



Universal Client Installation Guide

Version 8.0.



Contents

Chapter 1: Installation Overview	1
Installation Overview	2
Chapter 2: Installing Plant Applications Universal Client Without Using Docker	3
About Installing Plant Applications Universal Client Without Using Docker	4
About Preinstallation Requirements	4
Install the Plant Applications Universal Client Without Using Docker	7
About Post-Installation Tasks	16
Add a UAA User	16
Configure a GE Proficy Historian Server for the Analysis Application	18
Configure the Cache Settings for the Historian Tags	19
Performance Tuning Settings	20
Node Application Manager Utility	22
Chapter 3: Installing Plant Applications Universal Client Using Docker	24
About Installing Plant Applications Universal Client Using Docker	25
About Preinstallation Requirements	25
Components Required for Plant Applications Universal Client Installation	25
System Requirements	26
Software Requirements	26
Configure Docker Settings for Linux	27
Download Docker Images	28
Configure Apache CouchDB Settings	29
Configure Operations Hub UAA	31
Generate the Binary Files Required to Install Plant Applications Universal Client	33
Install Plant Applications Universal Client	42
Configure Plant Applications to Enable Discrete Applications	45
Uninstall Plant Applications Universal Client	45

Chapter 4: Upgrade Plant Applications Universal Client	46
Upgrade the Plant Applications Universal Client (Non-Docker Installer only)	47
Import the Historian UAA Certificate	53
Configure ThingWorx UAA Authenticator	54
Chapter 5: Troubleshooting	58
Frequently Asked Questions (Non-Docker only)	59
Troubleshoot the Tomcat Error	59
Troubleshoot Access Issues	60
Chapter 6: Reference	62
Configure the GE Proficy Historian Server Security Settings	63

Copyright GE Digital

© 2019 General Electric Company.

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

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

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

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

Chapter 1

Installation Overview

Topics:

- [Installation Overview](#)

Installation Overview

Plant Applications Universal Client contains two types of applications:

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

Depending on the type of applications you want to use, the following methods of installation are available:

- **Without using a Docker container:** This is used to install Plant Applications Universal Client for only process 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. However, the discrete applications are not installed using this method.
- **Using a Docker container:** This is used to install Plant Applications Universal Client for both process and discrete applications, except Analysis and Activities. You can choose this method only for a first-time installation of Plant Applications.

To troubleshoot any issues during the installation or upgrade process, refer to the [Troubleshooting](#) section in this guide.

Chapter 2

Installing Plant Applications Universal Client Without Using Docker

Topics:

- [About Installing Plant Applications Universal Client Without Using Docker](#)
- [About Preinstallation Requirements](#)
- [Install the Plant Applications Universal Client Without Using Docker](#)
- [About Post-Installation Tasks](#)
- [Add a UAA User](#)
- [Configure a GE Proficy Historian Server for the Analysis Application](#)
- [Configure the Cache Settings for the Historian Tags](#)
- [Performance Tuning Settings](#)
- [Node Application Manager Utility](#)

About Installing Plant Applications Universal Client Without Using Docker

Installing Plant Applications Universal Client without using a docker container installs only the process 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. However, the discrete applications are not installed using this method.

About Preinstallation Requirements

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

- [System requirements](#)
- [Port requirements](#)
- [Software requirements](#)
- [Plant Applications Server Requirements](#)
- [Plant Applications Message Bridge Requirements](#)

System Requirements

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

Item	Version
GE OpHub UAA	UAA 3.0.209.0
Web browsers	Chrome 65.0 or later
Operating system	64-bit Windows 7, Windows 10, Windows Server 2012, Windows Server 2016, or Windows Server 2019
Framework	Microsoft® .NET Framework 4.7 or later
SQL server	SQL server 2012, 2014, 2016 (64-bit), or 2017 (64-bit) Note: Ensure that you have configured the SQL server database as the Plant Applications database. For more information, refer to the <i>Plant Applications Getting Started Guide</i> for the latest release.
Hard drive	80 GB (minimum)

Item	Version
Processor	2.4 GHz clock-speed Intel Core i3, i5, or i7 CPU or equivalent AMD Phenom CPU with 16 GB RAM Note: It is recommended to use a quad core (4-cores) processor for better performance.
Memory	16 GB (recommended) Note: You must have 32 GB if you plan to install Plant Applications, Historian, OpHub UAA, Universal Client (UC), Message Bridge on the same node. However, it is recommended to install them in a distributed environment.

Port Requirements

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

Port	Description
5672	The default port for the RabbitMQ Message bridge required to communicate with the Plant Applications server for retrieving data updates.
8444	The default port for the Tomcat server.
1433	The default port for the Microsoft SQL server.

Software Requirements

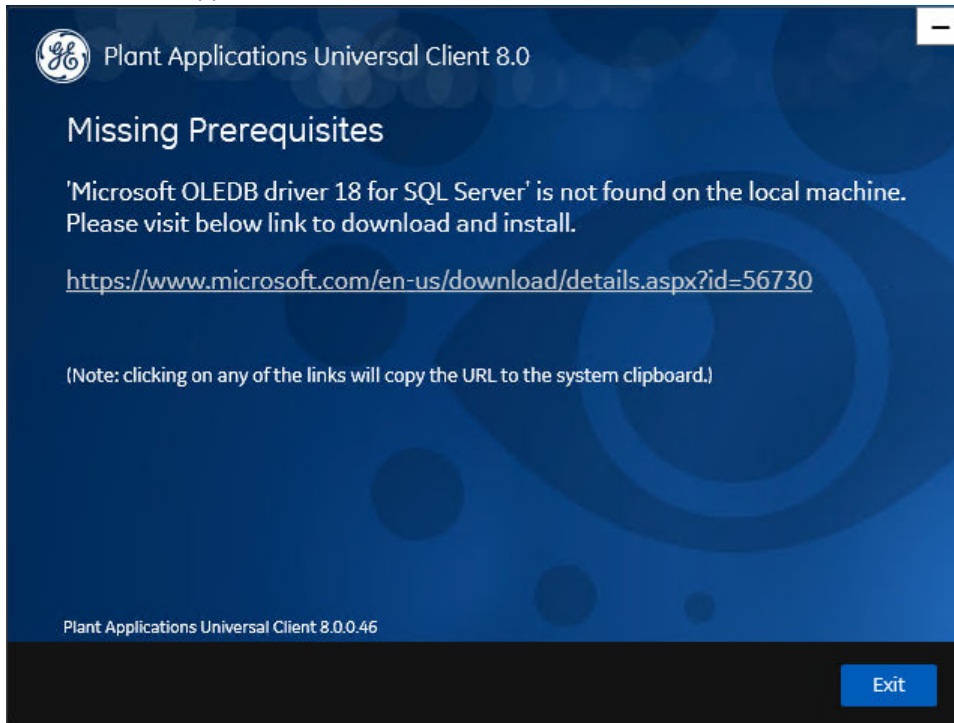
The installer identifies all available and missing software packages required before installing the Plant Applications Universal Client.

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

- Microsoft OLE DB Driver 18 for SQL Server

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

If you do not install Microsoft OLE DB Driver 18 for SQL Server, the following screen appears, and the installation is stopped.



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

- Apache Tomcat version 9.0.1
- Ruby 2.3.3
- Ruby DevKit version 4.65.0.0

Note:

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

- NodeJS 8.12
- Python 2.7
- OpenJDK 1.8

Plant Applications Server Requirements

Ensure that the Plant Applications Server 8.0 is installed. For more information, refer to the *Plant Applications Getting Started Guide* for the latest release.

Install Operations Hub UAA

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

Plant Applications Message Bridge Requirements

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

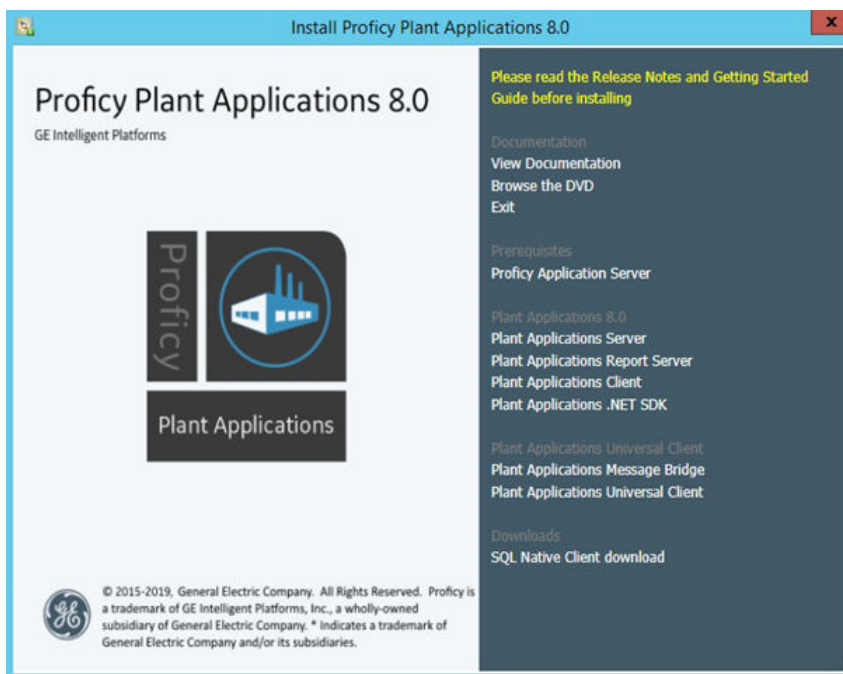
Install the Plant Applications Universal Client Without Using Docker

About This Task

Perform the [preinstallation tasks](#).

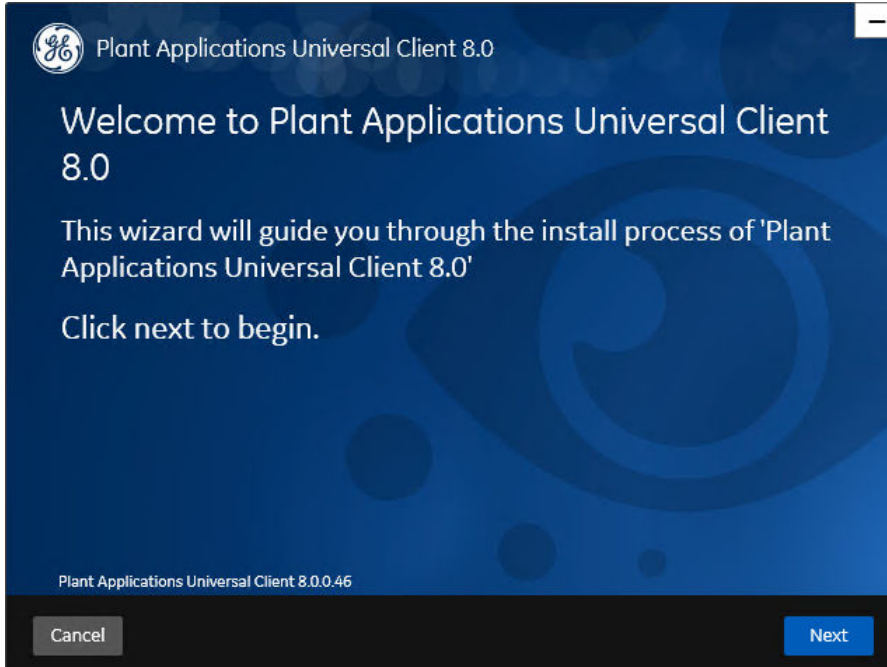
Procedure

1. Mount the ISO file for the Plant Applications Universal Client or load the DVD if you created one from the ISO file on the application server for Plant Applications.
2. Run the `installfrontend.exe` file as an Administrator.
The installation menu appears, displaying the **Install Proficy Plant Applications 8.0** screen.

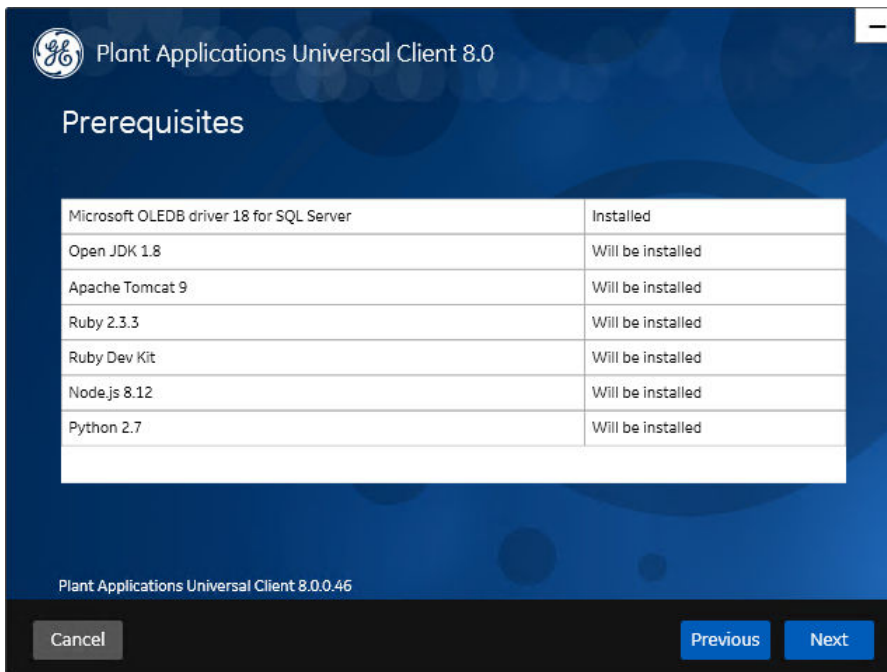


Tip: You can hover over each task that appears in the installation menu to refer to the tooltip associated with that task.

3. Select **Plant Applications Universal Client 8.0**.
The Plant Applications Universal Client installation wizard appears, displaying the **Welcome to Plant Applications Universal Client 8.0** screen.

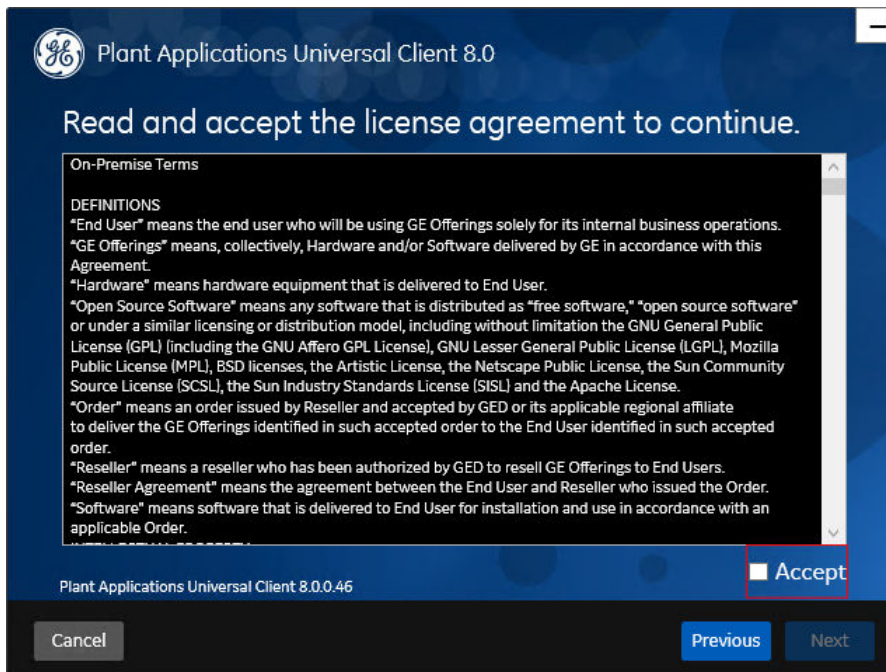


4. In the **Welcome to Plant Applications Universal Client 8.0** screen, select **Next**. The **Prerequisites** screen appears.

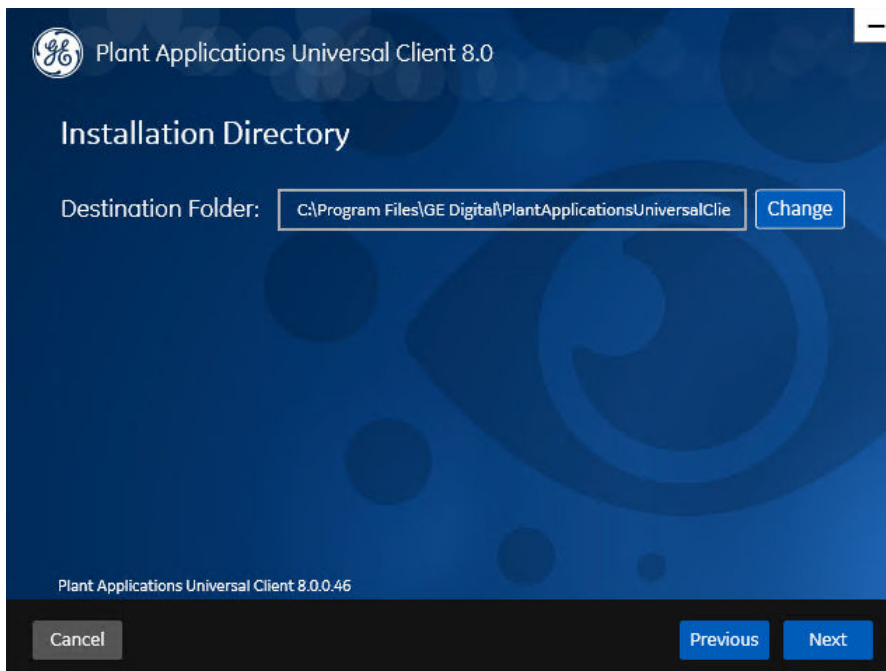


Note: If Microsoft OLE DB Driver 18 for SQL Server or later is not installed, the **Missing Prerequisites** screen appears informing you to install the required version of the missing software before you run the installer. You must exit the installation, and first install the required software.

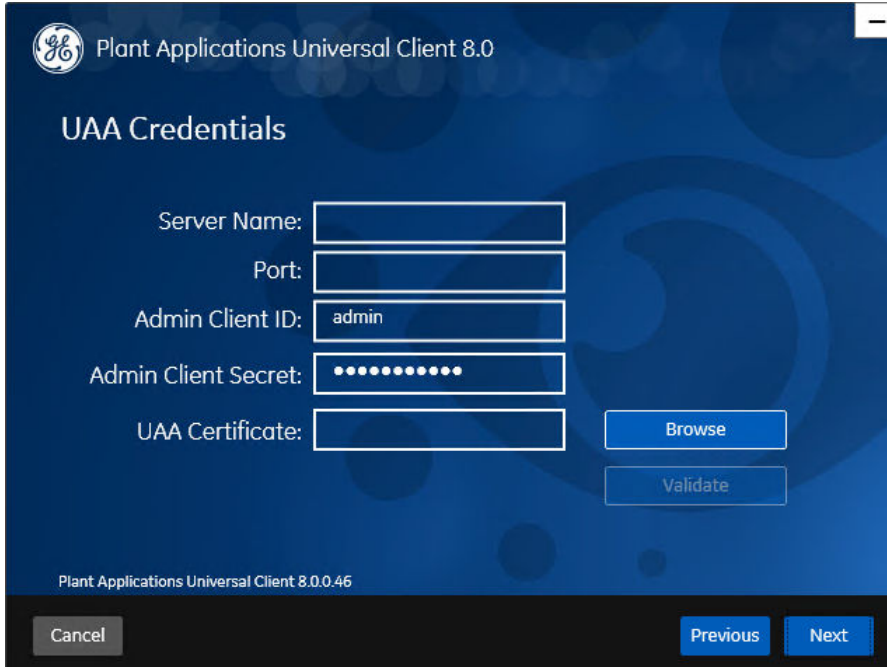
5. In the **Prerequisites** screen, select **Next** to view all installed prerequisites and install any missing prerequisites. The **Read and accept the license agreement to continue** screen appears.



6. Read the license agreement, select **Accept**, and then select **Next** to continue the installation. The **Installation Directory** screen appears with the default installation directory selected as `C:\Program Files\GE Digital\PlantApplicationsUniversalClient`.






7. **Optional:** In the **Destination Folder** box, select **Change** to browse and select the directory where you want to install the Plant Applications Universal Client.
8. In the **Installation Directory** screen, select **Next**. The **UAA Credentials** screen appears.



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

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

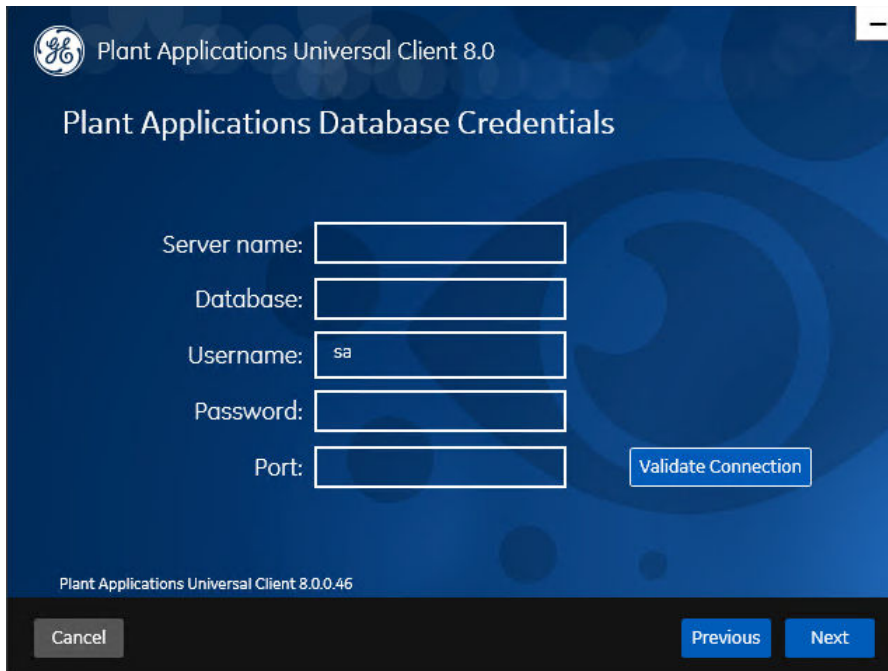
Credential	Description
UAA Certificate	Select Browse to locate the UAA server certificate and upload it. Note: Copy the certificate from the UAA installed node's location (C:\Program Files (x86)\GE_Digital\nginx\conf\cert to UC node).
Validate	Select Validate to validate the UAA server connection. Note: The following table describes each icon indicating a validation status that might appear during the validation process.

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

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

10. Select **Next**.

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






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

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

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.

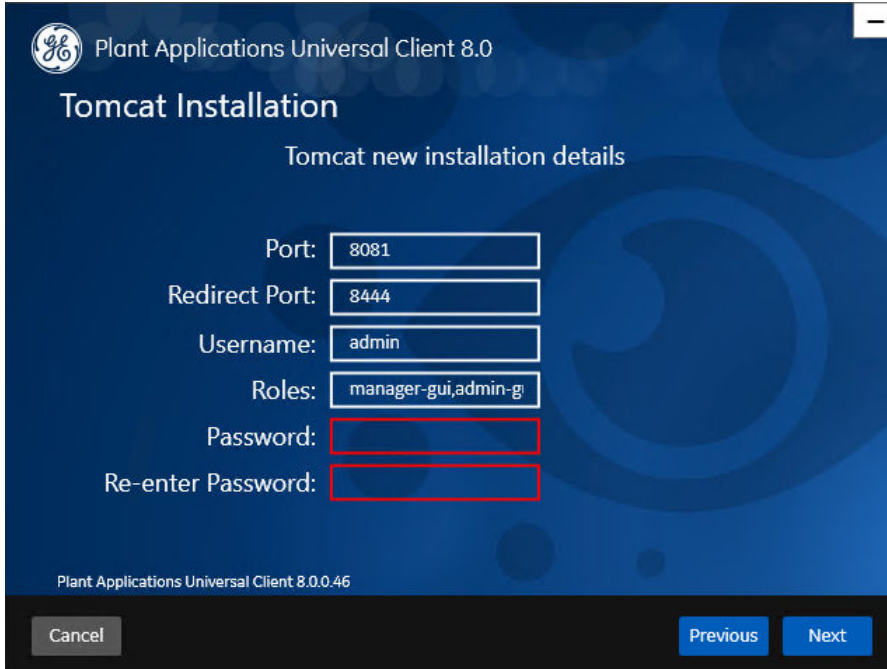
The following table describes each icon indicating a validation status that might appear during the validation process.

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

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

13. Select **Next**.

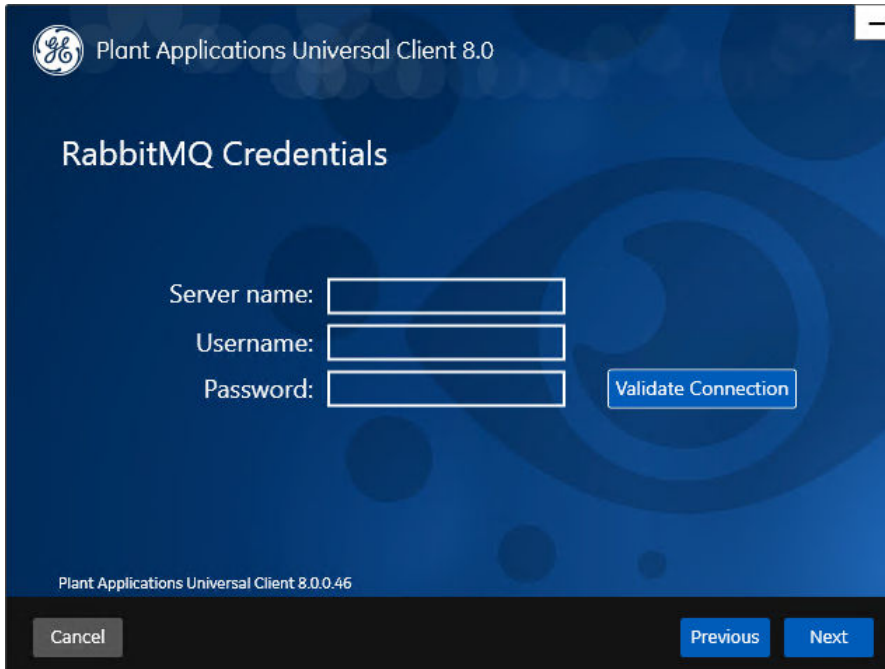
The **Tomcat Installation** screen appears.



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

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

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






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

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

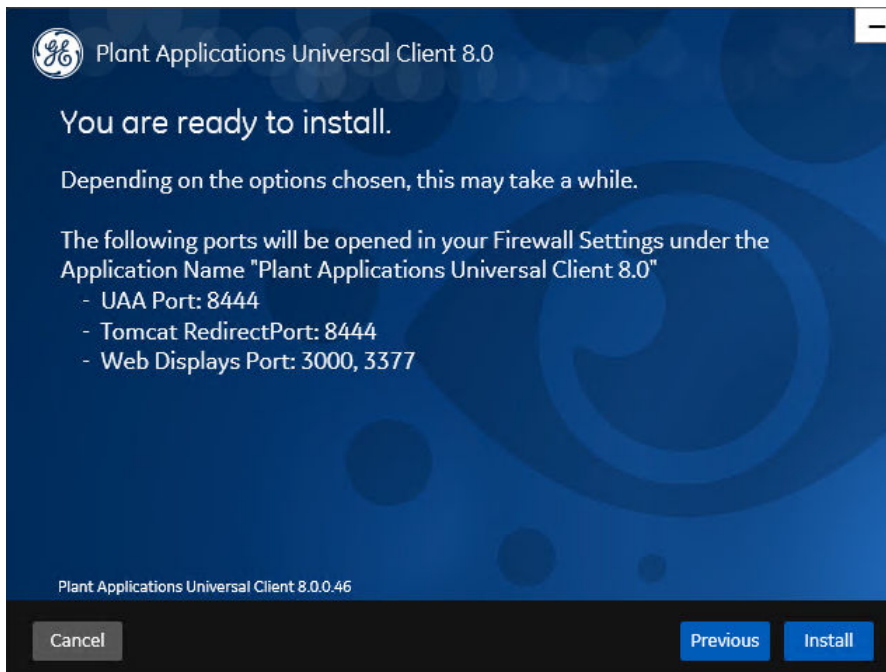
Credential	Description
Server name	Enter the computer name or IP address that hosts your Plant Applications Message Bridge.
Username	Enter the Administrator's user name that you set during Plant Applications Message Bridge installation.
Password	Enter the password for the Administrator's user name you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

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

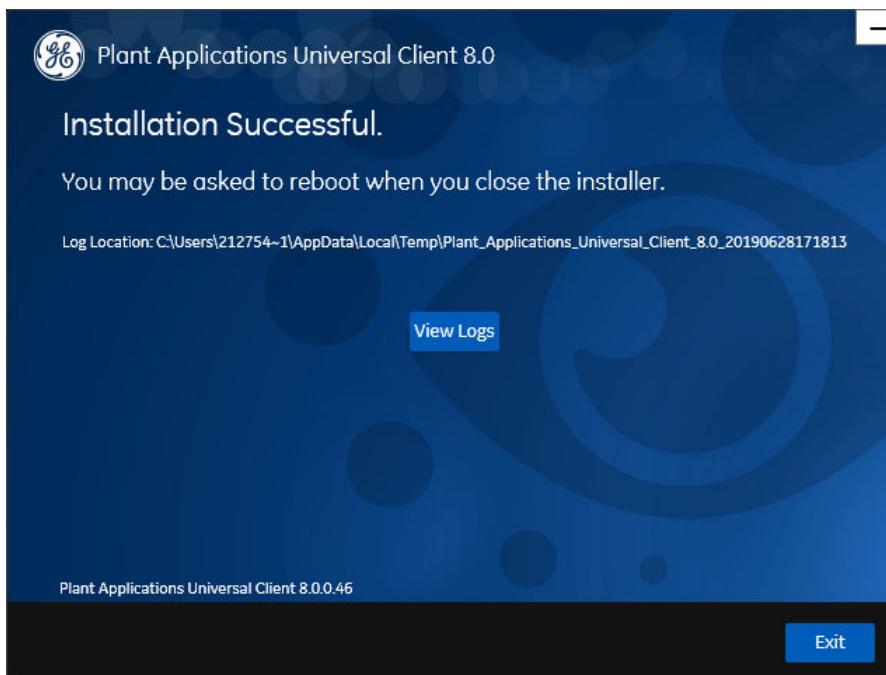
Icon	Description
	Indicates that the validation is in progress.
	Indicates that the validation was successful.
	Indicates that the validation was unsuccessful. In this case, make sure you enter the correct password.

17. Select **Next**.

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



18. Select **Install**, and then wait for the installation to complete. Depending on the options selected, the installation process may take some time. On successful installation, the **Installation Successful** screen appears.



19. **Optional:** Select **View Logs** to see the installation details.
20. In the **Installation Successful** screen, select **Exit** to close the wizard.

Results

The Plant Applications Universal Client is successfully installed on your computer.

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

Next Steps

Perform the [post-installation steps](#).

About Post-Installation Tasks

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

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

Add a UAA User

About This Task

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

Before You begin

Ensure that you [modify the `uaac-create-clients-and-users.bat` file to add the user details](#).

Procedure

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

Note: By default, the `uaac-create-clients-and-users.bat` file is located in the Plant Applications Universal Client installation directory.

5. In the command prompt, enter `uaac-create-clients-and-users.bat`.
6. Press Enter to run the `uaac-create-clients-and-users.bat` file.

Results

The user is added as a UAA user to the Operations Hub UAA with an access level you set for the user in the `uaac-create-clients-and-users.bat` file.

Modify the Batch File to Add the User Details

About This Task

You can use the `uaac-create-clients-and-users.bat` file located in the Plant Applications Universal Client installation directory to add a Universal Client user as a User Authentication Service (UAA) user and set the access level as `bm-line-leader` or `bm-operator`. The access levels `bm-line-leader` and `bm-operator` are defined in the Plant Applications Administrator. The `uaac-`

create-clients-and-users.bat file associates a default user for the access levels as described in the following table.

Access Levels	Default User
bm-operator	bm_operator_1
bm-line-leader	bm_lineleader_1

Procedure

1. In the Plant Applications Universal Client installation directory, open the uaac-create-clients-and-users.bat file using a text editor.
2. Depending on the access level, identify each instance of the default user, and then replace the default user with the required user name.

For example, if the user name is john and you want to define bm_operator as the access level, replace the instances of bm_operator_1 with john as shown in the following table.

Original Code Snippet	Modified Code Snippet
call uaac user add bm_operator_1 - p test --emails bm_operator_1@xx.com	call uaac user add john -p test -- emails john@xx.com
call uaac member add trend_client.read bm_operator_1	call uaac member add trend_client.read john
call uaac member add trend_client.write bm_operator_1	call uaac member add trend_client.write john
call uaac member add bm-operator bm_operator_1	call uaac member add bm-operator john
call uaac member add historian_rest_api.read bm_operator_1	call uaac member add historian_rest_api.read john
call uaac member add historian_rest_api.write bm_operator_1	call uaac member add historian_rest_api.write john

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

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

3. Save your changes to the uaac-create-clients-and-users.bat file.

Results

The uaac-create-clients-and-users.bat file is modified with the required user details.

Configure a GE Proficy Historian Server for the Analysis Application

About This Task

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

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

Procedure

1. In the directory `<tomcat_home>/Apache Software Foundation/Tomcat 9.0/webapps/mes-dataservice-impl-<version>/WEB-INF/classes`, access the `application.properties` file by using a text editor. Where:
 - `<tomcat_home>`: Is the directory where you installed Apache Tomcat. For example, `C:/Program Files`.
 - `<version>`: Is the version of the `mes-dataservice-impl` microservice created during the installation of the Plant Applications Universal Client. For example, `0.6.7`.
2. Enter the properties and their details for each GE Proficy Historian Server as described in the following table.

Property	Description
<code>hist<n>.service.origin</code>	Enter the IP address of the GE Proficy Historian Server. For example, <code>10.181.213.204</code> .
<code>hist<n>.service.port</code>	Enter the port number on which the GE Proficy Historian Server is installed. Tip: You can leave this property blank if the GE Proficy Historian Server is installed on the default port 8443.
<code>hist<n>.service.hostname</code>	Enter the host name of the GE Proficy Historian Server as configured in the Plant Applications Administrator. For example, <code>GESERVER</code> .
<code>hist<n>.service.client_secret</code>	Enter the client secret of the Historian Administrator.

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

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

Results

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

Configure the Cache Settings for the Historian Tags

About This Task

The Analysis application supports the caching and refreshing of the cached Historian tags after certain time interval. You configure the duration of the saved cached Historian tags in the `application.properties` file of the `mes-dataservice-impl` and `processanalyzer-service-impl` microservices for the Analysis application. After the set duration, the Historian tags are cached again.

Procedure

1. In the directory `<tomcat_home>/Apache Software Foundation/Tomcat 9.0/webapps/mes-dataservice-impl-<version>/WEB-INF/classes`, access the `application.properties` file by using a text editor. Where:
 - `<tomcat_home>`: Is the directory where you installed Apache Tomcat. For example, `C:/Program Files`.
 - `<version>`: Is the version of the `mes-dataservice-impl` microservice created during the installation of the Plant Applications Universal Client. For example, `0.6.2`.
2. Enter the properties and their details as described in the following table.

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

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

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

- `<version>`: Is the version of the `processanalyzer-service-impl` microservice created during the installation of the Plant Applications Universal Client. For example, `0.6.2`.
5. For the `tagVariableCacheTimeOut` property, enter the duration in the format `duration<timeformat>` after which the tags are cached again. Where: `<timeformat>` is `h`, `m`, or `s` to indicate time in hours, minutes, or seconds, respectively. The default value is `6h`. Example:
`tagVariableCacheTimeOut=6h`

Note: The value you enter for the `tagVariableCacheTimeOut` property must be of the same duration you enter for the `historianTagCacheTimeOut` and `scheduler.tagcaching.seconds` properties in the `mes-dataservice-impl` microservice.
 6. Save the changes to your file.
 7. Restart Tomcat to apply the changes.

Results

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

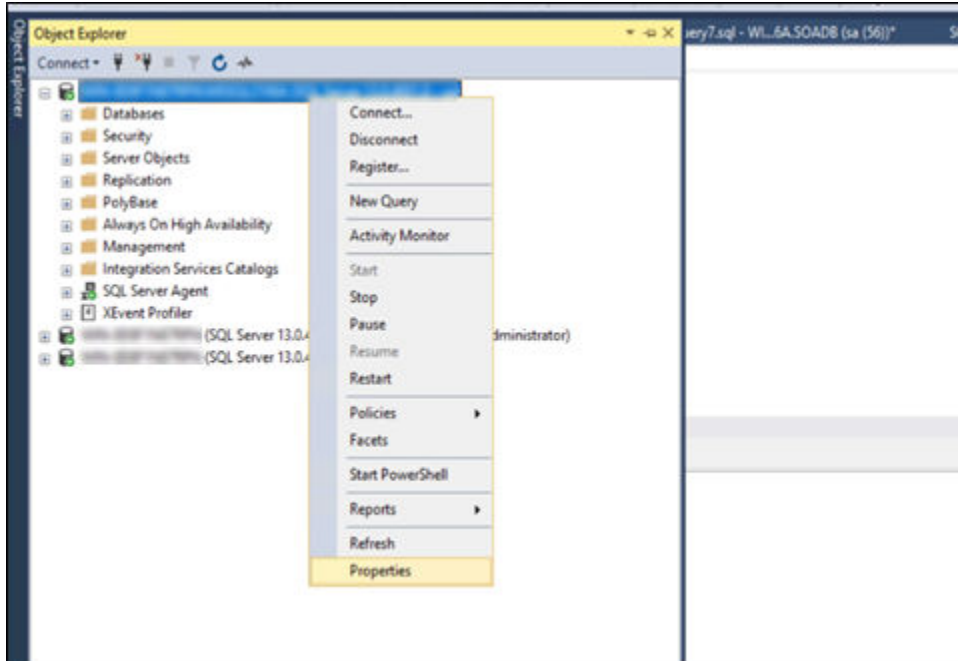
Performance Tuning Settings

About This Task

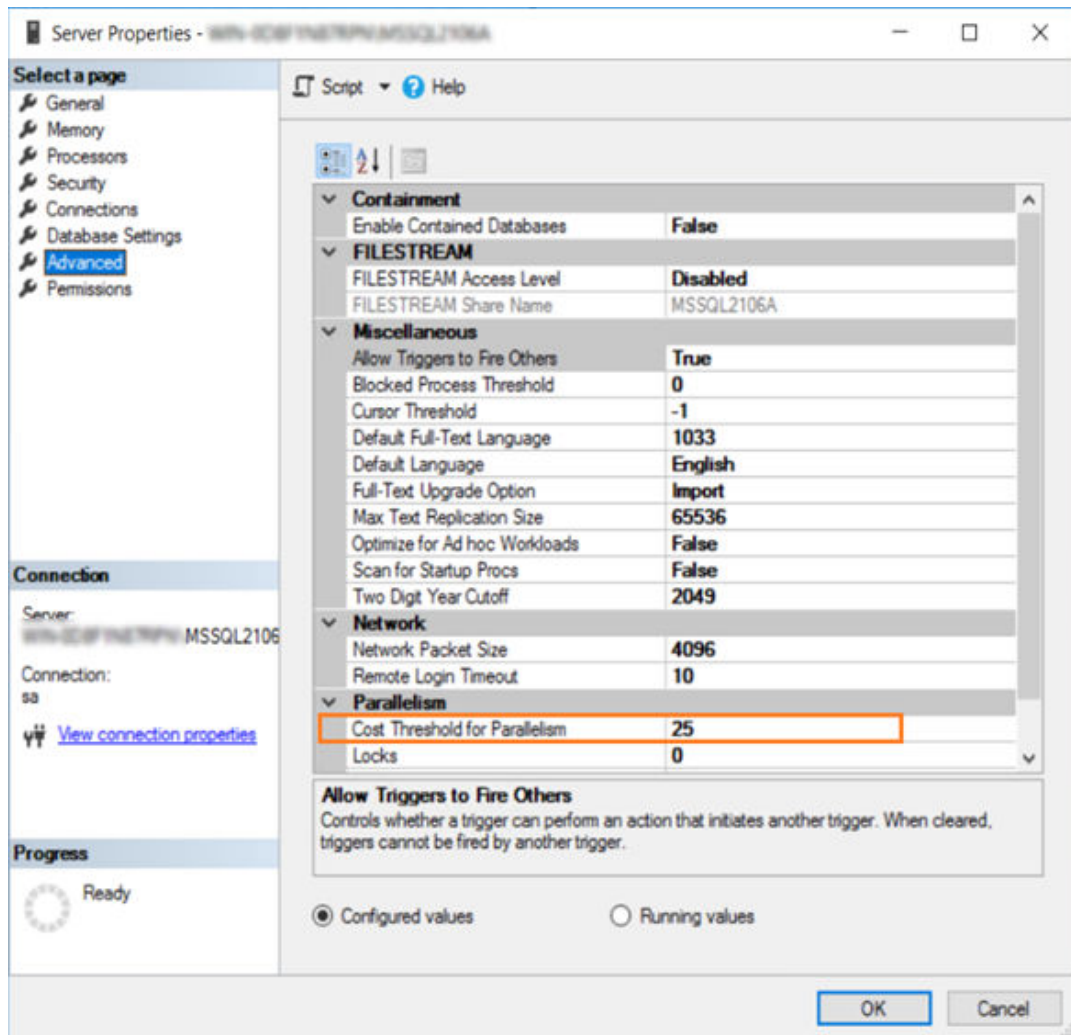
Here are the recommended performance tuning settings for your environment to achieve optimal performance.

Procedure

1. Update Tomcat default threads.
 - a) Navigate to **C:\Program Files\Apache Software Foundation\Tomcat 8.0\conf**
 - b) Open the **Server.xml** file in Notepad. In **Server.xml**, search for the line **102** or **<Connector protocol="org.apache.coyote.http11.Http11NioProtocol" maxThreads="150"**
 - c) Change the max thread count to **800** (`maxThreads="800"`).
 - d) **Save** the file.
2. Update JVM memory settings.
 - a) Navigate to **C:\Program Files\Apache Software Foundation\Tomcat 8.0\bin** and then run **Tomcat8w.exe**.
 - b) Select the **Java** tab.
 - c) Enter the following recommended values:
 - **Initial memory pool:** 4096 MB
 - **Maximum memory pool:** 4096 MB
 - **Thread stack size:** Leave this field empty
 - d) Select **OK**.
 - e) **Stop** and **Start** Tomcat.
3. Update database settings:
 - a) Update the **Cost Threshold for Parallelism** value:
 - i. Open SSMS connect to the instance, where SOA db is deployed.
 - ii. Select the instance. Now, right-click on the instance and then select **Properties**.



- iii. Select the **Advanced** tab. In the **Parallelism** section, in the **Cost Threshold for Parallelism** box, change the default value from **5** to **25**.



- b) Ensure that statistics (sp_updatestats) is updated in the database.
- c) It is recommended to move the transaction logs to a different drive to optimize disk I/O performance.

Node Application Manager Utility

About This Task

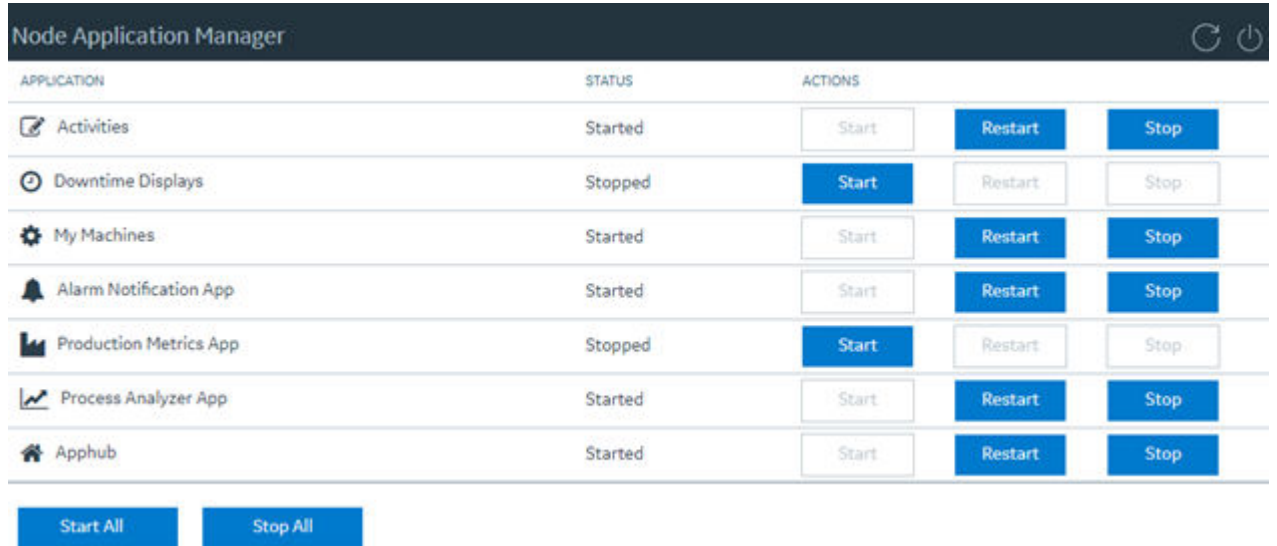
Node Application Manager is a simple utility that displays the health of the UI micro applications in a dashboard. You can use this utility to stop or restart the applications if you are not able to access them in the universal client from the browser.

Procedure

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

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



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



The screenshot shows the Node Application Manager dashboard. At the top, there is a header with the title "Node Application Manager" and two icons: a refresh icon and a power icon. Below the header is a table with three columns: "APPLICATION", "STATUS", and "ACTIONS". The table lists seven applications: Activities, Downtime Displays, My Machines, Alarm Notification App, Production Metrics App, Process Analyzer App, and Apphub. Each application row has a "Start" button, a "Restart" button, and a "Stop" button. Below the table are two buttons: "Start All" and "Stop All".

APPLICATION	STATUS	ACTIONS
Activities	Started	Start Restart Stop
Downtime Displays	Stopped	Start Restart Stop
My Machines	Started	Start Restart Stop
Alarm Notification App	Started	Start Restart Stop
Production Metrics App	Stopped	Start Restart Stop
Process Analyzer App	Started	Start Restart Stop
Apphub	Started	Start Restart Stop

Start All Stop All

3. You can either **Start**, **Stop**, or **Restart** an individual application by selecting corresponding button. You can also use **Start All** or **Stop All** buttons either to start or stop all applications respectively.
4. You can select  to reload the dashboard or refresh the browser.
5. You can select  to logout from Node Application Manager.

Chapter 3

Installing Plant Applications Universal Client Using Docker

Topics:

- [About Installing Plant Applications Universal Client Using Docker](#)
- [About Preinstallation Requirements](#)
- [Components Required for Plant Applications Universal Client Installation](#)
- [System Requirements](#)
- [Software Requirements](#)
- [Configure Docker Settings for Linux](#)
- [Download Docker Images](#)
- [Configure Apache CouchDB Settings](#)
- [Configure Operations Hub UAA](#)
- [Generate the Binary Files Required to Install Plant Applications Universal Client](#)
- [Install Plant Applications Universal Client](#)
- [Configure Plant Applications to Enable Discrete Applications](#)
- [Uninstall Plant Applications Universal Client](#)

About Installing Plant Applications Universal Client Using Docker

Installing Plant Applications Universal Client using Docker installs both the process and discrete applications. You must perform this method of installation on a Linux machine.

Important:

- Host names and server names must always be entered in lowercase.
- IP addresses of only the IPv4 version are supported.

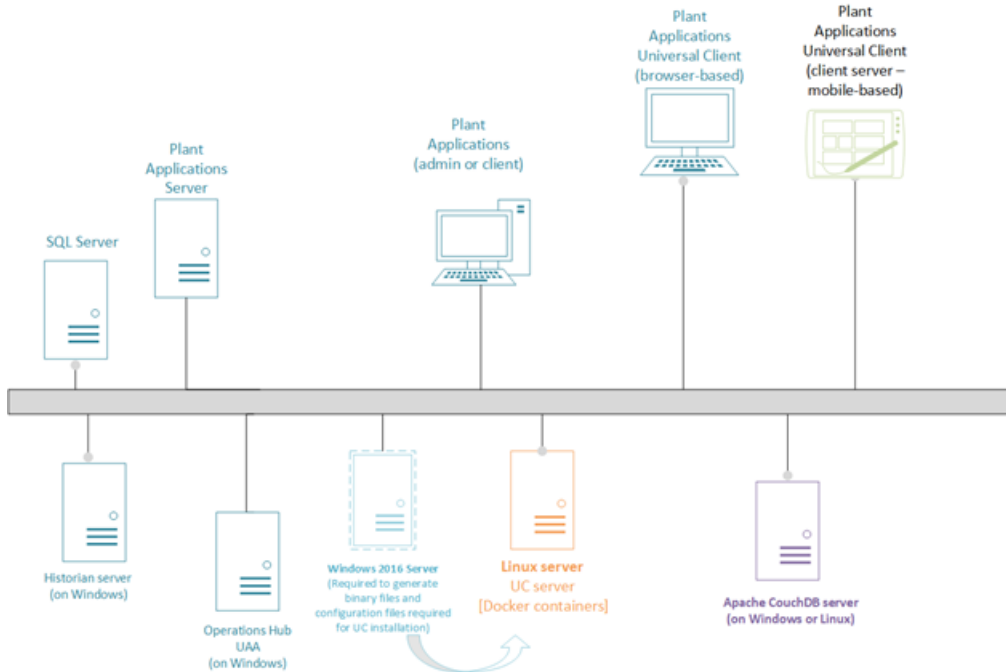
About Preinstallation Requirements

This section of the document explains you how to get started with the Docker-based installation of Plant Applications Universal Client. Ensure that you perform the following tasks before you perform the installation.

- [Check for the system requirements.](#)
- [Check for the software requirements.](#)
- [Configure Docker settings on the target Linux machine.](#)
- [Configure the Apache CouchDB settings.](#)
- [Configure the Operations Hub UAA settings.](#)

Components Required for Plant Applications Universal Client Installation

The following diagram provides the various components used while installing Plant Applications Universal Client:



System Requirements

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

Item	Requirement
Processor	Any processor with a clock speed of 3GHz or more and minimum 8-core configuration
RAM	64GB Note: For a test environment, you can use a 32GB RAM.
Hard drive	500GB
RAM allocation for Docker	45GB
Operating System	Both the following operating systems: <ul style="list-style-type: none"> RedHat Linux or Ubuntu 17 or later: You must use this machine to install Plant Applications Universal Client for a production environment. Windows Server 2016 (with a 16GB RAM and a 100GB hard disk): You must use this machine to export the binaries that you will use to install Plant Applications Universal Client on Linux.

Software Requirements

Before you install the Docker-based installation of Universal Client, verify that the following software applications are installed on the target machine.

- The following Docker components on the target Linux machine:
 - Docker version 18.06 (community edition)

- Docker Compose
- Docker images from public registries
- Operations Hub UAA on a Windows machine.

Note: For instructions, refer to the Operations Hub UAA Installation Guide provided along with the Operations Hub installation package.
- Apache CouchDB 2.3.1 on a Windows machine.

Configure Docker Settings for Linux

To install Plant Applications Universal Client on Linux, you must configure the Docker settings to work with Plant Applications Universal Client.

Before You begin

- Install Docker version 18.06 community edition.

Tip: You can download and install Docker 18.06 from the following URL: <https://docs.docker.com/install/>
- Install Docker Compose.

Tip: You can download and install Docker Compose from the following URL: <https://docs.docker.com/compose/install/>

Procedure

1. If you are running behind a proxy, perform steps 2 through 6. Otherwise, skip to step 7.
2. Create a directory by running the following command: `sudo mkdir -p /etc/systemd/system/docker.service.d`
3. Create a file named `http-proxy.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 number of the proxy server>/""NO_PROXY=localhost,127.0.0.1,<IP address>,<host name>"
```

5. Save the file, and exit.

Tip: To do so, press Ctrl+o, press Enter, and then press Ctrl+x.
6. Run the following commands to verify that the proxy details that you have entered are correct:

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

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

```
{
  "insecure-registries" : [<IP address>:5000", "<host name>:5000"]
}
```

Note: Depending on whether you will use IP address or host name while providing DTR details during installation, enter the IP address or the host name. You may enter both the details.

9. **Optional:** Add your user account to the Docker group so that you do not need to type `sudo` for each command, by running the following command: `sudo usermod -aG docker $USER`

10. Enable Docker Swarm by running the following command: `docker swarm init`

Note: If you have not performed the previous step (that is, you are not a member of the Docker group), run the following command to initialize Docker Swarm: `sudo docker swarm init`

A token will be generated, which you can use to add more nodes to Docker Swarm.

Results

- The Docker settings are configured.
- Docker Swarm is enabled.

Next Steps

[Download Docker Images](#) on page 28.

Download Docker Images

Before You begin

- [Configure Docker Settings for Linux](#) on page 27.
- Ensure that Docker is running.

Procedure

Open the terminal on the target Linux machine, and run the following commands to download the necessary dependent Docker images:

```
docker pull confluentinc/cp-kafka:5.1.2
```

```
docker pull confluentinc/cp-zookeeper:5.1.2
```

```
docker pull confluentinc/cp-schema-registry:5.1.2
```

```
docker pull thomsch98/kafdrop
```

```
docker pull haproxy:1.8
```

```
docker pull eventuateio/eventuate-tram-cdc-mysql- service:  
0.21.3.RELEASE
```

```
docker pull hyper/docker-registry-web:latest
```

```
docker pull registry:2.4.1
```

```
docker pull governmentpaas/cf-uaac
```

Configure Apache CouchDB Settings

Apache CouchDB is a document storage application that stores the documents used in discrete applications. This topic describes how to configure the Apache CouchDB settings so that it works with Plant Applications.

Before You begin

- Generate or procure SSL security certificates.
- Install Apache CouchDB version 2.3.1.

Important: Perform a single node installation.

Tip: You can download and install Apache CouchDB version 2.3.1 from the following URL: <https://couchdb.apache.org/fauxton-visual-guide/index.html#intro>

Procedure

1. Enable the https protocol by performing the following steps:
 - a) Create a folder named `certs` in the installation folder for Apache CouchDB.
 - b) In the `certs` folder that you have created, place the certificate and key files that you want to use for the https protocol.
2. Access the `default.ini` file located in the following folder: `<installation folder for Apache CouchDB>/etc`
3. Enter values for parameters as described in the following table.

Section	Parameter	Description
chttpd	port	Enter the port number that you want to use for Apache CouchDB.
	bind_address	Enter the IP address of the machine on which you have installed Apache CouchDB.
	authentication_handlers	Perform the following steps to enable proxy authentication: <ul style="list-style-type: none"> a. Comment out the following line: <pre>authentication_handlers = {chttpd_auth, cookie_authentication_handler}, {chttpd_auth, default_authentication_handler}</pre> b. Uncomment the following line: <pre>authentication_handlers = {chttpd_auth, proxy_authentication_handler}, {chttpd_auth, cookie_authentication_handler}, {chttpd_auth, default_authentication_handler}</pre>
httpd	port	Enter the port number that you want to use for Apache CouchDB.
	enable_cors	Enter true to enable cross-origin errors.
cors	origins	Enter the IP address of the machine on which Plant Applications is installed.
	headers	Enter the following value: <code>content-type, if-match, x-auth-couchdb-token, x-auth-couchdb-username, x-couch-full-commit</code>
	methods	Enter the following value: <code>GET, POST, PUT</code>

4. Access the `local.ini` file located in the following folder: `<installation folder for Apache CouchDB>/etc`
5. Enter values for parameters as described in the following table.

Section	Parameter	Description
chttpd	port	Enter the port number that you want to use for Apache CouchDB.
	bind_address	Enter the IP address of the machine on which you have installed Apache CouchDB.

Section	Parameter	Description
ssl	enable	Enter true to allow the usage of the https protocol.
	cert_file	Enter the file path of the certificate file in the following format: <code>../certs/<name of the certificate file>.cert</code>
	key_file	Enter the file path of the key file in the following format: <code>../certs/<name of the key file>.key</code>
couch_httpd_auth	require_valid_user	Enter true to prompt users to enter their user name and password to access Apache CouchDB. Important: You must create at least one user before you enter true for this parameter.
httpd	WWW-Authenticate	Uncomment the following line: <code>WWW-Authenticate = Basic realm="administrator"</code>

6. Save the `local.ini` and `default.ini` files.
7. Restart the Apache CouchDB service.

Results

Apache CouchDB settings are now configured. You can view all the changes that you have made by accessing https://<host name or IP address of Apache CouchDB>:<port number>/_utils/.

Note: By default, the port number is 6984.

Next Steps

1. Create an administrative user for Apache CouchDB.

Tip: Refer to the [Apache CouchDB documentation](#) for instructions on how to create an administrative user.

2. Create a database named `documents`.

Note: Do not change the database name to other than `documents` (for example, <https://<host name or IP address of Apache CouchDB>:6984/documents>).

Tip: Refer to the [Apache CouchDB documentation](#) for instructions on how to create a database.

Configure Operations Hub UAA

Before You begin

- Install Operations Hub UAA.

Note: For instructions, refer to the Operations Hub UAA Installation Guide provided along with the Operations Hub installation package.

- Ensure that Docker is up and running and that Docker Swarm is enabled.

Procedure

1. Download the following file from the customer portal: Proficiency_Plant_Applications_Universal_Client_Docker_v8.0_English.zip
 2. Copy the folder Configure_Operations_Hub_UAA to the target Linux machine.
 3. Access the Linux node where you have placed the folder, and then access the following folder: UAA_Config_Scripts
 4. Access the .env file, and for the CONFIG_FOLDER_PATH parameter, update the existing path with the path of the Configure_Operations_Hub_UAA/UAA_Config_Scripts/Config folder.
 5. Navigate to the Configure_Operations_Hub_UAA \UAA_Config_Scripts\Config folder that contains the uaac_setup.sh file.
 6. Access the uaac_setup.sh file, and perform the following tasks:
 - a) Replace UAASERVER with the host name or IP address of the machine on which you have installed Operations Hub UAA.
 - b) Replace 8443 with the port number of Operations Hub UAA.
 - c) If you want to modify the user name, password, and email ID of the user, update the corresponding values in the following line of code: `uaac user add bm_operator_1 -p bm_operator_1 -emails bm_operator_1@example.com`
- Important:** You must provide this modified user name during the docker Universal Client installation. This user must be a Plant Applications administrator user.
7. Assign the execute permission to the UAA_Config_Start_Lix.sh file.

Tip: To assign execute permission, run the following command: `chmod +x UAA_Config_Start_Lix.sh`
 8. Run the UAA_Config_Start_Lix.sh file.

Results

Operations Hub UAA is now configured. You can access Operations Hub UAA from the following URL: https://<Operations Hub UAA host name>:<port_number>/uaa

Tip: To verify that Operations Hub UAA is running:

1. Run the following command to verify that the stack (in this case, uaaconfig) is deployed: `docker stack ls`
 2. Run the following command to verify that the service (in this case, uaaconfig_uaac) is running: `docker service ls`
- A list of services that are deployed on Docker appear. In the **REPLICAS** column:
- The value **1/1** indicates that the service is running.
 - the value **0/1** indicates that the service is not running. If that happens, verify after some time, or access the service log by running the following command: `docker service logs <name of the service>` (for example, `docker service logs uaaconfig_uaac`).

If you want to remove the stack, run the following command: `docker stack rm <name of the stack>`

Next Steps

Verify if Operations Hub UAA is configured by logging in to Operations Hub UAA with the credentials that you have created.

Generate the Binary Files Required to Install Plant Applications Universal Client

To generate the binary files required to install Plant Applications Universal Client on the target Linux machine, you must first run the installer on a Windows machine.

Before You begin

Note: If you want to reinstall Plant Applications Universal Client, you must first uninstall the existing version of Plant Applications Universal Client using the Control Panel.

Ensure that:

- You are an Administrator with execute permissions.
- Your system meets the [preinstallation requirements](#).
- You have the following UAA and Apache CouchDB certificates in your system.
 - uaa_server.crt
 - uaa_server.pem
 - uaa_server.key
 - couch_server.crt

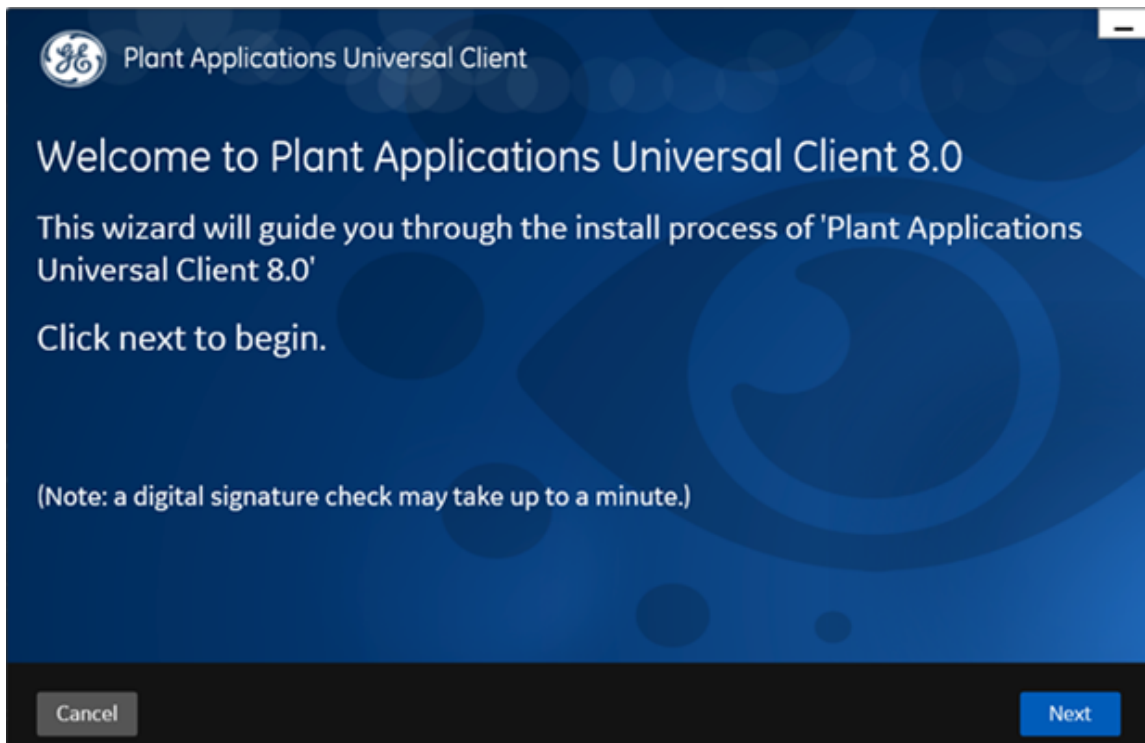
Important: It is mandatory to maintain the same certificate names.

Tip:

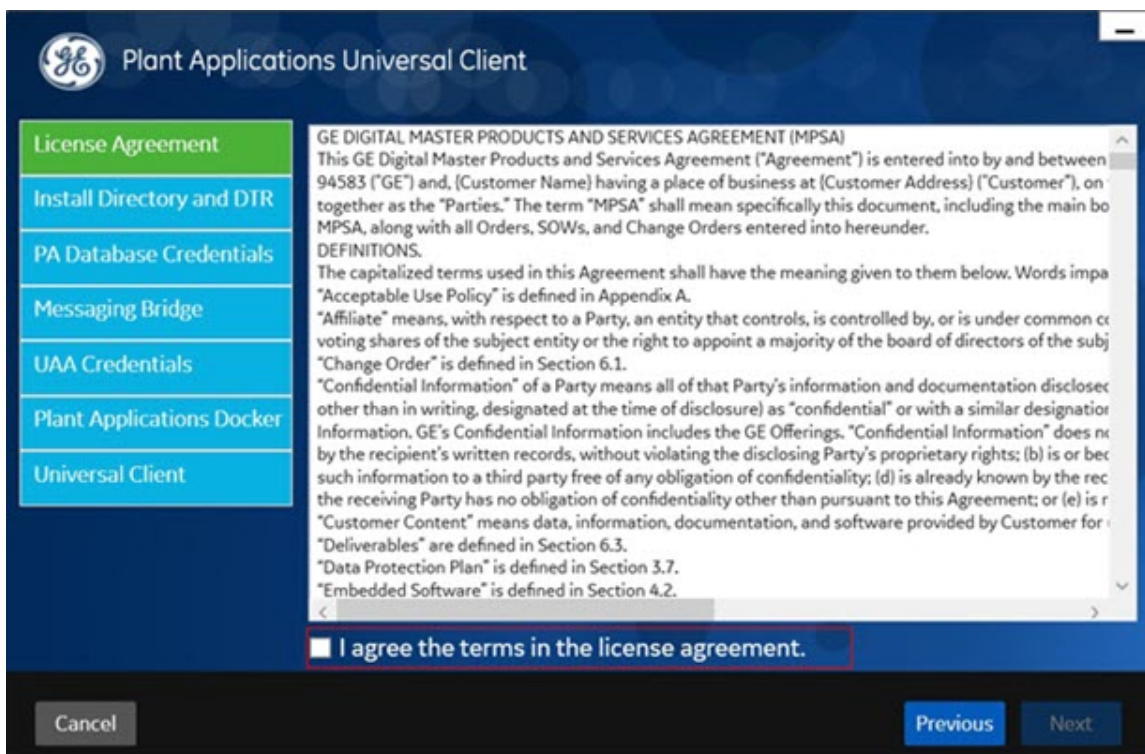
- To procure uaa_server.crt, uaa_server.pem, uaa_server.key files, perform the following steps:
 1. Navigate to the following folder on the machine on which Operations Hub UAA is installed: C:\Program Files (x86)\GE_Digital\nginx\conf\cert
 2. Copy the server.crt, server.pem, and server.key files to a folder on the Windows machine.
 3. Rename these files by adding uaa_ as the prefix (for example, server.crt to uaa_server.crt).
- To procure couch_server.crt file, perform the following steps:
 1. Navigate to the following folder on the machine on which Apache CouchDB is installed: <Apache CouchDB installation folder>/certs
 2. Copy the certificate file to a folder on the Windows machine.
 3. Rename the file to couch_server.crt.
- To procure the couch_server.crt file, generate a self-signed certificate or use a proprietary certificate.

Procedure

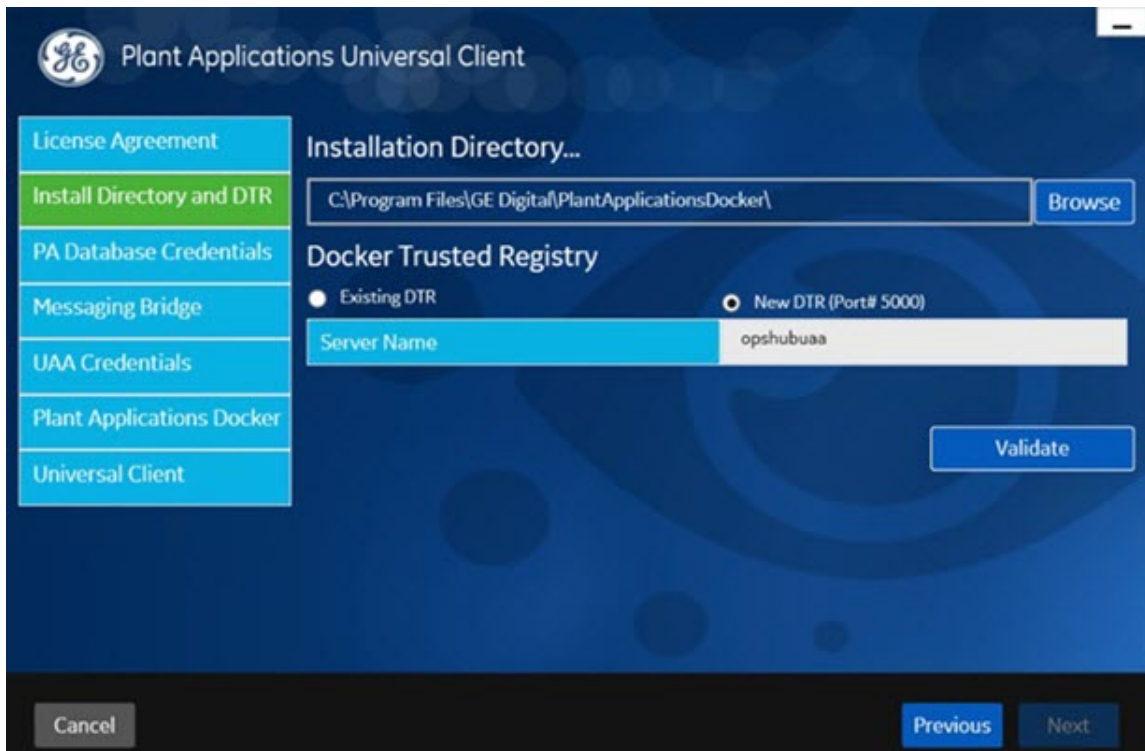
1. Download the Proficiency_Plant_Applications_Universal_Client_Docker_v8.0_English.zip file from the customer portal, extract the file to the Windows machine where you want to run the installer, and then run the Plant Applications Universal Client.exe file as an administrator.
The installer wizard appears, displaying the **Welcome to Plant Applications Universal Client** screen.



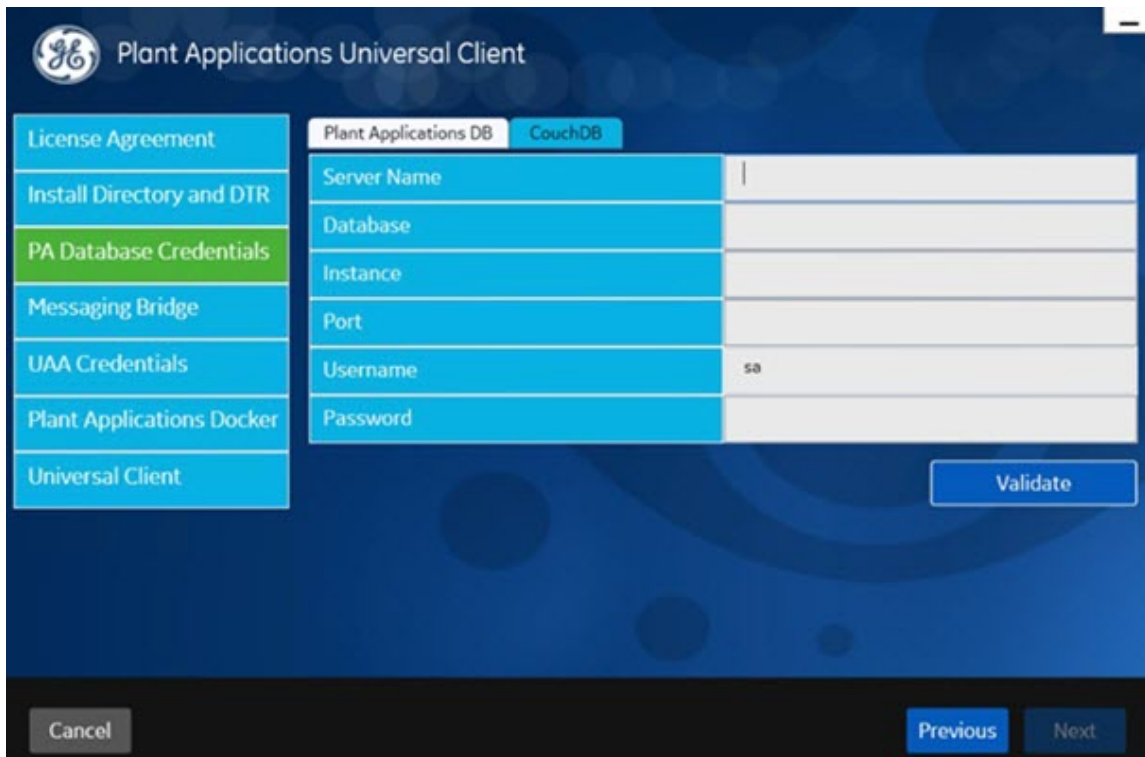
2. Select **Next**.
The **License Agreement** screen appears.



3. Read the license agreement, select the **I agree the terms in the license agreement** check box, and then select **Next**.
The **Install Directory and DTR** screen appears.



4. In the **Installation Directory** box, select the location where you want to place the binary and configuration files.
5. Enter a value in the **Server Name** box as follows:
 - If you select **Existing DTR**, enter a value in the following format: <host name or IP address>:<port number>, where <host name or IP address> is either a fully qualified domain name or IP address of the DTR. Installer uses these existing DTR details to push and pull Docker images for Plant Applications Universal Client.
 - If you select **New DTR**, the local host name appears. Replace the local host name with the host name of the target Linux machine.
6. Select **Validate** to validate the DTR details, and then select **Next**. The **Plant Applications DB Credentials** screen appears.



7. Enter the Plant Applications database and Apache CouchDB database credentials to establish connections with the databases.
 - a. In the **Plant Applications DB** section, enter values as described in the following table.

Credential	Description
Server Name	Enter the host name or IP address of the Plant Applications database.
Database	Enter the name of the Plant Applications database that you want to connect with the Plant Applications Universal Client.
Instance	Enter the instance name of the SQL server. Entering an instance is optional. Note: You can specify values either for Instance or Port .
Port	Enter the port number that the instance uses to listen for the client connections.
Username	Enter the user name of the administrator who has read-write permissions to access the database you entered in the Database box. By default, the user name appears as <i>sa</i> .
Password	Enter the password for the Administrator user you entered in the Username box.

- b. Select **Validate** to validate the Plant Applications database configuration.
 - c. In the **CouchDB** tab, enter your Apache CouchDB credentials as described in the following table.

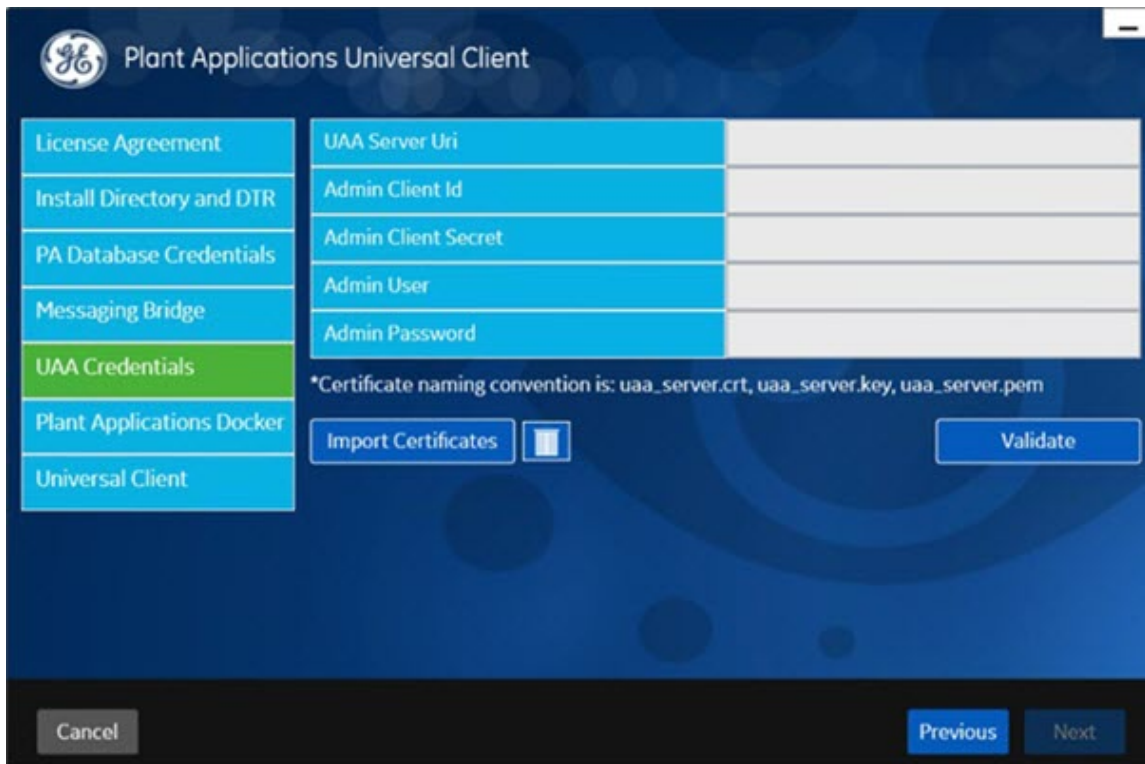
Credential	Description
CouchDB Server Uri	Enter the fully qualified web address of the Apache CouchDB in the format: <code>https://<host name or IP address>:<port number></code>
Database	Enter the value documents. This is the name of the Apache CouchDB database that you want to connect with the Plant Applications Universal Client.
Node	Enter the name of the node where Apache CouchDB is running. This is an optional field and, by default, the node value appears.
Username	Enter the user name of the administrator that has read-write permissions to access the database you entered in the Database box.
Password	Enter the password for the user you entered in the Username box.

- d. Select **Import Certificates** to import the Apache CouchDB server certificate (couch_server.crt) that you have generated.
8. Select **Validate** to validate the Apache CouchDB database credentials, and then select **Next**. The **Messaging Bridge** screen appears.

9. Enter the credentials of your RabbitMQ Administrator account for queuing the messages as described in the following table.

Credential	Description
Server Name	Enter the host name of the RabbitMQ server.
Username	Enter the username of the RabbitMQ administrator.
Password	Enter the RabbitMQ administrator password.

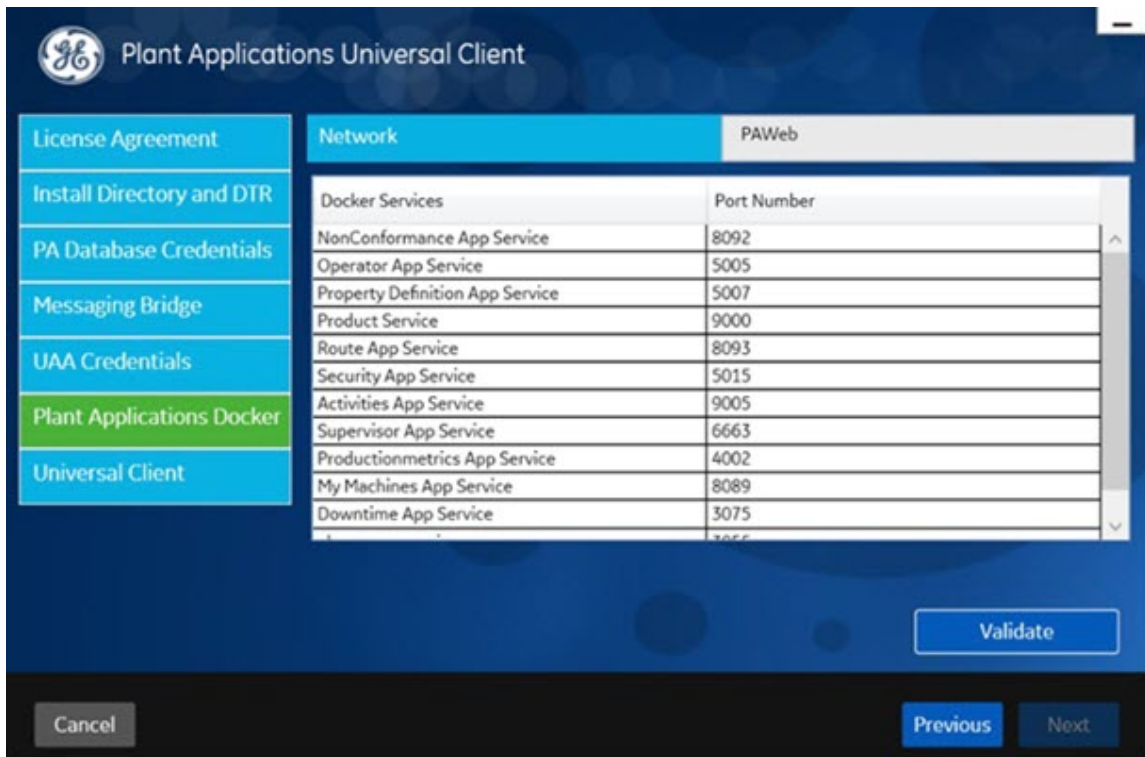
10. Select **Validate** to validate the RabbitMQ Administrator connection configuration, and then select **Next**.
The **UAA Credentials** screen appears.



11. Enter the Operations Hub UAA details for authenticating the users to access the Plant Application Universal Client as described in the following table.

Credential	Description
UAA Server Uri	Enter the service uri of Operations Hub UAA in the following format: <code>https://<IP address or host name of Operations Hub UAA>:<port number>/uaa</code>
Admin Client ID	Enter the client ID of the Operations Hub UAA administrator. By default, the client ID is pauc.
Admin Client Secret	Enter the client secret of Operations Hub UAA. By default, the client secret is paucsecret.
Admin User	Enter the user name of the administrative user account created in Operations Hub UAA and configured in the Plant Applications server. By default, the user name is bm_operator_1.
Admin Password	Enter the password of the administrative user. By default, the password is bm_operator_1.

12. Select **Import Certificates** and select the the UAA server certificates (uaa_server.crt, uaa_server.pem, and uaa_server.key) .
13. Select **Validate** to validate the Operations Hub UAA credentials, and then select **Next**.
The **Plant Applications Docker** screen appears, displaying all the exposed Plant Applications services that are integrated with the Universal Client. You can also modify the port numbers.



14. Ensure that the port numbers are valid and unused in the target Linux machine, then select **Validate** to validate the ports, and then select **Next**.

Note: Though the validation happens in the local machine, you must ensure that ports are available on the target Linux machine.

The **Universal Client** screen appears, displaying the host name and port number that enable you to access Plant Applications Universal Client.

Plant Applications Universal Client

License Agreement	Application	Universal Client
Install Directory and DTR	Server Name	dns.htclab.ge.com
PA Database Credentials	Port Number	8445

*Certificate naming convention is: pa_uc_cert.crt,pa_uc_cert.key, pa_uc_cert.pem

Generate UC Self-Signed Certificates
 Existing UC SSL Certificates

Applications and web service to facilitate the execution of discrete manufactures and includes Efficiency (Equipment, Reports, Downtime), Route Management, Order Management, Operation and Work Queue operator applications, Non-conformation Management, Property Definition and Security Management.

Validate

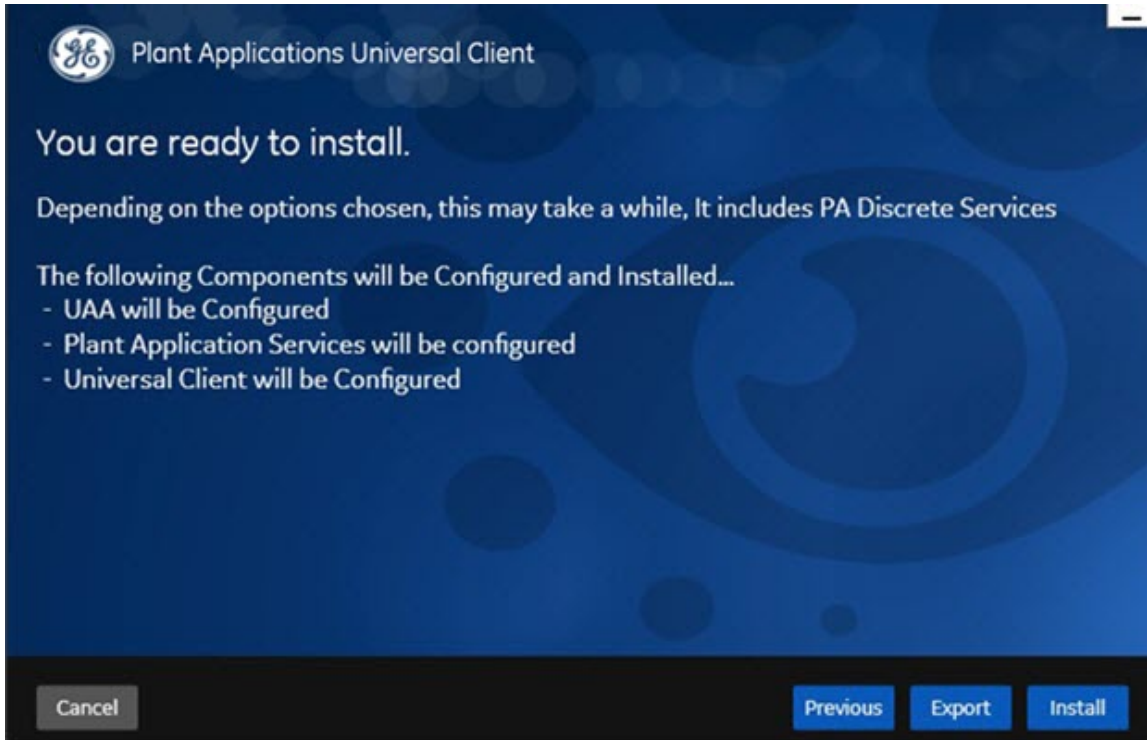
Cancel Previous Next

Important: By default, local host name appears in the **Server Name** box. You must replace it with the host name of the target Linux machine. The host name must be in lower case.

15. Ensure that the port number is valid and unused on the target Linux machine.
16. If you want to generate self-signed certificates, select **Generate UC Self-Signed Certificates**. If you want to use existing certificates, select **Existing UC SSL Certificates**, and then select the certificates. Ensure that the names of the files are `pa_uc_cert.crt`, `pa_uc_cert.key`, and `pa_uc_cert.pem`.
17. Select **Validate**, and then select **Next**.

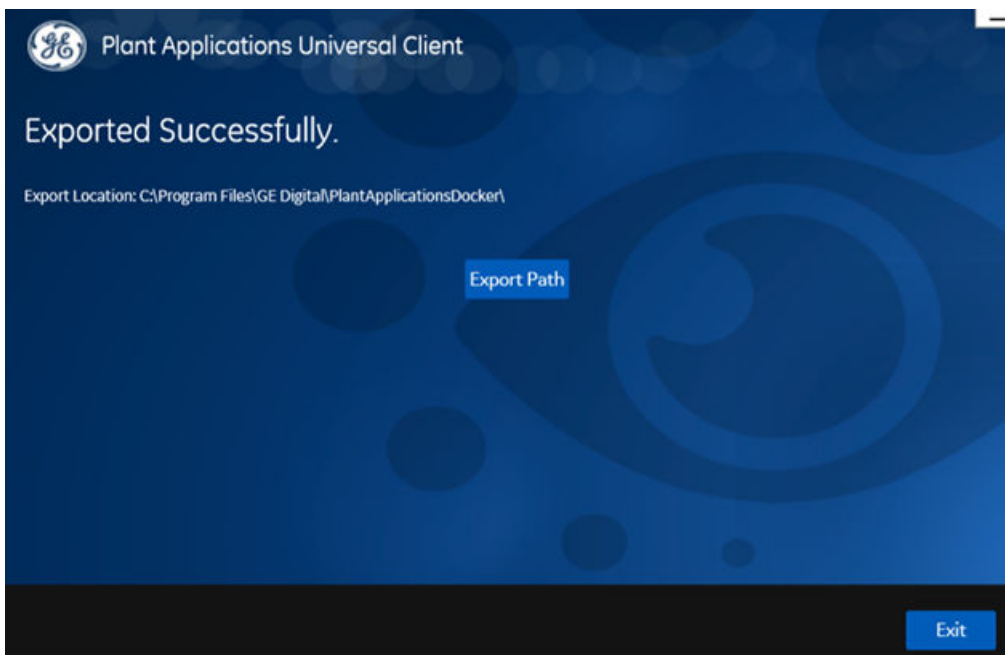
Note: Though the validation happens in the local machine, you must ensure that ports are available on the target Linux machine.

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



Important: Do not select **Install**.

18. Select **Export** to generate the binary files and configuration files required to install Plant Applications Universal Client on the target Linux machine. The **Exported Successfully** screen appears.



19. Select **Export Path** to navigate to the folder in which the binary files and configuration files are available. The `PlantApplicationsDocker` folder appears, displaying the binary files and configuration files.

Next Steps

- Use the binary files and configuration files that you have exported to [install Plant Applications Universal Client](#) on the target Linux machine.

Note: When you transfer files from the Windows machine to the target Linux machine using a file transfer program, ensure that all the text-based files (for example, .yml, .env, .sh, .cfg, json, and .txt files) are converted as text files. This is to replace all the carriage returns to line feeds.

Install Plant Applications Universal Client

Before You begin

Ensure that:

- You are an Administrator with execute permissions.
- Your system meets the [preinstallation requirements](#).
- You have [generated the binary files and configuration files required to Install Plant Applications Universal Client](#) and copied the exported files and folders to the Linux machine on which you want to install Plant Applications Universal Client.
- Docker is running.


Procedure

1. Copy the root folder (PlantApplicationsDocker) to a folder in the target Linux machine.
2. While generating binary and configuration files, if you selected the **New DTR** option, perform steps 3 through 7. Otherwise, log in to the existing Docker registry, and skip to step 8.

Note: To log in to a Docker registry, run the following command: `docker login <URL of the registry>`

3. Using terminal, navigate to the `pa-dtr` folder.
4. Edit the `.env` file, and update following parameters with the absolute path of the root folder.
 - `REGISTRY_WEB_CONFIG_VOLUME_PATH`
 - `REGISTRY_WEB_DB_VOLUME_PATH`
 - `REGISTRY_CONFIG_VOLUME_PATH`

```
COMPOSE_CONVERT_WINDOWS_PATHS=1
REGISTRY_WEB_IMAGE=hyper/docker-registry-web
REGISTRY_IMAGE=registry:2.4.1
REGISTRY_WEB_CONFIG_VOLUME_PATH=//C:/Program Files/GE Digital/PlantApplicationsDocker/pa-dtr/conf/registry-web
REGISTRY_WEB_DB_VOLUME_PATH>//C:/Program Files/GE Digital/PlantApplicationsDocker/pa-dtr/conf/registry-web/db
REGISTRY_CONFIG_VOLUME_PATH>//C:/Program Files/GE Digital/PlantApplicationsDocker/pa-dtr/conf/registry
```



5. In the `pa-dtr` folder, change the permission of the `PA_DTR_Start_Lix.sh` file to 775.
6. Access the `PA_DTR_Start_Lix.sh` file, and run the Shell script as an Administrator. This is necessary to create the Docker registry.
7. Go to the following locations to check if the docker registry is created successfully.
 - Registry-url: `http://<host name or IP address>:5000` for checking if the registry is up and running.
 - Registry-web-url: `http://<host name or IP address>:8080` for checking the docker images.
8. Using terminal, navigate to the `pa-service-tars` folder and run one of the following commands:
`docker-push-util.sh <host name or IP address of the machine on which DTR is running>:<port number>`
 - For a new DTR: `docker-push-util.sh <host name or IP address>:<port number>`

- For an existing DTR: `docker-push-util.sh <host name or IP address>`

Note: Ensure that you have added your `<host name or IP address>`: `<port number>` to the **Daemon** wizard and `<host name or IP address>` to the **Proxies** wizard in the Docker Settings.

9. Using terminal, navigate to the `plantapps-web-docker` folder, open the `.env` file. The FOLDER PATHS records appear.

10. In the `.env` file, update following parameters with the absolute path of the root folder.

- ERROR_LOGS_PATHS
- CONFIG_FOLDER_PATH
- SECRETS_FOLDER_PATH
- ZOOKEEPER_DATA_FOLDER_PATH
- ZOOKEEPER_LOGS_FOLDER_PATH
- KAFKA_DATA_FOLDER_PATH

```
ERROR_LOGS_PATHS=//C/Program Files/GE Digital/PlantApplicationsDocker/plantapps-web-docker/mnt/logs
CONFIG_FOLDER_PATH=//C/Program Files/GE Digital/PlantApplicationsDocker/plantapps-web-docker/mnt/paweb/config
SECRETS_FOLDER_PATH=//C/Program Files/GE Digital/PlantApplicationsDocker/plantapps-web-docker/Secrets
ZOOKEEPER_DATA_FOLDER_PATH=//C/Program Files/GE Digital/PlantApplicationsDocker/plantapps-web-docker/mnt/data/zookeeper
ZOOKEEPER_LOGS_FOLDER_PATH=//C/Program Files/GE Digital/PlantApplicationsDocker/plantapps-web-docker/mnt/logs/zookeeper
KAFKA_DATA_FOLDER_PATH=//C/Program Files/GE Digital/PlantApplicationsDocker/plantapps-web-docker/mnt/data/kafka
```

11. In the `plantapps-web-docker > mnt > paweb > config` folder, in the `workorder_entrypoint.sh` file, replace the value highlighted in red with the absolute path of the root folder.

```
#start the script to create the DB and data then start the sqlserver
chmod +x /config/*.sh

source /config/env_secrets_expand.sh

cp /run/secrets/uaa_cert.crt /usr/local/share/ca-certificates/uaa_cert.crt
cp /run/secrets/UAA_CA.pem /usr/local/share/ca-certificates/UAA_CA.crt
cp /run/secrets/pa_uc_cert.crt /usr/local/share/ca-certificates/pa_uc_cert.crt

update-ca-certificates

echo "3.26.123.14 uaa-server" >> /etc/hosts

dotnet GE.PlantApps.WorkOrderService.dll

docker run --rm --network MES_Services_PAWeb -v //C/Program Files/GE Digital/PlantApplicationsDocker/plantapps-web-docker/mnt/p
```

12. Using terminal, navigate to the `plantapps-web-docker` folder, change the file permission of `PA_Services_Start_Lix.sh` to 775.

13. Run the `PA_Services_Start_Lix.sh` file.

14. Using terminal, navigate to the `plantapps-universal-client` folder, and then open the `.env` file.

The records associated with the PATH and FILE keys appear.

15. In the `.env` file, update following parameters as shown in the image below with the absolute path of the root folder.

- CONFIG_FOLDER_PATH
- DOWNTIME_APP_PROPERTIES_FILE
- PRODUCTION_METRICS_APP_PROPERTIES_FILE
- APPHUB_LOCALCONFIG_FILE
- ALARM_CONFIG_FILE
- OPERATOR_APP_PROPERTIES_FILE
- PROPERTYDEFINITION_APP_PROPERTIES_FILE
- NONCONFORMANCE_APP_PROPERTIES_FILE
- SUPERVISOR_PROPERTIES_FILE
- ROUTEAPP_PROPERTIES_FILE
- WORKQUEUEAPP_PROPERTIES_FILE

- SECURITY_ADMINISTRATION_APP_PROPERTIES_FILE
- MYMACHINESAPP_PROPERTIES_FILE
- ALARM_NOTIFICATION_APP_PROPERTIES_FILE

```

CONFIG_FOLDER_PATH=//C/Program Files/GE Digital/PlantApplicationsDocker/plantapps-universal-client/Scripts
DOWNTIME_APP_PROPERTIES_FILE=//C/Program Files/GE Digital/PlantApplicationsDocker/plantapps-universal-client/downtime-app/app.properties.js
PRODUCTION_METRICS_APP_PROPERTIES_FILE=//C/Program Files/GE Digital/PlantApplicationsDocker/plantapps-universal-client/productionmetrics-app
APPBUS_LOCALCONFIG_FILE=//C/Program Files/GE Digital/PlantApplicationsDocker/plantapps-universal-client/localconfig.json
ALARM_CONFIG_FILE=//C/Program Files/GE Digital/PlantApplicationsDocker/plantapps-universal-client/alarm-widget-app/FAAlarmConfig.json
OPERATOR_APP_PROPERTIES_FILE=//C/Program Files/GE Digital/PlantApplicationsDocker/plantapps-universal-client/operatorapp/app.properties.json
PROPERTYDEFINITION_APP_PROPERTIES_FILE=//C/Program Files/GE Digital/PlantApplicationsDocker/plantapps-universal-client/propertydefinitionapp
NONCONFORMANCE_APP_PROPERTIES_FILE=//C/Program Files/GE Digital/PlantApplicationsDocker/plantapps-universal-client/nonconformance-app/app.pr
SUPERVISOR_PROPERTIES_FILE=//C/Program Files/GE Digital/PlantApplicationsDocker/plantapps-universal-client/supervisorapp/app.properties.json
ROUTEAPP_PROPERTIES_FILE=//C/Program Files/GE Digital/PlantApplicationsDocker/plantapps-universal-client/routeapp/app.properties.json
WORKQUEUEAPP_PROPERTIES_FILE=//C/Program Files/GE Digital/PlantApplicationsDocker/plantapps-universal-client/workqueue-app/app.properties.js
SECURITY_ADMINISTRATION_APP_PROPERTIES_FILE=//C/Program Files/GE Digital/PlantApplicationsDocker/plantapps-universal-client/securityadminist
MYMACHINESAPP_PROPERTIES_FILE=//C/Program Files/GE Digital/PlantApplicationsDocker/plantapps-universal-client/mymachines-app/app.properties.
ALARM_NOTIFICATION_APP_PROPERTIES_FILE=//C/Program Files/GE Digital/PlantApplicationsDocker/plantapps-universal-client/alarm-notification-ap
ALARM_LOG_FILE=//C/Program Files/GE Digital/PlantApplicationsDocker/plantapps-universal-client/logs/plantappscontainer/plantappscontainer.lo
ALARM_LOG_FILE1=//C/Program Files/GE Digital/PlantApplicationsDocker/plantapps-universal-client/logs/plantappscontainer/plantapps-container.

```

16. Using terminal, navigate to the `plantapps-universal-client` folder, and change the permission of the `PA_Apps_Start_Lix.sh` file to 775.
17. Run the `PA_Apps_Start_Lix.sh` file after changing the file permission to 775.

Results

The Docker-based installation of Plant Applications Universal Client is completed.

Tip: To verify that the installation is successful:

1. Run the following command to verify that the stacks (that is, PARegistry, PAServices, and PAContainer) are deployed: `docker stack ls`
2. Run the following command to verify that all the services in Plant Applications Universal Client are running: `docker service ls`

A list of services that are deployed on Docker appear. In the **REPLICAS** column:

- The value **1/1** indicates that the service is running.
- the value **0/1** indicates that the service is not running. If that happens, verify after some time, or access the service log by running the following command: `docker service logs <name of the service>` (for example, `docker service logs PAServices_assignmentservice`).

If you want to remove the stack, run the following command: `docker stack rm <name of the stack>`

Note: Wait for a few minutes (about 20 minutes) to access the Plant Applications Universal Client.

Next Steps

- Access Plant Applications Universal Client using the following URL: `https://<host name>:<port number>` where `<host name>` and `<port number>` are the values that you entered while generating the binary files and configuration files required to Install Plant Applications Universal Client.
- [Configure Plant Applications to Enable Discrete Applications](#) on page 45

Configure Plant Applications to Enable Discrete Applications

Only if a production line is route-enabled, you can use it in 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.

Uninstall Plant Applications Universal Client

Procedure

1. Navigate to the installation folder of Plant Applications Universal Client on the target Linux machine.
2. Using terminal, run the following commands:

```
chmod +x DockerFlush.sh
./DockerFlush.sh <IP address or host name of the DTR machine>:<port number>
```

Results

Plant Applications Universal Client is uninstalled.

Chapter 4

Upgrade Plant Applications Universal Client

Topics:

- [Upgrade the Plant Applications Universal Client \(Non-Docker Installer only\)](#)
- [Import the Historian UAA Certificate](#)
- [Configure ThingWorx UAA Authenticator](#)

Upgrade the Plant Applications Universal Client (Non-Docker Installer only)

Before You begin

[Upgrade the Plant Applications Universal Client \(Non-Docker Installer only\)](#) on page 47

- Ensure that you complete the following procedure specific to the Plant Applications Message Bridge:
 1. Uninstall the earlier version of the Plant Applications Message Bridge.
The Proficy Server Message Bridge service is disabled.
 2. Delete the directory - `C:\Program Files (x86)\Proficy\Proficy Server\RabbitMQMessageBridgeService`.
 3. Restart your computer.
 4. Install the version of the Plant Applications Message Bridge included in the Plant Applications installer.
 5. Restart the Proficy Server Manager service.
The Proficy Server Message Bridge service is automatically restarted.
- Ensure that you create a backup copy of the text file that includes the user-specific settings. The file is created in the directory `<tomcat_home>/Apache Software Foundation/Tomcat 9.0/users/<user>`, where:
 - `<tomcat_home>` is the directory where you installed Apache Tomcat. For example, `C:/Program Files`.
 - `<user>` is the name of a logged-in user.

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

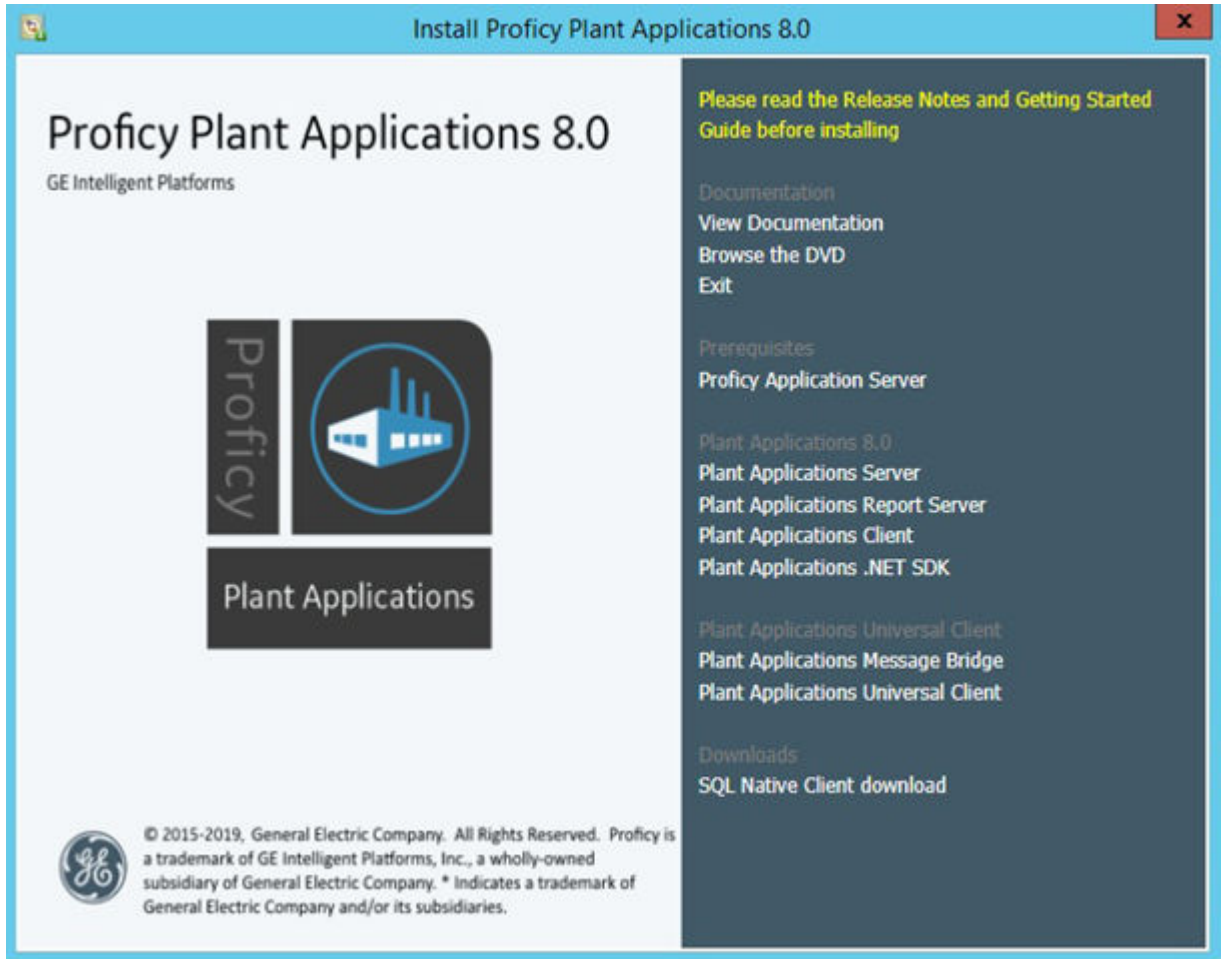
About This Task

You can upgrade any earlier service pack (SP) version of Plant Applications Universal Client 7.0 to 8.0.

Note: The Plant Applications 8.0 installer is the base installer for all upgrade requirements.

Procedure

1. Run the `installfrontend.exe` file as an Administrator.
The installation menu appears, displaying the **Install Proficy Plant Applications 8.0** screen.



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

2. Select **Plant Applications Universal 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 Universal Client** screen.



3. In the **Welcome to Plant Applications Universal Client** screen, select **Next**.
If any of the required software is missing, the **Prerequisites** screen appears. In the **Prerequisites** screen, select **Next** to view all installed prerequisites and install any missing prerequisites.

Plant Applications Universal Client 8.0

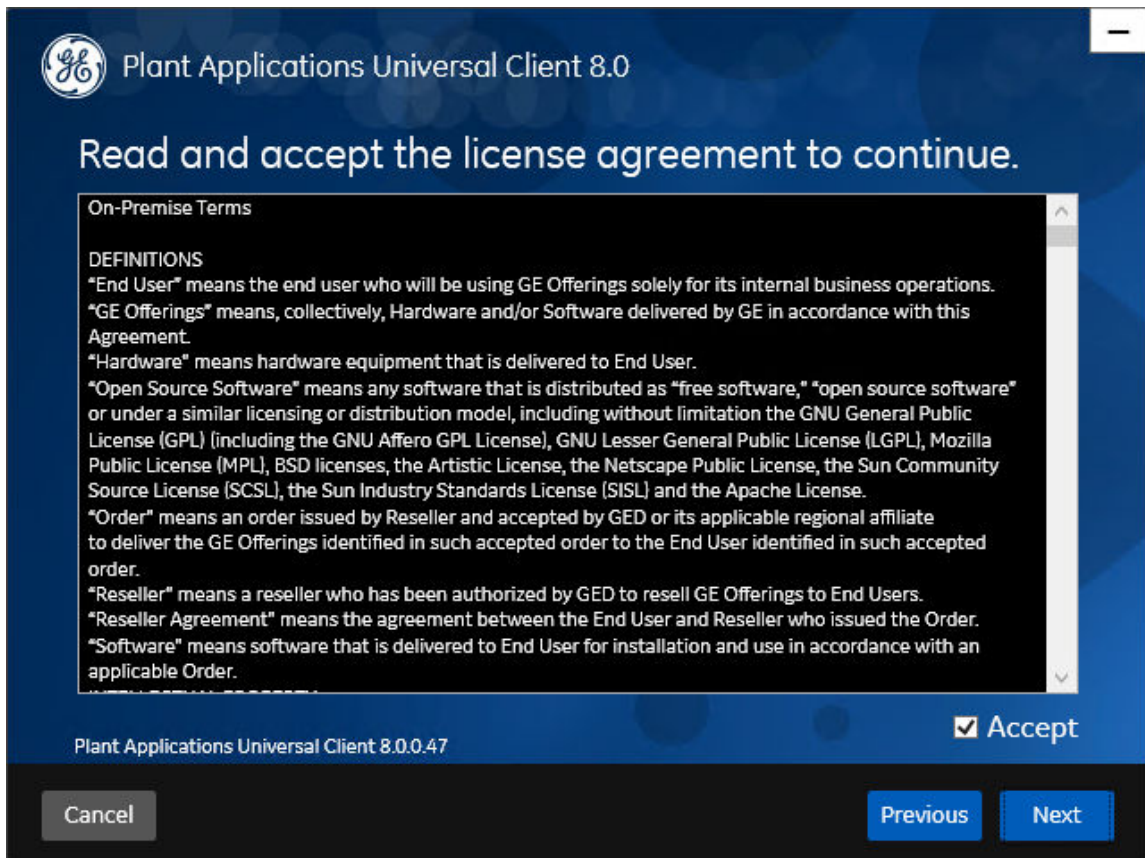
Prerequisites

Apache Tomcat	Installed
Ruby 2.3.3	Installed
Ruby Dev Kit	Installed
Microsoft OLEDB driver 18 for SQL Server	Installed
Open JDK 1.8	Will be installed
Node.js 8.12	Will be installed
Python 2.7	Will be installed

Plant Applications Universal Client 8.0.0.47

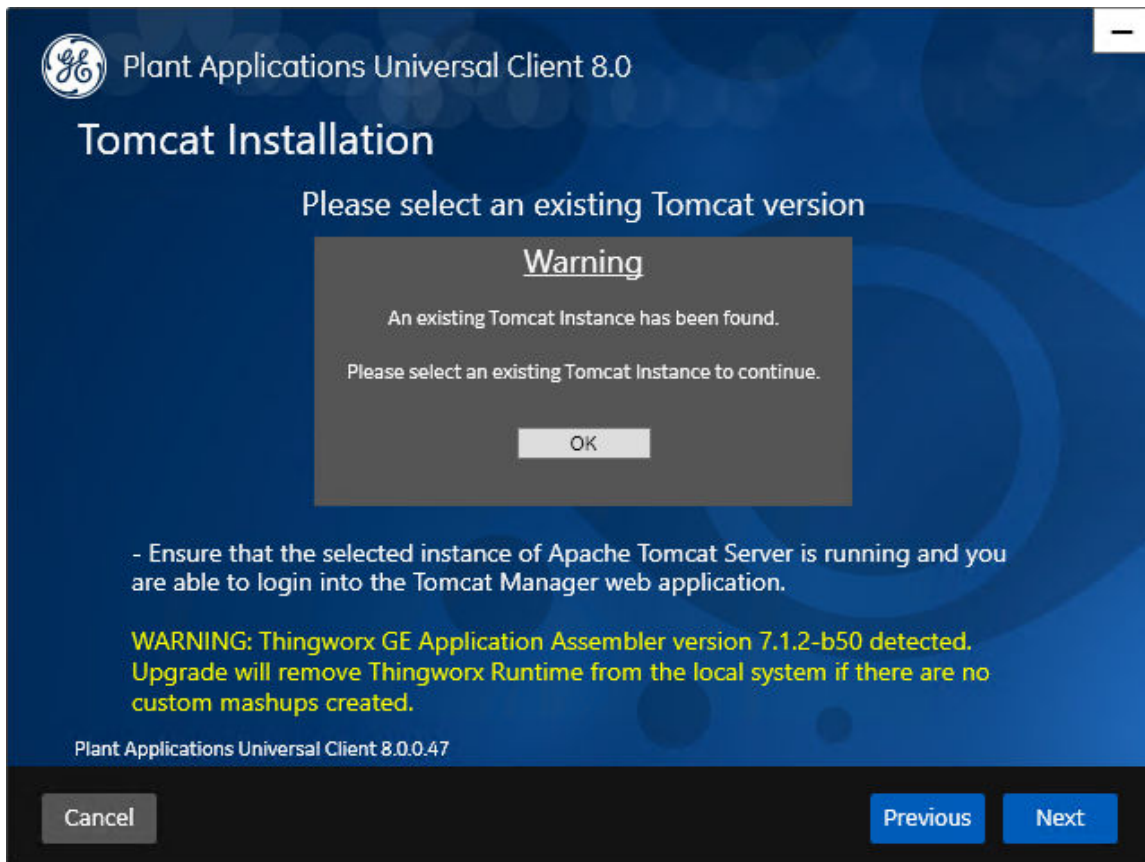
Cancel Previous Next

If all the required software is installed, then the **Read and accept the license agreement to continue** screen appears.



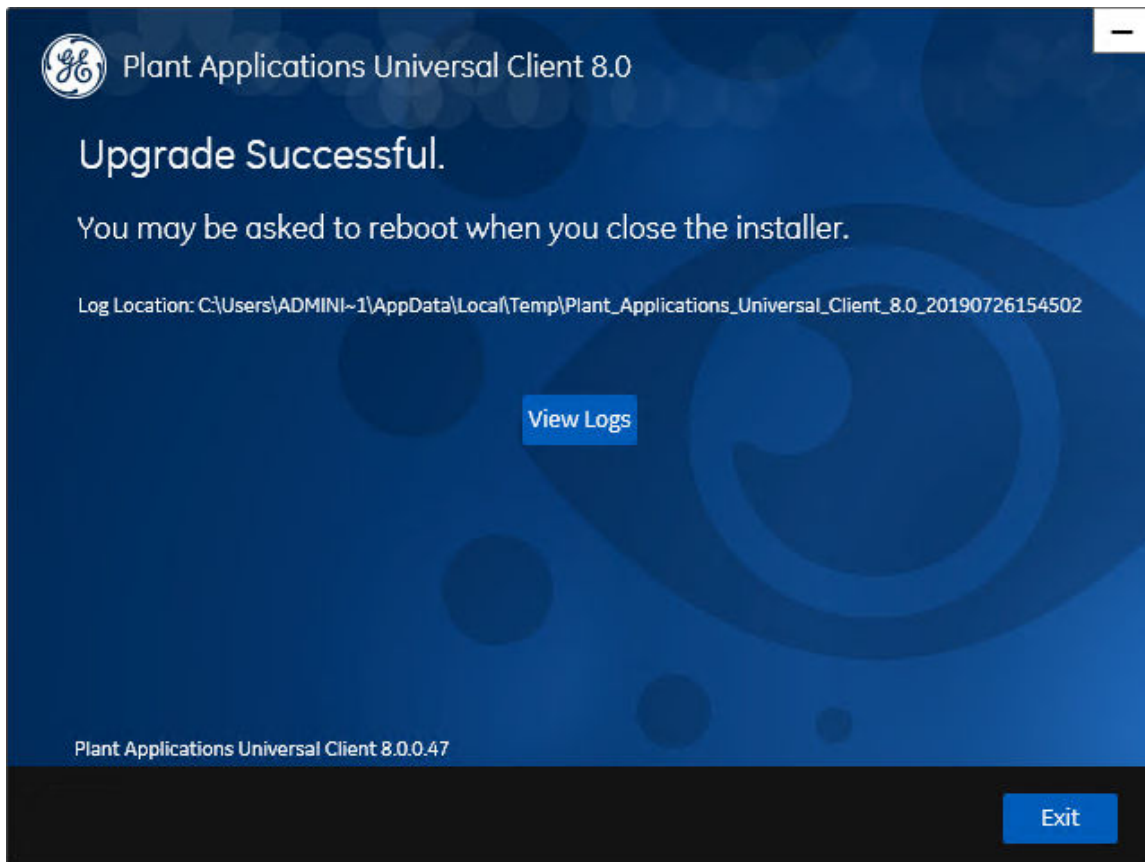
4. Read the license agreement, select **Accept**, and then select **Next** to continue the upgrade.

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.



Select **OK**. You can now select an appropriate Tomcat instance from the drop-down and then select **Next**.

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.



5. **Optional:** Select **View Logs** to see the upgrade details.
6. In the **Upgrade Successful** screen, select **Exit** to close the upgrade wizard.

Results

Plant Applications Universal Client has been upgraded to the latest version.

Next Steps

- [Import the Historian UAA certificate.](#)
- [Configure ThingWorx UAA Authenticator.](#)

Import the Historian UAA Certificate

If you have installed custom applications in the previous version of Plant Applications, you must import the Historian UAA certificate.

Procedure

1. In the Plant Applications Universal Client, in the application navigation menu, select **Custom Applications**.
2. Access the settings, and then open developer tools.
3. Select **Security**, and then select **View Certificate**.
The details of the certificate appear.
4. Select **Issuer**, and then select **Copy to File**.
The **Export Certificate** window appears.

5. Select **Next**.
6. Select **Base-64 encoded X.509 (.CER)**, and then select **Next**.
7. Select **Browse**, and assign a certificate name.
8. Select **Finish**.
The certificate has been exported.
9. Double-click the certificate, and then select **Install**.
10. Select **Local Machine**, and then select **place all certificates in following store**.
11. Select **Browse**, and then select **Trusted Root Certification Authorities**.
12. Select **Finish**.
The certificate has been imported.

Configure ThingWorx UAA Authenticator

This topic describes how to configure ThingWorx UAA authenticator to use Operations Hub UAA Authenticator to access custom applications that you have created in a previous version of Plant Applications.

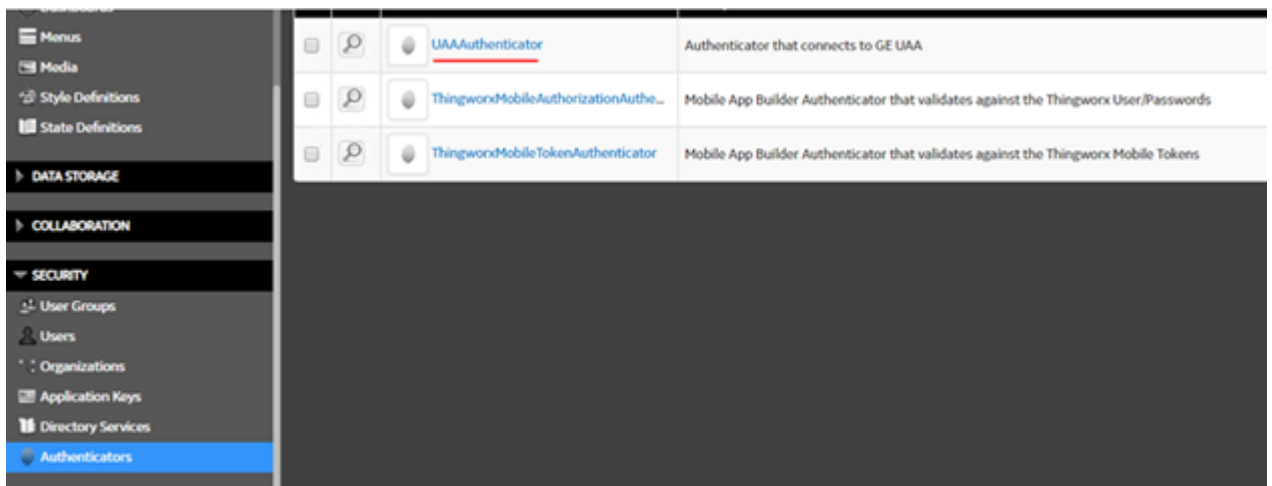
Before You begin

Ensure that:

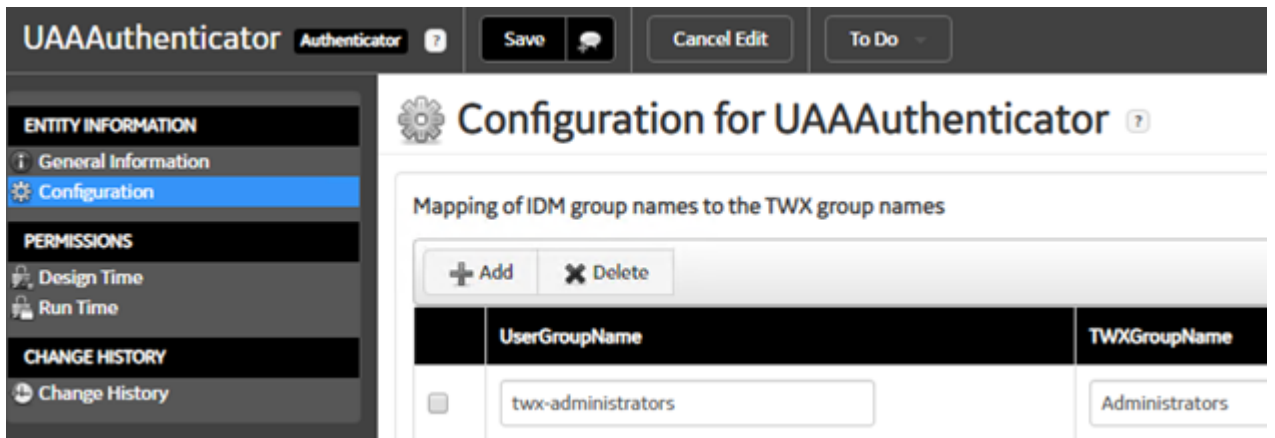
- Operations Hub UAA is installed. For instructions, refer to the Operations Hub UAA installation guide that is available in the Operations Hub UAA installation package.
- ThingWorx Application Assembler 7.1.2 is deployed in Apache Tomcat.
- ThingWorx Composer is accessible via the following URL: `https://<host name>:<Tomcat redirect port number>/Thingworx/Composer/index.html`

Procedure

1. Log in to ThinWorx Composer.
2. In the **Security** section, select **Authenticators**.
3. Select **UAA Authenticator**.



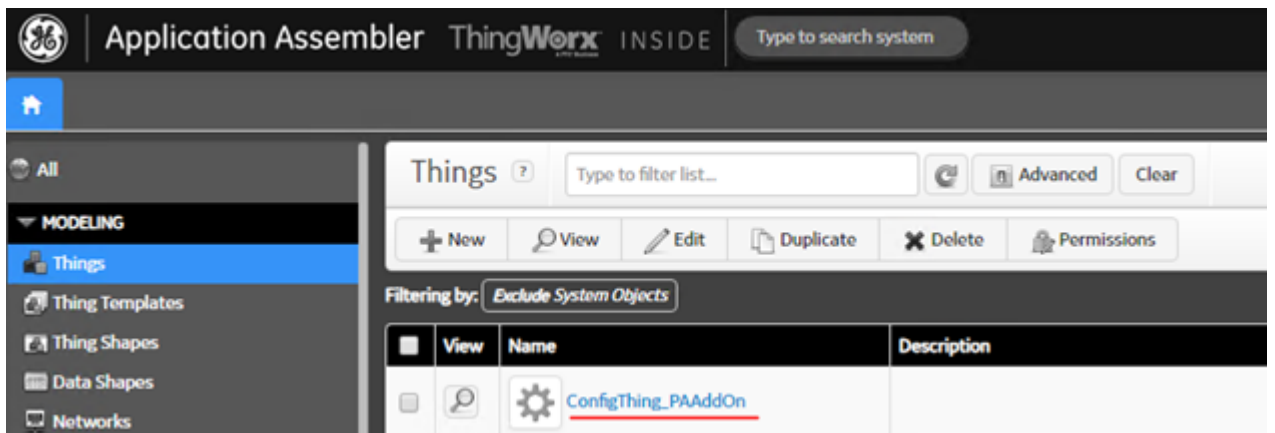
4. Select **Configuration**.



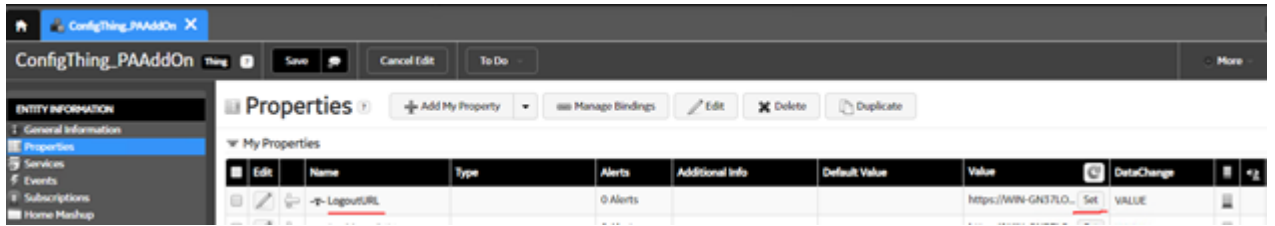
5. Scroll down the page to access the **UAA Authenticator Configuration** section.
6. Provide the following values.

Box	Description
SingleSignOnURL	Enter the Operations Hub UAA URL.
UAAClientId	Enter a value in the following format: <host name>_mes_process, where <host name> is the host name of the machine on which Plant Applications Universal Client is installed, in lowercase.
UAAClientSecret	Enter plantappssecret.
RedirectURL	Leave as is. If, however, the URL contains the host name in uppercase, replace it with lowercase (for example, replace https://UCNODE:8444/Thingworx/Home?postAuth=true with https://ucnode:8444/Thingworx/Home?postAuth=true).

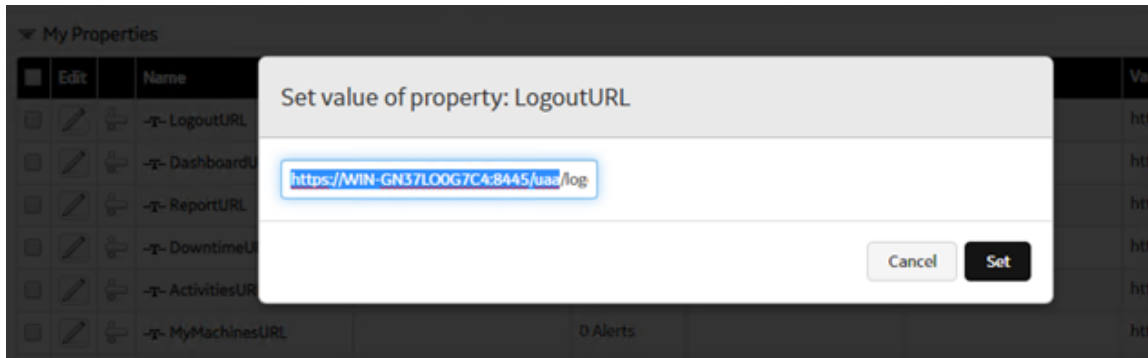
7. Select **Save**.
8. Access the home page of ThingWorx Composer.
9. In the **Modeling** section, select **Things**.
10. Select **ConfigThing_PAAddOn**.



11. Select **Properties > My Properties**.
12. In the row containing **LogoutURL**, select **Set**.



The **Set value of property: LogoutURL** window appears.



13. Replace the URL with the Operations Hub UAA URL, and then select **Set**.
Replace `https://WIN-GN37LOOG7C4:8443/uaa/logout.do?redirect=https://WIN-GN37LOOG7C4:8444/Thingworx` with Updated URL => `https://WIN-GN37LOOG7C4:8445/uaa/logout.do?redirect=https://WIN-GN37LOOG7C4:8444/Thingworx`
14. Select **Save**.
15. Log out of ThingWorx Composer.
16. Log in to ThingWorx Runtime by accessing Plant Applications Universal Client and selecting **Custom Applications** from the application navigation menu.
ThingWorx redirects you to the Operations Hub UAA authentication page.
17. Log in to Operations Hub UAA.
You can now access the custom applications that you have created in a previous version of Plant Applications.

Note: Sometimes, a blank page appears after you login to Operations Hub UAA. To fix this issue, you must add the Operations Hub UAA certificate to the the JRE keystore or Apache Tomcat by performing the following steps:

- a. Access the home page of Apache Tomcat that you use for Plant Applications Universal Client.
- b. Select **Manager App**.
- c. Log in with the Apache Tomcat administrative user credentials.
Tomcat Web Applications Manager appears.
- d. Scroll to the end of the page to find out the JVM version number.
- e. Access the JRE version folder that Apache Tomcat uses.
- f. Open Command Prompt as an administrator, and change the directory to the `<JRE version>\lib\security` folder.
- g. Run the following command to import the certificate: `keytool -keystore cacerts -import -noprompt -alias <alias name> -file "<UAA certificate file path>"`, where `<alias name>` is a name that you want to provide for the certificate, and `<UAA certificate path>` is the path of the Operations Hub UAA certificate.
You are be prompted to enter the keystore password.
- h. Enter `changeit`.

- The certificate is added to the JRE keystore of Apache Tomcat.
- i. Close the instance of ThingWorx, and open it again.

Chapter 5

Troubleshooting

Topics:

- [Frequently Asked Questions \(Non-Docker only\)](#)
- [Troubleshoot the Tomcat Error](#)
- [Troubleshoot Access Issues](#)

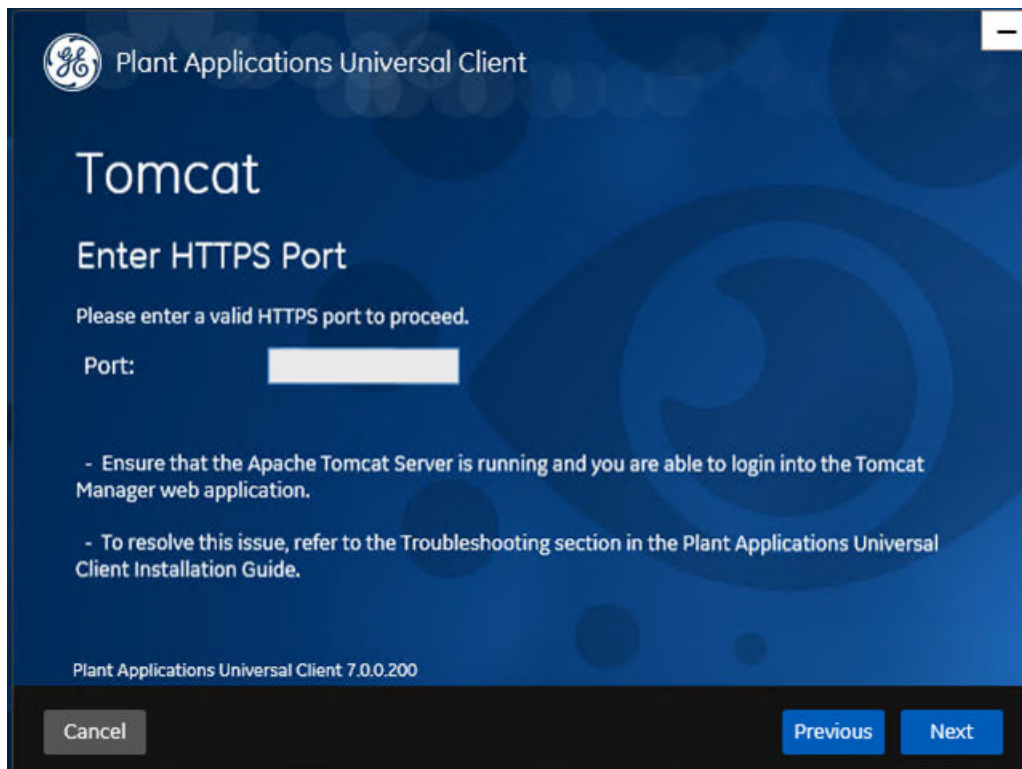
Frequently Asked Questions (Non-Docker only)

- Can I access the log files created after the Plant Applications Universal Client installation or upgrade process?
Yes. You can access the log files created during the installation process from the following directory: %USERPROFILE%\APPDATA\Local\Temp. The log files are available in the format Plant_Applications_Universal_Client_yyddmmhhmmss.
- What happens if I upgrade JAVA after installing the Plant Applications Universal Client?
If you upgrade JAVA later, it might create some issues in using the Plant Applications Universal Client, and Tomcat might stop. To resolve this issue, refer to the Community article 000020691 in the support site <http://support.ge-ip.com>.
- What should I do if the installation of GE Proficy Historian Server fails?
If Transport Layer Security (TLS) 1.1 or 1.2, or the security policy for using the FIPS compliant algorithms is enabled, the Historian installation process fails. To install Historian successfully, you must temporarily disable the required feature, and then after successful Historian installation enable the feature again.

Troubleshoot the Tomcat Error

About This Task

The following **Tomcat** screen appears when you try to upgrade the Plant Applications Universal Client and there is an issue with the Tomcat service.



To troubleshoot the Tomcat service error, perform the following steps:

Procedure

1. In the **Tomcat** window, ensure that you have entered the correct **HTTPS** port to continue with the installation.
2. Ensure that the Tomcat service is running.
 - a. Log in to the computer where you installed the Plant Applications Universal Client.
 - b. Select **Start**, and then search for the Services application.
 - c. In the command prompt, enter `services.msc`.
The **User Account Control** window appears.
 - d. Select **Yes**.
The **Services** window appears.
 - e. Verify that the **Status** of the Tomcat service configured during the Plant Applications Universal Client installation appears as **Running**. If not, start the service.

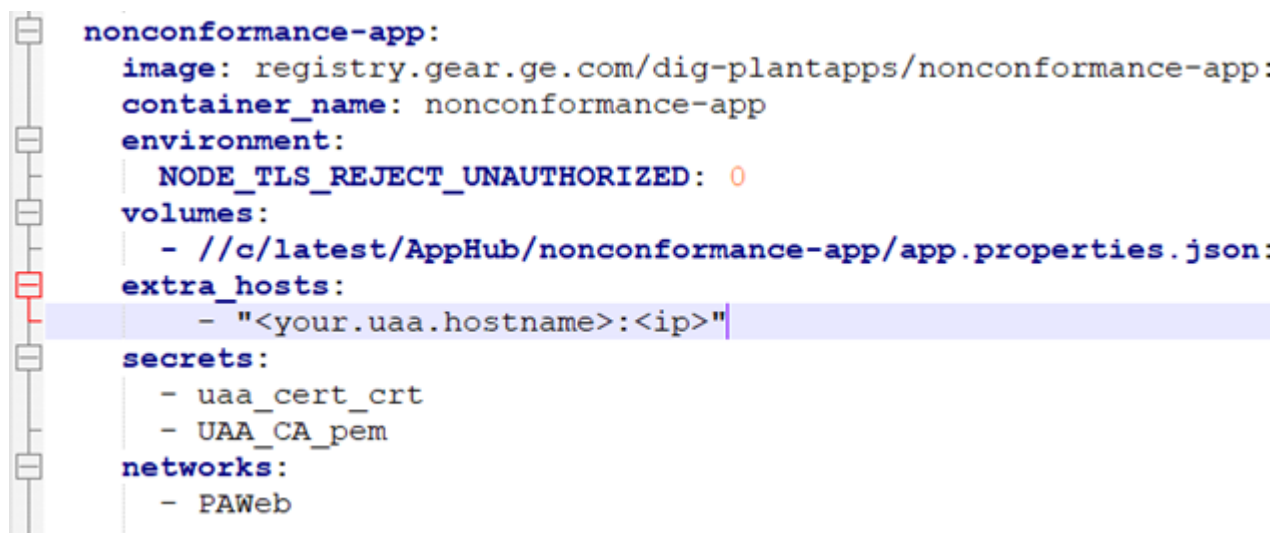
Troubleshoot Access Issues

This topic describes how to troubleshoot issues when you cannot access Operations Hub UAA, Apache CouchDB, or the Plant Applications database using the host name from the machine on which Docker has been installed. This is applicable only if you have installed Plant Applications Universal 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 Universal Client, add the following line in the `plantapps-web-docker/env.yml` and `plantapps-universal-client/env.yml` files:

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



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

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

- c) Using the Command Prompt, change the directory to `plantapps-universal-client`, and then run the following command: `./PA_Apps_Start_Lix.sh`
- 2. If the Apache CouchDB UAA server is not accessible using the host name from the machine on which Docker has been installed, perform the following steps:
 - a) For each application that will be deployed in Plant Applications Universal 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 Universal 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 Universal 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`

Chapter 6

Reference

Topics:

- [Configure the GE Proficy Historian Server Security Settings](#)

Configure the GE Proficy Historian Server Security Settings

About This Task

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

Procedure

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

The GE Proficy Historian Server is now configured for the Plant Applications Universal Client. You can now install the Plant Applications Universal Client on the same computer as the GE Proficy Historian Server.