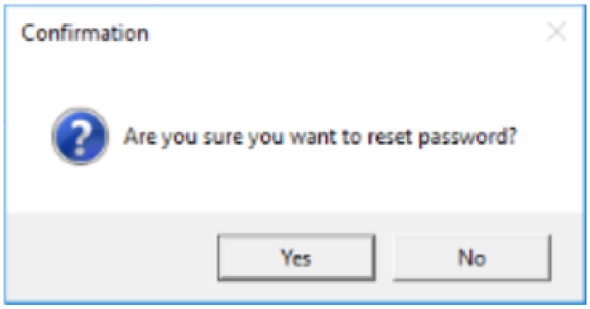
   If both the latest and current passwords are the same, a confirmation message appears.


Confirmation

Current password and Latest password are same for user 'sa'.
Are you sure you want to continue?

   c. Select **Yes** to confirm.

   A confirmation message appears for resetting the password.


Confirmation

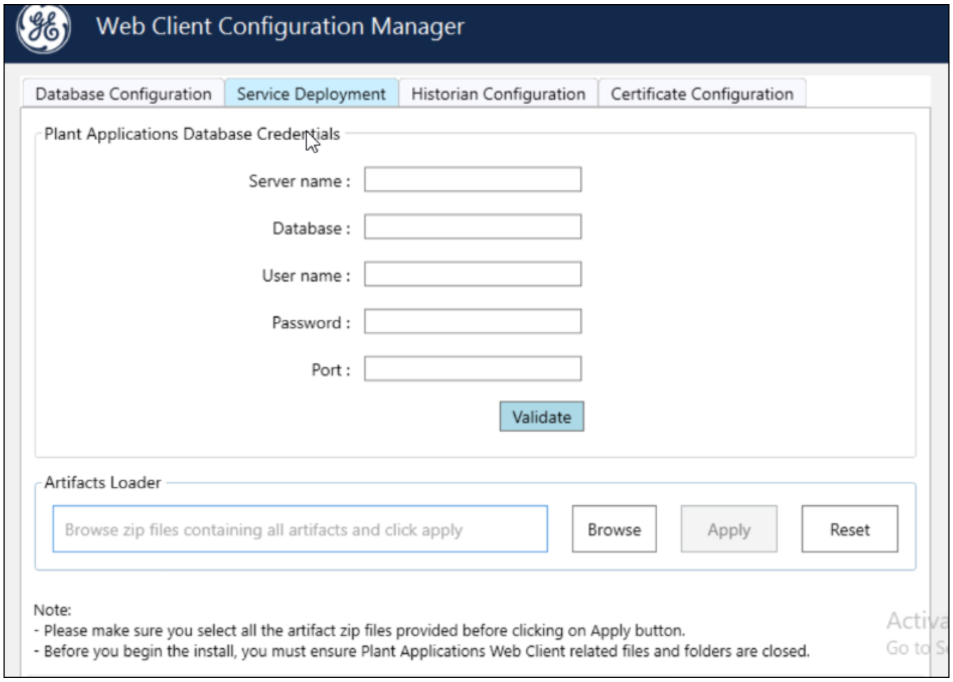
Are you sure you want to reset password?

   d. Select **Yes** to update all the `.war` files with the latest password.

The configuration process might take up to 15 minutes. When the password is successfully reset, the message appears: `Password is successfully reset`.

Deploy and Configure .War Files

This tab allows you to deploy and configure one or more `.war` files or node UI applications on a machine where the Web Client is already installed.



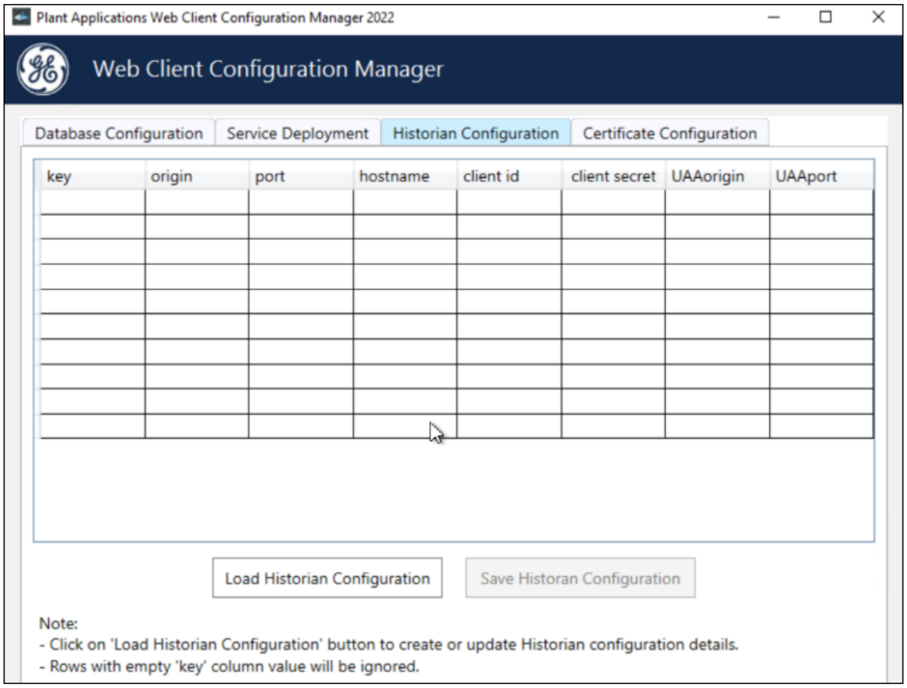
Note:
- Please make sure you select all the artifact zip files provided before clicking on Apply button.
- Before you begin the install, you must ensure Plant Applications Web Client related files and folders are closed.

1. Enter the required information in the fields for the Plant Applications Database credentials.
2. Select **Validate**.
3. In the Artifacts Loader section, select the services artifacts to modify, then select **Browse** to select the zip file.
4. Select **Apply**.

   The configuration process might take up to 20 minutes. When the configuration is complete, a message with a log file hyperlink appears in the Status Bar at the bottom of the screen.

Update Historian Administrator Client Credentials

This tab allows you to update Historian administrator client credentials.


Plant Applications Web Client Configuration Manager 2022
Web Client Configuration Manager
Database Configuration
Service Deployment
Historian Configuration
Certificate Configuration
Load Historian Configuration
Save Historan Configuration

key	origin	port	hostname	client id	client secret	UAAorigin	UAAport

Note:
- Click on 'Load Historian Configuration' button to create or update Historian configuration details.
- Rows with empty 'key' column value will be ignored.

1. When you launch the utility, all admin client credentials are automatically fetched and populated in the table.

2. When data is not loaded in the table, select **Load Data** to load the configuration data.

3. Enter the Historian Server details, and then select **Save Data**. The utility performs the following:
   a. Encrypts Client Secret value.
   b. Writes all the Historian Server details into the mes-dataservice application properties file.
   c. After the Save Data operation, the table is refreshed with the updated details.

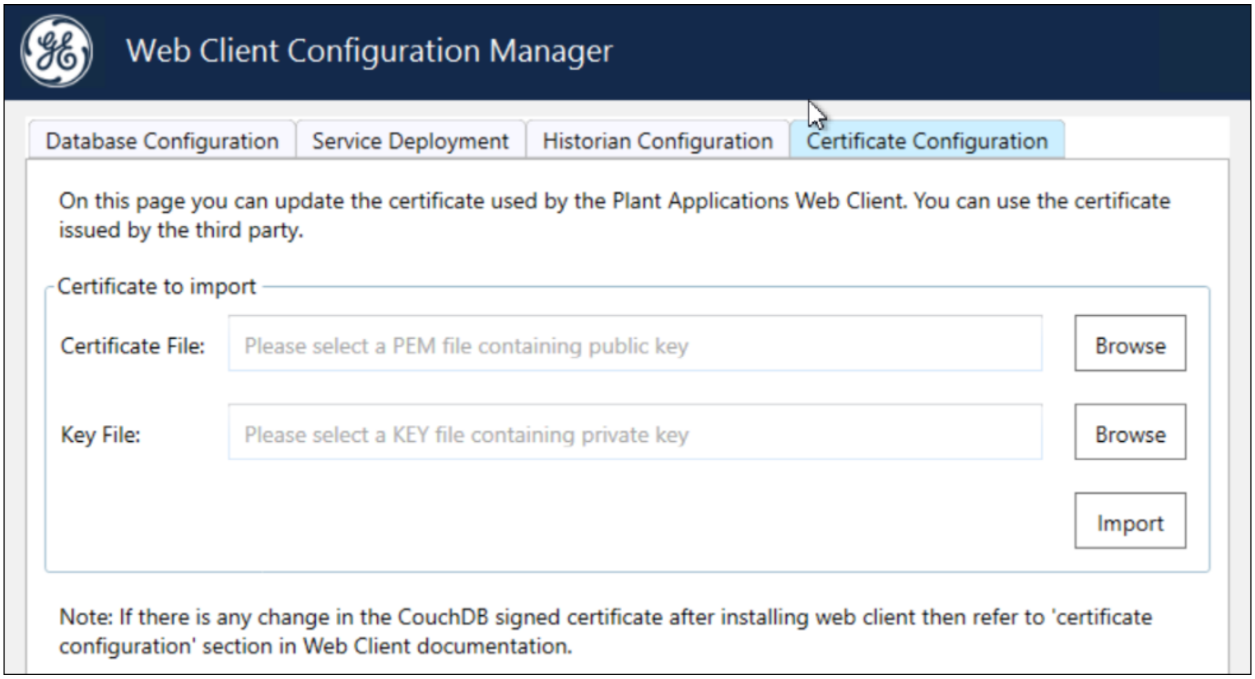
   Note:

   - If the `mes-dataservice` war file is not available in the Tomcat webapps directory, the table will be empty.
   - We recommend to follow the following steps when entering data into the table:
     a. The Key column cell value of a Row is a primary key and must be entered before values in any other cells of that Row.
     b. The Key column cell value of a Row must be a unique key. In case of duplicate key entry a validation error will occur and editing of any other cell will be disabled.

4. After saving the data, the Tomcat Application Manager automatically restarts the **mesdataservice-impl** and **analysis-uApp** services.

Import Certificates

This tab allows you to import the certificates.



On this page you can update the certificate used by the Plant Applications Web Client. You can use the certificate issued by the third party.

Certificate to import

Certificate File: Please select a PEM file containing public key

Key File: Please select a KEY file containing private key

Note: If there is any change in the CouchDB signed certificate after installing web client then refer to 'certificate configuration' section in Web Client documentation.

1. In the **Certificate File** field, select **Browse** to import the certificate file.
2. In the **Key File** field, select **Browse** to import the `Key` file.
3. Select **Import**.
   When the certificate import is successfull, a message appears in the Status bar at the bottom of the screen.

Chapter 9. Troubleshooting

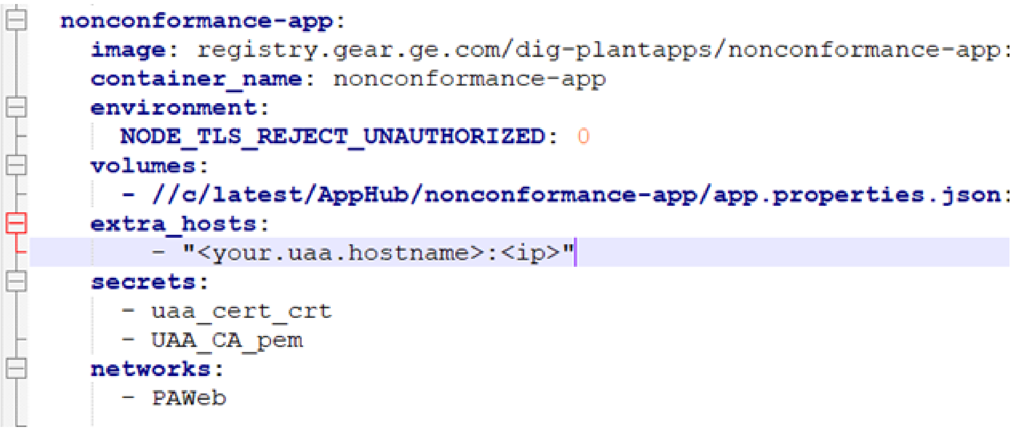
Troubleshoot Access Issues

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) Edition Web Client Logs

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

Access Enterprise (Linux) Edition 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 Edition 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 Edition 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 Edition 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 Edition 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 Edition 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 Edition 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 Edition 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, Proficy Authentication (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, Proficy Authentication (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.

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 wcserver, enter wcserver_mes.
client_secret	Enter the Plant Application API client secret that was used during the web client installation.

   The Proficy Authentication (UAA) login page appears.

2. In the Proficy Authentication (UAA) login page, enter the Proficy Authentication (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.key` files to the `<Webclient_Installation_path>\Service-Httpd\conf\cert` location.
5. Rename `server.crt` to `public.pem` and `server.key` to `key.pem`.
6. Start the **GE.PlantApps.Httpd** service.

Unable to log into Operations Hub

After installing the Plant Applications Web Client, if you try to log into Operations Hub with the following credentials:

- Operations Hub admin. The system redirects you to the Operations Hub login page.
- User. The system displays the following message:
    - `Access Denied`. Check the log file here: `{{install location}}/PlantApplicationsDocker/opshub-posting/mnt/log/opshub-posting.log.`

In the log file, if you find this error message: `Set user permission failed: Unable to get the UAA group Id.`, then restart the Operations Hub machine and post the Operations Hub Plug-in manually. See Post Applications into Operations Hub Manually *(page 128)*.

Post Applications into Operations Hub Manually

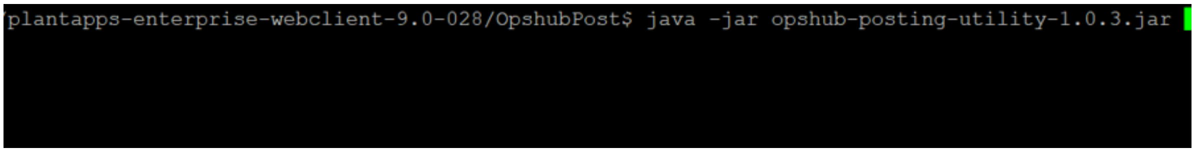
The Plant Applications 2022 Web Client installer can now post the applications into Operations Hub when installing.

When posting applications into Operations Hub fails, you can post them manually.

The `Operations_Hub_PostingUtility` directory within the installer has all the required files. One of the required files is the `application.properties` file. The `application.properties` file contains existing basic inputs. However, you must update the below properties in this file:

- opshub.tenant.password=
- proficyauthentication.admin.client.secret=
- proficyauthentication.client.secret=

1. Do the following: .
    - For Enterprise Web Client, navigate to this directory `{{Installer}}/OpshubPost/`.
    - For Standard Web Client, navigate to this directory `{{Installer}}/Operations_Hub_PostingUtility/`.
2. Update the `application.properties` file.
3. Run the `opshub-posting-utility-1.0.6.jar` with the following command: `java -jar opshub-posting-utility-1.0.6.jar`



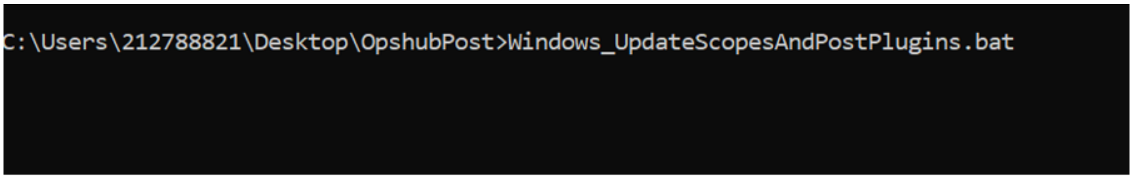
```
/plantapps-enterprise-webclient-9.0-028/OpshubPost$ java -jar opshub-posting-utility-1.0.3.jar
```

Create Clients, Scopes, User Groups and Post Applications into Operations Hub

Use this procedure to add the following when Operations Hub is reinstalled:

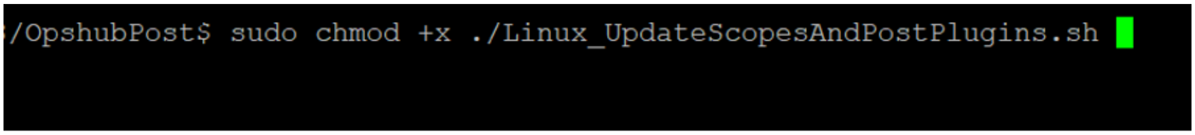
- Clients
- Scopes
- User Groups
- Applications

1. Do the following:
    - For Enterprise Web Client, navigate to this directory `{{Installer}}/OpshubPost/`.
    - For Standard Web Client, navigate to this directory `{{Installer}}/Operations_Hub_PostingUtility/`.
2. Update the `application.properties` file.
3. Do the following:
    - To run the script from Windows, navigate to the directory, and run this command: `Windows_UpdateScopesAndPostPlugins.bat`

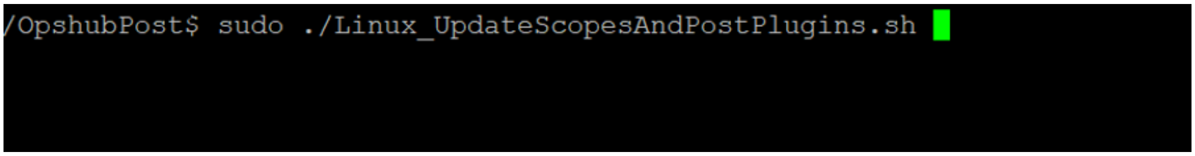
      ```
      C:\Users\212788821\Desktop\OpshubPost>Windows_UpdateScopesAndPostPlugins.bat
      ```

      To run the script from Linux, navigate to the directory, and run this comand: `Linux_UpdateScopesAndPostPlugins.sh`
4. Run the following command to give executable permissions: `sudo chmod +x ./Linux_UpdateScopesAndPostPlugins.sh`.



```
/OpshubPost$ sudo chmod +x ./Linux_UpdateScopesAndPostPlugins.sh
```

5. Run the `Linux_UpdateScopesAndPostPlugins.sh` script with the following command:
   `sudo ./Linux_UpdateScopesAndPostPlugins.sh`

   ```
   /OpshubPost$ sudo ./Linux_UpdateScopesAndPostPlugins.sh
   ```

About Renewing the Expired Self-Signed Certificate

When the self-signed certificate expires, you must renew it for validation. This is applicable only to the Standard version of the Plant Applications Web Client.

The high-level steps to renew the expired self-signed certificate are:

- Download and extract the files from the `UAASecrets.zip` folder, and then import the self-signed certificate to the Windows Trusted Store. See Import the Self-Signed Certificate to the Windows Trusted Store *(page 130)*
- Update IP.2, DNS.2, and DNS.3 in the `V3.txt` file. See Update V3 Txt *(page 132)*
- Update the CN in the `server.csr.cnf` file. See Update the Server.CSR.CNF File *(page 133)*
- Create certificates and keystore files. See Create Certificates and Keystore Files *(page 133)*
- Update the following services:
  - WorkOrder service
  - HTTPD service
  - Tomcat
  - Tomcat JRE keystore

  See Update Work Order, HTTPD, and Tomcat Services *(page 134)*

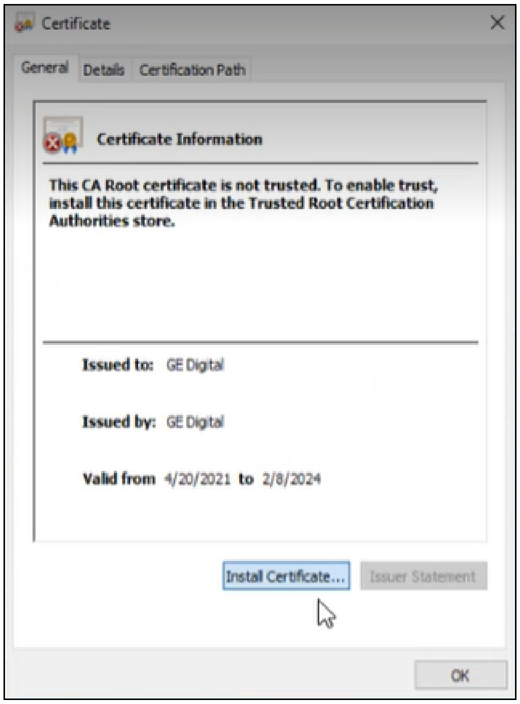
Import the Self-Signed Certificate to the Windows Trusted Store

1. Download the `UAASecrets.zip` folder.

2. Extract the files from the `UAASecrets.zip` folder.

3. In the `UAASecrets` folder, select and double-click the `UAA_CA.crt` file.

   The **Certificate** page appears.



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

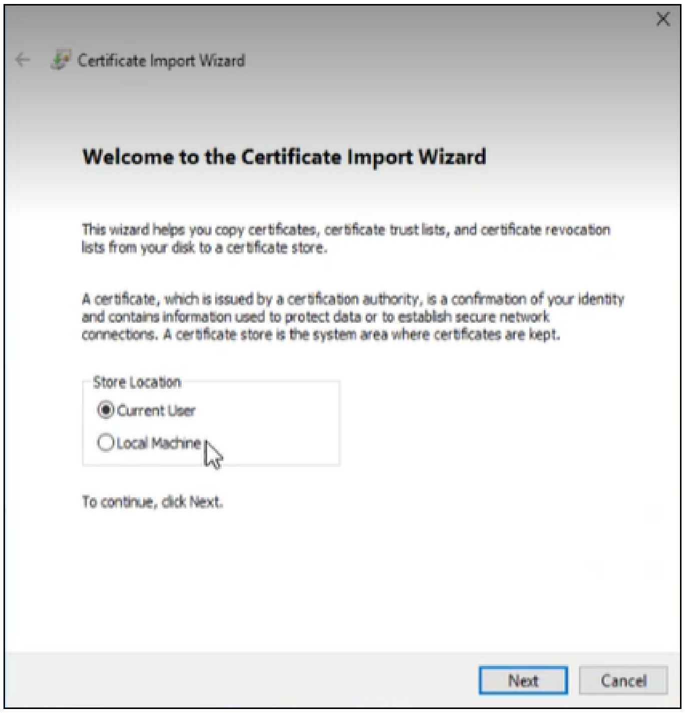
Issued to: GE Digital

Issued by: GE Digital

Valid from 4/20/2021 to 2/8/2024

4. Select **Install Certificate**.

   The **Certificate Import Wizard** appears.



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

● Current User

○ Local Machine

To continue, click Next.

5. Under **Store Location**, select **Local Machine**.

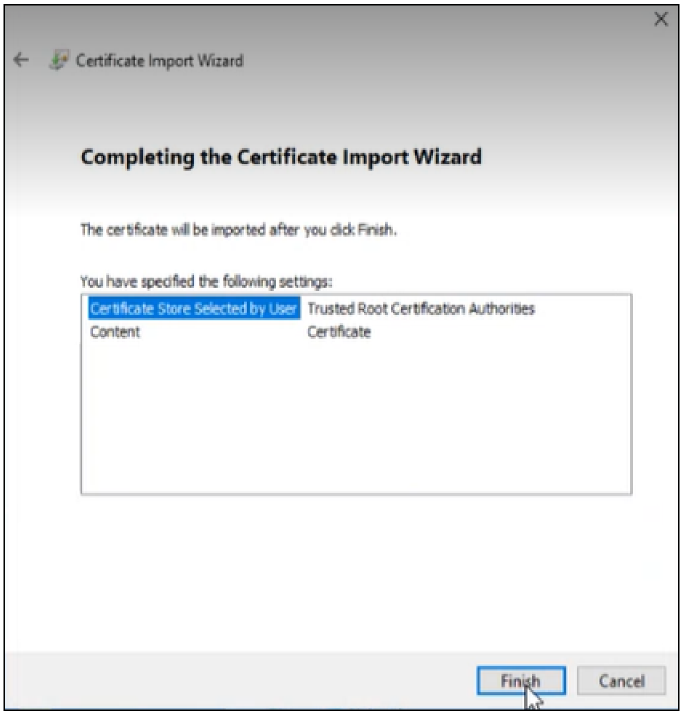
6. Select **Next**.

7. Under **Certificate Store**, select **Place all certificates in the following store**.

8. Select **Browse** to navigate to the location of the certificate store. For example, select `Trusted Root Certificate Authorities` folder.

9. Select **Next**.

   The **Completing the Certificate Import Wizard** appears.



Certificate Import Wizard

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

10. Select **Finish**.

    The `UAA_CA.crt` is imported to the Windows Trusted Store.

Update V3 Txt

Use this procedure to update the following in the `V3.txt` file:

- IP.2
- DNS.2
- DNS.3

1. Navigate to the `UAASecrets` folder, then select and open the `V3.txt` file using Notepad++.

2. Update the following details:
   - **IP.2**: Update the IP.2 address name to system IPv4 address.
   - **DNS.2**: Update the DNS.2 name to system fully qualified hostname.
   - **DNS.3**: Update the DNS.3 name to system short dns hostname.

3. Select **Save**.

Update the Server.CSR.CNF File

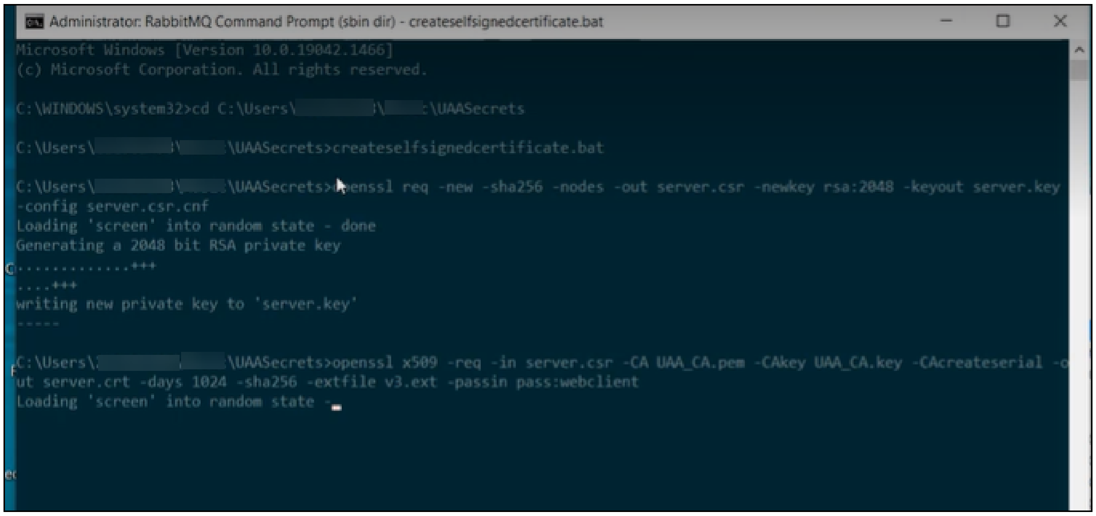
1. Navigate to the `UAASecrets` folder, then select the `server.csr.cnf` file, and open it using Notepad++.
2. Update the Commom Name (CN) to the system hostname.
3. Select **Save**.

Create Certificates and Keystore Files

Use this procedure to create certificates (`server.crt`, `server.key`) and the `keystore` file.

1. Open command prompt window in the administrator's mode, and then navigate to the `UAASecrets` folder.

2. To create the certificates and keystore files, execute `createselfsignedcertificate.bat`.


Administrator: RabbitMQ Command Prompt (sbin dir) - createselfsignedcertificate.bat

```
Microsoft Windows [Version 10.0.19042.1466]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd C:\Users\[redacted]\[redacted]\UAASecrets

C:\Users\[redacted]\[redacted]\UAASecrets>createselfsignedcertificate.bat

C:\Users\[redacted]\[redacted]\UAASecrets>openssl req -new -sha256 -nodes -out server.csr -newkey rsa:2048 -keyout server.key
-config server.csr.cnf
Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
.............+++
....+++
writing new private key to 'server.key'
-----

C:\Users\[redacted]\[redacted]\UAASecrets>openssl x509 -req -in server.csr -CA UAA_CA.pem -CAkey UAA_CA.key -CAcreateserial -o
ut server.crt -days 1024 -sha256 -extfile v3.ext -passin pass:webclient
Loading 'screen' into random state -
```

The certificates and keystore files are created.

3. Create a copy of the keystore file and rename it to `keystore.p12`.

4. To create pem files, execute `createpemfiles.bat` in the command prompt.

The `public.pem` and `key.pem` files are created.

Update Work Order, HTTPD, and Tomcat Services

After renewing the expired self-signed certificate, you must update and restart the following:

- WorkOrder service
- HTTPD
- Tomcat service and Tomcat JRE keystore

Do the following:

a. **WorkOrder service**: Navigate to the `UAASecrets` folder in the Web Client installation directory, then create a copy of keystore file and rename it to `keystore.pfx`. Copy this `keystore.pfx` file to the WorkOrder service folder: `C:\Program Files\GE Digital\PlantApplications\work-order-service-x.x.x`. Restart WorkOrder sevice 'GE.PlantApps.WorkOrder'.

b. **HTTPD service**: To update the HTTPD service, copy the `public.pem` and `key.pem` files to Httpd certificate directory: `C:\Program Files\GE Digital\PlantApplications\Service-HTTPD\conf\cert`. Restart service 'GE.PlantApps.HTTPD'.

c. **Tomcat**: To update Tomcat, copy the keystore file to Tomcat `conf` folder. Restart Tomcat service.

d. **Tomcat JRE keystore**: To update the Tomcat JRE keystore, navigate to the Web Client installation directory, then select `import_cert_Tomcat.ps1`, and edit it with PowerShell script.

   The `import_cert_Tomcat.ps1` opens in the PowerShell Script window.

   Update the `public.pem` path in the `import_cert_Tomcat.ps1` file. For example, `C:\Users\Administrator\Desktop\UAASecrets_Latest\public.pem`.

   In the Web Client installation directory, open the command prompt in the administrator's mode, then execute `<import_cert.bat import_cert_Tomcat.ps1>`.

Chapter 10. Reference

Configure the Proficy Historian Security Settings

Configure the security settings in the Proficy Historian to enable the Plant Applications Web Client to use the Proficy Historian 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 Proficy Historian is now configured for the Plant Applications Web Client. You can now install the Plant Applications Web Client on the same computer as the Proficy Historian.