GE VERNOVA

DIGITAL

PROFICY PLANT APPLICATIONS 2023

Web Client Installation Guide

GE VERNOVA

Proprietary Notice

Trademark Notices

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

Contents

Chapter 1. Installation Overview

Installation Overview

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

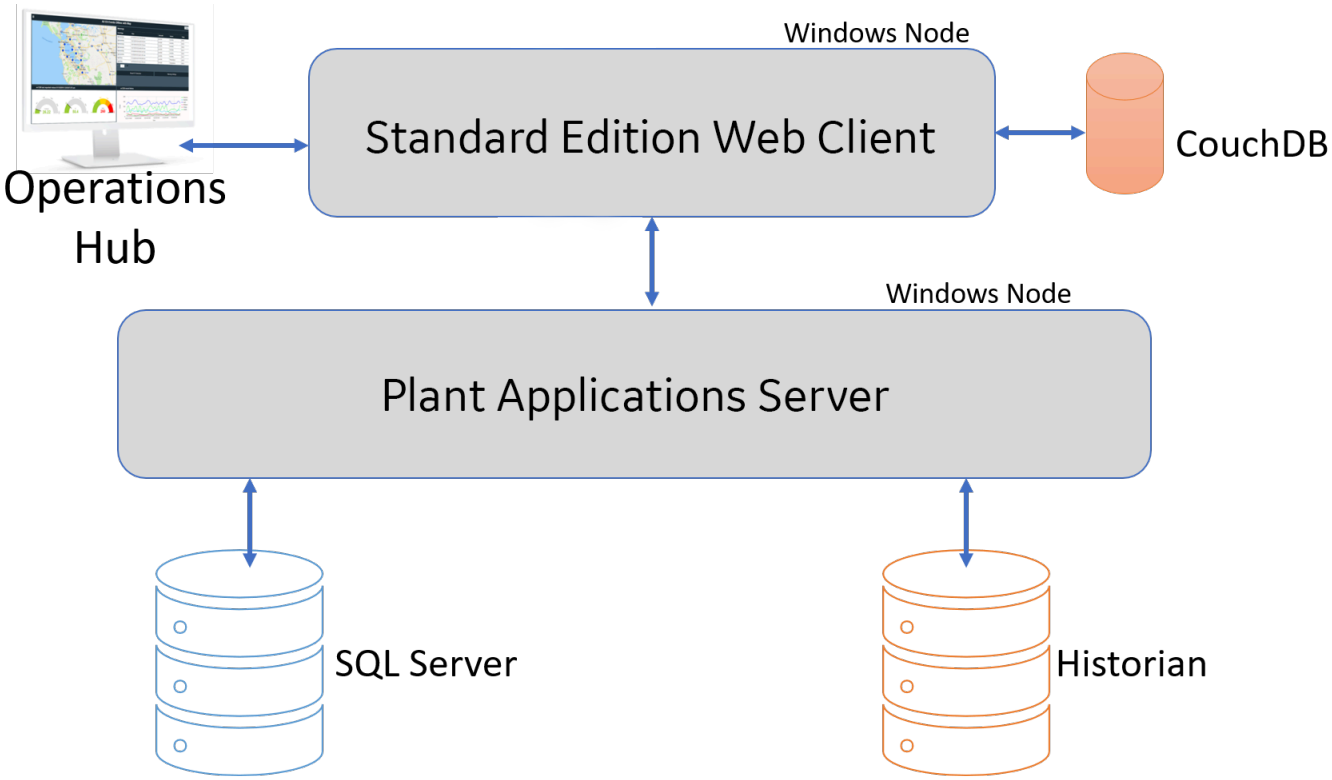
- **Standard Installation**: This is used to install Plant Applications Web Client for both Process and Discrete applications on a Windows machine. See About Installing Standard Web Client *(on page 22)*.
- **Enterprise Installation**: This is used to install Plant Applications Web Client for both Process and Discrete applications on a Linux machine. See About Installing Enterprise Edition Web Client *(on page 62)*.

Deployment Architecture

This section gives an overview on the recommended deployment architecture for both Standard and Enterprise Edition Web Client Installation.

Standard Deployment Architecture

The following diagram shows the recommended deployment architecture for Standard Edition Web Client Installation. In this diagram, the various servers suggest the order of installation of the various software packages on their respective servers. We recommend that you follow the same order.

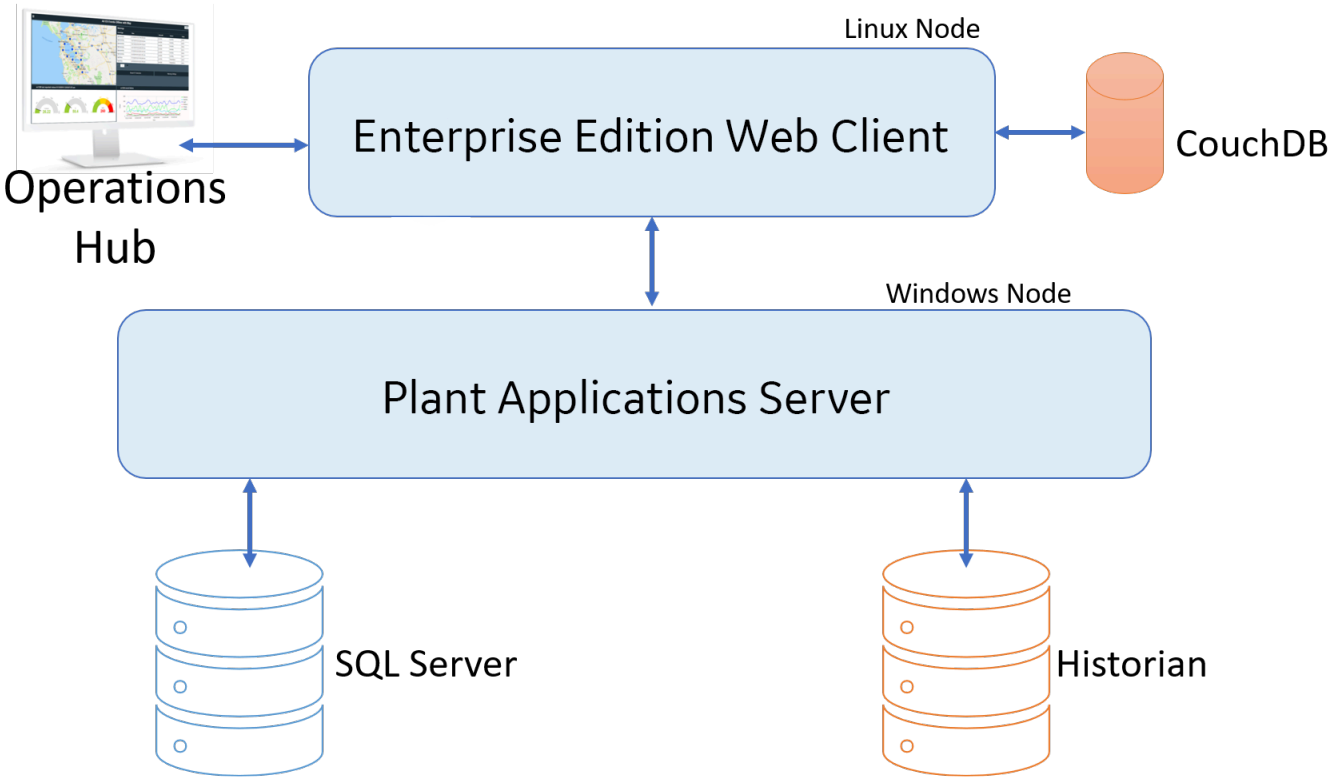


If, however, you choose the minimum-number-of-servers configuration for the deployment, resolve the following possible port conflicts:

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

Enterprise Deployment Architecture

The following diagram shows the recommended deployment architecture for Enterprise Edition Web Client Installation. In this diagram, the various servers suggest the order of installation of the various software packages on their respective servers. We recommend that you follow the same order.



If, however, you choose the minimum-number-of-servers configuration for the deployment, resolve the following possible port conflicts:

- **Operations Hub and Plant Applications Web Reports:** Operations Hub uses 443 as the port number for https binding. Therefore, use a different port for the Web Reports server.

Note:
If port 5986 is used by any other application, then modify the `default.ini` file of Apache CouchDB to set the port number under httpd to 5987.

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 *(on page 9)*
- Port requirements *(on page 11)*

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 or Windows Server 2022
Couch DB server	CouchDB version 2.3.1 or 3.2.2 **Note:** For more information on downloading, installing, configuring, or upgrading CouchDB, refer to the *Pre-installation Configuration (Enterprise and Standard)* section.
Operations Hub	2.1 with SIM3 and later, or Operations Hub 2022, 2022.4.1, or 2022.06
Web browsers	Chrome 107.0.5304.107 and later

Item	Version
	Devices: • **iPad**: Safari v13.1+, Chrome 107.0.5304.107 and later **Note:** To view the application content, you must select the desktop site option from the Chrome browser settings menu. • **Windows Tablet**: Chrome 107.0.5304.107 and later **Note:** Devices support only Unit Operations,Work Queue, and Non Conformance applications. **Note:** To view the application content, you must select the desktop site option from the Chrome browser settings menu. Microsoft Edge v94.0.992.31
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)

Item	Version
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

This section describes the port requirements for Plant Applications Web Client. Ensure that the ports described in the following table are opened before you install Plant Applications Web Client.

To open ports on the Plant Applications Core Server, refer to the **Port Requirements** section in the *Getting Started Guide*.

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.

Port	Description
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 *(on page 22)*.

Enterprise Edition Web Client Requirements

Before you begin

Ensure that you have completed the following tasks:

- Installation of Plant Applications Server
- Installation of Operations Hub 2.1 with SIM3 and later, or Operations Hub 2022, 2022.4.1, or 2022.06
- 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.

Item	Version
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 107.0.5304.107 and later **Devices**: • **iPad**: Safari v13.1+, Chrome 107.0.5304.107 and later **Note:** To view the application content, you must select the desktop site option from the Chrome browser settings menu. • **Windows Tablet**: Chrome 107.0.5304.107 and later, with minimum resolution 1920x1280

Item	Version
	Note: Devices supports only Unit Operations, Work Queue, and Non Conformance applications. **Note:** To view the application content, you must select the desktop site option from the Chrome browser settings menu. Microsoft Edge v94.0.992.31
Couch DB server	CouchDB version 2.3.1 or 3.2.2 **Note:** For more information on downloading, installing, configuring, upgrading CouchDB, and binding the certificates, refer to the *Pre-installation Configuration (Enterprise and Standard)* section.
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).

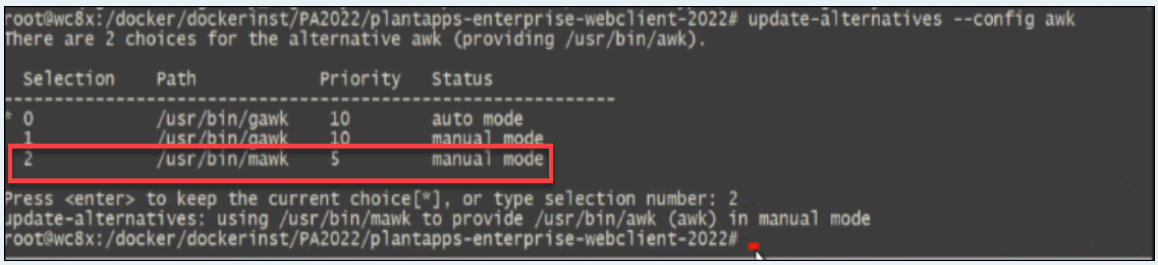
Item	Version
Memory	64 GB (recommended)

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.



Port Requirements

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

Port	Description
15672	The default port for the RabbitMQ Message bridge required to communicate with the Plant Applications server for retrieving data updates.
1433	The default port for the Microsoft SQL server.
9093	The default port for Kafka.

Port	Description
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 *(on page 62)*.

About Change Data Capture (CDC)

Change Data Capture (CDC) is used to identify and track changes to data in the SQL Server database.

Plant Applications Web Client uses CDC to make the following changes available to the user immediately:

- Adding new Line and Unit which reflects in Operator app and Work-Queue app.

If the CDC is not enabled, the changes become available when the caches are refreshed after a predefined interval.

The following applications support Change Data Capture (CDC):

- Work Queue
- Route Editor
- Operator

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

Install and Configure Apache CouchDB

About this task

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

Plant Applications support Apache CouchDB 2.3.1 and 3.2.2.

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 Apache CouchDB.

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.

Procedure

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

   The **Apache CouchDB Setup** page appears.

2. Select **Next**.

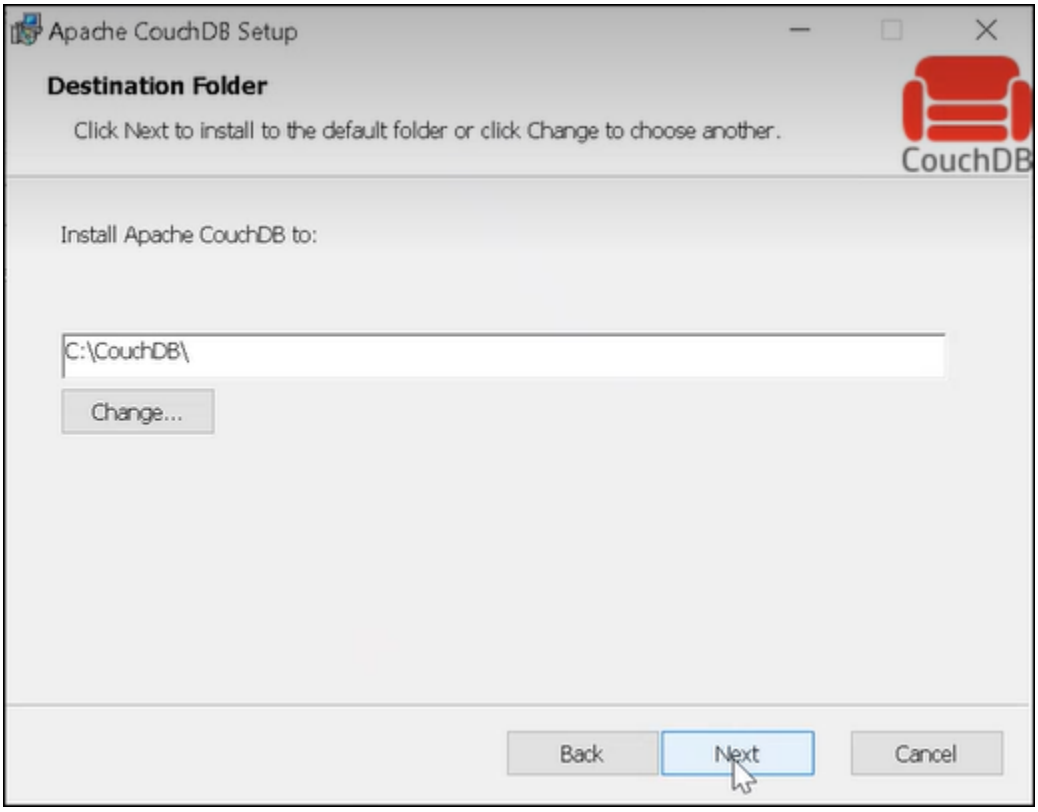
   The **License Agreement** page appears.

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

   The **Installation Directory Warning** page appears.

4. Select **Next**.

   The **Destination Folder** page appears.



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.

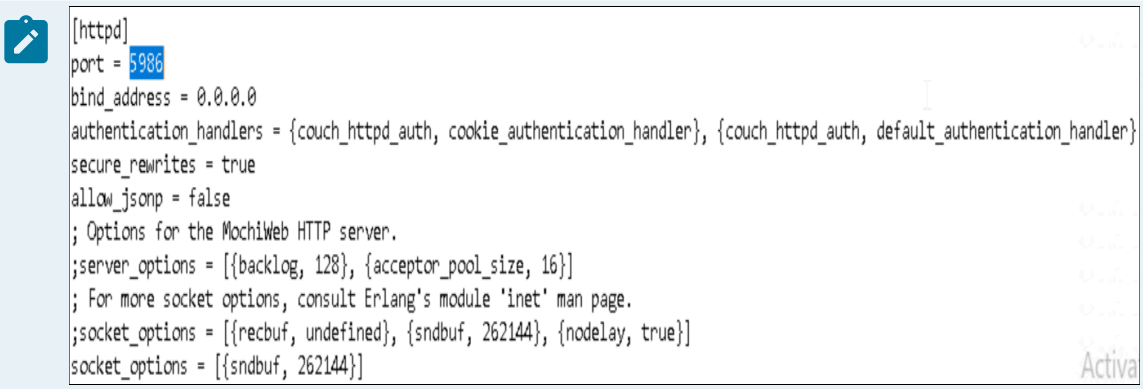
6. Select **Install**.

   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.



Note:
To authenticate users before accessing the documents database, you must manually set the option `require_valid_user` to `True` under Configuration settings of CouchDB.

Bind the Certificates to Apache CouchDB

Before you begin

- Verify that you have installed Apache CouchDB on a Windows machine.
- Ensure that you have retrieved the self-signed certificates such as `server.crt` and `server.key`, and then copied the certificates to the `Apache CouchDB` folder.

About this task

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:

Procedure

1. In a machine where CouchDB is installed, mount the ISO file for the Plant Applications Web Client or load the DVD if you created one from the ISO file for Plant Applications.
2. From the ISO root folder, 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

Procedure

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**.

What to do next

Proceed to install the Plant Applications Standard Edition Web Client (See About Installing Standard Web Client *(on page 22)*) or the Plant Applications Enterprise Edition Web Client (See About Installing Enterprise Edition Web Client *(on page 62)*)

Upgrade Apache CouchDB to a Recent Version

About this task

Use this procedure to upgrade CouchDB from version 2.3.1 to 3.2.2.

Procedure

1. Take backup of the existing CouchDB full install folder which also includes the "`data`" folder.
2. Uninstall the existing CouchDB version, and install the most recent Apache CouchDB version. See https://couchdb.apache.org/#download.
3. Replace the `data` folder from old CouchDB install and replace it to a new install path.
4. Run `config_couchDB.bat` file from Proficy Plant Applications ISO to make CouchDB accessible on https.

> **Note:**
> Ensure that the same certs are reused.

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 *(on page 17)*	This step is required.
5	Ensure that your system meets the requirements for the Standard Web Client installation. *(on page 9)*	This step is required.

Step	Task	Notes
6	• Install Standard Web Client Using GUI *(on page 24)* OR • Install Plant Applications Standard Web Client in Silent Mode *(on page 35)*	This step is required.
7	After the Standard Web Client installation, ensure to run the Message Bridge Configuration utility. *(on page 90)*	This step is required.
8	Verify the Installation *(on 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. Bind the Certificates to Apache CouchDB *(on page 19)*
    b. Add a User to Apache CouchDB *(on page 20)*
4. Install Standard Web Client Using GUI *(on page 24)* or Install Plant Applications Standard Web Client in Silent Mode *(on page 35)*
5. Run the Message Bridge Configuration Utility *(on 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 *(on page 24)*.
- **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 *(on page 35)*.

Install Standard Web Client Using GUI

About this task

Note:

- Before installing the Standard Edition Web Client, ensure that you first perform the preinstallation tasks *(on page 9)*.
- We recommend to use the signed certificates. The self-signed certificate which is provided during the Plant Applications Web Client installation expires on February 8, 2024.

Procedure

1. Mount the ISO file for the Plant Applications Web Client or load the DVD if you created one from the ISO file on the application server for Plant Applications.
2. Right-click the `installfrontend.exe` file, and then select **Run as an Administrator**.

   The **Install Proficy Plant Applications 2023** page appears and displays the installation menu.

   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 2023** page.

4. In the **Welcome to Plant Applications Web Client 2023** page, select **Next**.
   The **Read and accept the license agreement to continue** page appears.
5. Read the license agreement, select **Accept**, and then select **Next** to continue the installation.

   The **Prerequisites** page appears.

   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.

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

   The **Host Name** page appears.
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.
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.

Field	Description
	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`.
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`.

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.

11. 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.
User-name	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.

12. 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.

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

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

14. 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.

15. Select **Next**.
    The **Proficy Authentication Credentials** page appears.
16. 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**.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Admin Client Secret</td><td>Enter the password.</td></tr>
<tr><td>Validate</td><td>Validate the Proficy Authentication (UAA) server connection.

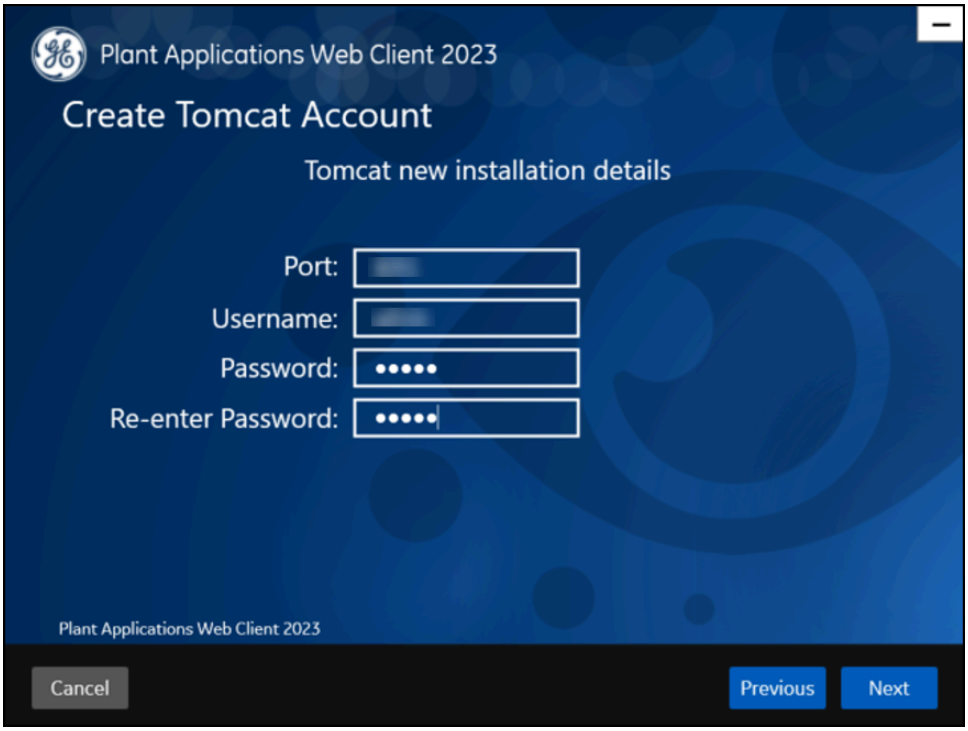
Note:
The following table describes each icon indicating a validation status that might appear during the validation process.

<table><tr><th>Icon</th><th>Description</th></tr><tr><td></td><td>Indicates that the validation is in progress.</td></tr><tr><td></td><td>Indicates that the validation was successful.</td></tr><tr><td></td><td>Indicates that the validation was unsuccessful. In this case, make sure you enter the correct password.</td></tr></table></td></tr>
</table>

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

17. Select **Next**.

The **Create Tomcat Account** page appears.



18. 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.

Field	Description
	Note: This field appears only when a new installation of Tomcat is initiated by the installer.

19. Select **Next**.

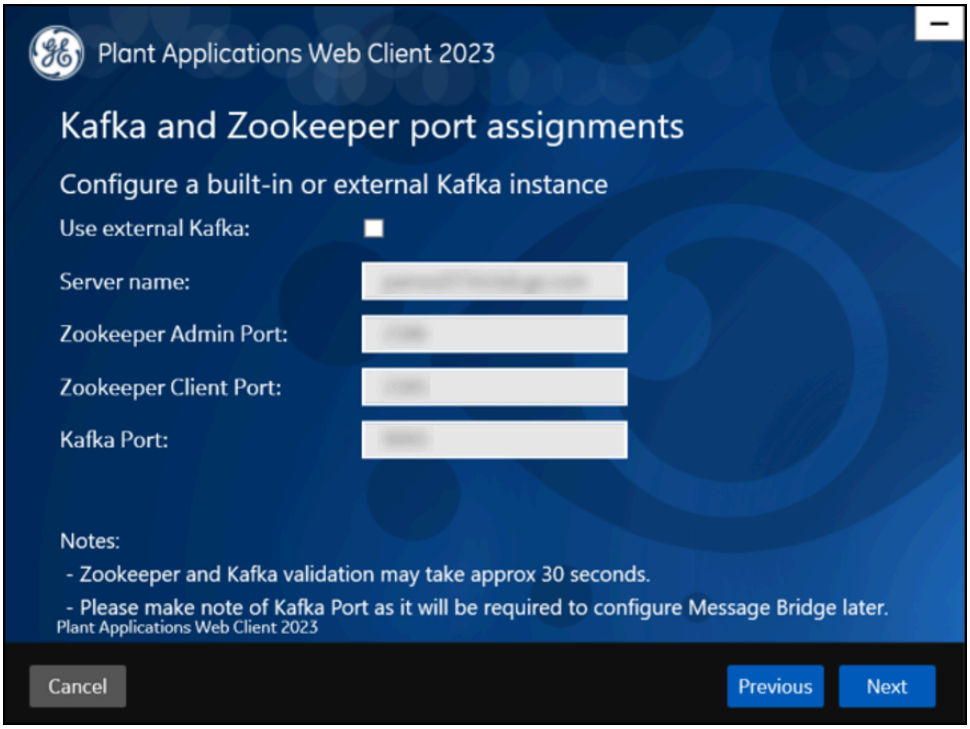
    The **RabbitMQ Credentials** page appears.

20. 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.

21. 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.



22. Select **Next**.
23. 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.
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.

Field	Description
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.

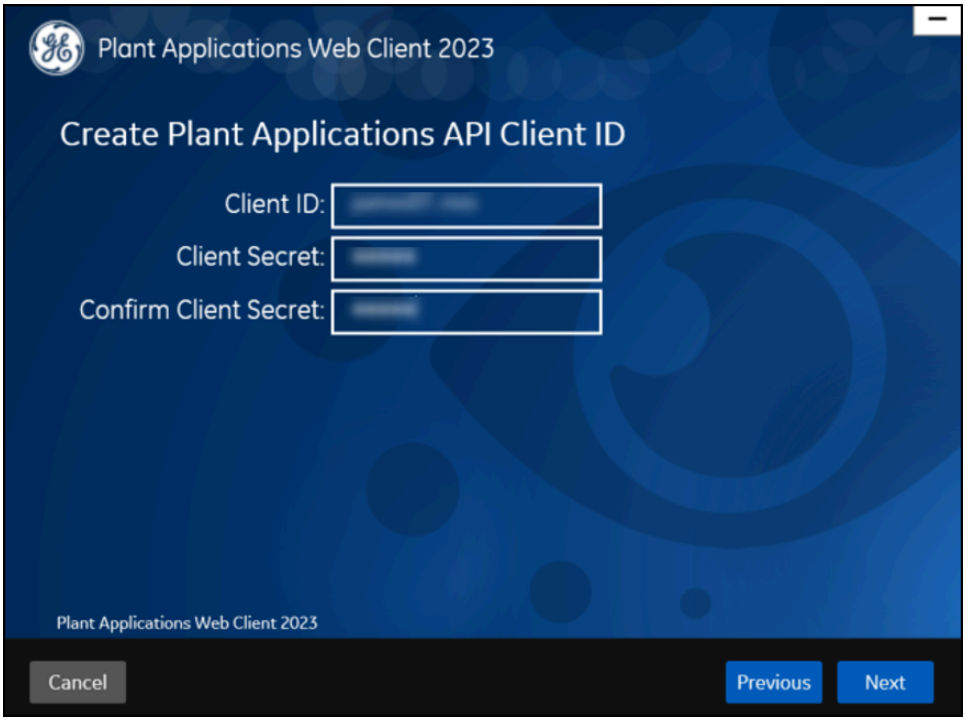
24. Enter the following Plant Applications administrator credentials.

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.

25. Select **Validate** to validate the Plant Applications administrator credentials.
When the Plant Applications administrator connection is successfully validated, the **Next** option is enabled.
26. 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.



27. 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.
Client Secret	Enter the password.
Confirm Client Secret	Enter the password to confirm the value in the **Confirm Client Secret** field.

28. Select **Next**.

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

29. 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.

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

30. **Optional:** Select **View Logs** to see the installation details.
31. 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 *(on 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.

32. When you have completed running Message Bridge Configuration, Verify the Installation *(on page 95)* if the Plant Applications Web Client applications are up and running.
33. Access the Plant Applications REST APIs *(on page 96)* to access the REST APIs for Plant Applications Web Client.
34. 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 *(on page 142)*.
35. 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 *(on page 43)*.

What to do next

Perform the post-installation steps *(on page 38)*.

Install Plant Applications Standard Web Client in Silent Mode

About this task

Note:
Before installing the Plant Applications Standard Edition Web Client, ensure that you first perform the preinstallation tasks *(on page 9)*.

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.

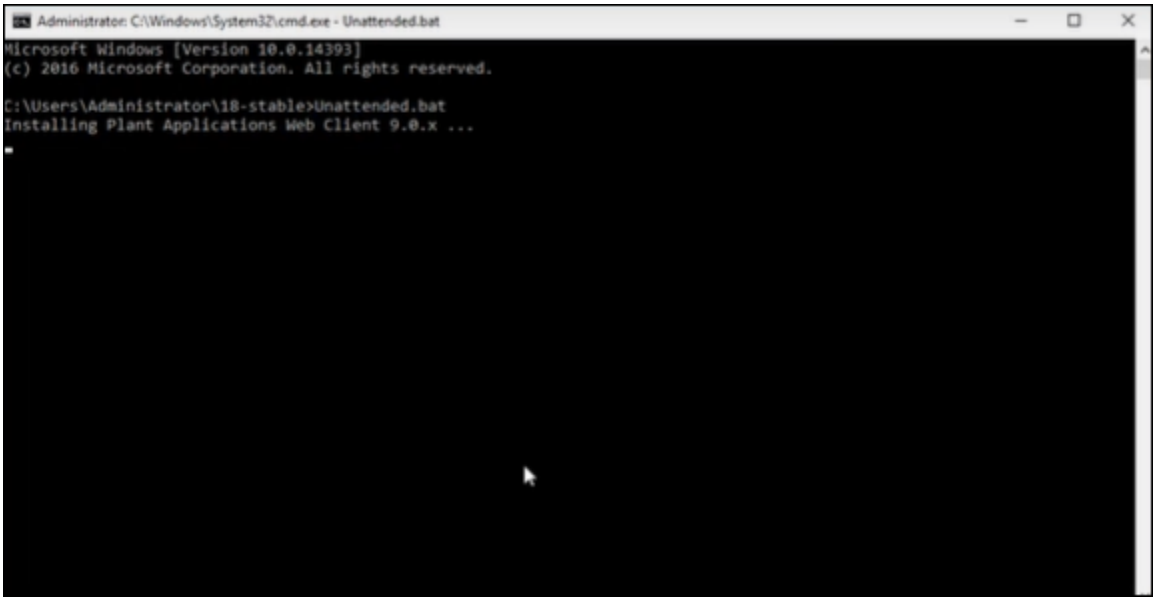
> **Note:**
> In silent mode installation, the installer by default is installed to the `C:` drive.

Procedure

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>”`.



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 *(on 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 *(on page 95)* if the Plant Applications Web Client applications are up and running.
7. Access the Plant Applications REST APIs *(on page 96)* 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 *(on page 142)*.
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`.

What to do next

Perform the post-installation steps *(on page 38)*.

About Post-Installation Tasks

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

- Configure a Proficy Historian for the Analysis application *(on page 103)*.
- Configure the cache settings for the Historian tags used in the Analysis application *(on page 105)*.

Disable Discrete Applications

About this task

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

Procedure

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

Procedure

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

About this task

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

Procedure

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

Procedure

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

About this task

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

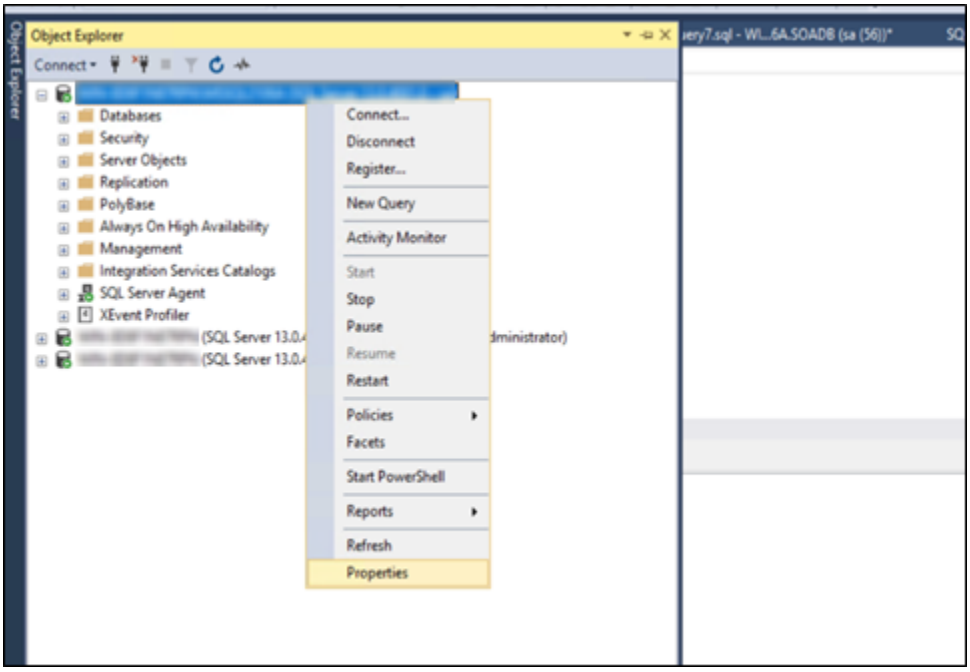
Procedure

Update database settings:

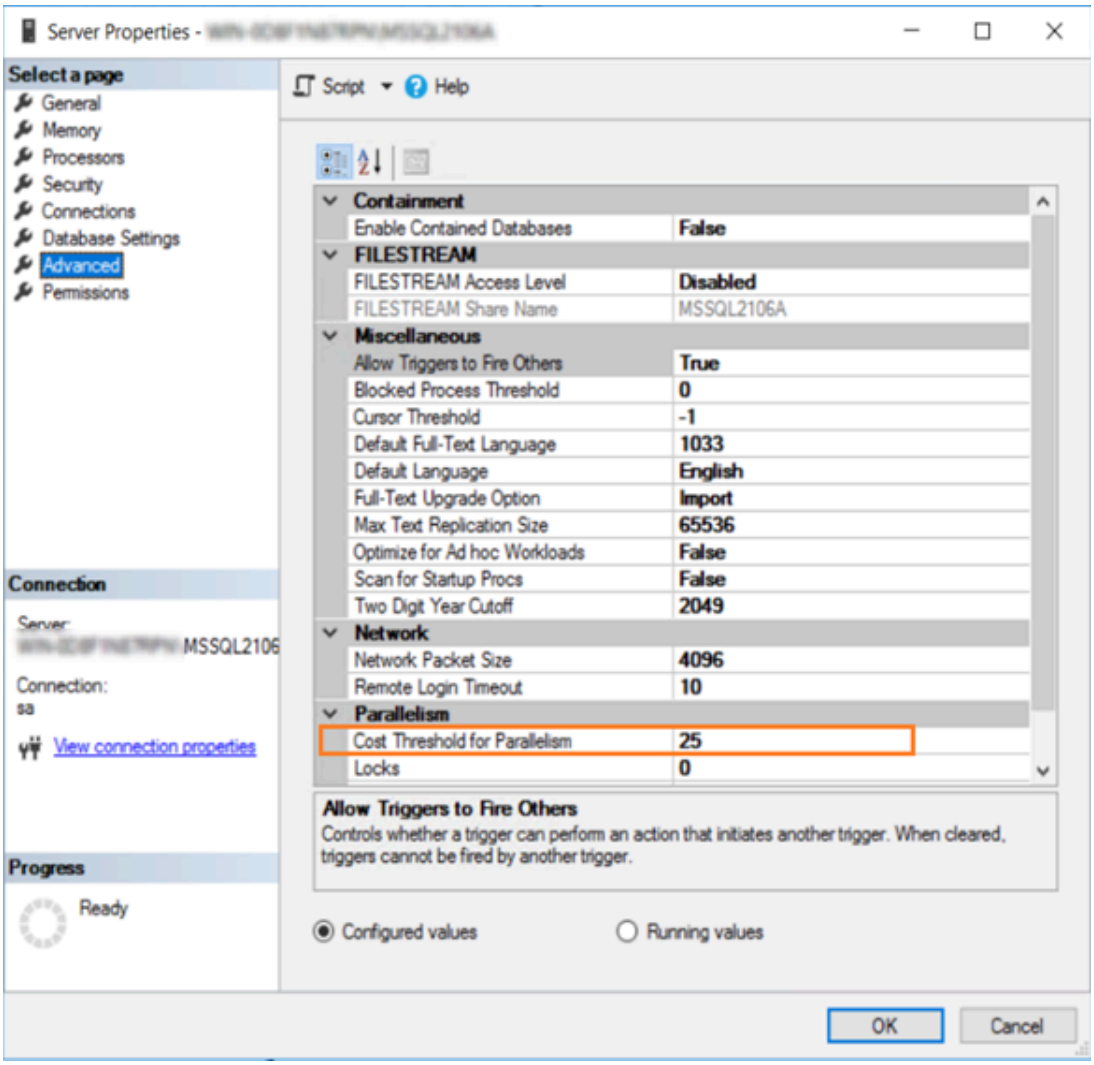
a. Update the **Cost Threshold for Parallelism** value:

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.



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.

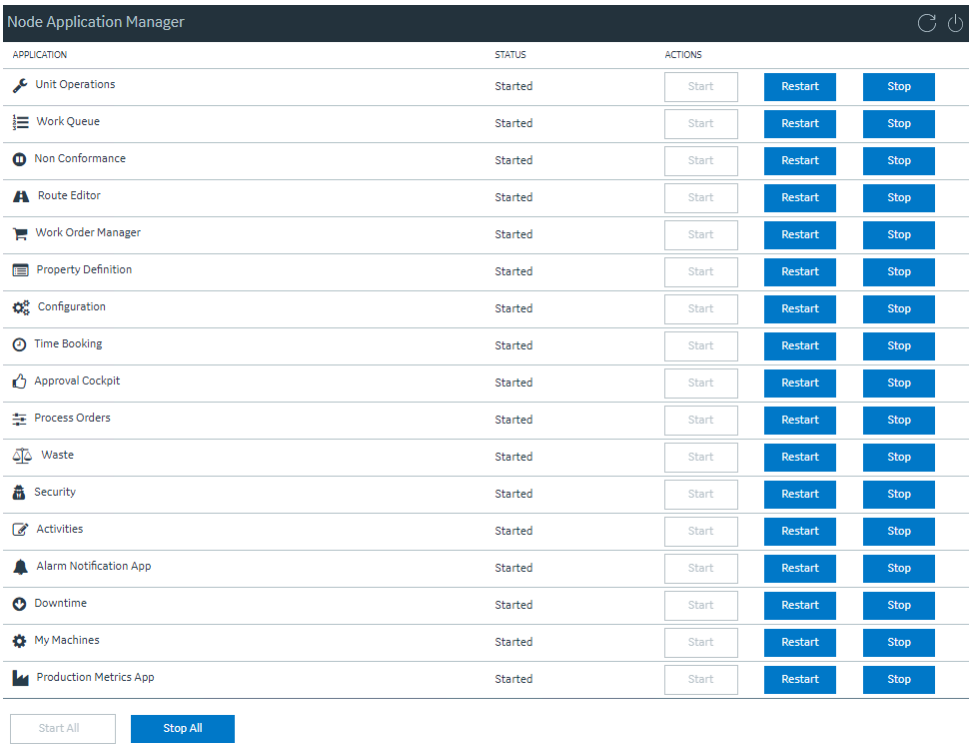
Node Application Manager Utility

About this task

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

Procedure

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.



   - 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

About this task

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.

Procedure

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

About this task

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

Procedure

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

Procedure

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

Serial No	Service Name
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
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

Serial No	Service Name
42	plantexecutionservice
43	ncmappservice
44	pa-mymachinesservice
45	operatorappservice
46	productionmetrics-app-service
47	productionschedulerappservice
48	rmsappservice
49	securityadministratorappser-vice
50	supervisorappservice
51	wastemanagementappservice
52	bommanagementappservice
53	receivinginspectionappservice
54	receivinginspectionservice
55	spcappservice
56	webgenealogyappservice
57	approvalcockpitservice
58	wastemanagementservice
59	operatorapplogservice
60	operatorlogservice
61	lineoverviewservice
62	lineoverviewappservice
63	autologservice
64	autologappservice

Resolve Apache CouchDb Certificate Error

About this task

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.

Procedure

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

Before you begin

- 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 2023.

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.

About this task

Note:
The Plant Applications 2023 installer is the base installer for all upgrade requirements.

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

Procedure

1. Run the `installfrontend.exe` file as an Administrator.
   The installation menu appears, displaying the **Install Proficy Plant Applications 2023** page.

   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 2023** page.

3. Select **Next**.

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

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

   The **Prerequisites** page appears.

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

   The **Host Name** page appears.

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.

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).

Field	Description
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.

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.

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.
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.

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.

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

15. Select **Next**.
The **Proficy Authentication Credentials** page appears.
16. Enter the credentials to access the Proficy Authentication server as described in the following table.

Field	Description
Server Name	Enter the host name of the Proficy Authentication (UAA) server. **Note:** Instead of IP address, it is recommended to use the Proficy Authentication (UAA) host name (computer name).
Port	Enter the Proficy Authentication (UAA) port number.
Admin Client ID	Enter the admin Client ID to access the Proficy Authentication (UAA) server instance.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>Note:
The default user name is <code>admin</code>.</td></tr>
<tr><td>Admin Client Secret</td><td>Enter the password.</td></tr>
<tr><td>Validate</td><td>Validate the Proficy Authentication (UAA) server connection.

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

<table><tr><th>Icon</th><th>Description</th></tr><tr><td>  </td><td>Indicates that the validation is in progress.</td></tr><tr><td>  </td><td>Indicates that the validation was successful.</td></tr><tr><td>  </td><td>Indicates that the validation was unsuccessful. In this case, make sure you enter the correct password.</td></tr></table></td></tr>
</table>

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

The **Create Tomcat Account** page appears.

> **Note:**
> If you already have a Tomcat instance running, a message stating that the Tomcat instance has been found appears in the Tomcat Installation screen informing you to select the existing Tomcat instance.

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.
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**.

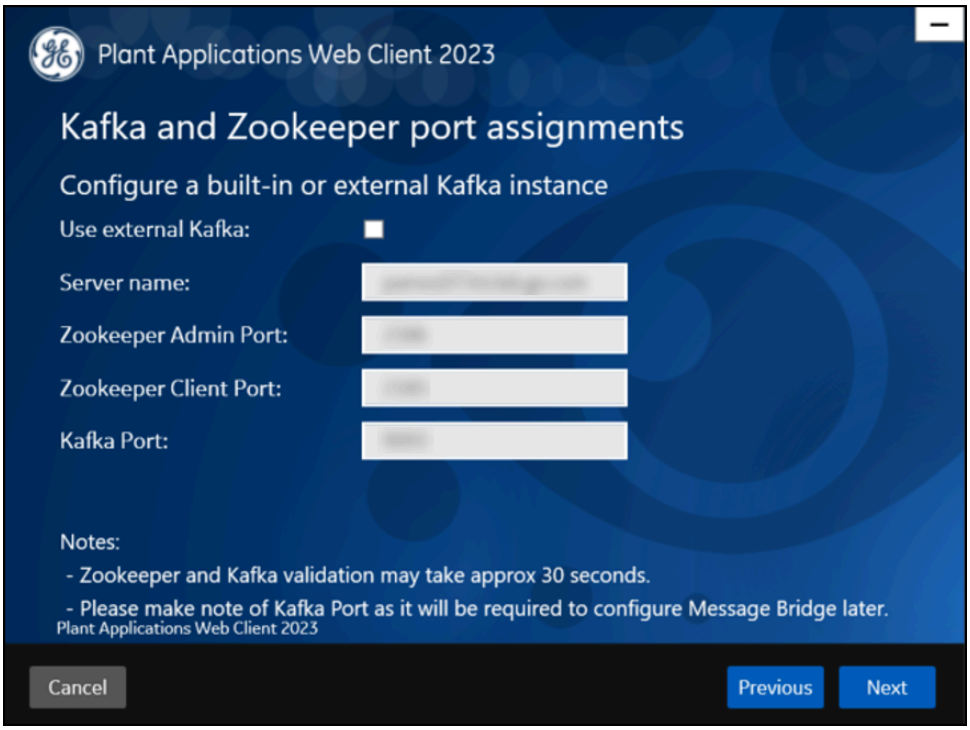
    The **RabbitMQ Credentials** page appears.

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.



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** option is enabled.

21. Select **Next**.

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

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.

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.
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 *(on 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 *(on page 95)* to verify if the Plant Applications Web Client applications are up and running.
31. Access the Plant Applications REST APIs *(on page 96)* 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 *(on page 142)*.

Upgrade Plant Applications Web Client in Silent Mode

About this task

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.

Procedure

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++.

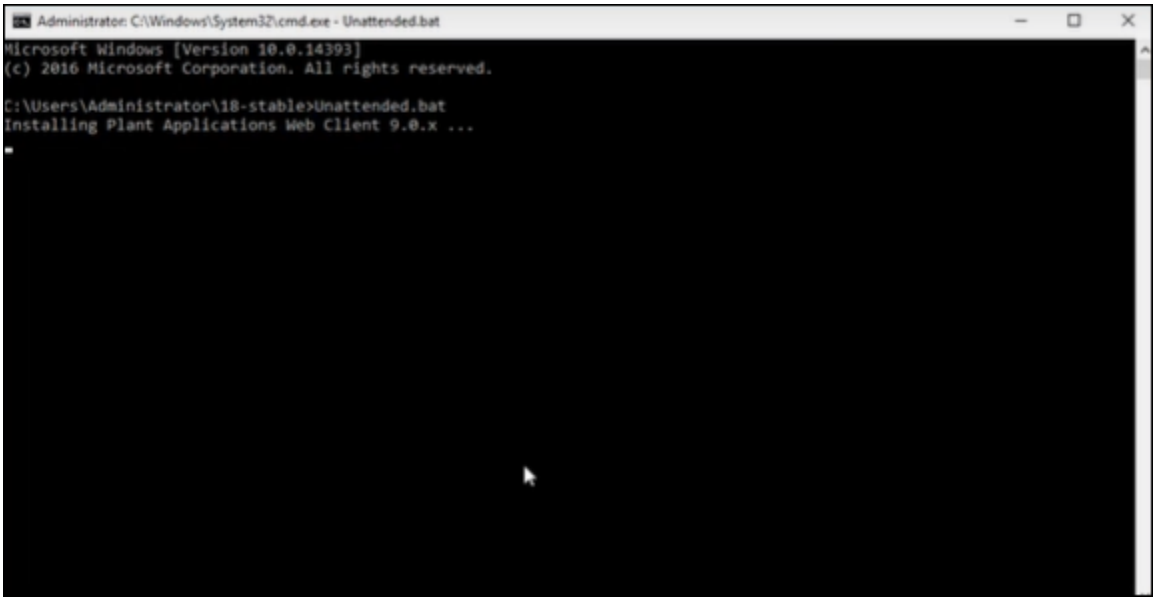
   Note:

   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>"`.



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 *(on 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 *(on 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 *(on page 96)* 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 *(on page 142)*.
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`.

What to do next

Perform the post-installation steps *(on page 38)*.

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-2023` 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, or Operations Hub 2022, 2022.4.1, or 2022.06	This step is required.
4	Install and Configure CouchDB for HTTPS *(on page 19)*	This step is required.
5	Ensure that your system meets the requirements for the Enterprise Edition Web Client installation. *(on page 12)*	This step is required.
6	Review the files provided by GE *(on page 63)*	This step is required.
7	Review the pre-installation checklist before installing Enterprise Edition Web Client. *(on page 64)*	This step is required.
8	Install Enterprise Edition Web Client *(on page 68)*	This step is required.
9	After the Enterprise Edition Web Client installation, ensure to run the Message Bridge Configuration utility. *(on page 90)*	This step is required.
10	Verify the Installation *(on page 95)*	This step is required.

Files Provided by GE

The following files are provided by GE:

- `plantapps-enterprise-webclient-2023`: Contains the installer and the supporting utilities.
- `plantapps2023-prereq.tar`: Contains the files required for installing Web Client pre-requisites.

> **Note:**
> Ensure you copy `plantapps2023-prereq.tar` and `plantapps-enterprise-webclient-2023` 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

Before you begin

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 *(on page 65)*.
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

About this task

Use this section to create and configure docker registry.

Procedure

1. From the Plant Applications Enterprise Edition Web Client installation package, download the `DTR2023` folder to the machine on which you want to run Docker Registry.

   Note:
   It is not mandatory to have local registry DTR2023. However, due to security concerns, we recommend to have a new local registry (DTR2023).

   Note:
   Ensure that you have enough space (minimum 50 GB) to store these extracted files.

2. 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
   ```

3. 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
   ```

4. 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/"NO_PROXY=localhost,127.0.0.1,<docker registry IP address>,<docker

    registry hostname>"
   ```

5. Save the file and close it.

   Note:
   To save and close the file, enter Ctrl+O and Ctrl+X, respectively.

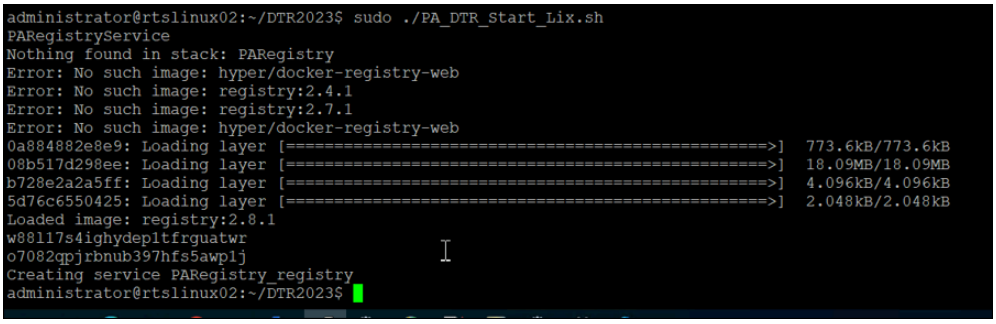
6. Create a file named `daemon.json` in the following folder: `/etc/docker`
7. Add the following lines of code in the `daemon.json` file:

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

8. Run the following commands to restart the docker:

```
sudo systemctl restart docker
```

9. Using terminal, change directory (cd) to the `DTR2023` folder.
10. In the `DTR2023` 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`.
11. Execute the PA_DTR_Start_Lix.sh Shell script with sudo privileges: `sudo ./PA_DTR_Start_Lix.sh`. The output of the command looks similar to the following:



12. Add the following to the Registry-url bullet:

    http:// <dockerregistry IP>/<docker registry hostname> :5000/v2/

    You should see the following text returned by the web server:

    {}

Configure the Load Balancer Rules

Before you install the Enterprise Web Client, you must configure the Load Balancer rules.

Load Balancer	Rules
/comments/	http 5984 Couch db windows instance
/comments/**	http 5984 Couch db windows instance
/documents/	http 5984 Couch db windows instance
/documents/**	http 5984 Couch db windows instance

Load Balancer	Rules
/_users	http 5984 Couch db windows instance
/_users/*	http 5984 Couch db windows instance
/_replicator	http 5984 Couch db windows instance
/_replicator/*	http 5984 Couch db windows instance
/_global_changes/*	http 5984 Couch db windows instance
/_global_changes	http 5984 Couch db windows instance
/iqp/	https 443 Operations Hub windows instance
/iqp/*	https 443 Operations Hub windows instance
/uaa/	https 443 Operations Hub windows instance
/uaa/*	https 443 Operations Hub windows instance
/run/	https 443 Operations Hub windows instance
/run/*	https 443 Operations Hub windows instance
/app/	https 443 Operations Hub windows instance
/app/*	https 443 Operations Hub windows instance
/site/	https 443 Operations Hub windows instance
/site/*	https 443 Operations Hub windows instance **Note:** /site/* is new ALB rule which is not part of 8.2 document.
/socket.io/	https 443 Operations Hub windows instance
/socket.io/*	https 443 Operations Hub windows instance
/custom/	https 443 Operations Hub windows instance
/custom/*	https 443 Operations Hub windows instance
/	https 443 Docker linux instance

Install Enterprise Edition Web Client

Before you begin

Note:
Before installing the Plant Applications Enterprise Edition Web Client, ensure that you first perform the preinstallation tasks *(on page 9)* 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`.

About this task

- 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`.

Procedure

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.

   Note:
   Ensure that you set the **WEBCLIENT_INSTALLATION_PATH** and **TARFILES_FOLDER_LOCATION** to different directories.

Parameter	Description
WEBCLIENT_-SERVER: ""	Enter the Linux node FQDN or hostname where you are going to install Plant Applications Enterprise Edition Web Client.

Parameter	Description
	For example, `WEBCLIENT_SERVER: "linuxnode.digital.com"`
WEBCLIENT_-SERVER_USER-NAME: ""	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_PASS-WORD: ""	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 *(on page 65)*. For example, `DTR_URL:<IP address or hostname>:<port number>`, where the default port number is 5000.

Parameter	Description
	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_USER-NAME: ""	Enter the username that have access to the Docker Registry. **Note:** Enter none if using insecure registry.
DTR_PASS-WORD: ""	Enter the password to the Docker Registry. **Note:** Enter none if using insecure registry.
TARFILES_FOLD-ER_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_-USERPASS-WORD: ""	Enter the Plant Applications Web Client password.
PROFICY_-AUTHENTI-CATION_-SERVICE_-ORIGIN: ""	Enter the Proficy Authentication Server (UAA) hostname.

Parameter	Description
PROFICY_-AUTHENTI-CATION_-SERVICE_PORT: ""	Enter the Proficy Authentication Server port number. By default, the port number is 443.
PROFICY_-AUTHENTI-CATION_-SERVICE_ ADMIN_CLIENT_-ID: ""	Enter the admin Client ID to access the Proficy Authentication server instance. **Note:** The default username is **admin**.
PROFICY_-AUTHENTI-CATION_-SERVICE_ ADMIN_CLIENT_-SECRET: ""	Enter the Client Secret for the username you entered.
PLANT_APPS_D-B_SERVER: ""	Enter the Plant Applications database server hostname that you want to connect with the Plant Applications Web Client.
PLANT_APPS_D-B_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_D-B_NAME: ""	Enter the Plant Applications Database name. For example, `PLANT_APPS_DB_NAME: "SOADB"`
PLANT_APPS_D-B_USERNAME: ""	Enter the username that has permissions to access the database you entered.

Parameter	Description
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.
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"`.

Parameter	Description
	Note: The OPHUB_TENANT_USERNAME field is case sensitive. You must always enter the user name as OphubAdmin.
OPHUB_TENANT_PASSWORD	Enter the tenant Hub password.
UPDATE_PASSWORDS:""	This field must be set to true and should not be modified during the upgrade or clean installation.
UPDATE_CERTS:""	Default value is true. Set this to false if you want to use the OLD signed certificates during upgrade. If you do not set this to false, then: ◦ The old signed certificates are replaced by the selfsigned certificates, and ◦ You must run the certificate utility again to deploy the signed certificates.
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.
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"`

Parameter	Description
	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:

- 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 *(on 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 *(on page 95)* if the Plant Applications Web Client applications are up and running.
8. Access the Plant Applications REST APIs *(on page 96)* 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 *(on page 142)*.

About Node-RED

Node-RED is a browser-based flow editor that allows you to wire together hardware devices, APIs, and online services.

Install the Node-RED Application

About this task

Procedure

1. Download the `nodered.zip` file, and copy it on your Linux machine.
2. Extract the `nodered.zip` file into a new folder by running the following command: `$ unzip nodered.zip`
3. Navigate to the extracted folder and update the `application.properties` file.
4. Give execute permissions to run the `setupNodered.sh` file by running the following command: `$ sudo chmod +x ./setupNodered.sh`.

What to do next

After giving executable permissions to the `setupNodered.sh`, you must run the collection (`NodeRed Post Config.postman_collection.json` and `NodeRed_Post.postman_environment.json`) using Postman.

Run NodeRED Collection Using Postman

About this task

You can run the collection (`NodeRed Post Config.postman_collection.json` and `NodeRed_Post.postman_environment.json`) using Postman.

Procedure

1. Navigate to the location of NodeRed installer, and then copy the postman collection from the directory `{{Node red installer}}/nodered/Postman_collections`.
2. Add scope and redirect the URL to the client.
3. Access the Postman application, then select **Import**.

   The **Import** window appears.
4. Select **Upload Files**, then browse and select the `NodeRed Post Config.postman_collection.json` and `NodeRed_Post.postman_environment.json` files.
5. Select the check boxes for the two files, then select **Import**.
6. In the right pane, in the **Environment** field, select **NodeRed_Post** from the list.
7. Select **Settings**.

   The **Settings** dialog box appears.
8. If UAA is running on the self-signed certificates, then disable **SSL certificate verification** by clicking the toggle button.
9. Select the collection, then select **Run collection**.
10. In the **Delay** field, type `1000`.
    It takes about one second to proceed to the next call.
11. Select **Run Nodered Post Config**.

    When the Postman runs successfully, it shows the status as pass.

Install NodeRED for Plant Applications Releases Earlier than SP1

About this task

Use this procedure to install NodeRed when you are using Plant Applications versions earlier than SP1.

Procedure

1. Update the `gateway-service-prod.properties` file in the following location: `{{installation path }}/PlantApplicationsDocker/plantapps-web-docker/mnt/configfiles/gateway-service/prod/{{version}}/`.
2. Verify that the NodeRED path already exists. If the NodeRED path is not available, then update the path by adding the following:

   a.
   ```
   spring.cloud.gateway.routes[57].id=nodered
   spring.cloud.gateway.routes[57].uri=http://node-red:1880/nodered
   spring.cloud.gateway.routes[57].predicates[0]=Path=/nodered/**
   spring.cloud.gateway.routes[57].filters[0]=RewritePath=/nodered/(?<segment>.*), /nodered/${segment}
   spring.cloud.gateway.routes[57].filters[1]=DedupeResponseHeader=Access-Control-Allow-Credentials
    Access-Control-Allow-Origin
   spring.cloud.gateway.routes[57].filters[2].name=Retry
   spring.cloud.gateway.routes[57].filters[2].args.retries=3
   spring.cloud.gateway.routes[57].filters[2].args.statuses=${retryable_statuses}
   spring.cloud.gateway.routes[57].filters[2].args.methods=GET,POST
   spring.cloud.gateway.routes[57].filters[2].args.backoff.firstBackoff=10ms
   spring.cloud.gateway.routes[57].filters[2].args.backoff.maxBackoff=50ms
   ```

   b.
   ```
   spring.cloud.gateway.routes[61].id=pa-nodered-app-2
   spring.cloud.gateway.routes[61].uri=http://panoderedapp:9003
   spring.cloud.gateway.routes[61].predicates[0]=Path=/pa-nodered-app/properties/**
   spring.cloud.gateway.routes[61].filters[0]=RewritePath=/pa-nodered-app/(?
   <segment>.*),/node-red/${segment}
   ```

   c.
   ```
   spring.cloud.gateway.routes[62].id=pa-nodered-app
   spring.cloud.gateway.routes[62].uri=http://panoderedapp:9003
   spring.cloud.gateway.routes[62].predicates[0]=Path=/confighub_plugin/pa-nodered-app/{segment}, /pa-
   nodered-app/{segment}
   spring.cloud.gateway.routes[62].filters[0]=SetPath=/node-red/{segment}
   spring.cloud.gateway.routes[62].filters[1]=DedupeResponseHeader=Access-Control-Allow-Credentials
    Access-Control-Allow-Origin
   spring.cloud.gateway.routes[62].filters[2].name=Retry
   spring.cloud.gateway.routes[62].filters[2].args.retries=3
   spring.cloud.gateway.routes[62].filters[2].args.statuses=${retryable_statuses}
   spring.cloud.gateway.routes[62].filters[2].args.methods=GET,POST
   ```

```
spring.cloud.gateway.routes[62].filters[2].args.backoff.firstBackoff=10ms

spring.cloud.gateway.routes[62].filters[2].args.backoff.maxBackoff=50ms
```

3. Restart Gateway service by typing the following commands:

   `docker service scale PAGatewayService_gateway-service=0docker service scale PAGatewayService_gateway-service=1`

```
administrator@ubuntusan02:~$ docker service scale PAGatewayService_gateway-service=0
PAGatewayService_gateway-service scaled to 0
overall progress: 0 out of 0 tasks
verify: Service converged
administrator@ubuntusan02:~$ docker service scale PAGatewayService_gateway-service=1
PAGatewayService_gateway-service scaled to 1
overall progress: 1 out of 1 tasks
1/1: running   [==================================================>]
verify: Service converged
administrator@ubuntusan02:~$
```

4. Update the `haproxy.cfg` file in the following location: `{{installation path }}/PlantApplicationsDocker/plantapps-web-docker/mnt/paweb/config/`.
5. Add the following configuration: `use_backend gatewayServiceBackend if { path -i -m reg -i ^[^\.]*-nodered-app }`

```
frontend localnodes-https

bind  *:5059 ssl crt /usr/local/etc/haproxy/haserver.pem

use_backend gatewayServiceBackend if { path -i -m reg -i ^[^\.]*-nodered-app }
```

6. Restart the Haproxy service by typing the following commands:

   `docker service scale PAHaproxy_haproxy=0docker service scale PAHaproxy_haproxy=1`

```
administrator@ubuntusan02:~$ docker service scale PAHaproxy_haproxy=0
PAHaproxy_haproxy scaled to 0
overall progress: 0 out of 0 tasks
verify: Service converged
administrator@ubuntusan02:~$ docker service scale PAHaproxy_haproxy=1
PAHaproxy_haproxy scaled to 1
overall progress: 1 out of 1 tasks
1/1: running   [==================================================>]
verify: Service converged
administrator@ubuntusan02:~$
```

Replace the SSL Certificate of Enterprise Edition Web Client

Before you begin

Install Plant Applications Enterprise Edition Web Client.

About this task

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.

Procedure

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

About this task

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 all certificate levels: the Root CA, the Intermediate Enterprise Certificate, and the Server Certificate. After you obtain the correct certificate, use the following steps.

Procedure

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

Parameter	Description
PROFICY_AUTHENTI-CATION_PEM_PATH: ""	Enter the path where the valid CA key file is located. For example, `PROFICY_AUTHENTICATION_PEM_PATH: "/home/adminis-trator/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

About this task

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 *(on page 81)*
- Message Bridge credentials. See Reset Message Bridge Credentials *(on page 82)*
- CouchDB credentials. See Reset CouchDB Credentials *(on page 83)*

Reset SQL Credentials

Procedure

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/"`

Parameter	Description
PLANT_APPS_DB_SERVER: ""	Enter the Plant Applications database server host-name 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

Procedure

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

Procedure

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_INSTAL-`

Parameter	Description
	`LATION_PATH: "/home/ administrator/in-stall/"`
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

About this task

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

Procedure

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

Procedure

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

About this task

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

Procedure

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

Procedure

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

About this task

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.

Procedure

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:

Issue	Resolution
	`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.

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-2023` 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

About this task

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

Procedure

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)

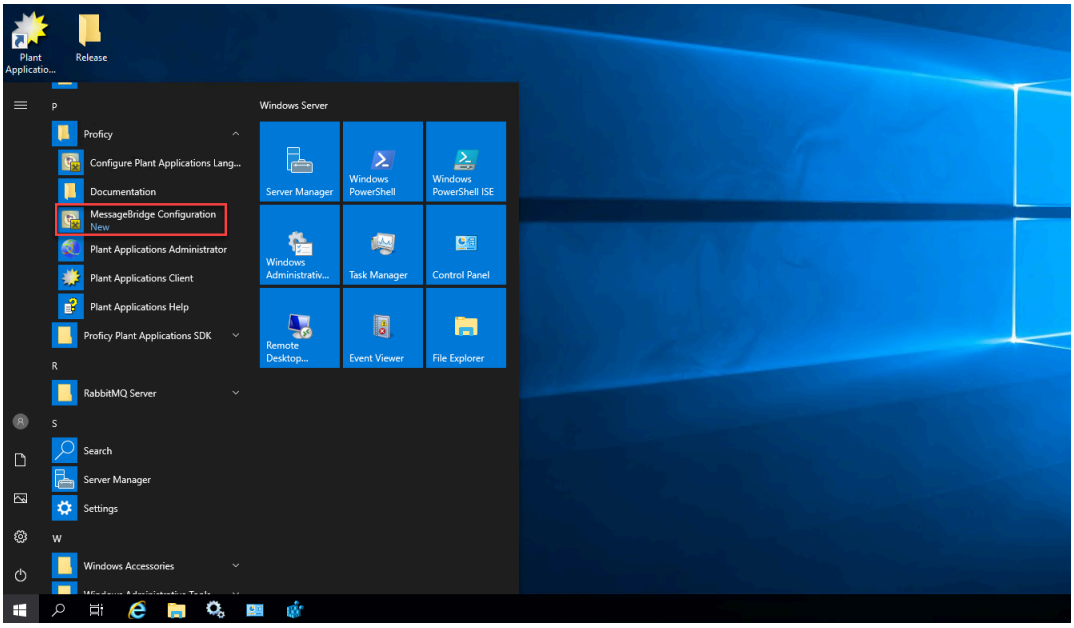
Run the Message Bridge Configuration Utility

About this task

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

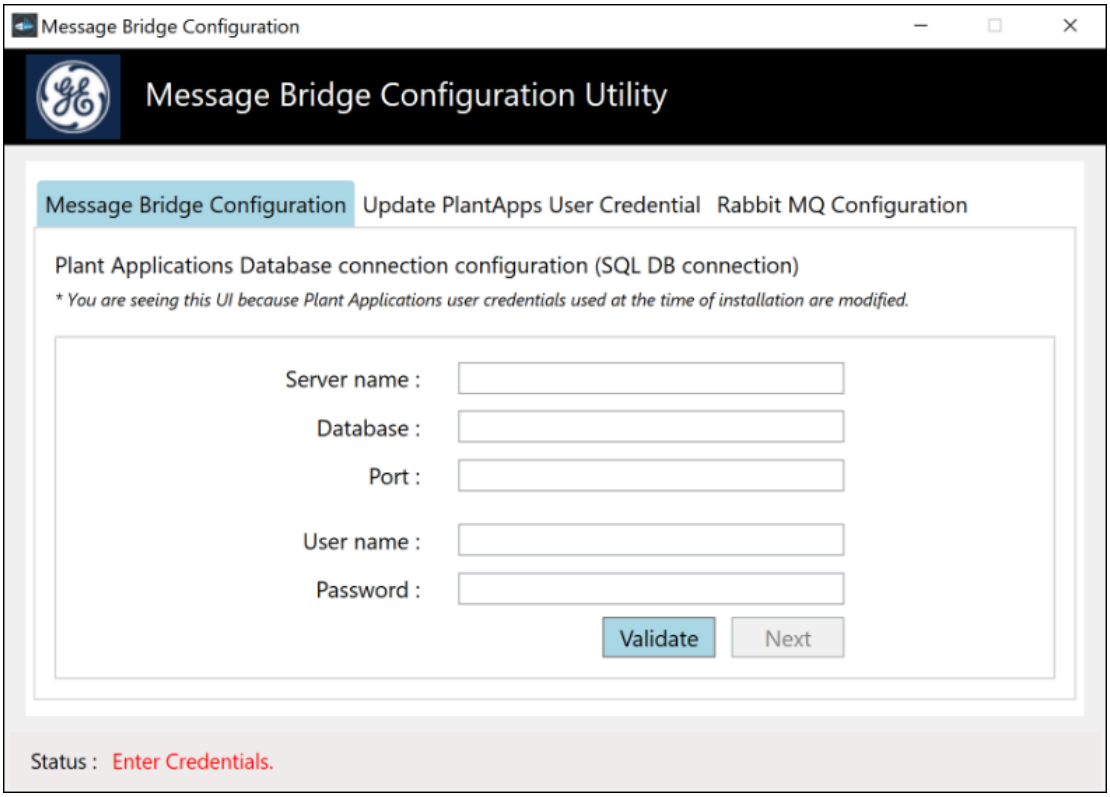
Procedure

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.



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

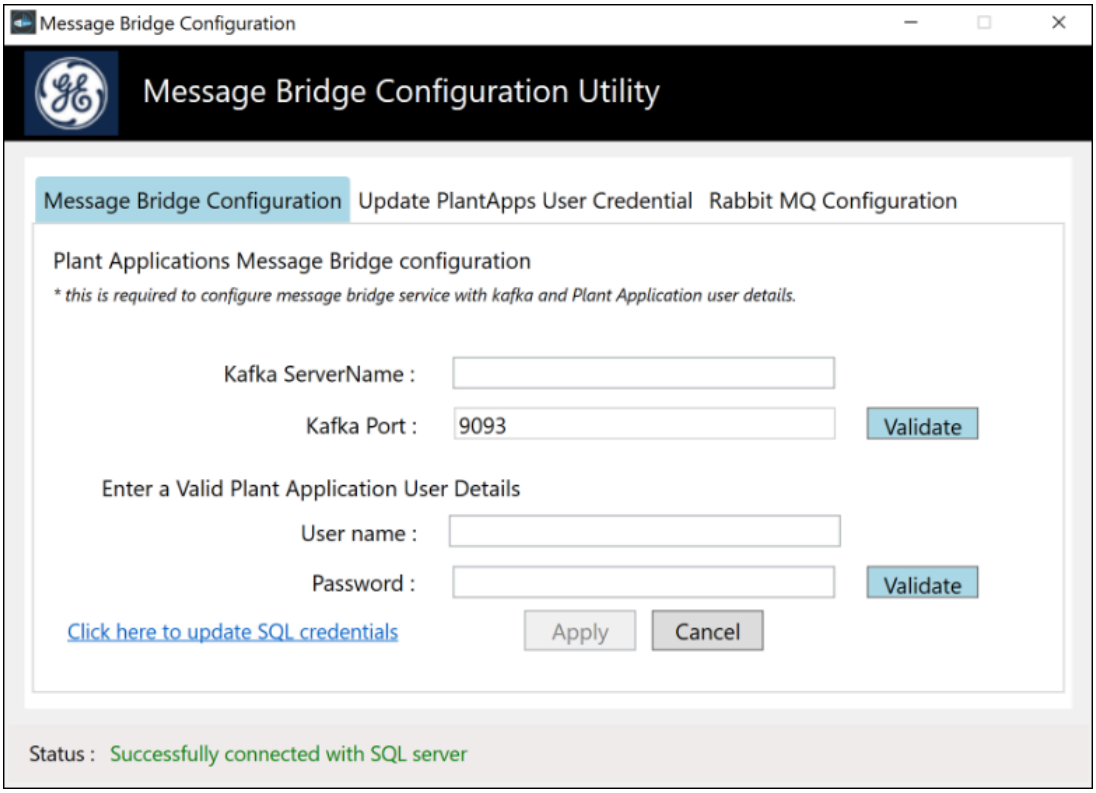
> **Note:**
> The **Message Bridge Configuration** utility prompts to enter the Plant Applications Database connection details only for the first time you access the utility. Once the connection is established, the utility automatically fetches the database details for the next time you access the utility.

Cre-dential	Description
Server name	Enter the server name where the SQL database is installed.
Data-base	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.

Cre-dential	Description
	Note: The default port is 1433.
User-name	Enter the user name that has permissions to access the database you entered in the **Database** field.
Pass-word	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.



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

Credential	Description
Kafka Server-Name	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.

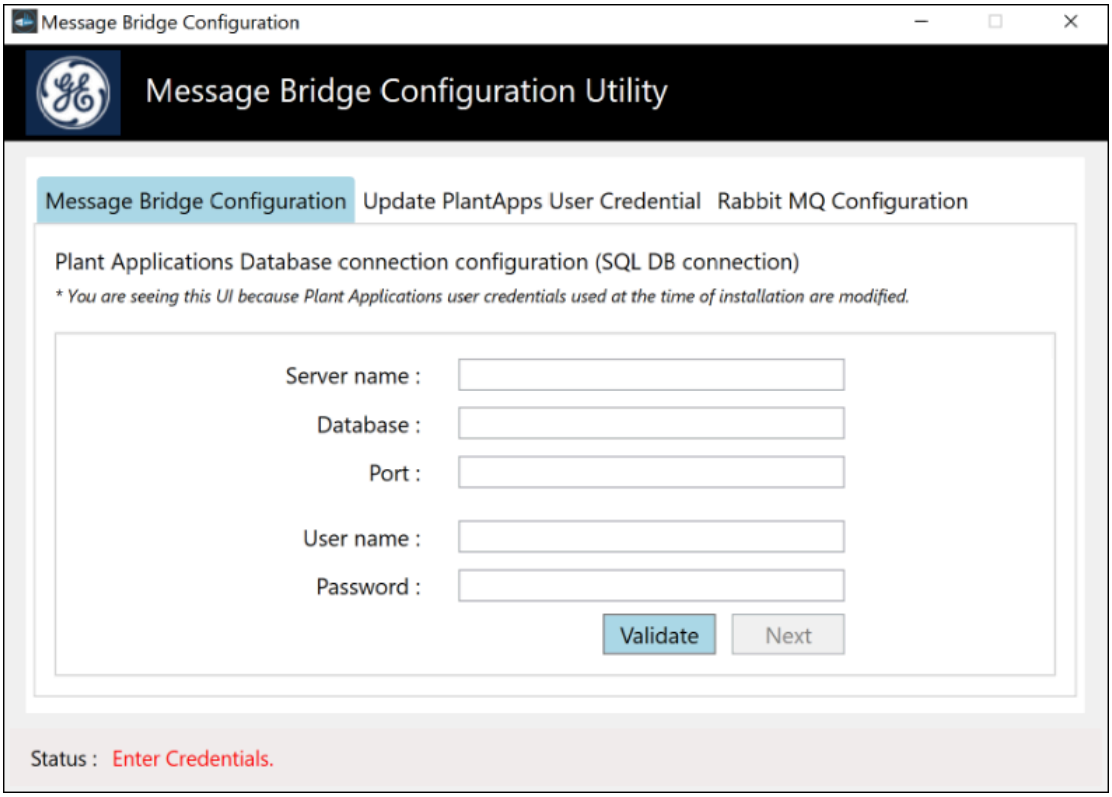
Update Message Bridge User Credentials

About this task

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

Procedure

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



Credential	Description
User Name	Enter the user name for an administrator account in Plant Applications.
Password	Enter the password.
Update	Select to update the Plant Applications Administrator credentials for Message Bridge service.

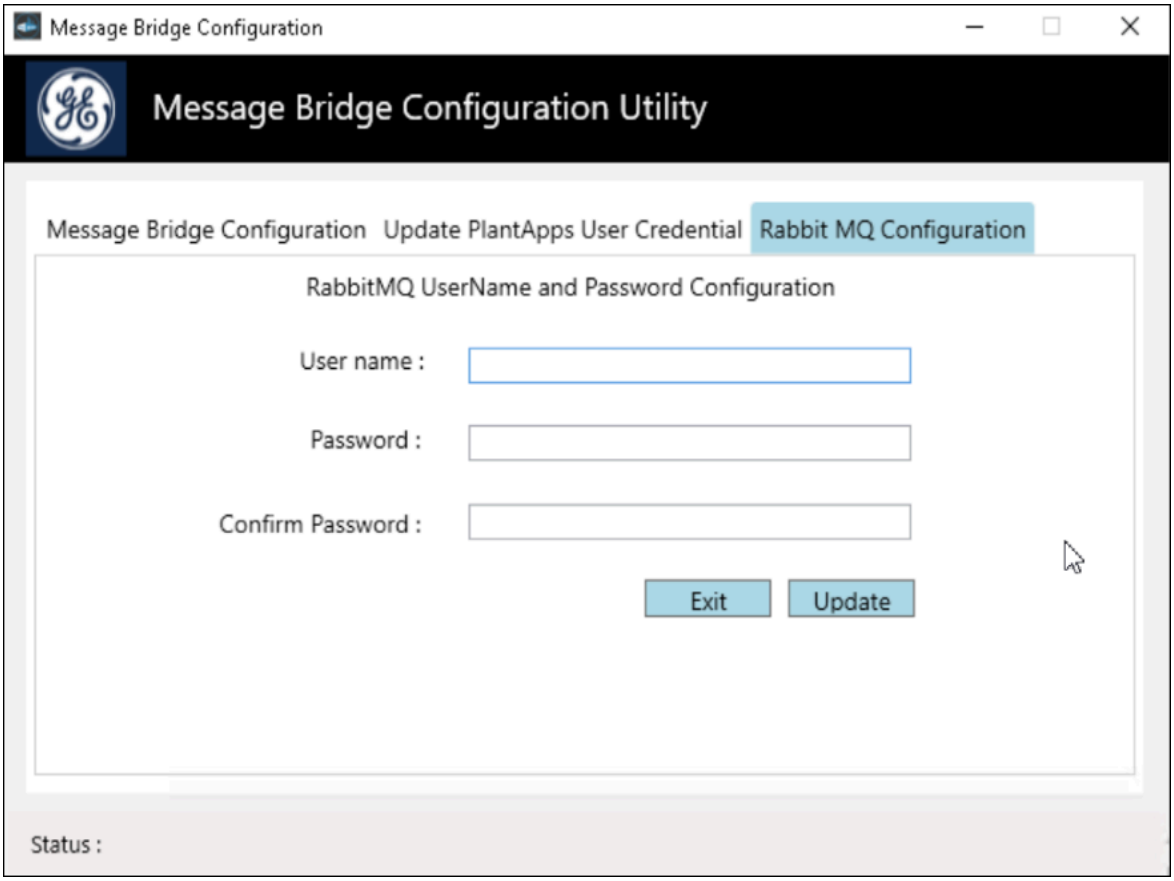
Update Rabbit MQ Credentials

About this task

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

Procedure

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



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

Before you begin

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

Procedure

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

About this task

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

Starting Plant Applications 2022, the default https port is 443. If you use the default port, you need not include it in the Rest API calls.

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. See Swagger URLs of Rest Services *(on page 98)*.

For exchanging data between the client-server system, user authentication is required.

Procedure

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. To access the Swagger UIs, you must perform following steps in the Operations Hub Server:
   a. Go to the `<Installation Drive>:\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.

Field	Description
	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}

Swagger URLs of Rest Services

Srno	Service Name	Swagger URLs
1	access-control-service	`https://<FQDN or Hostname>:5059/access-control-service/swagger-ui.html`
2	activities-app-service	`https://<FQDN or Hostname>:5059/activities-app-service/swagger-ui.html`
3	activities-service	`https://<FQDN or Hostname>:5059/activities-service/swagger-ui.html`

Srno	Service Name	Swagger URLs
4	alarm-app-service	`https://<FQDN or Hostname>:5059/alarm-app-service/swagger-ui.html`
5	alarm-service	`https://<FQDN or Hostname>:5059/alarm-service/swagger-ui.html`
6	approval-cockpit-app-service	`https://<FQDN or Hostname>:5059/approval-cockpit-app-service/swagger-ui.html`
7	approval-cockpit-service	`https://<FQDN or Hostname>:5059/approval-cockpit-service/swagger-ui.html`
8	assignment-service	`https://<FQDN or Hostname>:5059/assignment-service/swagger-ui.html`
9	bom-management-app-service	`https://<FQDN or Hostname>:5059/bom-management-app-service/swagger-ui.html`
10	comment-app-service	`https://<FQDN or Hostname>:5059/comment-app-service/swagger-ui.html`
11	comment-service	`https://<FQDN or Hostname>:5059/comment-service/swagger-ui.html`
12	document-management-service	`https://<FQDN or Hostname>:5059/document-management-service/swagger-ui.html`
13	downtime-app-service	`https://<FQDN or Hostname>:5059/downtime-app-service/swagger-ui.html`
14	downtime-service	`https://<FQDN or Hostname>:5059/downtime-service/swagger-ui.html`
15	erp-export-service	`https://<FQDN or Hostname>:5059/erp-export-service/swagger-ui.html`
16	erp-import-service	`https://<FQDN or Hostname>:5059/erp-import-service/swagger-ui.html`
17	erp-scheduler-service	`https://<FQDN or Hostname>:5059/erp-scheduler-service/swagger-ui.html`
18	erp-transformation-service	`https://<FQDN or Hostname>:5059/erp-transformation-service/swagger-ui.html`

Srno	Service Name	Swagger URLs
19	esignature-app-service	`https://<FQDN or Hostname>:5059/esignature-app-service/swagger-ui.html`
20	esignature-service	`https://<FQDN or Hostname>:5059/esignature-service/swagger-ui.html`
21	external-config-app-service	`https://<FQDN or Hostname>:5059/external-config-app-service/swagger-ui.html`
22	external-config-service	`https://<FQDN or Hostname>:5059/external-config-service/swagger-ui.html`
23	labor-service	`https://<FQDN or Hostname>:5059/labor-service/swagger-ui.html`
24	mes-dataservice	`https://<FQDN or Hostname>:5059/mes-dataservice/swagger-ui.html`
25	mes-service	`https://<FQDN or Hostname>:5059/mes-service/swagger-ui.html`
26	mymachines-service	`https://<FQDN or Hostname>:5059/mymachines-service/swagger-ui.html`
27	nonconformance-app-service	`https://<FQDN or Hostname>:5059/nonconformance-app-service/swagger-ui.html`
28	nonconformance-service	`https://<FQDN or Hostname>:5059/nonconformance-service/swagger-ui.html`
29	operator-app-service	`https://<FQDN or Hostname>:5059/operator-app-service/swagger-ui.html`
30	pa-mymachines-service	`https://<FQDN or Hostname>:5059/pa-mymachines-service/swagger-ui.html`
31	plant-execution-service	`https://<FQDN or Hostname>:5059/plant-execution-service/swagger-ui.html`
32	process-order-service	`https://<FQDN or Hostname>:5059/process-order-service/swagger-ui.html`
33	processanalyzer-service	`https://<FQDN or Hostname>:5059/processanalyzer-service/swagger-ui.html`

Srno	Service Name	Swagger URLs
34	product-service	`https://<FQDN or Hostname>:5059/product-service/swagger-ui.html`
35	productionmetrics-app-service	`https://<FQDN or Hostname>:5059/productionmetrics-app-service/swagger-ui.html`
36	productionmetrics-service	`https://<FQDN or Hostname>:5059/productionmetrics-service/swagger-ui.html`
37	productionscheduler-app-service	`https://<FQDN or Hostname>:5059/productionscheduler-app-service/swagger-ui.html`
38	property-definition-app-service	`https://<FQDN or Hostname>:5059/property-definition-app-service/swagger-ui.html`
39	property-definition-service	`https://<FQDN or Hostname>:5059/property-definition-service/swagger-ui.html`
40	reasons-service	`https://<FQDN or Hostname>:5059/reasons-service/swagger-ui.html`
41	receiving-inspection-app-service	`https://<FQDN or Hostname>:5059/receiving-inspection-app-service/swagger-ui.html`
42	receiving-inspection-service	`https://<FQDN or Hostname>:5059/receiving-inspection-service/swagger-ui.html`
43	route-app-service	`https://<FQDN or Hostname>:5059/route-app-service/swagger-ui.html`
44	route-service	`https://<FQDN or Hostname>:5059/route-service/swagger-ui.html`
45	security-administration-app-service	`https://<FQDN or Hostname>:5059/security-administration-app-service/swagger-ui.html`
46	security-service	`https://<FQDN or Hostname>:5059/security-service/swagger-ui.html`
47	segments-definition-service	`https://<FQDN or Hostname>:5059/segments-definition-service/swagger-ui.html`
48	spc-app-service	`https://<FQDN or Hostname>:5059/spc-app-service/swagger-ui.html`

Srno	Service Name	Swagger URLs
49	supervisor-app-service	`https://<FQDN or Hostname>:5059/supervisor-app-service/swagger-ui.html`
50	time-booking-app-service	`https://<FQDN or Hostname>:5059/time-booking-app-service/swagger-ui.html`
51	usersettings-service	`https://<FQDN or Hostname>:5059/usersettings-service/swagger-ui.html`
52	waste-management-app-service	`https://<FQDN or Hostname>:5059/waste-management-app-service/swagger-ui.html`
53	waste-management-service	`https://<FQDN or Hostname>:5059/waste-management-service/swagger-ui.html`
54	webgenealogy-app-service	`https://<FQDN or Hostname>:5059/webgenealogy-app-service/swagger-ui.html`
55	work-order-history-service	`https://<FQDN or Hostname>:5059/work-order-history-service/swagger-ui.html`
56	work-order-service	`https://<FQDN or Hostname>:5059/work-order-service/api-docs/index.html`
57	operator-app-log-service	`https://<FQDN or Hostname>:5059/operator-app-log-service/swagger-ui.html`
58	operator-log-service	`https://<FQDN or Hostname>:5059/operator-log-service/swagger-ui.html`
59	line-overview-service	`https://<FQDN or Hostname>:5059/line-overview-service/swagger-ui.html`
60	line-overview-app-service	`https://<FQDN or Hostname>:5059/line-overview-app-service/swagger-ui.html`
61	autolog-service	`https://<FQDN or Hostname>:5059/autolog-service/swagger-ui.html`
62	autolog-app-service	`https://<FQDN or Hostname>:5059/autolog-app-service/swagger-ui.html`

Configure a Proficy Historian Server for the Analysis Application

About this task

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.

Procedure

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 Web server.

Property	Description
`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.

Results

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

Configure the Cache Settings for the Historian Tags

About this task

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

Procedure

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`
`historianTagCa-`	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

Property	Description
`cheTime-Out`	`h`, `m`, or `s` to indicate time in hours, minutes, or seconds, respectively. The default value is `6h`. Example: `historianTagCacheTimeOut=6h`
`sched-uler.tag-caching-.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.

Results

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

About this task

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

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

The caching properties of each service depend on two main parameters:

- **Time** - Describes the duration of caching. For example, if the day cache expiry duration is 24 hours for a particular cache, the data is stored for 24 hours duration. You can modify the duration of cache, as required.
- **Size** - Describes the data storage or caching size of the services. The data storage size provides you the number of keys stored. For example, if the day cache size is 100, it indicates that the data stored for that cache is limited to 100 keys or entities.

Note:
The size and time for the cache properties of services can be modified by the user. The following changes are observed if there is a significant change in cache size or time:

- If the size is increased, the cached data will consume more RAM and it increases the response time of APIs. Also, the system performance will go down.
- If the size is decreased, the cached data will overflow, and the PA service will try to retrieve it from the database. In such case the APIs' response time will increase, and there will be chances of missing the information on cached data, and/or the cached data value will be null in the respective field.

- If the time is increased, the cached data will consume more time to reflect on the UI, and there will be chances of fetching the outdated data.
- If the time is decreased, the performance of that service will decrease as the system will utilize the resources in the back end. Also, the APIs' response time will increase.

Procedure

1. **Enterprise Installation:** In the directory `<installFolder>/installation/PlantApplicationsDocker/plantapps-we-docker/mnt/configfiles/`, access the folder for the required services. For example, access `alarm-app-service`, then open the `prod` folder to access the `application.properties` file.
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. The caching properties are described based on its configuration as listed in the table.

Service Name	Properties	Description
plant-execution-service	scheduler_workorder_-timer_seconds = 21600	This service caches all the work order information associated with non-conformance. The cached data from the non-conformance application will be refreshed every 21600 seconds (6 hours).
	scheduler_mes_timer_-seconds = 1800	The scheduler runs every 1800 seconds (30 minutes), and will retrieve all the information and caches the following data: ◦ NCM context type ◦ Reason trees ◦ Product family ◦ Units

Service Name	Properties	Description
route-service	maximumProduct-CacheSize = 1000 cacheProductExpire-AfterAccess = 15m	This parameter caches the following data: ◦ Line by Id using line Id ◦ Units using line Id The data cached will be limited to 1000 keys and will expire every 15 minutes.
route-app-service	maximumProduct-CacheSize = 1000 cacheProductExpire-AfterAccess = 15m	This parameter caches the following data: ◦ All labor type information using labor type Id ◦ List of lines ◦ Line details by line Id ◦ All the Unit of Measure (UoM) details ◦ UoM by Id using UoM Id ◦ All the property data types information from property definition service ◦ Product family information using product family Id The data cached will be limited to 1000 keys and will expire every 15 minutes.
supervisor-app-service	supervisor.scheduler.delay = 3600000	In this service, the scheduler delay runs every 3600000 milliseconds (1 hour) to retrieve the stored information.
segment-definition-service	maximumCacheSize = 100 cacheExpireAfterAccess = 50m	This parameter caches the following data: ◦ Lines using line Id ◦ Units for line using line Id for unit ◦ All units ◦ Labor type using labor type Id The data cached will be limited to 100 keys and will expire every 50 minutes.
operator-app-service	mes.redis.cache.duration = DAYS mes.redis.cache-.time-to-live = 1	In this service, the redis cache key is used to store the cached data for a day (24 hours). The data cached will be refreshed every 24 hours.

Service Name	Properties	Description
erp-import-service	maximumCacheSize = 100 cacheExpireAfterWrite = 5m	The ERP import service will cache the planned lines. The information cached will be limited to 100 keys and will expire every 5 minutes. **Note:** In the erp-import-service, the data is transferred from ERP to MES.
erp-export-service	maximumCacheSize = 100 cacheExpireAfterWrite = 5m	The ERP export service will cache the following data: ◦ Production lines ◦ Units The data cached will be limited to 100 keys and will expire every 5 minutes. **Note:** In the erp-export-service, the data is transferred from MES to ERP.
	cacheLaborExpireAfterAccess = 60m	The ERP export service will cache the labor type data. The data cached will expire every 60 minutes (1 hour).
process-analyzer-app-service	maximumCacheSize = 100 cacheExpireAfterAccess = 20m	This parameter is used to cache the event or the batch information. The information cached will be limited to 100 keys and will expire every 20 minutes.
	tagVariableMaxCacheSize = 100 tagVariableCacheTimeOut = 6h	This parameter is used to cache the tags and variables. The data cached will be limited to 100 keys and will expire every 6 hours.

Service Name	Properties	Description
	kpiMaxCacheSize = 40 kpiCacheTimeOut = 30m	This parameter is used to cache the KPIs. The data cached will be limited to 40 keys and will expire every 30 minutes.
	siteParameterMax-CacheSize = 20 siteParameterCache-TimeOut = 1h	This parameter is used to cache the site parameters. The data cached will be limited to 40 keys and will expire every hour.
mes-data-service	historianTagMaxCache-Size = 50000 historianTagCacheTime-Out = 6h	This parameter is used to cache the historian tag information. The data cached will be stored in 50000 keys and will expire every 6 hours.
	scheduler.tagcaching-.seconds = 21600	The scheduler runs every 21600 seconds (6 hours) to internally cache the tags.
alarm-app-service	maximumDayCacheSize = 100 cacheDayExpireAfterAc-cess = 12h	This parameter caches the following data: ◦ Variables under the unit ◦ Alarm sheet for the variables The data cached will be limited to 100 keys and will expire every 12 hours.
	maximumShiftCache-Size = 100 cacheExpireAfterShift-Access = 8h	This parameter caches the following data: ◦ Reason tree nodes ◦ Reason tree header The data cached will be limited to 100 keys and will expire every 8 hours.
	maximumHourCache-Size = 100 cacheExpireAfterHour-Access = 1h	This parameter is used to cache the specification limits for the variables. The data cached will be limited to 100 keys and will expire every hour.
productionmetrics-app-service	maximumDayCacheSize = 100	This parameter caches the following data for a day cache: ◦ Current day performance summary ◦ Current day performance categories

Service Name	Properties	Description
	cacheDayExpireAfterAccess = 1h	◦ Current day quality distribution ◦ Current availability pareto ◦ Current availability category ◦ Current availability line gantt chart ◦ Current availability unit gantt chart ◦ Current day KPI The data cached will be limited to 100 keys and will expire every hour.
	maximumWeekCacheSize = 100 cacheWeekExpireAfterAccess = 24h	This parameter caches the following data for a week cache: ◦ Week performance summary ◦ Week performance categories ◦ Week quality distribution ◦ Week availability pareto ◦ Week availability category ◦ Week availability line gantt chart ◦ Week availability unit gantt chart ◦ Week KPI The data cached will be limited to 100 keys and will expire every 24 hours.
	maximumShiftCacheSize = 1 cacheShiftExpireAfterAccess = 10m	The shift cache data stores the list of shift information (i.e., the list of shifts of type S88R) in a single key or entity. The data cached will expire every 10 minutes.
downtime-app-service	maximumHourCacheSize = 100 cacheDayExpireAfterHourAccess = 1h	This parameter caches the following data for an hour cache: ◦ Top five reasons for the unit ◦ Active products for the units for the given intervals The data cached will be limited to 100 keys and will expire every hour.
	maximumShiftCacheSize = 100	This parameter caches the following data for a shift cache:

Service Name	Properties	Description
	cacheExpireAfterShift-Access = 8h	◦ Reason headers for the unit ◦ Reason options for the unit ◦ Fault options for the unit ◦ Product information for the given product Id The data cached will be limited to 100 keys and will expire every 8 hours.
production-sched-uler-app-service	maximumSize = 500 configurationCacheEx-piryTime = 30m	This parameter caches the following data: ◦ Unit of measure ◦ Property definition data types The data cached will be limited to 500 keys and will expire every 30 minutes.
	maximumSize = 500 configurationCacheEx-piryTime = 2h	This parameter is used to cache the user-name details for the given user Id. The data cached will be limited to 500 keys and will expire every 2 hours.
process-order-service	maximumSize = 5000 configurationCacheEx-piryTime = 10m	This parameter caches the following data: ◦ User Id for the given username ◦ Execution path permissions The data cached will be limited to 5000 keys and will expire every 10 minutes.
waste-management-app-service	maximumDayCacheSize = 1000 cacheDayExpireAfterAc-cess = 24h	This parameter is used to cache all the product records using the page size. The da-ta cached will be limited to 1000 keys and will expire every 24 hours.
	maximumShiftCache-Size = 100 cacheShiftExpireAfter-Access = 4h	This parameter caches the following data: ◦ Reason headers for unit. ◦ Reasons for unit. ◦ Groups for unit. The data cached will be limited to 100 keys and will expire every 4 hours.

Service Name	Properties	Description
webgenealogy-app-service	genealogy.scheduler-.timer.seconds = 36000	The scheduler runs every 36000 seconds (10 hours), and will retrieve all the information and caches the following data: ◦ All lines ◦ All units ◦ All Product family ◦ Material lot status
Bom-management-app-service	maximumCacheSize = 100 cacheExpireAfterWrite = 1h	This parameter caches the following data: ◦ All lines with units ◦ All engineering units ◦ Engineering unit by Id The data cached will be limited to 100 keys and will expire every hour.
Approval-cockpit-service	NA (observed a few cache properties defined in application.properties file but they are not in use).	NA
Approval-cockpit-app-service	NA (observed a few cache properties defined in application.properties file but they are not in use).	NA
Receiving-inspection-app-service	maximumCacheSize = 100 cacheExpireAfterWrite = 1h	This parameter caches the following data: ◦ Unit ◦ Line ◦ Production status The data cached will be limited to 100 keys and will expire every hour.
Receiving-inspection-service	maximumCacheSize = 100 cacheExpireAfterWrite = 1h	This parameter caches the following data: ◦ All units for the given line Id ◦ All data types The data cached will be limited to 100 keys and will expire every hour.

Service Name	Properties	Description
Time-booking-app-service	maximumCacheSize = 100 cacheExpireAfterWrite = 1h	This parameter caches the following data: ◦ Reason tree nodes ◦ All reason trees ◦ Lines ◦ Units ◦ Labor type records The data cached will be limited to 100 keys and will expire every hour.
property-definition-app-service	NA (observed a few-cache properties defined in application.properties file but they are not in use).	NA
property-definition-service	NA (observed a few-cache properties defined in application.properties file but they are not in use).	NA
usersettings-service	maximumDayCacheSize = 100 cacheDayExpireAfterAccess = 24h	This parameter is used to cache the user settings information. The data cached will be limited to 100 keys and will expire every 24 hours.
activities-app-service	maximumHourCacheSize = 100 cacheDayExpireAfterHourAccess = 1h	This parameter caches the following data: ◦ The activity Ids for the test record Ids ◦ Sheet display options ◦ Sheet custom form data ◦ Historian tag names ◦ Array data for the given array Id ◦ E-signature level for the variable ◦ E-signature approvers ◦ Variable specifications The data cached will be limited to 100 keys and will expire every hour.

Service Name	Properties	Description
	maximum5MinCache-Size = 100 cacheExpireAfter5Min-Access = 5m	This parameter caches the following data: ◦ Products on a unit ◦ Override lock security permission values for the user ◦ E-signature records The data cached will be limited to 100 keys and will expire every 5 minutes.
	maximumShiftCache-Size = 100 cacheExpireAfterShift-Access = 8h	This parameter is used to cache the product groups on a unit. The data cached will be limited to 100 keys and will expire every 8 hours.
activities-service	maximumHourCache-Size = 100 cacheDayExpireAfter-HourAccess = 1h	This parameter caches the following data: ◦ Activities view by groups ◦ Activity variable history ◦ Activity variable by activity Id ◦ Activity Ids for test records ◦ Activity custom data types The data cached will be limited to 100 keys and will expire every hour.
	maximumDayCacheSize = 100 cacheExpireAfterDayAccess = 24h	This parameter caches the following data: ◦ Time selection options ◦ Shifts ◦ Activity variable groups ◦ User Id for the given username The data cached will be limited to 100 keys and will expire every 24 hours.
esignature-app-service	maximumShiftCache-Size = 10 cacheExpireAfterShift-Access = 8h	This parameter caches the following data: ◦ Preferred units for user ◦ Tree nodes ◦ E-signature session inactive interval ◦ E-signature configuration The data cached will be limited to 10 keys and will expire every 8 hours.

Service Name	Properties	Description
my-machines-service	maximumDayCacheSize = 100 cacheExpireAfterAccess = 24h	This parameter is used to cache the preferred units. The data cached will be limited to 100 keys and will expire every 24 hours.
product-service	maximumProducts-CacheSize=1000 cacheProductExpire-AfterAccess=15m	This parameter is used to cache the products. The data cached will be limited to 1000 products and will expire every 15 minutes.

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

Results

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

Configure to Route Enable a Production Line

About this task

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

Procedure

1. To use a production line in discrete applications, route-enable each production line that you want to use by right-clicking the production line, and selecting **Route enabled <name of the production line>**. For more information, refer to the *About Enabling a Production Line for Using a Route* topic in the Plant Applications Administrator Help.
2. To import route-enabled production lines from one Plant Applications server to another, perform the following steps:
    a. Export the production lines and related data from the source server.
    b. In the destination server, create a sample production line, and add a sample unit.
    c. Right-click the production line that you have created, and select **Route enabled <name of the production line>**.
    d. Import the production lines and related data to the destination server.

e. Right-click each production line that you have imported, and then select **Route enabled <name of the production line>**.

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

Map LDAP Groups with Operations Hub UAA

About this task

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

For configuring LDAP or non LDAP users to Plant Applications Web Client, see Add a New User to the Plant Applications Web Client *(on page 122)*.

Map LDAP Groups With Proficy Authentication

About this task

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.

Procedure

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.

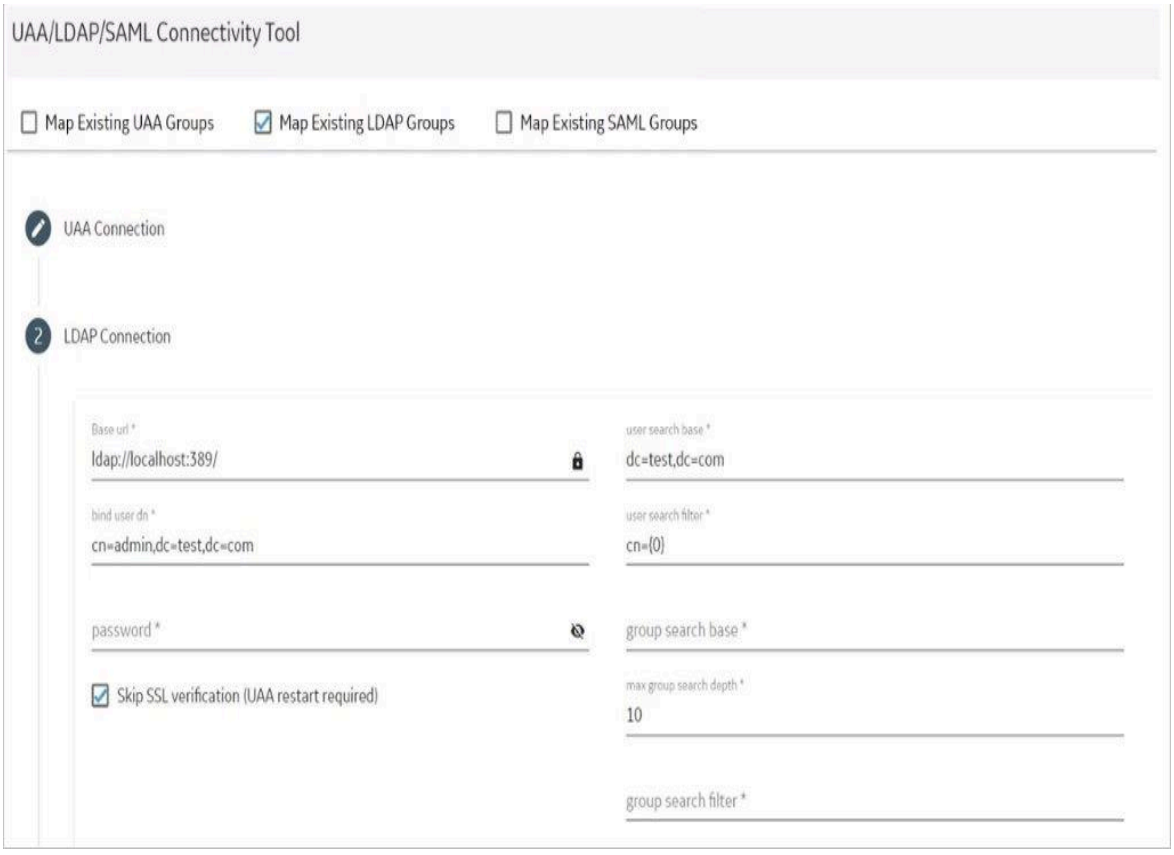
5. Select **Test**.
   If connection to the Proficy Authentication server is established, a message appears, confirming the same.

> **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.

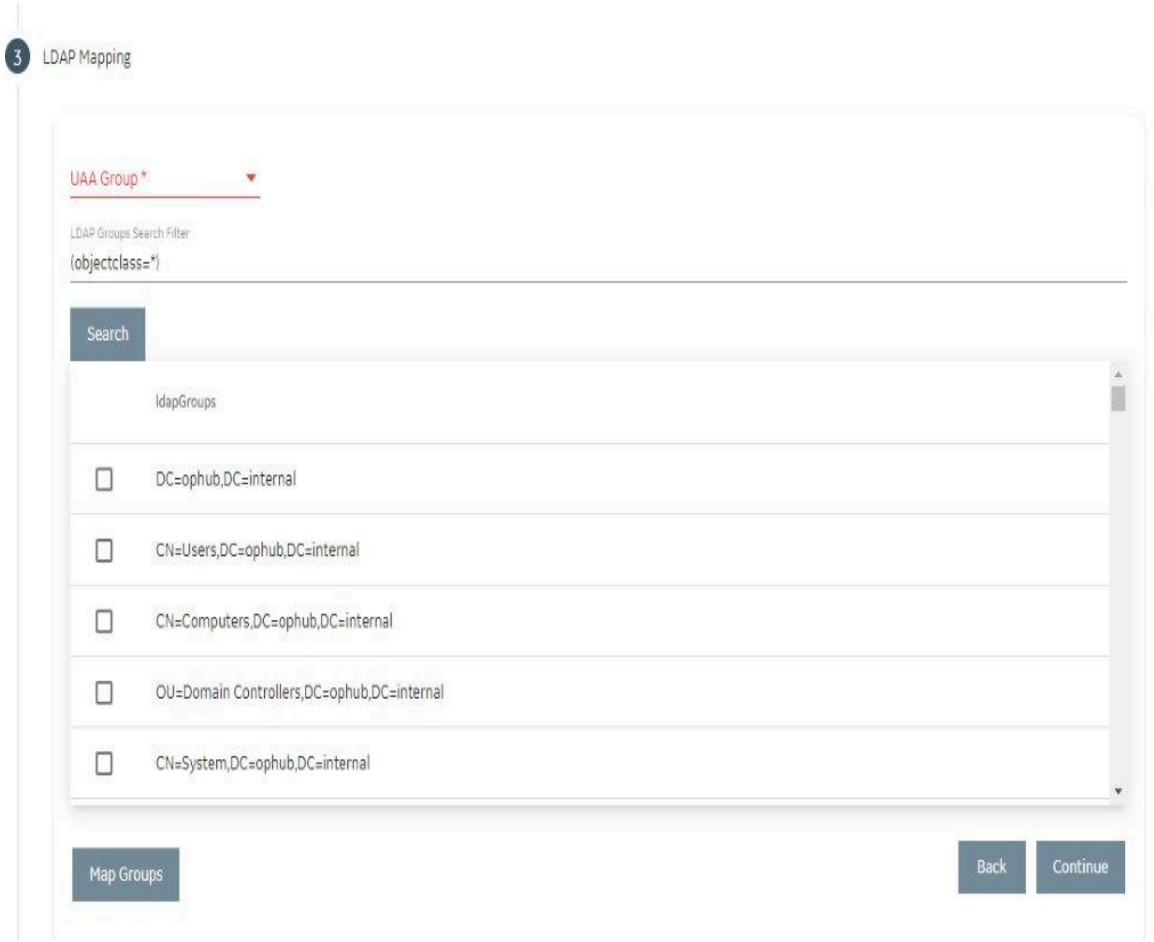
Field	Description
URL	Enter the base URL of the LDAP server (for example, https://localhost).
Bind User DN	Enter the distinguished name of the bind user (for example, cn=admin, ou=Users, dc=test, dc=com).
Password	Enter the password for the LDAP user ID that searches the LDAP tree for user information.
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}).

Field	Description
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}).



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.



> **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.

Results

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

About this task

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 *(on page 128)*. 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.

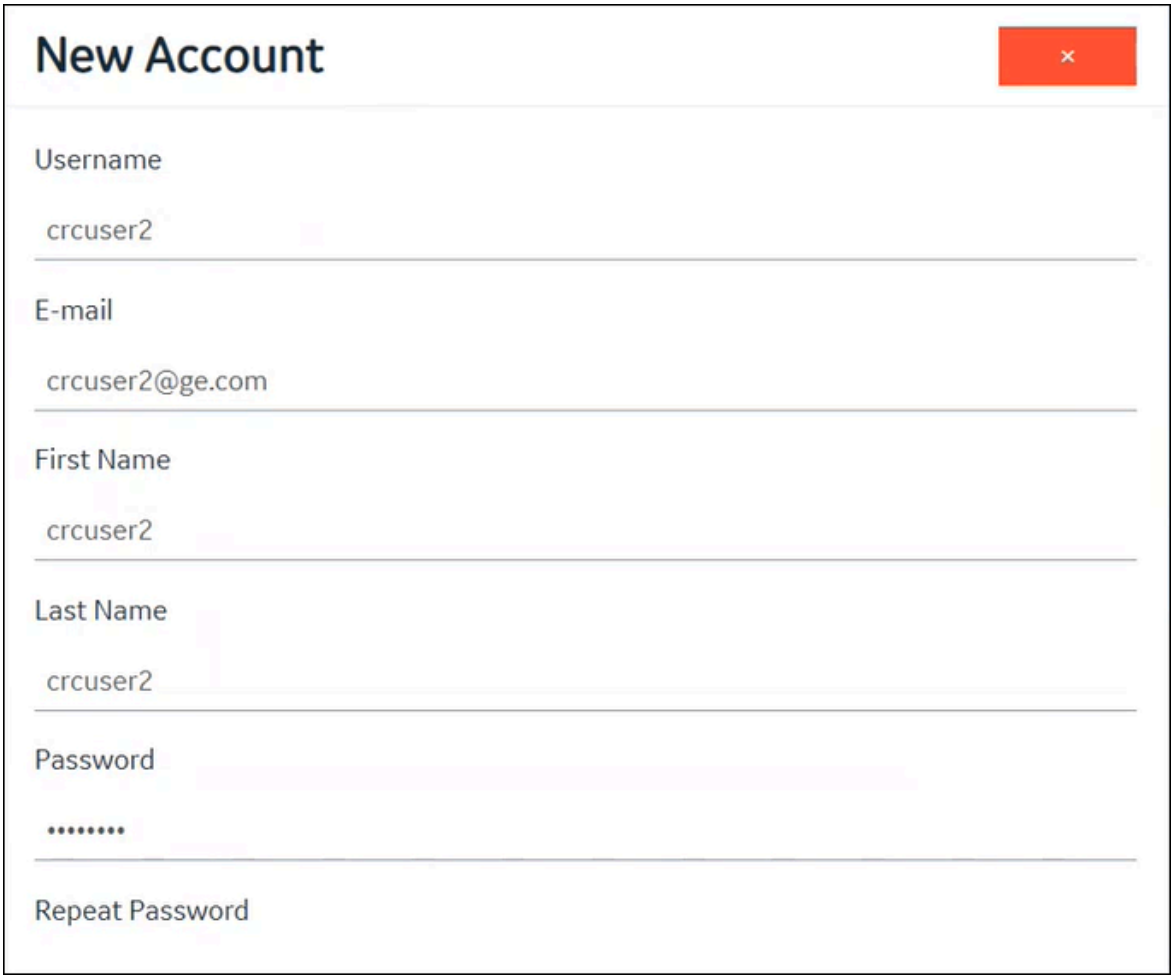
For LDAP user, see Map LDAP Groups With Proficy Authentication *(on page 118)*.

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.

Procedure

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.



3. Enter the required information in the following fields.

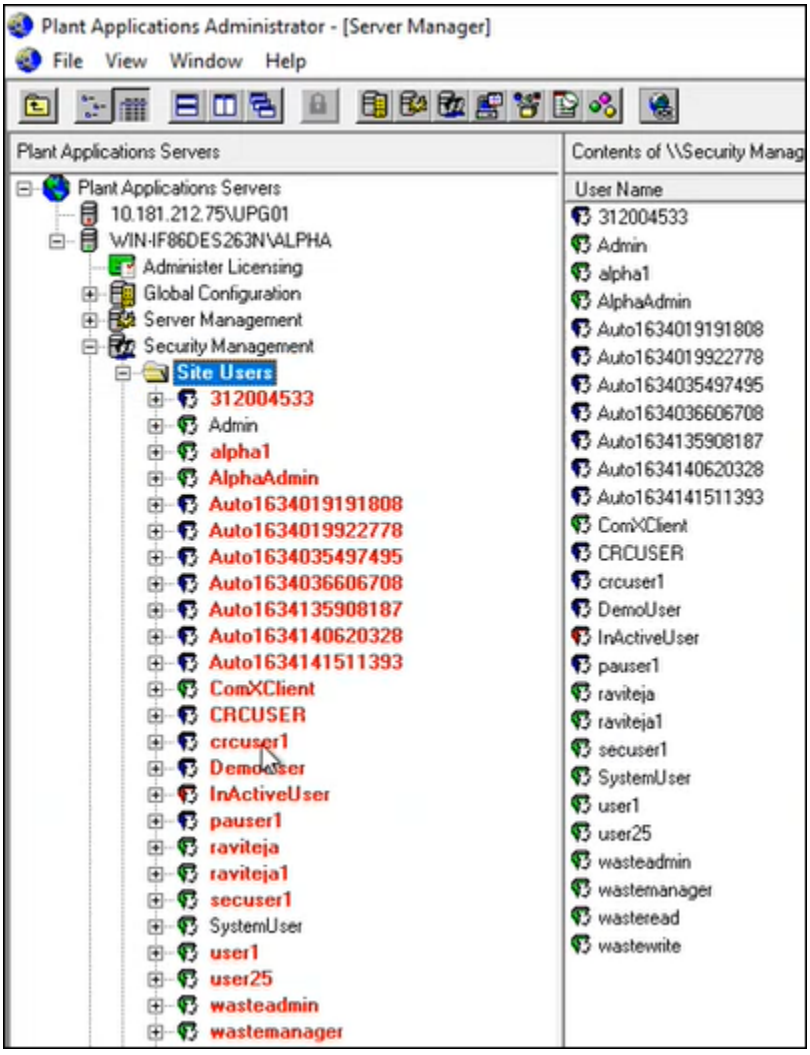
Field	Description
Username	Enter the user name the user will use to log in to Operations Hub. The value must be unique.
E-mail	Enter the email ID of the user. The value must be unique.
First Name	Enter the first name.
Last Name	Enter the last name.
Password	Enter a password that the user will use to log in to Operations Hub.
Repeat Password	Enter the password to confirm.

Field	Description
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.

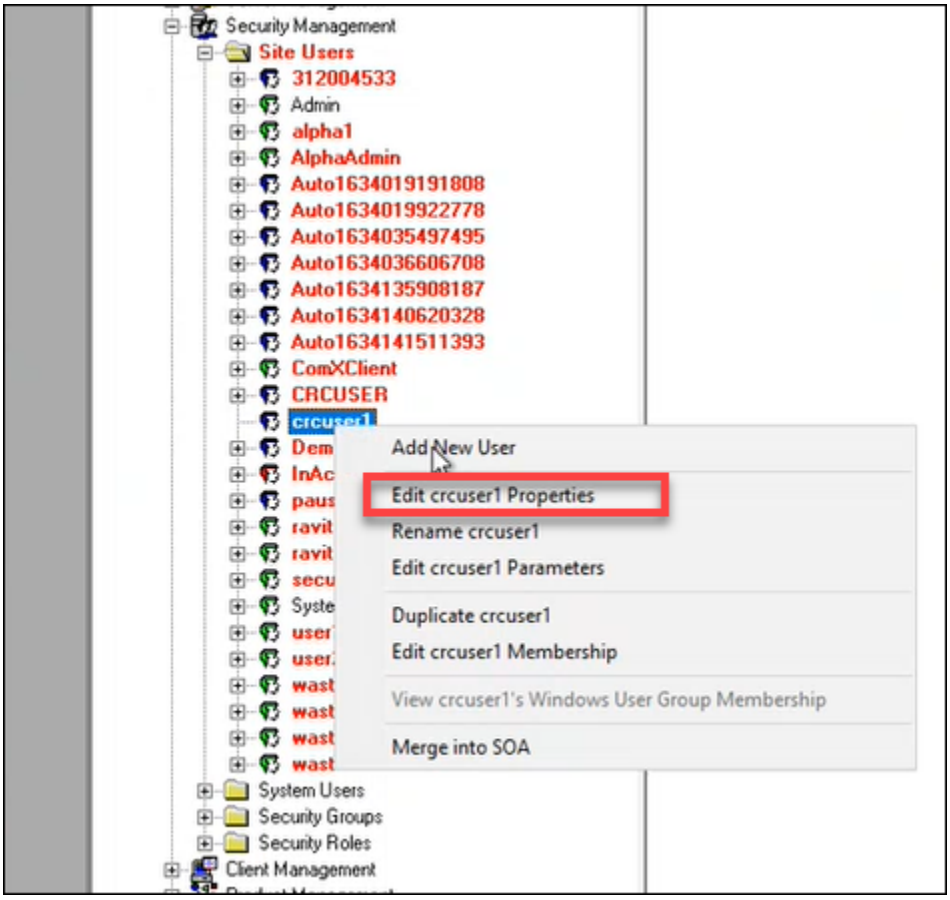
4. Select **Create**.
5. Log in to the Plant Application Web Client with the newly created user.

> **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.

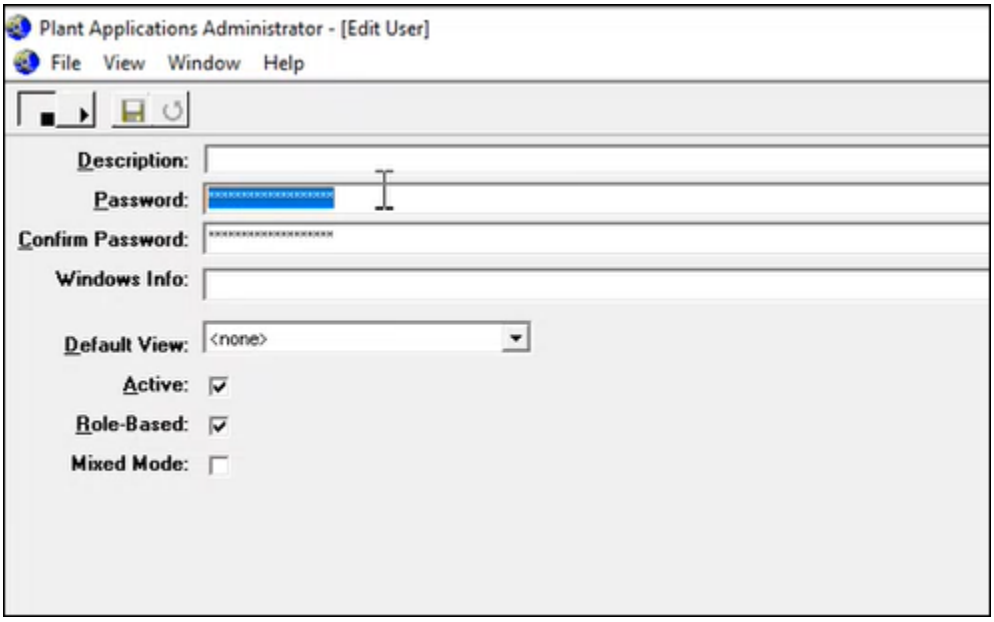
6. Log in to the **Plant Applications Administrator - [Server Manager]**.



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.



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.

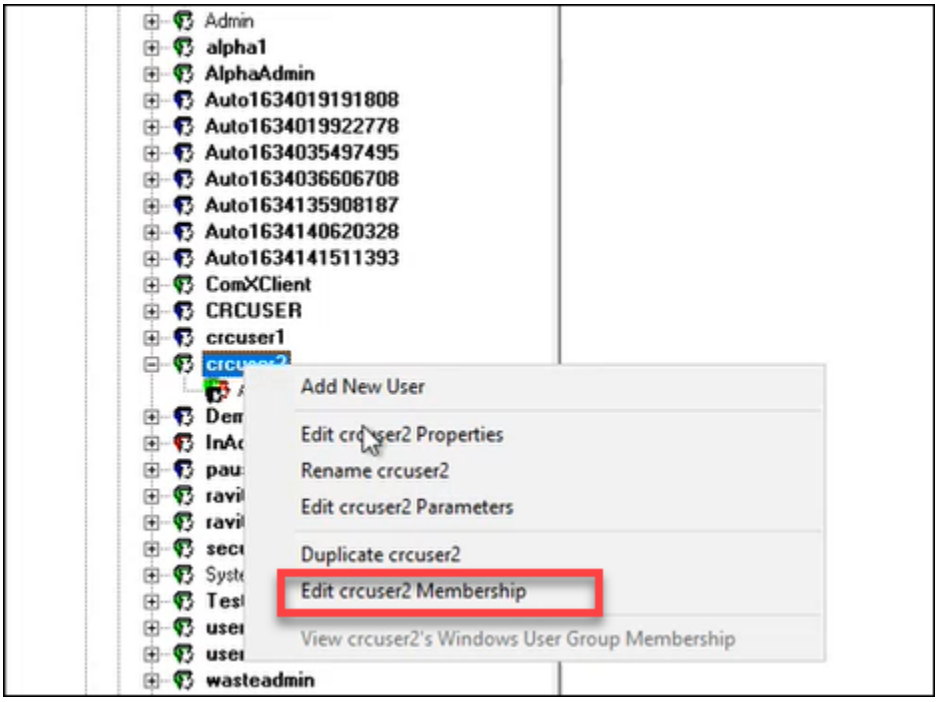
> **Note:**
> For LDAP users, you must update the **WindowsUser Info** field in **Users_Base** column in SQL directly. For example, update **Users_Base** for the following details: `SET WindowsUserInfo = 'xyzdomain.com\pa22user1'`, where Username = 'pa22user1'

> **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.

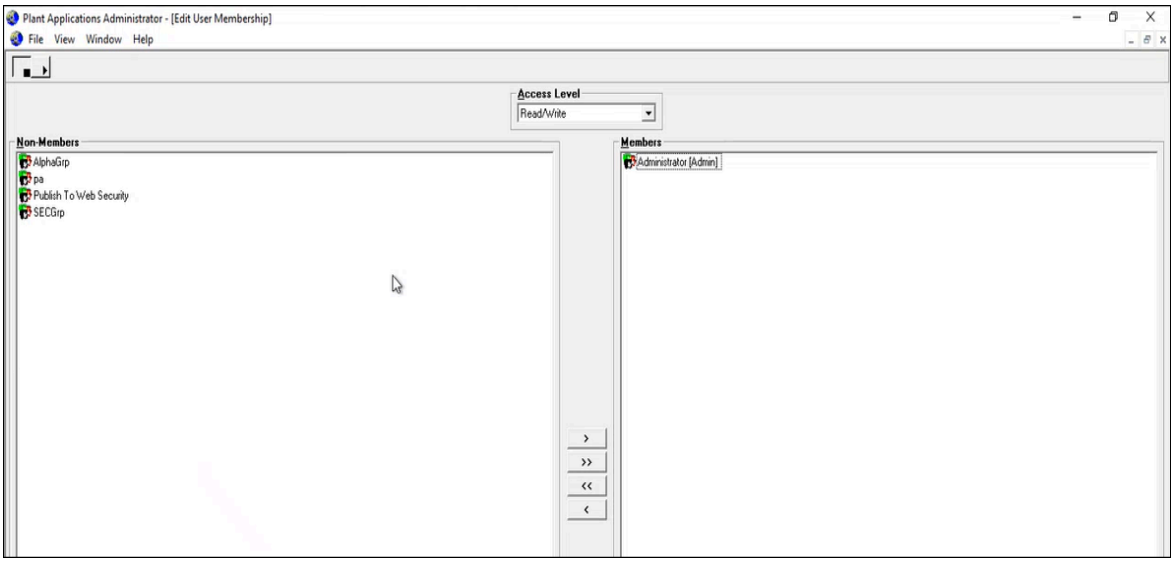
9. Select **Save**.

> **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.



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.

Procedure

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:

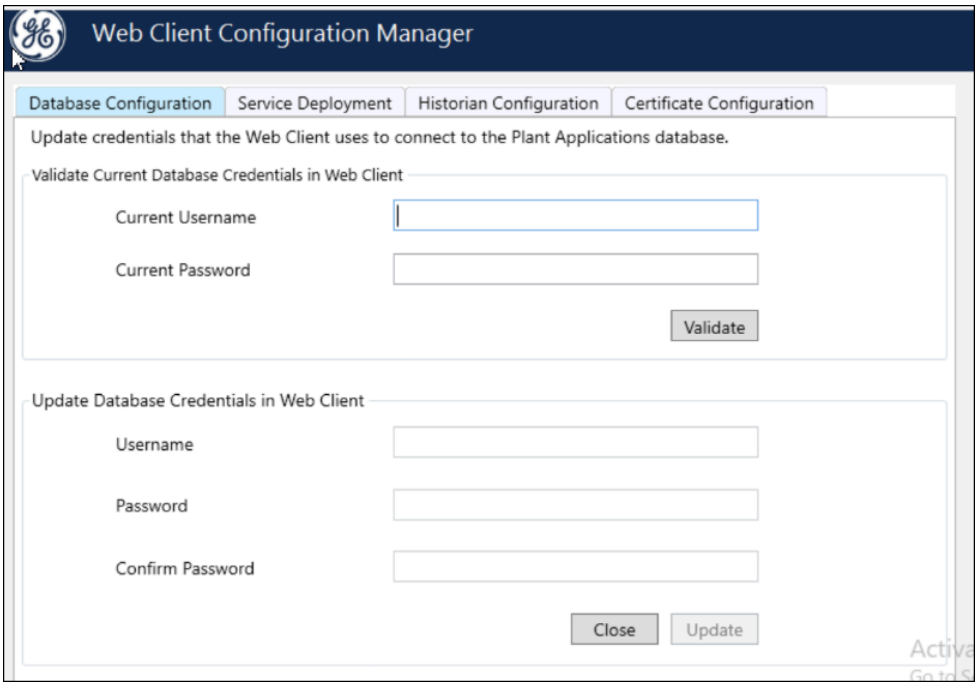
- Database passwords. See Update or Validate the Database Password *(on page 130)*
- Service deployments. See Deploy and Configure .War Files *(on page 132)*
- Historian configuration. See Update Historian Administrator Client Credentials *(on page 132)*
- Certificate configuration. See Import Certificates *(on page 134)*

Update or Validate the Database Password

About this task

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.



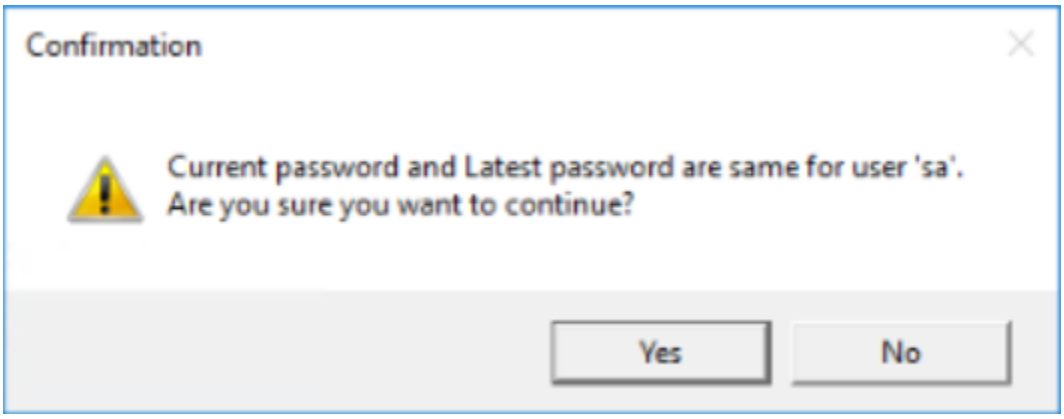
Procedure

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.

    c. Select **Yes** to confirm.

    A confirmation message appears for resetting the password.

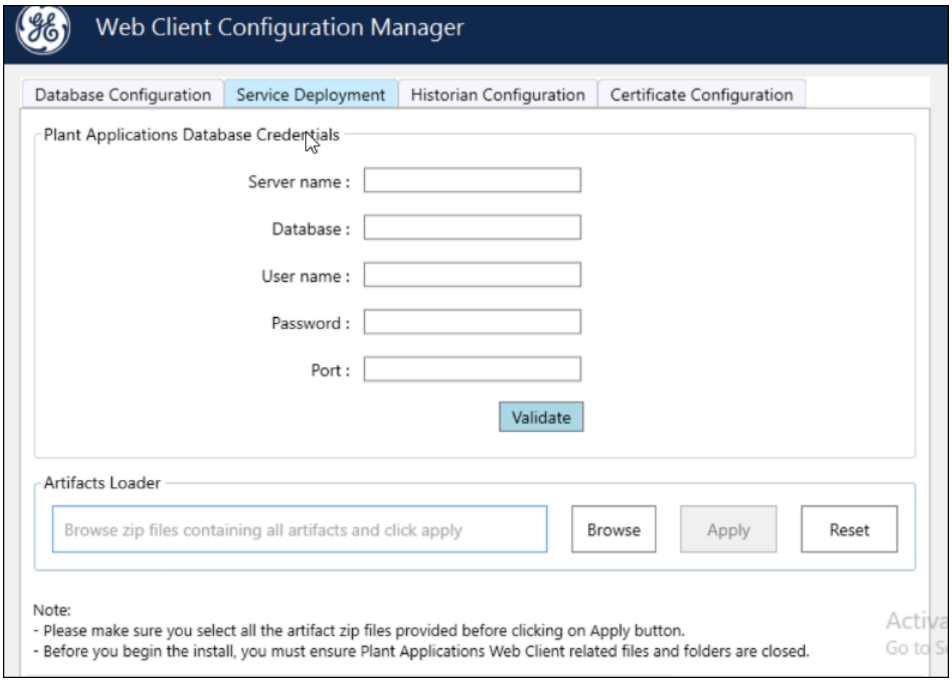
    d. Select **Yes** to update all the `.war` files with the latest password.

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

About this task

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.



Procedure

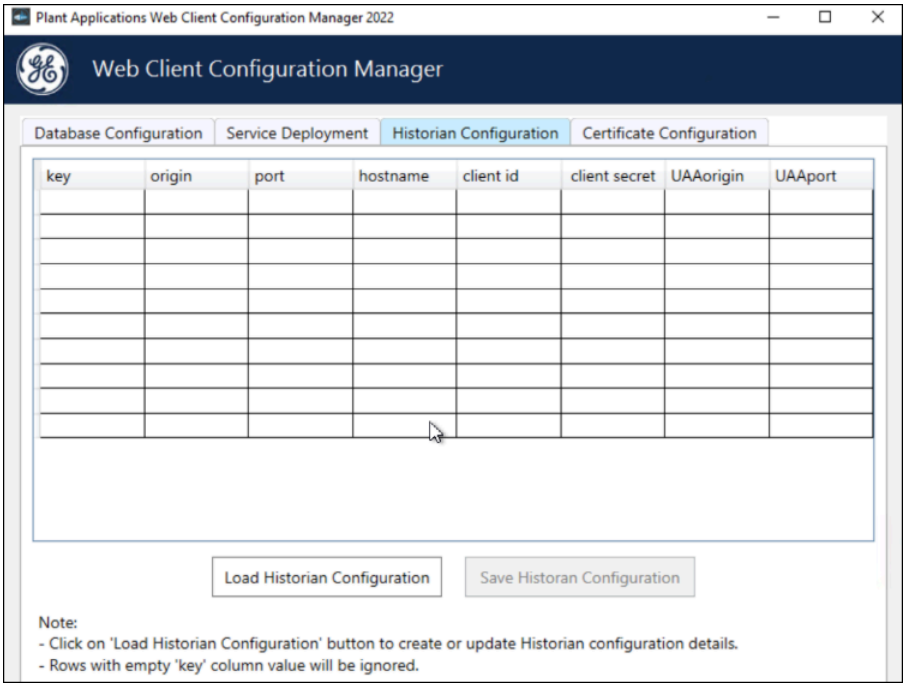
1. Enter the required information in the fields for the Plant Applications Database credentials.
2. Select **Validate**.
3. In the Artifacts Loader section, select the services artifacts to modify, then select **Browse** to select the zip file.
4. Select **Apply**.

   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

About this task

This tab allows you to update Historian administrator client credentials.



Procedure

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:

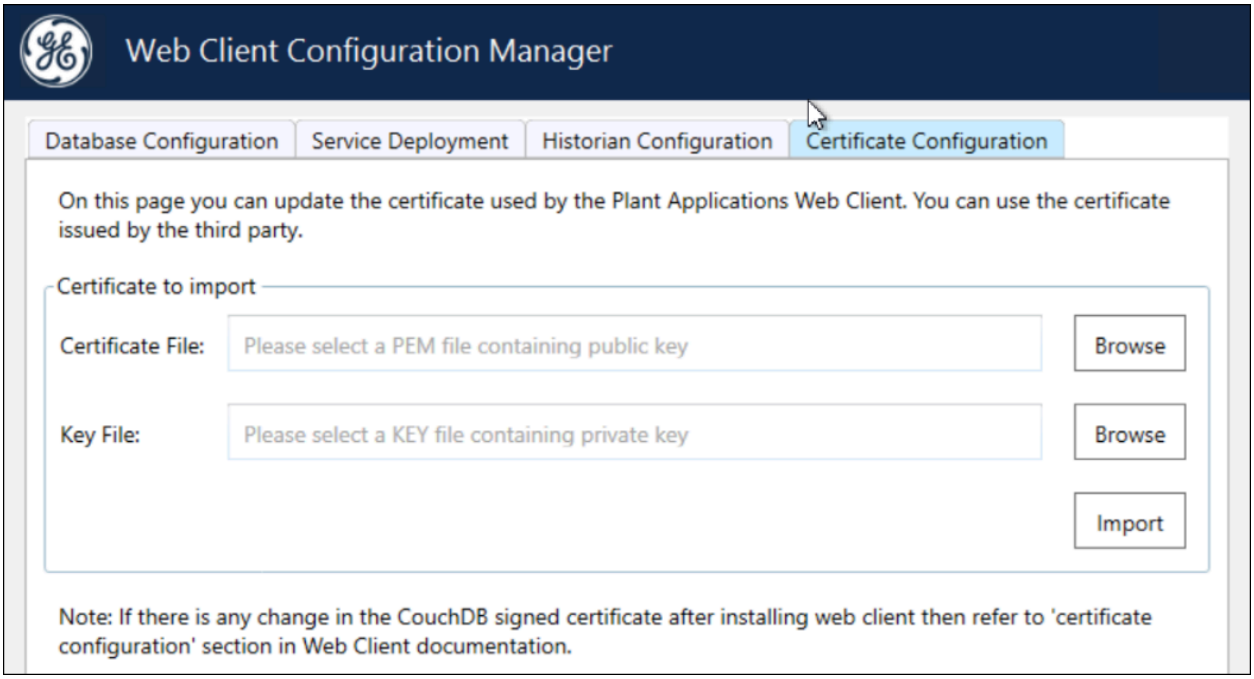
a. The Key column cell value of a Row is a primary key and must be entered before values in any other cells of that Row.
b. The Key column cell value of a Row must be a unique key. In case of duplicate key entry a validation error will occur and editing of any other cell will be disabled.

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

Import Certificates

About this task

This tab allows you to import the certificates.



Procedure

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.

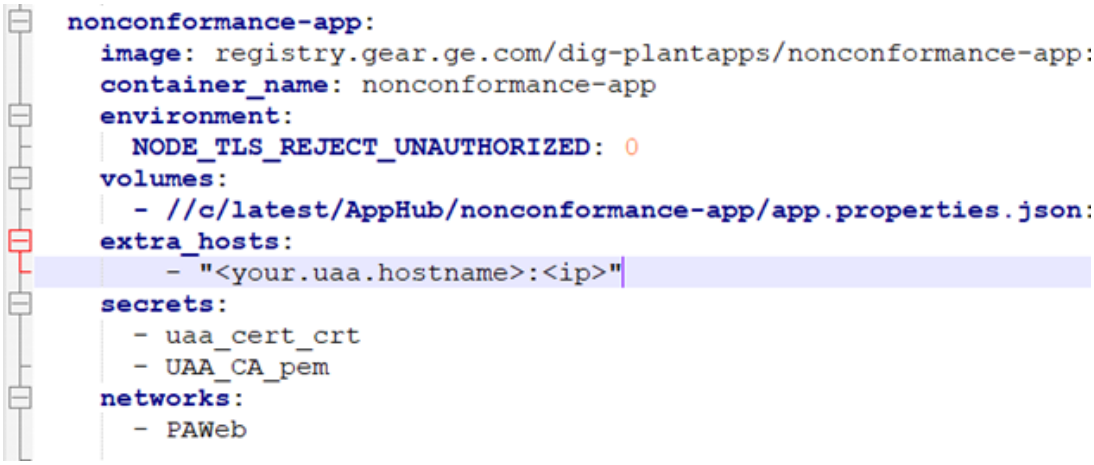
Procedure

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

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

    ```
    extra_hosts:

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

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

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

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

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

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

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

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

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

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

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

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

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

Renew the Docker Certificate

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

Procedure

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

5. Stop the Docker service using the following command: `sudo service docker stop`
6. Set the system date to current time using the following command: `sudo date -s “04 Feb 2020 11:00:00”`
7. Start the Docker service using the following command: `sudo service docker start`

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 Custom Configuration Properties File

You can access the `custom-config-prod.properties` file located at `<buildpath>/PlantApplicationsDocker/plantapps-web-docker/mnt/configfiles/custom-config/prod/<version>/custom-config-prod.properties`. The custom configuration file is used to add service custom property values and helps retain the modified settings during upgrade.

Note:
Ensure that you maintain the syntax in the `custom-config-prod.properties` which is shown as key-value pair. For example, property name = value.

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.

Note:
When there is a change in the logging level, services dynamically reflect these changes, and it is not required to restart the services.

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`

> **Note:**
> For work-order-service, you need to restart the service to debug after making modifications.

4. After making the modifications, save the file.

Access Connection Properties

About this task

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:

Procedure

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

About this task

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

Procedure

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 wc-server_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

About this task

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.

Procedure

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

About this task

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.`

Procedure

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 *(on page 142)*.

Post Applications into Operations Hub Manually

About this task

The Plant Applications 2023 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.

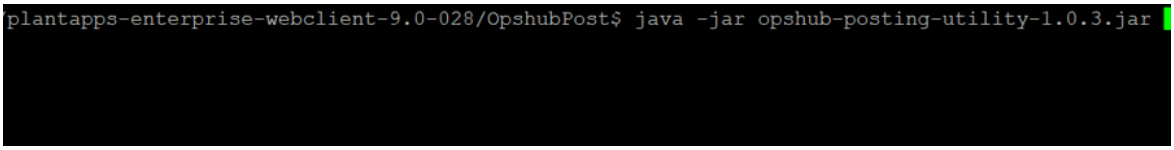
The `Operations_Hub_PostingUtility` directory within the installer has all the required files. One of the required files is the `application.properties` file. The `application.properties` file contains existing basic inputs. However, you must update the below properties in this file:

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

Procedure

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-1.2.0.jar` with the following command: `java -jar opshub-posting-utility-1.2.0.jar`



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

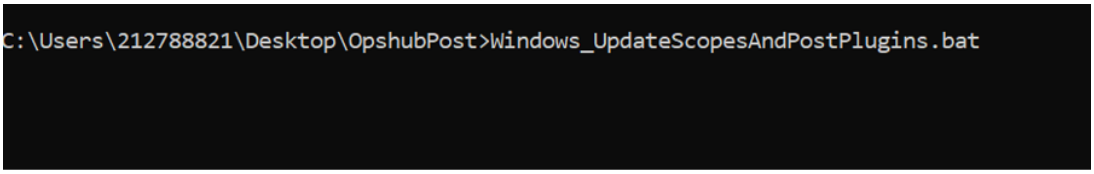
About this task

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

- Clients
- Scopes
- User Groups
- Applications

Procedure

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`

     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 *(on page 144)*
- Update IP.2, DNS.2, and DNS.3 in the V3.txt file. See Update V3 Txt *(on page 147)*
- Update the CN in the server.csr.cnf file. See Update the Server.CSR.CNF File *(on page 148)*
- Create certificates and keystore files. See Create Certificates and Keystore Files *(on page 148)*
- Update the following services:
  - WorkOrder service
  - HTTPD service
  - Tomcat
  - Tomcat JRE keystore

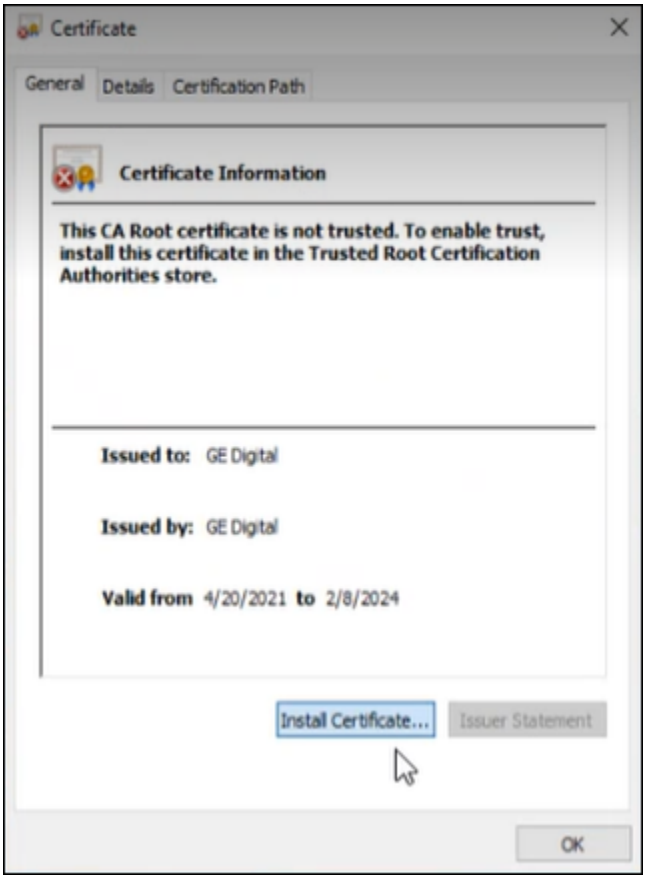
  See Update Work Order, HTTPD, and Tomcat Services *(on page 149)*

Import the Self-Signed Certificate to the Windows Trusted Store

Procedure

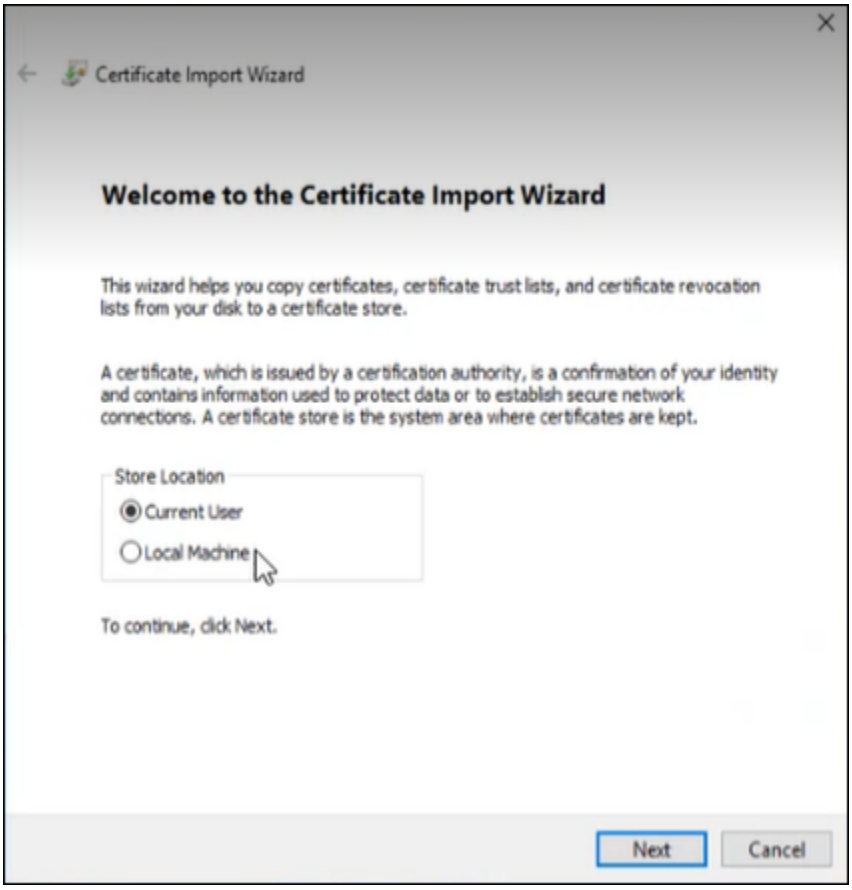
1. Download the UAASecrets.zip folder.
2. Extract the files from the UAASecrets.zip folder.
3. In the UAASecrets folder, select and double-click the UAA_CA.crt file.

   The **Certificate** page appears.



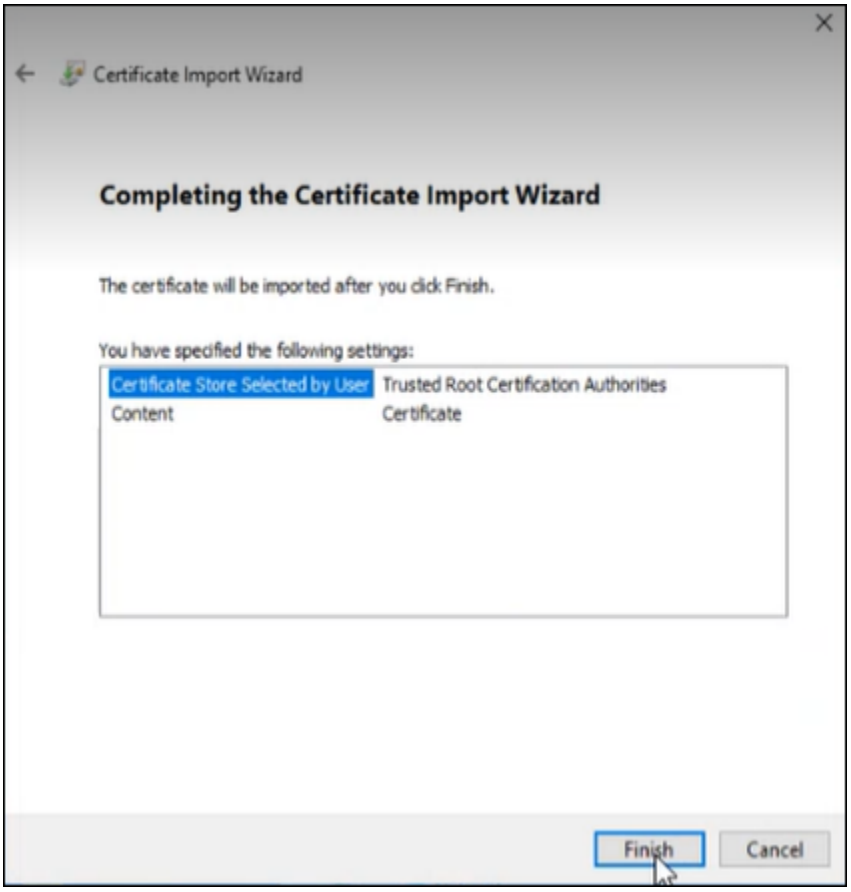
4. Select **Install Certificate**.

   The **Certificate Import Wizard** appears.



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.



10. Select **Finish**.

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

Update V3 Txt

About this task

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

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

Procedure

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

Procedure

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**.

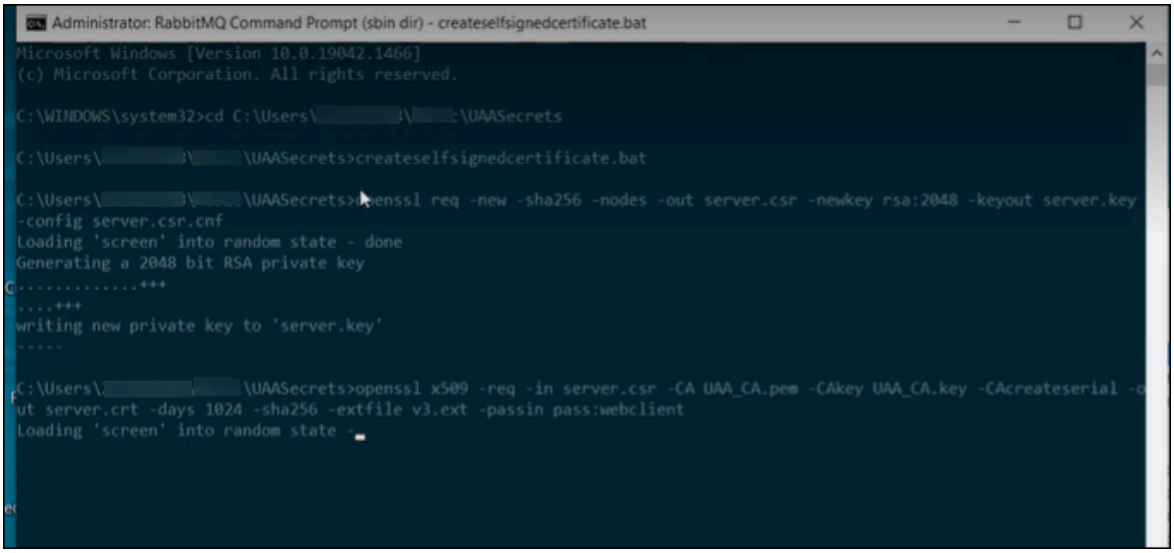
Create Certificates and Keystore Files

About this task

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

Procedure

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`.



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

About this task

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

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

Procedure

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

About this task

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.

Procedure

1. Log in to the Proficy Historian Administrator.
2. Select **DataStores**.
3. Select the **Security** tab.
4. In the **Enforce Strict Client Authentication** row, select **Disabled**.
5. In the **Enforce Strict Collector Authentication** row, select **Disabled**.
6. Select **Update**.

   The 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.