GE VERNOVA

DIGITAL

PROFICY CIMPLICITY HMI/SCADA

Getting Started

Proprietary Notice

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

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

Trademark Notices

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

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

All other trademarks are the property of their respective owners.

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

Contents

Chapter 1. CIMPLICITY Installation

Installation Prerequisites

Before you install CIMPLICITY v2023, complete the tasks listed below.

Keeping the CimEdit/CimView Global Configuration

Complete this task if global specifications were configured in the CimEdit Global Configuration dialog box. The global configuration can affect navigation, script selections, compatibilty, and so forth.

1. Locate the the CimView.cfg file located in the `..\<CIMPLICITY Installation>\Data directory`.
2. Move the file to a different location.
3. When the installation is complete, move the configured file back into the `..\<CIMPLICITY Installation>\Data directory` to continue using those settings.

Uninstalling CIMPLICITY

If you are upgrading from an earlier version, the existing CIMPLICITY version must be uninstalled before you install the new version.

To remove the older version:

1. Open Windows Control Panel and select **Programs and Features**.
2. From the list of programs, locate CIMPLICITY, then select the application and select **Uninstall**.
3. When the wizard displays the Uninstall Complete window, select **Yes, I want to restart my computer now**.
4. Select **Finish**.

> **Important:**
> You must uninstall Historian before upgrading from earlier version of CIMPLICITY. Historian is now available with CIMPLICITY integrated installer.
>
> The CIMPLICITY uninstall process attempts to remove components that depend on CIMPLICITY, such as Alarm Cast, CNC, GlobalView, and Tracker.

You should verify that these components were removed when you uninstalled CIMPLICITY. If they were not, you must uninstall them manually.

Note:
Ensure that your system is updated with the latest Microsoft updates.

CIMPLICITY Installation using Installers

(Recommended) Install CIMPLICITY using Integrated Installer

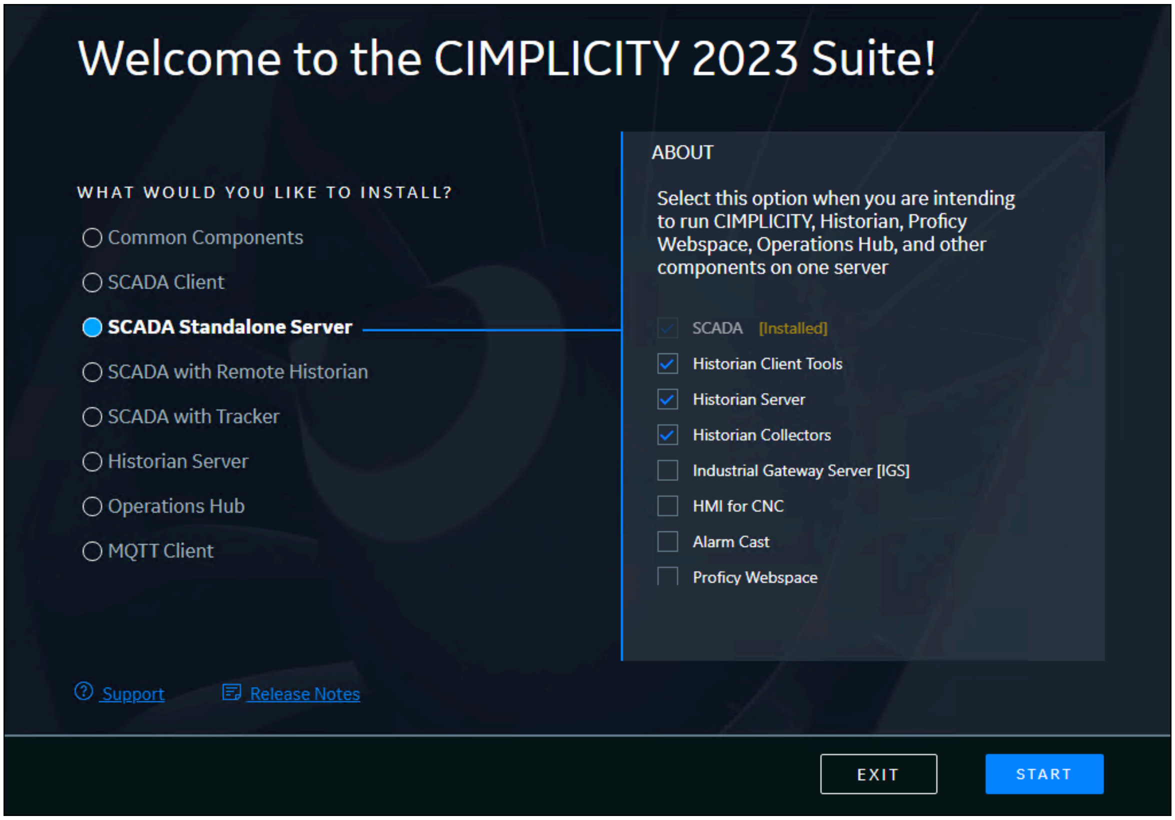
The CIMPLICITY integrated installer enables you to install different CIMPLICITY installations from viewer to Historian setups along with other supported products. You only need to download the installer once and install all the products you need to support your CIMPLICITY project.

Note:
You can also install CIMPLICITY in the usual method using the standalone installer available in the **CIMPLICITY** folder in the ISO. However, it is recommended to use the integrated installer to install CIMPLICITY and other products.

Installing CIMPLICITY:

1. Mount the downloaded CIMPLICITY ISO media.
2. From the ISO folder, double-click **Setup.bat**.

   The installer welcome screen appears, listing all the available packages that you can install as needed.



Welcome to the CIMPLICITY 2023 Suite!

WHAT WOULD YOU LIKE TO INSTALL?

○ Common Components
○ SCADA Client
● **SCADA Standalone Server**
○ SCADA with Remote Historian
○ SCADA with Tracker
○ Historian Server
○ Operations Hub
○ MQTT Client

ABOUT

Select this option when you are intending to run CIMPLICITY, Historian, Proficy Webspace, Operations Hub, and other components on one server

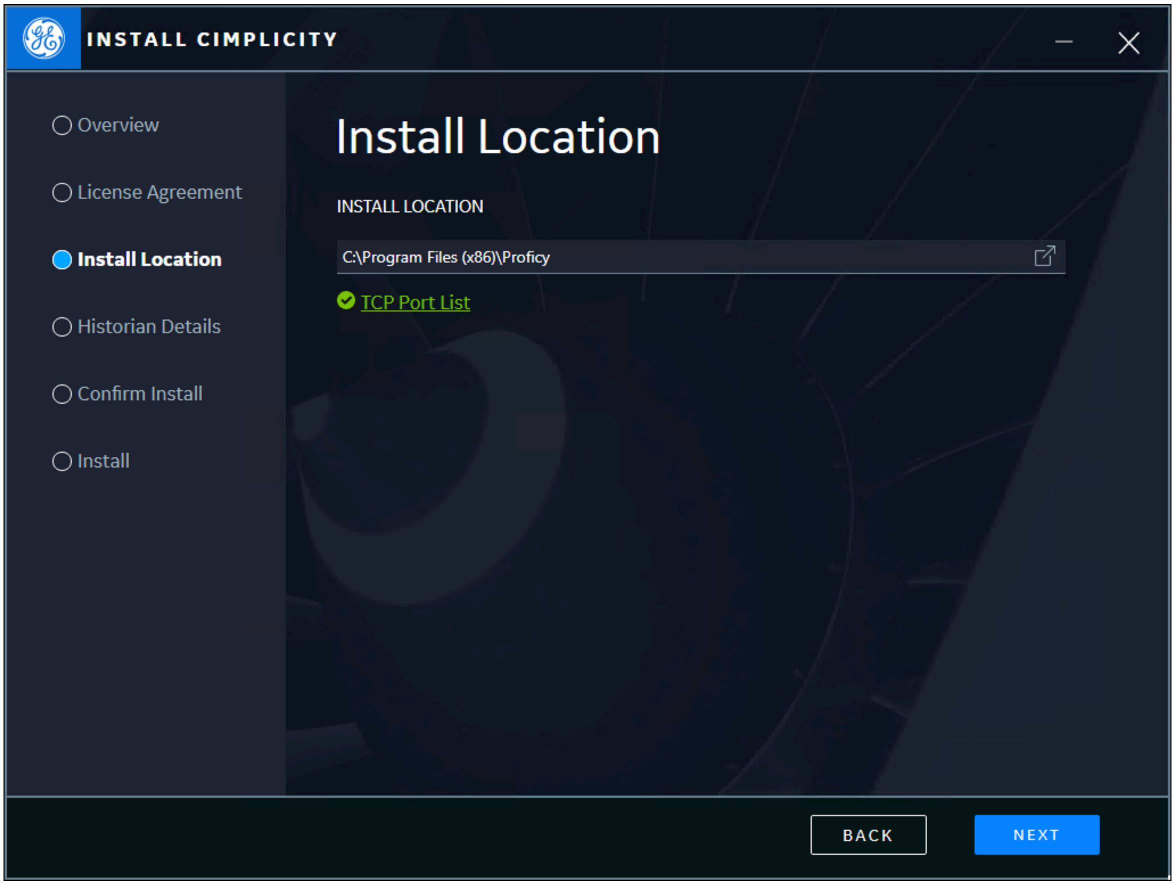
☑ SCADA [Installed]
☑ Historian Client Tools
☑ Historian Server
☑ Historian Collectors
□ Industrial Gateway Server [IGS]
□ HMI for CNC
□ Alarm Cast
□ Proficy Webspace

3. Select the package as needed and click **START**.

   The **Review License Agreement screen** appears.

4. Read the license agreement and click **ACCEPT**.

   The **Install Location** screen appears and validates for port conflicts.



Install Location

INSTALL LOCATION: C:\Program Files (x86)\Proficy

✓ TCP Port List

5. Browse and select a location for installation, then continue to the next screen.

   If there are port conflicts, the installer resolves the conflict and provides you the link to view the newly used ports.

6. Based on the selected package, you will be prompted to enter details pertaining to the products selected in that package. You can follow the installation screen to complete the installation. However, you can refer the below table that briefly explains about all the packages and their details.

Package	Description	Products Available	Details that you must provide while Installation
Common Components	Common Components are shared centralized services for all Proficy products. The common components should be installed once for your system running Proficy products on the same network.	◦ Configuration Hub ◦ Proficy Authentication ◦ Local License Server ◦ License Server Tool	In the Credentials screen, you will be prompted to enter the following details: ◦ **Configuration Hub** ▪ CLIENT ID- Enter a client id, which you can use to login to the Configuration Hub application. For example, `admin` ▪ CLIENT SECRET- Enter a secret password for your Configuration Hub client id. ◦ **Proficy Authentication** ▪ CLIENT ID- Enter a client id, which you can use to login to the Proficy Authentication application. ▪ CLIENT Secret- Enter a secret password for your Proficy Authentication client id.

Package	Description	Products Available	Details that you must provide while Installation
			Note: If you want your Client ID and Client Secret to be same as the Configuration Hub Client Id and Client Secret, you can select **Use the same credentials for Configuration Hub and Proficy Authentication**
SCADA Client	Select this option when you are intending to run CIMPLICITY as a client and Proficy Webspace.	◦ SCADA Viewer ◦ Historian Client Tools ◦ Proficy Webspace ◦ Operations Hub	If you are prompted to enter Operations Hub details, see the SCADA Standalone Server row below.
SCADA Standalone Server	Select this option when you are intending to run CIMPLICITY, Historian, Proficy Webspace, Operations Hub, and other components on one server. You can install Operations Hub and oth-	◦ SCADA ◦ Historian Client Tools ◦ Historian Server ◦ Historian Collectors ◦ Industrial Gateway Server (IGS) ◦ HMI for CNC ◦ Alarm Cast	In the **Historian details** screen, you will be prompted to enter the following details if you have Historian Installed: ◦ HISTORIAN SERVER- IP address or hostname in a fully qualified domain name format. ◦ Windows username and password of the default historian serv-

Package	Description	Products Available	Details that you must provide while Installation
	er products not included in this package separately post installing this package.	◦ Proficy Webspace ◦ Operations Hub	er to which the Remote Collector manager will connect. ◦ Historian data path- Path to install Historian Server. **Note:** You will be prompted with the Historian details only if you selected Historian product. In the **Historian details** screen, you will be prompted to enter the following details if you have not installed Historian server: ◦ Enable Historian services security- select this if you want to set up security while installation. ▪ CERTIFICATE PASSPHRASE- Enter a passphrase for the certificate generation.

Package	Description	Products Available	Details that you must provide while Installation
			In the **Operations Hub Details** screen, you will be prompted with the following details: **Credentials** ◦ Username- Enter a user name, which you can use to login to the Operations Hub application. For example, `ch_admin` ◦ Password- Enter a password for your Operations Hub user login. **Authentication** ◦ Use Locally Installed Proficy Authentication- If you select this check box, then the local instance of Proficy Authentication will be used.If you want to use an external Proficy Authentication (UAA), then leave this check box blank and proceed to provide more details. **Note:** Prior to Operations Hub installation, you must have a local or re-

Package	Description	Products Available	Details that you must provide while Installation
			mote instance of Proficy Authentication installed. The Operations Hub installation will not be allowed to continue if you select **Use Locally Installed Proficy Authentication** and it is not detected. ◦ BASE URL- Enter the url address to access the Proficy Authentication application. For example, `https://win10vm2/uaa` ◦ ADMIN CLIENT ID- Enter the administrator client id to login to Proficy Authentication. For example, `admin` ◦ ADMIN CLIENT ID SECRET- Enter the secret password for the Proficy Authentication administrator client id. ◦ CERTIFICATE FILE- You can browse and select

Package	Description	Products Available	Details that you must provide while Installation
			the security certificate, (or) let the system do it for you. When you test for validation, the system provides you with an option to use a detected certificate. ◦ TEST- Select this option to validate all your field entries. The validation results appear on the **Test External Proficy Authentication** screen, wherein you can do the following: ▪ Add and trust self-identified base url ▪ Add detected security certificate Proceed to next only after the validation test is successful. ◦ VIEW- Select this option if you want to open and check the added security certificate. **Configuration Hub Registration** ◦ Register After Install- If you select this check box, then you can skip registering Operations Hub with the Configu-

Package	Description	Products Available	Details that you must provide while Installation
			ration Hub application for now. You will then need to register after the current Operations Hub installation using the application shortcut on the Desktop. Refer to Register Operations Hub with Configuration Hub, in the Operations Hub online help.. If you choose to register along with the current Operations Hub installation, then leave this check box blank and proceed to provide more details. ◦ BASE URL- Enter the url address to access the Configuration Hub application. For example, `https://sbbco.meridium.com:5000/container-svc` ◦ CLIENT ID- Enter the url address to access the Configuration Hub application. For example, `https://sbbco.meridium-`

Package	Description	Products Available	Details that you must provide while Installation
			`.com:5000/container-svc` ◦ CLIENT SECRET- Enter the secret password created for your Configuration Hub client id.
SCADA with Remote Historian	Select this option when you are intending to run CIMPLICITY with Historian on a remote server and Proficy Webspace.	◦ SCADA ◦ Historian Client Tools ◦ Historian Collectors ◦ Industrial Gateway Server (IGS) ◦ HMI for CNC ◦ Alarm Cast ◦ Proficy Webspace ◦ Operations Hub	You will be prompted to enter Historian details and Operations Hub details. For more information, see the SCADA Standalone Server row above.
SCADA with Tracker	Select this option when you are intending to run CIMPLICITY with Tracker, Historian, Operations Hub on the server.	◦ SCADA ◦ Tracker ◦ Historian Client Tools ◦ Historian Server ◦ Historian Collectors ◦ Proficy Webspace ◦ Operations Hub	You will be prompted to enter Historian details and Operations Hub details. For more information, see the SCADA Standalone Server row above.
Historian Server	Select this option when you are intending to run Historian on a different serv-	Historian Server	You will be prompted to enter Historian details. For more information, see the SCADA Standalone Server row above.

Package	Description	Products Available	Details that you must provide while Installation
	er than CIMPLICITY SCADA.		
Operations Hub	Select this option when you are intending to run Operations Hub on the server.	Operations Hub	You will be prompted to enter Operations Hub details. For more information, see the SCADA Standalone Server row above.
MQTT Client	MQTT Client enables you to connect the SCADA/HMI clients with MQTT Brokers to communicate with the IoT devices in the plant. **Note:** Configuration of MQTT Client requires Configuration Hub to be installed in the SCADA network.	MQTT Client	For more information, see MQTT Client *(on page 147)*.

7. In the **Confirm Install** screen, select **START**.

Note:
If you selected Operations Hub, in the Confirm Install screen, you will be displayed with the following options:

- **Silent Install**- Select this option if you want to run a silent installation of products without any further user interaction or input.
- **Interactive Install**- Select this option if you want to customize additional settings.

8. After the installation is complete, select **CLOSE**.

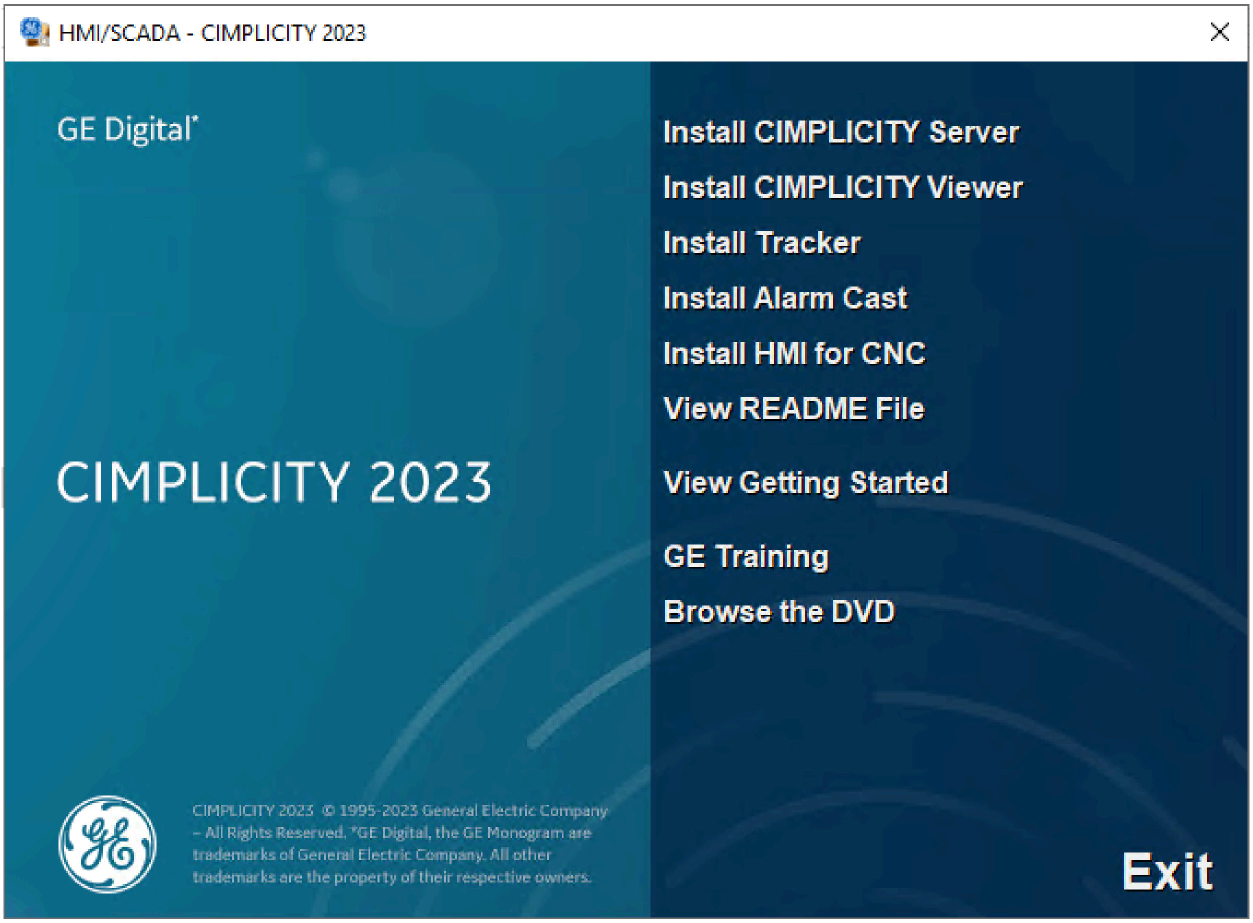
   A message appears asking whether you want to restart your computer, or install more products.

9. Select **Reboot Now** to restart your computer.

Install CIMPLICITY using Standalone Installer

The HMI/SCADA CIMPLICITY v2023 splash screen provides links to the core CIMPLICITY installation components and optional applications. You can install the components as needed.

Note:
If you need to install the products like Historian, Operations Hub, and more, you must install them using their respective install media, separately. To install CIMPLICITY and all the other products and components easily, it is recommended to use the integrated installer *(on page 6)*.



CIMPLICITY 2023 © 1995-2023 General Electric Company – All Rights Reserved. *GE Digital, the GE Monogram are trademarks of General Electric Company. All other trademarks are the property of their respective owners.

Before you begin

- You must install CIMPLICITY with a local Windows user account that has administrator rights. See your Windows documentation for details about creating this type of account.
- If you decide to install CIMPLICITY using the standalone installer, you must install Historian using Historian's install media.
- If you will be using a supported Historian version that is already installed, do not uninstall it.

> **Note:**
> Ensure that your system is updated with the latest Microsoft updates.

CIMPLICITY Server Installation

If you are upgrading to CIMPLICITY 2022 or higher, you will be prompted to manually uninstall the previous version and re-initiate the installation process.

1. Mount the downloaded CIMPLICITY ISO media.
2. From the ISO folder, open the CIMPLICITY folder.
3. In the CIMPLICITY folder, double-click **InstallFrontEnd.exe**.

   The CIMPLICITY splash screen opens.
4. In the CIMPLICITY splash screen, click **Install CIMPLICITY Server**.
5. When the Welcome screen opens, click **Next**.
6. Accept the license agreement terms and click **Next**.
7. If you want to keep the default location for the CIMPLICITY server files, click Next or click **Change** to select a new destination and then click **Next**. If you are installing CIMPLICITY on a 32-bit system, the default destination is C:\Program Files\Proficy\Proficy CIMPLICITY and on a 64-bit system, the default destination is C:\Program Files (x86)\Proficy\ Proficy CIMPLICITY.
8. Enter the Web TCP ports for Web TCP configuration, and then click **Next**:
   - Web: Default is 9443
   - Config: Default is 4955

   > **Important:**
   > SQL Express, Historian, and A&E Archiver are installed separately. If you did not install SQL Express before installing CIMPLICITY, you must ensure the DNS configuration is mapped to connect with CIMPLICITY logging.
9. If the Windows Firewall is enabled, a pop-up message appears, asking if you want to integrate CIMPLICITY with the Windows Firewall. Do one of the following:
   - Click **Yes** to add applicable CIMPLICITY applications to the Windows Firewall exception list.
   - Click **No** if CIMPLICITY applications should not have off-node communications enabled.

     > **Note:**
     > If you click **No** but keep the Windows Firewall enabled, CIMPLICITY does not perform correctly. However, you can add applications to the exception list after the installation is finished. A complete list of CIMPLICITY exceptions is stored in the Proficy CIMPLICITY\Firewall directory.
10. Click **Next**.
11. Select one of the following Help options:

- **Online Help (Internet)**: To access the Help available online. All the help requests from the product are directed to the latest Online Help on GE website. The Online Help is always up-to-date with latest changes.
- **Remote Help Server (Intranet)**: To access the Help available on other CIMPLICITY server.
    - If you have selected the Remote Help option, enter the following details:
        - **Help Server Name**: Enter the name of the server that has CIMPLICITY Help installed.
        - **Port Number**: Enter the port number of the Server. Default is 9443.

        > **Note:**
        > You must change the port number only if you have explicitly changed the CIMPLICITY Web port on the remote server.

> **Note:**
> The default help option is Online Help. If you need to install the help locally (offline help) on your machine, select Online Help and proceed. Once the installation is complete, you can manually install the help locally by following the steps mentioned in Install local help *(on page 43)*.

12. Click **Install**.
13. Click **OK** to display the licensing message.
14. Click **OK** again to display the InstallShield Wizard Complete dialog.
15. Select a button to either restart the computer now or postpone the restart, then click **Finish**.

CIMPLICITY Server is ready to perform as soon as the restart is complete.

CIMPLICITY Viewer Installation

Ensure you are installing the viewer on a client machine. You cannot install the viewer on the computer hosting CIMPLICITY server.

1. Mount the downloaded CIMPLICITY ISO media.
2. From the ISO folder, open the CIMPLICITY folder.
3. In the CIMPLICITY folder, double-click **InstallFrontEnd.exe**.

    The CIMPLICITY splash screen opens.

4. In the CIMPLICITY splash screen, click **Install CIMPLICITY Viewer**.
5. When the Welcome screen opens, click **Next**.

6. Accept the license agreement terms and click **Next**.
7. If you want to keep the default location for the CIMPLICITY Runtime Viewer files, click Next or click **Change** to select a new destination and then click **Next**. If you are installing CIMPLICITY on a 32-bit system, the default destination is C:\Program Files\Proficy\ Proficy CIMPLICITY and on a 64-bit system, the default destination is C:\Program Files (x86)\Proficy\ Proficy CIMPLICITY.
8. If the Windows Firewall is enabled, a pop-up message appears, asking if you want to integrate CIMPLICITY with the Windows Firewall. Do one of the following:

    - Click **Yes** to add applicable CIMPLICITY applications to the Windows Firewall exception list.

    - Click **No** if CIMPLICITY applications should not have off-node communications enabled.

    > **Note:**
    > If you click **No** but keep the Windows Firewall enabled, CIMPLICITY does not perform correctly. However, you can add applications to the exception list after the installation is finished. A complete list of CIMPLICITY exceptions is stored in the Proficy CIMPLICITY\Firewall directory.

9. Select one of the following Help options:
    - **Online Help (Internet)**: To access the Help available online. All the help requests from the product are directed to the latest Online Help on GE website. The Online Help is always up-to-date with latest changes.
    - **Remote Help Server (Intranet)**: To access the Help available on other CIMPLICITY server.
        - If you have selected the Remote Help option, enter the following details:
            - **Help Server Name**: Enter the name of the server that has CIMPLICITY Help installed.
            - **Port Number**: Enter the port number of the Server. Default is 9443.**Note:**You must change the port number only if you have explicitly changed the CIMPLICITY Web port on the remote server.

    > **Note:**
    > The default help option is Online Help. If you need to install the help locally (offline help) on your machine, select Online Help and proceed. Once the installation is complete, you can manually install the help locally by following the steps mentioned in Install local help *(on page 43)*.

10. Click **Install**.
11. Click **OK** to display the licensing message.

12. Click **OK** again to display the InstallShield Wizard Complete dialog.
13. Select a button to either restart the computer now or postpone the restart, then click **Finish**.

CIMPLICITY Installation using Command Line

Running the Integrated Install from a Command Line

CIMPLICITY installations may be performed without requiring any user input. This mode of installation is called Quiet Mode or Silent Mode. You can use this option to run the integrated installer from a command line or programmatically. This can be helpful, for instance, if you have several computers on your network that you need to run the installer on. This topic describes the steps required to setup a Quiet Mode installation of CIMPLICITY. When you run the integrated installer, a **SilentInstallResponse.json** file is created with information about the package, components, and settings that you selected and saved at **[Install location]\Proficy**. You can run the file using a command line and install CIMPLICITY.

1. Before you begin, in the **SilentInstallResponseFile.json** file, in the client secret and password fields, ensure to replace ****** with the actual secret and password.
2. To run the integrated installer from a command prompt, use the following command:

   ```
   [Install media location]\Setup\setup.exe --response SilentInstallResponseFile.json
   ```

   The installation will begin.

   You can further customize CIMPLICITY installation options in addition to the options provided in the **SilentInstallResponseFile.json** file. For more information, see the Customize Options to Run the Integrated Install from a Command Line *(on page 27)* section.
3. Reboot your system after silent installation to successfully register the components.

   Sample of the SilentInstallResponseFile.json file for different components

   Common Components

   ```
   {
     "packageSelected": "CommonComponents",
     "installLocation": "C:\\Program Files (x86)\\Proficy",
     "configHubClientId": "ADMIN",
     "configHubClientSecret": "*******",
     "uaaClientId": "ADMIN",
     "uaaClientSecret": "*******",
     "selectedPackageProducts": [
       {
         "productName": "Configuration Hub",
         "installType": "installText"
   ```

```
    },
    {
      "productName": "Proficy Authentication",
      "installType": "installText"
    }
  ]
}
```

SCADA Client

```
{
  "packageSelected": "ScadaClient",
  "installLocation": "C:\\Program Files (x86)\\Proficy",
  "selectedPackageProducts": [
    {
      "productName": "SCADA Viewer",
      "installType": "installText"
    },
    {
      "productName": "Historian Client Tools",
      "installType": "installText"
    }
  ],
  "historianServerLocation": "HISTORIANSERVERNAME"
}
```

SCADA Standalone Server

```
{
  "packageSelected": "ScadaStandAloneServer",
  "installLocation": "C:\\Program Files (x86)\\Proficy",
  "selectedPackageProducts": [
    {
      "productName": "SCADA",
      "installType": "installText"
    },
    {
      "productName": "Historian Client Tools",
      "installType": "installText"
    },
    {
      "productName": "Historian Server",
      "installType": "installText"
    },
    {
      "productName": "Historian Collectors",
      "installType": "installText"
    }
  ],
  "dataPathFolder": "C:\\Proficy Historian Data",
  "enableCertificateSecurity": false,
  "serverCertPassPhrase": ""
}
```

SCADA with Remote Historian

```
{
  "packageSelected": "ScadaWithRemoteHistorian",
  "installLocation": "C:\\Program Files (x86)\\Proficy",
  "selectedPackageProducts": [
    {
      "productName": "SCADA",
      "installType": "installText"
    },
    {
      "productName": "Historian Client Tools",
      "installType": "installText"
    },
    {
      "productName": "Historian Collectors",
      "installType": "installText"
    }
  ],
  "dataPathFolder": "C:\\Proficy Historian Data",
  "historianServerLocation": "HISTORIANSERVERNAME",
  "historianUserName": "ADMINISTRATOR",
  "historianPassword": "******"
}
```

SCADA with Tracker

```
{
  "packageSelected": "ScadaMES",
  "installLocation": "C:\\Program Files (x86)\\Proficy",
  "selectedPackageProducts": [
    {
      "productName": "SCADA",
      "installType": "installText"
    },
    {
      "productName": "Tracker",
      "installType": "installText"
    },
    {
      "productName": "Historian Client Tools",
      "installType": "installText"
    },
    {
      "productName": "Historian Server",
      "installType": "installText"
    },
    {
      "productName": "Historian Collectors",
      "installType": "installText"
    }
  ],
  "dataPathFolder": "C:\\Proficy Historian Data",
  "enableCertificateSecurity": false,
  "serverCertPassPhrase": ""
}
```

Historian Server

```
{
"packageSelected": "HistorianServer",
"installLocation": "C:\\Program Files (x86)\\Proficy",
"selectedPackageProducts": [
{
```

```
"productName": "Historian Server",
"installType": "installText"
}
],
"dataPathFolder": "C:\\Proficy Historian Data",
"enableCertificateSecurity": false,
"serverCertPassPhrase": ""
}
```

Operations Hub

```
{
"packageSelected": "productOpsHub",
"installLocation": "C:\\Program Files (x86)\\Proficy",
"opshubusername": "ch_admin",
"opshubpassword": "******",
"ophub": {
"useLocalUaa": false,
"uaaBaseUrl": https://server/uaa,
"adminClientId": "admin",
"adminClientSecret": "******",
"configHubRegClientId": "admin",
"configHubRegClientSecret": "******",
"deferConfigHubRegistration": true
},
"opshubdrivelocation": "C:",
"selectedPackageProducts": [
{
"productName": "Operations Hub",
"installType": "installText",
"opshubinstalltype": "Silent Install"
}
]
}
```

Customize Options for Integrated Install from a Command Line

You can further customize the options for CIMPLICITY install in addition to the options provided in the **SilentInstallResponseFile.json** file. To customize the options for installation, you can use the **quiet.ini-**

template file available at the locations mentioned below. This file is updated with all the configurations that are saved in the **SilentInstallResponseFile.json** file that was run to install CIMPLICITY.

- Server- **[Instal media location]\CIMPLICITY\ServerSetup**
- Viewer- **[Install media location]\CIMPLICITY\ViewerSetup**
- Tracker- **[Install media location]\CIMPLICITY\Tracker**
- CNC- **[Install media location]\CIMPLICITY\Setup\CNC**
- AlarmCast- **[Install media location]\CIMPLICITY\Setup\AlarmCast**
- help- **[Install media location]\CIMPLICITY\Setup\help**

To customize the options for CIMPLICITY install,

1. In Windows Explorer, create a folder on your local drive named isoimage. For example: C:\isoimage.
2. Copy all of the files and folders from the integrated installer, and paste them to your isoimage folder.
3. Navigate to the folder as needed to locate the **quiet.ini-template** file. For example, **C:\isoimage\CIMPLICITY\ServerSetup**.
4. Customize the options as needed, and save the file as **quiet.ini-template**.
5. You can run the integrated install *(on page 23)* from a command line.
6. Reboot your system after silent installation to successfully register the components.

Sample of the options within the quiet.ini-template file

Server

```
[Config]

QuietMode=1

InstallDir=${installLocation}\Proficy CIMPLICITY\

InstallType=COMPLETE

StopClusterOnUpgrade=TRUE

ContinueAfterStopClusterFail=TRUE

ClusterStartRetries=3

AutostartService_0=1

FirewallIntegration=TRUE

WebConfigPort=${webServerPort}

CimConfigServicePort=${cimConfigPort}

HelpMode=3
```

```
ComputerAdminUser=Nothing
ComputerAdminPassword=Nothing
```

Viewer

```
[Config]
QuietMode=1
InstallDir=${installLocation}\Proficy CIMPLICITY\
InstallType=COMPLETE
OverwriteExisting=1
StopClusterOnUpgrade=TRUE
ContinueAfterStopClusterFail=TRUE
ClusterStartRetries=3
FirewallIntegration=TRUE
```

Tracker

```
[Config]
QuietMode=1
InstallDir=${installLocation}\Proficy CIMPLICITY\
InstallType=COMPLETE
OverwriteExisting=1
StopClusterOnUpgrade=TRUE
ContinueAfterStopClusterFail=TRUE
ClusterStartRetries=3
FirewallIntegration=TRUE
```

CNC

```
[Config]
QuietMode=1
InstallDir=${installLocation}\Proficy CIMPLICITY\
InstallType=COMPLETE
OverwriteExisting=1
StopClusterOnUpgrade=TRUE
ContinueAfterStopClusterFail=TRUE
ClusterStartRetries=3
```

AlarmCast

```
[Config]
QuietMode=1
InstallDir=${installLocation}\Proficy CIMPLICITY\
InstallType=COMPLETE
OverwriteExisting=1
StopClusterOnUpgrade=TRUE
ContinueAfterStopClusterFail=TRUE
ClusterStartRetries=3
FirewallIntegration=TRUE
```

Help

```
[Config]
QuietMode=1
InstallDir=%CIMPATH%\..\
```

Parameter	Description
QuietMode	• A value of 1 indicates that the install should proceed quietly (without user input). • A value of 0 indicates user input (a standard install).
InstallDir	This is the directory in which CIMPLICITY will be installed. If the command- line parameter **/target-dir="C:\Some Folder\"** is used, this parameter will be ignored.
InstallType	InstallType=COMPLETE indicates complete installation.
OverwriteExisting	If any CIMPLICITY component already exists in the machine, this parameter determines if the installation must continue or abort. • 0- this is the default value. The installation will be aborted. • 1- The installation will continue and the existing component will be overwritten.

Parameter	Description
StopClusterOnUpgrade	If installing on a cluster, this is the same as the “Stop Cluster Service” dialog in setup. A value of FALSE will abort the install if it is a cluster.
ContinueAfterStopClusterFail	If we are unable to stop the cluster service, this determines if we continue the install. A value of FALSE will abort, TRUE will continue.
ClusterStartRetries	The number of tries to be attempted to start the cluster service after install.
AutostartService_0	Do we auto-start the services that would normally be listed in a dialog near the end of the installation interview. They are numbered sequentially in the same order as they would appear in the dialog. • A value of 1 indicates that the service should be auto-started, • A value of 0 indicates that the service should not be auto-started .
FirewallIntegration	To integrate CIMPLICITY with the firewall: • A value of TRUE will trigger firewall integration. • A value of FALSE will not trigger firewall integration.
WebConfigPort	The port of Web configuration. Default is 9443.
CimConfigServicePort	The CIMPLICITY Configuration Service Port. Default is 4955.
HelpMode	The type of Help you want to configure with CIMPLICITY: • 0= Remote Help (To access Help installed in another server). • 1= Local Help (To install local Help and use it with CIMPLICITY).

Parameter	Description
	- 3= Online Help (To access Online Help available on internet). This the default Help option. If the parameter is not specified the Online Help is integrated with the product. **Note:** HelpMode=1 is not a valid option for a viewer.
HelpServerName	Host Name or IP Address of the server that has help installed. This parameter is required only if you selected Remote Help (HelpMode=0). **Note:** This value defaults to **localhost** if it is not specified in `quiet.ini`. It is useful to specify help server name if helpfiles feature is not included as part of installation using the **InstallFeatures** parameter.
HelpServerPort	Port of the Help Server. Default is 9443.
ComputerAdminUser	User name of the computer admin who can to create a new project user or enable the project for web configuration using the following REST APIs: - /user-config - /rest-settings
ComputerAdminPassword	Password for the computer admin.

Running the Standalone Install from a Command Line

CIMPLICITY installations may be performed without requiring any user input. This mode of installation is called Quiet Mode or Silent Mode.

If you installed CIMPLICITY Server and Viewer using the standalone installer, you can use the below method to do a silent install:

1. Create a `quiet.ini`quiet.ini file specifying the install options to be used.
2. Add the `quiet.ini` file to the folder given below based on the component you are about to install, and then run the corresponding .exe file in the command prompt.

Component	Folder	Executable
Server	`ServerSetup`	`ServerSetup.exe`
Viewer	`ViewerSetup`	`ViewerSetup.exe`
Tracker	`Tracker`	`TrackerSetup.exe`
Help	`Setup\help`	`Setup.bat`

> **Note:**
> If you add the `quiet.ini` file to a different location, you must specify the location in the command prompt: `ServerSetup\ServerSetup.exe /quietinifile="<File Location>\quiet.ini"`
>
> In the case of CIMPLICITY Help standalone installer, you must perform the following, before you run the **Setup.bat** file:
>
> a. From **[Install media location]\CIMPLICITY\Setup\**, copy the **help** folder to the location as needed.
> b. In the **help** folder, open the **Setup.bat** file with any text editor.
> c. Replace the `helpinstaller.exe /srcdir="%TEMP%\cimplicity-help\Help"` line with `helpinstaller.exe /srcdir="%TEMP%\cimplicity-help\Help" /quietinifile="<File Location>\help-quiet.ini"`.
> d. Save the **Setup.bat** file.

   You can also customize the CIMPLICITY install options in the quiet.ini file before you run the silent installation. For more information, see the Customize Options for Standalone Install from a Command Line *(on page 35)* section.

3. Reboot your system after silent installation to successfully register the components.

   Sample of the quite.ini file for different components

   Server

```
[Config]

QuietMode=1

InstallDir=${installLocation}\Proficy CIMPLICITY\
InstallType=COMPLETE
StopClusterOnUpgrade=TRUE
ContinueAfterStopClusterFail=TRUE
ClusterStartRetries=3
AutostartService_0=1
FirewallIntegration=TRUE
WebConfigPort=${webServerPort}
CimConfigServicePort=${cimConfigPort}
HelpMode=3
ComputerAdminUser=Nothing
ComputerAdminPassword=Nothing
```

Viewer

```
[Config]
QuietMode=1
InstallDir=${installLocation}\Proficy CIMPLICITY\
InstallType=COMPLETE
OverwriteExisting=1
StopClusterOnUpgrade=TRUE
ContinueAfterStopClusterFail=TRUE
ClusterStartRetries=3
FirewallIntegration=TRUE
```

Tracker

```
[Config]
QuietMode=1
InstallDir=${installLocation}\Proficy CIMPLICITY\
InstallType=COMPLETE
OverwriteExisting=1
StopClusterOnUpgrade=TRUE
ContinueAfterStopClusterFail=TRUE
ClusterStartRetries=3
FirewallIntegration=TRUE
```

CNC

```
[Config]
QuietMode=1
InstallDir=${installLocation}\Proficy CIMPLICITY\
InstallType=COMPLETE
OverwriteExisting=1
StopClusterOnUpgrade=TRUE
ContinueAfterStopClusterFail=TRUE
ClusterStartRetries=3
```

AlarmCast

```
[Config]
QuietMode=1
InstallDir=${installLocation}\Proficy CIMPLICITY\
InstallType=COMPLETE
OverwriteExisting=1
StopClusterOnUpgrade=TRUE
ContinueAfterStopClusterFail=TRUE
ClusterStartRetries=3
FirewallIntegration=TRUE
```

Help

```
[Config]
QuietMode=1
InstallDir=%CIMPATH%\..\
```

Customize Options for Standalone Install from a Command Line

You can further customize the options for CIMPLICITY install in the **quiet.ini** file that you created *(on page 32)* for the corresponding components that you are about to install.

To customize the options for CIMPLICITY install,

1. Open the `quiet.ini` file for the component that you are about to install.
2. Edit the installation options as needed.
3. Save the file.

Sample of the options within the quiet.ini file

Server

```
[Config]
QuietMode=1
InstallDir=${installLocation}\Proficy CIMPLICITY\
InstallType=COMPLETE
StopClusterOnUpgrade=TRUE
ContinueAfterStopClusterFail=TRUE
ClusterStartRetries=3
AutostartService_0=1
FirewallIntegration=TRUE
WebConfigPort=${webServerPort}
CimConfigServicePort=${cimConfigPort}
HelpMode=3
ComputerAdminUser=Nothing
ComputerAdminPassword=Nothing
```

Viewer

```
[Config]
QuietMode=1
InstallDir=${installLocation}\Proficy CIMPLICITY\
InstallType=COMPLETE
OverwriteExisting=1
StopClusterOnUpgrade=TRUE
ContinueAfterStopClusterFail=TRUE
ClusterStartRetries=3
FirewallIntegration=TRUE
```

Tracker

```
[Config]
QuietMode=1
InstallDir=${installLocation}\Proficy CIMPLICITY\
InstallType=COMPLETE
OverwriteExisting=1
StopClusterOnUpgrade=TRUE
ContinueAfterStopClusterFail=TRUE
```

```
ClusterStartRetries=3

FirewallIntegration=TRUE
```

CNC

```
[Config]

QuietMode=1

InstallDir=${installLocation}\Proficy CIMPLICITY\

InstallType=COMPLETE

OverwriteExisting=1

StopClusterOnUpgrade=TRUE

ContinueAfterStopClusterFail=TRUE

ClusterStartRetries=3
```

AlarmCast

```
[Config]

QuietMode=1

InstallDir=${installLocation}\Proficy CIMPLICITY\

InstallType=COMPLETE

OverwriteExisting=1

StopClusterOnUpgrade=TRUE

ContinueAfterStopClusterFail=TRUE

ClusterStartRetries=3

FirewallIntegration=TRUE
```

Help

```
[Config]

QuietMode=1

InstallDir=%CIMPATH%\..\
```

Parameter	Description
QuietMode	• A value of 1 indicates that the install should proceed quietly (without user input). • A value of 0 indicates user input (a standard install).
InstallDir	This is the directory in which CIMPLICITY will be installed. If the command- line parameter **/targetdir="C:\Some Folder\"** is used, this parameter will be ignored.

Parameter	Description
InstallType	InstallType=COMPLETE indicates complete installation.
OverwriteExisting	If any CIMPLICITY component already exists in the machine, this parameter determines if the installation must continue or abort. • 0- this is the default value. The installation will be aborted. • 1- The installation will continue and the existing component will be overwritten.
StopClusterOnUpgrade	If installing on a cluster, this is the same as the “Stop Cluster Service” dialog in setup. A value of FALSE will abort the install if it is a cluster.
ContinueAfterStopClusterFail	If we are unable to stop the cluster service, this determines if we continue the install. A value of FALSE will abort, TRUE will continue.
ClusterStartRetries	The number of tries to be attempted to start the cluster service after install.
AutostartService_0	Do we auto-start the services that would normally be listed in a dialog near the end of the installation interview. They are numbered sequentially in the same order as they would appear in the dialog. • A value of 1 indicates that the service should be auto-started, • A value of 0 indicates that the service should not be auto-started .
FirewallIntegration	To integrate CIMPLICITY with the firewall: • A value of TRUE will trigger firewall integration. • A value of FALSE will not trigger firewall integration.
WebConfigPort	The port of Web configuration. Default is 9443.
CimConfigServicePort	The CIMPLICITY Configuration Service Port. Default is 4955.
HelpMode	The type of Help you want to configure with CIMPLICITY: • 0= Remote Help (To access Help installed in another server). • 1= Local Help (To install local Help and use it with CIMPLICITY). • 3= Online Help (To access Online Help available on internet). This the default Help option. If the parameter is not specified the Online Help is integrated with the product.

Parameter	Description
	Note: HelpMode=1 is not a valid option for a viewer.
HelpServerName	Host Name or IP Address of the server that has help installed. This parameter is required only if you selected Remote Help (HelpMode=0). **Note:** This value defaults to **localhost** if it is not specified in `quiet.ini`. It is useful to specify help server name if helpfiles feature is not included as part of installation using the **InstallFeatures** parameter.
HelpServerPort	Port of the Help Server. Default is 9443.
ComputerAdminUser	User name of the computer admin who can to create a new project user or enable the project for web configuration using the following REST APIs: • /user-config • /rest-settings
ComputerAdminPassword	Password for the computer admin.

CIMPLICITY Program File Components

The following CIMPLICITY components are installed with the CIMPLICITY program files. Licensed features will be enabled when installation is complete. You can enable other features at any time by simply obtaining the appropriate license.

Important:
Components that are identified as:

Legacy	Accommodate clients who are still using them from previously configured CIMPLICITY versions. This will give you time to upgrade your systems.
As-Is	Are not actively being developed or supported.

These features support equipment that is obsolete or functionality that has been superseded by far more effective and efficient functionality. Therefore, these features will not be available in the next major CIMPLICITY release after version 10.

Server/Viewer Development components

Component/Option	Description
HMI Server Base	The Proficy CIMPLICITY Server for supported operating systems provides configuration and runtime support for graphic monitoring (CimEdit/CimView) and control, alarm management and Viewer support (Alarm Viewer/Historical Alarm Viewer).
ApplicationOptions	Proficy CIMPLICITY Application Options supplement the base functionality of the Proficy CIMPLICITY Server and Viewer products.
Action Calendar	Allows calendar based scheduling of set points.
A&E OPC Server	Allows you to provide alarm information to OPC clients through COM and DCOM.
Change Management	Enables users who also have a licensed Change Management product can now manage CIMPLICITY project configuration revisions. Change Management functionality includes: • Check-in • Check-out • History • Roll-back capabilities
Change Approval	Requires valid users to electronically sign a setpoint action for selected points.
Document Delivery	Provides the ability to send files to remote locations using mapped network drives, FTP and HTTP.
Dynamic Graphic Replay	Provides dynamic replay of Historian or SQL historical point data through CimView. Note: Dynamic Graphic Replay (DGR) replaces VCR.
Marquee Driver	Controls Marquee display devices on COM ports.

Component/Option	Description
OPC Server	Allows you to provide point management information to OPC clients through COM and DCOM.
Alarm Cast	Allows a user to send alarm messages to alphanumeric Pagers, SMS, and SMTP Servers.
Recipes	Allows the user to • (Server only) configure recipe groups. • (Server and Viewer) Upload/download recipes.
Screen Navigation	Allows you to create buttons and menus that aid a user to navigate through your system's CimView screens and global scripts.
Server Redundancy	Provides server level redundancy for Proficy CIMPLICITY applications.
SPC Charts	(Statistical process control) allows users to collect quality data and make control charts.
System Sentry	Allows you to monitor the functioning of your computer.
Alarm Management	Allows a user to integrate custom software to Proficy CIMPLICITY by generating and clearing Proficy CIMPLICITY alarms.
Devcom Toolkit	Allows a user to create a communication module to third party hardware not directly supported by Proficy CIMPLICITY.
Point Management	Allows a user to integrate custom software to Proficy CIMPLICITY by passing real time point data between the applications.
Communications	Options allow Proficy CIMPLICITY Servers to gather data from, or send data to, controller devices, as follows.
CCM2	Series 6, Series 5 and Series 90 Model 90-70 and 90-30 PLC's.
S90 Triplex	TCP/IP communications to redundant and non-redundant Model 90-70, Model 90-30, Rx3i, and Rx7i PLCs.
SNP	Series 90 PLC's.
SNPX	Series 90 PLC's.
AB Ethernet	Utilizes Rockwell's RSLinx software to communicate to Allen-Bradley PLC's over Ethernet.
Allen Bradley RFID	Allen Bradley Intelligent Antennas

Component/Option	Description
Allen Bradley DF-1	Serial communications protocol to Allen-Bradley device communications.
DDE Client	(As-Is-Local only) DDE communications to DDE server.
FloPro/FloNet Ethernet	FloPro via Ethernet.
Genius PCI	Genius PCI communications via a supported PCIM card.
Honeywell IPC 620	Honeywell IPC 620 PLC's.
Mitsubishi Serial	Mitsubishi A Series Serial communications.
Mitsubishi TCP/IP	Melsec PLC via Ethernet.
Modbus RTU	Modicon PLC's.
Modbus TCP/IP	Modicon PLC's.
N2 Serial	(Johnson Controls N2) to Johnson Controls Unitary and DX9100 Controllers.
Omron Host Link	Omron Host Link.
OMRON TCP/IP	(Omron Ethernet) TCO/IP communications to OMRON PLC's.
OPC Client	COM and DCOM communications to an OPC server.
Reflective Memory	(As-is) Reflective Memory communications via a supported Reflective Memory card.
Sharp TCP/IP	Sharp PLC via Ethernet.
Smarteye	SMARTEYe Readers via SMARTEYE Electronic Assemblies.
Square D	SYMAX PLC's.
TI Serial	Texas Instruments PLC's.
TOYOPUC TCP/IP	Toyota Machine Work's Toyopuc PC2 Series programmable controllers via Ethernet.
SystemUtilities	System utilities for Proficy CIMPLICITY Server and viewer products.
Login Panel	Displays the current project the local node connects to. It shows whether the projects are logged in or logged out.
Process Control	Provides control of programs running on a Proficy CIMPLICITY system.
Show Users	Displays the current users of a Proficy CIMPLICITY system.

Viewer Runtime Components

Components/Options	Description
Viewer	Configuration and runtime support for graphic monitoring and control. Information is received from a Proficy CIMPLICITY Server.
Advanced Viewer	Viewers can report point values straight from a PLC. A CIMPLICITY project does not have to be running.
ApplicationOptions	Supplement the base functionality of the Proficy CIMPLICITY Server and Viewer products.
Dynamic Graphic Replay (DGR)	Provides dynamic replay of Historian or SQL historical point data through CimView. Note: Dynamic Graphic Replay (DGR) replaces VCR
Help Files	Detailed CIMPLICITY documentation.
Recipes	Allows the user to upload/download recipes.
Server Redundancy Support	Provides Viewer support for Server level redundancy for Proficy CIMPLICITY applications.
SPC Charts	(Statistical Process Control option) allows users to collect quality data and make control charts.
TrackerDisplay	Provides factory tracker/routing interfaces.
OrderExec. Mgt. Display	Provides factory tracking/routing interfaces.
SystemUtilities	System utilities for Proficy CIMPLICITY server and viewer products.
Process Control	Provides control of programs running on a Proficy CIMPLICITY system.
Show Users	Displays the current users of a Proficy CIMPLICITY system.
Login Panel	Displays the current projects that the node is logged into.
CablingRedundancy	Provides network cabling redundancy to a Proficy CIMPLICITY server.

Install Local Help

When you install CIMPLICITY using the integrated installer, by default, the online help mode is selected and pointed to the online help on the GE documentation server. However, if you want to install the help locally, you can do it. It is recommended to use the online help, as it is always updated with the latest changes.

To install the help locally,

1. Open Windows PowerShell as an administrator.

   The Windows PowerShell prompt appears.
2. In the PowerShell prompt, navigate to **[Install media location]\CIMPLICITY\Setup\help**.

   For example, if the install media is in the D:\ drive, you can enter **cd D:\CIMPLICITY\Setup\help**.
3. Execute the **Setup.bat** file by entering the **.\Setup.bat** command.

   The help installation begins.
4. After the installation completes, reboot your system to successfully register your component.
5. After rebooting, change the help option to **Local Help**. For more information, see Configure Help *(on page)* section available in Project Setup.

Chapter 2. CIMPLICITY Post-Installation Tasks

After you install CIMPLICITY, you must reset your global configuration:

1. Locate the configured CimView.cfg file that you saved before you began the installation.
2. Copy the file to the `..\<CIMPLICITY Installation>\Data directory`.

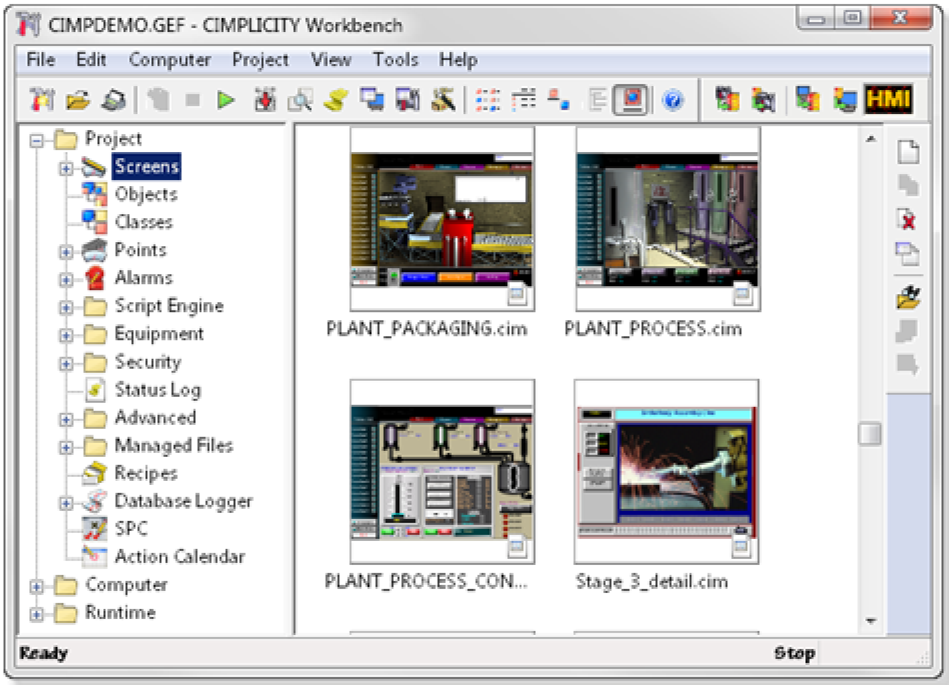
Any global specifications that were configured in the CimEdit Global Configuration dialog box (such as Navigation, script selections, compatibility, and so forth.) are applied to CIMPLICITY v2023 global specifications.

If you did not save the file, global specifications are represented by default values. You can use the global dialog boxes to redo the configuration. See CimEdit Global Specifications.

Chapter 3. HMI/SCADA CIMPLICITY Introduction

About HMI/SCADA CIMPLICITY

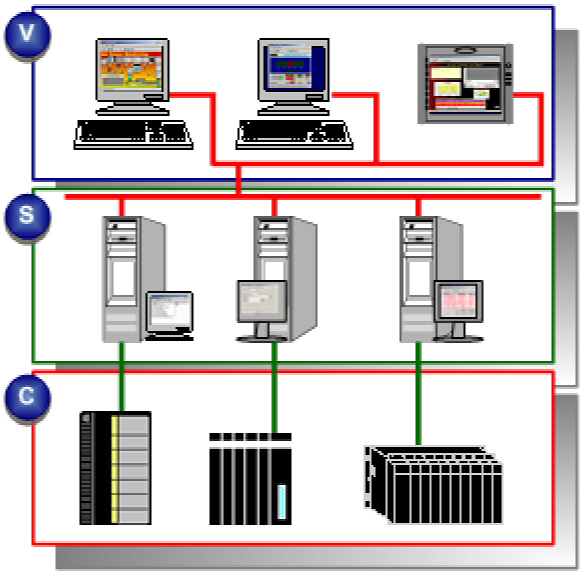
This section contains information on customer and technical support, the basic CIMPLICITY architecture, a tutorial describing CIMPLICITY applications, and some information on optimal usage of the CIMPLICITY online help system.



System Architecture Overview

System Architecture Overview

CIMPLICITY software is scalable from a Human Machine Interface to a fully networked Supervisory Control and Data Acquisition (SCADA) system. The networking capabilities inherent at all levels within the product line let you achieve levels of integration that virtually eliminate redundant configuration within a network.



1. #unique_14_Connect_42_V *(on page 47)*
2. #unique_14_Connect_42_S *(on page 47)*
3. #unique_14_Connect_42_C *(on page 47)*

V	Viewer	Connects to Server
		Status monitoring and control
		Viewer options available
		Development configuration
		Graphics configuration
S	Server	Connects to Viewer
		Status monitoring and control
		Development configuration
		Graphics configuration
		Data collection
		Server options available
C	Industrial controllers	N/A

CIMPLICITY is based on a client–server architecture consisting of Servers and Viewers. Servers are responsible for the collection and distribution of data. Viewers connect into Servers and have full access to the collected data for viewing and control actions.

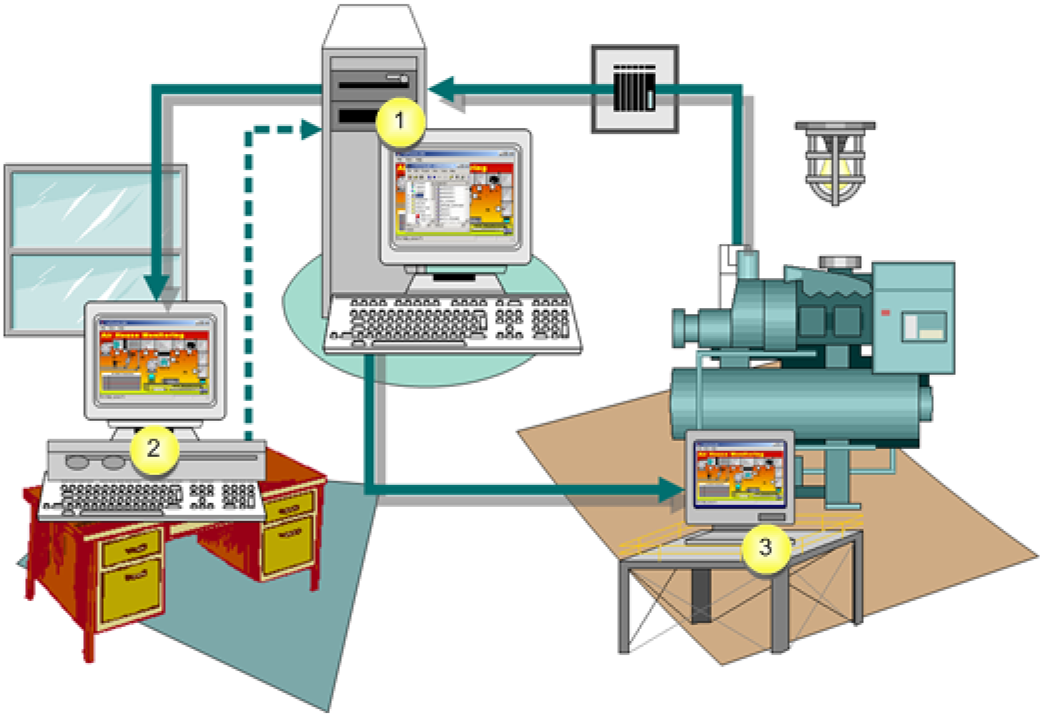
Servers and Viewers can be easily networked together to seamlessly share data without the need to replicate your point database from node to node. For example, points are configured once and only once on a server. Screens can be developed and stored in a single location on the network and accessed by any other CIMPLICITY display on the network.

CIMPLICITY provides the flexibility to build a larger system through multiple smaller nodes without forcing you to purchase large and expensive server hardware to service multiple users.

CIMPLICITY Server and Viewer Defined

HMI/SCADA CIMPLICITY provides the following three options. The server or viewer's license determines which option it will use.

Options are:



1	CIMPLICITY Server	Receives data from the PLC.
		Stores data.
		Provides CIMPLICITY configuration tools.
		Performs calculations.
		Displays data through Viewers

		Displays data
2	Viewer	Enables configuration on the server from a separate computer.
		Displays data from the server.
		Displays data from the server.
3	Web Client	N/A

You have to install at least one CIMPLICITY server. The total number of servers and viewers you can install depends on your licensing agreement.

Tip:
CIMPLICITY also provides numerous options *(on page 56)* for remotely interacting with your CIMPLICITY projects.

Contact your sales representative with questions about purchase options.

Chapter 4. CIMPLICITY Applications Tour

CIMPLICITY Applications Tour

CIMPLICITY provides an extraordinary selection of features that enable you to configure comprehensive and robust projects.

Once you have installed CIMPLICITY this quick tour will guide you through the order for configuring a basic project.

This tour provides links to the related subject in the documentation. Once you think you understand the basic concepts about the subject, you can come back to the tour at any time.

The tour is divided into five parts that provide links to documentation that describes:

CIMPLICITY APPLICATIONS TOUR	
Part 1 *(on page 50)*	How to set up the foundation for your system goals.
Part 2 *(on page 51)*	How to set up points and alarms.
Part 3 *(on page 52)*	How to create powerful applications that can graphically deal with system data for whoever has access privileges.
Part 4 *(on page 54)*	Many other powerful tools.
Part 5 *(on page 56)*	CIMPLICITY options.

Part 1. CIMPLICITY Tour

Part 1 of the CIMPLICITY tour provides links to documentation that describes how to set up the foundation for your system goals.

Part 1 of CIMPLICITY Tour	
Step 1.	Open the CIMPLICITY Workbench. The Workbench is at the center of your CIMPLICITY project.

Part 1 of CIMPLICITY Tour	
Step 2.	Create a new project. A project contains the configuration that defines what CIMPLICITY will do for your system and how it will work.
Step 3.	Look over the Workbench. The Workbench provides the power you need to view, configure, organize, and manage every component of your project through one easy to use window.
Step 4.	Configure a device including: • A port, which is a communication socket, connects one or more factory devices such as PLC's to the computer • A device is anything that can communicate point data to CIMPLICITY software. CIMPLICITY software can read data from and write data to devices. Examples of devices are programmable controllers such as the Series 90. The *Quick Device Setup* in the documentation gives you quick start for both.
Step 5.	Define security and routing including: • Resources are the physical or conceptual units that comprise your facility. • A user is an individual person working with a CIMPLICITY project. • A role specifies what privileges its users have when they work in CIMPLICITY.

Part 2. CIMPLICITY Tour

Part 2 of the CIMPLICITY tour provides links to documentation that describes how to set up points and alarms.

Note:
CIMPLICITY collects or calculates point data that it distributes to:

- CimView screens
- Alarm Viewer screens
- Alarm printers
- Logging tables
- Other CIMPLICITY software options

The collection and distribution of point data is handled by the Point Management subsystem.

Part 2 of CIMPLICITY Tour	
Step 6.	Create points including: • A device point communicates back and forth with a device that is attached to the server for monitoring and control purposes. • A virtual point provides you with the ability to calculate and report data that is independent of any one device.
Step 7.	Configure alarms. • Point alarms alert users when points are in a defined alarm states. You create and modify point alarms in the Point Properties dialog box or the Alarm Definition dialog box through the Alarms folder. • System event alarms alert users for alarm states such as device failures, program terminations, system startups, and system shutdowns. You create and modify system event alarms in the Alarm Definition dialog box through the Alarms folder.
Step 8.	Test your configuration in the Point Control Panel. • The Point Control Panel provides you with a forum in which you can easily review and change point values and status during runtime.

Part 3. CIMPLICITY Tour

Part 3 of the CIMPLICITY tour provides links to documentation that describes how to create powerful applications that graphically deal with system data for whoever has access privileges.

Part 3 of CIMPLICITY Tour	
Step 9.	• Configure a CimEdit screen.

Part 3 of CIMPLICITY Tour	
	• CimEdit combines the features commonly found in high-powered graphics applications, with an abundant number of state of the art configuration tools. They all help you take advantage of CIMPLICITY's extensive runtime capabilities. Consequently, you can create CimView screens that are clear, easy, and robust. • CimEdit Screens provide you with several diverse features and capabilities that you can use at any time during your screen design session. Some, but not all of the capabilities include: ◦ Preliminary Layout CimEdit offers you a wide assortment of objects and object types to place on your CimEdit screen. Consequently, you can place objects that deal with data from any source you specify and display the data or evaluation results in a manner that is most effective for your project's runtime requirements. ◦ Inanimate Visual Features enable you to modify the appearance of an object. They range from modifying its size so it will fit where you want it go, to displaying a several similar objects that represent similar but independent functions. ◦ Runtime movement and Animation provides several choices to create activity on your screens that makes it easy for a CimView user to quickly determine the status of a point or expression. ◦ Points report specific conditions in the system. Points are the result of detailed configuration, which is done in the Point Properties dialog box. As with other CIMPLICITY applications, when you are in CimEdit, you can find and use any point that is already in any broadcasting project on your network. In addition, you can create new points by opening the Point Properties dialog box through CimEdit. ◦ Variables can be used in an expression to represent different types of values ◦ Events trigger a procedure or call a script. CimEdit provides a long list of events from which you can choose the best one for your requirements.

Part 3 of CIMPLICITY Tour	
	◦ Procedures contain one or more actions that are triggered in the specified order when an event occurs and while the screen is displayed in CimView. CimEdit provides several actions from which a screen designer can easily compile a meaningful list.
Step 10.	Test your configuration through CimView. • CimView is a runtime, interactive graphical user interface through which you can monitor and control your facility. CimView displays screens that were created in CimEdit for specific applications.

Part 4. CIMPLICITY More Features

CIMPLICITY is so powerful that you will constantly discover new possible solutions as you continue to use it.

Part 4 provides links to documentation for CIMPLICITY's many other powerful tools. Which tools you use depend on your system needs. (Some of the tools are options that you can purchase through your CIMPLICITY representative.)

Feature	Description
Alarm Management	• Alarm Classes are groups of Alarms with similar characteristics. • Alarm Strings name alarm states. An alarm displays the string for its alarm state when **%State** is included in the alarm message. • The Stand-alone Alarm Viewer, AMV, is useful for a user to quickly monitor and responds to alarms anywhere in the system. • The Alarm Viewer Control is an ActiveX object that you embed in a CimEdit screen. The AMV Control provides a powerful tool for you to fully integrate the Alarm Viewer capability with your other CimEdit screens. • Database Logging provides you with a seamless way to analyze your system processes and equipment performance by logging data to and reporting data from a wide variety of ODBC (Open Database Connectivity)-compliant databases.

Feature	Description
	• Trend Control is an ActiveX Control that enables you to review, evaluate and log point values over time. • Historical Alarm Viewer Control is an ActiveX control through which you can easily review logged alarm data through CimView in an easy-to-read table format and print one or more pages of the display at any time during a session.
Basic Control Engine	The Basic Control Engine option consists of three main components: • Program Editor provides a set of sophisticated development tools that let you create programs with a Visual Basic compliant programming language. These programs can then be executed as actions in response to events. The programming language has a rich set of nearly 500 standard Basic functions, and also provides an object interface to CIMPLICITY points, alarms and the Status Logger, further enriching the language. • Event Editor enables you to define actions to take in response to events that occur in a process. An event can be defined as a changing point, alarm state, or even a particular time of day. One event may invoke multiple actions, or one action may be invoked by many events. • Basic Control Engine monitors for events and executes the configured actions. The Basic Control Engine is based on a multi-threaded design that allows the system to invoke and execute multiple Visual Basic programs concurrently. • Classes enable you to do the basic configuration once and use it over and over instead of repeating configuration, which may include creating complex CimEdit/CimView screens, for several objects that have similar requirements. • Class Objects provide an easy way to do complex configuration for one or more objects that are similar. Class objects, which are based on a Class template, can include pre-configured attributes, points, events, actions and scripts. • Dynamic Graphic Replay is a powerful tool to help you troubleshoot problems that have occurred in your processes.

Feature	Description
	• XY Plot provides you with the ability to visually represent values in relation to each other. For example, you can plot real data vs. calculated date, or elements such pressure vs. temperature. • Remote Projects need to be defined when a project starts, the Point Bridge or Point Data Logger need to get points from projects on other computers running CIMPLICITY projects. • Recipes enable you to create and manage recipe data for your production processes. The Recipes interface consists of a spreadsheet format in which you enter the configuration data for each of your recipes. This format allows you to group similar products together.
Object Model	Interfaces into components (e.g. objects, services, CimEdit screens both configuration and runtime, Project configuration Trend control, XY Plot control) that enable a developer to manipulate the components from a programming or scripting language, such as CIMPILICITY Basic, VB, C++, VBA, VBScript. • CIMPLICITY Configuration Object Model • CimEdit/CimView Object Model • CIMPLICITY XY Plot Object Model • CIMPLICITY Safe Array Object Model • CIMPLICITY Historical Data Connector Object Model

Part 5. CIMPLICITY Options

Option	Description
Options	• CIMPLICITY OPC Server provides a standards-based interface to some form of run-time data. The data may come from a specific physical device (e.g. a PLC) or from a Distributed Control System. The OPC Server conforms to the OLE for Process Control (OPC) 2.0 Data Access standards, a technology standard initially developed by a group of automation industry companies and now managed by the not-for-profit organization called the OPC Foundation.

Option	Description
	• Server Redundancy in automated systems, provides for switchover of functionality to a backup component in case of failure of a primary component. The switchover is considered automatic if no operator intervention is required. Redundancy applies to both hardware and software, and implies minimal loss of continuity during the transfer of control between primary (active) and redundant (backup) components. • Statistical Process Control enhances your ability to manage a quality control program by addressing the four major phases of quality control: measurement, analysis, improvement, control.
Tracker	There are two distinct, yet interrelated pieces to Tracker: Production Tracking (PRT) and Routing Control Objects (RCO). • Production Tracking module monitors the progress of items through the production process. • Routing Control Objects performs routing decisions for enhanced production flow.
Order Execution Management	Order Execution Management provides a comprehensive addition to Tracker that enables you to track, store, categorize and sequence your customers' orders based on your configured criteria. Order Execution Management includes: • XMLT tools take raw data orders, translates them into an .xml format and enters valid data into PRT and TADB. • Directory Watcher confirms that order files have completed downloading to XMLT output directory and moves files to the POMS input directory. • Product Order Management System (POMS) can be the hub of your Order Execution Management order management system. POMS is essentially a project that contains the basic configuration on which you can build your customized system. • CimView Order Entry provides order entry screens if you find that you have to manually edit an order item.

Option	Description
	• Tracker Attribute Database (TADB) stores comprehensive data about items, including orders and product components. • Range Source Architecture (RSA) enhances the traditional RCO concept of a Tracker source (source region). • Tracker Query Engine is a powerful high level query engine that has its own syntax for forming queries. It pulls data from both the Tracker Attribute Database and the Order Execution Management runtime memory map. Queries may be named and stored for future use, or for subdividing and abbreviating complicated queries. • Order Execution Management Broadcast is the delivery of a configurable list of product related information (including at least build options, location information, other/supporting data and subsets of the unit bill of material) to plant floor devices and to suppliers. • Alarm Cast messaging engine is a standardized interface between personal communication devices and applications sending messages through either an internal paging service and/or external service providers. • Marquee Manager product family monitors manufacturing environments and sends real time, automated messages to visual and/or audible devices.

Chapter 5. Common Licensing

About Common Licensing

Common Licensing simplifies administration and support while providing more secure license activation and management.

You can use Common Licensing to:

- View current licenses for GE products on your computer.
- Choose your licensing method: Internet, local intranet, GE USB Hardware Key, file-based.
- Manage your licenses: Activate, return, refresh, and clean.

Visit the GE Customer Center web site at https://digitalsupport.ge.com to obtain information about the latest GE product offerings.

Table 1. Common Licensing documentation links to view the latest updates:

Document	Link
Common Licensing Quickstart Guide (Online)	https://www.ge.com/digital/documentation/licensing/quickstart/g_licensing_-quick_start_overview.html
Common Licensing Help (Online)	https://www.ge.com/digital/documentation/licensing/index.html

The following Common Licensing software enable you to activate your GE product licenses:

1. License client
2. Local License Server (LLS)
3. License Server Tools

> **Note:**
> You do not have to install all the above software in your system. The software required to activate your licenses depend on whether you are using a physical machine or a virtual machine.

To configure Common Licensing on your computer (physical machine or virtual machine), you should go through the following:

Prerequisites *(on page)*| Step 1: Order Email and Downloads *(on page)*| Step 2: Common Licensing Software *(on page)*| | Step 3: Activating Licenses *(on page)*| Step 4: Returning Licenses *(on page)*

1
2
3
4
Order Email & Downloads
Common Licensing Software
Activating Licenses
Returning Licenses

Prerequisites

Use the following links to check the supported operating system requirements and virtual machines. Ensure you have enough disk space and memory.

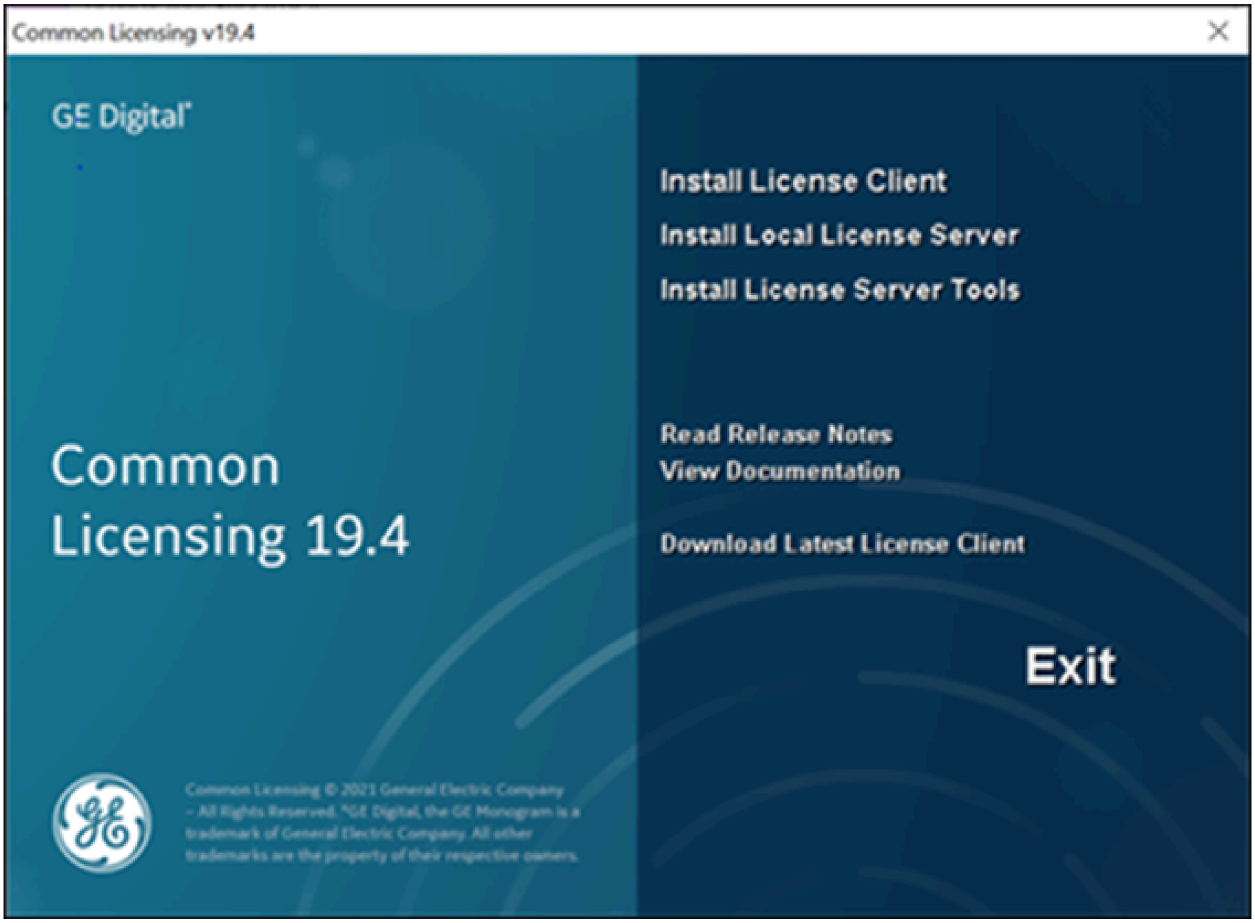
- #unique_24 *(on page)*
- System Requirements *(on page 63)*

1. Order Email and Downloads

You will receive an order e-mail from GE Digital after your successful purchase of GE products. Login to the website as specified in the order email using the same e-mail address. For more details, refer Step 1: Order Email and Downloads *(on page 64)*.

2. Common Licensing Software

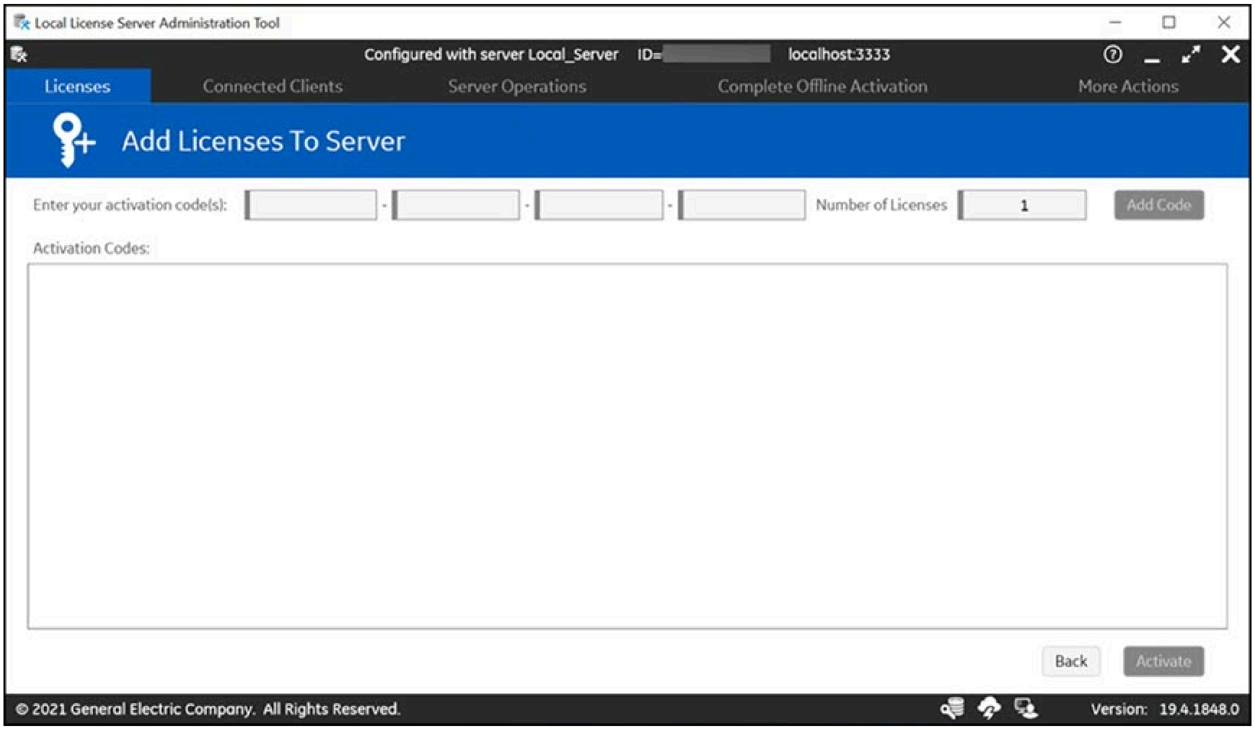
After you execute `CommonLicensing_<version>.exe`, you can install the software: 1) License Client, 2) Local License Server, and 3) License Server Tools



Common Licensing © 2021 General Electric Company – All Rights Reserved. *GE Digital, the GE Monogram is a trademark of General Electric Company. All other trademarks are the property of their respective owners.

You must run `CommonLicensing_<version>.exe` as an Administrator. After installing the licensing software, restart your computer.

Download your codes using the **Local License Server Administration Tool**. Run **License Client** to activate your GE Digital software product licenses. After you complete the installation steps, confirm that all the product licenses appear in License Client. For detailed steps, refer Step 2: Common Licensing Software *(on page 65)*

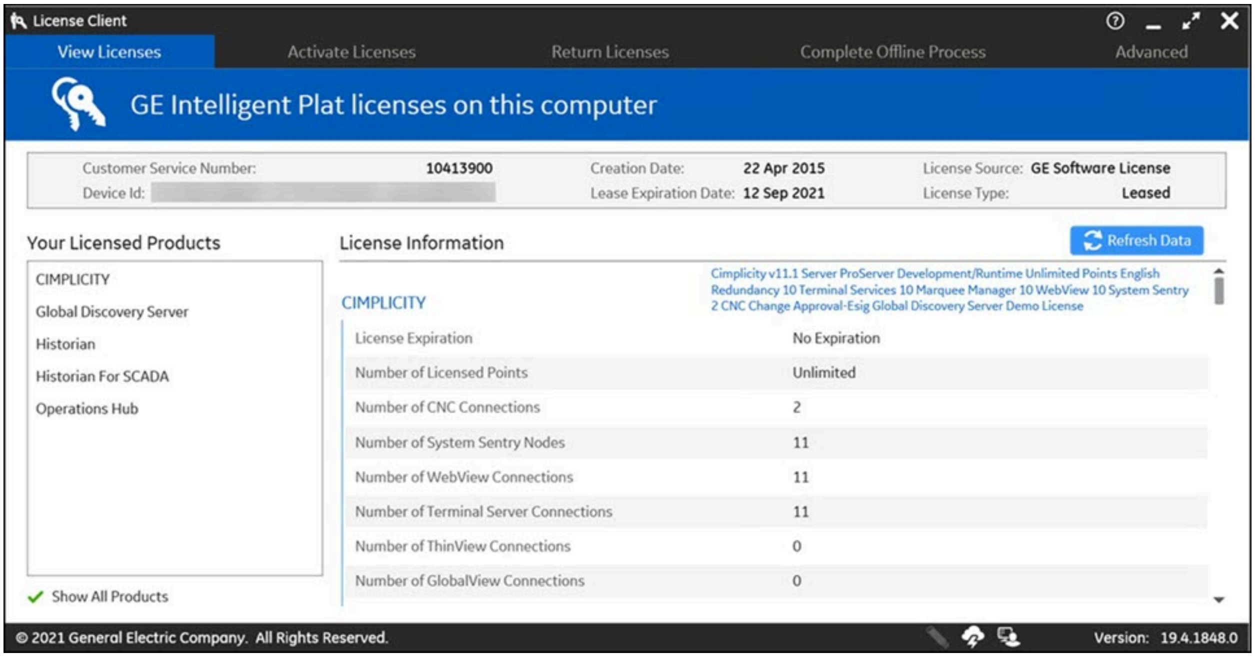

Local License Server Administration Tool
Configured with server Local_Server ID=[redacted] localhost:3333
Licenses
Connected Clients
Server Operations
Complete Offline Activation
More Actions
Add Licenses To Server
Add Code
Back
Activate

Enter your activation code(s): [ ] - [ ] - [ ] - [ ] Number of Licenses 1

Activation Codes:

© 2021 General Electric Company. All Rights Reserved.

Version: 19.4.1848.0



Customer Service Number: 10413900
Device Id: [redacted]
Creation Date: 22 Apr 2015
Lease Expiration Date: 12 Sep 2021
License Source: GE Software License
License Type: Leased

Your Licensed Products

- CIMPLICITY
- Global Discovery Server
- Historian
- Historian For SCADA
- Operations Hub

License Information

CIMPLICITY

Cimplicity v11.1 Server ProServer Development/Runtime Unlimited Points English Redundancy 10 Terminal Services 10 Marquee Manager 10 WebView 10 System Sentry 2 CNC Change Approval-Esig Global Discovery Server Demo License

License Expiration	No Expiration
Number of Licensed Points	Unlimited
Number of CNC Connections	2
Number of System Sentry Nodes	11
Number of WebView Connections	11
Number of Terminal Server Connections	11
Number of ThinView Connections	0
Number of GlobalView Connections	0

© 2021 General Electric Company. All Rights Reserved.

Version: 19.4.1848.0

3. Activating Licenses

In License Client, the **Activate Licenses** tab provides several options for activating a license on your computer. You can select one of the options based on your system configuration. For detailed steps, refer Step 3: Activating Licenses *(on page 72)*.

4. Returning Licenses

The Return Licenses tab is used to return licenses from your computer to the GE Cloud Server or a Local License Server. For detailed steps, refer Step 4: Returning Licenses *(on page 87)*.

System Requirements

The following are the system requirements for Common Licensing.

Supported Operating System

GE recommends using the latest service packs for Windows operating systems. The user should have the software that support Common Licensing installers:

You must have one of the following operating systems :

- Microsoft Windows 7 SP1
- Microsoft Windows 8.1
- Microsoft Windows 10
- Microsoft Windows Server 2019 Standard
- Microsoft Windows Server 2016 Standard
- Microsoft Windows Server 2012 Standard
- Microsoft Windows Server 2012 Standard R2
- Microsoft Windows Server 2008 Standard R2 SP1

Note:
Microsoft Windows 7 SP1, Microsoft Windows Server 2008 R2 SP1, and Microsoft Windows Server 2012, with Common Licensing 18.8 and higher, require the latest Windows Updates to enable TLS 1.2 as default secure protocol.

Note:
Microsoft Windows XP, Microsoft Windows Server 2003, and Microsoft Windows Server 2008 are no longer supported in Common Licensing 18.4 and higher. If you are using one of these operating systems, use Common Licensing 18.3.

Supported Virtual Machines

License Client

- VMware ESXi 5.X
- Microsoft Hyper-V on Windows Server 2008 R2, 2012, 2016, or 2019

Local License Server

- VMware ESXi 5.x
- Microsoft Hyper-V 6.1, 6.3

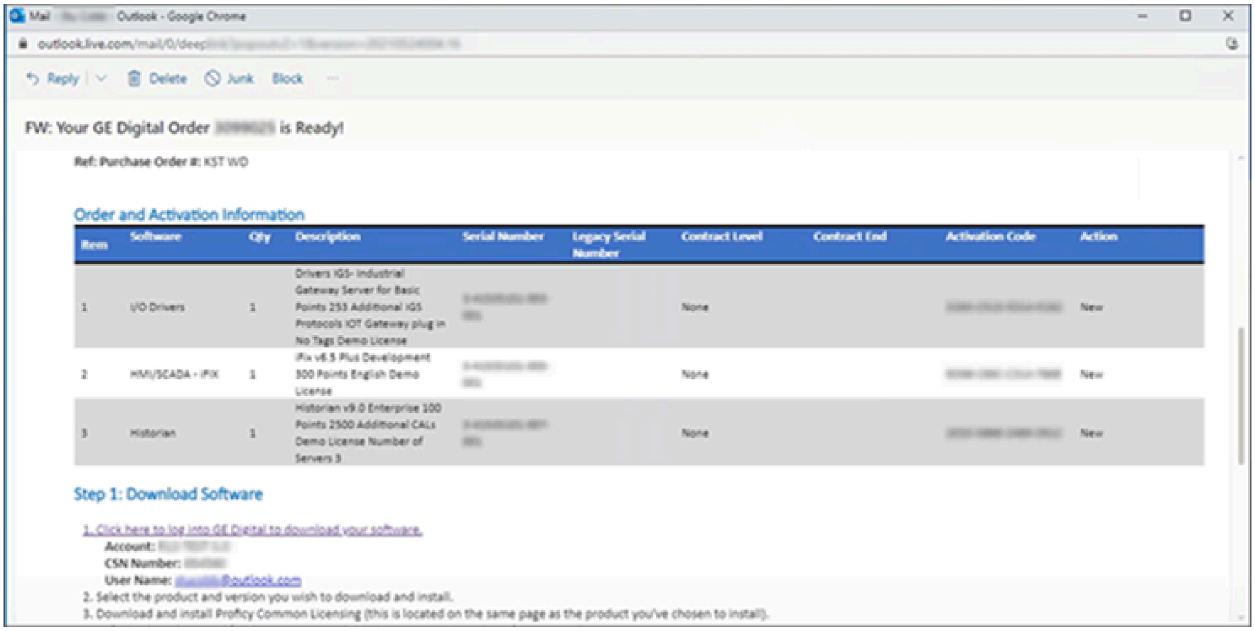
Common Licensing was tested on VMware and the Parallels virtual machine software running on a Macintosh computer.

Configure Common Licensing

Step 1: Order Email and Downloads

Order Email

After you receive an order email from GE Digital with your activation codes, similar to the one below. You can download the required products and install them on your computer (physical machine or virtual machine). After you download the required product, you will see `CommonLicensing_<version>.exe` (for example: CommonLicensing_v19_4_1848_0.exe). Use the steps that follow to accomplish the license activation task.


Mail [redacted] Outlook - Google Chrome
outlook.live.com/mail/0/deep[redacted]
Reply
Delete
Junk
Block

FW: Your GE Digital Order [redacted] is Ready!

Ref: Purchase Order #: KST WD

Order and Activation Information

Item	Software	Qty	Description	Serial Number	Legacy Serial Number	Contract Level	Contract End	Activation Code	Action
1	I/O Drivers	1	Drivers IGS- Industrial Gateway Server for Basic Points 253 Additional IGS Protocols IOT Gateway plug in No Tags Demo License	[redacted]		None		[redacted]	New
2	HMI/SCADA - iFIX	1	iFix v6.5 Plus Development 300 Points English Demo License	[redacted]		None		[redacted]	New
3	Historian	1	Historian v9.0 Enterprise 100 Points 2500 Additional CALs Demo License Number of Servers 3	[redacted]		None		[redacted]	New

Step 1: Download Software

1. Click here to log into GE Digital to download your software.
   Account: [redacted]
   CSN Number: [redacted]
   User Name: [redacted]@outlook.com
2. Select the product and version you wish to download and install.
3. Download and install Proficy Common Licensing (this is located on the same page as the product you've chosen to install).

Download Common Licensing

1. Select the link in the email from GE Digital to access the web site.
2. Login using the same e-mail address that the activation codes were sent to. After a successful login, you will be navigated to the **Software Order Download** page, that includes **Product List**, and a link to **Proficy License Installer**.
3. Select **Proficy License Installer** from **Other helpful links**. The **GE Licensing Installer** page that contains Common Licensing software appears.
4. Double-click `CommonLicensing<version>.exe` to start the licensing download.

> **Note:**
> This license install will have all the licensing functionalities that can be administrated from the same computer.

Refer, Step 2: Common Licensing Software *(on page 65)* to proceed to next steps.

(on page 65)

Step 2: Common Licensing Software

Overview

Perform the following steps to install the required Common Licensing software on your computer:

1. Execute `CommonLicensing<version>.exe` *(on page 66)*
2. Install License Client *(on page 67)*
3. Install the Local License Server *(on page 69)*
4. Install License Server Tools *(on page 70)*

> **Important:**
> When you run `CommonLicensing_<version>.exe`, you must be logged in as an Administrator.

Before you begin, follow the below important notes on the Common Licensing software installation for your system configuration.

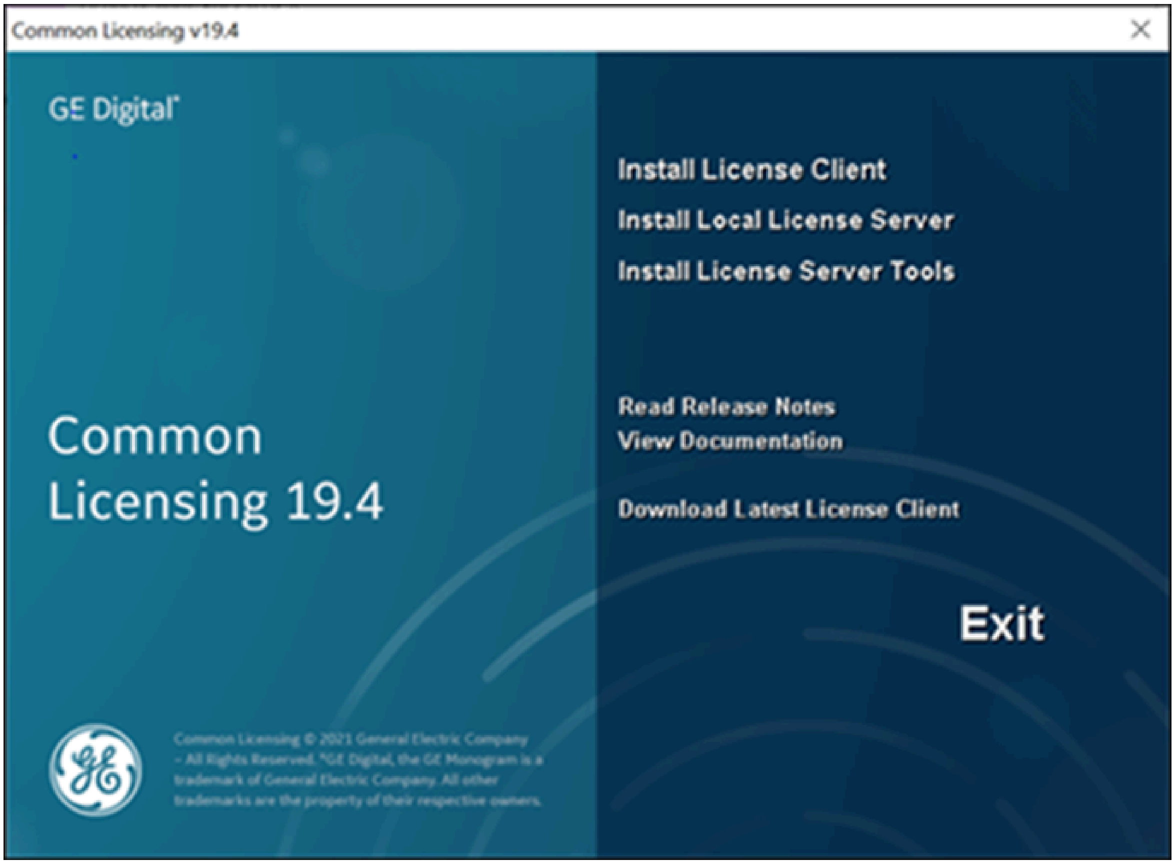
Note:

- For a physical machine, the License Client is the only software that must be configured. The physical machine can collect the GE product licenses from the GE cloud server or from the Local License Server, and then the GE products are activated through the License Client.
- For a virtual machine, all the three software: 1) License Client, 2) Local License Server, and the 3) License Server Tools must be installed. If you have a separate computer pre-installed with Local License Server, you do not have to install Local License Server in your virtual machine. The virtual machine can collect the GE product licenses from the Local License Server and then the GE products are activated through the License Client.

Execute `CommonLicensing<version>.exe`

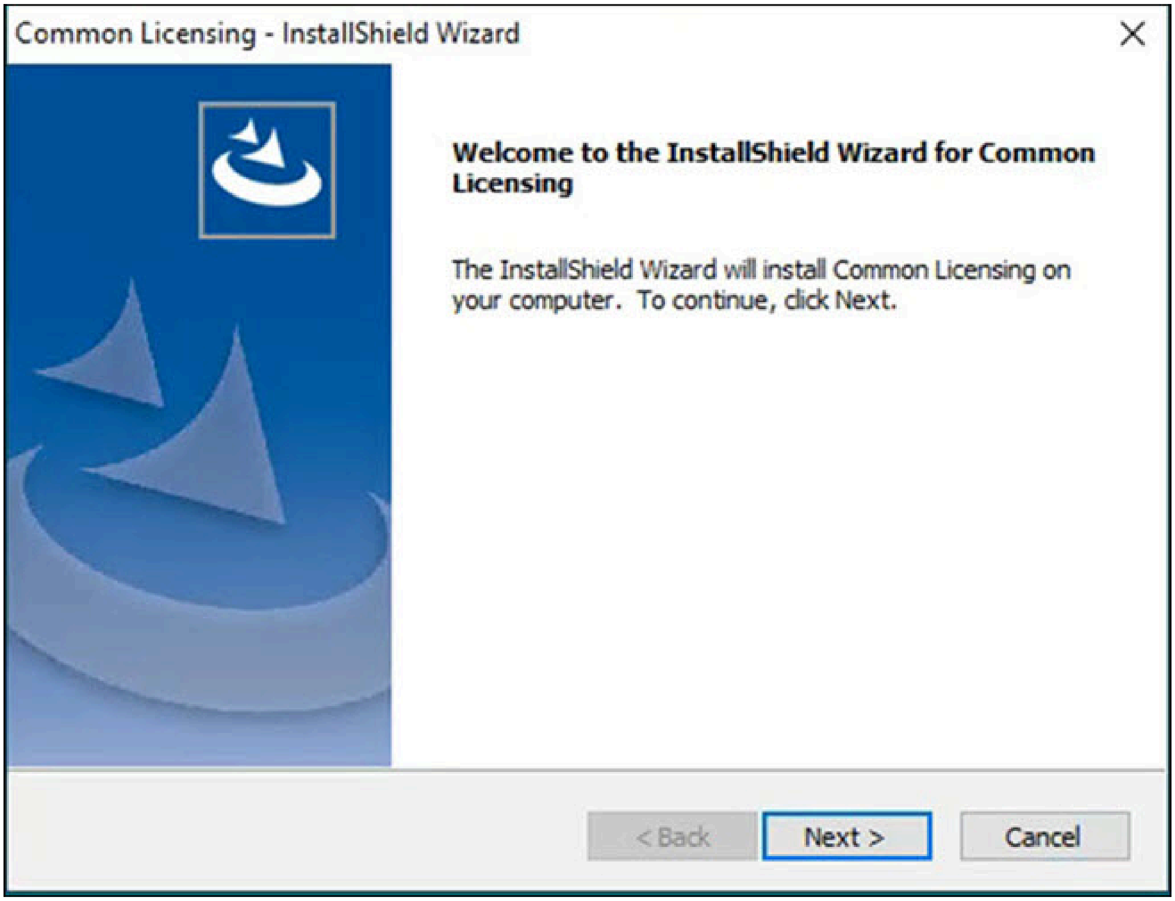
1. Confirm that you are logged in as an Administrator.
2. Browse the folder where you downloaded the `CommonLicensing<version>.exe` file.
3. Right-click the `CommonLicensing<version>.exe` file, and select **Run as Administrator**. A message appears asking if you want to allow this application to make changes to your device.

4. Select **Yes**. The **Common Licensing** screen appears, as shown in the following figure.



Install License Client

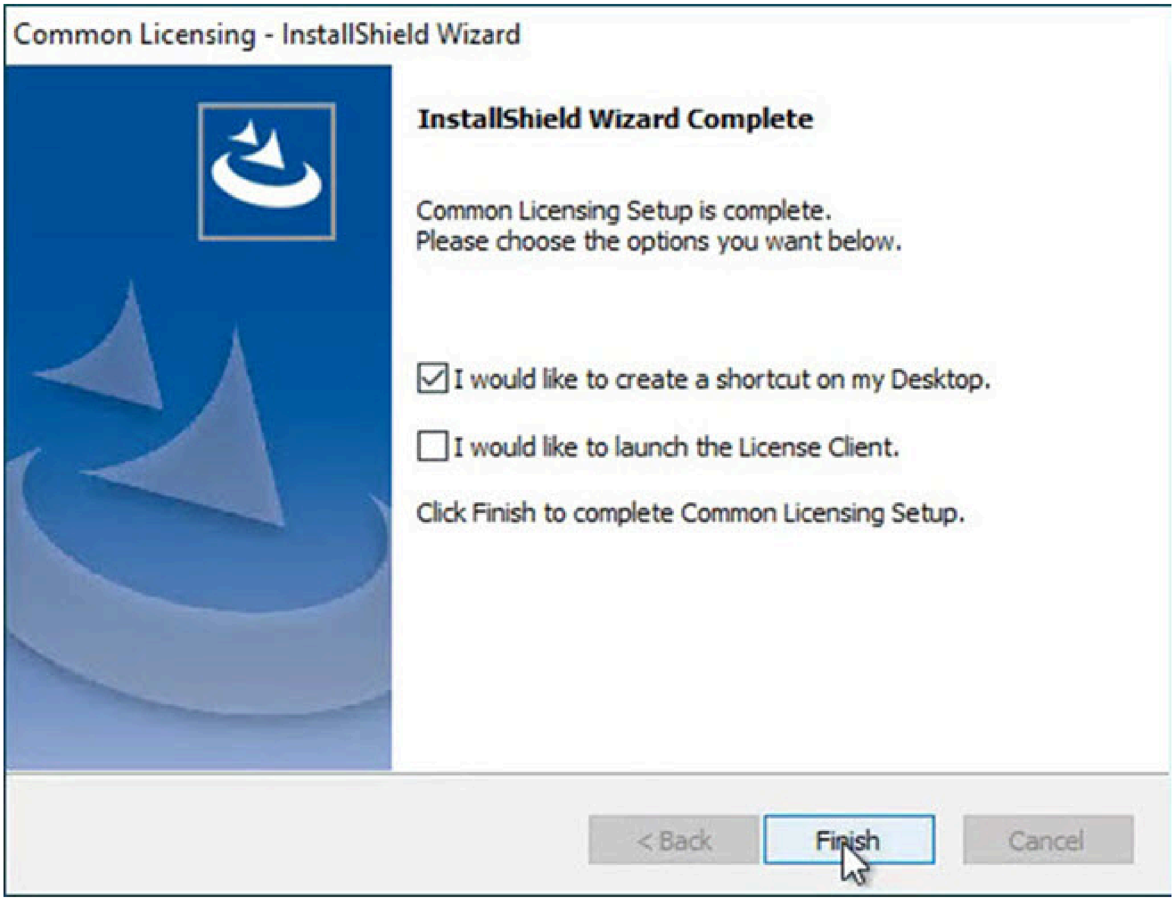
1. From the Common Licensing screen, select **Install License Client**.
2. The installation process may take a few moments, and may require some prerequisites to install. The following screen appears.



Welcome to the InstallShield Wizard for Common Licensing

The InstallShield Wizard will install Common Licensing on your computer. To continue, click Next.

3. Select **Next**. The License Agreement appears.
4. Select **I accept the terms of this license agreement** and select **Next** to continue.
5. If a message to install USB HASP Drivers appears, leave the default (selected), and select **Next**. Otherwise, the **Ready to Install the Program** screen appears.
6. Select **Install**. When the installation completes, the **InstallShield Wizard Complete** screen appears.



Common Licensing - InstallShield Wizard

InstallShield Wizard Complete

Common Licensing Setup is complete.
Please choose the options you want below.

☑ I would like to create a shortcut on my Desktop.

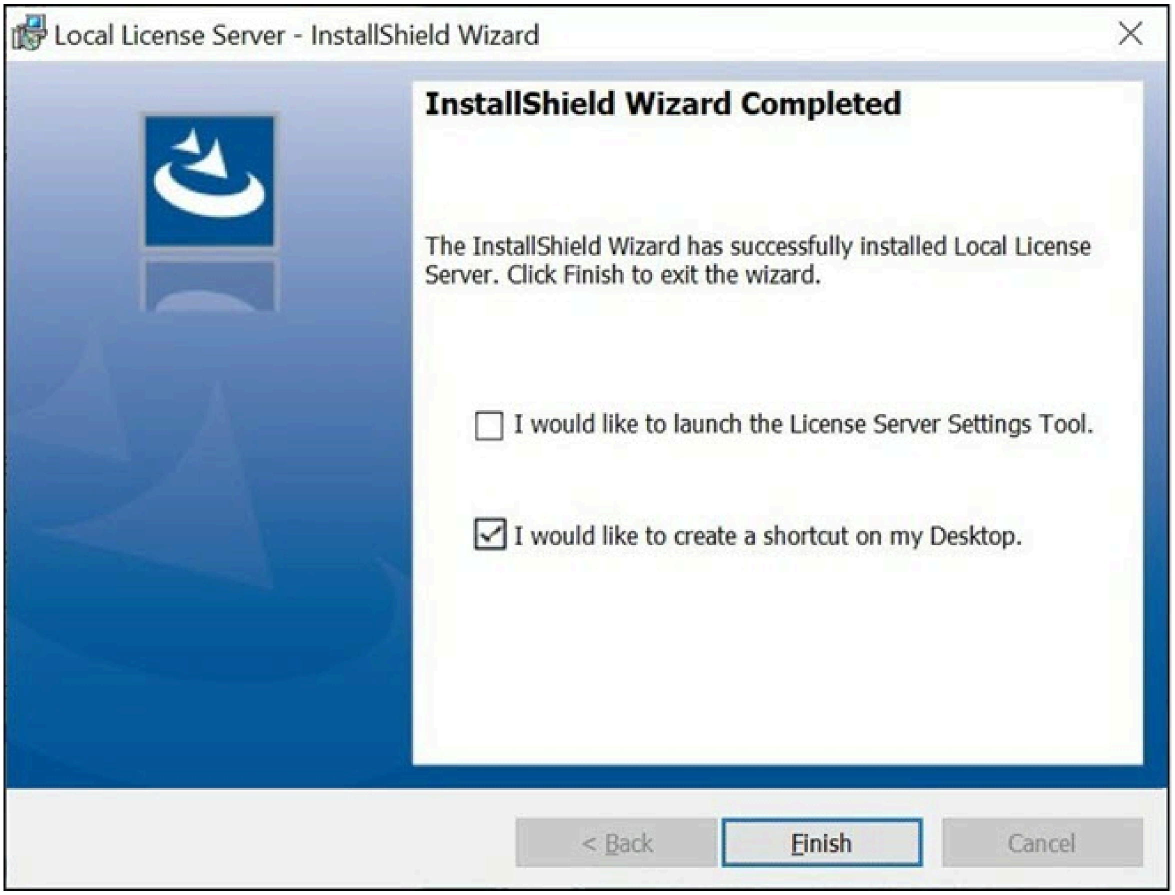
□ I would like to launch the License Client.

Click Finish to complete Common Licensing Setup.

7. Select the **I would like to create a shortcut on my Desktop** check box.
8. Select **Finish** to complete the installation.

Install Local License Server

1. From the Common Licensing screen, select **Install Local License Server** .
2. The installation process may take a few moments, and may require some prerequisites to finish the installation. When the installation completes, the **InstallShield Wizard Completed** screen appears.



Local License Server - InstallShield Wizard

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed Local License Server. Click Finish to exit the wizard.

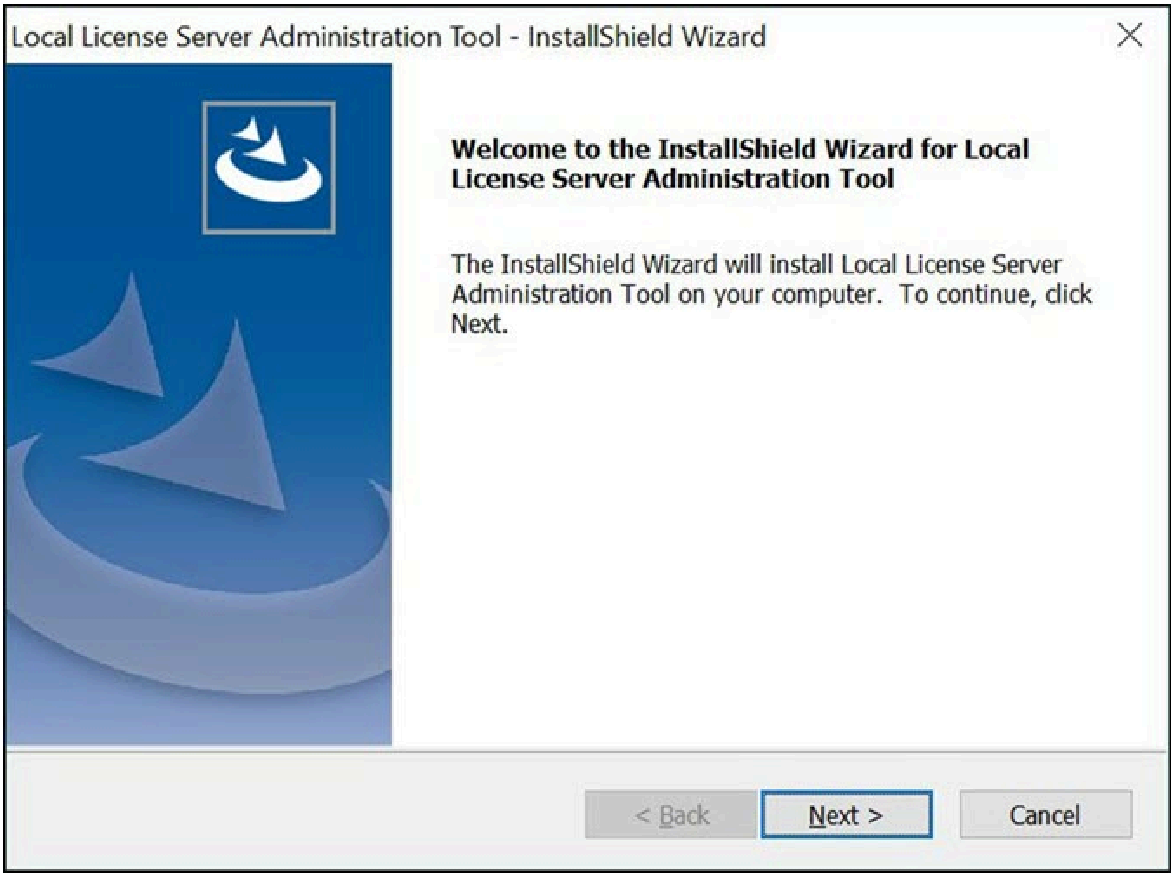
□ I would like to launch the License Server Settings Tool.

☑ I would like to create a shortcut on my Desktop.

3. Select the **I would like to create a shortcut on my Desktop** check box.
4. Select **Finish** to complete the installation.

Install License Server Tools

1. From the Common Licensing screen, select **Install License Server Tools**.
2. The installation process may take a few moments, and may require some prerequisites to install. The welcome screen appears.

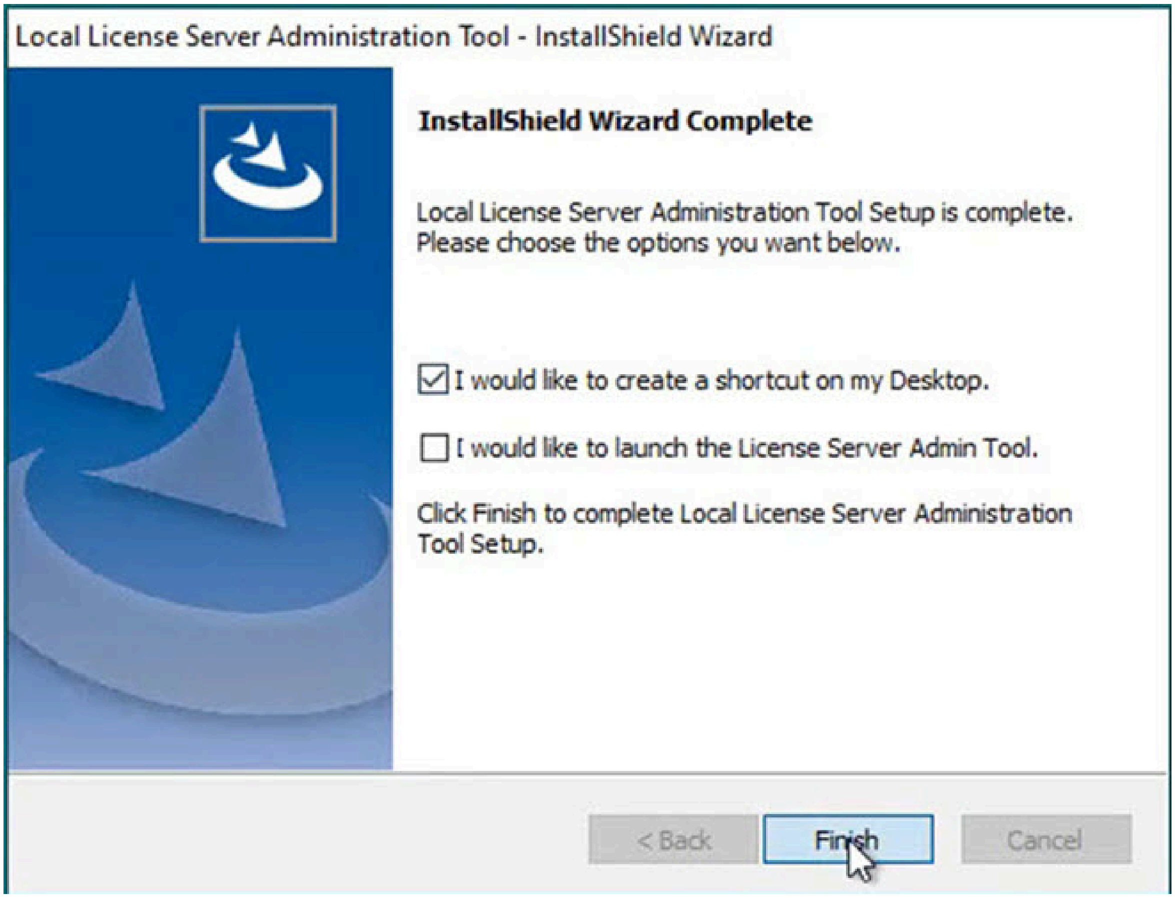


Local License Server Administration Tool - InstallShield Wizard

Welcome to the InstallShield Wizard for Local License Server Administration Tool

The InstallShield Wizard will install Local License Server Administration Tool on your computer. To continue, click Next.

3. Select **Next**. The License Agreement page appears.
4. Select **I accept the terms of this license agreement** option, and then select **Next**. The **Ready to Install the Program** page appears.
5. Select **Install**. When the installation completes, the **InstallShield Wizard Complete** screen appears.



Local License Server Administration Tool - InstallShield Wizard

InstallShield Wizard Complete

Local License Server Administration Tool Setup is complete. Please choose the options you want below.

☑ I would like to create a shortcut on my Desktop.

□ I would like to launch the License Server Admin Tool.

Click Finish to complete Local License Server Administration Tool Setup.

6. Select the **I would like to create a shortcut on my Desktop** option.
7. Select **Finish** to complete the installation.

After you have configured the software as per your system requirements from the Common Licensing screen, you can proceed to the next step, Step 3: Activating Licenses *(on page 72)*.

→

Next Step

(on page 72)

Step 3: Activating Licenses

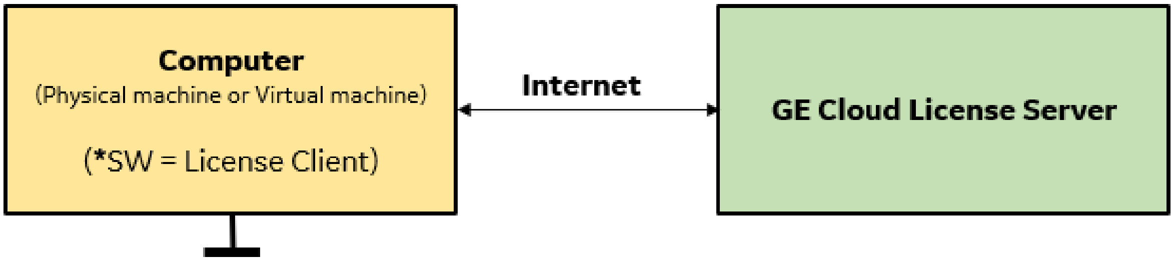
Activating Licenses Scenarios

Following are the scenarios to activate your GE product licenses:

1. Computer (online) connected to the GE Cloud License Server *(on page 73)*
2. Computer (online) or VM connected to a Local License Server *(on page 74)*

3. Computer (offline) Licenses Activation by using GE USB Hardware Key *(on page 79)*
4. Computer (offline) Licenses Activation by using Request and Response Files *(on page 81)*

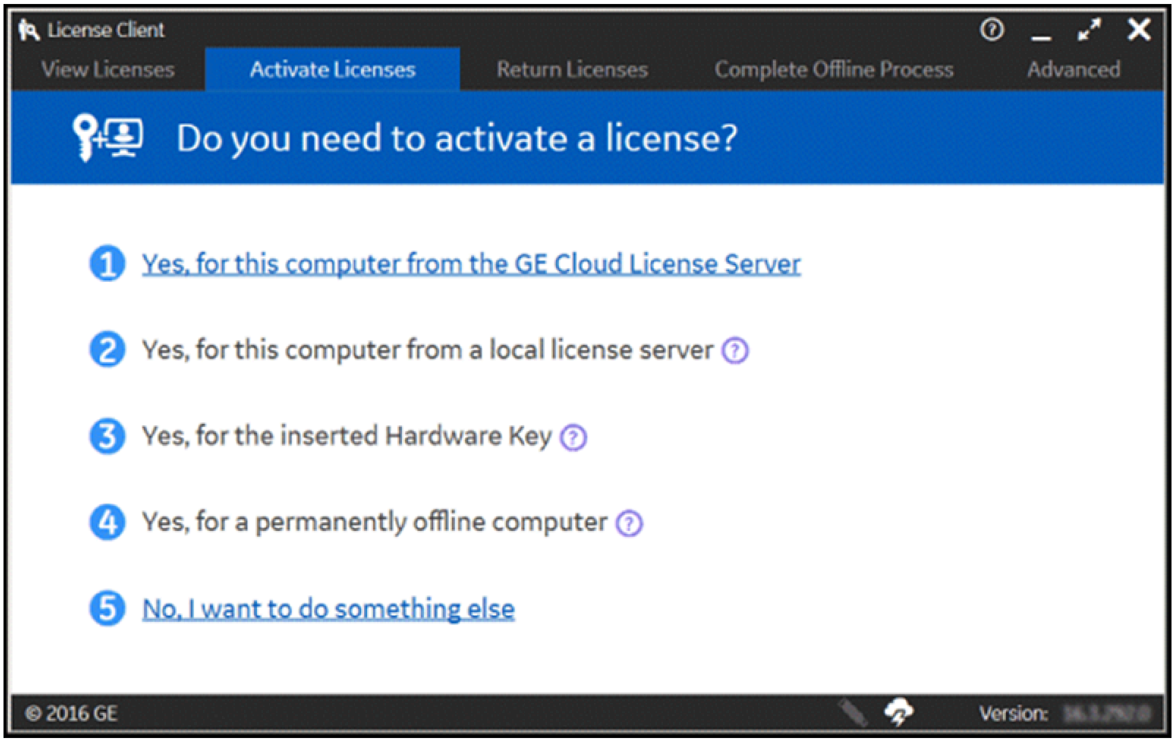
Scenario 1: Computer (online) connected to the GE Cloud License Server



*Software

The computer (physical machine or virtual machine) with **GE Cloud License Server** is connected to internet, the GE product licenses are collected from GE Cloud License Server and then the licenses are activated in the computer installed with License Client.

1. In License Client, select **Activate Licenses**, select the option 1, **Yes, for this computer from the GE Cloud License Server**.



Do you need to activate a license?

1 Yes, for this computer from the GE Cloud License Server

2 Yes, for this computer from a local license server

3 Yes, for the inserted Hardware Key

4 Yes, for a permanently offline computer

5 No, I want to do something else

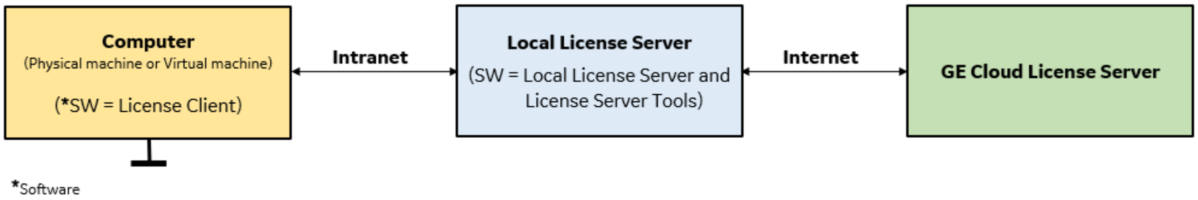
© 2016 GE Version: [redacted]

2. The **Activate Licenses from the GE Cloud Server** page appears.

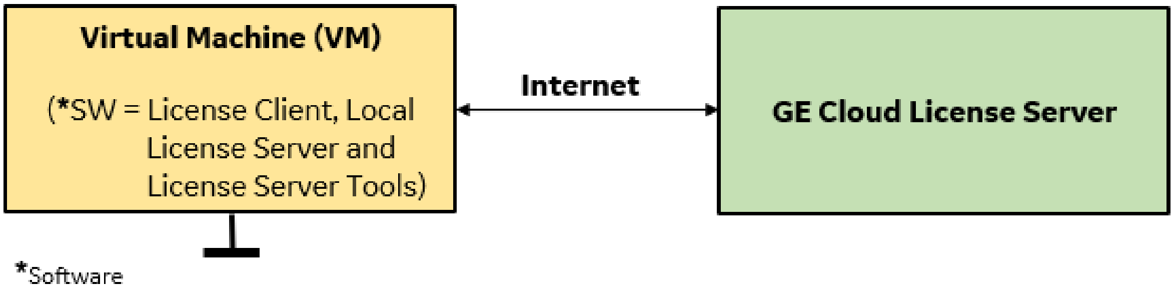
Note:
Internet connectivity is verified before this page is displayed. An error message is displayed if the GE Cloud License Server is not accessible, and the No Licenses on this Computer page is automatically displayed.

3. Enter your first activation code, and then select **Add Code**.
4. Repeat the previous step for each license you have.
5. Select **Activate**. The Licenses screen should now display all the licenses activated on the server.

Scenario 2: Computer (online) or VM connected to a Local License Server



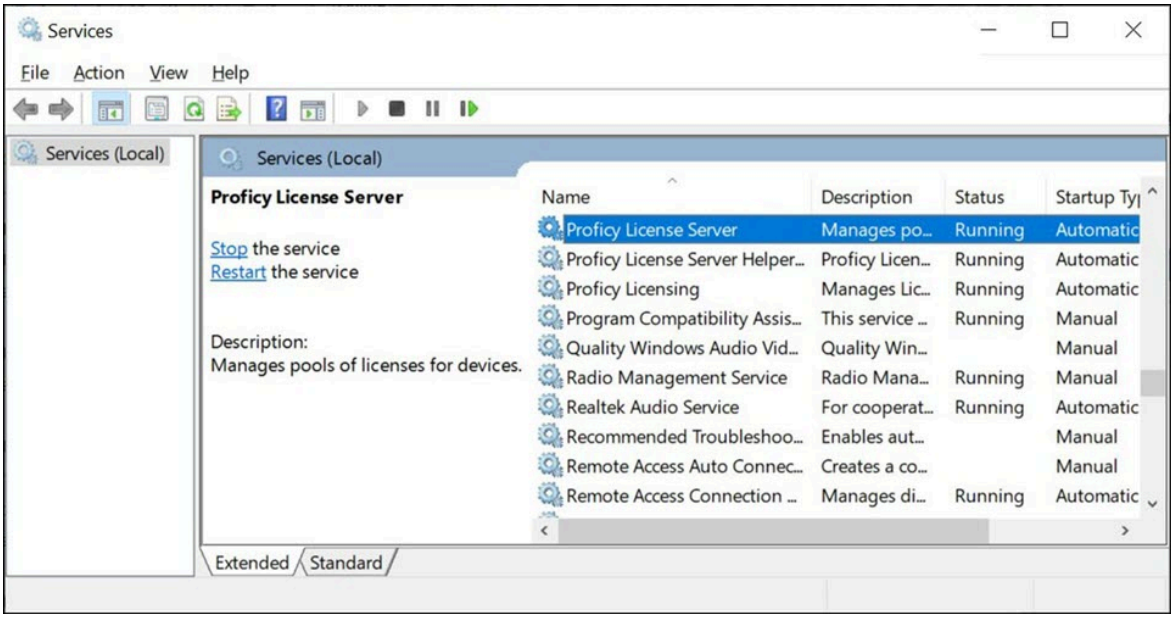
The computer (physical machine or virtual machine) with **Local License Server** is connected to internet, the GE product licenses are collected by communicating with GE Cloud License Server and then the licenses are activated in the intranet computer installed with License Client.


Virtual Machine (VM)
(*SW = License Client, Local License Server and License Server Tools)
Internet
GE Cloud License Server
*Software

The virtual machine with all the three software: 1) License Client, 2) Local License Server and the 3) License Server Tools must be installed. If you have a separate computer pre-installed with Local License Server, you do not have to install Local License Server in your virtual machine.

Follow the below steps for a physical machine or a virtual machine installed with Local License Server software:

1. From the Windows Services console (Press **Windows+R** on your keyboard, then enter **services.msc** and press the **Enter** button), confirm that the License Server is running.



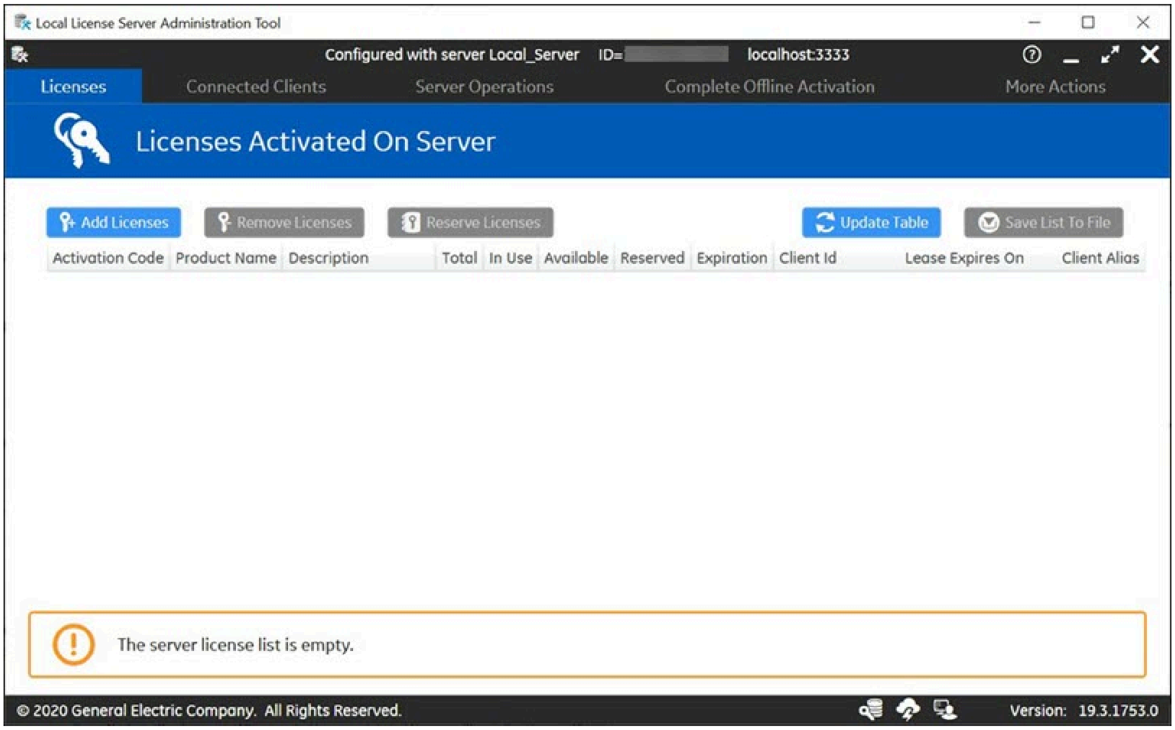
Proficy License Server

Stop the service
Restart the service

Description:
Manages pools of licenses for devices.

Name	Description	Status	Startup Ty
Proficy License Server	Manages po...	Running	Automatic
Proficy License Server Helper...	Proficy Licen...	Running	Automatic
Proficy Licensing	Manages Lic...	Running	Automatic
Program Compatibility Assis...	This service ...	Running	Manual
Quality Windows Audio Vid...	Quality Win...		Manual
Radio Management Service	Radio Mana...	Running	Manual
Realtek Audio Service	For cooperat...	Running	Automatic
Recommended Troubleshoo...	Enables aut...		Manual
Remote Access Auto Connec...	Creates a co...		Manual
Remote Access Connection ...	Manages di...	Running	Automatic

2. Navigate to `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\General Electric`, and then select **Local License Server Administration Tool**. A message appears prompting you to confirm the changes.
3. Select **Yes** to continue. The **Local License Server Administration Tool** screen appears, as shown in the following figure.



Configured with server Local_Server ID=[redacted] localhost:3333

Licenses Activated On Server

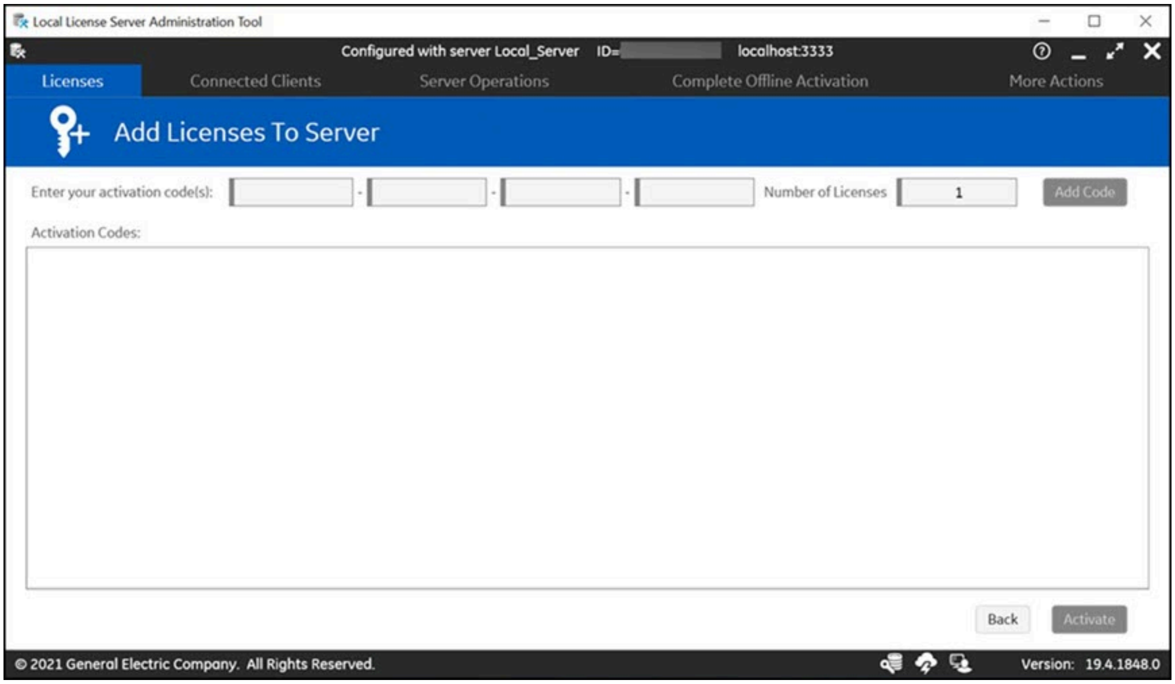
Activation Code	Product Name	Description	Total	In Use	Available	Reserved	Expiration	Client Id	Lease Expires On	Client Alias

The server license list is empty.

© 2020 General Electric Company. All Rights Reserved.

Version: 19.3.1753.0

4. Select **Add Licenses**. The following screen appears.

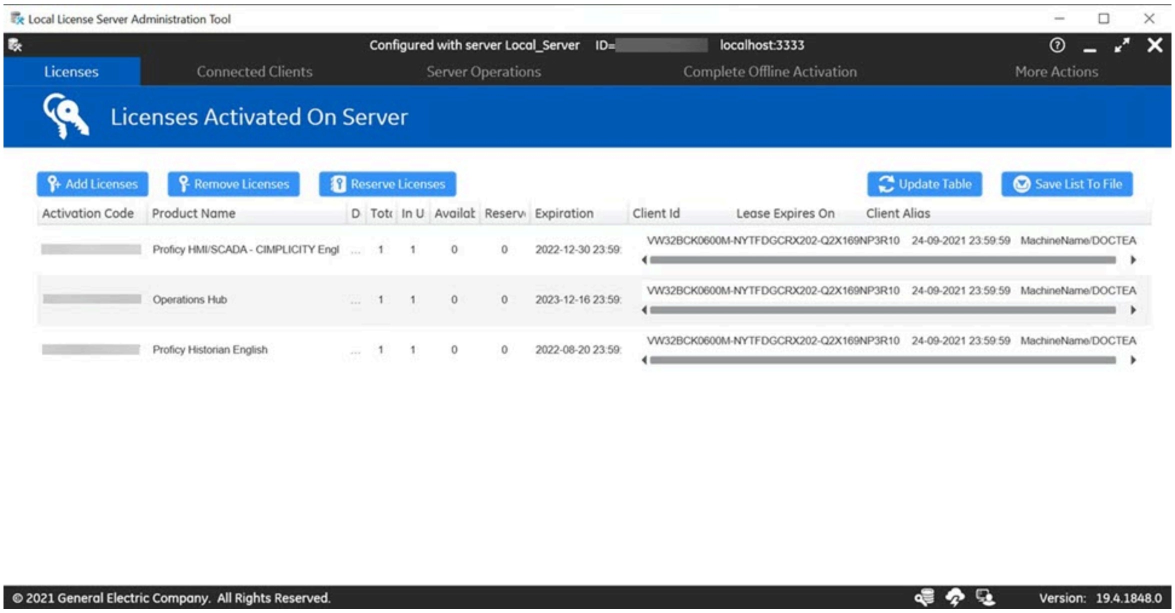

Local License Server Administration Tool
Configured with server Local_Server ID=[redacted] localhost:3333
Licenses
Connected Clients
Server Operations
Complete Offline Activation
More Actions
Add Licenses To Server
Enter your activation code(s):
Number of Licenses
1
Add Code
Activation Codes:
Back
Activate
© 2021 General Electric Company. All Rights Reserved.
Version: 19.4.1848.0

5. Enter your first activation code, and then select **Add Code**.

> **Note:**
> You can find the activation codes in your GE order e-mail.

6. Repeat the previous step for each license you have.

7. Select **Activate**. The Licenses screen should now display all the licenses activated on the server, as shown in the following figure.

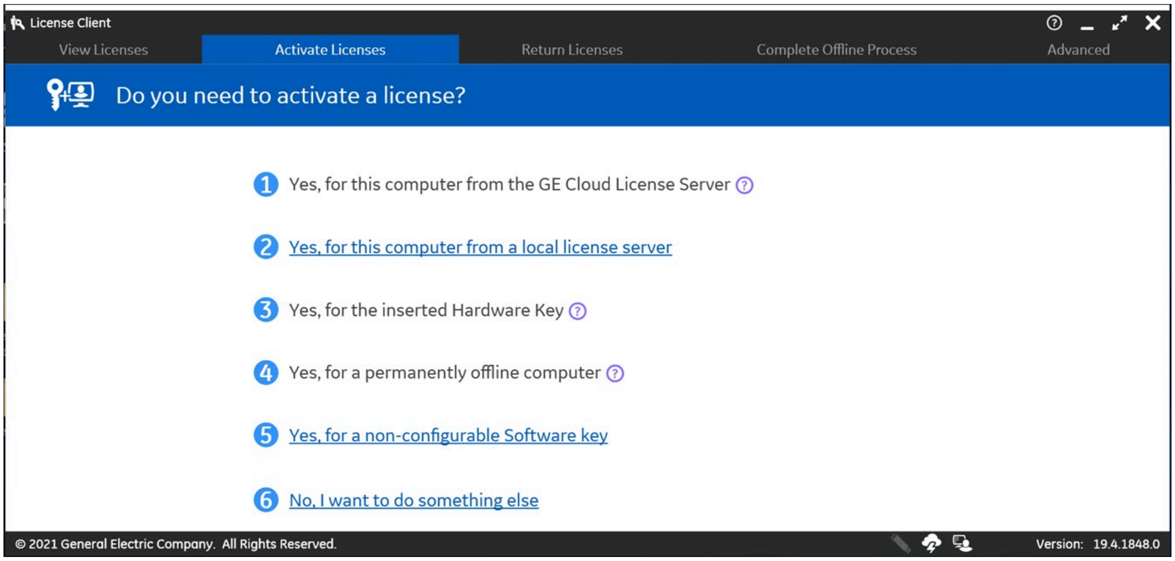

Local License Server Administration Tool
Configured with server Local_Server ID=[redacted] localhost:3333
Licenses
Connected Clients
Server Operations
Complete Offline Activation
More Actions
Licenses Activated On Server
Add Licenses
Remove Licenses
Reserve Licenses
Update Table
Save List To File
Version: 19.4.1848.0

Activation Code	Product Name	D	Tot	In U	Availat	Reserv	Expiration	Client Id	Lease Expires On	Client Alias
[redacted]	Proficy HMI/SCADA - CIMPLICITY Engl	...	1	1	0	0	2022-12-30 23:59:	VW32BCK0600M-NYTFDGCRX202-Q2X169NP3R10	24-09-2021 23:59:59	MachineName/DOCTEA
[redacted]	Operations Hub	...	1	1	0	0	2023-12-16 23:59:	VW32BCK0600M-NYTFDGCRX202-Q2X169NP3R10	24-09-2021 23:59:59	MachineName/DOCTEA
[redacted]	Proficy Historian English	...	1	1	0	0	2022-08-20 23:59:	VW32BCK0600M-NYTFDGCRX202-Q2X169NP3R10	24-09-2021 23:59:59	MachineName/DOCTEA

© 2021 General Electric Company. All Rights Reserved.

Activate your Product Licenses on License Client

1. Navigate to `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\General Electric` and then select **License Client**. A message appears prompting you to confirm the changes.
2. Select **Yes** to continue. The **License Client** screen appears, as shown in the following figure.



Do you need to activate a license?

1 Yes, for this computer from the GE Cloud License Server

2 Yes, for this computer from a local license server

3 Yes, for the inserted Hardware Key

4 Yes, for a permanently offline computer

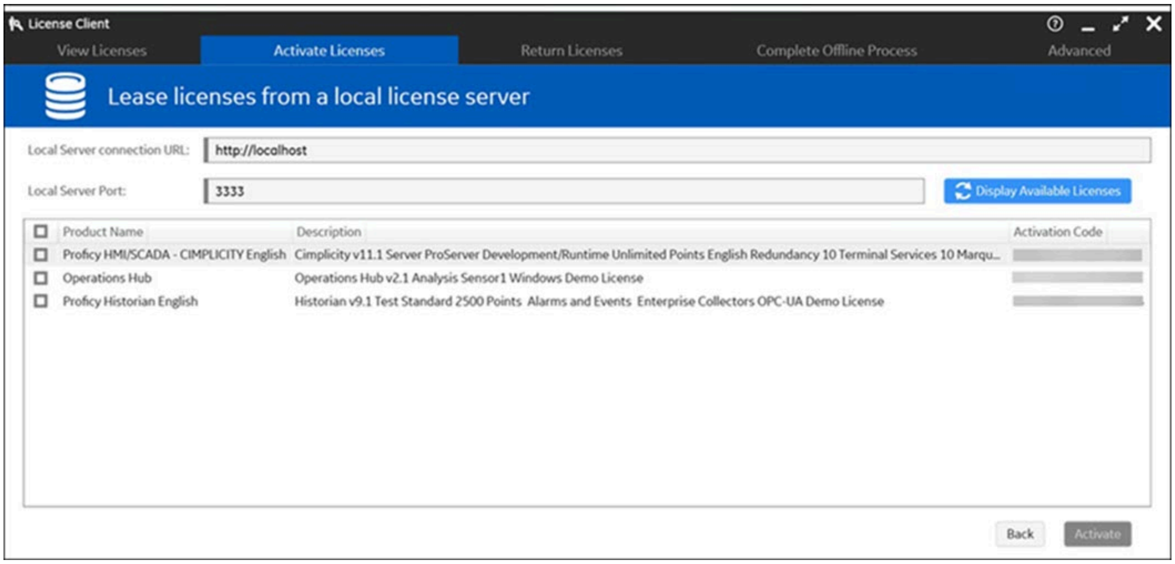
5 Yes, for a non-configurable Software key

6 No, I want to do something else

© 2021 General Electric Company. All Rights Reserved.

3. In License Client, select **Activate Licenses**.

4. You have the Local Licensing Server already installed on the same computer, hence select the option 2, **Yes, for this computer from a local license server** . The **Lease licenses from a local license server** screen appears, as shown in below figure.



Lease licenses from a local license server

Local Server connection URL: http://localhost

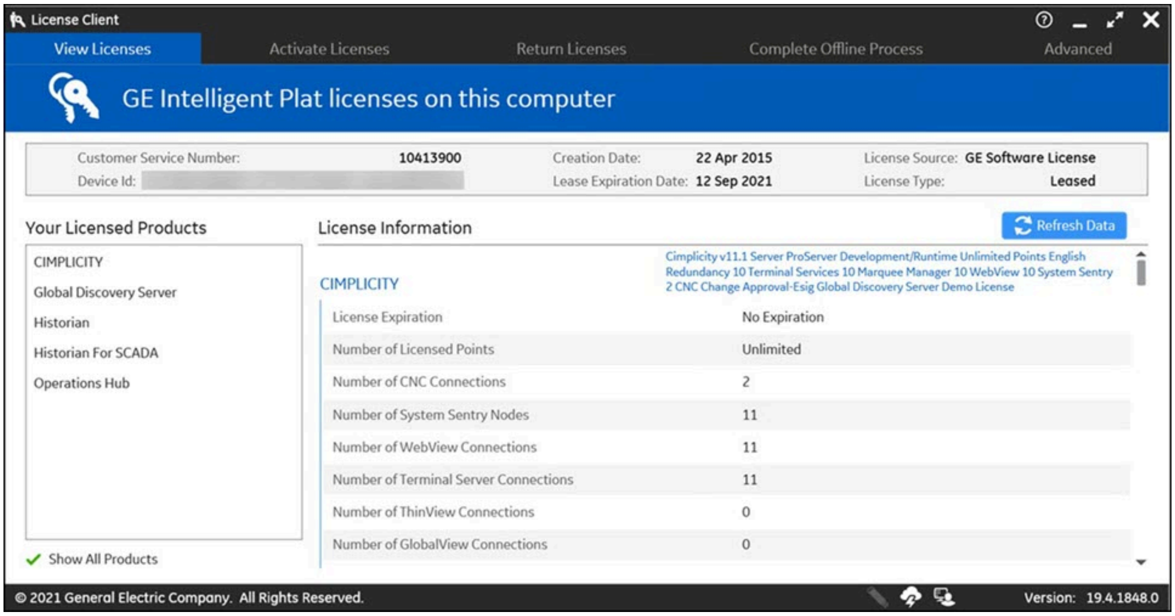
Local Server Port: 3333

□	Product Name	Description	Activation Code
□	Proficy HMI/SCADA - CIMPLICITY English	Cimplicity v11.1 Server ProServer Development/Runtime Unlimited Points English Redundancy 10 Terminal Services 10 Marqu...	[redacted]
□	Operations Hub	Operations Hub v2.1 Analysis Sensor1 Windows Demo License	[redacted]
□	Proficy Historian English	Historian v9.1 Test Standard 2500 Points Alarms and Events Enterprise Collectors OPC-UA Demo License	[redacted]

5. Select the check box for the products you want to activate, and then select **Activate**.

Confirm the License Client Displays Licenses

1. In License Client, select **View Licenses**. The activated licenses for the selected server appears, similar to the screen below. In the Licensed Products section, select the products listed to view the license information.



GE Intelligent Plat licenses on this computer

Customer Service Number:	10413900	Creation Date:	22 Apr 2015	License Source:	GE Software License
Device Id:	[redacted]	Lease Expiration Date:	12 Sep 2021	License Type:	Leased

Your Licensed Products

- CIMPLICITY
- Global Discovery Server
- Historian
- Historian For SCADA
- Operations Hub

✓ Show All Products

License Information

CIMPLICITY

Cimplicity v11.1 Server ProServer Development/Runtime Unlimited Points English Redundancy 10 Terminal Services 10 Marquee Manager 10 WebView 10 System Sentry 2 CNC Change Approval-Esig Global Discovery Server Demo License

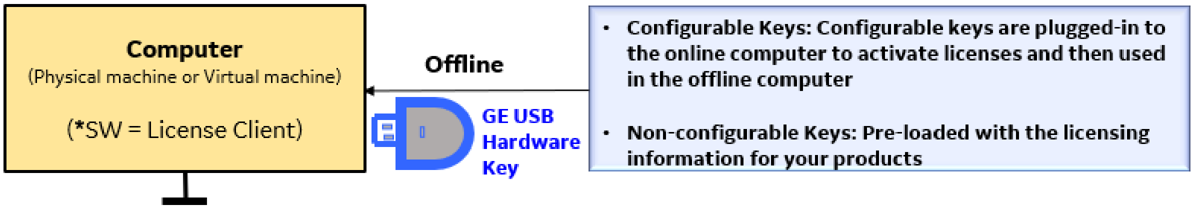
License Expiration	No Expiration
Number of Licensed Points	Unlimited
Number of CNC Connections	2
Number of System Sentry Nodes	11
Number of WebView Connections	11
Number of Terminal Server Connections	11
Number of ThinView Connections	0
Number of GlobalView Connections	0

© 2021 General Electric Company. All Rights Reserved.

Version: 19.4.1848.0

2. Confirm that your license information appears correctly for each product you activated.

Scenario 3: Computer (offline) Licenses Activation by using GE USB Hardware Key



- Configurable Keys: Configurable keys are plugged-in to the online computer to activate licenses and then used in the offline computer
- Non-configurable Keys: Pre-loaded with the licensing information for your products

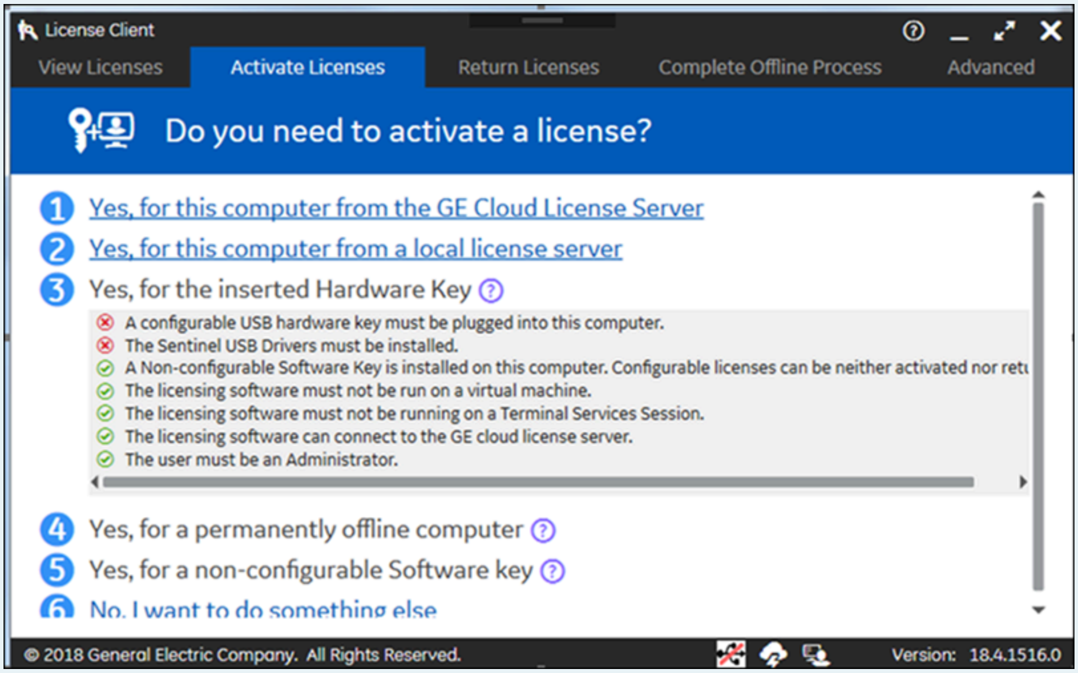
*Software

- Configurable GE USB Hardware Keys: Configurable keys are plugged-in to a computer with internet to activate licenses and then used in the computer that does not have internet.
- Non-configurable GE USB Hardware Keys: Pre-loaded with the licensing information for your products.

1. Insert the GE USB Hardware Key to your online computer (physical machine or a virtual machine).
2. In License Client, select **Activate Licenses**, select the option 3, **Yes, for the inserted Hardware key**.

Note:

If you did not install the Sentinel USB drivers, error messages appear and the disabled USB icon appears in the footer.



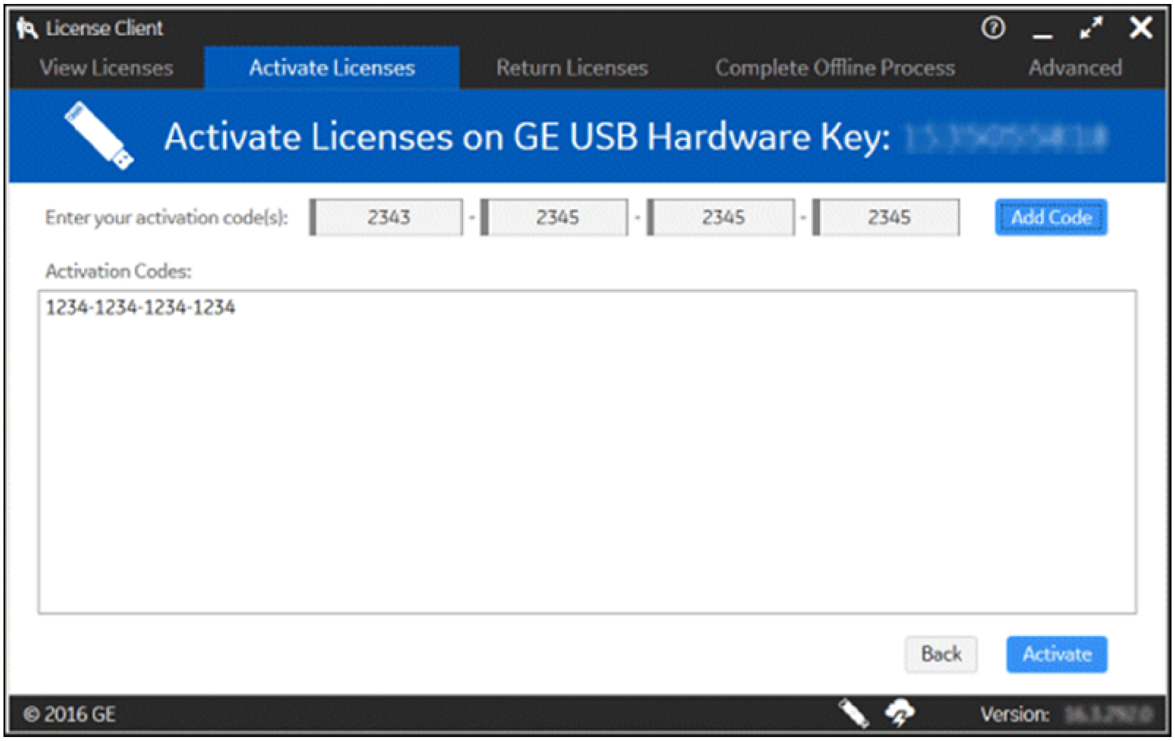
Do you need to activate a license?

1. Yes, for this computer from the GE Cloud License Server
2. Yes, for this computer from a local license server
3. Yes, for the inserted Hardware Key ?
   - ☒ A configurable USB hardware key must be plugged into this computer.
   - ☒ The Sentinel USB Drivers must be installed.
   - ✓ A Non-configurable Software Key is installed on this computer. Configurable licenses can be neither activated nor retu
   - ✓ The licensing software must not be run on a virtual machine.
   - ✓ The licensing software must not be running on a Terminal Services Session.
   - ✓ The licensing software can connect to the GE cloud license server.
   - ✓ The user must be an Administrator.
4. Yes, for a permanently offline computer ?
5. Yes, for a non-configurable Software key ?
6. No, I want to do something else

© 2018 General Electric Company. All Rights Reserved.

Version: 18.4.1516.0

If you did install the Sentinel USB drivers, the License Client detects and reads the GE USB Hardware Key (up to two minutes), and then the **Activate Licenses on GE USB Hardware Key** page appears, as shown below.



Activate Licenses on GE USB Hardware Key: [redacted]

Enter your activation code(s): 2343 - 2345 - 2345 - 2345

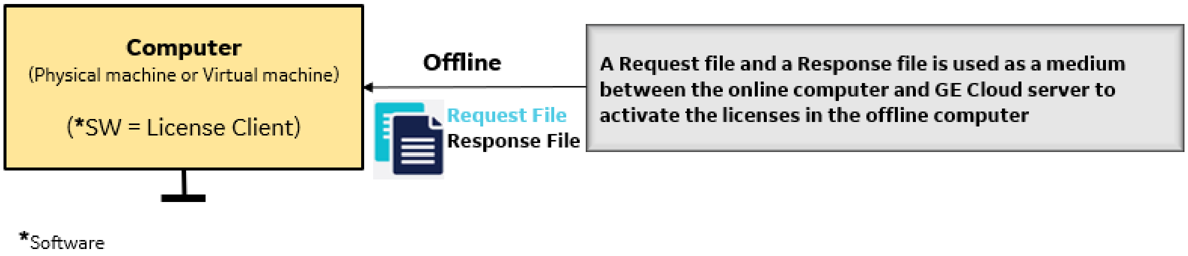
Activation Codes:

1234-1234-1234-1234

Version: [redacted]

3. Enter your first activation code, and then select **Add Code**.
4. Repeat the previous step for each license you have.
5. Select **Activate**. The Licenses screen should now display all the licenses activated on the server.
6. Remove the GE USB Hardware Key from your online computer and plug-in to the offline computer.

Scenario 4: Computer (offline) Licenses Activation by using Request and Response Files



A Request file and a Response file is used as a medium between the online computer and GE Cloud server to activate the licenses in the offline computer

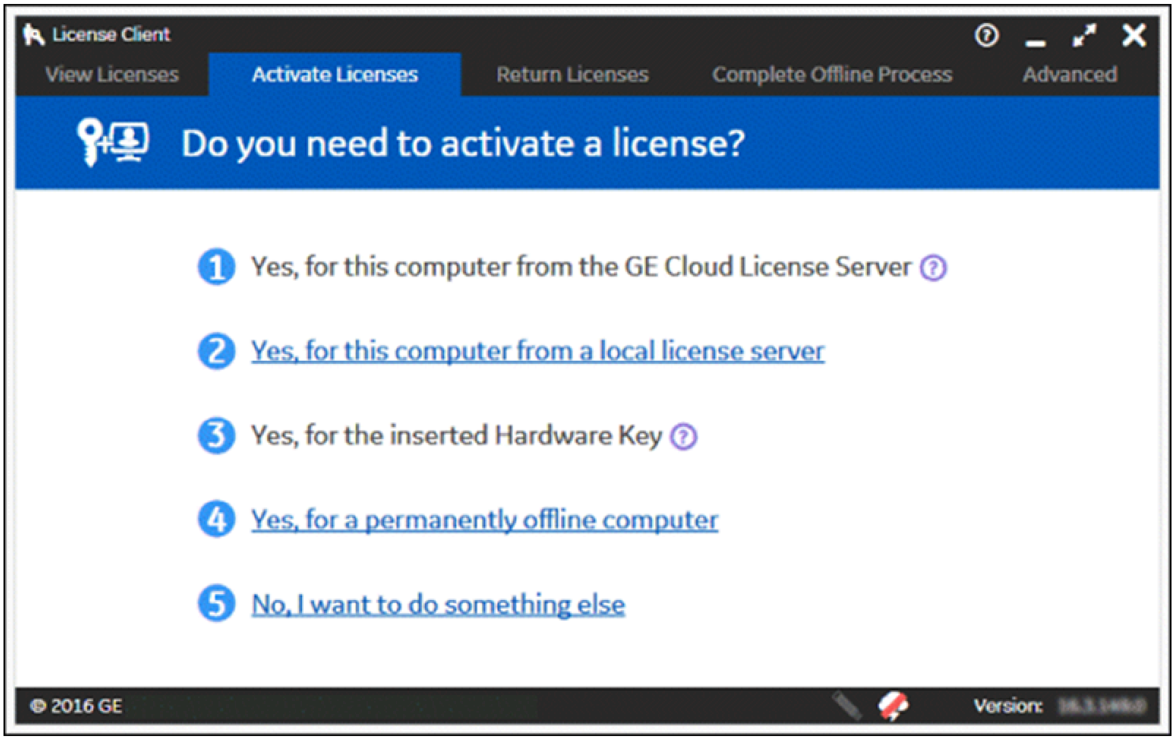
A **Request file** and a **Response file** is used as a medium between a computer having internet and GE Cloud server to activate the licenses in the offline computer.

In License Client, select **Activate Licenses**, to activate licenses on client computers that are not connected to the internet. Activating licenses on an offline computer includes the following steps:

1. Generate a request file from the offline computer. Send the request file to the online computer.
2. From an online computer, send the request file to the GE cloud license server and generate a response file.
3. Send the response file to the offline computer and activate the licenses.

Generating a Request File

1. From License Client, select the **Activate Licenses** tab. The License Client detects that the client computer is not connected to the internet. The "Do you need to activate a License?" page appears.



Do you need to activate a license?

1 Yes, for this computer from the GE Cloud License Server

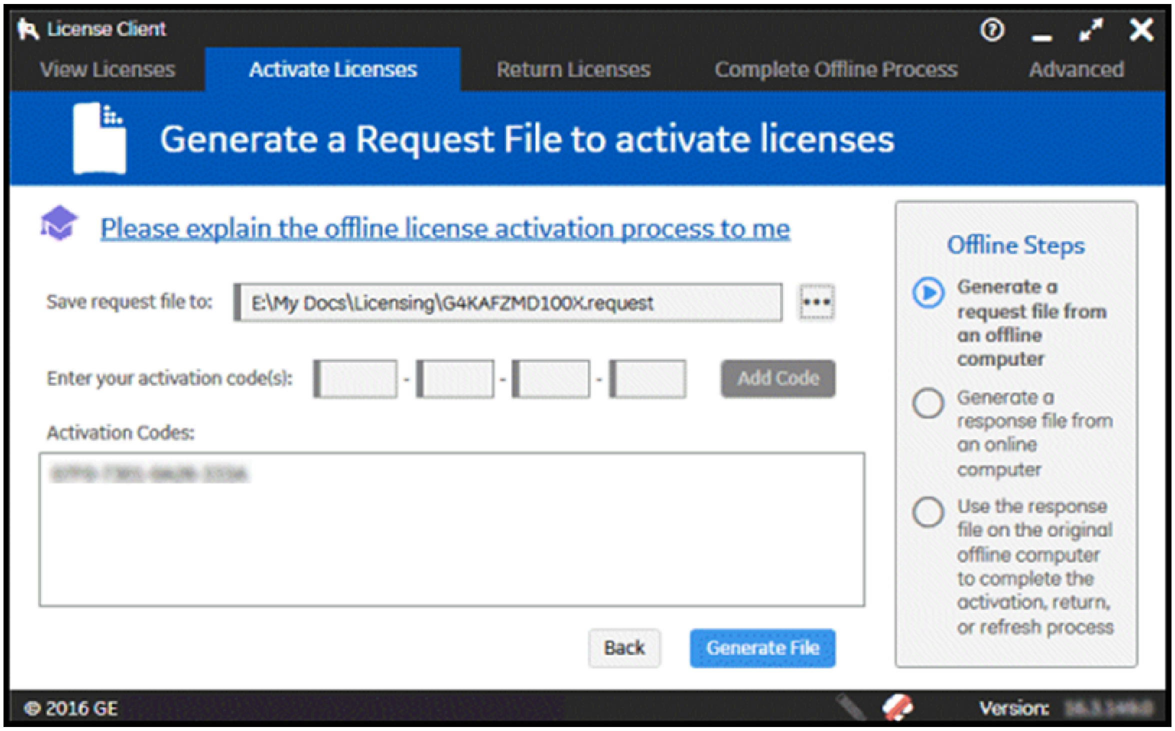
2 Yes, for this computer from a local license server

3 Yes, for the inserted Hardware Key

4 Yes, for a permanently offline computer

5 No, I want to do something else

2. Select **Yes, for a permanently offline computer**. The **Generate a Request File to activate licenses** page appears.


License Client
View Licenses
Activate Licenses
Return Licenses
Complete Offline Process
Advanced
Generate a Request File to activate licenses
Please explain the offline license activation process to me
Add Code
Back
Generate File
Offline Steps
Generate a request file from an offline computer
Generate a response file from an online computer
Use the response file on the original offline computer to complete the activation, return, or refresh process
© 2016 GE

Save request file to: E:\My Docs\Licensing\G4KAFZMD100X.request

Enter your activation code(s): - - -

Activation Codes:

[redacted]

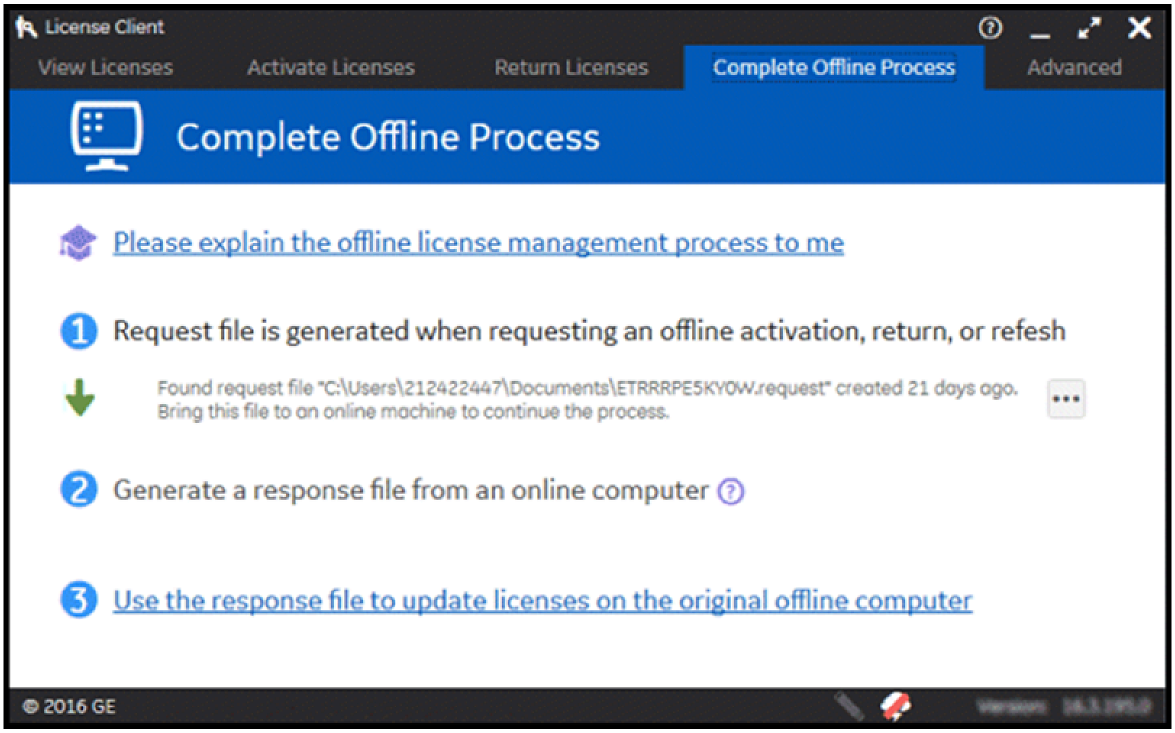
Version: [redacted]

3. Browse to the media device or the network location where the request file is saved.
4. Enter each activation code and select **Add Code** to add it to the Activation Codes area.

> **Note:**
>
> You can find the activation code(s) in your GE order e-mail.

5. Select **Generate File** to create and save a request file to the specified location.

6. The **Complete Offline Process** page appears. A message appears indicating the request file location and when it was created.



Complete Offline Process

Please explain the offline license management process to me

1 Request file is generated when requesting an offline activation, return, or refesh

Found request file "C:\Users\212422447\Documents\ETRRRPE5KY0W.request" created 21 days ago. Bring this file to an online machine to continue the process.

2 Generate a response file from an online computer

3 Use the response file to update licenses on the original offline computer

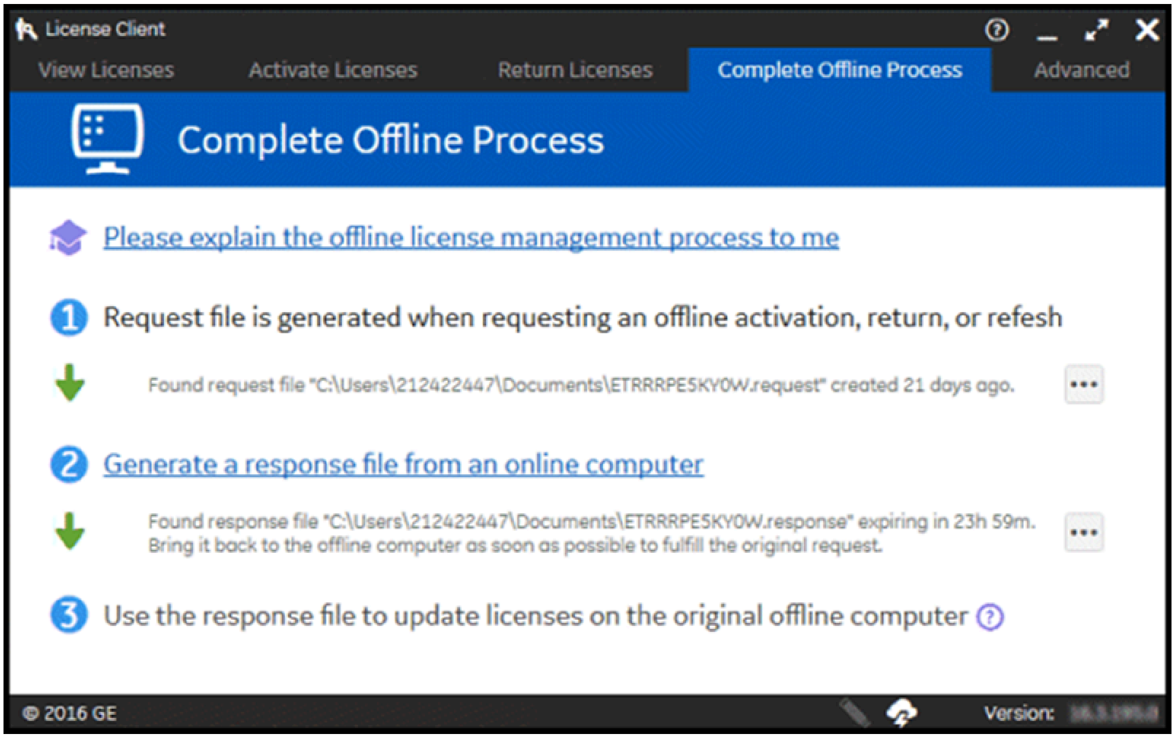
© 2016 GE

[illegible]

Generating a Response File

Collect the request file from the offline computer and then generate a response file from an online computer.

1. Select **Complete Offline Process**. The **Complete Offline Process** page appears. A message appears indicating the response file location and when it expires.



Complete Offline Process

Please explain the offline license management process to me

1 Request file is generated when requesting an offline activation, return, or refesh

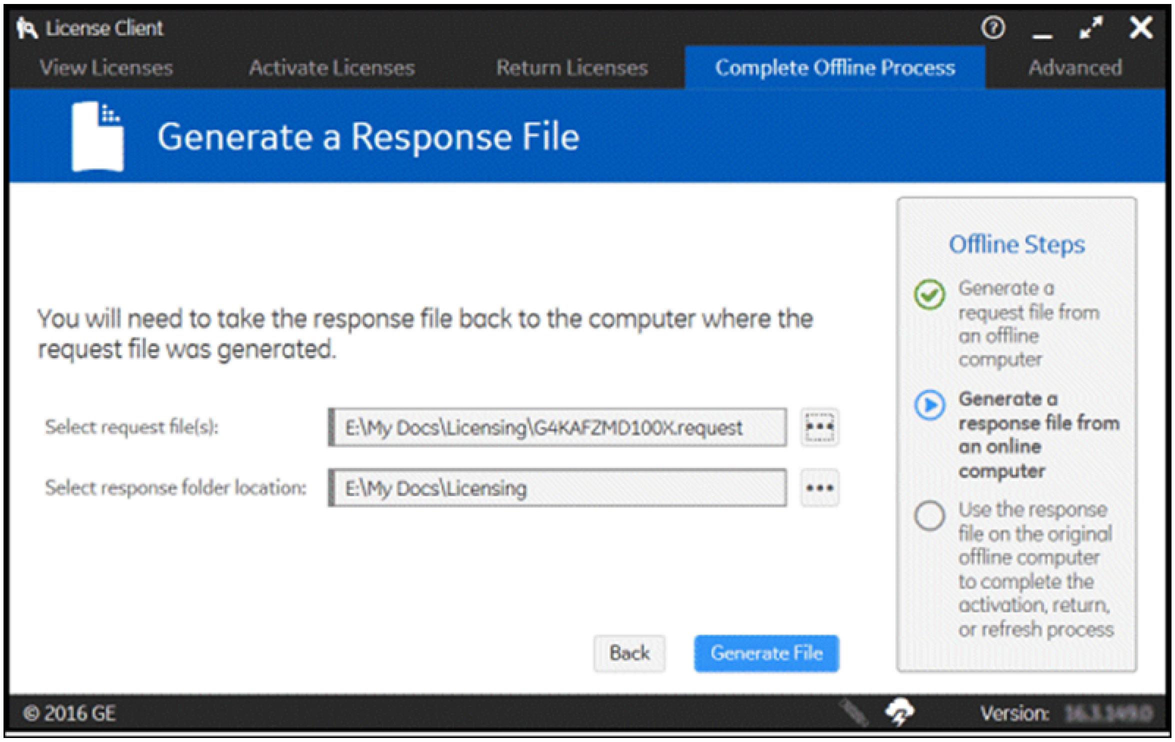
Found request file "C:\Users\212422447\Documents\ETRRRPE5KY0W.request" created 21 days ago.

2 Generate a response file from an online computer

Found response file "C:\Users\212422447\Documents\ETRRRPE5KY0W.response" expiring in 23h 59m. Bring it back to the offline computer as soon as possible to fulfill the original request.

3 Use the response file to update licenses on the original offline computer

2. Select **Generate a response file from an online computer**. The **Generate a Response File** page appears.



Generate a Response File

You will need to take the response file back to the computer where the request file was generated.

Select request file(s): E:\My Docs\Licensing\G4KAFZMD100X.request

Select response folder location: E:\My Docs\Licensing

Offline Steps

- Generate a request file from an offline computer
- Generate a response file from an online computer
- Use the response file on the original offline computer to complete the activation, return, or refresh process

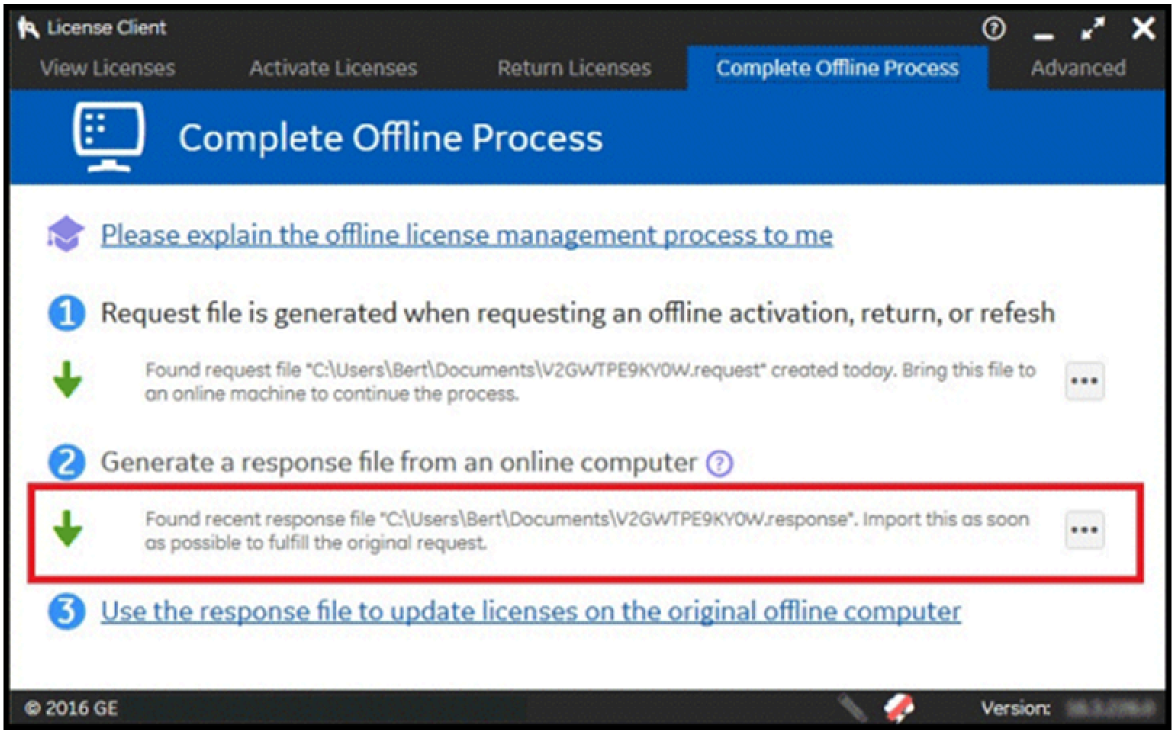
3. If necessary, insert the media device into the computer.
4. Select the request file and response folder location, then select **Generate File**. The response file is generated and saved to the specified location on a media device or network drive that can be accessed by the offline computer.

> **Note:**
> The response file expires 24 hours after being created. The application indicates the time remaining before the response file expires.

Activating Licenses

After generating a request file from your offline computer and a response file from an online computer, you can activate licenses on the offline computer.

1. On the **Complete Offline Process** page, select **Use the response file to update licenses on the original offline computer**.



1 Request file is generated when requesting an offline activation, return, or refesh

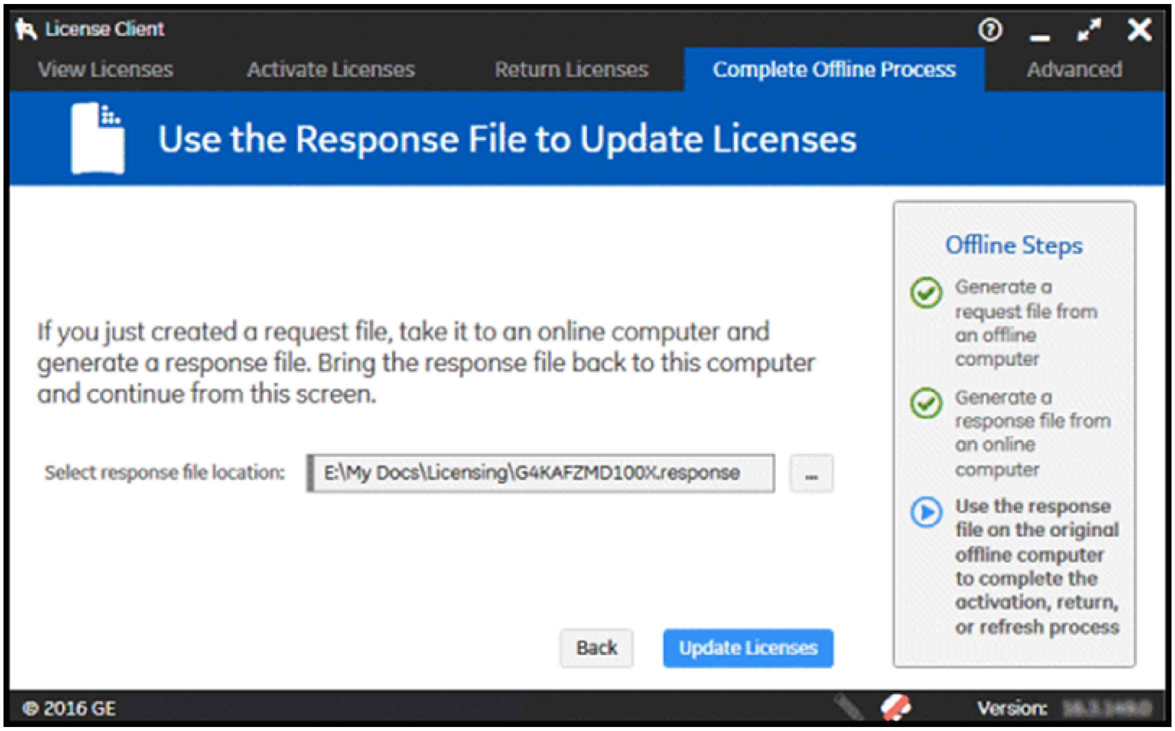
Found request file "C:\Users\Bert\Documents\V2GWTPE9KY0W.request" created today. Bring this file to an online machine to continue the process.

2 Generate a response file from an online computer

Found recent response file "C:\Users\Bert\Documents\V2GWTPE9KY0W.response". Import this as soon as possible to fulfill the original request.

3 Use the response file to update licenses on the original offline computer

The **Use the Response File to Update Licenses** page appears.



Use the Response File to Update Licenses

If you just created a request file, take it to an online computer and generate a response file. Bring the response file back to this computer and continue from this screen.

Select response file location: E:\My Docs\Licensing\G4KAFZMD100X.response

Offline Steps

- ✓ Generate a request file from an offline computer
- ✓ Generate a response file from an online computer
- ▶ Use the response file on the original offline computer to complete the activation, return, or refresh process

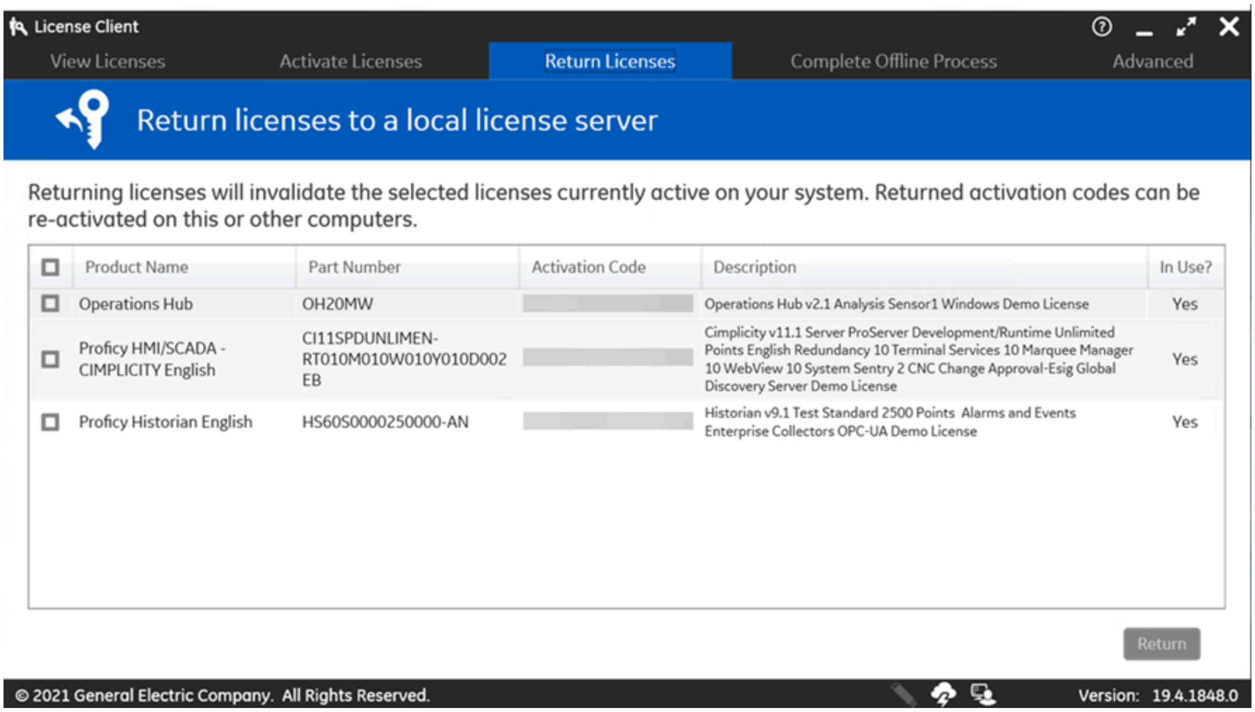
2. If necessary, insert the media device with the response file into the computer.
3. Browse to the location of the response file, and select the file.
4. Select **Update Licenses**.

Note:
After the response file is imported, the response file extension is modified to "response_imported".

Step 4: Returning Licenses

You can return your licenses for time being and re-activate them later. You can also re-active your licenses on a different computer using License Client.

The **Return Licenses** tab in License Client is used to return licenses from your computer (physical machine or virtual machine).



Return licenses to a local license server

Returning licenses will invalidate the selected licenses currently active on your system. Returned activation codes can be re-activated on this or other computers.

□	Product Name	Part Number	Activation Code	Description	In Use?
□	Operations Hub	OH20MW	[redacted]	Operations Hub v2.1 Analysis Sensor1 Windows Demo License	Yes
□	Proficy HMI/SCADA - CIMPLICITY English	CI11SPDUNLIMEN-RT010M010W010Y010D002EB	[redacted]	Cimplicity v11.1 Server ProServer Development/Runtime Unlimited Points English Redundancy 10 Terminal Services 10 Marquee Manager 10 WebView 10 System Sentry 2 CNC Change Approval-Esig Global Discovery Server Demo License	Yes
□	Proficy Historian English	HS60S0000250000-AN	[redacted]	Historian v9.1 Test Standard 2500 Points Alarms and Events Enterprise Collectors OPC-UA Demo License	Yes

© 2021 General Electric Company. All Rights Reserved.

Version: 19.4.1848.0

Following are the steps for returning your licenses if your computer is connected to a Local License Server, or to the GE Cloud License Server, or a computer with a GE USB Hardware key:

1. In License Client, select **Return Licenses**.
2. The return licenses server page displays information for each license on your computer.
3. Select the check box for each license to return, and then select **Return**.

Note:
The **Activate Licenses** tab appears, indicating that licenses have been successfully returned to your respective license server.

Following are the steps for returning your licenses if your computer is offline, that is your computer is not connected to the internet:

1. Generate a request file from the offline computer. Send the request file to the online computer.
2. From an online computer, send the request file to the GE cloud license server and generate a response file.
3. Send the response file to the offline computer and return the licenses.

Generating a Request File

Note:
Generate a request file from an online computer before returning licenses from an offline computer.

1. On the offline computer, in License Client, select the **Return Licenses** tab. The License Client detects that the client computer is not connected to the internet.
2. The **Generate a Request File to return licenses** page appears.
3. Select the licenses to be returned.
4. Browse the location where you want to save the request file.
5. Save the license request file to a device or network drive that can be accessed by the online computer.
6. If you are using a portable media device, remove it and return to the online computer.

Generating a Response File

Note:
Generate a response file from an online computer before returning licenses from an offline computer.

1. Select **Complete Offline Process**. The **Complete Offline Process** page appears. A message appears indicating the response file location and when it expires.
2. Select **Generate a response file from an online computer**. The **Generate a Response File** page appears.
3. If necessary, insert the media device into the computer.
4. Select the request file(s) and response folder location, then select **Generate File**. The response file is generated and saved to the specified location on a media device or network drive that can be accessed by the offline computer.

   Note:
   The response file expires 24 hours after being created. The application indicates the time remaining before the response file expires.

5. If you are using a portable media device to store the response file, remove it and return to the offline computer.

Returning a License

After generating a request file from your offline computer and a response file from an online computer, you can return licenses from the offline computer.

1. On the **Complete Offline Process** page, select **Use the response file to update licenses on the original offline computer**. The **Use the Response File to Update Licenses** page appears.
2. If necessary, insert the media device with the response file into the computer.
3. Browse the location of the response file, and select the file.
4. Select **Return License**.

> **Note:**
> After the response file is imported, the response file extension is modified to "response_imported".

Reconcile Device ID with Tolerant ID

Reconcile Device ID with Tolerant ID

If your device ID changes, you may face some issues with your GE product licenses. You must perform the reconcile operation to make your device ID tolerant against any further changes to the device ID.

Follow the below important notes on Common Licensing software version requirements.

> **Note:**
>
> - If you are installing Common Licensing software for the first time in your computer, then your device ID will be tolerant when you install Common Licensing version 19.4 or higher and reconcile operation is not required.
> - If you are already using Common Licensing software in your computer, you must upgrade to Common Licensing version 19.4 or higher, and run the reconcile operation to make your device ID tolerant.

The reconcile operation is required to:

- Avoid any license issues when the device ID changes
- Run your activated licenses seamlessly and more efficiently.

Note:

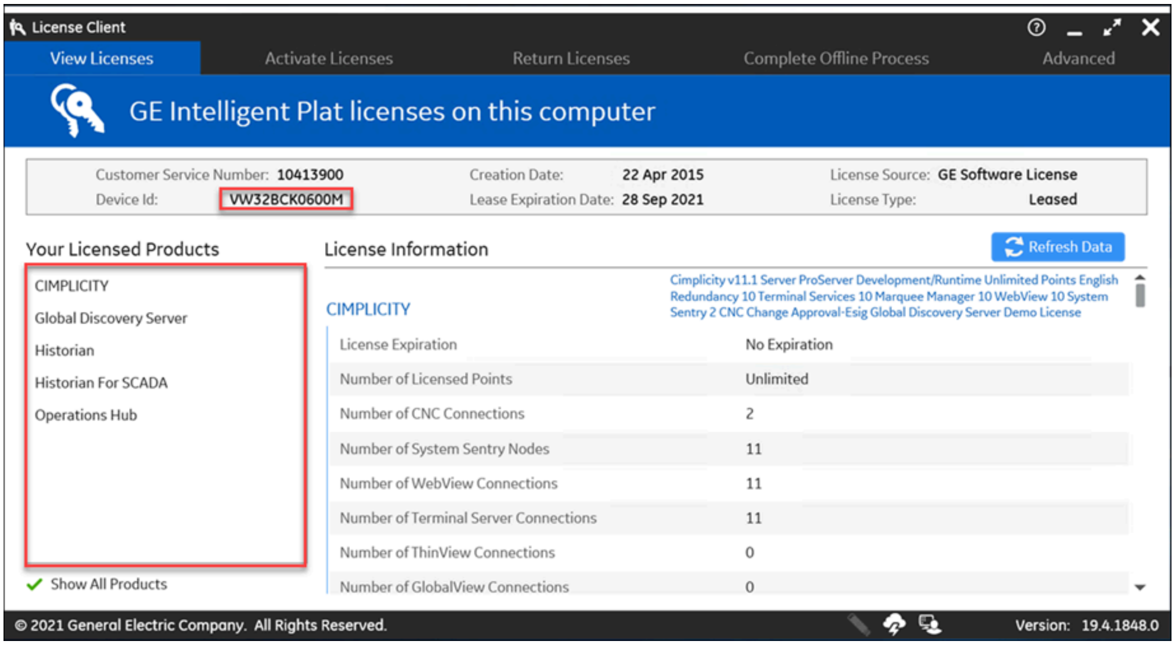
Perform the reconcile operation, to ensure your device ID is tolerant even if your computer device ID is intact and not changed.

Before you begin with your reconcile operation:

- You must not use the GE products while reconciling the device ID.
- If you are not connected to GE Cloud Server, you must return the existing licenses offline before the reconcile operation. However, if you are connected to GE Cloud Server, the existing licenses are automatically returned when you reconcile the device ID.

Following are the steps for reconciliation of your device ID with new tolerant device ID:

1. In License Client, select **View Licenses** tab. The activated licenses are already mapped to 12 characters device ID.



Customer Service Number: 10413900
Device Id: VW32BCK0600M
Creation Date: 22 Apr 2015
Lease Expiration Date: 28 Sep 2021
License Source: GE Software License
License Type: Leased

CIMPLICITY
Global Discovery Server
Historian
Historian For SCADA
Operations Hub

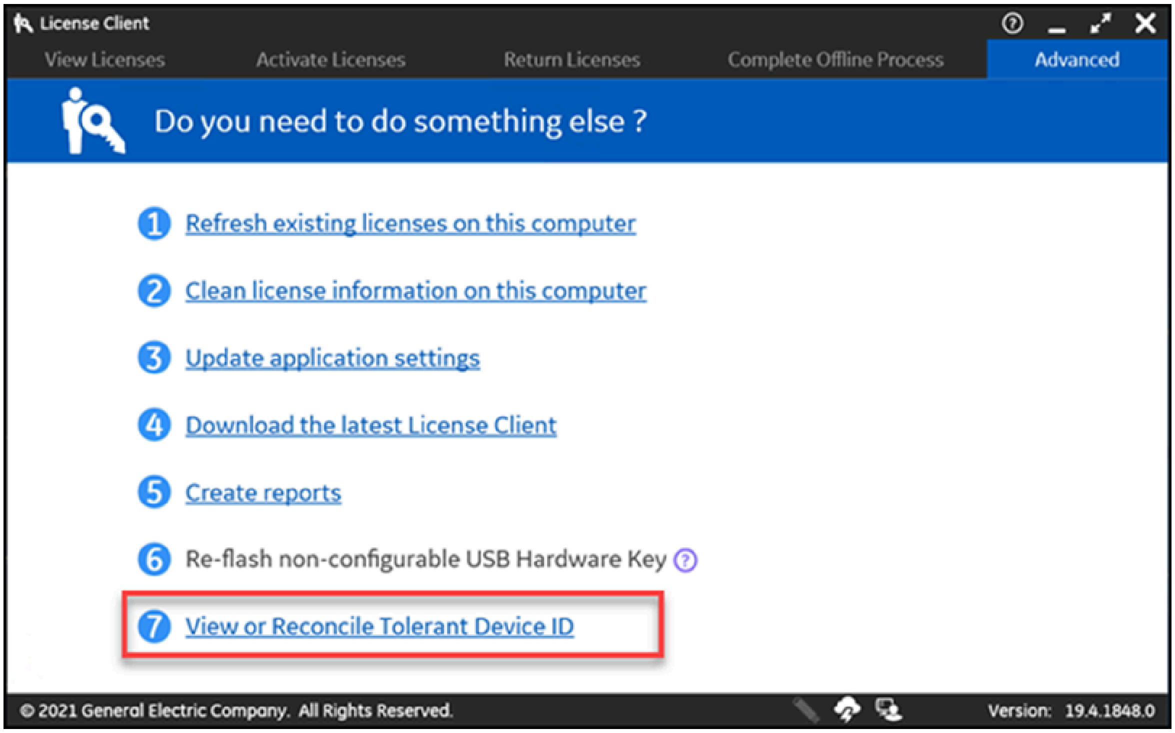
CIMPLICITY

Cimplicity v11.1 Server ProServer Development/Runtime Unlimited Points English Redundancy 10 Terminal Services 10 Marquee Manager 10 WebView 10 System Sentry 2 CNC Change Approval-Esig Global Discovery Server Demo License

License Expiration	No Expiration
Number of Licensed Points	Unlimited
Number of CNC Connections	2
Number of System Sentry Nodes	11
Number of WebView Connections	11
Number of Terminal Server Connections	11
Number of ThinView Connections	0
Number of GlobalView Connections	0

Version: 19.4.1848.0

2. Select **Advanced** tab, and then select **View or Reconcile Tolerant Device ID**.

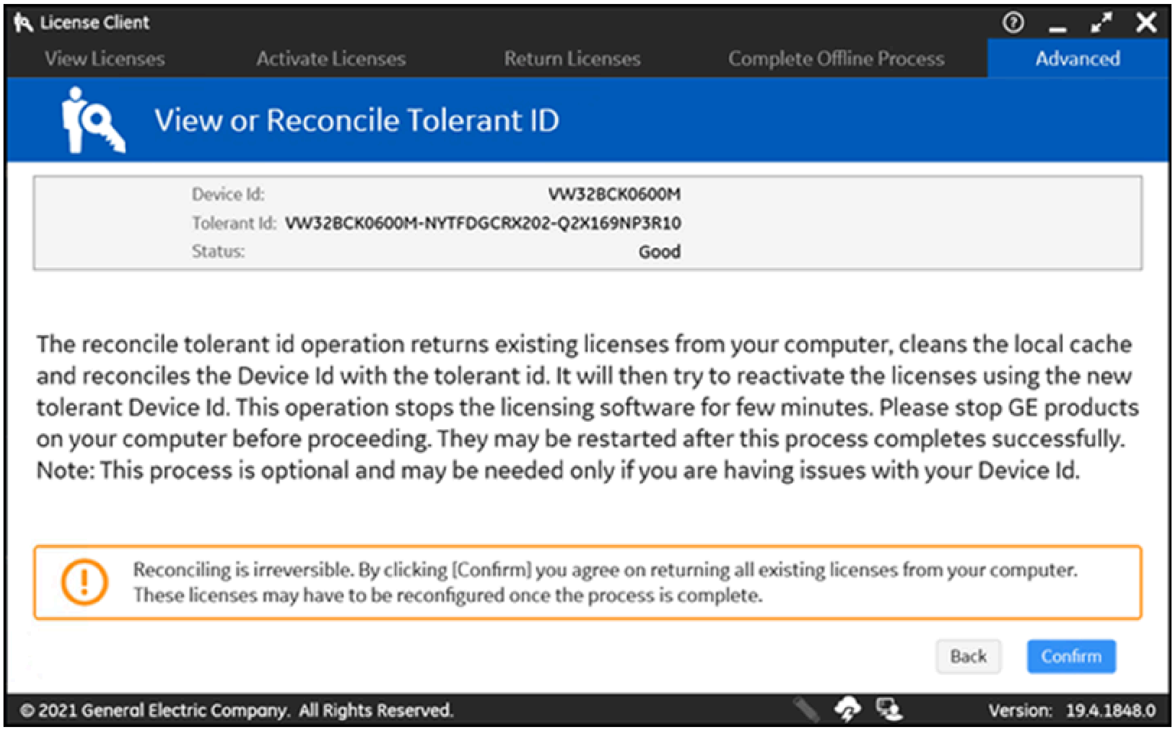


Do you need to do something else ?

1. Refresh existing licenses on this computer
2. Clean license information on this computer
3. Update application settings
4. Download the latest License Client
5. Create reports
6. Re-flash non-configurable USB Hardware Key
7. View or Reconcile Tolerant Device ID

© 2021 General Electric Company. All Rights Reserved. Version: 19.4.1848.0

3. Select the **Confirm** button to start your reconciling operation.



View or Reconcile Tolerant ID

Device Id: VW32BCK0600M
Tolerant Id: VW32BCK0600M-NYTFDGCRX202-Q2X169NP3R10
Status: Good

The reconcile tolerant id operation returns existing licenses from your computer, cleans the local cache and reconciles the Device Id with the tolerant id. It will then try to reactivate the licenses using the new tolerant Device Id. This operation stops the licensing software for few minutes. Please stop GE products on your computer before proceeding. They may be restarted after this process completes successfully. Note: This process is optional and may be needed only if you are having issues with your Device Id.

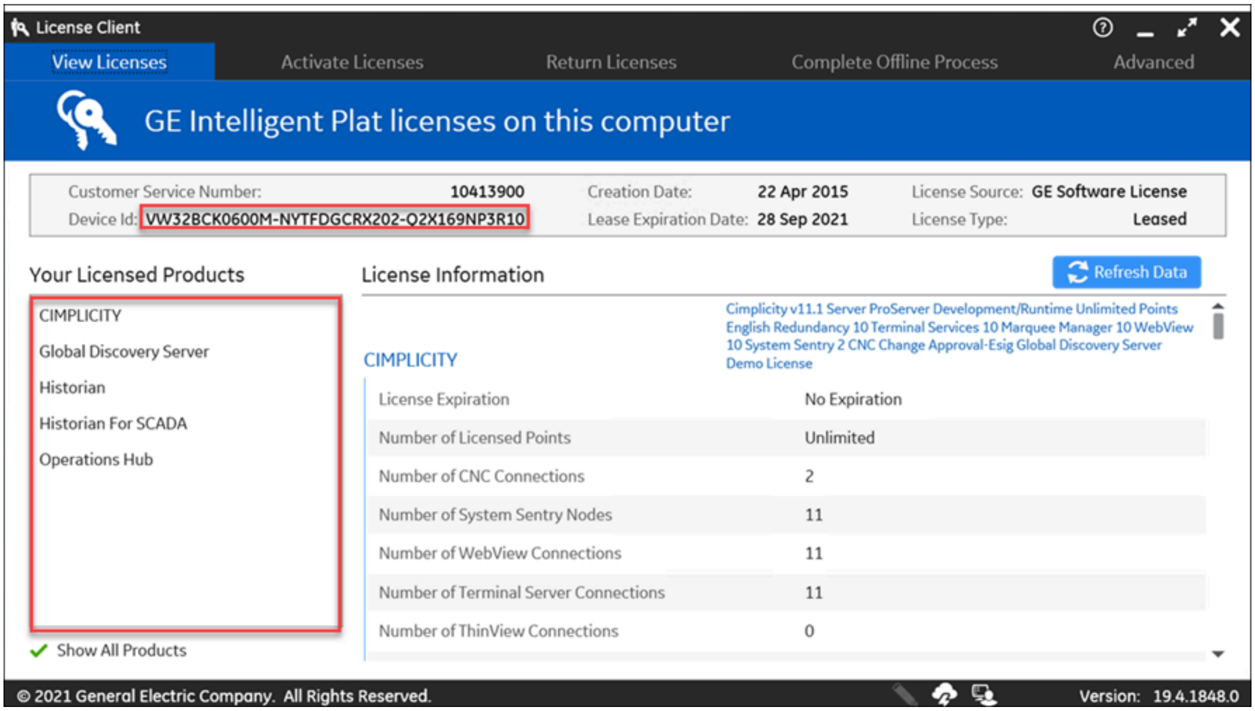
Reconciling is irreversible. By clicking [Confirm] you agree on returning all existing licenses from your computer. These licenses may have to be reconfigured once the process is complete.

© 2021 General Electric Company. All Rights Reserved. Version: 19.4.1848.0

Note:

After the reconcile operation, the 12 characters of existing device ID will change to 36 characters.

In the **View Licenses** tab, you will see that your licenses are still valid and are now mapped to 36 characters device ID.



Customer Service Number:	10413900	Creation Date:	22 Apr 2015	License Source:	GE Software License
Device Id:	VW32BCK0600M-NYTFDGCRX202-Q2X169NP3R10	Lease Expiration Date:	28 Sep 2021	License Type:	Leased

Your Licensed Products

- CIMPLICITY
- Global Discovery Server
- Historian
- Historian For SCADA
- Operations Hub

License Information

CIMPLICITY

Cimplicity v11.1 Server ProServer Development/Runtime Unlimited Points English Redundancy 10 Terminal Services 10 Marquee Manager 10 WebView 10 System Sentry 2 CNC Change Approval-Esig Global Discovery Server Demo License

License Expiration	No Expiration
Number of Licensed Points	Unlimited
Number of CNC Connections	2
Number of System Sentry Nodes	11
Number of WebView Connections	11
Number of Terminal Server Connections	11
Number of ThinView Connections	0

Chapter 6. Manage SSL Certificate to Secure CIMPLICITY Web Clients

Self Signed SSL Certificate

Generate Self Signed SSL Certificate to Secure CIMPLICITY Web Clients

The CIMPLICITY web clients are secured through an SSL certificate.

The SSL certificate is generated through the config_service_cert batch file, which is executed during the CIMPLICITY installation process.

> **Note:**
> When you launch CIMPLICITY web client, the browser validates the domain name provided in the URL with the value of the USERDNSDOMAIN environment variable.

If the USERDNSDOMAIN environment variable is unavailable, the connection to the CIMPLICITY web client is not secure. To make the connection secure, replace the domain name in the URL with the computer name.

For more information on how to regenerate a self signed SSL certificate, and update its validity, see the following topics:

- Regenerate the Self Signed SSL Certificate *(on page 94)*
- Update validity of the Self Signed SSL Certificate *(on page 95)*

Regenerate the Self Signed SSL Certificate

The default validity of an SSL certificate is 2 years. You can use the below steps to regenerate the self signed SSL certificate.

You must know the following parameters:

- <**InstallationPath**>: The installation directory of Proficy CIMPLICITY.
- <**ConfigServicePortNumber**>: Port number for the CIMPLICITY Configuration Service (typically 4955).
- <**UABrowseServicePortNumber**>: Port number for the UA Browse Service (typically 4956).
- <**RootCertificateName**>: The name of the root certificate file without the extension.
- <**ServerCetificateName**>: The name of the Server certificate/key files without the extensions.

Note:
The default value of ServerCertificateName is server_cert. To use a different file name, update the variables ssl_certificate and ssl_certificate_key in the httpd.conf file with the new values and restart the CIMPLICITY HTTPD Service.

- <**Passphrase**>: Passphrase used to protect the generated Server certificate file.

Important:
Go to the path where CIMPLICITY is installed, and delete the **ScadaConfigPki** folder containing the installed SSL certificates.

1. Open the command prompt.
2. In the command prompt, navigate to the path where CIMPLICITY is installed.

   ```
   Example: cd C:\Program Files (x86)\Proficy\Proficy CIMPLICITY
   ```

3. Enter the following command in the command prompt:

   ```
   config_service_cert.bat <InstallationPath> <ConfigServicePortNumber> <UABrowseServicePortNumber>
    <RootCertificateName> <ServerCertificateName> <passphrase>
   ```

   ```
   Example: config_service_cert.bat "C:\Program Files (x86)\Proficy\Proficy CIMPLICITY\" 4855 4865
    CimScadaConfigRootCA server_cert cimplicity
   ```

   The SSL certificate is now regenerated.

Update validity of the Self Signed SSL Certificate

The default validity of an SSL certificate is 2 years.

You can update the validity of the SSL certificate by applying the following steps:

1. Access the config_service_cert batch file.
2. Update the number of days for which the SSL certificate should be valid in the following occurrences in the batch file:

   ```
   REM create the rootCA certificate
   %1\OpenSSL\openssl x509 -req -sha256 -extfile %rootCfgFileName% -days <validity period in days> -signkey
    %rootKeyFileName% -in %rootCsrFileName% -out %rootCrtFileName%
   ```

```
REM create the server certificate
%1\OpenSSL\openssl x509 -req -sha256 -extfile %serverCfgFileName% -days <validity period in days> -CA
 %rootCrtFileName% -CAkey %rootKeyFileName% -CAserial %serverSerialFileName% -in %serverCsrFileName% -out
 %serverCrtFileName%
```

The validity of the SSL certificate is now updated.

External CA signed SSL Certificate

Generate SSL Certificate Using an External Certificate Authority

Following are the three main steps required to get an SSL certificate from an external Certificate Authority (CA) and use it with CIMPLICITY. Follow these steps when requesting the initial certificate and when renewing the certificate when it expires.

1. Generate the Certificate Signing Request (CSR)
2. Send the CSR to the CA and get the resulting server SSL certificate
3. Process the SSL certificate for use in CIMPLICITY

Before you begin, you must know the following parameters:

- <**InstallationPath**>: The installation directory of Proficy CIMPLICITY.
- <**CrtFileName**>: The name of the certificate/key files without the extensions.
- <**ConfigServicePortNumber**>: Port number for the CIMPLICITY Configuration Service (typically 4955).
- <**UABrowseServicePortNumber**>: Port number for the UA Browse Service (typically 4956).
- <**WsmServicePortNumber**>: Port number for the Webspace Session Management Service (typically 4957).
- <**KeyPassPhraseFilePath**>: Path to the pass phrase file protecting the .key file.
- <**PfxPassPhrase**>: Pass phrase used to protect the generated .pfx file. This is the pass phrase itself, not a path to a pass phrase file.
- <**CSRCertificateName**>: The name of the CSR certificate/key files without the extensions.
- <**ServerCetificateName**>: The name of the Server certificate/key files without the extensions.

> **Note:**
> The default value of ServerCertificateName is server_cert. To use a different file name, update the variables ssl_certificate and ssl_certificate_key in the httpd.conf file with the new values and restart the CIMPLICITY HTTPD Service.

To generate the SSL certificate, perform the following steps:

1. **Generate CSR**

    a. Open the command prompt.

    b. In the command prompt, navigate to the path where **Generate_CSR.bat** is saved.

    ```
    Example: cd C:\Program Files (x86)\Proficy\Proficy CIMPLICITY\exe
    ```

    c. Enter the following command in the command prompt.

    ```
    Generate_CSR.bat <InstallationPath> <CSRCertificateName> <PassPhraseFilePath(optional)>
    ```

    ```
    Example: Generate_CSR.bat “c:\Program Files (x86)\Proficy\Proficy CIMPLICITY” server_cert
    ```

    d. Optional: To secure the private key with a password, add a password to a text file and save the file. Provide the file path in the command.

    ```
    Example: Generate_CSR.bat “c:\Program Files (x86)\Proficy\Proficy CIMPLICITY” server_cert

     “c:\Passwords\password.txt”
    ```

    e. If the certificate signing request (.crt) file or the private key (.key) file already exists in the specified folder, you are notified and prompted to delete the files. Select **Y** to delete the existing files and create new files. Select **N** to exit.

    f. Enter the following details:

        - Country Name (2 letter code) [AU]
        - State or Province Name (full name) [Some-State]
        - Locality Name (eg, city) [Some-City]
        - Organization Name (eg, company) [Internet Widgits Pty Ltd]
        - Organizational Unit Name (eg, section) []:
        - Common Name (e.g. server FQDN or YOUR name) []
        - Email Address []
        - A challenge password []
        - An optional company name []:

    g. Press Enter.

    The certificate signing request (.crt) file and the private key (.key) file are generated in the **ScadaConfigPki** folder in the installation path. (Example: **C:\Program Files (x86)\Proficy \Proficy CIMPLICITY\ScadaConfigPki**).

2. **Obtain SSL Certificate**

   a. Send the certificate signing request (.csr) file to an external Certificate Authority (CA), such as VeriSign or DigiCert, and request for a CA certificate.
   b. Save the certificate in the **ScadaConfigPki** folder.

3. **Process SSL certificate**
   a. Open the command prompt.
   b. In the command prompt, navigate to the path where **process_server_cert.bat** is saved.

   ```
   Example: cd C:\Program Files (x86)\Proficy\Proficy CIMPLICITY\exe
   ```

   c. Enter the following command in the command prompt.

   ```
   process_server_cert.bat <InstallationPath> <CrtFileName> <ConfigServicePortNumber>
    <UABrowseServicePortNumber>  <KeyPassPhraseFilePath> <PfxPassPhrase> <WsmServicePortNumber>
   ```

   ```
   Example: process_server_cert.bat “c:\Program Files (x86)\Proficy\Proficy CIMPLICITY” server_cert 4955
    4956 c:\passwords\password.txt secret-pass-phrase 4957
   ```

Install SSL Certificate on a Viewer or Remote Machine

On CIMPLICITY Server:

1. Navigate to `<Installation_Path>\Proficy\Proficy CIMPLICITY\ScadaConfigPki`.
2. Copy the root certificate `CimScadaConfigRootCA.crt` from CIMPLICITY server to a Viewer/Remote machine. This is a manual step.

On Viewer/Remote Machine:

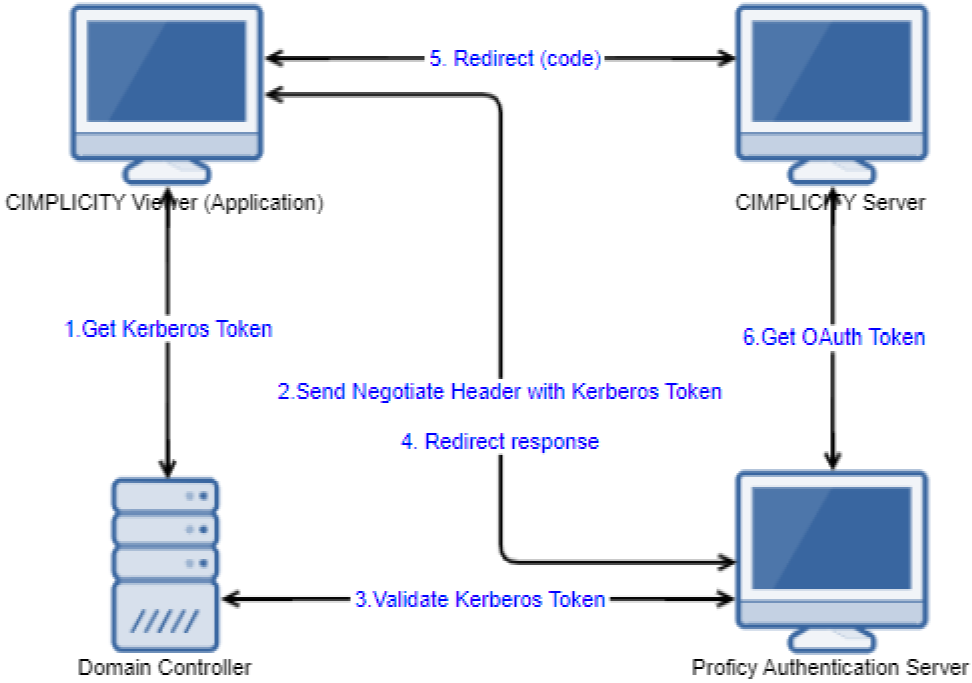
1. Right-click the certificate file copied from CIMPLICITY server, and select **Install Certificate**.
2. Select the **Store Location** as **Local Machine**.
3. Select **Place all certificates in the following store**.
4. Select **Browse**, and then select **Trusted Root Certification Authorities** folder.
5. Select **OK**, and then select **Next**.
6. Select **Finish**. The certificate is imported.

Chapter 7. Windows Auto-login Configuration

Autologin Configuration Checklist

CIMPLICITY supports Windows Autologin functionality to connect to Proficy Authentication server in a domain-based environment. You can use this topic as a checklist to know how Autologin feature in CIMPLICITY works. For more detailed information on Proficy Authentication, it is recommended that you read the Proficy Authentication help at https://www.ge.com/digital/documentation/uaa/version2023/index.html.

Proficy Authentication works based on Kerberos authentication protocol to authenticate Windows user. Since Kerberos authentication works only in a domain-based environment, to deploy and configure Autologin, you must at least need three nodes to get the Kerberos authentication working. The following image is an example of a typical configuration.


5. Redirect (code)
CIMPLICITY Viewer (Application)
CIMPLICITY Server
1.Get Kerberos Token
6.Get OAuth Token
2.Send Negotiate Header with Kerberos Token
4. Redirect response
3.Validate Kerberos Token
Domain Controller
Proficy Authentication Server

The following table lists the configuration that must be performed to get the Autologin functionality working:

Node	Configuration	Description
CIMPLICITY Nodes	Configure Security Policy	Ensure that correct encryption types are associated to Kerberos authentication is selected.

Node	Configuration	Description
		1. To access Local Security Policy, enter `secpol.msc` in Windows Run dialog and select **OK**. 2. Navigate to **Security Settings** > **Local Policies** > **Security Options**. 3. Double-click and open `Network security: Configure encryption types allowed for Kerberos` security policy setting. 4. Select the valid encryption types that you want to use. Ensure that the selection is same across all the nodes. Encryption types allowed for Kerberos: AES256_HMAC_SHA1 Configure Proficy Authentication on CIMPLICITY server *(on page 107)*. **Note:** • Ensure that the fully qualified domain name is specified in Proficy authentication server configuration

Node	Configuration	Description
		- Ensure that the required security groups are published.
Domain Controller	Configure Security Policy	Ensure that correct encryption types are associated to Kerberos authentication is selected. 1. To access Local Security Policy, enter `secpol.msc` in Windows Run dialog and select **OK**. 2. Navigate to **Security Settings** > **Local Policies** > **Security Options**. 3. Double-click and open `Network security: Configure encryption types allowed for Kerberos` security policy setting. 4. Select the valid encryption types that you want to use. Ensure that the selection is same across all the nodes.
	Create Service Principal Name	Before you begin, ensure that you have performed the following: - Created a dummy user account on the Active Directory Server node to represent the Proficy Authenti-

Node	Configuration	Description
		cation application in the active directory registry. • Configured Security Policy. To perform this task, you must be an administrator. 1. Log in to your Active Directory machine. 2. Open the Windows Command Prompt application. 3. Run the following command replacing with the appropriate code: `setspn -S HTTP/<FQDN> <user account>` <FQDN>- Fully Qualified Domain Name (FQDN) of the server on which Proficy Authentication service is running. <user account>- Dedicated user account created for Proficy Authentication service.
	Generate Keytab File	Before you begin, ensure that you have performed the following: • Created Service Principal. To perform this task, you must be an administrator.

Node	Configuration	Description
		1. Log in to your system and open the Windows Command Prompt application. 2. Run the following command replacing with the appropriate code: `ktpass -out <filename> -princ HTTP/<service pincipal name> -mapUser <user account> -mapOp set -pass <password> -crypto AES256-SHA1 -pType KRB5_NT_PRINCIPAL` You can do the following to verify if the service principal is mapped to the dummy account, and a keytab is created: 1. Go to **Active Directory Users and Computers** > **Users**. 2. Access the properties of the user account for which you created the keytab file. 3. On the **Account** tab, verify **User logon name**. is pointing to your service principal name.
Proficy Authentication Server	Configure Security Profile	Ensure that correct encryption types are associated to Kerberos authentication is selected.

Node	Configuration	Description
		1. To access Local Security Policy, enter `secpol.msc` in Windows Run dialog and select **OK**. 2. Navigate to **Security Settings** > **Local Policies** > **Security Options**. 3. Double-click and open `Network security: Configure encryption types allowed for Kerberos` security policy setting. 4. Select the valid encryption types that you want to use. Ensure that the selection is same across all the nodes.
	Configure Proficy Authentication Services	Before you begin, ensure that you have performed the following: • Generated keytab file. • Copied the keytab file from the Active Directory server, and pasted it anywhere on the Proficy Authentication machine. • Noted the keytab file location on the Proficy Authentication machine. To perform this task, you must be an administrator:

Node	Configuration	Description
		1. Log in to the computer machine where Proficy Authentication is installed. 2. Access the `uaa.yml` file. The file is located at `C:\ProgramData\GE\Operations Hub\uaa-config\uaa.yml` 3. To modify, open `uaa.yml` in any text editor. 4. Search for `kerberos` and enter values for the following keys:service-principal and keytab-location 5. Save and close the modified file. 6. Restart the `GE Proficy Authentication Tomcat Web Server` service. a. Access the Windows Run dialog. b. Enter `services.msc` to open the **Services** screen. c. Right-click `GE Proficy Authentication Tomcat Web Server` and select **Restart**.
	Configure LDAP Provider	Add an LDAP provider and make appropriate mappings. Ensure that the logged in user name can work with user filter specified in Proficy Authentication.

Chapter 8. Proficy Authentication Configuration in CIMPLICITY

Best Practices and Limitations

Before you configure Proficy Authentication, ensure to read the best practices that you must follow and some limitations to be considered.

Best Practices

- **CIMPLICITY Webserver Port**

  For the Proficy Authentication to work, CIMPLICITY Webserver must be running on the default port, that is, 9443.

- **Optimal Token Size**

  As a security best practice and to minimize the size of JWT token, ensure that the scopes of the token are relevant with the intended service of that token.

- **Optimal Token Header Size and Group Name**

  Since JWT tokens are generated based on the combination of character length of all the mapped groups, if the character length of the group name exceeds, then the request's header size will also increase. Ensure to keep the group names length within 255 characters.

- **Effective Security Control**

  For effective security control, as an administrator, ensure that you provide the users with the relevant scopes to which they are entitled to. This will limit the users from having access to all Proficy Authentication groups across all the applications and services.

- **Trust the Root Certificate**

  When using Proficy Authentication, ensure that Proficy Authentication root certificate is installed and trusted on all the viewer nodes.

  > **Note:**
  > Once Proficy Authentication is trusted on server, you can find the uaa_root_cert.crt file in the **<Installdirectory>\admin_data\pauth_pki\trusted** folder.

Limitations

- For Proficy Authentication to work, CIMPLICITY project name and Project ID must be same.
- Proficy Authentication supports group names with a length of 255 characters and Apache keeps the header size limited to 8190 bytes. As mentioned in the best practices section, ensure to maintain an optimal token header size.
- Proficy Authentication is not supported for CIMPLICITY Configuration security.
- Configuration of security using Proficy Authentication is not supported.
- To access the screens on Webspace using Proficy Authentication credentials, you must enable Mixed Authentication along with Proficy Authentication in the Project Properties.

Configure Proficy Authentication in CIMPLICITY

Before you begin to configure Proficy Authentication, read the Best Practices and Limitations *(on page 106)* section.

Proficy Authentication provides support for multi-factor authentication. It also provides centralized management of Proficy users and groups, and a common security model across Proficy products.

Note:

- For CIMPLICITY security to work in the network, all the CIMPLICITY nodes must be connected to a same Proficy Authentication server. If you have any previous versions of CIMPLICITY, you can continue to log in to CIMPLICITY 2023 using the existing security users.
- If you are connecting to the CIMPLICITY 2023 Server using the previous version of the CIMPLICITY Viewer, you must set the ONLY_ACCEPT_ENCRYPTED_PWD *(on page)* global parameter value to **N**.

You can use Proficy Authentication in the following scenarios:

- You want to use a common, multi-factor authentication to log in to CIMPLICITY and other Proficy products, regardless if you are using Configuration Hub.
- You installed CIMPLICITY, Configuration Hub, and the Proficy Authentication(UAA) server, and you want to host CIMPLICITY plug-in in Configuration Hub.

To configure and register CIMPLICITY nodes to the Proficy Authentication server, you must initially configure the Proficy Authentication server parameters in CIMPLICITY.

To configure Proficy Authentication in CIMPLICITY, you must do the following:

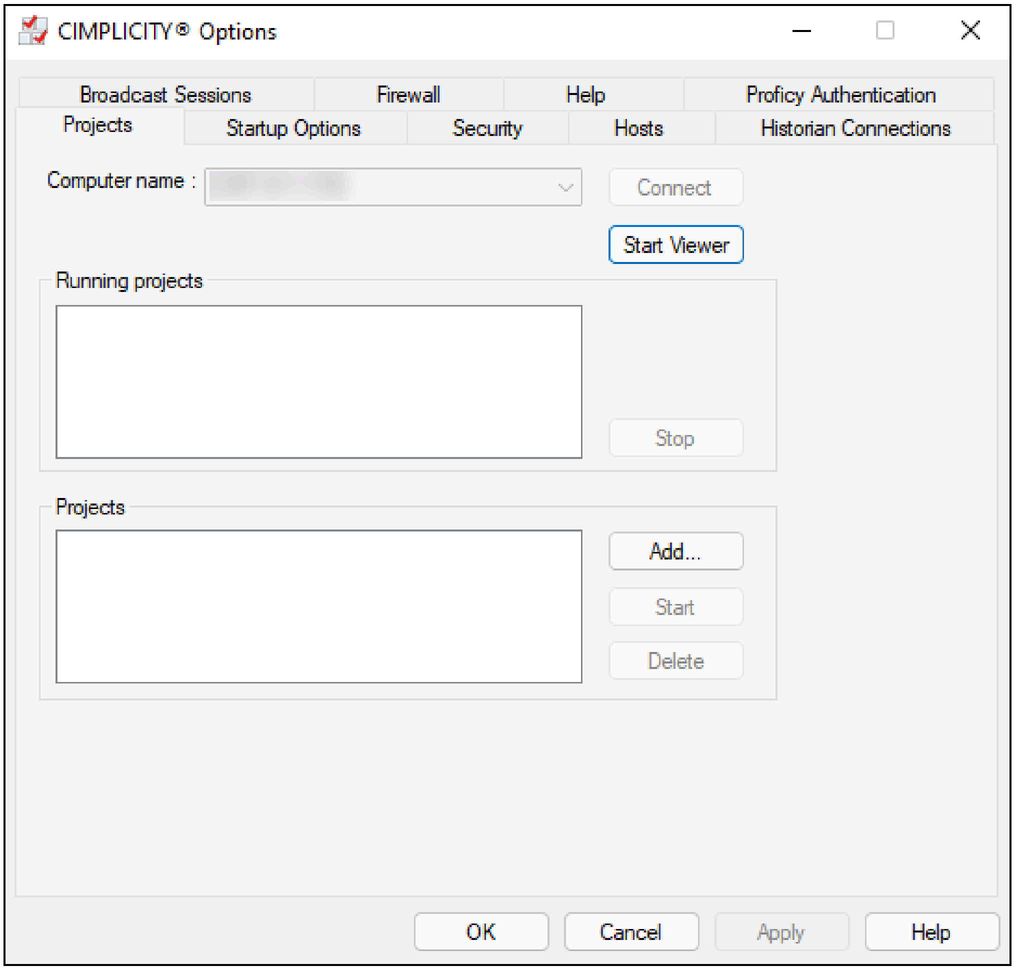
- Configure Proficy Authentication Parameters in CIMPLICITY Options *(on page 108)*.
- Enable and configure Proficy Authentication in Project Properties *(on page 111)*.

Configure Proficy Authentication

To register the Proficy Authentication server in CIMPLICITY, you must configure the Proficy Authentication server details, trust the certificate of the server, and then register.

To configure the Proficy Authentication server in CIMPLICITY, do the following:

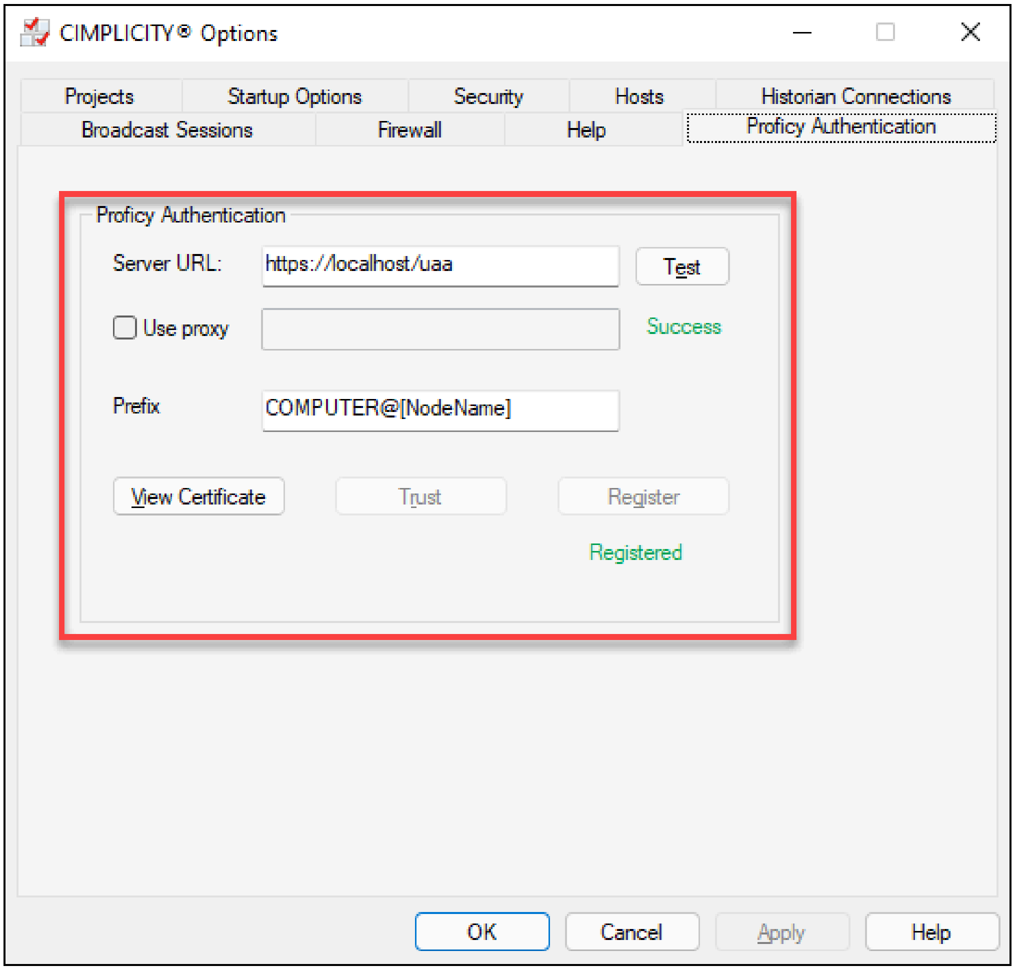
1. Open **CIMPLICITY Options**. For more information on how to open **CIMPLICTIY Options**, see Access CIMPLICITY Options *(on page)*.
   The **CIMPLICITY Options** dialog box opens.



2. In the **CIMPLICITY Options** dialog box, click the **Proficy Authentication** tab.

   The Proficy Authentication options are displayed.

   > **Note:**
   >
   > To access this tab, you must be in administrator mode.



CIMPLICITY® Options

Proficy Authentication

Server URL: https://localhost/uaa

□ Use proxy

Success

Prefix COMPUTER@[NodeName]

Registered

3. Enter the following details:

Options	Description
Server URL	The URL of the Proficy Authentication server to which you want to register. In the <Fully qualified domain name> format.

Options	Description
	You can click the Test button to check the connection status of the Proficy Authentication server. If the connection to the Proficy Authentication server is successful, you will receive a success dialog. If your connection is unsuccessful, retry to connect to another valid Proficy Authentication server.
Use Proxy	Select this check box if you want to use a proxy for the Proficy Authentication server.
Prefix	The prefix for machine/ node level security group in the **COMPUTER@[NodeName]** format. The security group you enter here will be published to the Proficy Authentication server. Only the users mapped to this security group will be able to see the projects associated to the computer/node on Configuration Hub.

4. If the root certificate of the Proficy Authentication server is trusted, you will see Trusted. If not, you will see Not trusted; then you must manually trust the certificate. For more information on how to trust the certificate, refer to the section Trust an Untrusted Certificate while Configuring Proficy Authentication Parameters in CIMPLICITY *(on page 110)*.
5. Click **Register**.

   You will be prompted to enter the Proficy Authentication Client ID and Client Secret.
6. Enter the **Client ID** and **Client Secret**.

   If the entered credentials are valid, the Proficy Authentication server is registered in CIMPLICITY successfully.

Trust an Untrusted Certificate while Configuring Proficy Authentication Parameters in CIMPLICITY

While you register Proficy Authentication server parameters in CIMPLICITY, if CIMPLICITY could not find the Proficy Authentication server's root certificate in the local computer's trusted certificate folder, you can manually trust the certificate.

To manually trust the certificate:

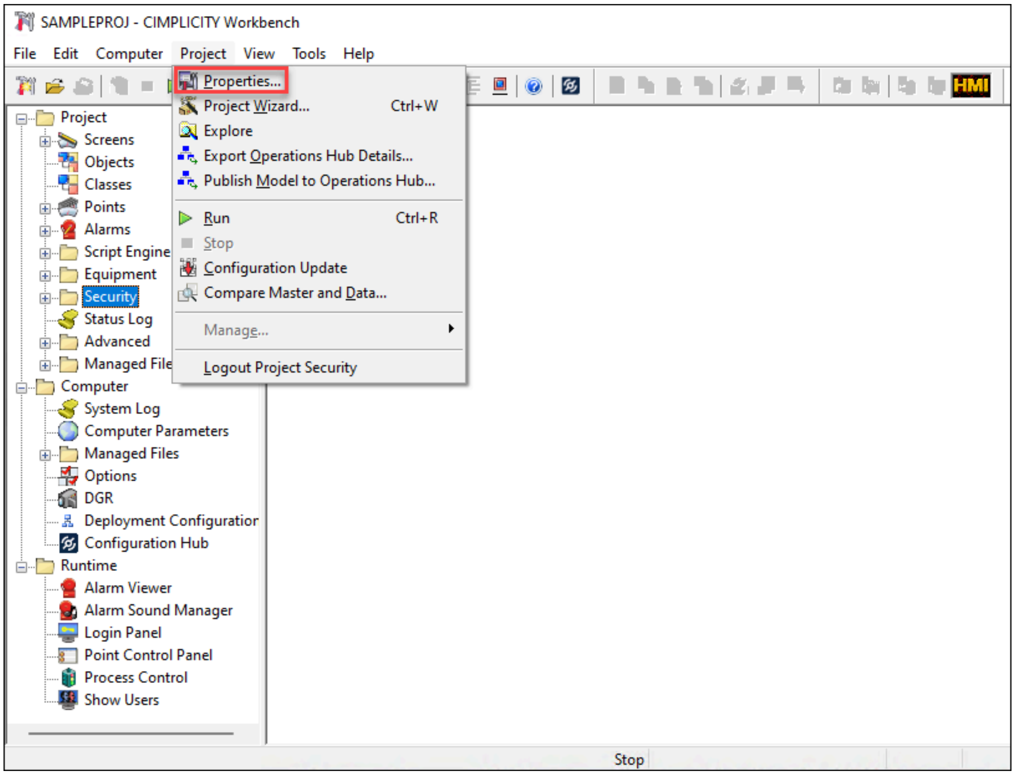
1. In the **CIMPLICITY Options** dialog box > **Proficy Authentication** tab, to view the certificate details, click **View Certificate**.
   The **Certificate Viewer** dialog box opens.
2. If you trust the certificate and want to add the certificate to the trusted folder, click **Trust**. The certificate is added to the local computer's trusted certificate folder. You can now proceed with the CIMPLICITY registration with the Proficy Authentication server.

Enable and configure Proficy Authentication in Project Properties

After you register the Proficy Authentication server in CIMPLICITY, you must enable and configure Proficy Authentication.

To enable and configure the Proficy Authentication, do the following:

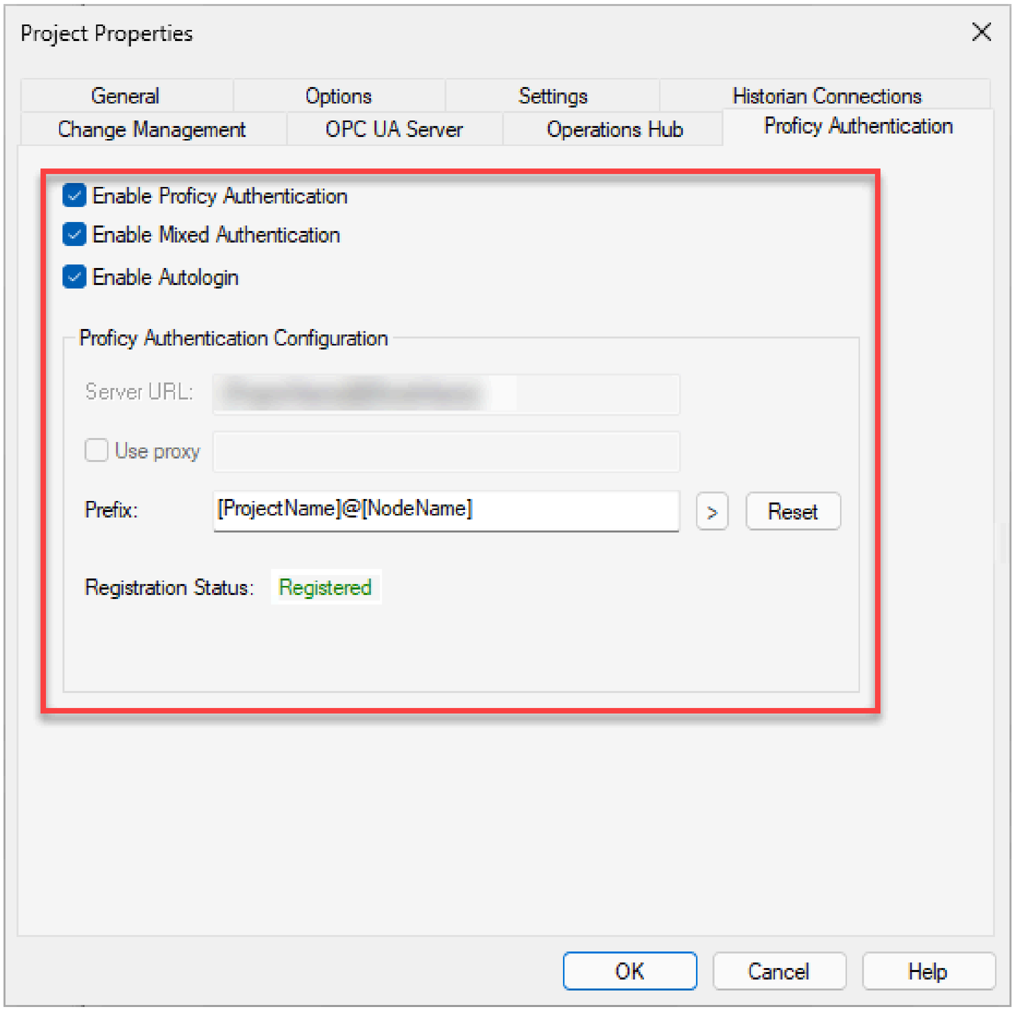
1. Open the project in **CIMPLICITY Workbench** as needed. For more information on Workbench, refer to the section About the CIMPLICITY Workbench. *(on page)*
2. In the Menu bar, click **Project**, and then click **Properties**.
   The **Project Properties** dialog box opens.



3. In the **Project Properties** dialog box, click the **Proficy Authentication** tab.

   The Proficy Authentication options are displayed.

> **Note:**
> The Proficy Authentication server URL and the other options that you selected at the time of Proficy Authentication server registration are displayed. To access this tab, you must be in administrator mode.



Project Properties

☑ Enable Proficy Authentication

☑ Enable Mixed Authentication

☑ Enable Autologin

Proficy Authentication Configuration

Server URL: [redacted]

□ Use proxy

Prefix: [ProjectName]@[NodeName]

Registration Status: Registered

4. Select the **Enable Proficy Authentication** check box.

Note:

- If you select the **Enable Proficy Authentication** check box, the **Allow web configuration for this project** check box in the **Project Properties**> **Options** tab will also be selected.
- When you enable Proficy Authentication and log in to the CIMPLICITY Workbench applications using the Proficy Authentication user, that user will automatically be added to the list of users in CIMPLICITY Workbench for security reasons. You can

> double-click the user to view the configured properties. However, you cannot edit the properties of that user.
>
> - On Operations Hub, if you want to access screens in runtime using the Webspace widget with the Proficy Authentication credentials, you must enable **Mixed Authentication** along with the **Proficy Authentication**.

For more information on the authentication types, see Configure Authentication Types *(on page)*.

5. In the **Prefix** field, enter the name for the prefix. This prefix is added to the Security Group that you publish to the Proficy Authentication server. The prefix enables you to use the same group names across different projects in the same node but with different privileges.

   By default, a prefix in the **[ProjectName]@[NodeName]** format will be added to the group(s).

   For example,

   Project Name- **SAMPLEPROJ**

   Node Name- **CIM-123-B2**

   Group in CIMPLICITY- **SYSMADMIN**

   The group will be published as **scada.SAMPLEPROJ@CIM-123-B2.SYSMADMIN**. Where, **scada** is the default namespace. For more information on Groups, refer to About Security Groups *(on page 116)*.

   > **Note:**
   > You can edit the prefix as needed, and the modified prefix will be added to the newly published Security Groups.

6. Click **OK** to complete the configuration and close the **Project Properties** dialog box.
   The configuration process is completed successfully. Now you can register CIMPLICITY with Proficy Authentication, and Configuration Hub.

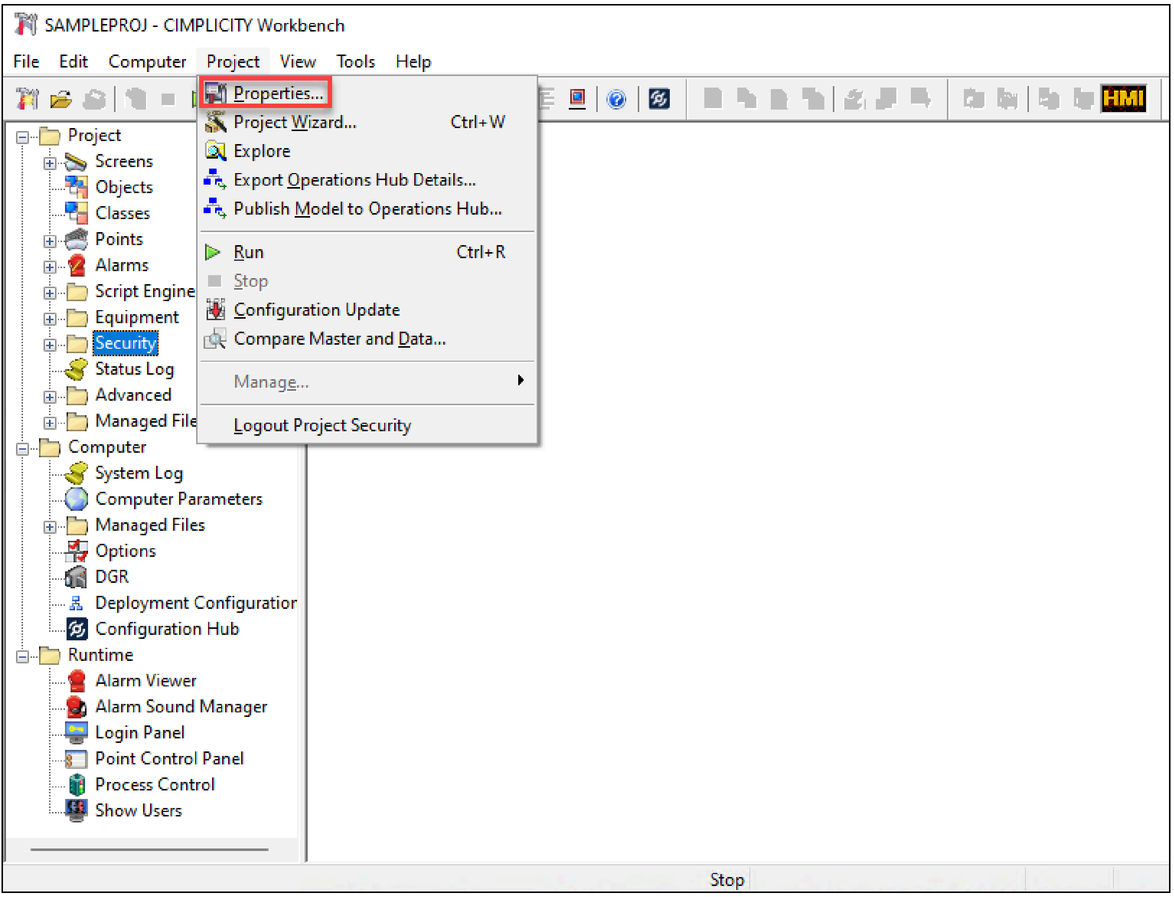
Enable web configuration in Project Properties

To host a project in Configuration Hub, you must enable the web configuration option for that project. When you configure and select the **Enable Proficy Authentication** check box in the **Project Properties**> **Proficy Authentication** tab, the **Allow web configuration for this project** check box in the **Project Properties**> **Options** tab will also be selected. However, for any reason, if the **Allow web configuration for**

this project check box is not selected, you can follow the steps mentioned in this topic and enable web configuration for a project.

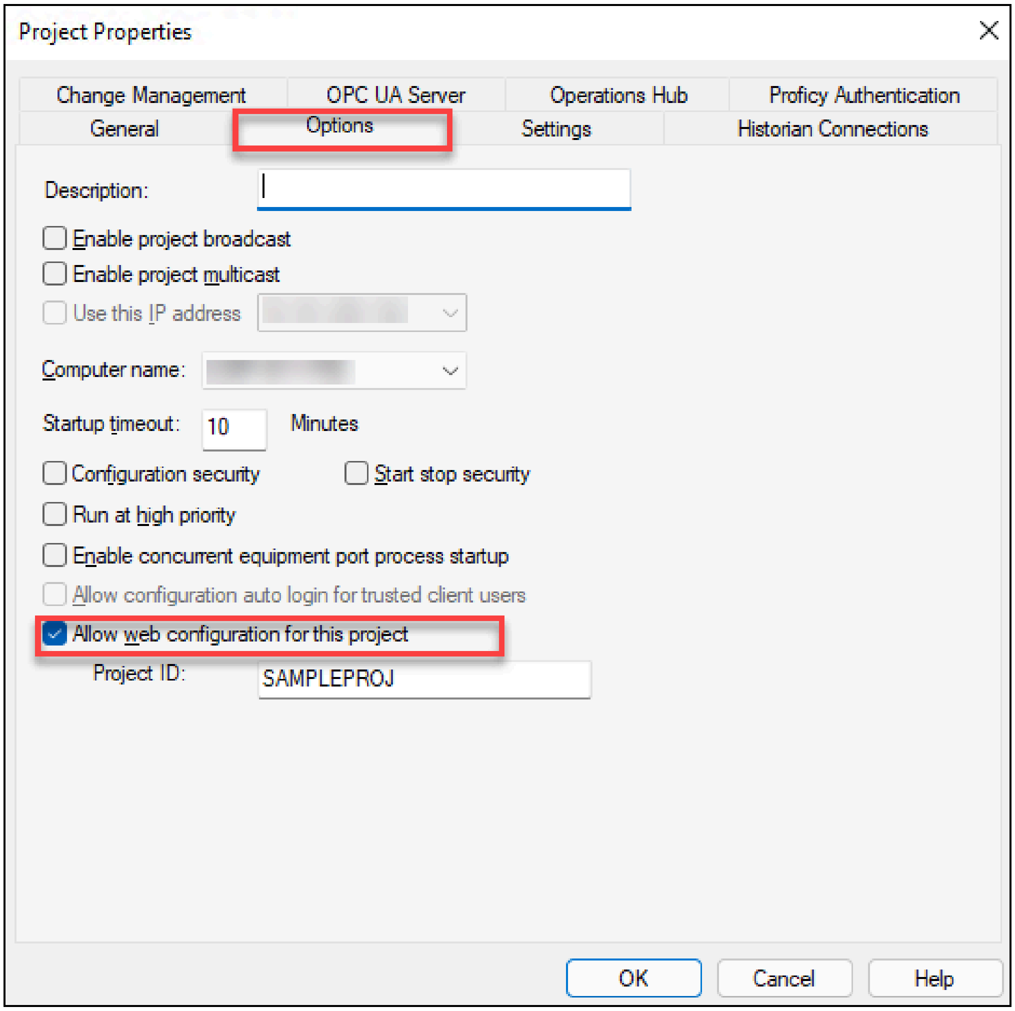
To enable the web configuration option, do the following:

1. Open the project in **CIMPLICITY Workbench** as needed. For more information on Workbench, refer to the section About the CIMPLICITY Workbench *(on page)*.
2. In the menu bar, click **Project**, and then click



Properties.

The **Project Properties** dialog box opens.



Project Properties

Description:

☐ Enable project broadcast

☐ Enable project multicast

☐ Use this IP address [redacted]

Computer name: [redacted]

Startup timeout: 10 Minutes

☐ Configuration security ☐ Start stop security

☐ Run at high priority

☐ Enable concurrent equipment port process startup

☐ Allow configuration auto login for trusted client users

☑ Allow web configuration for this project

Project ID: SAMPLEPROJ

3. In the **Project Properties** dialog box, click the **Options** tab.

   The project options are displayed.
4. In the options, select the **Allow web configuration for this project** check box.

About Security Groups

In CIMPLICITY, a Security group contains a set of roles and privileges assigned to it. You can add a security group in CIMPLICITY and publish it to the Proficy Authentication server, and also assign users of same security class to a group.

Note:

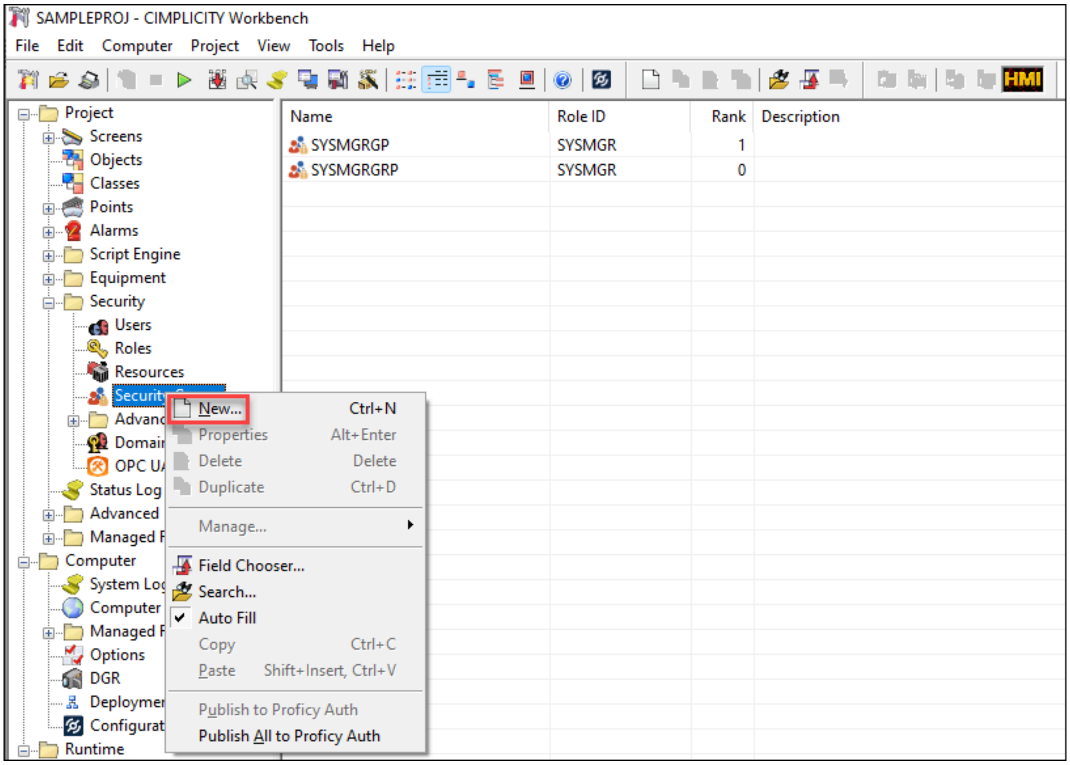
If you delete a group in CIMPLICITY, the Proficy Authentication users assigned to that group will not have the permission to use the assigned privileges.

You can create *(on page 117)*, edit *(on page 121)*, and duplicate *(on page 122)* a security group.

Create Security Groups in CIMPLICITY

To create a security group, do the following:

1. Open a project in **CIMPLICITY Workbench** as needed. For more information on Workbench, refer to the section About the CIMPLICITY Workbench. *(on page)*.
2. In the top-level folders, click and expand **Project > Security**.
3. Right-click **Security Groups** and then click **New**.

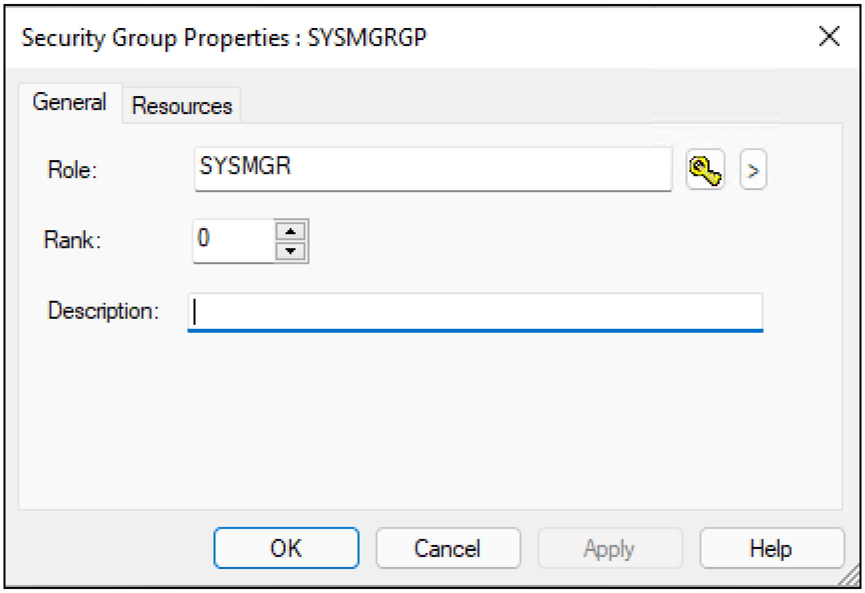


Name	Role ID	Rank	Description
SYSMGRGP	SYSMGR	1	
SYSMGRGRP	SYSMGR	0	

The **New Security Group** dialog box opens.

4. In the **Name** field, enter a name for the group.
5. After you enter a group name, click **OK**.

The **Security Group Properties** dialog box opens.



Security Group Properties : SYSMGRGP

Role: SYSMGR

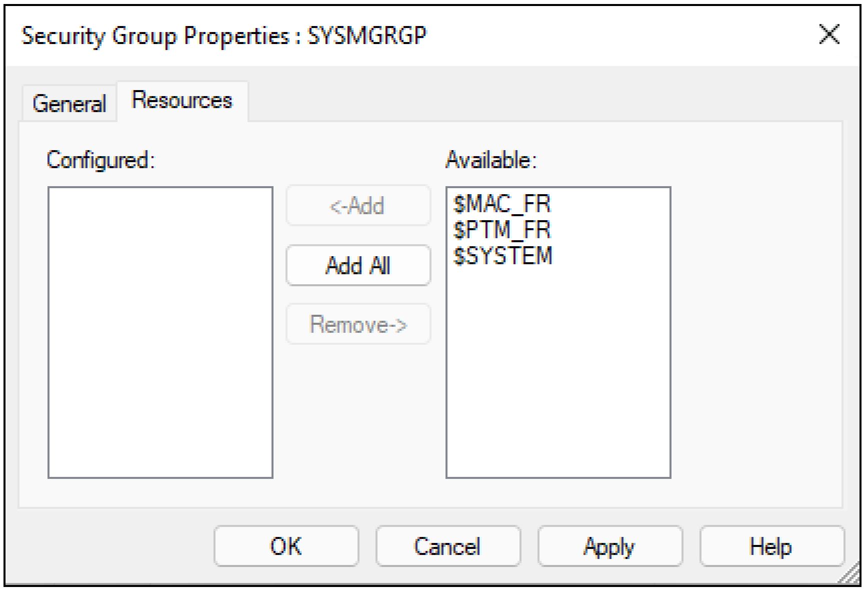
Rank: 0

Description:

6. In the **Role** field, select a role ID for the group. You can either click 🔑 or click the arrow button to browse the available roles.
   By default, the following role IDs are available: SYSMGR, OPER, and USER. You can add roles as need. For more information on adding roles, refer to the section Role Configuration *(on page)*.
7. In the **Rank** field, enter or select a rank for the group.
   By default, the role mapped to the group with the highest rank in the hierarchy will be assigned to the user. If all the groups are of the same rank, then the groups and their roles are assigned based on alphabetical order.
   For a better understanding, consider the following example scenario:
   The following three groups are added and assigned a rank for each group:
   - Group A: Rank 10
   - Group B: Rank 1
   - Group C: Rank 15

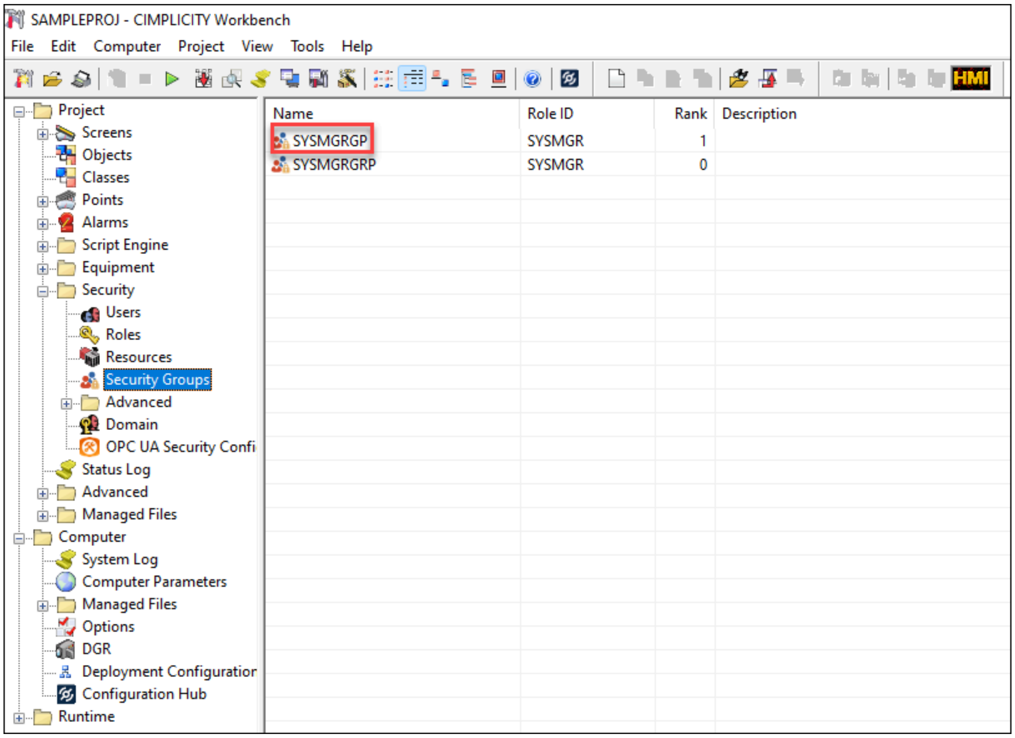
   By default, since Group C is of the highest rank, the role mapped to Group C will be assigned to the user.
   If all three groups are of the same rank, then the role mapped to Group A is assigned to the user.
8. In the **Description** filed, enter a description for the group.
   You can describe what a user is entitled if assigned to this group.
9. Click the **Resources** tab.
   All the available resources are displayed.
10. From the **Available** column, move the available resources to the **Configured** column.

By default, the following resources are available: $MAC_FR, $PTM_FR, and $SYSTEM. You can add resources as needed. For more information, refer to the section Resource Configuration *(on page)*.



11. Click **Apply** to apply the settings.
12. Click **OK** to save the details and close the **Security Group Properties** dialog box.

The group is added.



Name	Role ID	Rank	Description
SYSMGRGP	SYSMGR	1	
SYSMGRGRP	SYSMGR	0	

After you add a group, if you want to edit the properties, you can right-click the group and edit the properties. Also, to quickly create a new group with the same properties of another group, you can right-click that group and duplicate.

> **Note:**
> Ensure that the group names are unique.

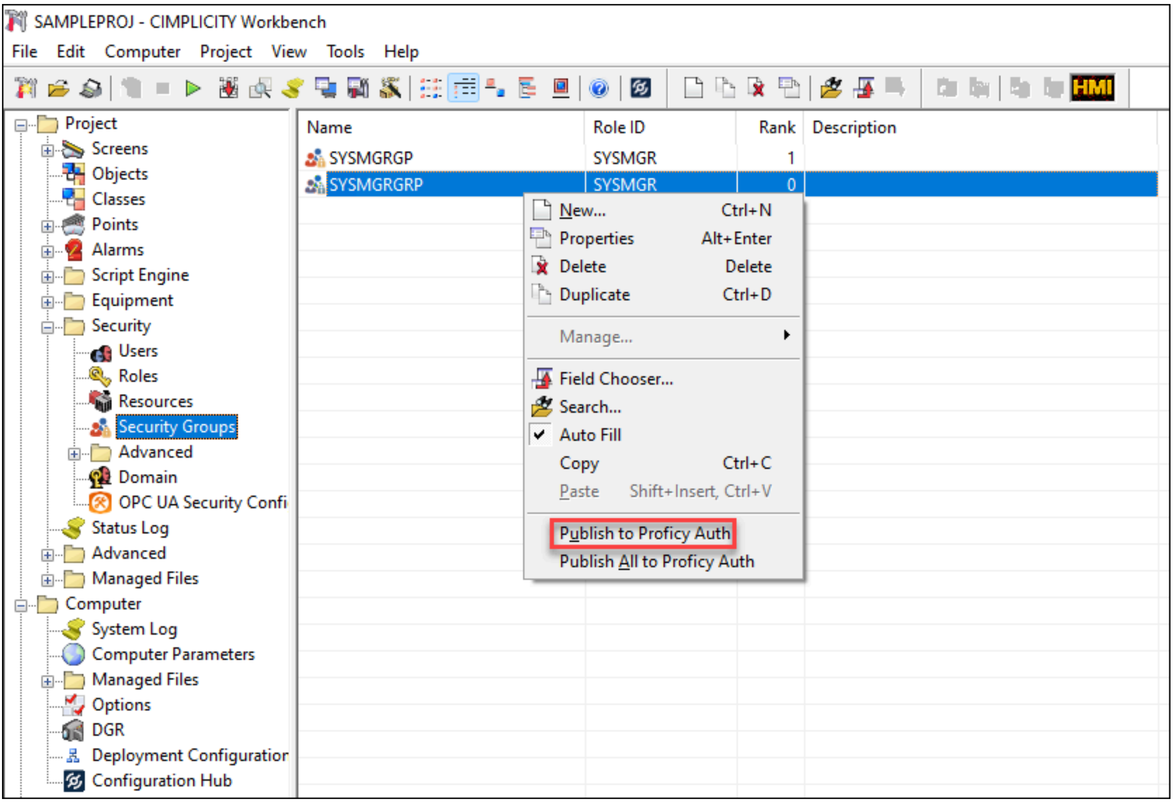
Publish Group(s) to Proficy Authentication server

After the security group are added, you can publish the group(s) to the Proficy Authentication server. The published groups are added to the Proficy Authentication server with a prefix that you entered while Configuring Proficy Authentication in CIMPLICITY *(on page 111)*.

To publish group(s) to the Proficy Authentication server, do the following:

1. Open a project in **CIMPLICITY Workbench** as needed. For more information on Workbench, refer to the section About the CIMPLICITY Workbench. *(on page)*.
2. In the top-level folders, click and expand **Project > Security**.
3. In the **Security** node, click **Security Groups**.
   All the available security groups are listed.

4. Right-click the group that you want to publish, and then click **Publish to Proficy Auth**.



Name	Role ID	Rank	Description
SYSMGRGP	SYSMGR	1	
SYSMGRGRP	SYSMGR	0	

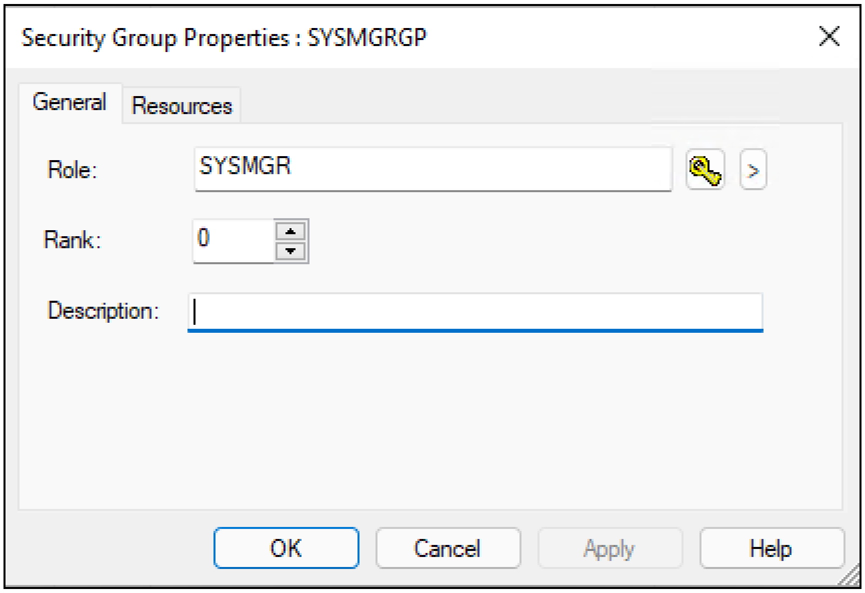
Alternatively, if you want to publish all the available groups simultaneously, you can right-click **Security Groups** in the Security node, or a group, and then click **Publish All to Proficy Auth**.

> **Note:**
>
> The publish option is enabled only when you enable Proficy Authentication in the **Project Properties**, and you will be able to publish the groups to the Proficy Authentication server only when the Proficy Authentication server is configured in CIMPLICITY **Project Properties**. For more information on how to enable and configure Proficy Authentication, refer to the section Enable and Configure Proficy Authentication *(on page 111)*.

Edit an Existing Security Group

1. Open a project in **CIMPLICITY Workbench** as needed. For more information on Workbench, refer to the section About the CIMPLICITY Workbench. *(on page)*.
2. In the top-level folders, click and expand **Project > Security**.
3. From the list of the security groups, right-click the security group, and then select **Properties**.

   The **Security Group Properties** dialog box opens.



Role: SYSMGR

Rank: 0

Description:

4. Edit the required properties.
5. Click **Apply** to apply the changes.
6. Click **OK** to save the changes and close the **Security Group Properties** dialog box.

Duplicate an Existing Security Group

You can quickly create a new group with the same properties of another group.

1. Open a project in **CIMPLICITY Workbench** as needed. For more information on Workbench, refer to the section About the CIMPLICITY Workbench. *(on page)*.
2. In the top-level folders, click and expand **Project > Security**.
3. From the list of the security groups, right-click the security group from which you want to create a new group, and then select **Duplicate**.

   The **Duplicate Security Group** dialog box opens.
4. In the **Destination Security Group** field, enter the name for the new group.

   > **Note:**
   >
   > Ensure that the group names are unique.
5. Click **OK** to create and save the new group.

   The new security group is created with the same properties of the group that you duplicated.

Chapter 9. CIMPLICITY Plug-in Registration with Configuration Hub

CIMPLICITY Plug-in Registration with Configuration Hub Using Proficy Authentication

CIMPLICITY Plug-in allows you to browse OPC UA devices, and MQTT devices in Configuration Hub. You can configure CIMPLCITY Plug-in in Configuration Hub using the Proficy Authentication.

Before you begin the configuration of CIMPLICITY Plug-in, ensure that you have completed the following:

- Set up Proficy Authentication Server.
- Set up Configuration Hub.
- Configure Proficy Authentication Server in CIMPLICITY *(on page 107)*.

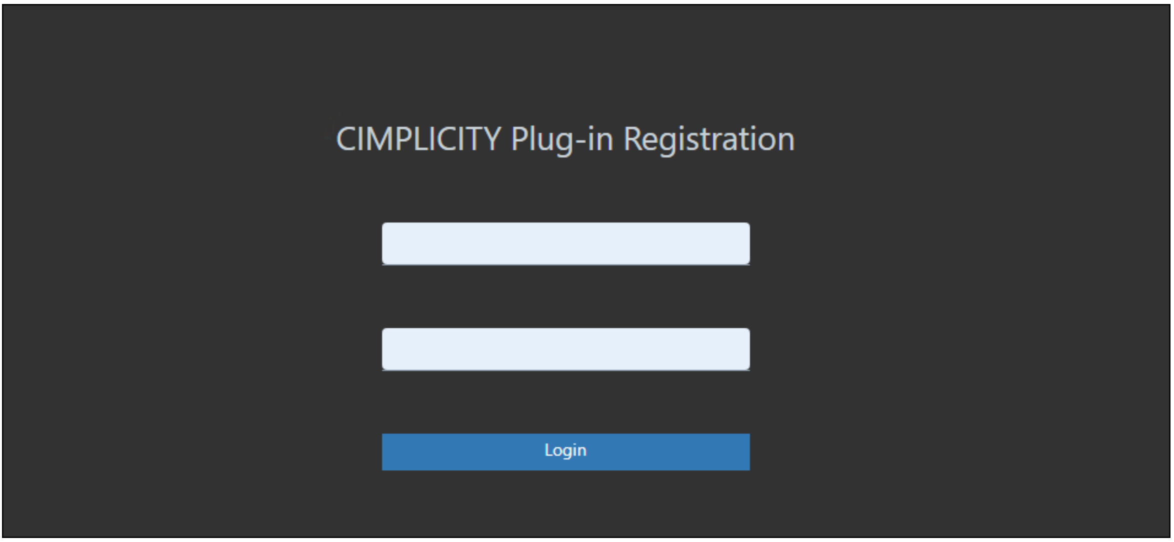
Register CIMPLICITY with Configuration Hub, and Proficy Authentication

To use the CIMPLICITY plug-in in Configuration Hub using Proficy Authentication, you must register CIMPLICITY with both the Configuration Hub and Proficy Authentication. You can use a single webpage to register CIMPLICITY to Configuration Hub, CIMPLICITY to Proficy Authentication server.

To register CIMPLICITY with Configuration Hub, Proficy Authentication, do the following:

1. Open the project in **CIMPLICITY Workbench** as needed. For more information on Workbench, refer to the section About the CIMPLICITY Workbench. *(on page)*.
2. From the toolbar, click

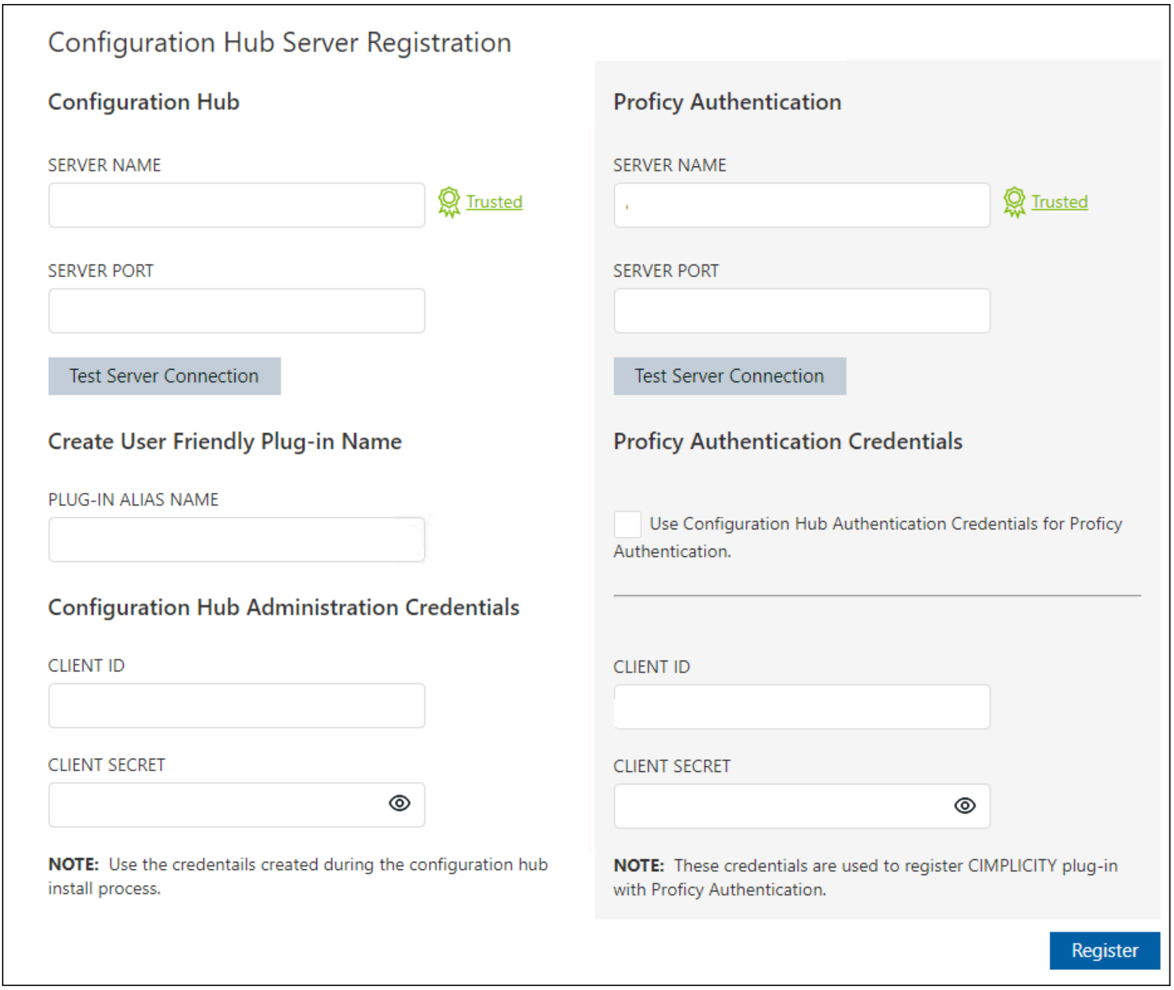
The **CIMPLICITY Plug-in Registration** page opens.



CIMPLICITY Plug-in Registration

3. In the **CIMPLICITY Plug-in Registration** page, enter the computer level username and password that you generated in CIMPLICITY using the **RegisterComputerUser.exe** tool that is available at **[Install location]\Proficy\Proficy CIMPLICITY\exe**.
4. Click **Login**.

The **Configuration Hub Server Registration** page opens.



Configuration Hub Server Registration

Configuration Hub

SERVER NAME

Trusted

SERVER PORT

Test Server Connection

Create User Friendly Plug-in Name

PLUG-IN ALIAS NAME

Configuration Hub Administration Credentials

CLIENT ID

CLIENT SECRET

NOTE: Use the credentails created during the configuration hub install process.

Proficy Authentication

SERVER NAME

Trusted

SERVER PORT

Test Server Connection

Proficy Authentication Credentials

□ Use Configuration Hub Authentication Credentials for Proficy Authentication.

CLIENT ID

CLIENT SECRET

NOTE: These credentials are used to register CIMPLICITY plug-in with Proficy Authentication.

Register

5. In **Configuration Hub**, fill the following details:

Options	Description
SERVER NAME	The name of the Configuration Hub server to which you want to register. In the <Fully qualified domain name> format.
SERVER PORT	The port number of the Configuration Hub server to which you want to register.
PLUG-IN ALIAS NAME	The alias name for the CIMPLICITY plug-in that you want to see in the Configuration Hub.

Options	Description
	Note: By default, the name populated is the CIMPLICITY node's name. However, you can update it to how you want to see the CIMPLICITY plug-in name in the configuration Hub.
CLIENT ID	The client ID of the Configuration Hub server that you provided during the Configuration Hub installation.
CLIENT SECRET	The client secret of the Configuration Hub server that you provided during the Configuration Hub installation.

6. In **Proficy Authentication**, fill the following details:

Options	Description
SERVER NAME	The name of the Proficy Authentication server to which you want to register Configuration Hub. In the<Fully qualified domain name> format.
SERVER PORT	The port number of the Proficy Authentication server to which you want to register Configuration Hub.
Use Configuration Hub Authentication Credentials for Proficy Authentication	Select this check box if you had entered same credentials (Client ID and Client Secret) for both Configuration Hub and Proficy Authentication during installation.
CLIENT ID	The Client ID of the Proficy Authentication server.
CLIENT SECRET	The Client secret of the Proficy Authentication server.

7. If the root certificate of the Proficy Authentication server is trusted, you will see Trusted. If not, you will see Not trusted; then you must manually trust the certificate. For more information, refer to the section Trust an Untrusted Certificate while Registering CIMPLICITY with Configuration Hub and Proficy Authentication server *(on page 127)*.
8. To test the connection, click **Test Server Connection**.
9. If the connection to the Configuration Hub or the Proficy Authentication server is successful, you will receive a success dialog. If your connection is unsuccessful, retry to connect to another valid Configuration Hub or Proficy Authentication server.
10. Click **Register**.
    The **Configuration Hub Server Registration** dialog box opens, with a success message.
11. Click **OK**.
    The **Proficy Authentication Client** dialog box is closed.

Trust an Untrusted Certificate while Registering CIMPLICITY with Configuration Hub and Proficy Authentication server

While you register CIMPLICITY with Configuration Hub and Proficy Authentication server and also register (Configuration Hub with Proficy Authentication server in the background), if CIMPLICITY could not find Configuration Hub's or Proficy Authentication server's root certificate in the local computer's trusted certificate folder, you must manually trust the certificate.

To manually trust the certificate:

1. In the **Configuration Hub Server Registration** page, if you want to trust the certificate, click the **Not trusted** link.
   The Certificate Details dialog box opens, displaying the details of the certificate.
2. If you want to add the certificate to the trusted folder, click **Trust**.
3. The certificate is added to the local computer's trusted certificate folder. You can now proceed with the registration of CIMPLICITY with Configuration Hub and Proficy Authentication server and also register (Configuration Hub with Proficy Authentication server in the background).
4. If you do not trust the certificate, click **Don't Trust**.
   If the certificate details cannot be retrieved due to network issue, you can click the Browse button and manually locate the certificate in your local machine, and then Trust the certificate.

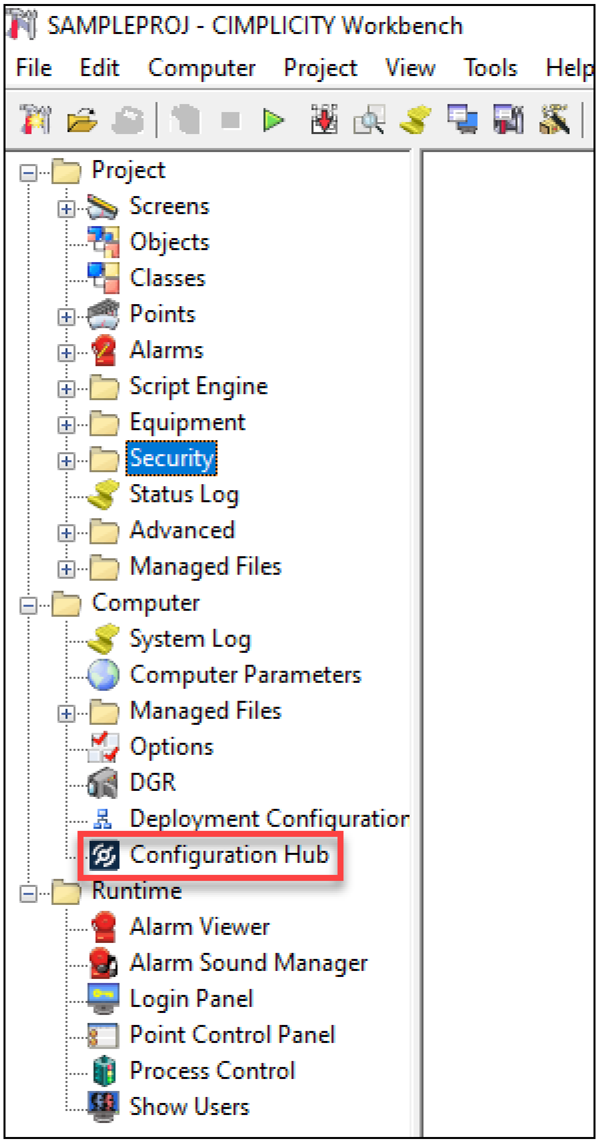
Access Configuration Hub

After you register CIMPLICITY with Configuration Hub, and Proficy Authentication, you can access the Configuration Hub within CIMPLICITY Workbench, or on the desktop, click the Configuration Hub icon.

Note:
If you open Configuration Hub from the desktop, ensure that CIMPLICITY is running and you are logged into CIMPLICITY.

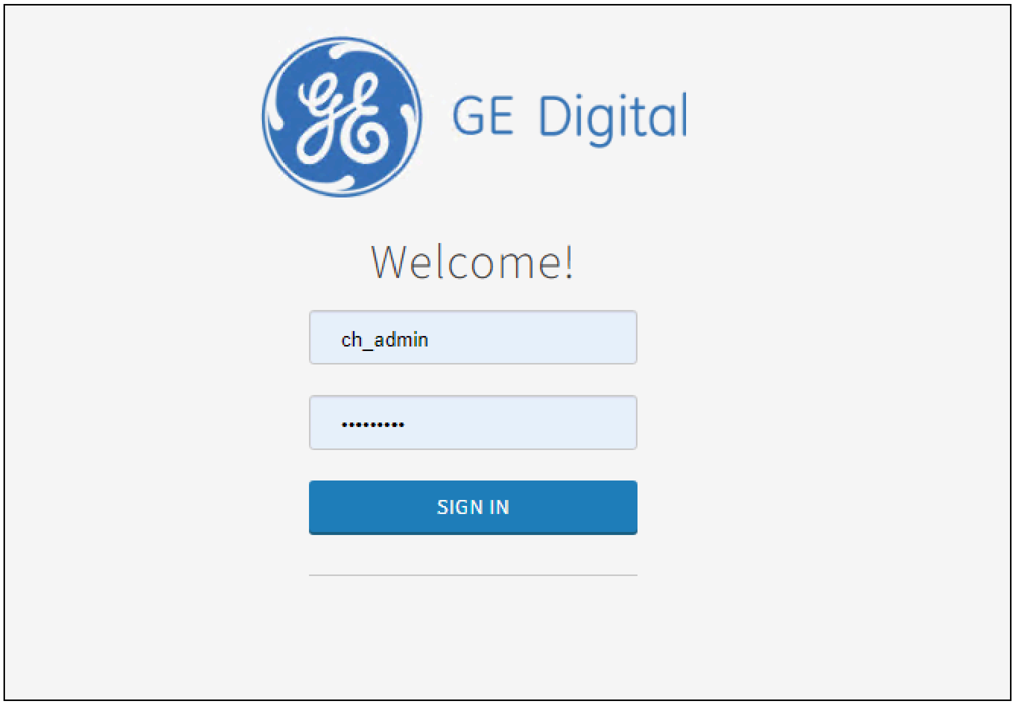
To access Configuration Hub from CIMPLICITY, do the following:

1. Open a project in **CIMPLICITY Workbench** as needed. For more information on Workbench, refer to the section About the CIMPLICITY Workbench. *(on page)*.
2. In the top-level folders, click and expand **Computer**.



3. Double-click Configuration Hub.

The CIMPLICITY Proficy Authentication login page opens.



ch_admin

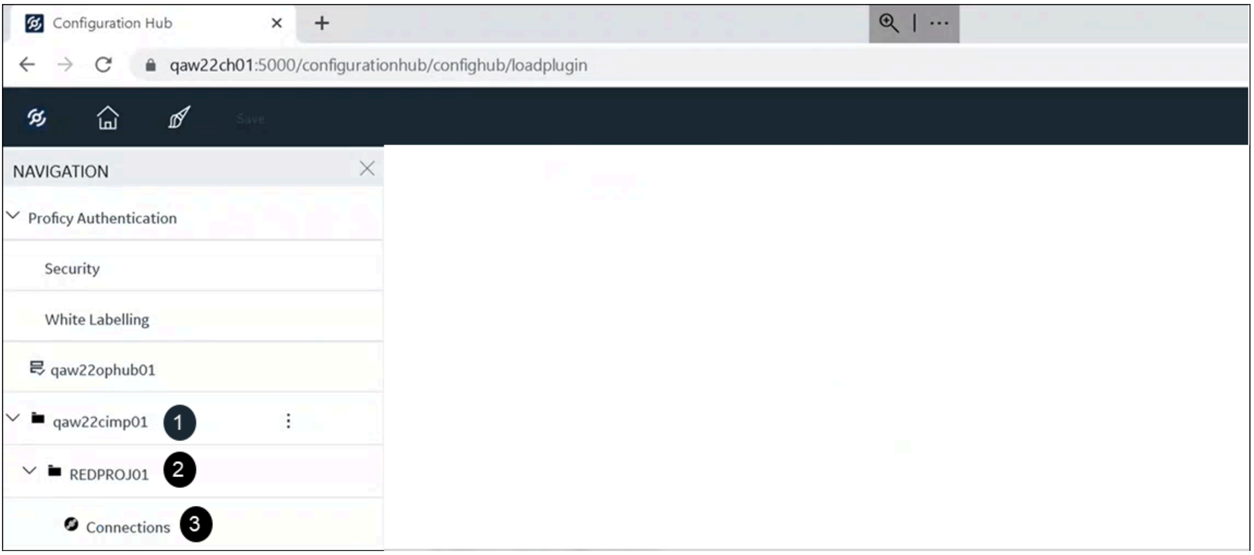
•••••••••

4. Log in using ch_admin as username and your Proficy Authentication secret as password.

   After a successful authentication, the Configuration Hub page opens.

Overview of CIMPLICITY Plug-in within Configuration Hub

After registering CIMPLICITY with Configuration Hub and Proficy Authentication, if you log in and open Configuration Hub *(on page 127)*, you will see all the CIMPLICITY nodes that you registered with all their associated projects on the left side panel as shown below.



Marker	Description
1	CIMPLICITY Node/ computer registered with Configuration Hub and Proficy Authentication.
2	Project associated to the CIMPLICITY node.
3	Devices associated to the project. **Note:** **Connections** is displayed only if a Project is configured with devices. You can click **Connections** to browse *(on page 132)* devices and create *(on page 138)* points.

Start and Stop a CIMPLICITY Project

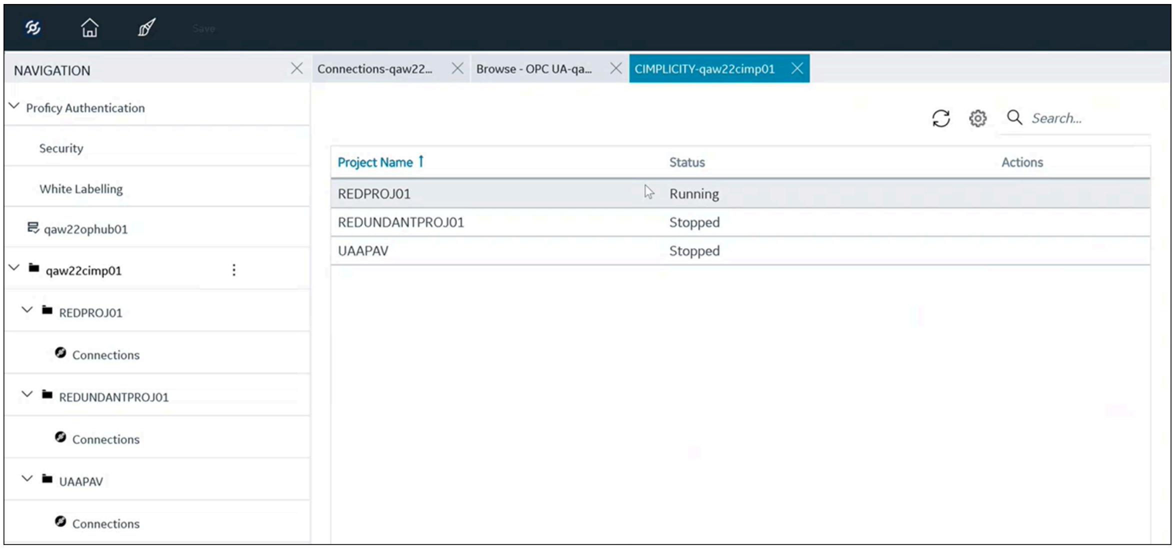
You can start a project and stop a running project from Configuration Hub. In case of a Redundant server configured *(on page)* project, you will have additional options to start or stop projects at the primary or secondary level.

To start a project, perform the following:

1. Log in to Configuration Hub. For more information, see Access Configuration Hub *(on page 127)*.

   The Configuration Hub page opens listing all the CIMPLICITY nodes and their associated projects on the left pane.
2. From the left pane, select the required node.

   All the associate projects are listed.



Project Name	Status	Actions
REDPROJ01	Running	
REDUNDANTPROJ01	Stopped	
UAAPAV	Stopped	

3. Select a project, and then select the ellipsis (...) to the right of your entry in the **Actions** column. Alternatively, you can right-click on the required project and select the actions as needed.

   A popup menu appears.
4. Select an action as needed.

   The below table explains the available options:

Option	Description
Start	Select this to start a stopped project.
Stop	Select this to stop a running project.
Start Primary and Secondary	Select this to start a stopped project in both primary and secondary servers.
Start Primary	Select this to start a stopped project in primary server only.
Start Secondary	Select this to start a stopped project in secondary server only.
Stop Primary and Secondary	Select this to stop a running project in both primary and secondary servers.

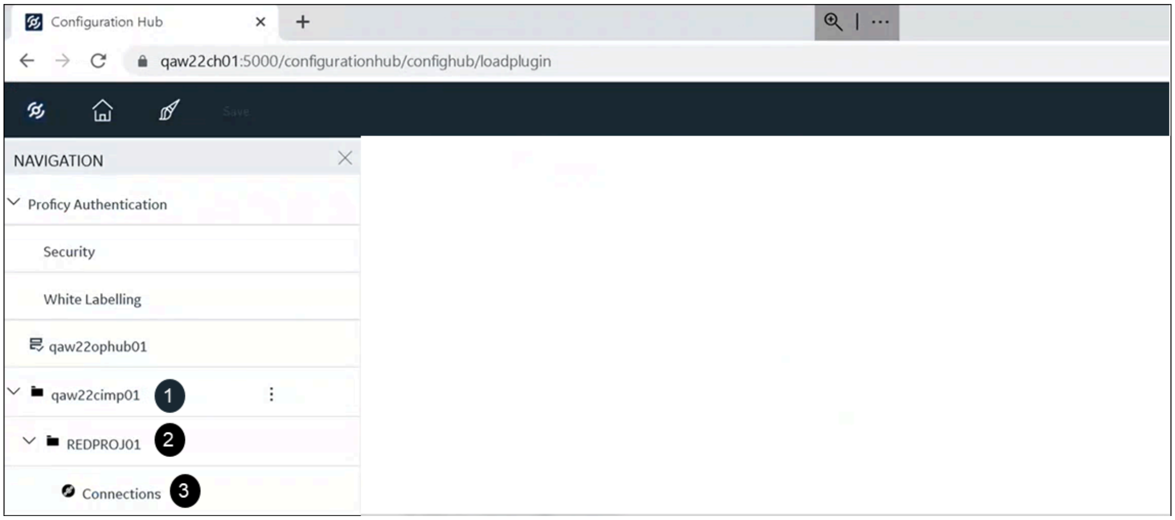
Option	Description
Stop Primary	Select this to stop a running project in primary server only.
Stop Secondary	Select this to stop a running project in secondary server only.

If you select **Stop**, a confirmation popup appears. Select **Yes** to stop the project.

Select and Browse Devices

You can log in to Configuration Hub and browse through all the OPC UA devices that are associated to a project.

1. Log in to Configuration Hub. For more information, see Access Configuration Hub *(on page 127)*. The Configuration Hub page opens listing all the CIMPLICITY nodes and their associated projects on the left pane.

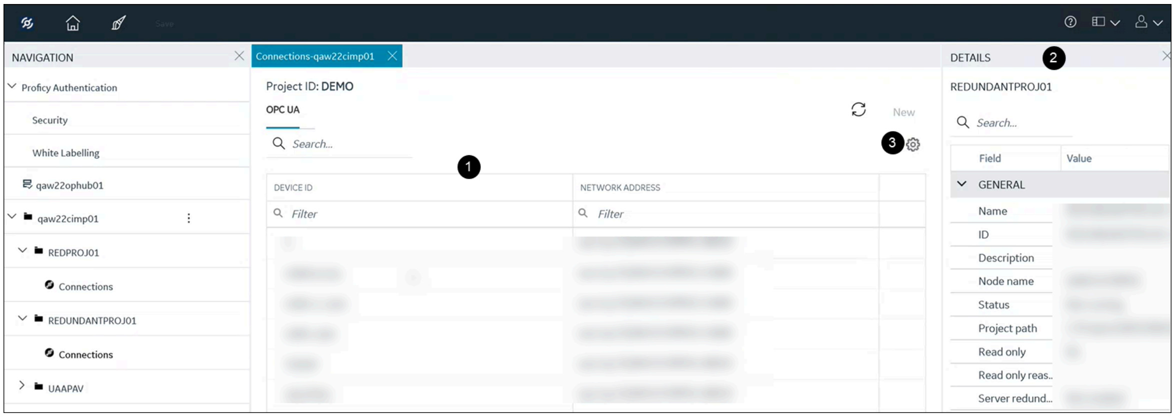


Marker	Description
1	CIMPLICITY Node/ computer registered with Configuration Hub and Proficy Authentication.
2	Project associated to the CIMPLICITY node.
3	**Connections** is displayed only if a Project is configured with devices. You can click **Connec-**

Marker	Description
	tions to browse all the available devices and create points.

2. From the left pane, expand the required project and select **Connections**.

   The devices tab opens listing all the associated devices.



Marker	Description
1	List of all the OPC UA devices associated to the project.
2	Details of the selected device. **Note:** This is read-only. In case of a redundancy project, you can see the details like node name, status, and path of the configured primary and secondary servers. For more information on configuring redundancy, refer to Configuring Redundancy *(on page)*.
3	Column chooser. You can select what all information of a device you want to view in the grid. **Available options**:

Marker	Description
	◦ Device ID ◦ Network Address ◦ Description ◦ Port Type ID

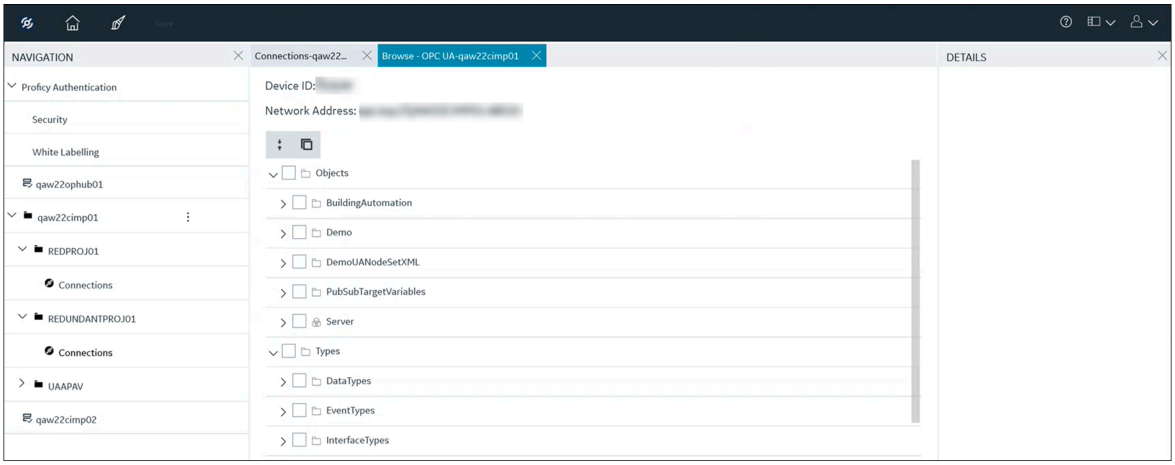
3. Select a device, and then select the ellipsis (...) to the right of your entry.

   A popup menu appears.

4. From the popup menu, select **Browse**.

   A new tab opens, listing the device and all its associated objects.

> **Note:**
> If you are already browsing a device, you will be prompted with a popup stating that you are already browsing a device and whether you want to replace it. If you select **Yes**, the existing device tab is replaced with the selected device.



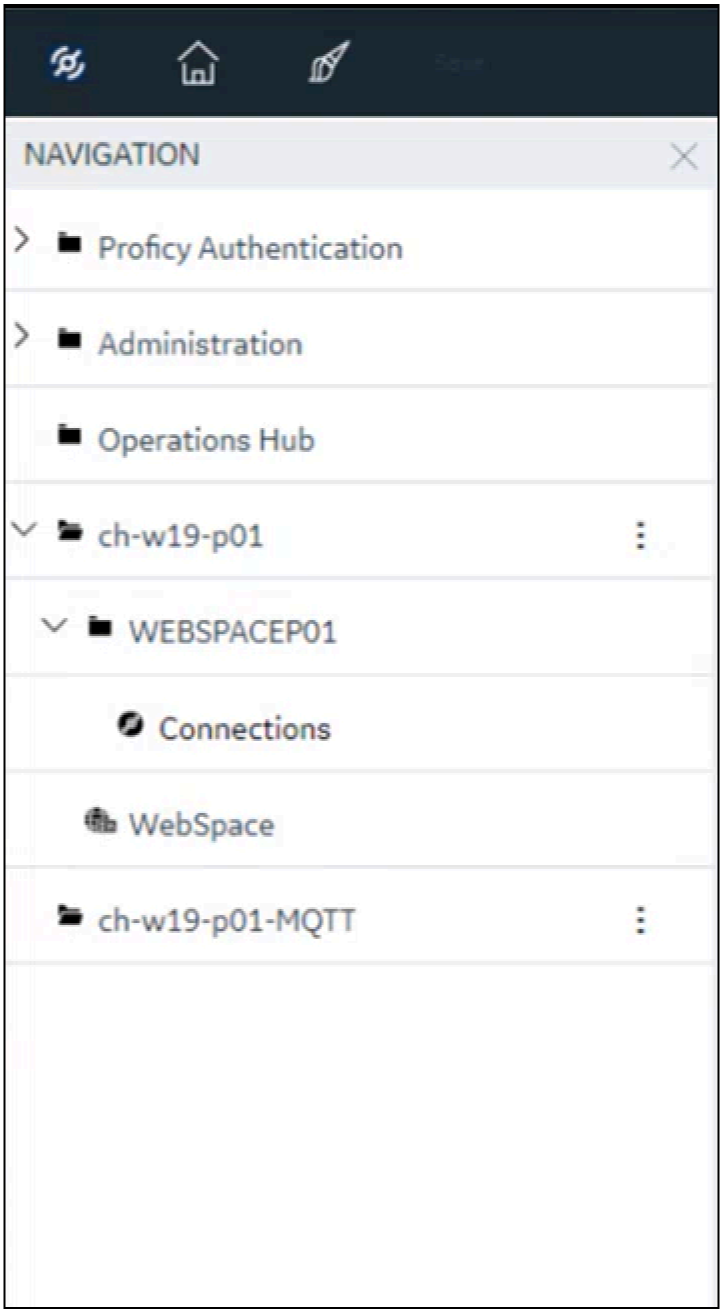
You can now create SCADA points from the objects displayed for the selected Device.

Select and Browse Tags from an MQTT Device

You can log in to Configuration Hub and browse through all the configured MQTT Devices and read the values. For you to be able to browse an MQTT device using CIMPLICITY plug-in, you must do the following configurations:

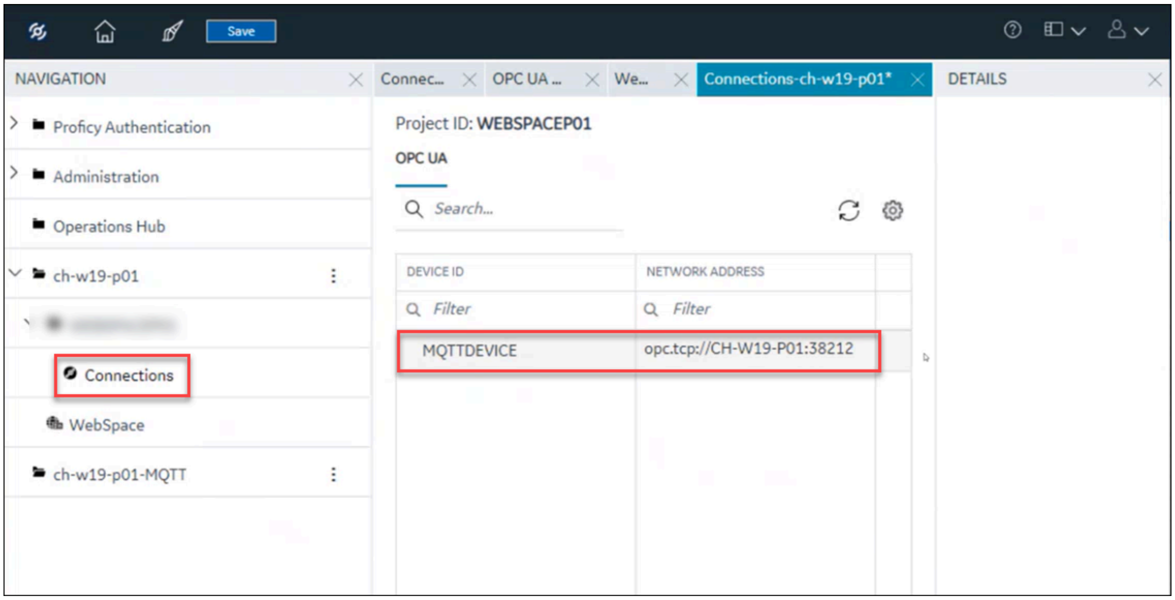
- Configure MQTT Client on Configuration Hub where your CIMPLICITY plug-in is registered. For more information, see the MQTT Client documentation in the *Getting Started* section.
- After you configure the MQTT Client, you must create an MQTT Device in the CIMPLICITY Workbench. And add the MQTT Client's endpoint URL. For example, opc.tcp://<Host-name>:3812 in the OPC UA DA Configuration tab. Creating an MQTT device is similar to creating an OPC UA device as described in the 2.1 OPC UA DA Configuration: Connection *(on page)* as mentioned in the Device Communication > *CIMPLICITY OPC UA Client* section.

1. Log in to Configuration Hub. For more information, see Access Configuration Hub *(on page 127)*.
   The Configuration Hub page opens listing all the CIMPLICITY nodes and their associated projects on the left pane.



2. From the left pane, expand the required project and select **Connections**.

   The devices tab opens listing all the associated devices.



Project ID: WEBSPACEP01

DEVICE ID	NETWORK ADDRESS
MQTTDEVICE	opc.tcp://CH-W19-P01:38212

3. Select a device, and then select the ellipsis (...) to the right of your entry.

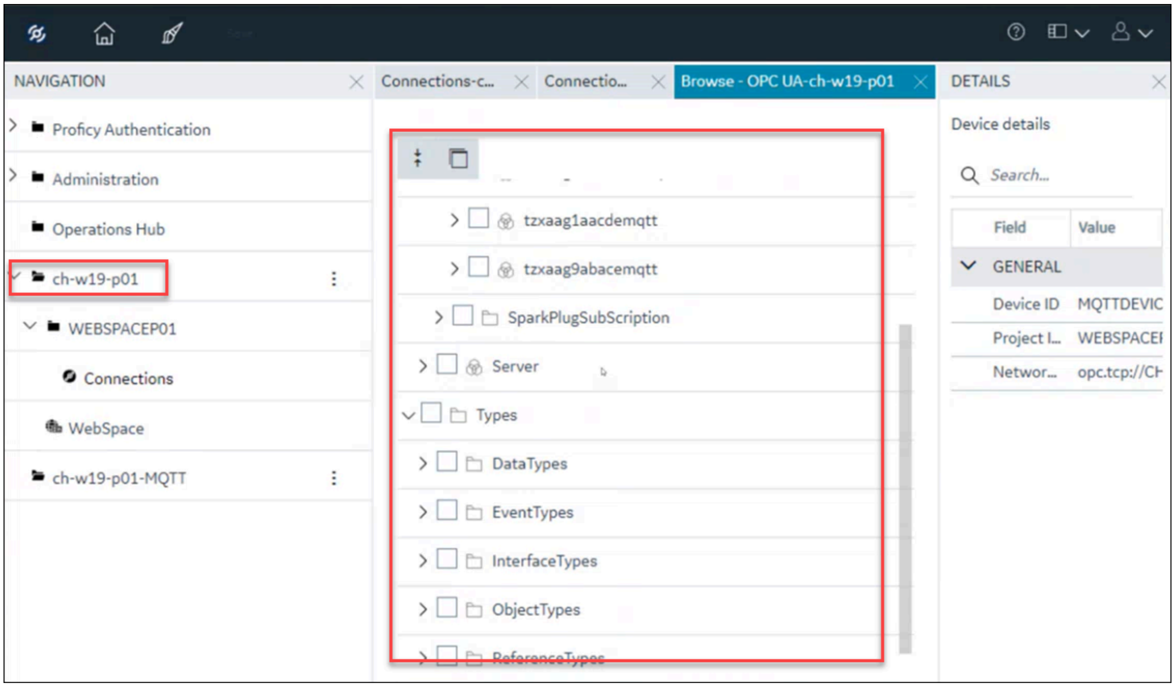
   A popup menu appears.

4. From the popup menu, select **Browse**.

   A new tab opens, listing the device and all its associated objects.

Note:

If you are already browsing a device, you will be prompted with a popup stating that you are already browsing a device and whether you want to replace it. If you select **Yes**, the existing device tab is replaced with the selected device.



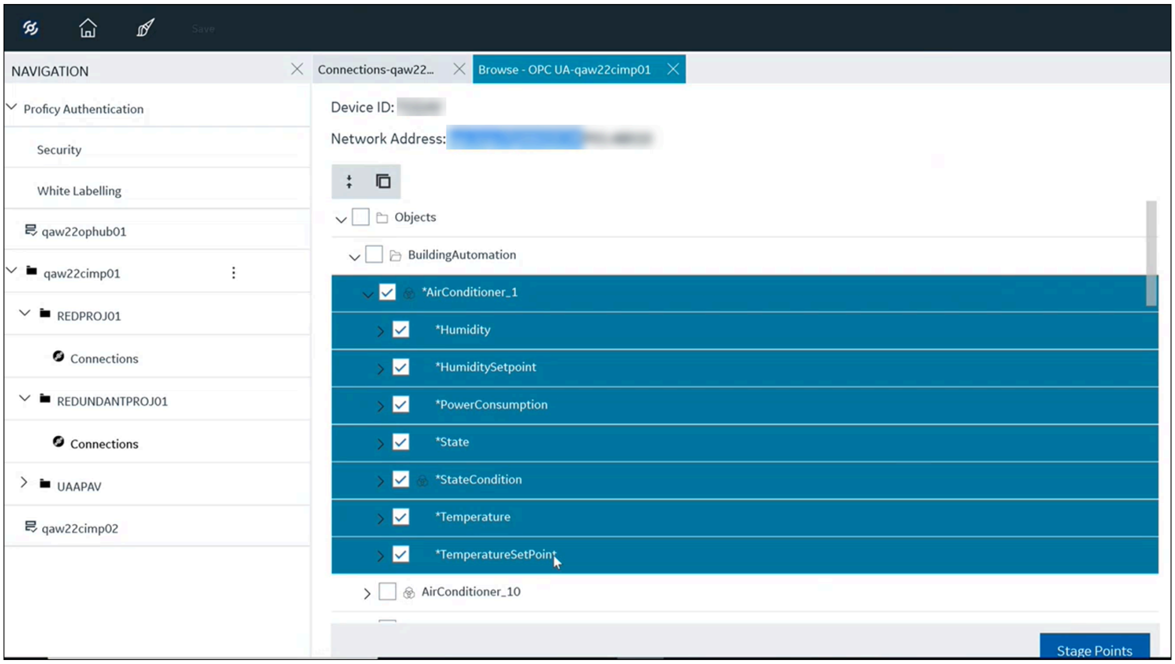
You can see the tags from the MQTT device and view their details.

Create SCADA Points

Create SCADA points from the objects. Ensure that you browsed a device to proceed with point creation.

To create points, perform the following:

1. Select the objects.
   You can either right-click the node, and then select **Select all children**, or to select the children of a node, you can double-click the node.
   Once you select an object, **Stage Points** button is enabled.



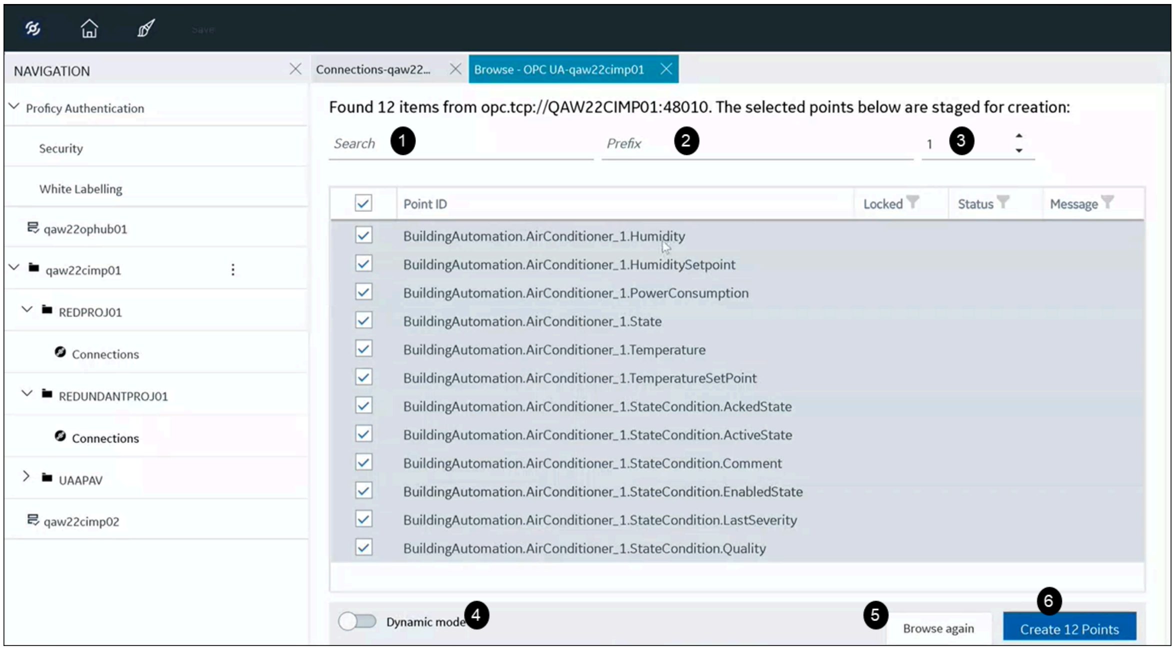
Device ID: [redacted]

Network Address: [redacted]

- □ Objects
  - □ BuildingAutomation
    - ☑ *AirConditioner_1
      - ☑ *Humidity
      - ☑ *HumiditySetpoint
      - ☑ *PowerConsumption
      - ☑ *State
      - ☑ *StateCondition
      - ☑ *Temperature
      - ☑ *TemperatureSetPoint
    - □ AirConditioner_10

2. Select **Stage Points**.

   All the selected points are staged and listed.



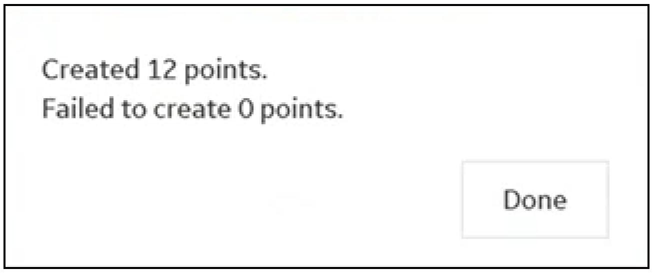
Found 12 items from opc.tcp://QAW22CIMP01:48010. The selected points below are staged for creation:

☑	Point ID	Locked	Status	Message
☑	BuildingAutomation.AirConditioner_1.Humidity			
☑	BuildingAutomation.AirConditioner_1.HumiditySetpoint			
☑	BuildingAutomation.AirConditioner_1.PowerConsumption			
☑	BuildingAutomation.AirConditioner_1.State			
☑	BuildingAutomation.AirConditioner_1.Temperature			
☑	BuildingAutomation.AirConditioner_1.TemperatureSetPoint			
☑	BuildingAutomation.AirConditioner_1.StateCondition.AckedState			
☑	BuildingAutomation.AirConditioner_1.StateCondition.ActiveState			
☑	BuildingAutomation.AirConditioner_1.StateCondition.Comment			
☑	BuildingAutomation.AirConditioner_1.StateCondition.EnabledState			
☑	BuildingAutomation.AirConditioner_1.StateCondition.LastSeverity			
☑	BuildingAutomation.AirConditioner_1.StateCondition.Quality			

Marker	Description
1	Enter text to display point IDs that contain the entered text.

Marker	Description
2	Enter a prefix to the name of the points that will be created.
3	Enter the number of levels in the namespace to be stripped off from the beginning of the point IDs. For example, if you do not want AirConditioner_1 in the namespace, you must select 2.
4	When the project is running, if you toggle on **Dynamic mode**, the points that are created will be available immediately. If you toggle off **Dynamic mode**, the points that are created will become available only after you restart the project **Note:** In a redundant system, for dynamic configuration to work, the CIMPLICITY Configuration Microservice should run as the same user with the same password configured in the redundant pair of systems. .
5	Select this to browse the devices and objects again. **Note:** This will be enabled only after you create points for the selected objects.
6	Select this to create points.

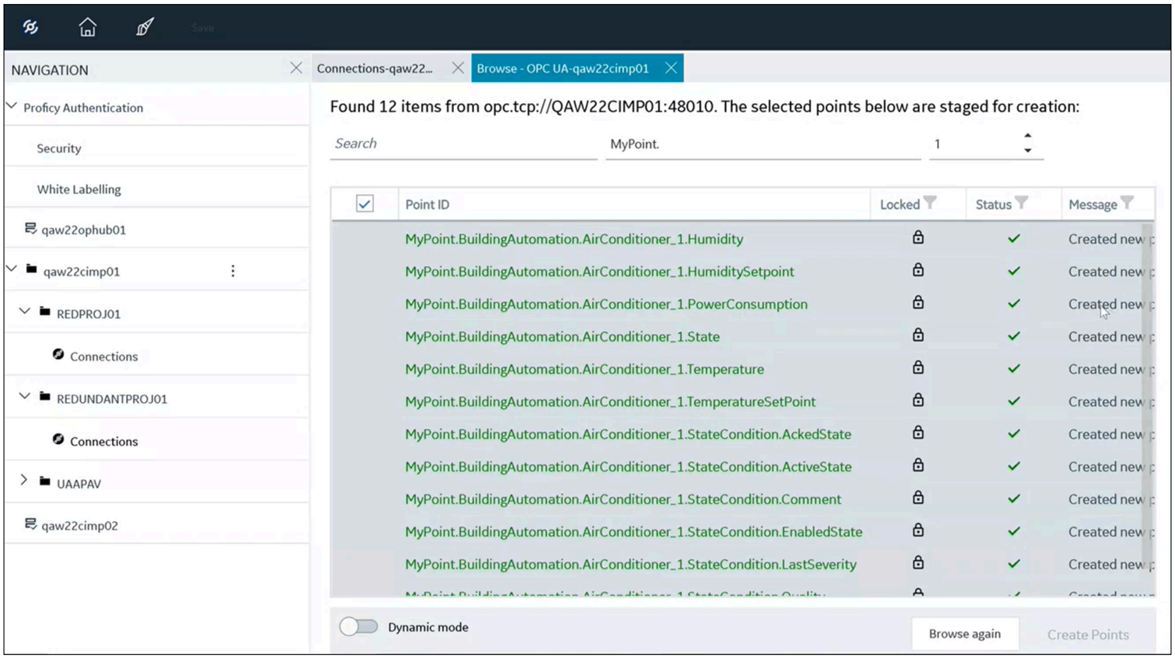
3. Select **Create** (number of points selected) **Points**.
   The points are created, and the results are displayed.



Created 12 points.
Failed to create 0 points.

4. Select **Done**.

   All the created points and their status are listed.



Found 12 items from opc.tcp://QAW22CIMP01:48010. The selected points below are staged for creation:

Search: MyPoint. 1

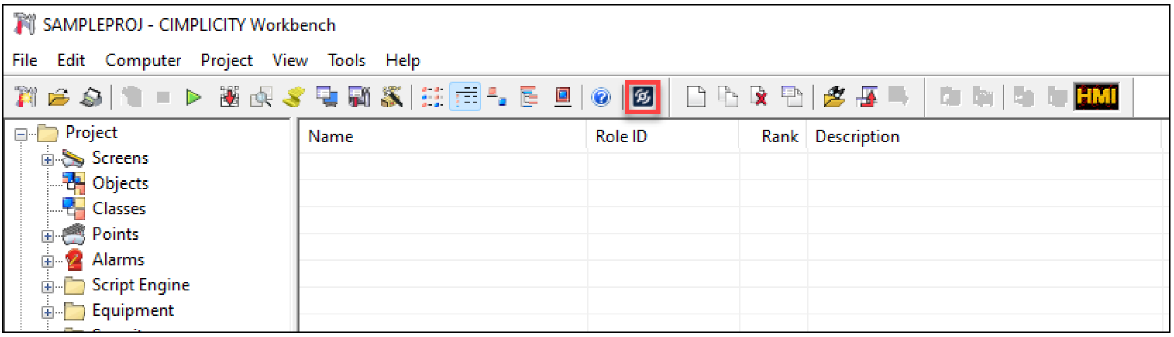
☑	Point ID	Locked	Status	Message
	MyPoint.BuildingAutomation.AirConditioner_1.Humidity	🔒	✓	Created new p
	MyPoint.BuildingAutomation.AirConditioner_1.HumiditySetpoint	🔒	✓	Created new p
	MyPoint.BuildingAutomation.AirConditioner_1.PowerConsumption	🔒	✓	Created new p
	MyPoint.BuildingAutomation.AirConditioner_1.State	🔒	✓	Created new p
	MyPoint.BuildingAutomation.AirConditioner_1.Temperature	🔒	✓	Created new p
	MyPoint.BuildingAutomation.AirConditioner_1.TemperatureSetPoint	🔒	✓	Created new p
	MyPoint.BuildingAutomation.AirConditioner_1.StateCondition.AckedState	🔒	✓	Created new p
	MyPoint.BuildingAutomation.AirConditioner_1.StateCondition.ActiveState	🔒	✓	Created new p
	MyPoint.BuildingAutomation.AirConditioner_1.StateCondition.Comment	🔒	✓	Created new p
	MyPoint.BuildingAutomation.AirConditioner_1.StateCondition.EnabledState	🔒	✓	Created new p
	MyPoint.BuildingAutomation.AirConditioner_1.StateCondition.LastSeverity	🔒	✓	Created new p
	MyPoint.BuildingAutomation.AirConditioner_1.StateCondition.Quality	🔒	✓	Created new p

Update or Modify CIMPLICITY Plug-in

If you want to modify the alias name for the CIMPLICITY plug-in that is registered with Configuration Hub, or if there are any changes in the Client ID and Client Secret of Configuration Hub or Proficy Authentication server, you can update or modify the plug-in.

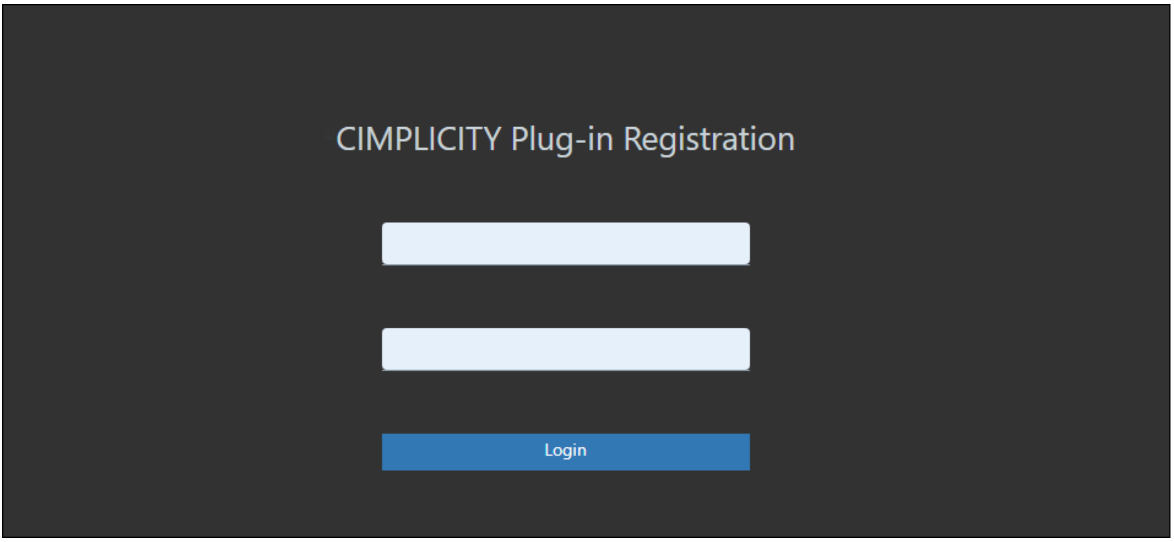
To update or modify the plug-in, do the following:

1. Open the project in **CIMPLICITY Workbench** as needed. For more information on Workbench, refer to the section About the CIMPLICITY Workbench. *(on page*

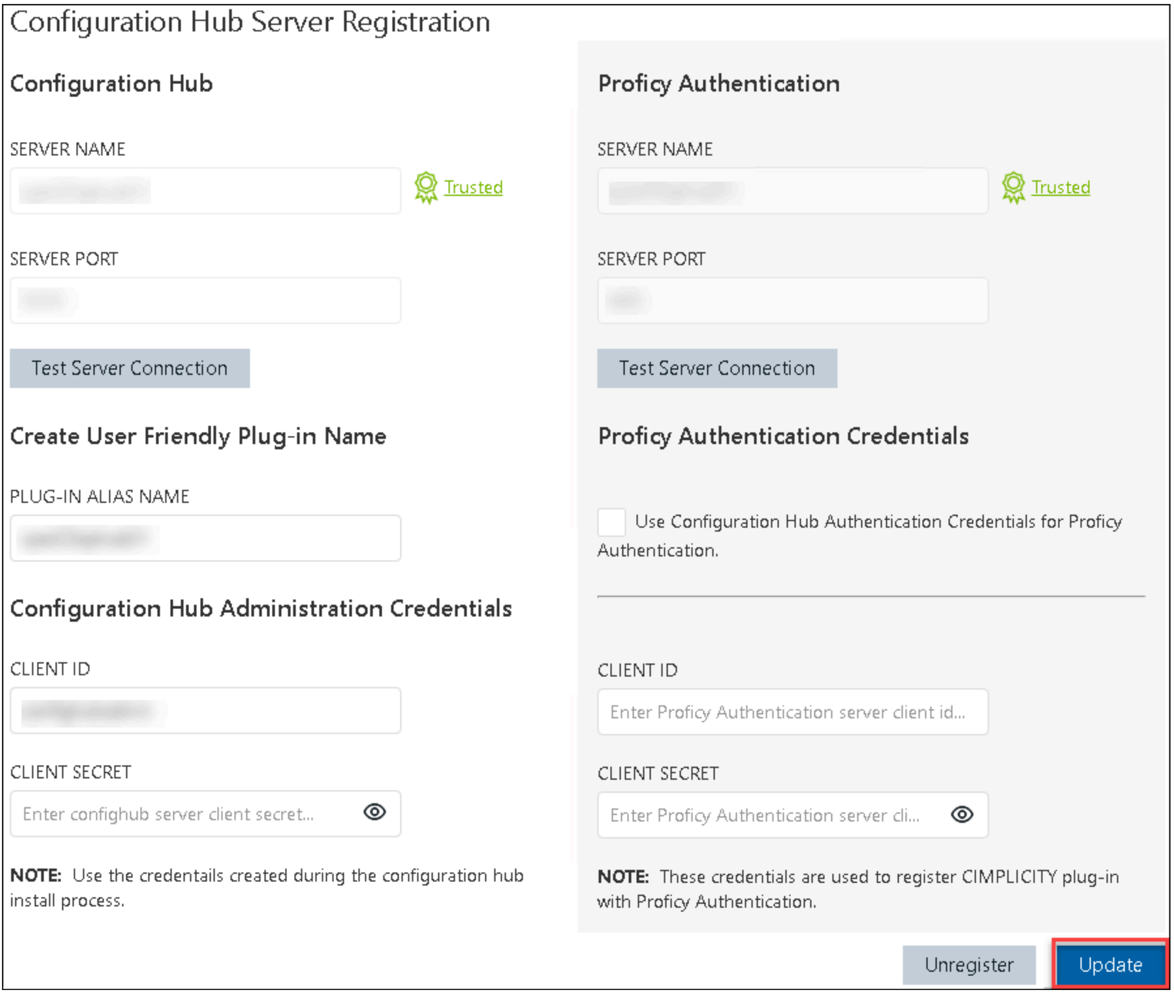
).
2. From the toolbar, click

   The **CIMPLICITY Plug-in Registration** page

   opens.
3. In the **CIMPLICITY Plug-in Registration** page, enter the computer level username and password that you generated in CIMPLICITY using the **RegisterComputerUser.exe** tool that is available at **[Install location]\Proficy\Proficy CIMPLICITY\exe**.
4. Click **Login**.

The **Configuration Hub Server Registration** page opens.



Configuration Hub Server Registration

Configuration Hub

SERVER NAME

[redacted] Trusted

SERVER PORT

[redacted]

Create User Friendly Plug-in Name

PLUG-IN ALIAS NAME

[redacted]

Configuration Hub Administration Credentials

CLIENT ID

[redacted]

CLIENT SECRET

Enter confighub server client secret...

NOTE: Use the credentails created during the configuration hub install process.

Proficy Authentication

SERVER NAME

[redacted] Trusted

SERVER PORT

[redacted]

Proficy Authentication Credentials

☐ Use Configuration Hub Authentication Credentials for Proficy Authentication.

CLIENT ID

Enter Proficy Authentication server client id...

CLIENT SECRET

Enter Proficy Authentication server cli...

NOTE: These credentials are used to register CIMPLICITY plug-in with Proficy Authentication.

5. Modify the **PLUG-IN ALIAS** as needed.
6. Enter the Configuration Hub Administration Credentials and Proficy Authentication Credentials. In case if there is an update in the Client ID and Secret credentials, enter the updated credentials.
7. Click **Update**.

   The updated plug-in is registered.

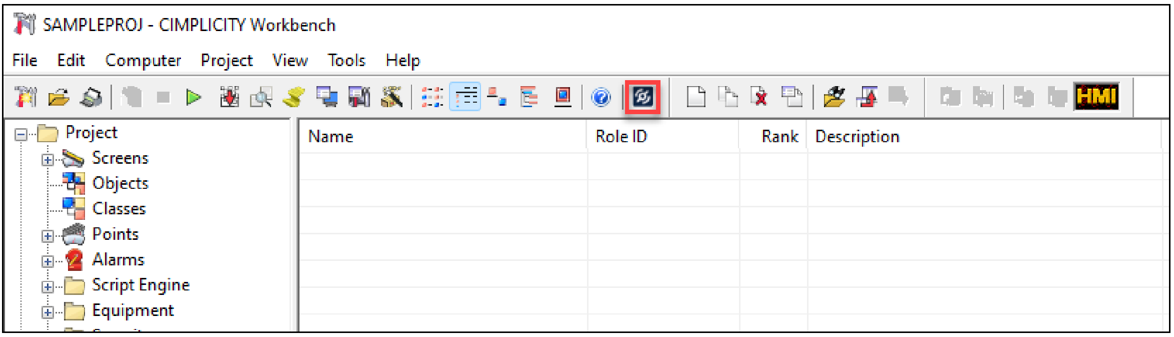
> **Note:**
> When you update the Plug-in alias name, only the name of the plug-in changes and all the associated projects to that specific plug-in node do not change.

Unregister CIMPLICITY Plug-in from Configuration Hub

If you do not need a CIMPLICITY plug-in in Configuration Hub for any reason, you can unregister the plug-in completely from Configuration Hub. Once you unregister the plug-in, that plug-in node is completely removed along with all the associated projects.

To unregister a CIMPLICITY plug-in, do the following:

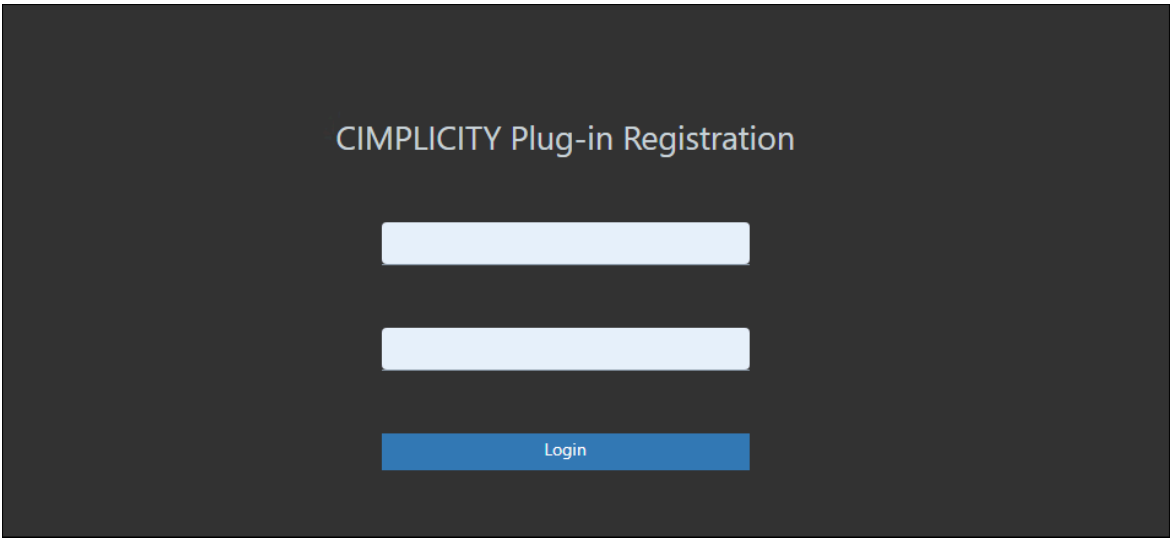
1. Open the project in **CIMPLICITY Workbench** as needed. For more information on Workbench, refer to the section About the CIMPLICITY Workbench. *(on page*



).

2. From the toolbar, click

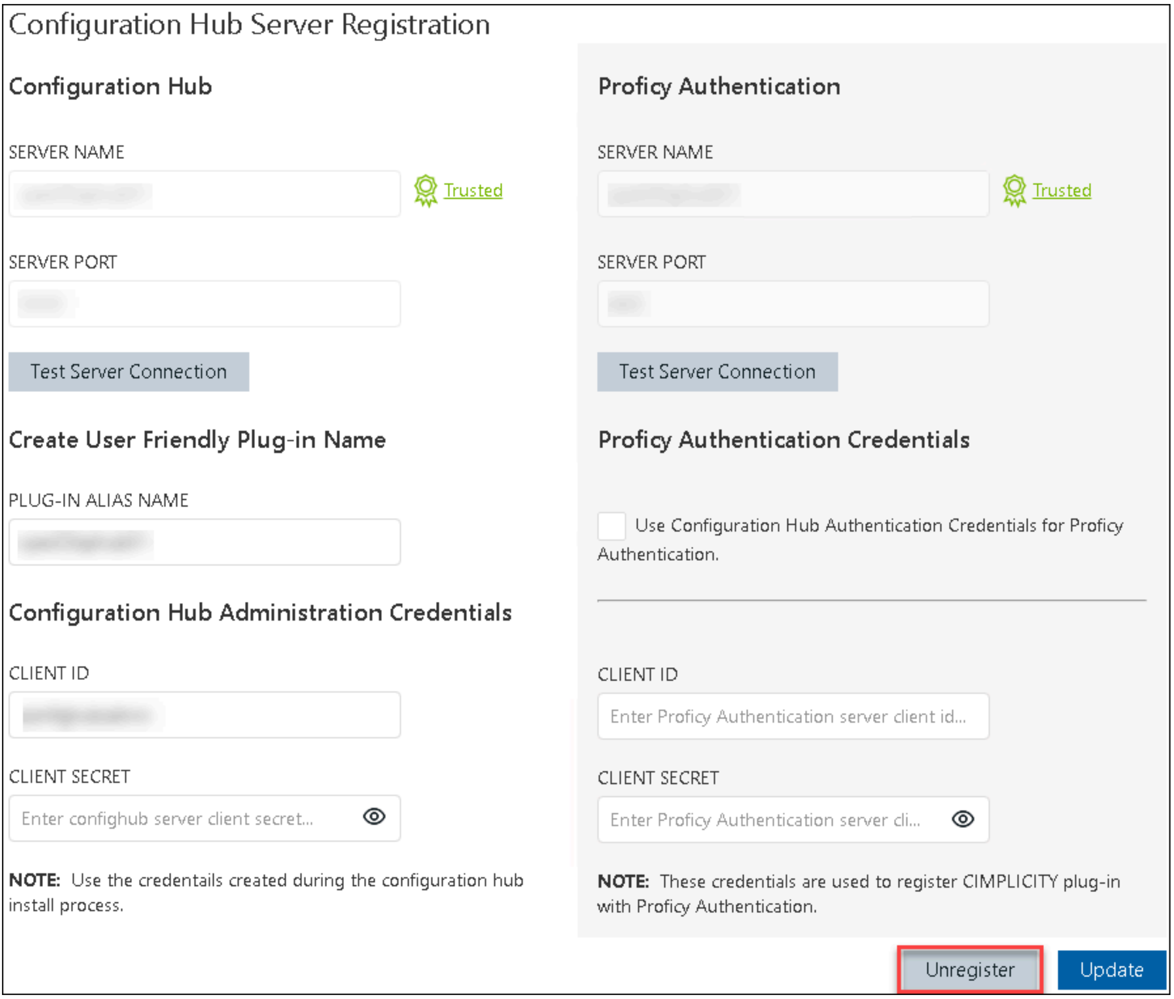
   The **CIMPLICITY Plug-in Registration** page



   opens.

3. In the **CIMPLICITY Plug-in Registration** page, enter the computer level username and password that you generated in CIMPLICITY using the **RegisterComputerUser.exe** tool that is available at **[Install location]\Proficy\Proficy CIMPLICITY\exe**.
4. Click **Login**.

The **Configuration Hub Server Registration** page opens.



Configuration Hub Server Registration

Configuration Hub

SERVER NAME

Trusted

SERVER PORT

Test Server Connection

Create User Friendly Plug-in Name

PLUG-IN ALIAS NAME

Configuration Hub Administration Credentials

CLIENT ID

CLIENT SECRET

Enter confighub server client secret...

NOTE: Use the credentails created during the configuration hub install process.

Proficy Authentication

SERVER NAME

Trusted

SERVER PORT

Test Server Connection

Proficy Authentication Credentials

□ Use Configuration Hub Authentication Credentials for Proficy Authentication.

CLIENT ID

Enter Proficy Authentication server client id...

CLIENT SECRET

Enter Proficy Authentication server cli...

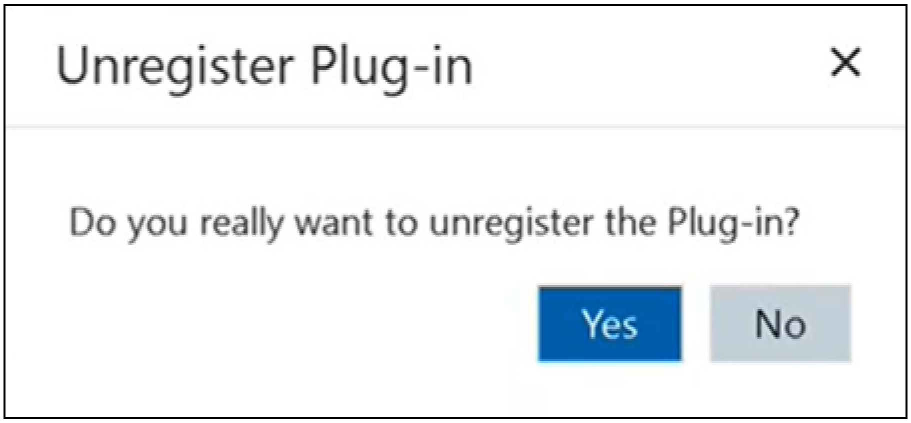
NOTE: These credentials are used to register CIMPLICITY plug-in with Proficy Authentication.

5. Enter the Configuration Hub Administration Credentials and Proficy Authentication Credentials.

> **Note:**
> Ensure to enter valid credentials for both Configuration Hub Administration and Proficy Authentication. Accidentally, if you provide invalid Proficy Authentication credentials and unregister, the plug-in will be unregistered and removed from Configuration Hub; however, the Proficy Authentication registration will still be active for the project.

6. Click **Unregister**.

   The **Unregister Plug-in** window opens.



Unregister Plug-in

Do you really want to unregister the Plug-in?

7. To unregister, click **Yes**.

   The plug-in is unregistered successfully.

   To see the changes, you must log out of Configuration hub and log in again. If you need to register another plug-in, you can register a plug-in again. For more information, refer to section Register CIMPLICITY with Configuration Hub, and Proficy Authentication *(on page 123)*.

Chapter 10. MQTT Client

Getting Started

Introduction

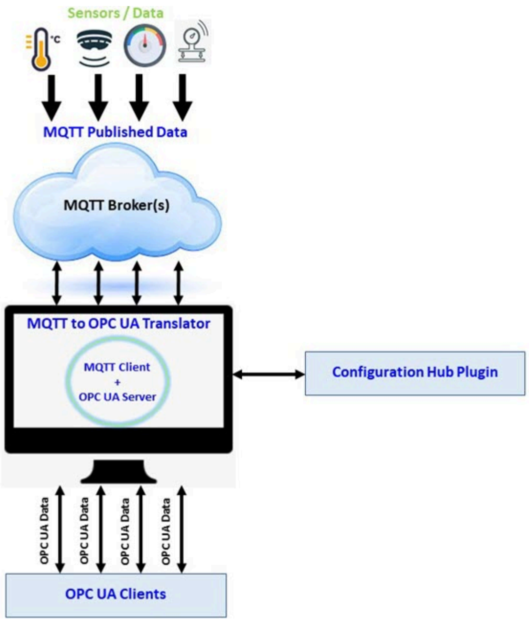
This document describes the importance of the MQTT Client application and its purpose in the GE Proficy product suite. The MQTT Client application can be installed along with the SCADA products using the CIMPLICITY Integrated installer.

Data published from devices such as sensors, units, and other PLCs, is consumed by the MQTT clients. For better communication and interoperability of the SCADA products with MQTT data, we need to support the MQTT protocol. Data received by the MQTT Client is translated to OPC UA data. The translated data is then used by the SCADA products to visualize and monitor the data. This allows you to leverage the advantages of both the MQTT and OPC UA protocols.

The MQTT Client establishes a connection with the MQTT broker and subscribes to the data published on various topics. The published data received through the MQTT Client is then translated into OPC UA data. The OPC UA clients in products such as iFIX, CIMPLICITY, Operations Hub, and so on can connect to the OPC UA server and subscribe to the data.

All the SCADA products at GE can now leverage this application to handle and support MQTT data received from the Client applications.

MQTT in Configuration Hub helps you to configure the MQTT Client and OPC UA Server. For more information, refer to MQTT Client in Configuration Hub *(on page 165)*.



Prerequisites and Hardware Requirements

The following should be installed on your machine before you install the MQTT Client application:

- Proficy Authentication 2023
- Configuration Hub 2023
- CIMPLICITY 2023

Note:
The Proficy products can be installed using the CIMPLICITY Integrated installer.

Hardware Requirements

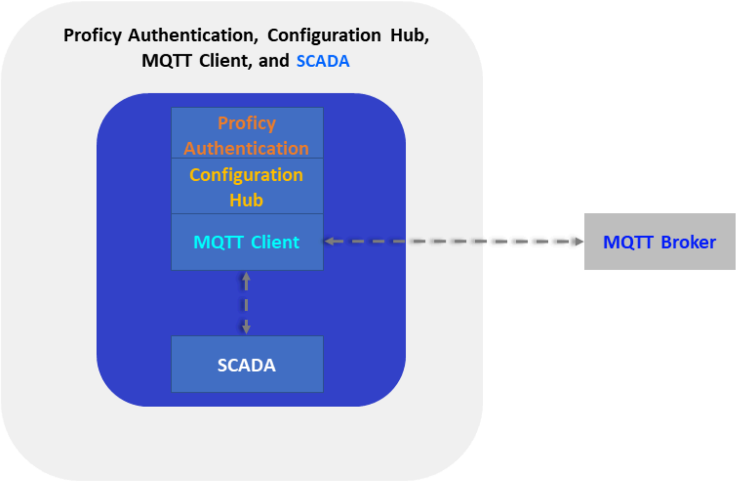
- Operating System Windows 2019 Server, Windows 2022 Server, Windows 10, and Windows 11
- RAM - 8 GB
- CPU - Quad Core

Sample Deployment Architectures

The following examples show different types of deployment architectures to use with the MQTT Client. Configuration Hub and Proficy Authentication are installed only once in each architecture.

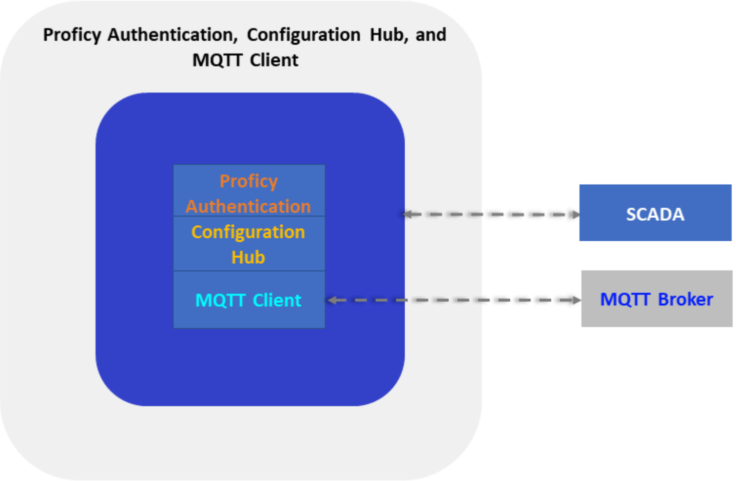
Example 1

The following example shows Configuration Hub, Proficy Authentication, and the MQTT Client installed with SCADA in one computer.



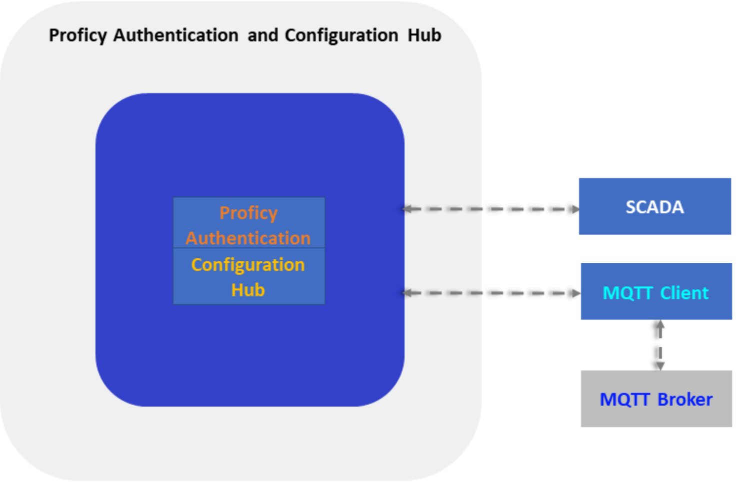
Example 2

The following example shows Configuration Hub, Proficy Authentication, and the MQTT Client installed in one computer, and SCADA on different computer.



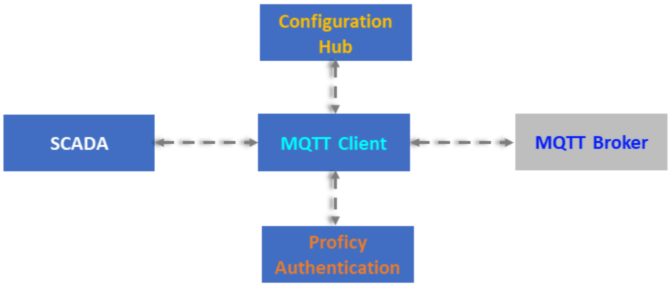
Example 3

The following example shows Configuration Hub and Proficy Authentication in one computer and another computer with SCADA and the MQTT Client.



Example 4

The following deployment architecture illustrates Configuration Hub, Proficy Authentication, SCADA, and the MQTT Client are installed on separate computers.



Installation

The MQTT Client software application is installed using the CIMPLICITY 2023 Integrated installer.

The integrated installer helps you setup and install the following applications on your machine. The MQTT Client enables you to connect the SCADA/HMI clients with MQTT Brokers to communicate with the IoT devices.

1. MQTT Client
2. License Client
3. Proficy Authentication
4. Configuration Hub

Note:

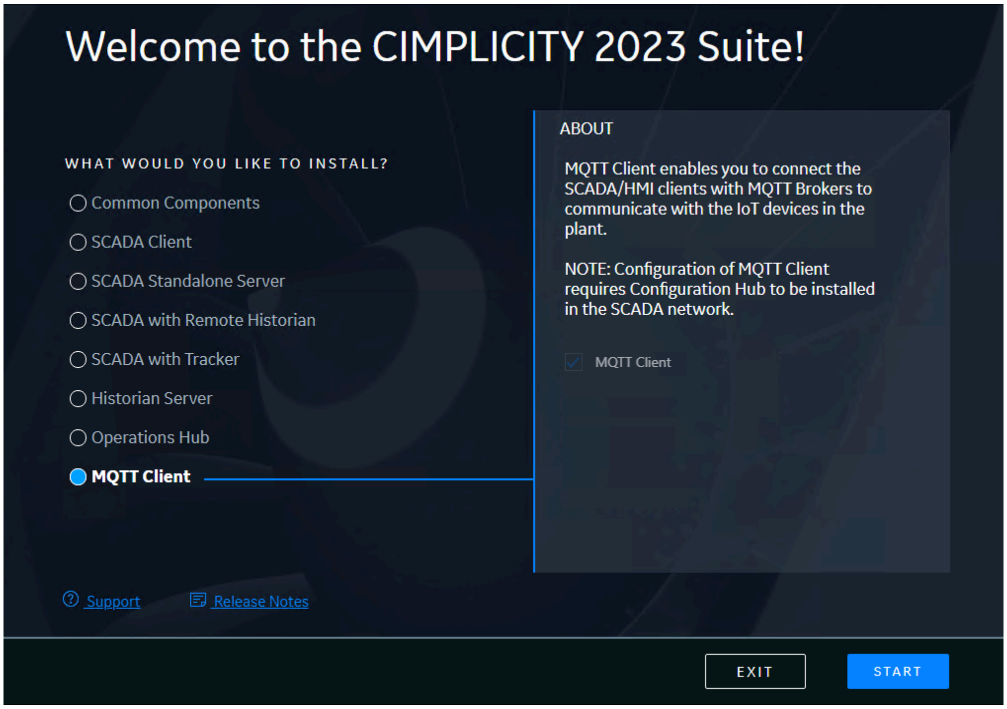
- When you select MQTT Client from the CIMPLICITY Integrated installer, along with the MQTT Client software installation, the License Client will also be installed silently. The License Client helps you manage the license for the MQTT Client software and authenticates you to use the application on your machine.
- Configuration of the MQTT Client requires Configuration Hub to be installed on the SCADA network. Refer to the Configuration Hub documentation for more details.
- Setting up Proficy Authentication provides access to all the products (CIMPLICITY) registered with Configuration Hub. You use the same Proficy Authentication server to authenticate the user of all the products. Refer to the Proficy Authentication documentation for more details.

To install the MQTT Client using the CIMPLICITY Integrated installer:

1. Double-click the `<Integrated Installer>.iso` disc file or select **Mount** from the context menu.
2. Double-click the **Setup.bat** windows batch file, which will launch the CIMPLICITY Integrated installer.

   Note:
   You can also navigate through the **Setup** folder, and then double-click the `setup.exe` application to launch the CIMPLICITY Integrated installer.

   The welcome screen for the CIMPLICITY installation suite appears.
3. Select **MQTT Client**, and then click **START**.



Welcome to the CIMPLICITY 2023 Suite!

WHAT WOULD YOU LIKE TO INSTALL?

- ○ Common Components
- ○ SCADA Client
- ○ SCADA Standalone Server
- ○ SCADA with Remote Historian
- ○ SCADA with Tracker
- ○ Historian Server
- ○ Operations Hub
- ● MQTT Client

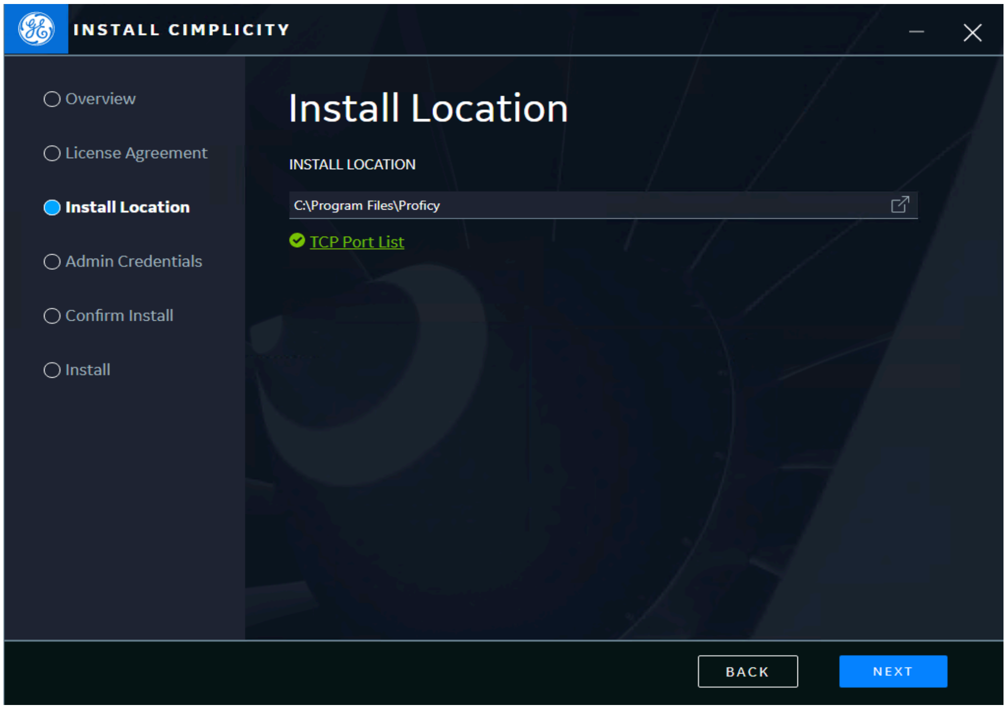
ABOUT

MQTT Client enables you to connect the SCADA/HMI clients with MQTT Brokers to communicate with the IoT devices in the plant.

NOTE: Configuration of MQTT Client requires Configuration Hub to be installed in the SCADA network.

☑ MQTT Client

4. Click **ACCEPT** to proceed with the License Agreement.
5. Click **NEXT** to install the MQTT Client in the default location `C:\Program Files\Proficy` or click ↗ to modify the install location.



Install Location

INSTALL LOCATION

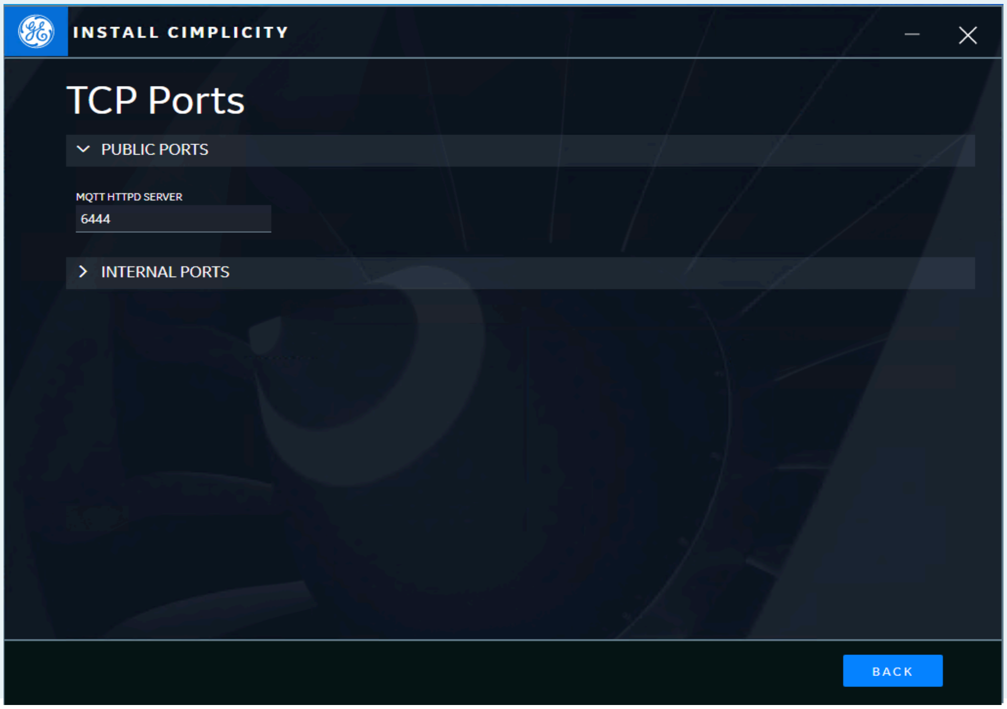
C:\Program Files\Proficy

Note:

- It is recommended to install the MQTT Client application in its default location, that is, `C:\Program Files\Proficy\MqttClient\`.
- You can choose to install the MQTT Client application in a different path, however you cannot install the MQTT Client in the `Program Files (x86)` folder. If you choose `C:\Program Files (x86)\Proficy\MqttClient\` the MQTT Client application will still be installed in its default location, that is, `C:\Program Files\Proficy\MqttClient\`.

Note:

If the default ports are already in use, the Integrated installer will automatically resolve to the next available port numbers. You can check the ports used by the MQTT Client application by selecting TCP Port List.



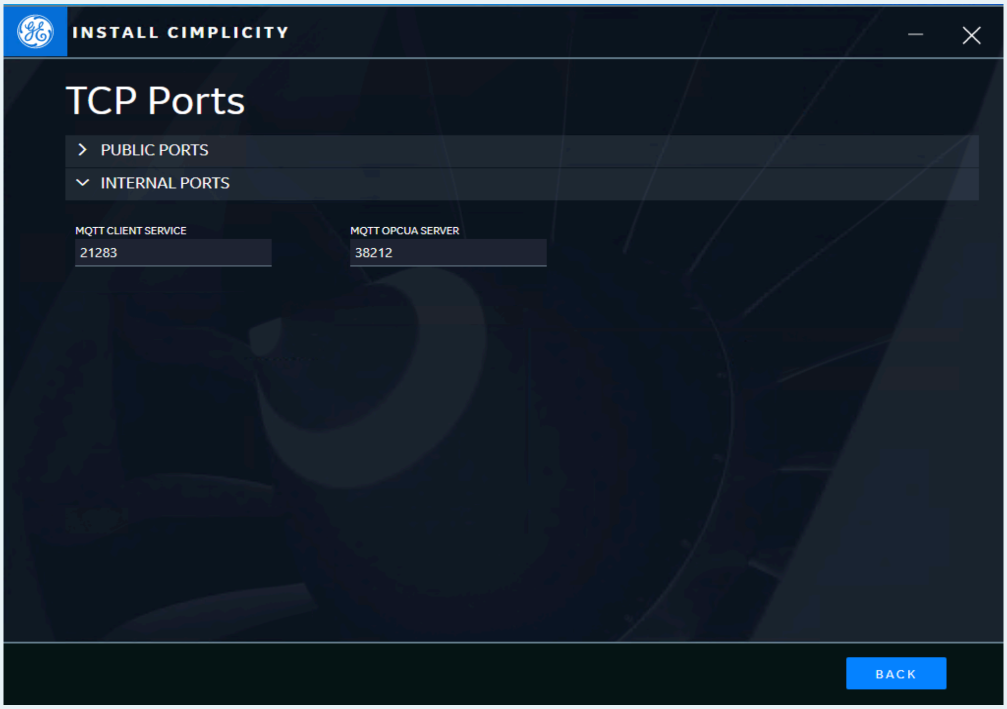
INSTALL CIMPLICITY

TCP Ports

PUBLIC PORTS

MQTT HTTPD SERVER: 6444

INTERNAL PORTS

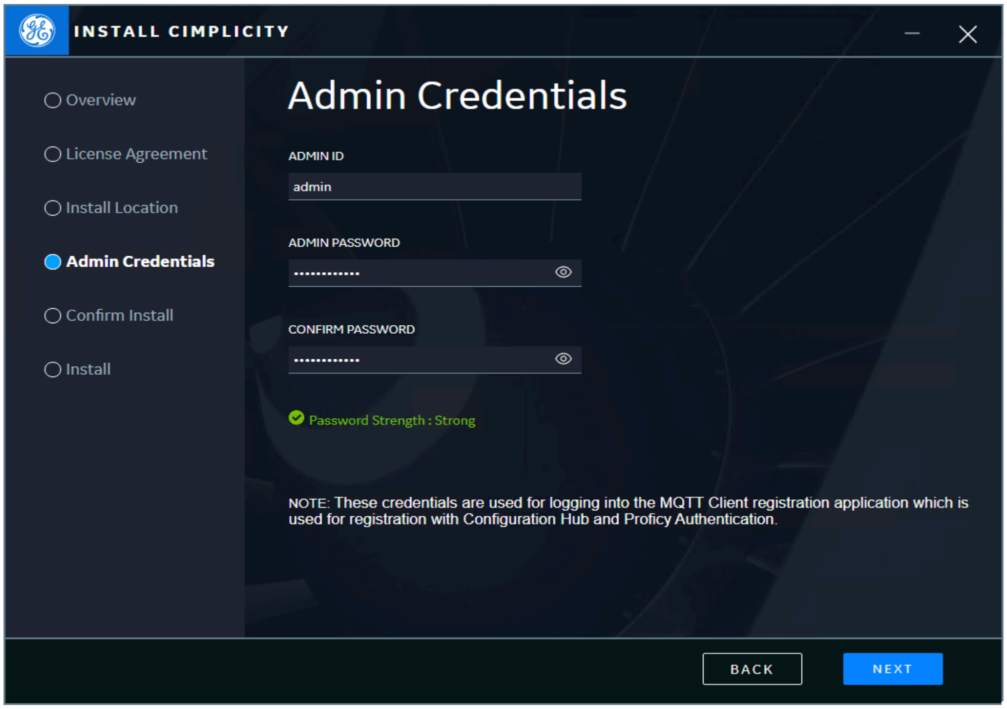


TCP Ports

MQTT CLIENT SERVICE: 21283

MQTT OPCUA SERVER: 38212

6. Create login credentials for MQTT Client, and then click **NEXT**.



Admin Credentials

ADMIN ID: admin

ADMIN PASSWORD: ••••••••••••

CONFIRM PASSWORD: ••••••••••••

✓ Password Strength : Strong

NOTE: These credentials are used for logging into the MQTT Client registration application which is used for registration with Configuration Hub and Proficy Authentication.

Note:

- For a strong password, you must use an alphabet and a number.
- Make a note of the credentials, as the same credentials are used for logging into **MQTT Plug-in Registration**.

7. Click **START** in the **Confirm Install** screen to start the MQTT Client installation.

   The MQTT Client application is installed on your machine.

   Note:
   You can click **Log** for MQTT Client and Proficy Installer to view the respective installation logs.

8. Click **CLOSE**.

   Note:
   You can now enable your HMI/SCADA OPC UA clients to communicate with IoT devices and MQTT brokers by using the MQTT Client application.

9. You must restart your system for proper functioning of the MQTT Client application. Click **REBOOT NOW** to restart your system.

   Note:
   Click **REBOOT LATER** if you want to restart your system at a later time, or click **INSTALL MORE PRODUCTS** if you want to install common components (Configuration Hub and Proficy Authentication) and other products from the Integrated installer.

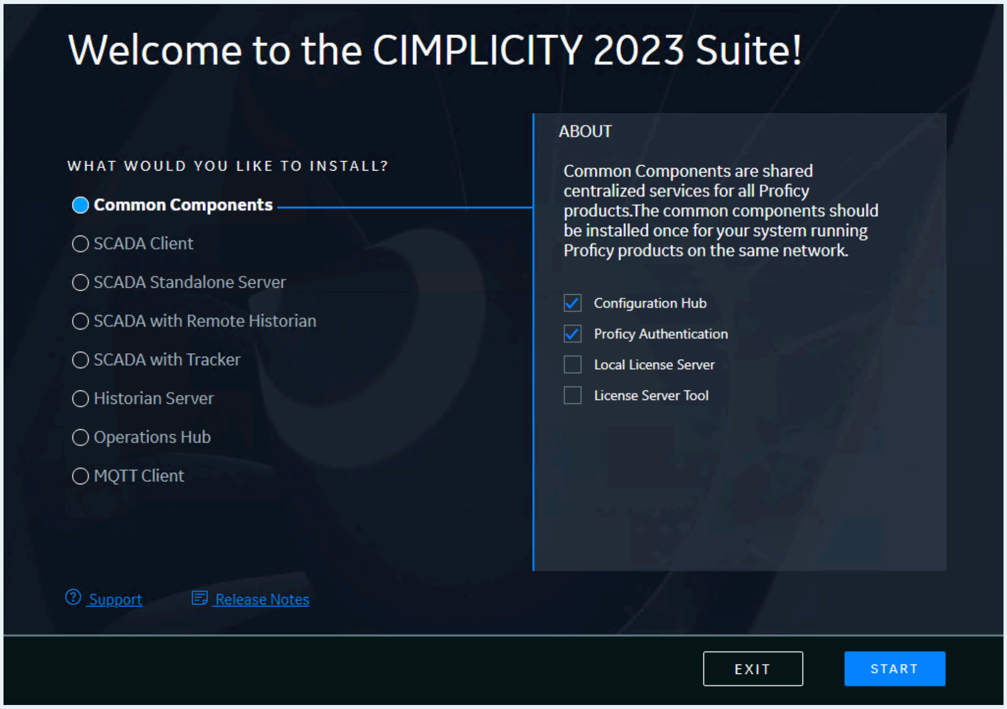
10. Double-click the **MQTT Client Registration** desktop shortcut to register the MQTT Plug-in with the Proficy Authentication and the Configuration Hub servers. Refer to Registration and Proficy Authentication *(on page 156)* for more information.

Registration and Proficy Authentication

You must register the MQTT Client with the Proficy Authentication server and the Configuration Hub server.

After installing the MQTT Client application from the `<Integrated Installer>.iso` disc file, ensure that you have the Configuration Hub and the Proficy Authentication servers installed on the same machine or on a machine that is accessible on the network.

Note:
If the Configuration Hub and Proficy Authentication servers are not installed, you can install them from the Common Components of `<Integrated Installer>.iso` disc file.



Welcome to the CIMPLICITY 2023 Suite!

WHAT WOULD YOU LIKE TO INSTALL?

● Common Components
○ SCADA Client
○ SCADA Standalone Server
○ SCADA with Remote Historian
○ SCADA with Tracker
○ Historian Server
○ Operations Hub
○ MQTT Client

ABOUT

Common Components are shared centralized services for all Proficy products.The common components should be installed once for your system running Proficy products on the same network.

☑ Configuration Hub
☑ Proficy Authentication
□ Local License Server
□ License Server Tool

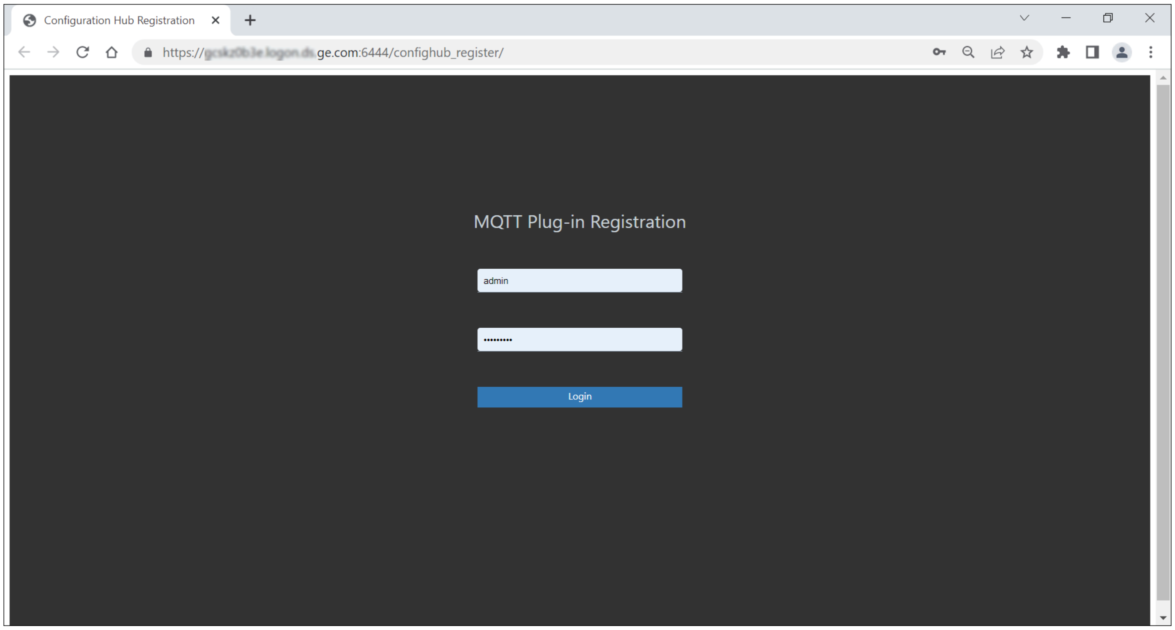
To enable the connection between the MQTT server and Configuration Hub, you must register the MQTT Client with the Proficy Authentication and the Configuration Hub servers.

To register the MQTT Client with the Proficy Authentication and the Configuration Hub servers:

1. Double-click the **MQTT Client Registration** desktop shortcut.

   Note:
   The MQTT Client Registration desktop shortcut appears only after you install the MQTT Client application from the `<Integrated Installer>.iso` disc file. Refer to MQTT Client Installation *(on page 151)* for more information.

   The **MQTT Plug-in Registration** page appears.



Configuration Hub Registration

https://[redacted]ge.com:6444/confighub_register/

MQTT Plug-in Registration

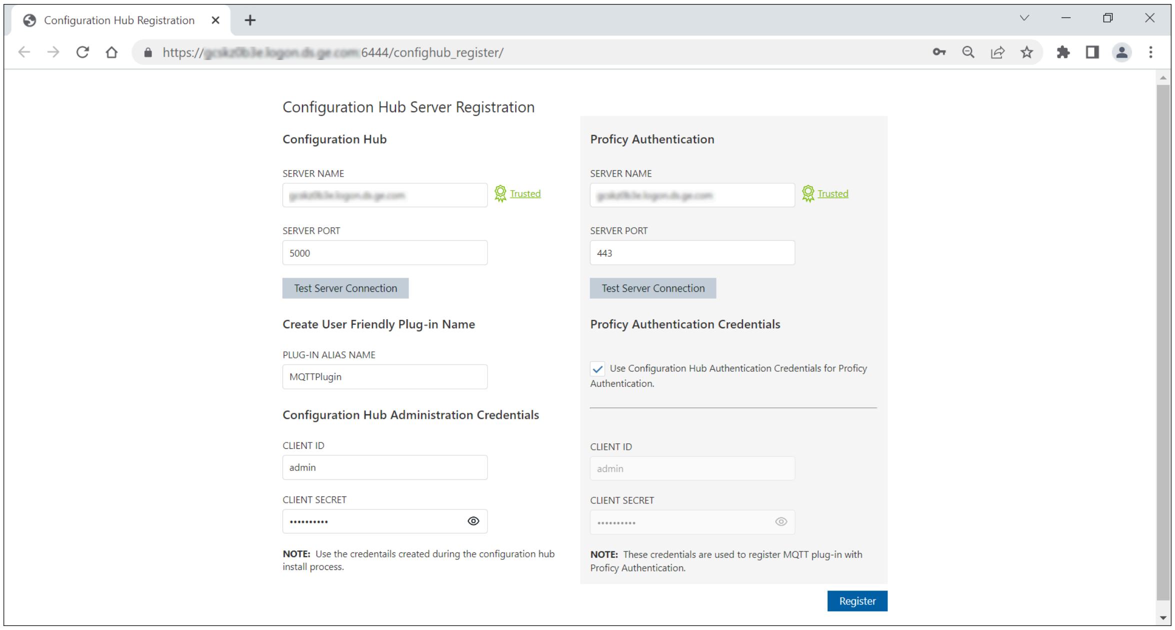
admin

•••••••••

2. Enter your login credentials and then, click **Login**.

> **Note:**
> Enter the login credentials you created during the MQTT Client installation.

The **Configuration Hub Server Registration** page appears.



Configuration Hub Registration

https://[redacted]6444/confighub_register/

Configuration Hub Server Registration

Configuration Hub

SERVER NAME

[redacted] Trusted

SERVER PORT

5000

Create User Friendly Plug-in Name

PLUG-IN ALIAS NAME

MQTTPlugin

Configuration Hub Administration Credentials

CLIENT ID

admin

CLIENT SECRET

••••••••••

NOTE: Use the credentails created during the configuration hub install process.

Proficy Authentication

SERVER NAME

[redacted] Trusted

SERVER PORT

443

Proficy Authentication Credentials

☑ Use Configuration Hub Authentication Credentials for Proficy Authentication.

CLIENT ID

admin

CLIENT SECRET

••••••••••

NOTE: These credentials are used to register MQTT plug-in with Proficy Authentication.

3. In the **Configuration Hub** section, enter the following details:

Field	Description
SERVER NAME	The name of the Configuration Hub server to which you want to register. In the <Fully qualified domain name> format.
SERVER PORT	The port number of the Configuration Hub server to which you want to register.
PLUG-IN ALIAS NAME	The alias name for the MQTT plugin that you want to see in the Configuration Hub. **Note:** By default, the name populated is the machine name where the MQTT Client is installed. However, you can update it to how you want to see the MQTT plugin name in the Configuration Hub. **Important:** Do not use the dot (.) character for the MQTT plugin alias name.
CLIENT ID	The client ID of the Configuration Hub server that you provided during the Configuration Hub installation.
CLIENT SECRET	The client secret of the Configuration Hub server that you provided during the Configuration Hub installation.

4. In the **Proficy Authentication** section, enter the following details:

Field	Description
SERVER NAME	The name of the Proficy Authentication server to which you want to register the Configuration Hub server and the MQTT Client. In the<Fully Qualified Domain Name> format.

Field	Description
SERVER PORT	The port number of the Proficy Authentication server to which you want to register the Configuration Hub server and the MQTT Client.
Use Configuration Hub Authentication Credentials for Proficy Authentication	Select this check box if you entered the same credentials (Client ID and Client Secret) for both Configuration Hub and Proficy Authentication during installation.
CLIENT ID	The Client ID of the Proficy Authentication server.
CLIENT SECRET	The Client secret of the Proficy Authentication server.

5. If the root certificates of the Configuration Hub server and the Proficy Authentication server are not trusted:

    - Click **Not trusted**.

      The **Certificate Details** page appears.

    - Click **Trust**.

   The **Root certificate Import successful** message appears.

6. To test the server connection, click **Test Server Connection**.

   If the connection to the Configuration Hub or the Proficy Authentication server is successful, you will receive a success dialog. If your connection is unsuccessful, retry to connect to another valid Configuration Hub or Proficy Authentication server.

7. Click **Register**.

   The Configuration Hub Server registration success message appears.

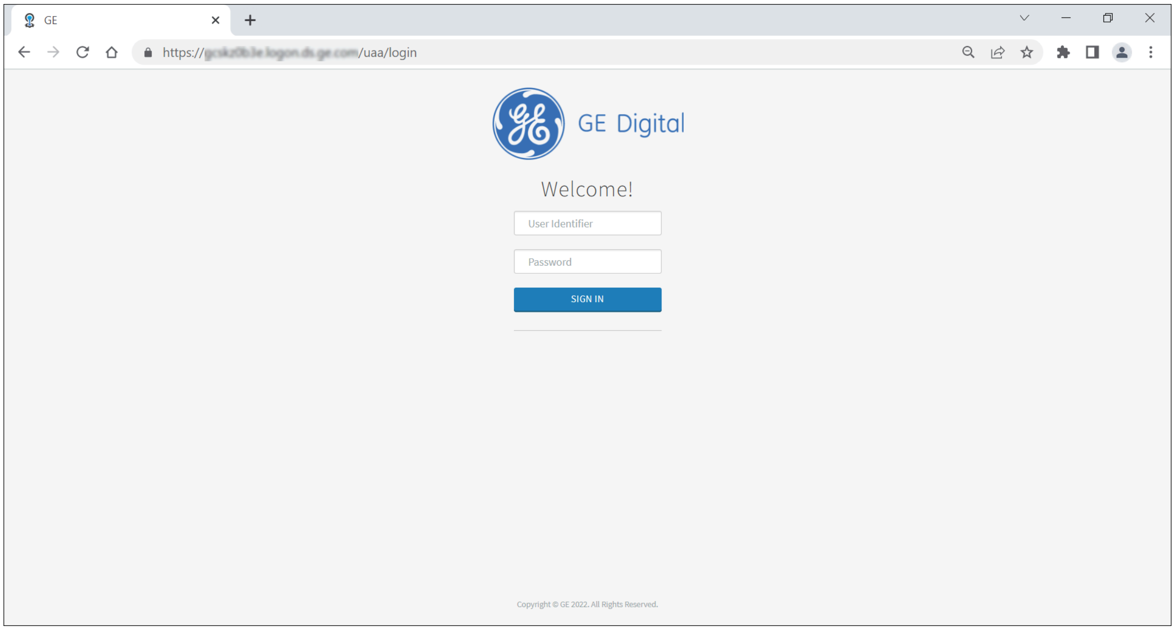
   By default, the ch_admin user is created with a password the same as the Proficy Authentication secret, and the required Group Membership is assigned to the ch_admin user to access the MQTT Client. For more information, refer to Manage Identity Providers, Groups, and Users *(on page 165)*.

8. Click **OK**.

Note:

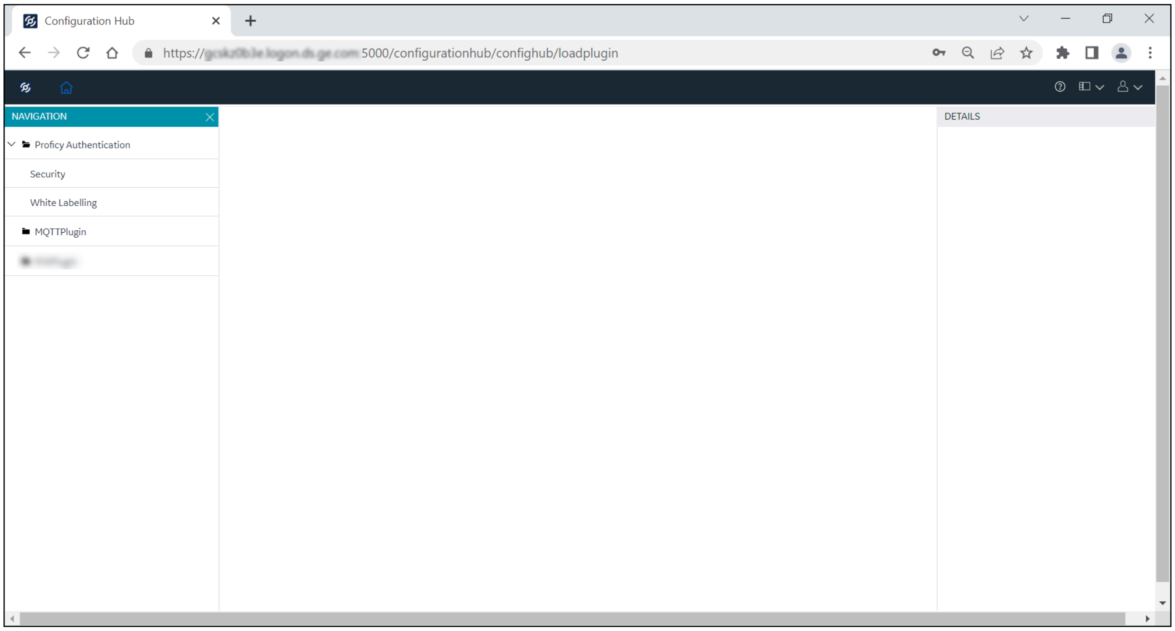
- You can return to the Configuration Hub Server Registration window to modify the field entries in the Configuration Hub and Proficy Authentication sections, and then click **Update** to apply the changes.
- If you uninstall and then reinstall the MQTT Client application, you must register your MQTT Client with Configuration Hub again (See step 1 to step 8).

9. Double-click the **Configuration Hub** desktop shortcut.


GE
https://[redacted]/uaa/login
GE Digital
Welcome!
User Identifier
Password
SIGN IN
Copyright © GE 2022. All Rights Reserved.

10. Enter the following credentials, and then click **SIGN IN**.
    - User Identifier: The default user id for first time users, that is, **ch_admin**.
    - Password: The password you created during Proficy Authentication installation.

The Configuration Hub user interface window appears.



This indicates that you have the MQTT and Proficy Authentication server plugins or connections in the Configuration Hub server. You can see the **PLUG-IN ALIAS NAME** that you entered during the registration. Now you can configure your MQTT Client and communicate with IoT devices.

Note:

- If you are not licensed to use the MQTT Client application, the MQTT Client application will run in Demo mode for two hours, after which the following message will be displayed in the Configuration Hub user interface.

  Demo license expired. Restart the MQTTClient service.

  When you try to load the MQTT plugin connection, the following error message will be displayed.

  Service unavailable. Restart the MqttClient service.

- Perform the following steps to start the MQTT Client Service:
  - Right-click the Windows **Start** menu, and then click **Computer Management**.
  - Click **Services and Applications** and then, double-click **Services**.
  - Click **GE MQTT Client Service** and click **Start** to start the GE MQTT Client Service.
- After you start the GE MQTT Client Service, the Configuration Hub user interface will display the Demo license expiry time.

Utilities

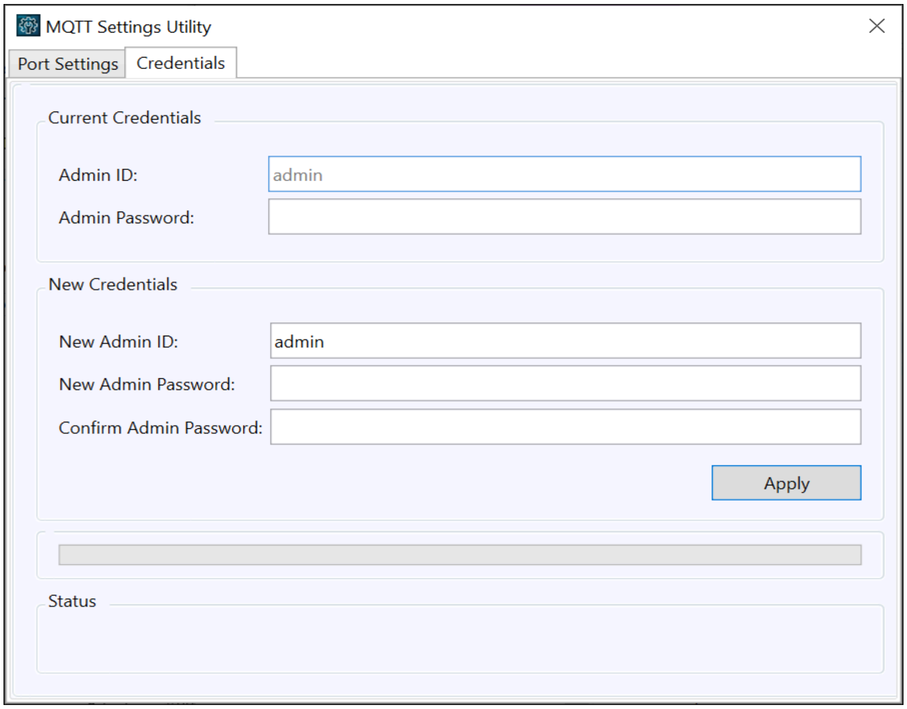
Changing Admin Credentials

After installing the MQTT Client application, if you need to change the MQTT admin credentials, you must perform the following steps.

> **Note:**
> Before you make any changes, you must stop the `GE MQTT Client Httpd Service` and `GE MQTT Client Service` from ⚙ **Services**.

1. Navigate to the MQTT Client install location `<Install location>\MqttClient`.
2. Double-click `MQTTSettingsUtility.exe`.

   The **MQTT Settings Utility** dialog appears.
3. Select the **Credentials** tab.



MQTT Settings Utility

Current Credentials

Admin ID: admin

Admin Password:

New Credentials

New Admin ID: admin

New Admin Password:

Confirm Admin Password:

Status

4. In **Current Credentials**, enter:
   - **Admin Password:** The password you created during MQTT Client installation.

   In **New Credentials**, enter:

- **New Admin ID:** Enter the new admin Id.
- **New Admin Password:** Enter the new admin password.
- **Confirm Admin ID:** Confirm the admin password.

5. Click **Apply**.
6. Restart `GE MQTT Client Service` and `GE MQTT Client Httpd Service` from **Services**.

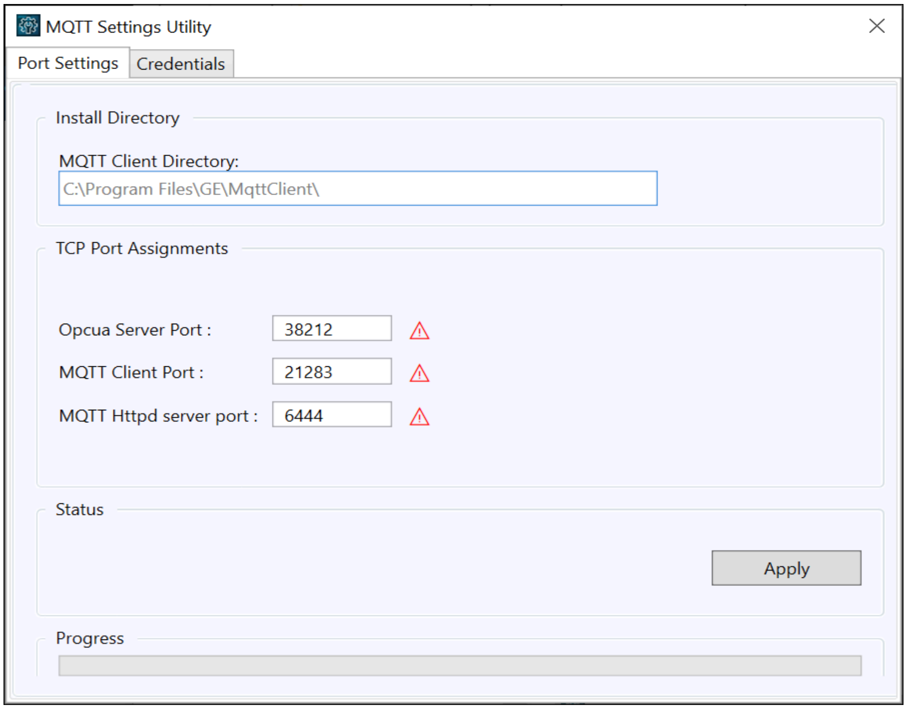
Port Changes

After installing the MQTT Client application, if you need to change any of the MQTT ports, that is, MQTT Client, MQTT OPC UA server, and MQTT Httpd server, you must perform the following steps.

> **Note:**
> Before you make any changes, you must stop `GE MQTT Client Httpd Service` and `GE MQTT Client Service` from **Services**.

1. Navigate to the MQTT Client install location `<Install location>\MqttClient`.
2. Double-click `MQTTSettingsUtility.exe`.

   The **MQTT Settings Utility** dialog appears.
3. Select the **Port Settings** tab.



MQTT Settings Utility

Port Settings | Credentials

Install Directory

MQTT Client Directory: C:\Program Files\GE\MqttClient\

TCP Port Assignments

Opcua Server Port : 38212

MQTT Client Port : 21283

MQTT Httpd server port : 6444

Status

Progress

4. Edit the port numbers you need to change, and then click **Apply**.
5. Restart `GE MQTT Client Service` and `GE MQTT Client Httpd Service` from ⚙ **Services**.

Configuration

MQTT Client in Configuration Hub

Configuration Hub allows you to manage the MQTT Client connections to multiple broker(s) that collect, store, and retrieve data parameters.

To take advantage of the configuration of different data parameters from the MQTT broker(s), you must register the MQTT Client with the Configuration Hub server. Refer to Registration and Proficy Authentication *(on page 156)* on how to register the MQTT client connections.

For more information on configuration, refer to MQTT Client Configuration *(on page 165)*.

MQTT Client Configuration

Use the following steps to configure the MQTT connections in the Configuration Hub.

1. Manage Identity Providers, Groups, and Users *(on page 165)*.
2. Add MQTT Server for Broker Connection *(on page 167)*.
3. Add Subscriptions to Broker Connection *(on page 173)*.
4. Add Tags to Subscription *(on page 184)*.

Manage Identity Providers, Groups, and Users

By default, the username *ch_admin* is created in the Proficy Authentication server after registering MQTT Client with the Configuration Hub server. For the first time, you can log in to the Configuration Hub user interface using this username (the password will be the same as the Proficy Authentication secret). After you log in to Configuration Hub, as an administrator, navigate to **Proficy Authentication > Security**. Depending on the groups assigned to the user, the user will have permissions to access the MQTT client configuration.

Select the user to whom you want to assign a group membership. The **DETAILS** section displays the details of the user. Click **GROUP MEMBERSHIP** ↗; the group membership window displays the list of available groups that can be assigned to the user. Depending on the groups assigned, the user will have scope to access MQTT client configuration. Only the administrator with admin rights in **Security-Proficy Authentication** can provide user permissions to the groups.

Refer to the **Proficy Authentication** help documentation for more details on managing Groups and Users.

For more information on MQTT groups and access provisions, refer to MQTT Groups in Proficy Authentication *(on page 166)*.

MQTT Groups in Proficy Authentication

Proficy Authentication provides group membership access for MQTT clients, such that the users can access the MQTT client configuration from Configuration Hub and read/write OPC UA data.

Table 2. Group Membership

MQTT Group Membership	Access Provision
protocoltranslators.mqtt.<PLUG-IN ALIAS NAME>.config.read	Retrieve the list of broker, subscriptions, and tags on the specific MQTT client node that has the Alias name registered with Configuration Hub.
protocoltranslators.mqtt.<PLUG-IN ALIAS NAME>.config.write	• Retrieve/modify/add/delete the list of broker, subscriptions, and tags on the specific MQTT client node that has that Alias name registered with Configuration Hub. • Save and Publish the data.
protocoltranslators.mqtt.<PLUG-IN ALIAS NAME>.opcua.read	This group provides read access to OPC UA clients, so that the OPC UA clients can connect to the MQTT OPC UA server and read the OPC UA data on the specific node.
protocoltranslators.mqtt.<PLUG-IN ALIAS NAME>.opcua.write	This group provides read/write access to OPC UA clients, so that the OPC UA clients can connect to the MQTT OPC UA server and read/write the OPC UA data on the specific node.

Note:
The following groups are shared access groups that provide access to all MQTT client nodes on the network.

- **protocoltranslators.mqtt.shared.config.read**
- **protocoltranslators.mqtt.shared.config.write**

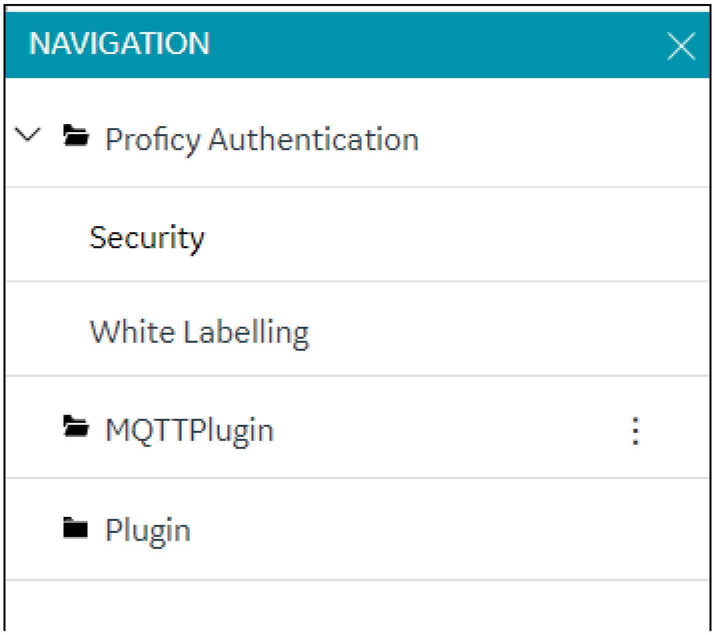
- **protocoltranslators.mqtt.shared.opcua.read**
- **protocoltranslators.mqtt.shared.opcua.write**

Important:
If the groups are not assigned to the user, the MQTT plugin connection will not load any data. Shared access groups are added by default to the **ch_admin** user during plugin registration.

Add MQTT Server for Broker Connection

MQTT Plugin for Broker connections are edited in the **DETAILS** section. After selecting a server configuration in the **Connections** panel, the **DETAILS** section populates the broker details such as server details, reconnect parameters, and so on.

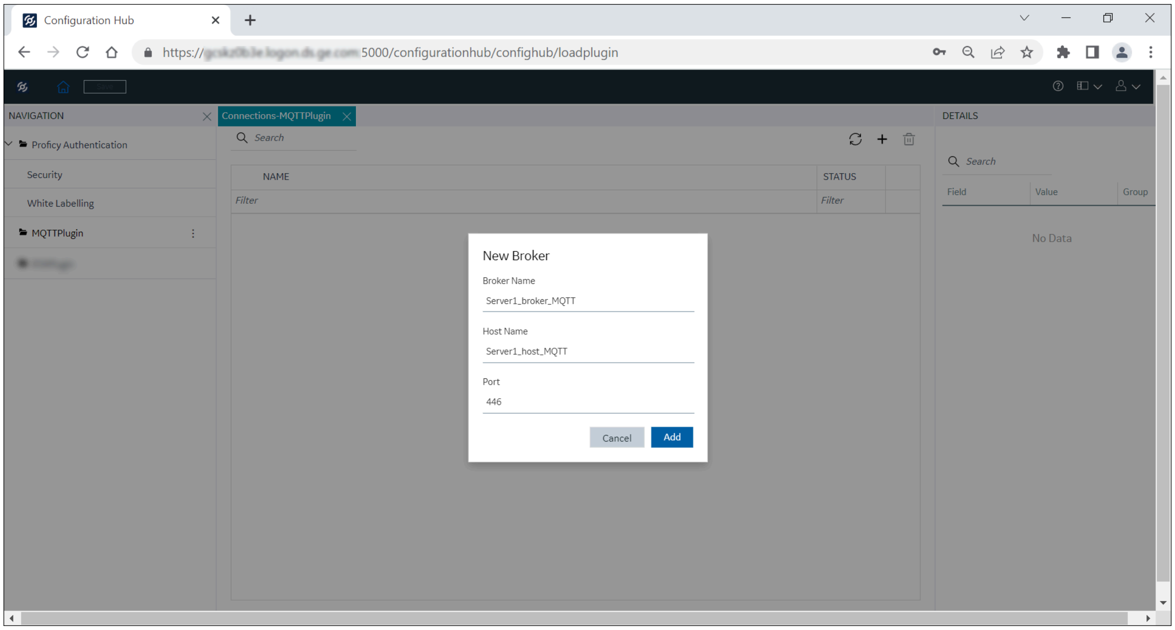
To add the Server for Broker Connection, you must log into Configuration Hub with Proficy Authentication credentials. After you login, the enabled connections appear in the **Navigation** panel.



To add the Server for Broker Connection:

1. Click + to add a new broker.

   The **New Broker** dialog appears.



New Broker

Broker Name: Server1_broker_MQTT

Host Name: Server1_host_MQTT

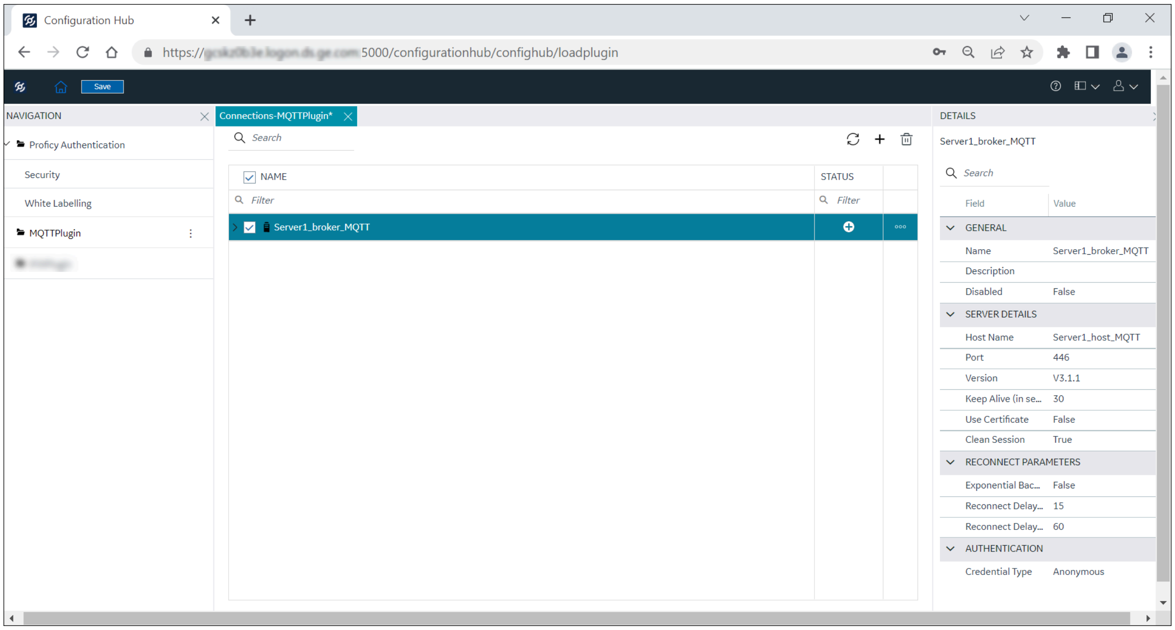
Port: 446

2. Enter the **Broker Name**, **Host Name**, and **Port**. Click **Add**.

Note:

- Adhere to the following rules when entering information:
  - The broker name must start with a letter and cannot exceed 255 characters.
  - Do not include spaces in between names.
  - Names cannot have leading or trailing spaces.
  - The only special characters allowed in the broker name are '-' and '_'.
  - All special characters and numbers are allowed in a Host name. Spaces are not allowed.
  - The port name field cannot include letters. The port number must be in the range 1 to 65535.
  - Field names cannot be left blank. Duplicate names are not allowed.

The new broker is added, and the broker details are displayed in the **DETAILS** section. Click **Save**.



DETAILS

Server1_broker_MQTT

Field	Value
GENERAL	
Name	Server1_broker_MQTT
Description	
Disabled	False
SERVER DETAILS	
Host Name	Server1_host_MQTT
Port	446
Version	V3.1.1
Keep Alive (in se...	30
Use Certificate	False
Clean Session	True
RECONNECT PARAMETERS	
Exponential Bac...	False
Reconnect Delay...	15
Reconnect Delay...	60
AUTHENTICATION	
Credential Type	Anonymous

3. Edit the broker in the **DETAILS** section as required.

Table 3. MQTT Server Details

Field	Value
GENERAL	
Name	Enter a name for the broker connection.
Description	Enter the description for the broker connection.
Disabled	You can enable or disable the broker connection with the client. ◦ **True**: The client is disabled from connecting to the MQTT broker. ◦ **False**: The client is enabled to connect to the MQTT broker. This is the default value.
SERVER DETAILS	
Host Name	Host name of the server on which the MQTT broker is installed.
Port	The port number of the MQTT broker.

Field	Value
Version	The MQTT version (V5 or, V3.1.1 or, V3.1) used to connect to the MQTT broker.
Keep Alive (in seconds)	When there is no exchange of messages or no data flow between the client and the broker for a certain time period, the client will generate a PING request to the broker and the broker will reciprocate by sending a PING response to the client. This confirms the connection is active and the time period to confirm the active connection is the *Keep Alive* period. By default, the *Keep Alive* period is set to 30 seconds. You can modify the *Keep Alive* default value as required to establish the connection.
Use Certificate	To establish a secure connection with the broker, you must import the broker certificate and trust the certificate. ◦ If set to **True**, the following message appears: *'Use certificate' field is set to true, Please upload your certificate by clicking on 'Import certificate' option in the broker context menu.* This indicates that you must import the certificate to enable a secure connection with the MQTT broker. Refer to Secure Connection with Broker *(on page 191)* to import the certificate. Similarly, the MQTT broker must import the client certificate to enable a secure connection with the client. Refer to the broker documentation to import the client certificate. The MQTT Client root certificate is avail-

Field	Value
	able at `<Installation Path>/Pki/own/MqttClientRootCA.crt` ◦ If set to **False**, the MQTT broker connection is not secured.
Clean Session	◦ **True**: The broker does not store any information about the client and disconnects the existing session (for the topic subscribed). However, a new session will be created, and this session will remain active until the network connection is active. The client must re-subscribe to the topics in the new session. This is the default value. ◦ **False**: The broker stores the client information for the topic subscribed so that when the client disconnects and reconnects, the client does not have to re-subscribe to the topics because the information is stored by the broker. Also, the broker stores the QoS1 and QoS2 messages subscribed to by the client when the session is disconnected.
Session Expiry Interval	The Session Expiry Interval is the period after disconnection (client to broker or, broker to client session) during which the messages are persisted. **Note:** The Session Expiry Interval is applicable only when you connect to the broker using MQTT version V5, and if the Clean Session is set to **False**.
RECONNECT PARAMETERS	

Field	Value
Exponential BackOff	The Exponential Backoff helps minimize the number of retries during the connection establishment process. ◦ **True**: Requests or retries to reconnect to the broker are sent as the time increases exponentially. ◦ **False**: Requests are sent according to the reconnect delay parameters.
Reconnect Delay (in seconds)	By default, the Reconnect Delay value is set to 15 seconds. That means, after a connection fails to the server, reconnection to the server will connect every 15 seconds.
Reconnect Delay Max (in seconds)	By default, the reconnect delay maximum value is set to 60 seconds. That means reconnection is attempted as per the values specified in **Reconnect Delay** until the **Reconnect Delay Max** is reached. Subsequently, the reconnection is attempted at the interval specified in the **Reconnect Delay Max** parameter.
AUTHENTICATION	
Credential Type	Valid entries are: ◦ Anonymous ◦ UserName/Password ◦ PreShared Key It is recommended that you select UserName/Password or PreShared Key to provide optimum security. If the UserName/Password

Field	Value
	option is selected, enter the username and password to connect to the MQTT server. **Note:** The Anonymous credential type does not provide any access protection for the data.

After editing the broker details, the **Save** button on the toolbar is enabled to indicate that the Connections panel has changes to be saved. By clicking the **Save** button, the changes made to broker connections are persisted until the changes are published to the MQTT node.

In addition to editing a broker connection, the connection panel supports creating subscriptions under the broker connections. For more details, refer to Add Subscriptions to Broker Connection *(on page 173)*.

Add Subscriptions to Broker Connection

Subscriptions are created under the Broker(s) to subscribe to the data parameters.

The following subscription types are supported:

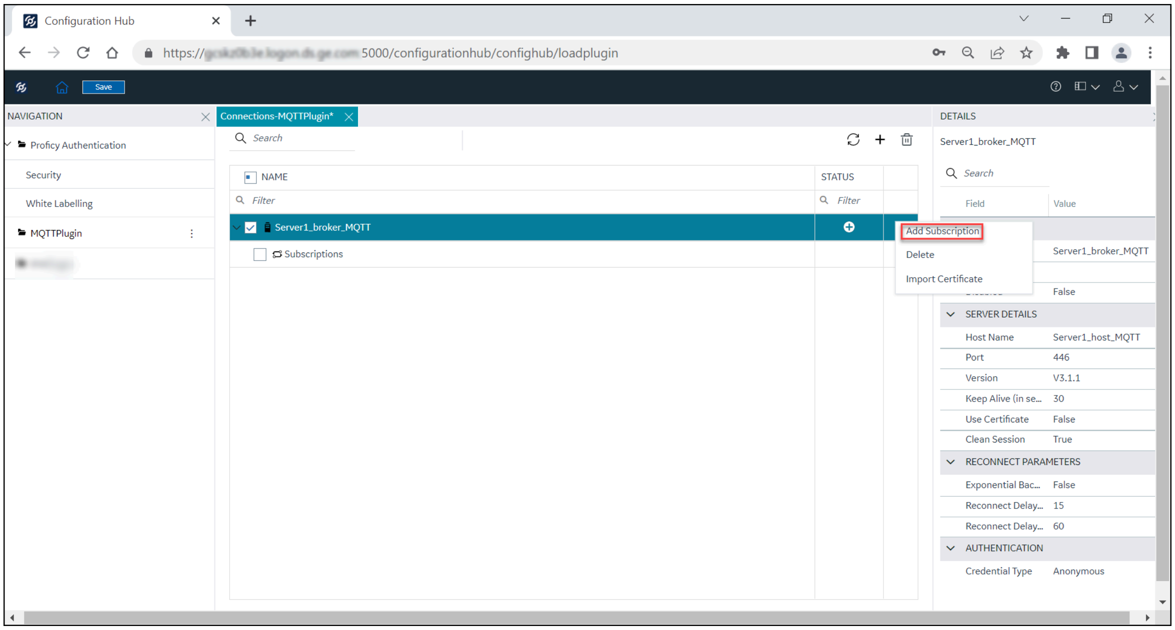
1. JSON
2. Sparkplug-B

Note:
Depending on the IoT data received from the client, you can select the JSON or Sparkplug subscription type.

A subscription is added to a broker connection and a tag is added to a subscription.

To add a Subscription to a Broker Connection:

1. Select **Add Subscription**.

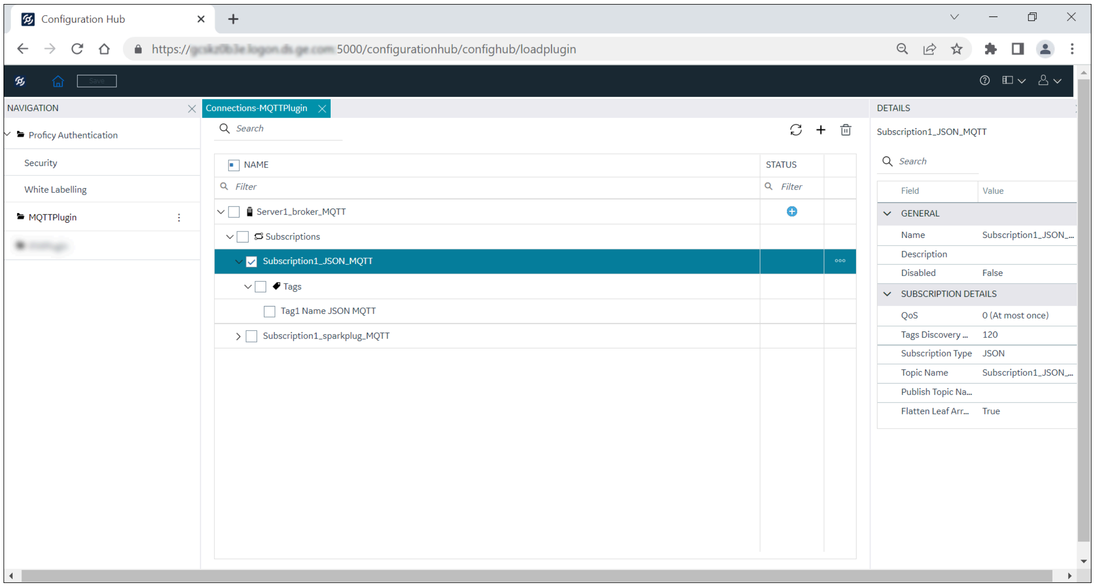


Field	Value
	Server1_broker_MQTT
	False
SERVER DETAILS	
Host Name	Server1_host_MQTT
Port	446
Version	V3.1.1
Keep Alive (in se...	30
Use Certificate	False
Clean Session	True
RECONNECT PARAMETERS	
Exponential Bac...	False
Reconnect Delay...	15
Reconnect Delay...	60
AUTHENTICATION	
Credential Type	Anonymous

The **New Subscription** dialog appears.

2. Select **Subscription Type** (JSON or Sparkplug Bv1.0).
   - If you select JSON, enter a **Subscription Name**, and a **Topic Name**, and then click **Add**.

> **Note:**
>
> - Adhere to the following rules when entering information:
>   - Do not include spaces in between the names.
>   - Names cannot have leading or trailing spaces.
>   - The only special characters allowed are '_' and '-'.
>   - Subscription names must start with a letter.
>   - Field names cannot be blank. Duplicate names are not allowed.
>   - Subscription names cannot exceed 255 bytes.



NAME	STATUS
Server1_broker_MQTT	
Subscriptions	
☑ Subscription1_JSON_MQTT	
Tags	
Tag1 Name JSON MQTT	
Subscription1_sparkplug_MQTT	

Subscription1_JSON_MQTT

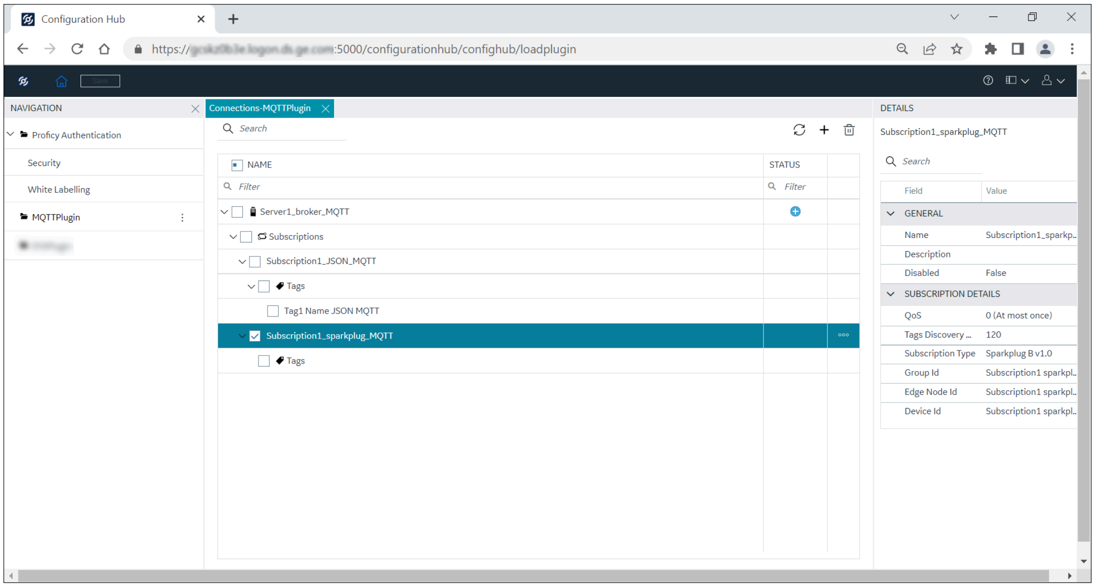
Field	Value
GENERAL	
Name	Subscription1_JSON_...
Description	
Disabled	False
SUBSCRIPTION DETAILS	
QoS	0 (At most once)
Tags Discovery ...	120
Subscription Type	JSON
Topic Name	Subscription1_JSON_...
Publish Topic Na...	
Flatten Leaf Arr...	True

The JSON subscription is added to the broker connection. Click **Save**.

- If you select Sparkplug, enter **Subscription Name**, **Group Id**, **Edge Node Id**, and **Device Id**, and then click **Add**.

Note:

- Adhere to the following rules when entering information:
  - Subscription names must start with a letter and cannot exceed 255 characters.
  - The only special characters allowed are '_' and '-'.
  - Do not include spaces in between the names.
  - Names cannot have leading or trailing spaces.
  - For *Group Id* and *Edge Node Id*, the special characters **+** and **#** are not allowed.
  - Field names cannot be left blank (the *Device Id* field can be left blank if the subscription is for an Edge Node). Duplicate names are not allowed.



Subscription1_sparkplug_MQTT

Field	Value
GENERAL	
Name	Subscription1_sparkp...
Description	
Disabled	False
SUBSCRIPTION DETAILS	
QoS	0 (At most once)
Tags Discovery ...	120
Subscription Type	Sparkplug B v1.0
Group Id	Subscription1 sparkpl...
Edge Node Id	Subscription1 sparkpl...
Device Id	Subscription1 sparkpl...

The Sparkplug subscription is added to the broker connection. Click **Save**.

Table 4. Subscription Details

Field	Value
GENERAL	
Name	Enter a name for the subscription.
Description	Enter the description for the subscription.
Disabled	Enables or disables the subscription with the client: ▪ **True**: The subscription is disabled. ▪ **False**: The subscription is enabled.
SUBSCRIPTION DETAILS	
QoS	The Quality of Service (QoS) specifies three levels (QoS0, QoS1, and QoS2) at which the messages are delivered between the publishing client (sender) to the broker (receiver) and from the broker (sender) to the subscribing client (receiver). The QoS level selection provides easy communication even when the network is not reliable.

Field	Value
	▪ QoS0: At most once ▪ No assurance of message delivery. ▪ Best efforts to deliver message only once. ▪ No acknowledgement receipt of the message from the receiver, message is not transmitted back to the sender, and the message is not stored. ▪ QoS1: At least once ▪ Ensures message delivery at least once to the receiver. ▪ Does not prevent delivering the messages multiple times to the receiver. ▪ Receiver acknowledges the message, and the sender stores the message. ▪ QoS2: Exactly once ▪ Ensures each message is delivered to the receiver only once. ▪ Receiver confirms the message delivery for each message from the sender. ▪ Requires two request/response flows between the sender and the receiver. ▪ Receiver acknowledges the message, and the sender stores the messages. ▪ Acknowledgement of delivered messages are received

Field	Value
	by the sender until the published messages are available to use. **Note:** QoS2 level is most reliable, but the quality of service is slower than QoS0 and QoS1.
Tags Discovery Duration (in sec)	The Tags Discovery Duration is the duration period to fetch the tags. Tags fetched after the discovery are then added to the topic subscribed. This parameter helps the user to dynamically fetch the tags for a specific topic name and for a specific time duration. By default, the tags discovery duration is set to 120 seconds. You can modify the value as required. **Note:** ▪ You can select **Start Tag Discovery**, **Stop Tag Discovery**, and **Show Discovered Tags** by using the overflow icon ⋮, next to the subscription. ▪ If you select **Start Tag Discovery**, the Time Remaining in seconds is displayed. ▪ After the time remaining ends, or if you prematurely stop the tag discovery, select **Show Discovered Tags** to view the published tags. You can modify the Data Type and Read Write parameters. If modified, select the spe-

Field	Value
	cific tag, and then click **Add** to view the modified tag to the tags list for the topic subscribed.
Subscription Type	Displays the subscription type.
JSON Subscription	
Topic Name	Enter a topic name to which you want to subscribe. **Example:** - Entering **test1/#** indicates that the client can listen to any topic that starts with test1/. **Note:** The character # is a key word that has to be the last value. You can choose to enter any topic name in place of the key word # to differentiate multiple topics. That is, if you enter test1/test2, the client can listen explicitly to test1/test2. - Entering **test1/+/temperature** indicates that the client can listen to any topic name used in place of + to differentiate a single topic. **Note:** The character + is a key word between test1 and temperature. If you enter test1/

Field	Value
	test2/temperature, the client can listen explicitly to test1/test2/temperature.
Publish Topic Name	Publish Topic Name, if provided by the user, will be used by the MQTT client when publishing the data; that is, when a user writes to a specific tag in the subscription using the OPC UA client, the data will be published with that specific publish topic name. **Note:** If the Publish Topic Name field is left empty, then no data will be published to the broker even though the user modifies on the OPC UA side.
Flatten Leaf Arrays	The Flatten Leaf Array parameter is used to consider the array tags as a whole or flatten the tag arrays (for example, if you have 100 elements in a JSON array, then you can choose to create a single array tag or, create 100 unique tags each pointing to an array element). By default, Flatten Leaf Arrays is set to True. ▪ True: A unique tag for each element of the array will be created. ▪ False: A single array tag for all the elements will be created. Also, the **Configure Leaf Array Elements** are enabled to configure the respective tag elements in **TAG DETAILS** section.

Field	Value
	Note: The **Configure Leaf Array Elements** (that is, Leaf Array Rank, Leaf Array Dimensions, and Leaf Array Data Type) are able to be configured only if the **Data Type** is set to **DataSet**.
Sparkplug Subscription	
Group Id	Enter a Group Id for the topic subscribed.
Edge Node Id	Enter an Edge Node Id for the topic subscribed.
Device Id	Enter a Device Id for the topic subscribed. The topic device id is the identification of a device attached to the MQTT Edge node. The device id field is optional. **Note:** ▪ If the Device ID field is left empty, it will be considered an Edge node. ▪ If you enter the Device ID field, it will be considered as a Device node.

Important:
After configuring the changes, click **Save** to save the connection parameters.

Any application requesting the data from the MQTT broker is subscribed to the JSON or Sparkplug type depending on the data loaded from the IoT.

Tags are added under the Subscriptions to store specific data from the subscription. Refer to Add Tags to Subscription *(on page 184)* to add Tags under each Subscription.

JSON Supported Payload

The JSON payload must have the root as a JSON object. Other root types are not supported.

The following are examples of JSON supported payloads:

Simple JSON

```
{
 "IntVal":56,
 "DoubleVal":2.9574e58,
 "BoolVal":false,
 "StringVal":"this is a string"
}
```

In the above payload, the tags created are *IntVal*, *DoubleVal*, *BoolVal*, and *StringVal*.

Nested JSON

```
{
 "IntVal":56,
 "DoubleVal":2.9574e58,
 "BoolVal":false,
 "StringVal":"this is a string",
 "parent/child":-88,
 "FirstLeve1Obj":{
  "IntVal":56,
  "DoubleVal":2.9574e58,
  "BoolVal":false,
  "StringVal":"this is a string",
  "SecondLevelObj":{
   "IntVal":56,
   "DoubleVal":2.9574e58,
   "BoolVal":false,
   "StringVal":"this is a string"
  }
 }
}
```

In the above payload, the tags created are: *IntVal, DoubleVal, BoolVal, StringVal, parent/child, FirstLeve1Obj/IntVal, FirstLeve1Obj/DoubleVal, FirstLeve1Obj/BoolVal, FirstLeve1Obj/StringVal, FirstLeve1Obj/SecondLevelObj/IntVal, FirstLeve1Obj/SecondLevelObj/DoubleVal, FirstLeve1Obj/SecondLevelObj/BoolVal*, and *FirstLeve1Obj/SecondLevelObj/StringVal*.

- The `Is Hierarchical` parameter in the *parent/child* tag must be set to **False** to indicate that it is not a nested level tag.
- The `Is Hierarchical` parameter in the tags starting with *FirstLeve1Obj* and *FirstLeve1Obj/SecondLeve1Obj* must be set to **True** to indicate that they are nested level tags. The '/' is considered a delimiter that separates the first level *parent* and the second level *child* tags.

JSON Payload with Arrays

```
{
 "FirstLevelObj":{
  "ObjArrayVars":[
   {
    "Name": "my name",
    "Age": 30,
    "Languages":["English", "Hindi", "Telugu"]
   },
   {
    "Name": "your name",
    "Age": 20,
    "Languages":["Spanish", "French", "Latin"]
   }
  ],
  "IntArrayVars":[10, 20, 30]
 },
 "MultiDimArray":[[56.54, 23.45],[100.4,23.45]]
}
```

There are two different ways in which the arrays are considered:

- Each element of the array as an individual tag.
- Entire array as a single array tag.

The Flatten Leaf Arrays parameter of the Subscription determines whether to consider the array as a single array tag or to flatten the individual elements into tags.

If `Flatten Leaf Arrays` is set to **True**, the tags for the above payload are created as: *FirstLevelObj/ObjArrayVars[0]/Name, FirstLevelObj/ObjArrayVars[0]/Age, FirstLevelObj/ObjArrayVars[0]/Languages[0], FirstLevelObj/ObjArrayVars[0]/Languages[1], FirstLevelObj/ObjArrayVars[0]/Languages[2], FirstLevelObj/ObjArrayVars[1]/Name, FirstLevelObj/ObjArrayVars[1]/Age, FirstLevelObj/ObjArrayVars[1]/Languages[0], FirstLevelObj/ObjArrayVars[1]/Languages[1], FirstLevelObj/ObjArrayVars[1]/Languages[2], FirstLevelObj/IntArrayVars[0],FirstLevelObj/IntArrayVars[1],FirstLevelObj/IntArrayVars[2], MultiDimArray[0][0], MultiDimArray[0][1], MultiDimArray[1][0], MultiDimArray[1][1]*

If you set Flatten Leaf Arrays to **True**, values written from OPC UA clients to the tags cannot be published back to the MQTT client.

If you set `Flatten Leaf Arrays` to **False**, the tags for the above payload are created as: *FirstLevelObj/ObjArrayVars[0]/Name, FirstLevelObj/ObjArrayVars[0]/Age, FirstLevelObj/ObjArrayVars[0]/Languages, FirstLevelObj/ObjArrayVars[1]/Name, FirstLevelObj/ObjArrayVars[1]/Age, FirstLevelObj/ObjArrayVars[1]/Languages, FirstLevelObj/IntArrayVars, MultiDimArray*

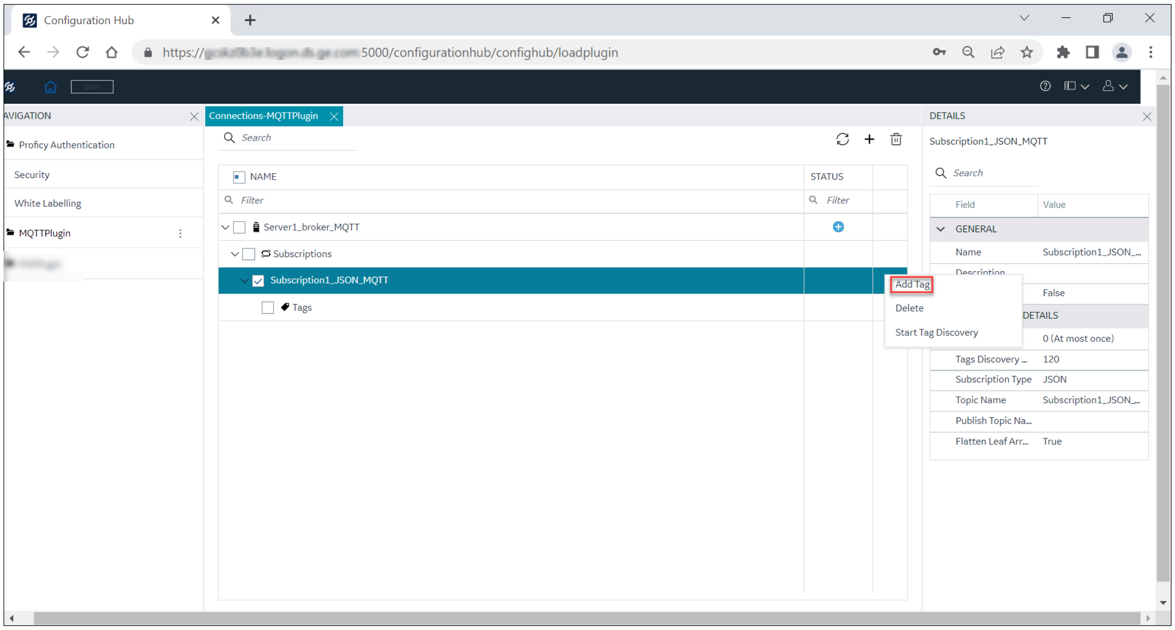
Add Tags to Subscription

For a Subscription, a Tag is added to load the subscribed MQTT data. Data stored in the tags will be translated from MQTT to OPC UA when the data is published.

To add Tags for a JSON or Sparkplug Subscription:

Tag for JSON Subscription

1. Select **Add Tag**.



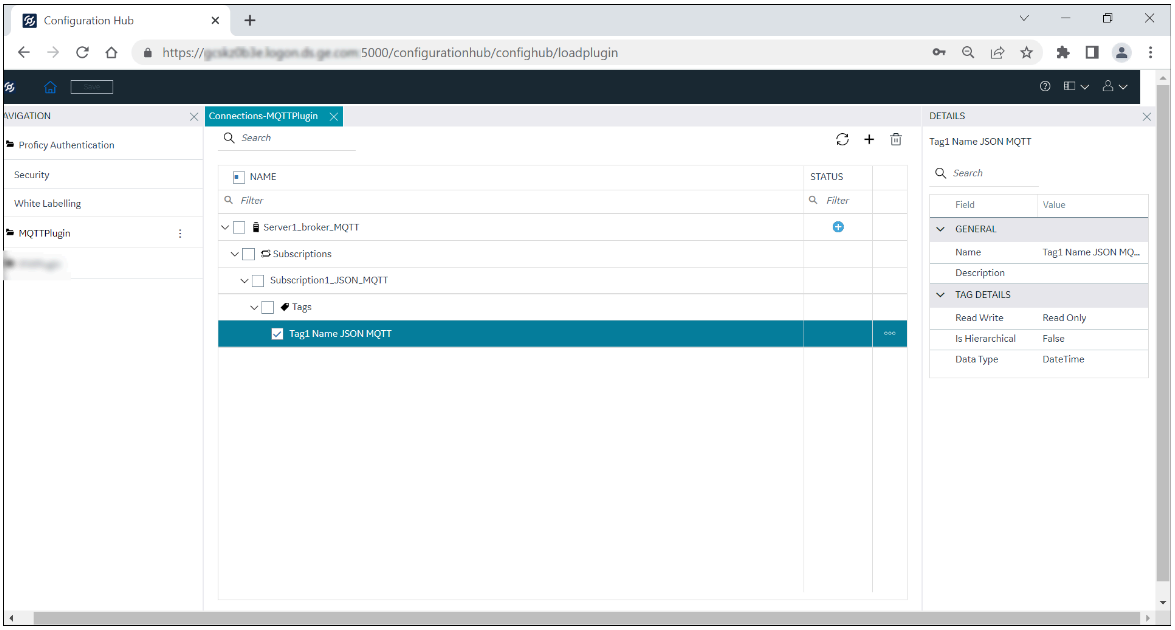
Field	Value
Name	Subscription1_JSON_...
Description	
	False
	0 (At most once)
Tags Discovery ...	120
Subscription Type	JSON
Topic Name	Subscription1_JSON_...
Publish Topic Na...	
Flatten Leaf Arr...	True

The **New Tag** dialog appears.

2. Enter a **Tag Name** and select the required **Data Type**.

> **Note:**
>
> - Ensure the following while you enter the information:
>   - Tag names must start with a letter and cannot exceed 1024 bytes.
>   - Do not include spaces in between names.
>   - Names cannot have leading or trailing spaces.
>   - Only the special characters ! # $ % & ( ) _ - [ ] | \ > < / are allowed.
>   - Field names cannot be left blank. Duplicate names are not allowed.

3. Click **Add**.



Field	Value
GENERAL	
Name	Tag1 Name JSON MQ...
Description	
TAG DETAILS	
Read Write	Read Only
Is Hierarchical	False
Data Type	DateTime

The Tag is added to the JSON subscription. Click **Save**.

> **Note:**
>
> You can modify the Data Type value for the JSON Subscription.

Table 5. JSON Tag Details

Field	Value
GENERAL	

Table 5. JSON Tag Details (continued)

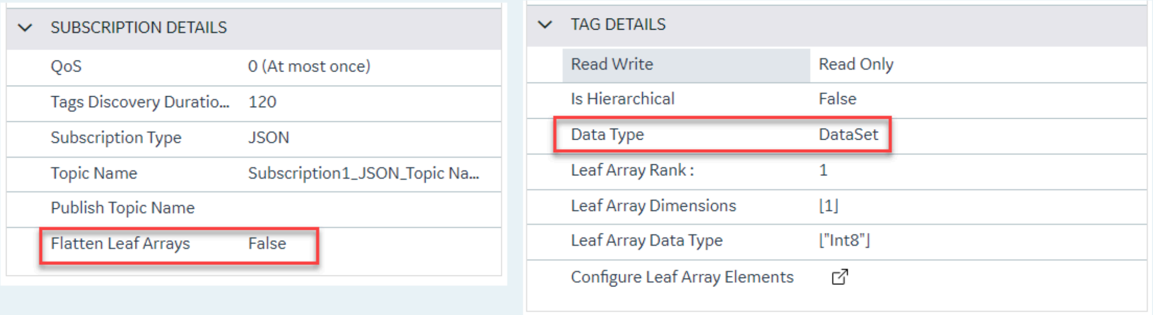
Field	Value
Name	Enter a tag name.
Description	Enter the tag description.
TAG DETAILS	
Read Write	You can set the value to Read Only or Read and Write. Read Only: You can only read the tag values from the OPC UA client. Read and Write: You can read and write/modify the tag values from the OPC UA client.

Is Hierarchical	Is Hierarchical parameter helps to indicate whether the tag is at the root level of a JSON object or at a nested level. Nested tags are represented using a complete tag name delimited using a forward slash (/).
	By default, this parameter is set to False.
	- True: It is a nested tag.
	- False: It is not a nested tag.
	For a JSON object:
	- `{`
	`  "level1":{`
	`            "level2":68`
	`          }`
	`}`
	If you want to refer to the level2 tag embedded in a level1 object, the tag name will be represented as level1/level2 where / is the delimiter. The **Is Hierarchical** parameter

Table 5. JSON Tag Details (continued)

Field	Value
	must be set to True to indicate that it is a nested tag. • `{` `"level1/level2":"my string"` `}` If you want to refer to a level1/level2 tag at the root level, then the tag name will be represented as level1/level2. The **Is Hierarchical** parameter must be set to False to indicate that it is not a nested tag.
Data Type	You can select the data type value from the list of available data type entries.

Note:
If Flatten Leaf Arrays is set to False in the JSON **SUBSCRIPTION DETAILS** section, and then if the **Data Type** is set to **DataSet** in the **TAG DETAILS** section, the **Configure Leaf Array Elements** will be displayed to configure the leaf array properties.



SUBSCRIPTION DETAILS

QoS	0 (At most once)
Tags Discovery Duratio...	120
Subscription Type	JSON
Topic Name	Subscription1_JSON_Topic Na...
Publish Topic Name	
Flatten Leaf Arrays	False

TAG DETAILS

Read Write	Read Only
Is Hierarchical	False
Data Type	DataSet
Leaf Array Rank :	1
Leaf Array Dimensions	[1]
Leaf Array Data Type	["Int8"]
Configure Leaf Array Elements	↗

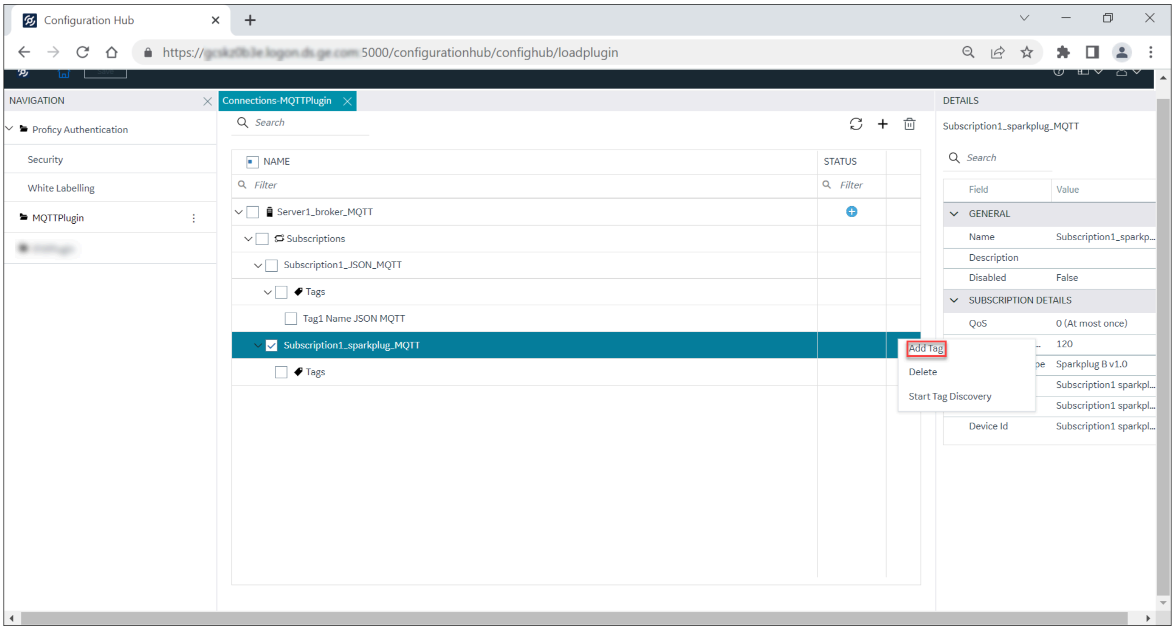
You must select **Configure Leaf Array Elements** ↗ to configure the leaf array elements (that is, Leaf Array Rank, Leaf Array Dimensions, and Leaf Array Data Type).

Leaf Array Elements	Description
Leaf Array Rank	The Leaf Array Rank value is the number of dimensions of an array.

Leaf Array Elements	Description
	• 1 - One dimensional • 2 - Two dimensional **Note:** The Leaf Array Rank is set up to two ranks only.
Leaf Array Dimensions	Number of elements in each dimension available corresponding to the Leaf Array Rank number.
Leaf Array Data Type	Select the Data Type as required. **Note:** When you select the **Variant** data type, the Leaf Array Data Types table is displayed with the Index of Elements and its Data Types. That is, you will be populated with the heterogeneous data types in the multi-dimensional array. You can modify the data type per each index in an array.

Tag for Sparkplug Subscription

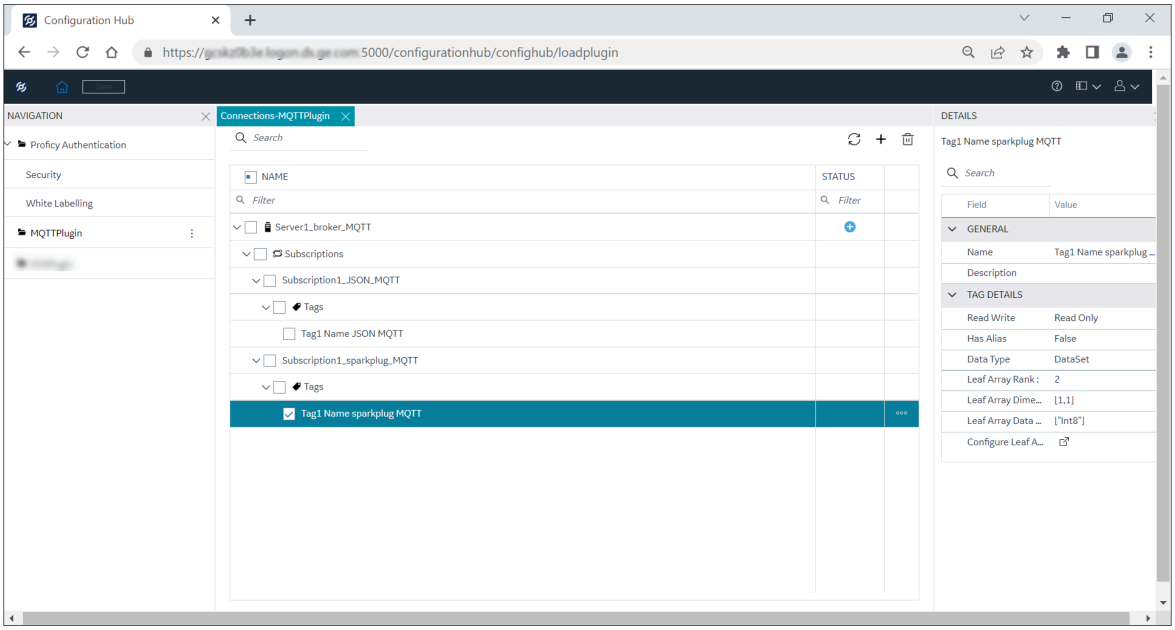
1. Select **Add Tag**.



Field	Value
Name	Subscription1_sparkp...
Description	
Disabled	False
QoS	0 (At most once)
...	120
...pe	Sparkplug B v1.0
	Subscription1 sparkpl...
	Subscription1 sparkpl...
Device Id	Subscription1 sparkpl...

The **New Tag** dialog appears.

2. Enter a **Tag Name** and select the required **Data Type**.
3. Click **Add**.



Field	Value
Name	Tag1 Name sparkplug ...
Description	
Read Write	Read Only
Has Alias	False
Data Type	DataSet
Leaf Array Rank :	2
Leaf Array Dime...	[1,1]
Leaf Array Data ...	["Int8"]
Configure Leaf A...	↗

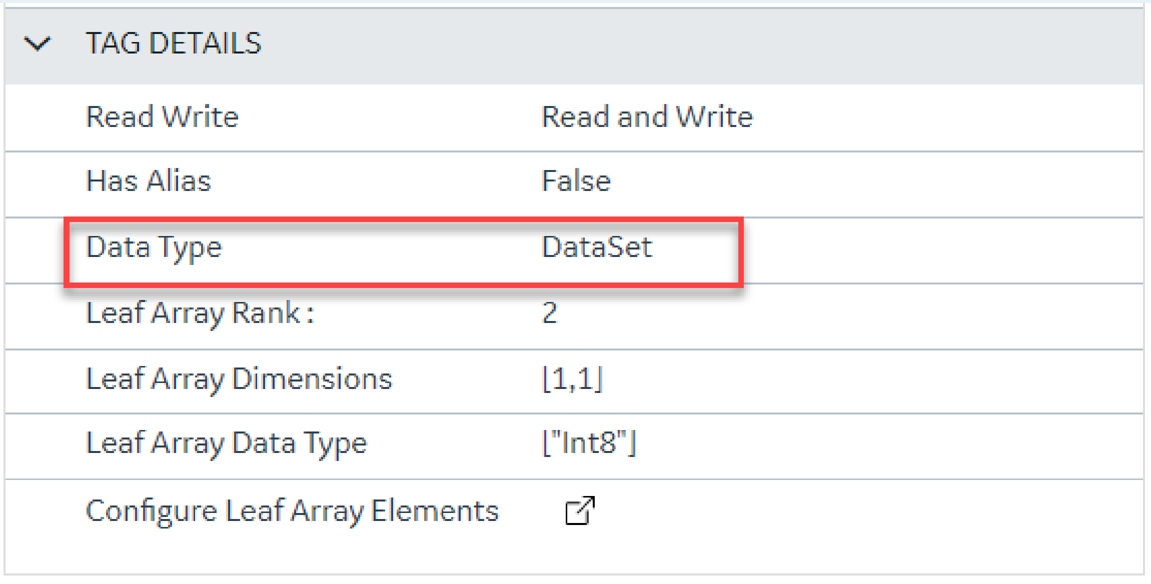
The Tag is added to the Sparkplug subscription. Click **Save**.

Note:
You cannot modify the Data Type value for the Sparkplug Subscription.

Table 6. Sparkplug Tag Details

Field	Value
GENERAL	
Name	Enter a tag name.
Description	Enter the tag description.
TAG DETAILS	
Read Write	You can set the value to Read Only or Read and Write. Read Only: You can only read the tag values from the OPC UA client. Read and Write: You can read and write/modify the tag values from the OPC UA client.
Has Alias	Has Alias is an integer value that is used as a substitute name to reduce the long and repeated usage of the same tag name. By default, this parameter is set to False. • True: The Alias field is displayed. Enter the publisher provided integer value in the **Alias** field. • False: The tag has no Alias name.
Data Type	Displays the data type.

Note:
In **TAG DETAILS**, if the **Data Type** is **DataSet**, then the **Configure Leaf Array Elements** will be displayed to configure the leaf array properties.



TAG DETAILS

Read Write	Read and Write
Has Alias	False
Data Type	DataSet
Leaf Array Rank :	2
Leaf Array Dimensions	[1,1]
Leaf Array Data Type	["Int8"]
Configure Leaf Array Elements	↗

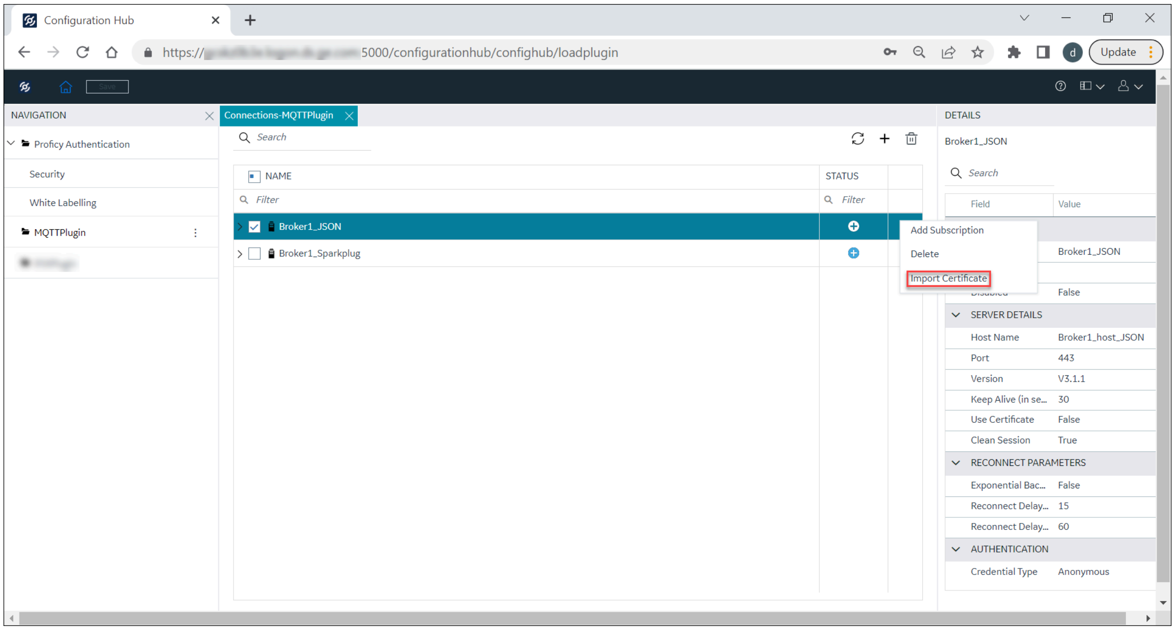
Refer to the above table for more information on Leaf Array Elements.

Secure Connection with Broker

To establish a secure connection with the MQTT broker, you must import the broker certificate and trust the certificate. This encrypts the data and keeps the broker connection data secure and authenticated.

To import the broker certificate:

1. From the **MQTTPlugin**, click the overflow icon ••• of the broker connection and then select **Import Certificate**.



NAME
Broker1_JSON
Broker1_Sparkplug

Broker1_JSON

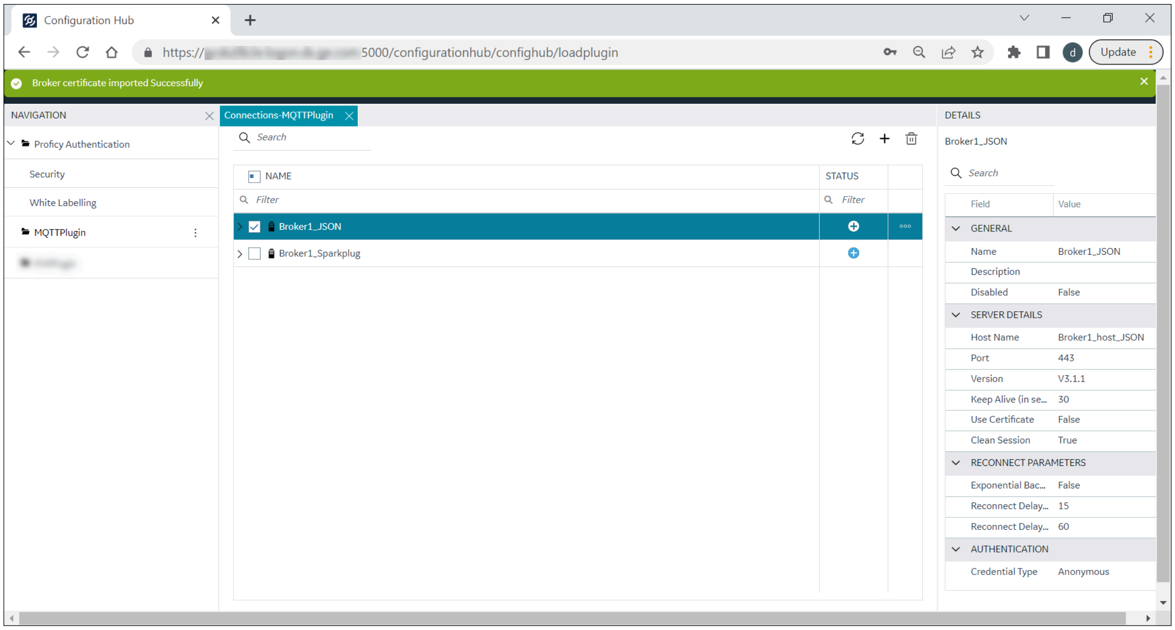
Field	Value
	Broker1_JSON
Disabled	False
SERVER DETAILS	
Host Name	Broker1_host_JSON
Port	443
Version	V3.1.1
Keep Alive (in se...	30
Use Certificate	False
Clean Session	True
RECONNECT PARAMETERS	
Exponential Bac...	False
Reconnect Delay...	15
Reconnect Delay...	60
AUTHENTICATION	
Credential Type	Anonymous

The **Import Service Certificate** dialog appears.

2. Click **Browse** and navigate to the source location of the broker certificate.
3. Double-click the broker root certificate.
4. Click **View** to view the certificate details.

   The **Certificate Details** page appears.

5. Click **Close** on the **Certificate Details** page.
6. Click **Trust** in the **Import Service Certificate** dialog.

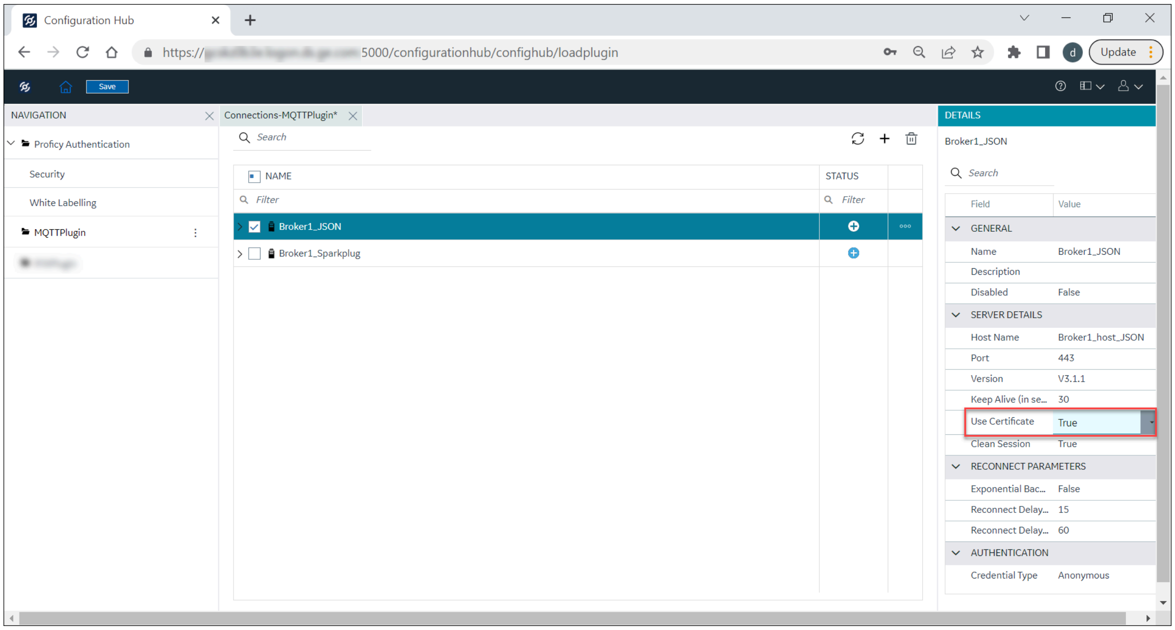


Broker certificate imported Successfully

Field	Value
GENERAL	
Name	Broker1_JSON
Description	
Disabled	False
SERVER DETAILS	
Host Name	Broker1_host_JSON
Port	443
Version	V3.1.1
Keep Alive (in se...	30
Use Certificate	False
Clean Session	True
RECONNECT PARAMETERS	
Exponential Bac...	False
Reconnect Delay...	15
Reconnect Delay...	60
AUTHENTICATION	
Credential Type	Anonymous

The **Broker certificate imported Successfully** message appears.

7. Copy the root certificate `MqttClientRootCA.crt`, and save it to your broker certificate import location.
8. In the **DETAILS** panel, ensure that the **Use Certificate** field is set to **True** in the **SERVER DETAILS** section.



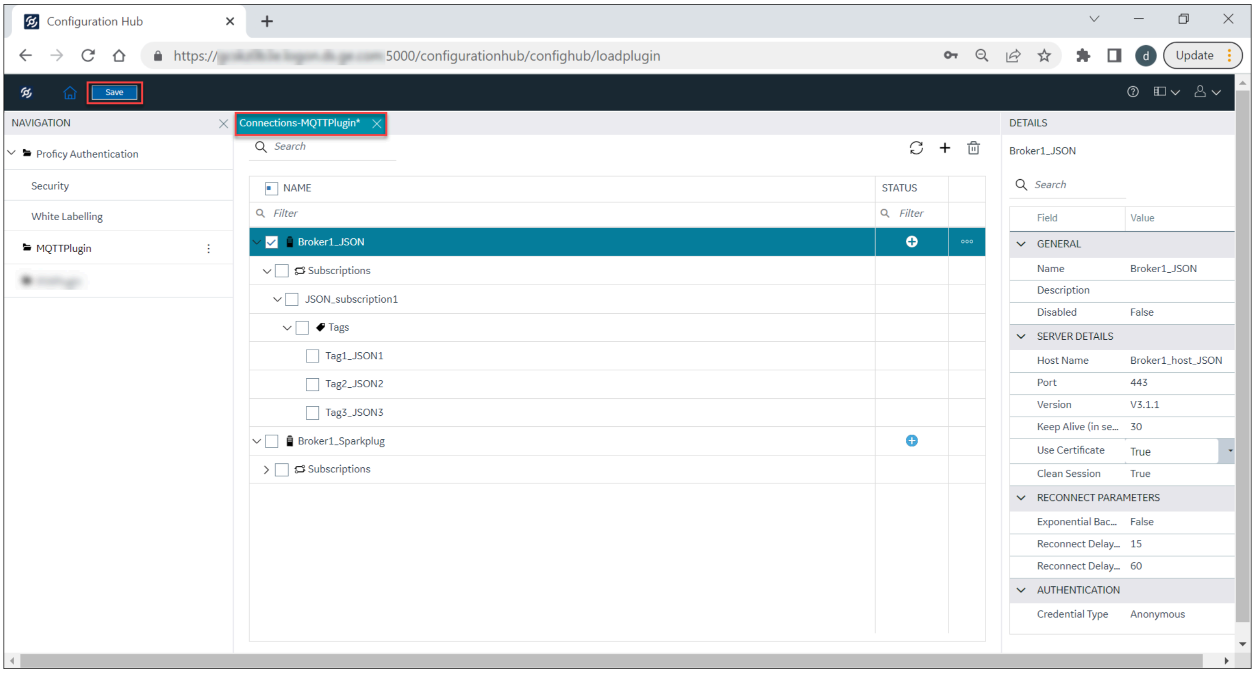
Field	Value
GENERAL	
Name	Broker1_JSON
Description	
Disabled	False
SERVER DETAILS	
Host Name	Broker1_host_JSON
Port	443
Version	V3.1.1
Keep Alive (in se...	30
Use Certificate	True
Clean Session	True
RECONNECT PARAMETERS	
Exponential Bac...	False
Reconnect Delay...	15
Reconnect Delay...	60
AUTHENTICATION	
Credential Type	Anonymous

9. Click **Save** and then **Publish**.

   Refer to Save and Publish *(on page 194)* for more details.

Save and Publish

When the MQTT node is plugged-in with Configuration Hub, the common toolbar will contain the **Save** button at the top left. Changes made in Configuration Hub for MQTT nodes are not saved on the server until the changes are published. Until then, any changes are stored in a separate directory on the node being configured.



https://[redacted]5000/configurationhub/confighub/loadplugin

- Proficy Authentication
  - Security
  - White Labelling
- MQTTPlugin
- [redacted]

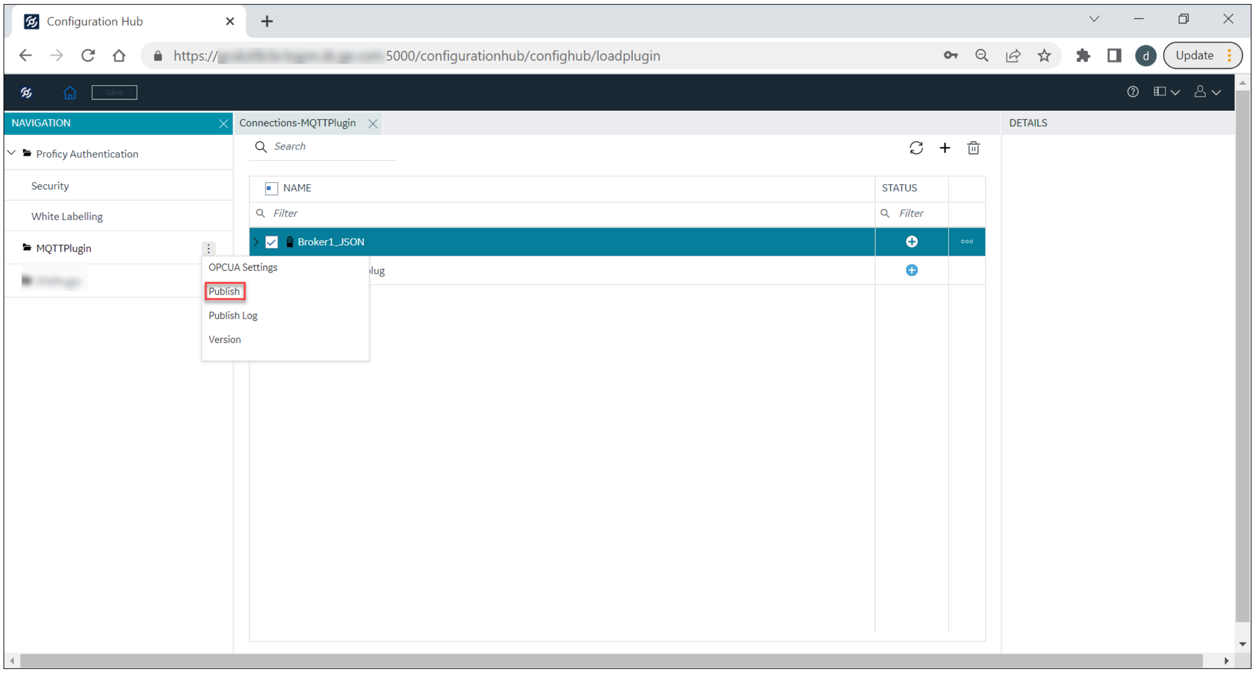
- Broker1_JSON
  - Subscriptions
    - JSON_subscription1
      - Tags
        - Tag1_JSON1
        - Tag2_JSON2
        - Tag3_JSON3
- Broker1_Sparkplug
  - Subscriptions

Broker1_JSON

Field	Value
GENERAL	
Name	Broker1_JSON
Description	
Disabled	False
SERVER DETAILS	
Host Name	Broker1_host_JSON
Port	443
Version	V3.1.1
Keep Alive (in se...	30
Use Certificate	True
Clean Session	True
RECONNECT PARAMETERS	
Exponential Bac...	False
Reconnect Delay...	15
Reconnect Delay...	60
AUTHENTICATION	
Credential Type	Anonymous

The Save button responds to certain panel actions that can queue up and will not be applied to the unpublished list until the Save button is clicked. For example, any changes in the Connections panel must be saved before they are applied. If you do not want to save the changes you made, close the panel, and choose not to save. An asterisk (*) appears in the panel tab when there are unsaved changes. Click **Save** to save the connection panel details.

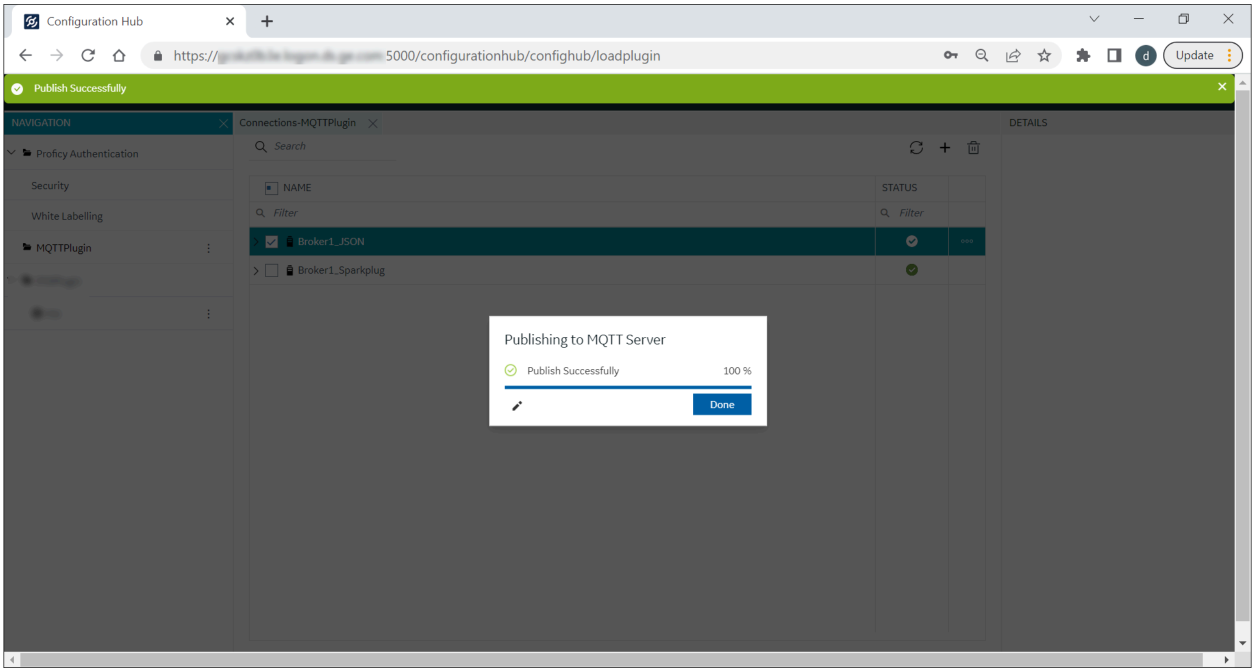
When you are ready to apply the changes to the running system, select **Publish** from the MQTT connection plugin overflow icon ⋮ to push the changes to the server.



A prompt message appears to select **Publish**. Click the Publish button to publish the changes to MQTT server.

The publish operation begins, after you click the publish button. It may take a while depending on the number of tags being published to the active MQTT node.

The *Publish Successfully* message appears when the changes are published to the MQTT Server.



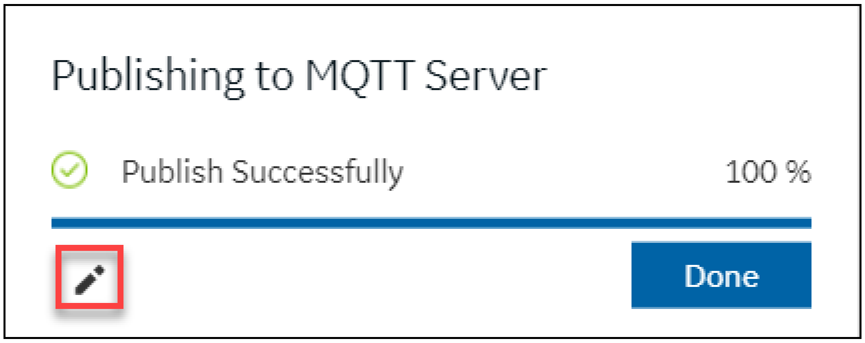
Publish Successfully

Publishing to MQTT Server

Publish Successfully 100 %

Publish Log and Version

After you publish the MQTT plugin changes, you can directly view the published log reports by clicking the ✎ icon.



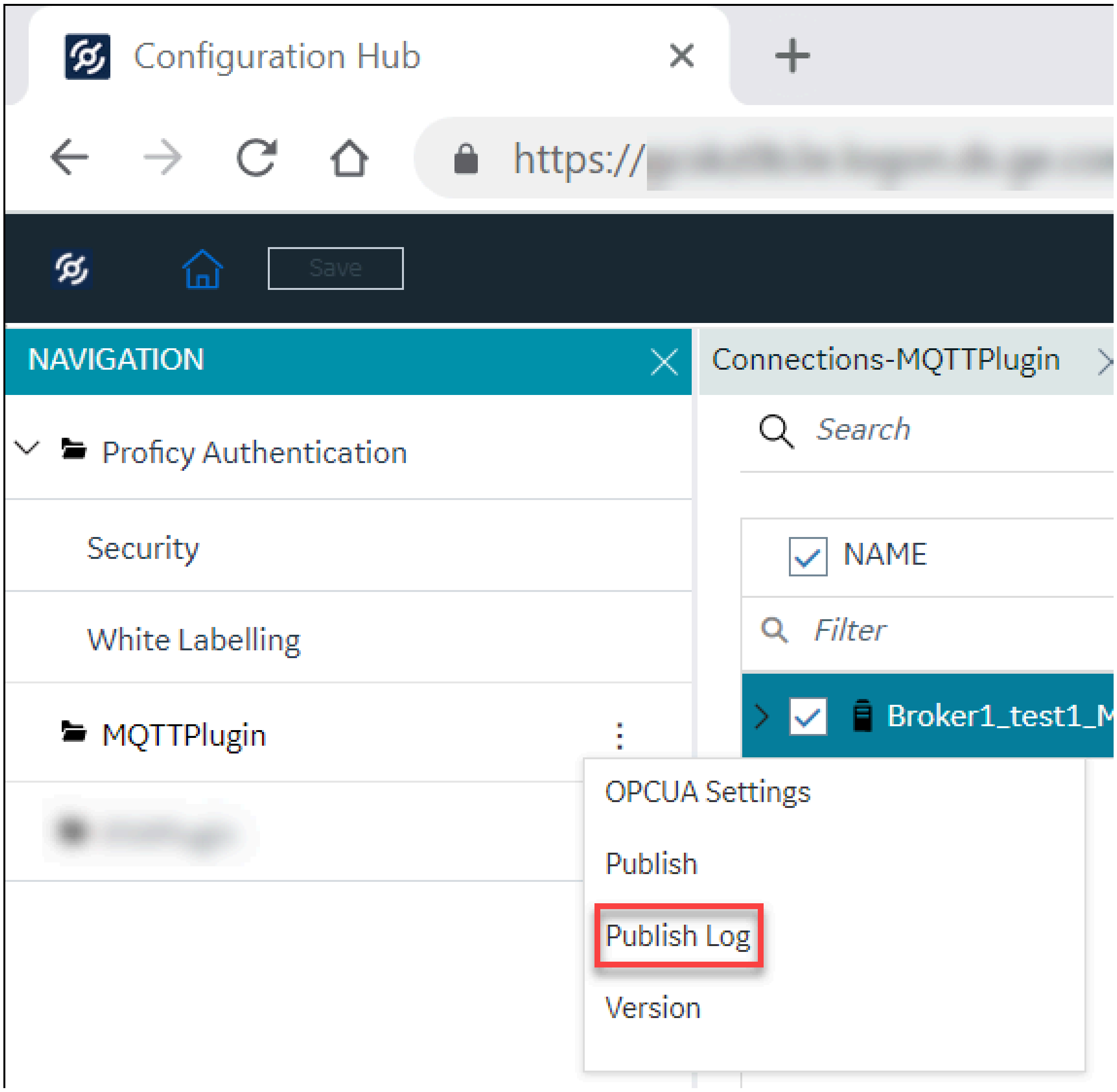
Publishing to MQTT Server

✓ Publish Successfully 100 %

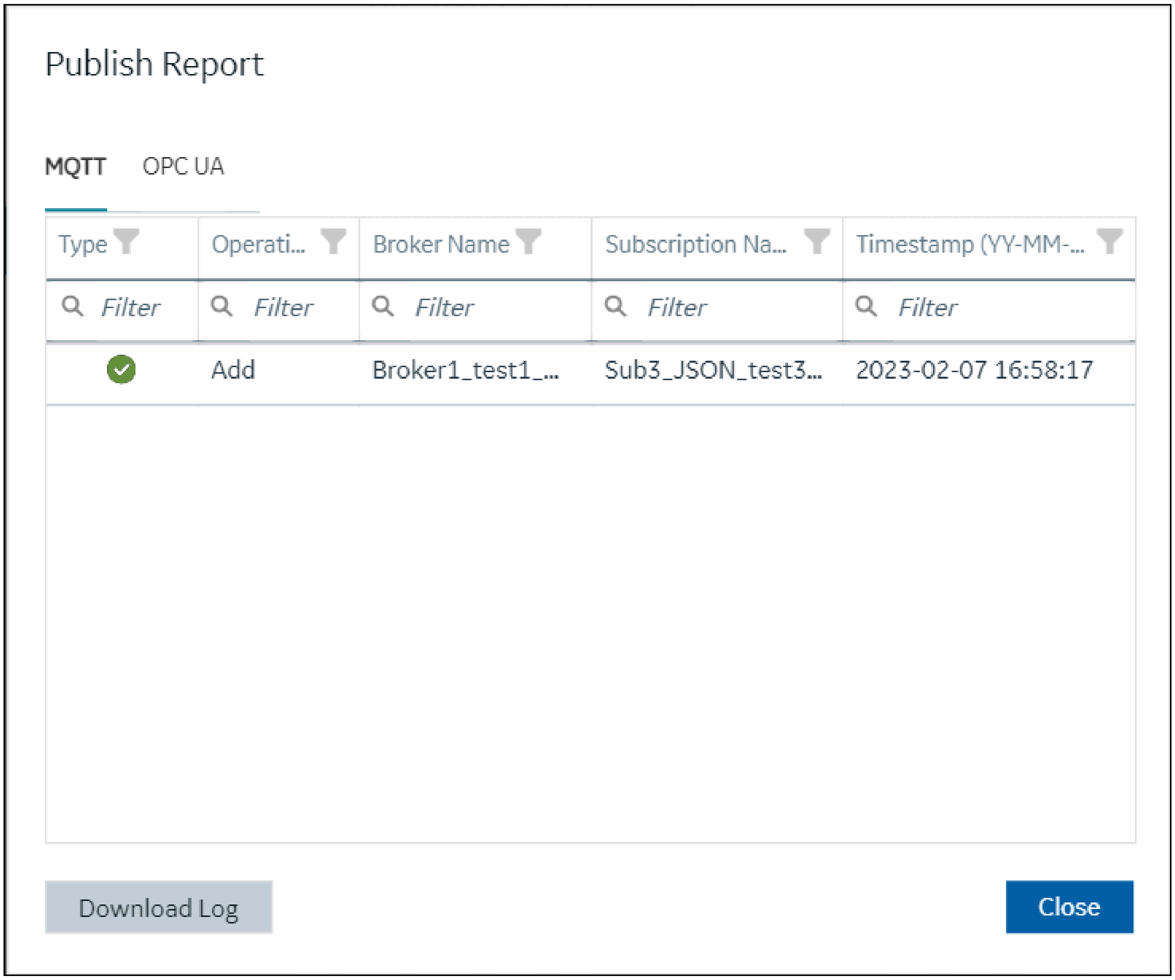
Publish Log

To view the publish log reports:

1. Click the MQTT plugin overflow ⋮ icon.
2. Select **Publish Log**.



The **Publish Report** dialog appears.



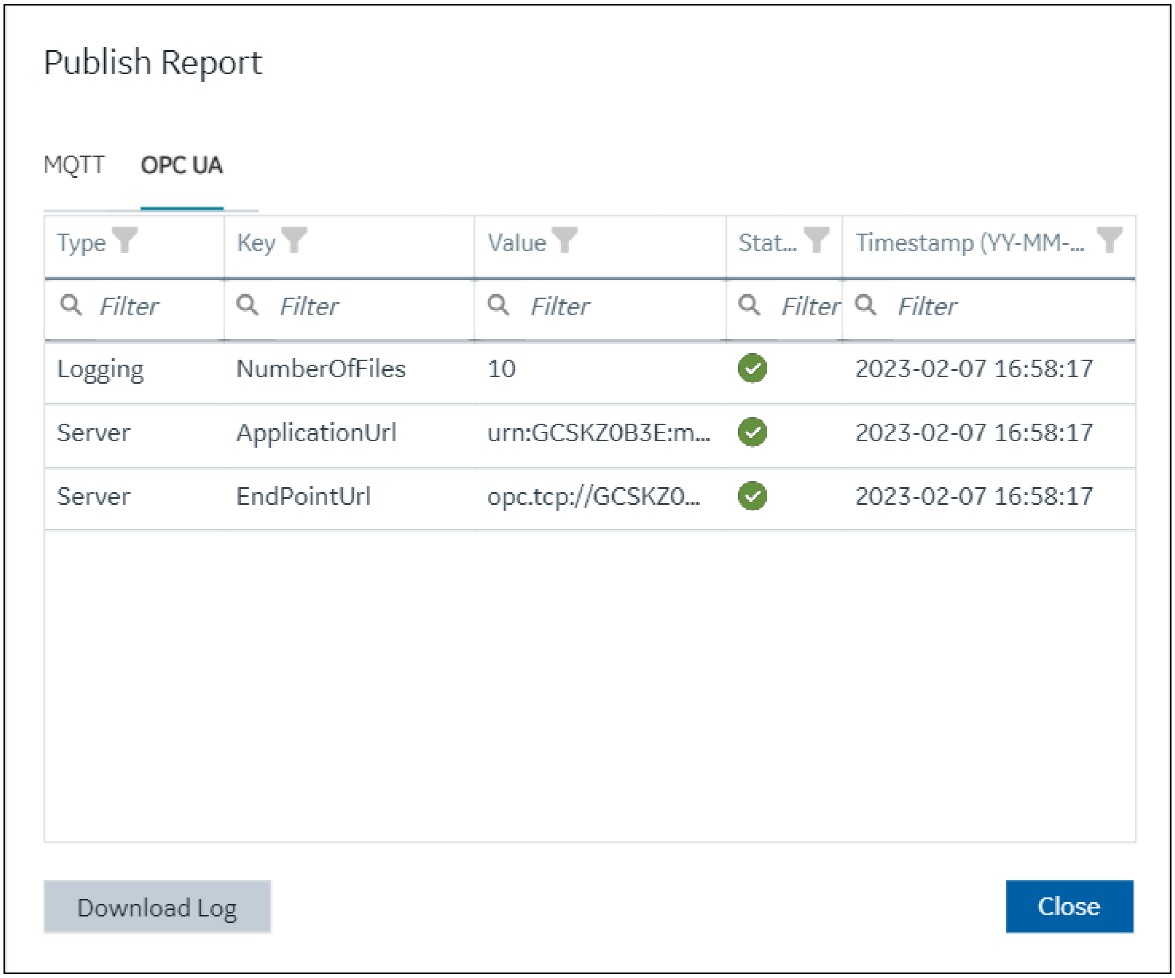
Publish Report

Type	Operati...	Broker Name	Subscription Na...	Timestamp (YY-MM-...
Filter	Filter	Filter	Filter	Filter
✓	Add	Broker1_test1_...	Sub3_JSON_test3...	2023-02-07 16:58:17

Table 7. MQTT Publish Log Report

Field	Description
Operation	Indicates whether the operation is added, modified, or deleted.
Broker Name	Name of the Broker.
Subscription Name	Name of the Subscription.
Timestamp (YY-MM-DD HH:mm:ss)	Record of the event in the format YY-MM-DD HH:mm:ss.

3. Select the **OPC UA** tab to view the OPC UA log reports.



Publish Report

Type	Key	Value	Stat...	Timestamp (YY-MM-...
Logging	NumberOfFiles	10	✓	2023-02-07 16:58:17
Server	ApplicationUrl	urn:GCSKZ0B3E:m...	✓	2023-02-07 16:58:17
Server	EndPointUrl	opc.tcp://GCSKZ0...	✓	2023-02-07 16:58:17

Table 8. OPC UA Publish Log Report

Field	Description
Key	The key refers to the field names in the OPC UA Settings page.
Value	The value entered in the fields of the OPC UA Settings page.
Status	The status of the published log information.
Timestamp (YY-MM-DD HH:mm:ss)	Record of the event in the format YY-MM-DD HH:mm:ss.

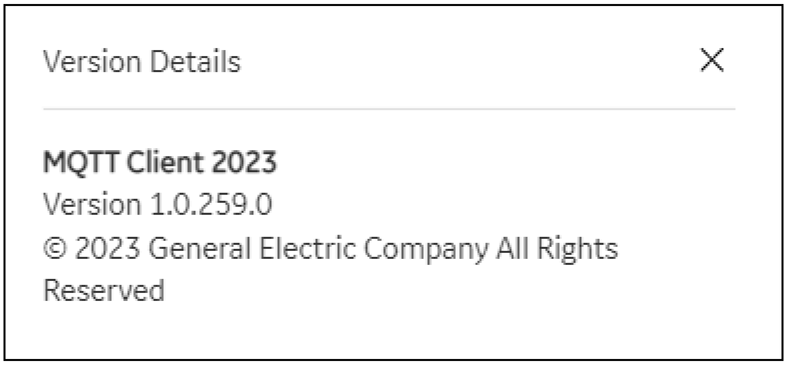
Note:

- You can click the 🔍 icon to filter the data as required.
- You can click the **Download Log** button to download the log information.

Important:
Only the last published log information will be displayed in the **Publish Report** window.

Version

You can click the MQTT plugin overflow ⋮ icon, and then select **Version**.



Version Details

MQTT Client 2023
Version 1.0.259.0
© 2023 General Electric Company All Rights Reserved

The **Version Details** dialog appears.

The MQTT Client application version details are displayed.

OPC UA

The OPC UA protocol is a standard communication mechanism for transferring data between interfaces. OPC UA clients connect to the OPC UA server and collect data from UA Variables.

OPC UA is an independent open communication platform for both industrial and business application needs. The OPC UA server acts as a bridge between the IIoT devices (such as sensors, HMI software, SCADA systems, and so on) and OPC UA clients. It protects data integrity and helps in creating a scalable, reliable, and secure connection. OPC UA supports communication protocols, and also the exchanging of data between devices. Information requested by OPC UA clients is translated through the OPC UA server.

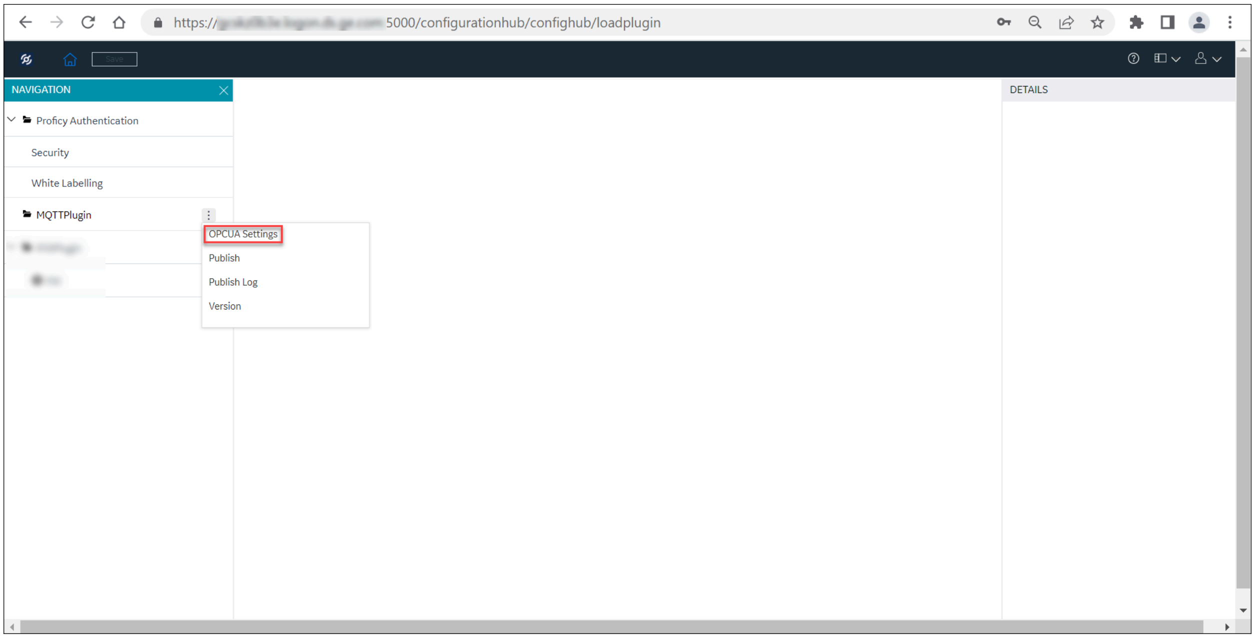
The MQTT client application is used as a two-way data communication. You can also write from OPC UA clients to MQTT clients or from IIoT devices.

After you configure MQTT Client information (that is, establishing the connections, subscriptions, and tags), the OPC UA server reads the configuration and displays the tags in a hierarchical manner. The hierarchy includes the client's name (unique per broker), topic, and the tag name within the topic. The OPC UA server reads the values of the data subscribed to by the MQTT clients. The OPC UA data is then published to OPC UA Clients.

Refer to OPC UA Settings *(on page 201)* to configure the OPC UA settings page.

OPC UA Settings

After establishing broker connections, subscriptions, and tags information, click the overflow icon ⋮ of the MQTT plugin, and then select **OPC UA Settings** to connect to the OPC UA server and establish the OPC UA client connection.

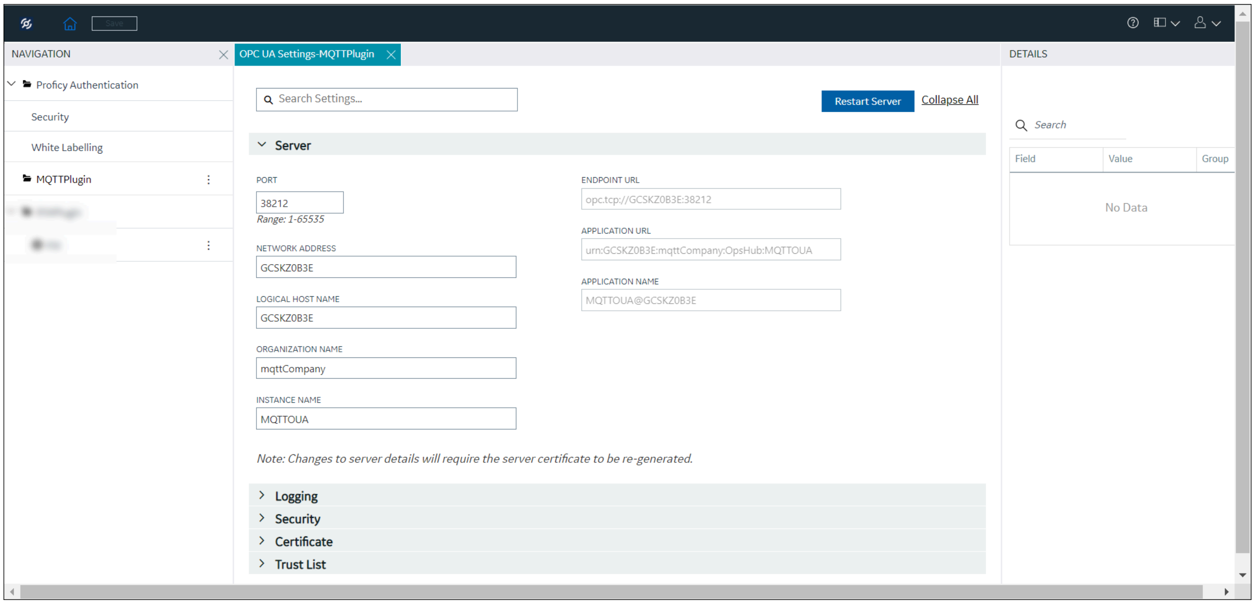


https://[redacted]5000/configurationhub/confighub/loadplugin

Enter the required details in the following sections of OPC UA Settings page:

- Server
- Logging
- Security
- Certificate
- Trust List

Server



Server

PORT: 38212

Range: 1-65535

NETWORK ADDRESS: GCSKZ0B3E

LOGICAL HOST NAME: GCSKZ0B3E

ORGANIZATION NAME: mqttCompany

INSTANCE NAME: MQTTOUA

ENDPOINT URL: opc.tcp://GCSKZ0B3E:38212

APPLICATION URL: urn:GCSKZ0B3E:mqttCompany:OpsHub:MQTTOUA

APPLICATION NAME: MQTTOUA@GCSKZ0B3E

Note: Changes to server details will require the server certificate to be re-generated.

Logging

Security

Certificate

Trust List

The server connection fields are populated automatically by the system. You can also change the server details as required.

Table 9. OPC UA Server Details

Field	Description
PORT	The OPC UA Client port the device will use.
NETWORK ADDRESS	The unique identification of your physical computer or a device name.
LOGICAL HOST NAME	Host name of the server on which OPC UA is installed.
ORGANIZATION NAME	Name of the Organization that owns the application.
INSTANCE NAME	Information about the OPC UA client.
ENDPOINT URL	A network location that OPC UA Client applications can use to find and connect to an OPC UA Server.

Table 9. OPC UA Server Details (continued)

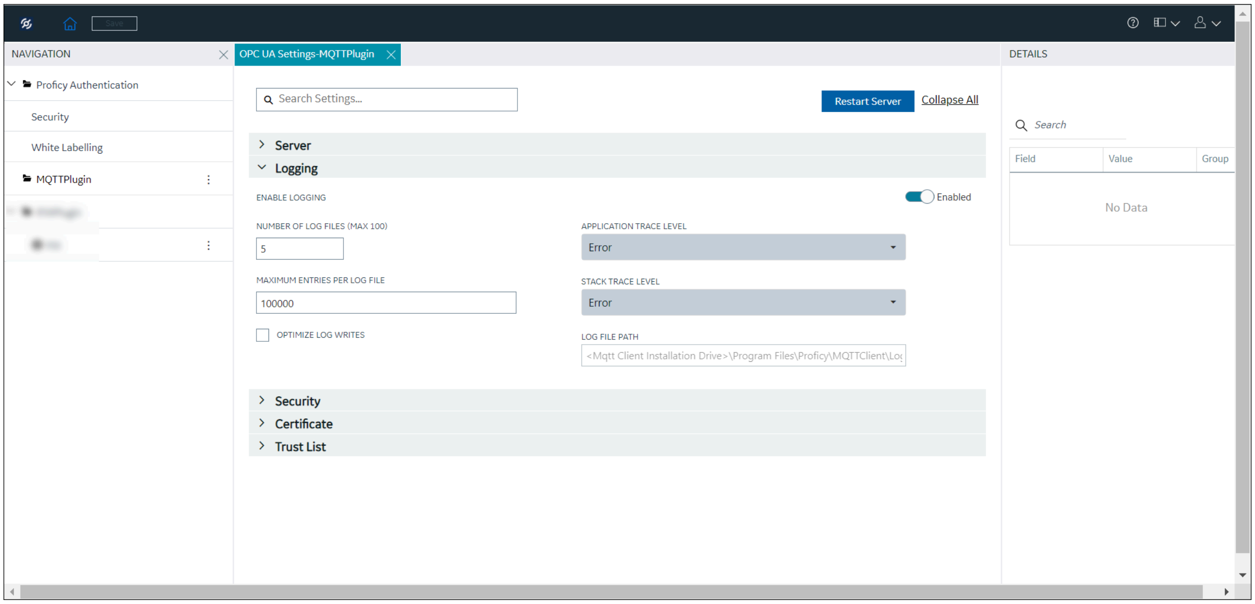
Field	Description
	Note: • An endpoint is a physical address available on a network that allows clients to access one or more services provided by a server. • An OPC UA Endpoint URL (Uniform Resource Locator) is a formatted text string that consists of three or four parts (substrings): 1. Network protocol ((must be opc.tcp (case sensitive)). 2. Host name or IP address. 3. Port number. 4. (Optional) File or resource location. The OPC UA specific URL, it shows as: `opc.tcp://hostname:38212/<file or resource location>`
APPLICATION URL	The unique address reference on the Internet. Also, referred to as the web address.
APPLICATION NAME	Name of the application.

Note:

- If you modify the OPC UA server details, it is recommended to select **Restart Server** to establish the OPC UA server connection.
- If you want to restart the OPC UA server, select **Restart Server** and then, click **Yes** to the **Confirm Regenerate** prompt message. After successful server connection, the following message appears.

  OPC UA Server successfully restarted.

Logging



ENABLE LOGGING: Enabled

NUMBER OF LOG FILES (MAX 100): 5

MAXIMUM ENTRIES PER LOG FILE: 100000

□ OPTIMIZE LOG WRITES

APPLICATION TRACE LEVEL: Error

STACK TRACE LEVEL: Error

LOG FILE PATH: <Mqtt Client Installation Drive>\Program Files\Proficy\MQTTClient\Lo

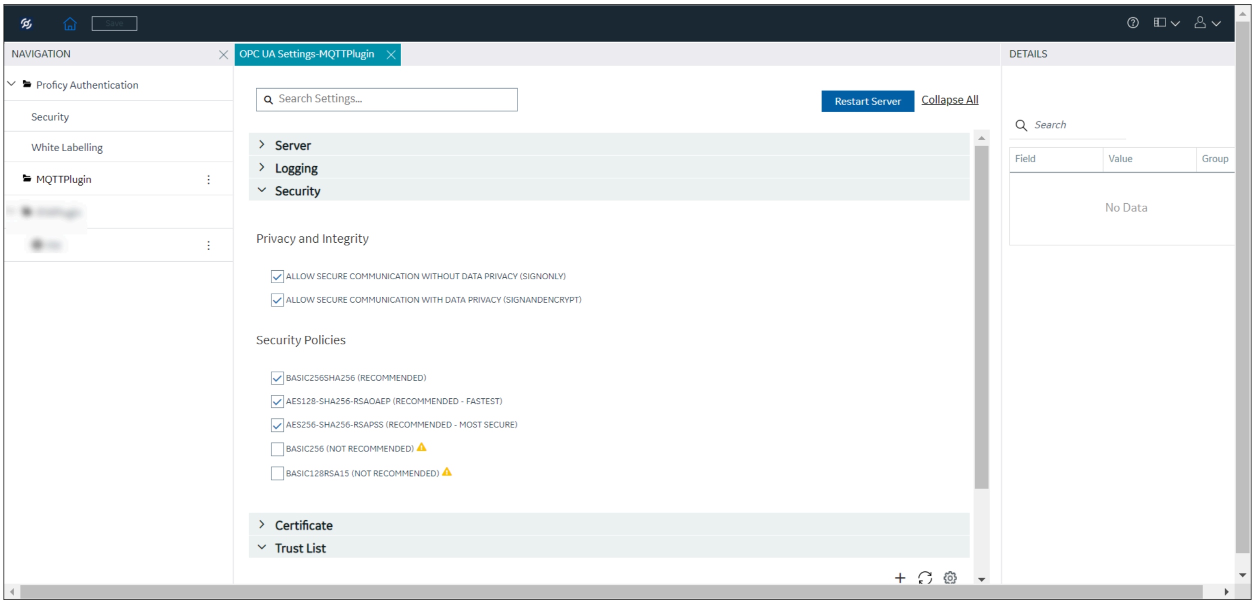
Logging helps you to record the error reports. The logging section displays the number of log files, maximum entries per log file, application trace level, stack trace level, and log file path fields. You can select the application level and stack level log files as required from the respective drop-down list.

Note:
You can enable or disable logging using the toggle switch in the **Logging** section.

Table 10. Logging Configuration

Field	Description
NUMBER OF LOG FILES (MAX 100)	The number of files for log backups (range is from 1 to 100).
MAXIMUM ENTRIES PER LOG FILE	The number of entry per log file (range is from 0 to 1000000000).
APPLICATION TRACE LEVEL	You can trace the errors or warnings to generate the trace messages. From the application trace level, you can select None, Error, Errors and Warnings, Error, Warnings and Information or, Detailed (may impact performance) as required.
STACK TRACE LEVEL	You can trace the information about frequently used operations. The stack trace helps to find out the debugs in an operation and to figure out the problems for any bug generated in the operation. From the application trace level, you can select None, Error, Errors and Warnings, Error, Warnings and Information or, Detailed (may impact performance) as required.
LOG FILE PATH	Location of the log file. `<Installation Location Drive>\Program Files\Proficy\MQTTClient\Logs\OpcUa-Server.log`
□ OPTIMIZE LOG WRITES	Select the Optimize Log Writes check box to optimize log events, use structured logging, exclude sensitive information, and to store the data.

Security



Privacy and Integrity

☑ ALLOW SECURE COMMUNICATION WITHOUT DATA PRIVACY (SIGNONLY)

☑ ALLOW SECURE COMMUNICATION WITH DATA PRIVACY (SIGNANDENCRYPT)

Security Policies

☑ BASIC256SHA256 (RECOMMENDED)

☑ AES128-SHA256-RSAOAEP (RECOMMENDED - FASTEST)

☑ AES256-SHA256-RSAPSS (RECOMMENDED - MOST SECURE)

☐ BASIC256 (NOT RECOMMENDED) ⚠

☐ BASIC128RSA15 (NOT RECOMMENDED) ⚠

Use the check boxes in the **Privacy and Integrity** and **Security Policies** sections to ensure data is secured and protected from unauthorized access. Only authorized users can access the data to view and modify as per user access privileges.

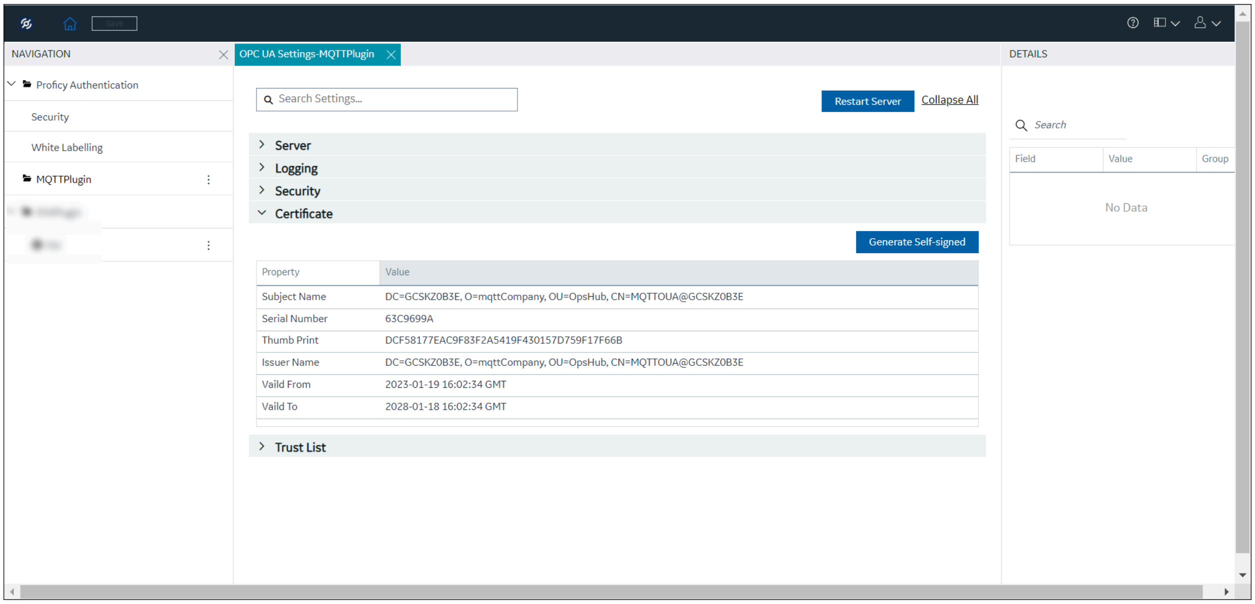
Privacy and Integrity	
ALLOW SECURE COMMUNICATION WITHOUT DATA PRIVACY (SIGNONLY)	Encryption is still used in the initial handshake. This mode is not appropriate when legal requirements prohibit the use of encryption.
ALLOW SECURE COMMUNICATION WITH DATA PRIVACY (SIGNANDENCRYPT)	All messages are signed and encrypted.
Security Policies	
BASIC256SHA256 (RECOMMENDED)	For configurations that require high security.
AES128-SHA256-RSAOAEP (RECOMMENDED - FASTEST)	For configurations that require high speed with average security.
AES256-SHA256-RSAPSS (RECOMMENDED - MOST SECURE)	For configurations that require very high security.

Note:

- BASIC256 and BASIC128RSA15 are deprecated due to vulnerability and theoretical issues.
- You can verify the security permissions at the following location.

```
<Installation Location Drive>\Program Files\Proficy\MQTTClient
\ServerConfig.xml
```

Certificate



Property	Value
Subject Name	DC=GCSKZ0B3E, O=mqttCompany, OU=OpsHub, CN=MQTTOUA@GCSKZ0B3E
Serial Number	63C9699A
Thumb Print	DCF58177EAC9F83F2A5419F430157D759F17F66B
Issuer Name	DC=GCSKZ0B3E, O=mqttCompany, OU=OpsHub, CN=MQTTOUA@GCSKZ0B3E
Vaild From	2023-01-19 16:02:34 GMT
Vaild To	2028-01-18 16:02:34 GMT

To establish the trusted connection with the OPC UA client, you must generate the self-signed certificate.

1. Select **Generate Self-signed** certificate.
2. A prompt message appears. Click **Yes** to regenerate the server certificate.

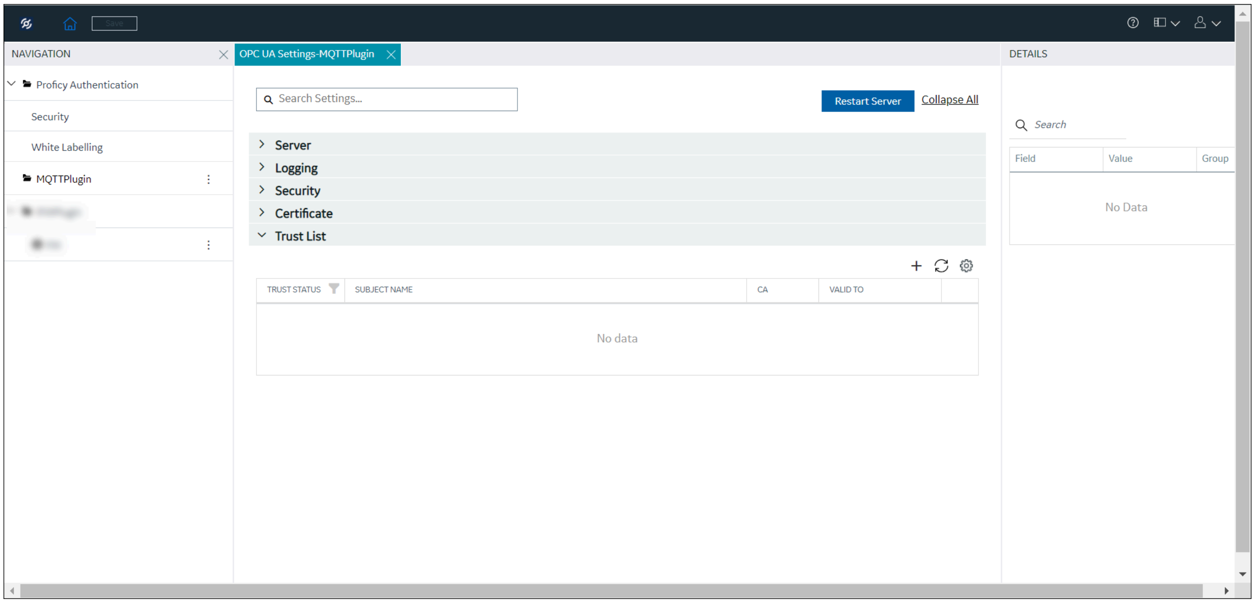
Important:

All previous server settings will be removed, and new details are updated.

OPC UA certification created successfully message appears.

3. Select **Restart Server** to use the certificate. The new server certificate details are populated in the **Certificate** section.
4. To view the server certificate, navigate to `<Install Location Drive>\Proficy \MQTTClient\UA\pkiserver\own\certs`.

Trust List



The trust list will display the certificate status (trusted and rejected) and its validity period. Use the overflow icon ••• and select **Trust** to trust the rejected certificate, or select **Reject** to reject the already trusted certificate, and select **Delete** to delete the certificate from the trust list.

If a client certificate is not displayed in the Trust List table:

- Select the **Refresh** ⟳ icon. This will load the client certificate to the Trust List table or,
- Select the **Add Certificate** + icon. The **Import Trust Certificate** dialog appears. You can then browse to the client certificate location and Trust the certificate.

After the OPC UA settings information is saved, you can select the overflow icon ⋮ of the MQTT plugin and select **Publish** to publish the changes to the MQTT server. Refer to Save and Publish *(on page 194)* for more details.