



GE VERNOVA

PROFICY® SOFTWARE & SERVICES

CIMPLICITY

Getting Started

Proprietary Notice

The information contained in this publication is believed to be accurate and reliable. However, GE Vernova 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 GE Vernova. Information contained herein is subject to change without notice.

© 2024 GE Vernova and/or its affiliates. All rights reserved.

Trademark Notices

“VERNOVA” is a registered trademark of GE Vernova. “GE VERNOVA” is a registered trademark of GE Aerospace exclusively licensed to GE Vernova. The terms “GE” and the GE Monogram are trademarks of GE Aerospace and are used with permission.

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. HMI/SCADA CIMPLICITY Introduction.....5**
 - About HMI/SCADA CIMPLICITY..... 5
 - System Architecture Overview..... 5
 - CIMPLICITY Server and Viewer Defined.....7
- Chapter 2. CIMPLICITY Installation..... 9**
 - Installation Prerequisites.....9
 - Install CIMPLICITY using Proficy Installer..... 10
 - Running the Proficy Installer from a Command Line..... 26
 - Customize Options for Proficy Installer from a Command Line..... 31
 - CIMPLICITY Program File Components..... 36
 - Install Local Help.....40
- Chapter 3. CIMPLICITY Post-Installation Tasks42**
- Chapter 4. CIMPLICITY Applications Tour..... 43**
 - CIMPLICITY Applications Tour..... 43
 - Part 1. CIMPLICITY Tour.....43
 - Part 2. CIMPLICITY Tour.....44
 - Part 3. CIMPLICITY Tour.....45
 - Part 4. CIMPLICITY More Features.....47
 - Part 5. CIMPLICITY Options..... 49
- Chapter 5. Manage SSL Certificate to Secure CIMPLICITY Web Clients.....52**
 - Self Signed SSL Certificate..... 52
 - Generate Self Signed SSL Certificate to Secure CIMPLICITY Web Clients..... 52
 - Regenerate the Self Signed SSL Certificate.....52
 - Update validity of the Self Signed SSL Certificate..... 53
 - External CA signed SSL Certificate..... 54
 - Generate SSL Certificate Using an External Certificate Authority 54
 - Install SSL Certificate on a Viewer or Remote Machine..... 56

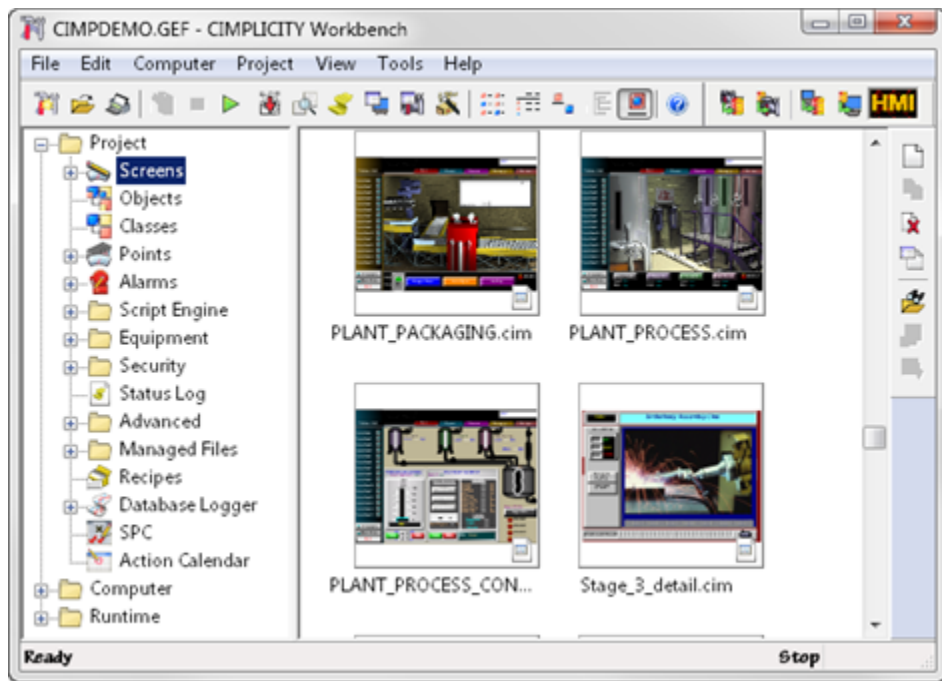
Secure REST Calls using SSL Certificate Validation.....	56
Chapter 6. Windows Auto-login Configuration.....	58
Autologin Configuration Checklist.....	58
Chapter 7. Proficy Authentication Configuration in CIMPLICITY.....	65
Best Practices and Limitations.....	65
Configure Proficy Authentication in CIMPLICITY.....	66
Configure Proficy Authentication.....	67
Trust an Untrusted Certificate while Configuring Proficy Authentication Parameters in CIMPLICITY.....	70
Enable and configure Proficy Authentication in Project Properties.....	71
Enable web configuration in Project Properties.....	74
About Security Groups.....	75
Create Security Groups in CIMPLICITY.....	76
Publish Group(s) to Proficy Authentication server.....	79
Edit an Existing Security Group.....	80
Duplicate an Existing Security Group.....	81
Chapter 8. CIMPLICITY Plug-in in Configuration Hub.....	82
About Registering CIMPLICITY Plug-in in Configuration Hub.....	82
CIMPLICITY Plug-in Registration Use Cases.....	83
Central Registration of CIMPLICITY Plug-in with Configuration Hub.....	86
About Central Registration.....	86
Configure the CIMPLICITY Node to use Proficy Authentication.....	87
Add the CIMPLICITY Node and Register the Plug-in with Configuration Hub.....	89
Access Configuration Hub.....	93
Overview of CIMPLICITY Plug-in within Configuration Hub.....	95
Managing CIMPLICITY Plug-in in Configuration Hub.....	96
Start and Stop a CIMPLICITY Project.....	96
Select and Browse Devices.....	99
Select and Browse Tags from an MQTT Device.....	103

Create SCADA Points.....	106
Update or Modify CIMPLICITY Node or Plug-in	109
Unregister CIMPLICITY Plug-in from Configuration Hub.....	112
Delete CIMPLICITY Node.....	115
Chapter 9. MQTT Client.....	119
Introduction.....	119
Chapter 10. Licensing.....	121
Licensing.....	121
Chapter 11. About Term Licensing in CIMPLICITY.....	122
About Term Licensing.....	122
Best Practices.....	125

Chapter 1. HMI/SCADA CIMPLICITY Introduction

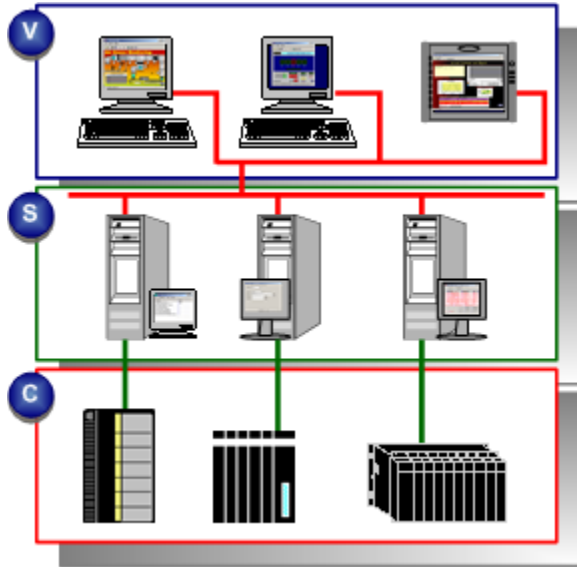
About HMI/SCADA CIMPLICITY

This section contains information on the basic CIMPLICITY architecture, a tutorial describing CIMPLICITY applications.



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_2_Connect_42_V (on page 6)
2. #unique_2_Connect_42_S (on page 6)
3. #unique_2_Connect_42_C (on page 6)

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.

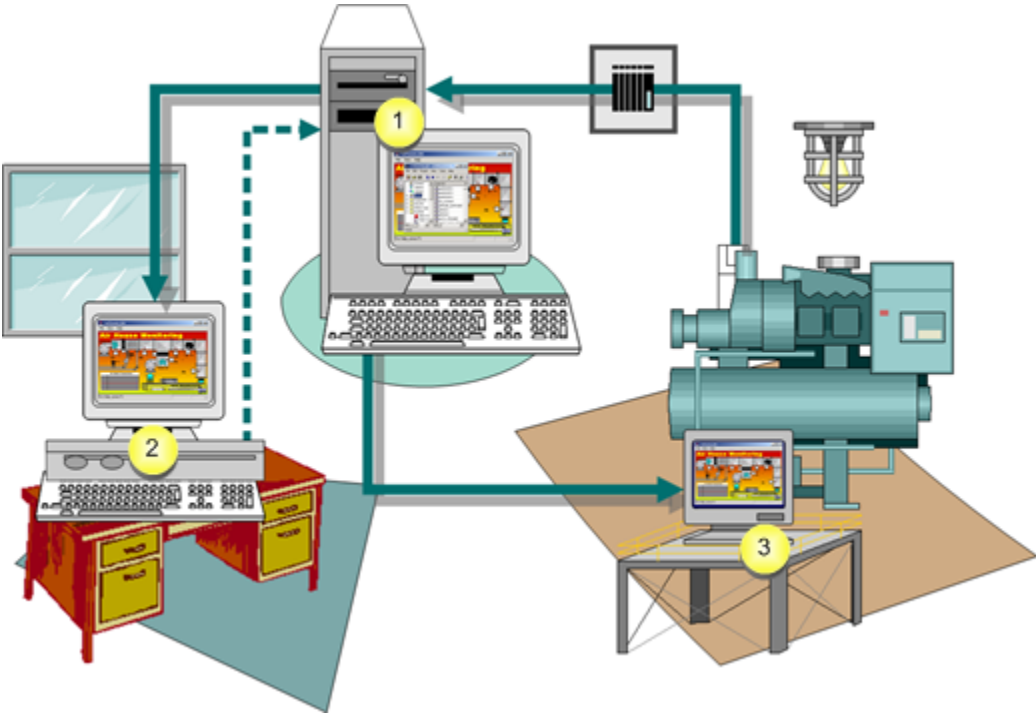
Servers and Viewers can be easily networked together to seamlessly share data without the need to replicate your point database from node to node. For example, points are configured once and only once on a server. Screens can be developed and stored in a single location on the network and accessed by 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 \(on page 49\)](#) for remotely interacting with your CIMPLICITY projects.

Contact your sales representative with questions about purchase options.

Chapter 2. CIMPLICITY Installation

Installation Prerequisites

Before you install CIMPLICITY v2024, 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, compatibility, 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 the Proficy 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.

Install Proficy Authentication 2024 and Configuration Hub 2024

If you want to register your CIMPLICITY node as a plug-in with Configuration Hub that is installed locally or remotely during the installation of CIMPLICITY, you must install Proficy Authentication 2024 and Configuration Hub 2024, or upgrade them to 2024. For more information, refer to [Proficy Authentication 2024](#), and [Configuration Hub 2024](#).

Install CIMPLICITY using Proficy Installer

The CIMPLICITY Proficy installer enables you to install various CIMPLICITY setups, from viewer to Historian configurations, along with other supported products. You only need to download the installer once and install all the products necessary to support your CIMPLICITY project. Additionally, you can register your CIMPLICITY node as a plug-in in Configuration Hub during the installation, saving you time by eliminating the need for additional registration tasks after installing CIMPLICITY. However, you still need to perform tasks such as creating a project in CIMPLICITY and more.

What is a CIMPLICITY Plug-in?

A CIMPLICITY plug-in with Configuration Hub represents a CIMPLICITY server node. Using the CIMPLICITY plug-in, you can browse your CIMPLICITY project's OPC UA devices, and MQTT devices in Configuration Hub, which operates as a web-based application.

How Can I register my CIMPLICITY Node as a Plug-in with Configuration Hub?

You can register a CIMPLICITY node as a plug-in either during the installation, also called as the **Install Time Registration** method, or post installation, also called as the **Central Registration method**. For more information on the CIMPLICITY plug-in, supported registration types, and the different registration methods, refer to About CIMPLICITY Plug-in with Configuration Hub, in Getting Started..

Supported Setup for CIMPLICITY Plug-in Registration

Components	Version
CIMPLICITY	2024
Configuration Hub	2024
Proficy Authentication	2024

**Note:**

If you are using previous version of Configuration Hub and Proficy Authentication, kindly upgrade to version 2024.

All the three components can be on the same machine, or the components can be installed on three different machines. However, both CIMPLICITY and Configuration Hub must use the same Proficy Authentication.

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.



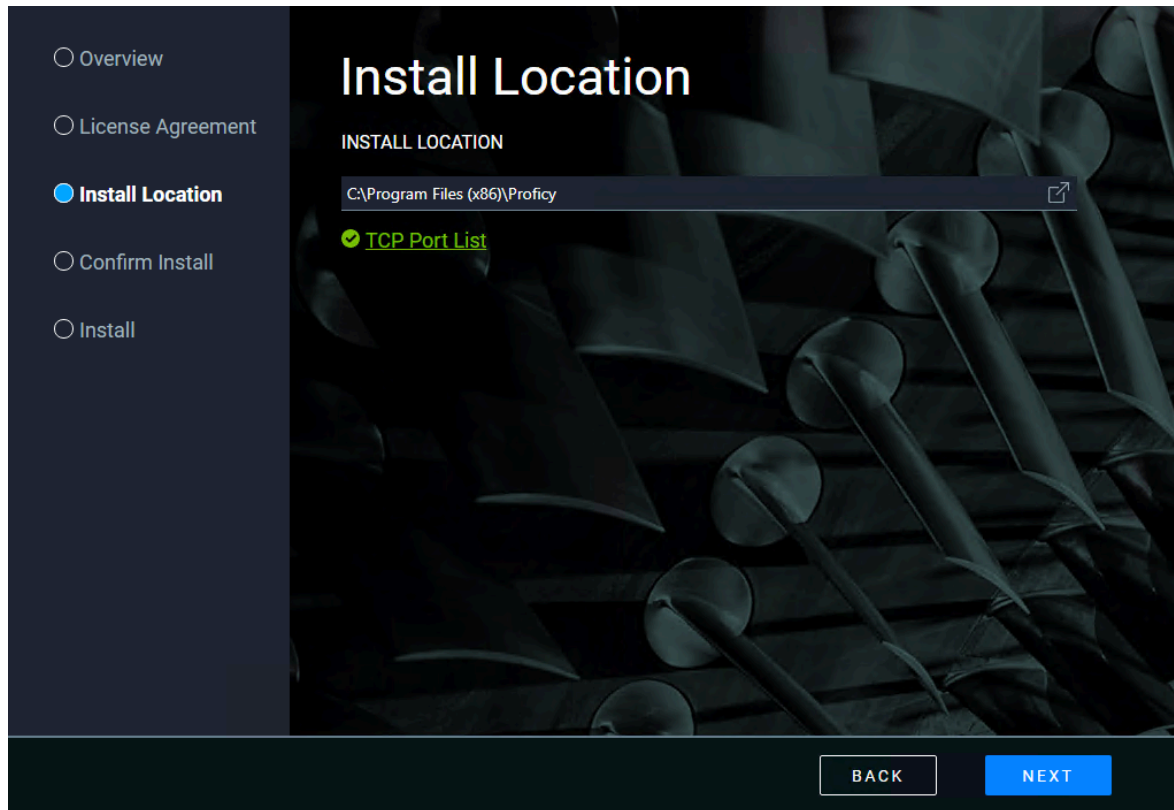
3. To install the CIMPLICITY server, select the package as needed and click **START**.

- SCADA Standalone Server
- SCADA with Remote Historian
- SCADA with Tracker

The **Review License Agreement** screen appears.

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

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



5. Leave the default location, or 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.

The **Registration with Configuration Hub** screen appears.

Registration with Configuration Hub

Skip this step to continue with installation and register later with utility.

CONFIGURATION HUB

BASE URL
 Not trusted

ADMIN CLIENT ID

ADMIN CLIENT SECRET

PROFICY AUTHENTICATION

Use Configuration Hub Authentication Credentials

BASE URL:
 Not trusted

ADMIN CLIENT ID:

ADMIN CLIENT SECRET:

Warning: A valid Configuration Hub URL must be provided.
 A valid Proficy Authentication server URL must be provided.

HINTS

- Hover over specific fields to see hints
- Use the credentials created during the Configuration Hub & Proficy Authentication install process
- Validate button will be enabled after filling all mandatory fields and trusting the certificate

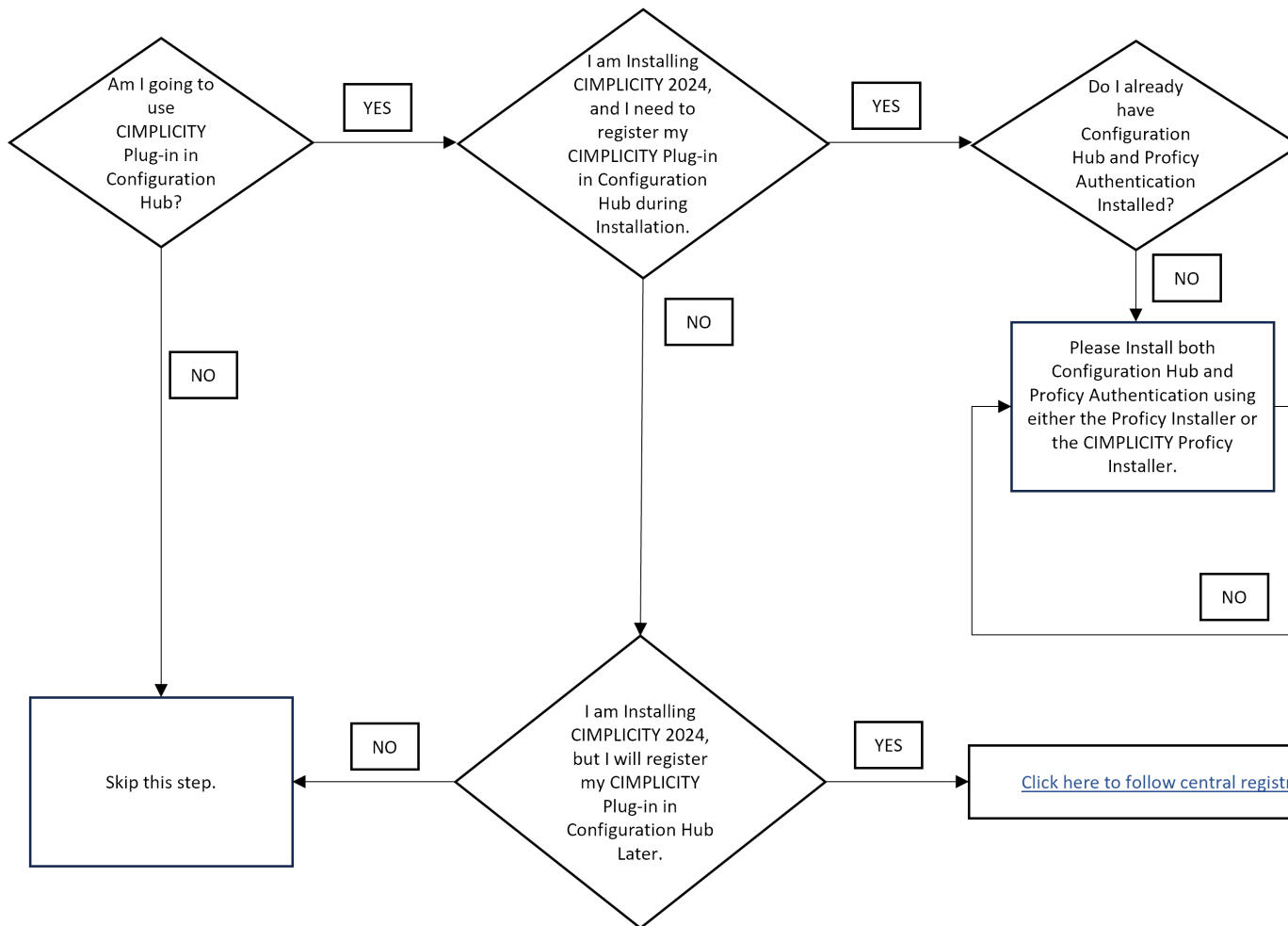
BACK **VALIDATE**

6. On this screen you can register CIMPLICITY plug-in with Configuration Hub, provided, you have already installed Configuration Hub 2024 and Proficy Authentication 2024, either locally or remotely.

How do I decide if I can continue registering CIMPLICITY plug-in with Configuration Hub?

If you are new to the CIMPLICITY plug-in and Configuration Hub, or if you are interested to know more before you decide the registration method, it is recommended that you refer to [CIMPLICITY plug-in registration use cases \(on page 83\)](#), or if you are already aware of CIMPLICITY plug-in and you need a quick guidance to decide the registration method, you can see the below image.



CIMPLICITY Plug-in Registration in Configuration Hub



1. [#unique_6_Connect_42_ol_crj_vk2_2bc](#) (on page 14)
2. [About Central Registration](#) (on page 86)
 - a. If you decided to register CIMPLICITY plug-in with Configuration Hub, provide the following Configuration Hub and Proficy Authentication details:



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

Field	Description
BASE URL	Enter a valid base URL in the following format <code>https://hostname:<port number>/configurationhub</code> .

Field	Description
	<ul style="list-style-type: none"> ▪ hostname: The hostname of the Configuration Hub server to which you want to register. ▪ <port number>: The port number of the Configuration Hub server to which you want to register. <p>Note:</p> <ul style="list-style-type: none"> ▪ Do not enter a slash at the end of the base URL. ▪ If the base URL indicates  Not trusted, it means there is no trust established with the host, or the root certificate of Configuration Hub server is incorrect. You must verify the base URL and enter a valid URL to establish the trust  with the host and with the correct root certificate details.
ADMIN CLIENT ID	The admin client ID of the Configuration Hub server that you provided during the Configuration Hub installation.
ADMIN CLIENT SECRET	The admin client secret of the Configuration Hub server that you provided during the Configuration Hub installation.

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

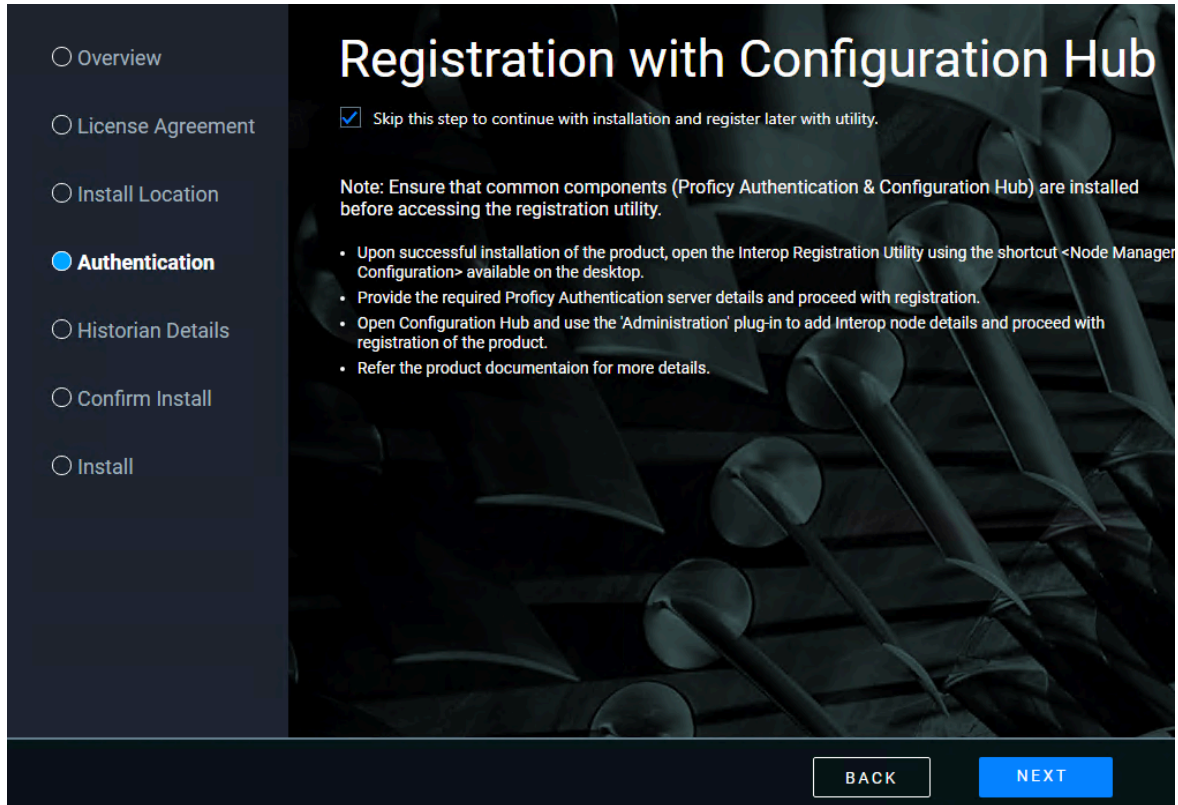
Field	Description
Use Configuration Hub Authentication Credentials	Select this check box if you used the same credentials for both Configuration Hub and Proficy Authentication during installation.
BASE URL	Enter a valid base URL in the following format https://hostname:<port number>/uaa.

Field	Description
	<ul style="list-style-type: none"> ▪ hostname: The hostname of the Proficy Authentication server to which you want to register. In the <Fully Qualified Domain Name> format. ▪ <port number>: The port number of the Proficy Authentication server to which you want to register. <p>Note:</p> <ul style="list-style-type: none"> ▪ Do not enter a slash at the end of the base URL. ▪ If the base URL indicates  Not trusted, it means there is no trust established with the host, or the root certificate of Proficy Authentication server is incorrect. You must verify the base URL and enter a valid URL to establish the trust  with the host and with the correct root certificate details.
ADMIN CLIENT ID	The admin client ID of the Proficy Authentication server.
ADMIN CLIENT SECRET	The admin client secret of the Proficy Authentication server.

b. Select **Validate**.


If the provided details are correct, the next screen appears based on the installation packages that you selected.



If you decided to register the CIMPLICITY plug-in later, select the **Skip this step to continue with installation and register later with utility** check box, and complete the installation. You can register the CIMPLICITY plug-in using the [central registration \(on page 86\)](#) method.




7. 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.	<ul style="list-style-type: none"> ◦ Configuration Hub ◦ Proficy Authentication ◦ Local License Server ◦ License Server Tool 	<p>In the Credentials screen, you will be prompted to enter the following details:</p> <ul style="list-style-type: none"> ◦ Configuration Hub <ul style="list-style-type: none"> ▪ CLIENT ID- Enter a client id, which you can use to login to the Configuration Hub application. <p>For example, ad- min</p>


Package	Description	Products Available	Details that you must provide while Installation
			<ul style="list-style-type: none"> ▪ CLIENT SECRET- Enter a secret password for your Configuration Hub client id. ◦ Proficy Authentication <ul style="list-style-type: none"> ▪ 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. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px; background-color: #E6F2FF;"> <p> 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</p> </div>

Package	Description	Products Available	Details that you must provide while Installation
			 Hub and Proficiency Authentication
SCADA Client	Select this option when you are intending to run CIMPLICITY as a client and Proficy WebSpace.	<ul style="list-style-type: none"> ◦ 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	<p>Select this option when you are intending to run CIMPLICITY, Historian, Proficy WebSpace, Operations Hub, and other components on one server.</p> <p>You can install Operations Hub and other products not included in this package separately post installing this package.</p>	<ul style="list-style-type: none"> ◦ SCADA ◦ Historian Client Tools ◦ Historian Server ◦ Historian Collectors ◦ Industrial Gateway Server (IGS) ◦ HMI for CNC ◦ Alarm Cast ◦ Proficy WebSpace ◦ Operations Hub 	<p>In the Historian details screen, you will be prompted to enter the following details if you have Historian Installed:</p> <ul style="list-style-type: none"> ◦ HISTORIAN SERVER- IP address or hostname in a fully qualified domain name format. ◦ Windows username and password of the default historian server to which the Remote Collector manager will connect. ◦ Historian data Path to install Historian Server. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;">  <p>Note: You will be prompted with the Historian details only if you selected</p> </div>


Package	Description	Products Available	Details that you must provide while Installation
			<div data-bbox="1138 306 1422 420" style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px; background-color: #E6F2FF;">  Historian product. </div> <p data-bbox="1138 457 1422 709">In the Historian details screen, you will be prompted to enter the following details if you have not installed Historian server:</p> <ul style="list-style-type: none"> <li data-bbox="1122 737 1422 947">◦ Enable Historian services security- select this if you want to set up security while installation. <ul style="list-style-type: none"> <li data-bbox="1203 961 1422 1220">▪ CERTIFICATE PASSPHRASE- Enter a passphrase for the certificate generation. <p data-bbox="1060 1262 1422 1381">In the Operations Hub Details screen, you will be prompted with the following details:</p> <p data-bbox="1060 1423 1198 1451">Credentials</p> <ul style="list-style-type: none"> <li data-bbox="1122 1493 1422 1661">◦ Username- Enter a user name, which you can use to login to the Operations Hub application. For example, <code>ch_admin</code> <li data-bbox="1122 1759 1422 1879">◦ Password- Enter a password for your Operations Hub user login.

Package	Description	Products Available	Details that you must provide while Installation
			<p>Authentication</p> <p>Configuration Hub</p> <ul style="list-style-type: none"> ◦ Register After Install- If you select this check box, then you can skip registering Operations Hub with the Configuration 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.. <p>If you choose to register along with the current Operations Hub installation, then leave this check box blank and proceed to provide more details.</p> <ul style="list-style-type: none"> ◦ BASE URL- Enter the url address to access the Configuration Hub application. <p>For example, <code>https://sbbco.meridium-</code></p>

Package	Description	Products Available	Details that you must provide while Installation
			<p><code>.com:5000/contain-</code> <code>er-svc</code></p> <ul style="list-style-type: none"> ◦ CLIENT ID- Enter the url address to access the Configuration Hub application. <p>For example, <code>https://</code> <code>sbbco.meridium-</code> <code>.com:5000/contain-</code> <code>er-svc</code></p> <ul style="list-style-type: none"> ◦ CLIENT SECRET- Enter the secret password created for your Configuration Hub client id. <p>Proficiency Authentication</p> <ul style="list-style-type: none"> ◦ Use Locally Installed Proficiency Authentication- If you select this check box, then the local instance of Proficiency Authentication will be used. If you want to use an external Proficiency Authentication (UAA), then leave this check box blank and proceed to provide more details. <div data-bbox="1138 1654 1422 1852" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Prior to Operations Hub installation,</p> </div>

Package	Description	Products Available	Details that you must provide while Installation
			<div data-bbox="1143 306 1427 1050" style="border: 1px solid #0070c0; border-radius: 10px; padding: 10px; background-color: #e6f2ff;">  you must have a local or remote 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. </div> <ul style="list-style-type: none"> ◦ BASE URL- Enter the url address to access the Proficy Authentication application. For example, <code>https://win10vm2/uaa</code> ◦ ADMIN CLIENT ID- Enter the administrator client id to login to Proficy Authentication. For example, <code>admin</code> ◦ ADMIN CLIENT SECRET- Enter the secret password for the Proficy Authentication administrator client id.

Package	Description	Products Available	Details that you must provide while Installation
SCADA with Remote Historian	Select this option when you are intending to run CIMPLICITY with Historian on a remote server and Proficy WebSpace.	<ul style="list-style-type: none"> ◦ 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.	<ul style="list-style-type: none"> ◦ 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 server than CIMPLICITY SCADA.	Historian Server	You will be prompted to enter Historian details. For more information, see the SCADA Standalone Server row above.
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.

Package	Description	Products Available	Details that you must provide while Installation
MQTT Client	<p>MQTT Client enables you to connect the SCADA/HMI clients with MQTT Brokers to communicate with the IoT devices in the plant.</p> <div data-bbox="496 657 743 1150" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: Configuration of MQTT Client requires Configuration Hub to be installed in the SCADA network. </div>	MQTT Client	For more information, see MQTT Client (<i>on page</i>).

8. Select **Next**.

9. 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.

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

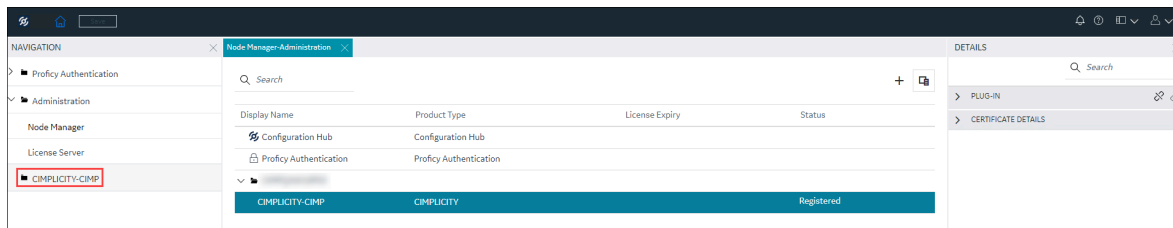
A message appears asking whether you want to restart your computer, or install more products.

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

If you selected to register CIMPLICITY plug-in with Configuration Hub, when you reboot your machine and log into Configuration Hub, the CIMPLICITY plug-in will appear in the **Navigation** pane, as shown in the image below. You can use your CIMPLICITY plug-in. For more information, refer to [Overview of the CIMPLICITY plug-in within Configuration Hub \(on page 95\)](#)

**Note:**

To access the plug-in, you must have the **SCADA.COMPUTER@[NodeName].\$CONFIGSECGRP** scope published to Proficy Authentication. By default, all the needed scopes are added to the ch_admin user.



Running the Proficy Installer 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 Proficy 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 Proficy 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 Proficy 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 Proficy Installer from a Command Line \(on page 31\)](#) 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 Proficy Installer 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- **[Install 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 Proficy 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 Proficy installer \(on page 26\)](#) 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	<ul style="list-style-type: none"> 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.

Parameter	Description
InstallType	InstallType=COMPLETE indicates complete installation.
OverwriteExisting	<p>If any CIMPLICITY component already exists in the machine, this parameter determines if the installation must continue or abort.</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <ul style="list-style-type: none"> • 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	<p>To integrate CIMPLICITY with the firewall:</p> <ul style="list-style-type: none"> • A value of TRUE will trigger firewall integration. • A value of FALSE will not trigger firewall integration.

Parameter	Description
WebConfigPort	The port of Web configuration. Default is 9443.
CimConfigServicePort	The CIMPLICITY Configuration Service Port. Default is 4955.
HelpMode	<p>The type of Help you want to configure with CIMPLICITY:</p> <ul style="list-style-type: none"> • 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. <div data-bbox="820 961 1421 1138" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;">  Note: HelpMode=1 is not a valid option for a viewer. </div>
HelpServerName	<p>Host Name or IP Address of the server that has help installed. This parameter is required only if you selected Remote Help (HelpMode=0).</p> <div data-bbox="820 1318 1421 1633" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;">  Note: This value defaults to localhost if it is not specified in <code>quiet.ini</code>. It is useful to specify help server name if helpfiles feature is not included as part of installation using the InstallFeatures parameter. </div>
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:

Parameter	Description
	<ul style="list-style-type: none"> • /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.

Component/Option	Description
Change Management	<p>Enables users who also have a licensed Change Management product can now manage CIMPLICITY project configuration revisions.</p> <p>Change Management functionality includes:</p> <ul style="list-style-type: none"> • 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	<p>Provides dynamic replay of Historian or SQL historical point data through CimView.</p> <p>Note: Dynamic Graphic Replay (DGR) replaces VCR.</p>
Marquee Driver	Controls Marquee display devices on COM ports.
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	<p>Allows the user to</p> <ul style="list-style-type: none"> • (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.

Component/Option	Description
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
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.

Component/Option	Description
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.

Components/Options	Description
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 Proficy installer, the online help mode is selected by default. Pressing F1 in the application will direct you to the help on the GE Vernova documentation server. However, if you prefer to install the help locally, you can follow the steps provided in this topic.



Note:

It is recommended to use the [online help](#), as it is always updated.

To install the help locally,

1. Ensure that projects are not running.
2. Open Windows PowerShell as an administrator.

The Windows PowerShell prompt appears.

3. In the PowerShell prompt, navigate to **[ISO media location]\CIMPLICITY\Setup\help**.

For example, if the ISO media is in the D:\ drive, you can enter **cd D:\CIMPLICITY\Setup\help**.

4. Execute the **Setup.bat** file by entering the **.\Setup.bat** command.

The help installation begins.

5. After installing, in CIMPLICITY Options, change the help option to **Local Help**. For more information, refer to the **Configure Help** section in the *Project Setup* guide.

Chapter 3. 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 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 43)	How to set up the foundation for your system goals.
Part 2 (on page 44)	How to set up points and alarms.
Part 3 (on page 45)	How to create powerful applications that can graphically deal with system data for whoever has access privileges.
Part 4 (on page 47)	Many other powerful tools.
Part 5 (on page 49)	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: <ul style="list-style-type: none"> • 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 <i>Quick Device Setup</i> in the documentation gives you quick start for both.
Step 5.	Define security and routing including: <ul style="list-style-type: none"> • 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.	<p>Create points including:</p> <ul style="list-style-type: none"> • 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.	<p>Configure alarms.</p> <ul style="list-style-type: none"> • 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.	<p>Test your configuration in the Point Control Panel.</p> <ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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	
	<ul style="list-style-type: none"> ◦ 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.	<p>Test your configuration through CimView.</p> <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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
	<ul style="list-style-type: none"> • 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	<p>The Basic Control Engine option consists of three main components:</p> <ul style="list-style-type: none"> • 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
	<ul style="list-style-type: none"> • 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 data, 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	<p>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 CIMPLICITY Basic, VB, C++, VBA, VBScript.</p> <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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
	<ul style="list-style-type: none"> • 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	<p>There are two distinct, yet interrelated pieces to Tracker: Production Tracking (PRT) and Routing Control Objects (RCO).</p> <ul style="list-style-type: none"> • 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	<p>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:</p> <ul style="list-style-type: none"> • 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
	<ul style="list-style-type: none"> <li data-bbox="477 275 1416 348">• Tracker Attribute Database (TADB) stores comprehensive data about items, including orders and product components. <li data-bbox="477 401 1386 474">• Range Source Architecture (RSA) enhances the traditional RCO concept of a Tracker source (source region). <li data-bbox="477 527 1398 730">• 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. <li data-bbox="477 783 1406 947">• 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. <li data-bbox="477 999 1414 1119">• 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. <li data-bbox="477 1171 1398 1245">• Marquee Manager product family monitors manufacturing environments and sends real time, automated messages to visual and/or audible devices.

Chapter 5. 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 \(on page 52\)](#)
- [Update validity of the Self Signed SSL Certificate \(on page 53\)](#)

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.
- **<ServerCertificateName>**: 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\" 4955 4956
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.
- **<ServerCertificateName>**: 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 %BSM_ROOT%\ScadaConfigPki\CimScadaConfigRootCA.cert. For example, C:\Program Files (x86)\Proficy\Proficy CIMPLICITY\ScadaConfigPki\CimScadaConfigRootCA.cert.
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.

Secure REST Calls using SSL Certificate Validation

CIMPLICITY system internally makes REST calls to remote systems for some of the operations such as starting and stopping remote projects. SSL certificate validation will ensure that the REST calls are secure.

To ensure that these REST calls are secure, you must add the CIM_SSL_STRICTPOLICY (on page) global parameter in both Project and system and set it to Y.

**Note:**

Root certificates must be in the PEM format (usually with .crt extension)

To establish trust, you must perform the following steps:

On the primary server machine

Before you begin, ensure that you have copied the secondary server's certificate from `%ROOT%\admin_data\pauth_pki\trusted\
\<secondary_server_computer>_CimScadaConfigRootCA`.

For example, `C:\Program Files (x86)\Proficy\Proficy CIMPLICITY\admin_data\
\pauth_pki\trusted\Server2_CimScadaConfigRootCA`.

1. Go to `%ROOT%\admin_data\pauth_pki\trusted`.
2. Paste the secondary server's certificate in this location.

On the secondary server machine

Before you begin, ensure that you have copied the primary server's certificate from `%ROOT%\admin_data\
\pauth_pki\trusted\
\<primary_server_computer>_CimScadaConfigRootCA`.

For example, `C:\Program Files (x86)\Proficy\Proficy CIMPLICITY\admin_data\
\pauth_pki\trusted\Server1_CimScadaConfigRootCA`.

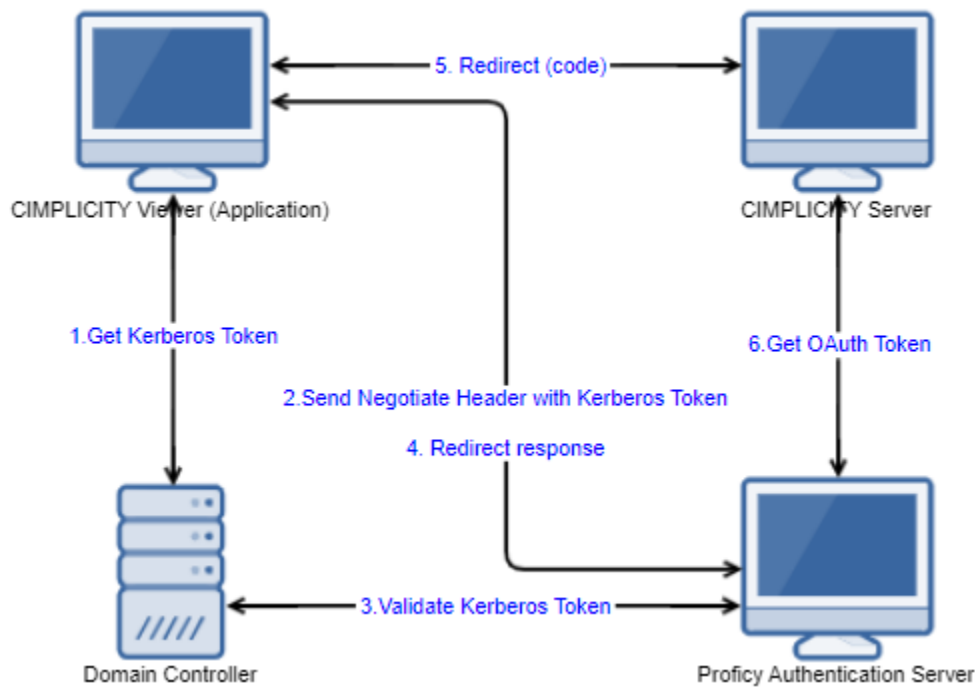
1. Go to `%ROOT%\admin_data\pauth_pki\trusted`.
2. Paste the primary server's certificate in this location.

Chapter 6. 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.



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
		<ol style="list-style-type: none"> To access Local Security Policy, enter <code>secpol.msc</code> in Windows Run dialog and select OK. Navigate to Security Settings > Local Policies > Security Options. Double-click and open <div data-bbox="1117 632 1419 821" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <pre>Network security: Configure encryption types allowed for Kerberos</pre> </div> security policy setting. Select the valid encryption types that you want to use. Ensure that the selection is same across all the nodes. <p>Encryption types allowed for Kerberos: AES256_HMAC_SHA1</p> <p>Configure Proficy Authentication on CIMPLICITY server (on page 66).</p> <div data-bbox="1024 1415 1419 1827" style="border: 1px solid #0070c0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note:</p> <ul style="list-style-type: none"> Ensure that the fully qualified domain name is specified in Proficy authentication server configuration </div>

Node	Configuration	Description
		 <ul style="list-style-type: none"> • Ensure that the required security groups are published.
Domain Controller	Configure Security Policy	<p>Ensure that correct encryption types are associated to Kerberos authentication is selected.</p> <ol style="list-style-type: none"> 1. To access Local Security Policy, enter <code>secpol.msc</code> in Windows Run dialog and select OK. 2. Navigate to Security Settings > Local Policies > Security Options. 3. Double-click and open <div data-bbox="1117 1058 1419 1247" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Network security: Configure encryption types allowed for Kerberos</p> </div> 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	<p>Before you begin, ensure that you have performed the following:</p> <ul style="list-style-type: none"> • Created a dummy user account on the Active Directory Server node to represent the Proficy Authenti-

Node	Configuration	Description
		<p>cation application in the active directory registry.</p> <ul style="list-style-type: none"> • Configured Security Policy. <p>To perform this task, you must be an administrator.</p> <ol style="list-style-type: none"> 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: <code>setspn -S HTTP/<FQDN> <user account></code> <p><FQDN>- Fully Qualified Domain Name (FQDN) of the server on which Proficy Authentication service is running.</p> <p><user account>- Dedicated user account created for Proficy Authentication service.</p>
	Generate Keytab File	<p>Before you begin, ensure that you have performed the following:</p> <ul style="list-style-type: none"> • Created Service Principal. <p>To perform this task, you must be an administrator.</p>

Node	Configuration	Description
		<ol style="list-style-type: none"> 1. Log in to your system and open the Windows Command Prompt application. 2. Run the following command replacing with the appropriate code: <code>ktpass -out <filename> -principal HTTP/<service principal name> -mapUser <user account> -mapOp set -password <password> -crypto AES256-SHA1 -pType KRB5_NT_PRINCIPAL</code> <p>You can do the following to verify if the service principal is mapped to the dummy account, and a keytab is created:</p> <ol style="list-style-type: none"> 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
		<ol style="list-style-type: none"> 1. To access Local Security Policy, enter <code>secpol.msc</code> in Windows Run dialog and select OK. 2. Navigate to Security Settings > Local Policies > Security Options. 3. Double-click and open <div data-bbox="1117 632 1419 821" style="background-color: #f0f0f0; padding: 5px; margin: 10px 0;"> <pre>Network security: Configure encryption types allowed for Kerberos</pre> </div> 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	<p>Before you begin, ensure that you have performed the following:</p> <ul style="list-style-type: none"> • 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. <p>To perform this task, you must be an administrator:</p>

Node	Configuration	Description
		<ol style="list-style-type: none"> 1. Log in to the computer machine where Proficy Authentication is installed. 2. Access the <code>uaa.yml</code> file. The file is located at <code>c:\ProgramData\GE\Operations Hub\uaa-config\uaa.yml</code> 3. To modify, open <code>uaa.yml</code> in any text editor. 4. Search for <code>kerberos</code> and enter values for the following keys: <code>service-principal</code> and <code>keytab-location</code> 5. Save and close the modified file. 6. Restart the <code>GE Proficy Authentication Tomcat Web Server</code> service. <ol style="list-style-type: none"> a. Access the Windows Run dialog. b. Enter <code>services.msc</code> to open the Services screen. c. Right-click <code>GE Proficy Authentication Tomcat Web Server</code> and select Restart.
	<p>Configure LDAP Provider</p>	<p>Add an LDAP provider and make appropriate mappings.</p> <p>Ensure that the logged in user name can work with user filter specified in Proficy Authentication.</p>

Chapter 7. 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 and CIMPLICITY server certificates are installed and trusted on all the viewer nodes.

1. Copy the following certificates from the CIMPLICITY server machine:

- **ProficyAuth_Root.cert:**

```
%INTEROP_ROOT%\CentralCerts\ProficyAuthentication  
\ProficyAuth_Root.cert
```

For example,

```
C:\Program Files (x86)\Proficy\InteropService\CentralCerts  
\ProficyAuthentication\ProficyAuth_Root.cert.
```

▪ **CimScadaConfigRootCA.cert:**

```
%BSM_ROOT%\ScadaConfigPki\CimScadaConfigRootCA.cert
```

For example,

```
C:\Program Files (x86)\Proficy\Proficy CIMPLICITY  
\ScadaConfigPki\CimScadaConfigRootCA.cert.
```

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

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 Webspaces 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 \(on page 65\)](#) 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 with 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:

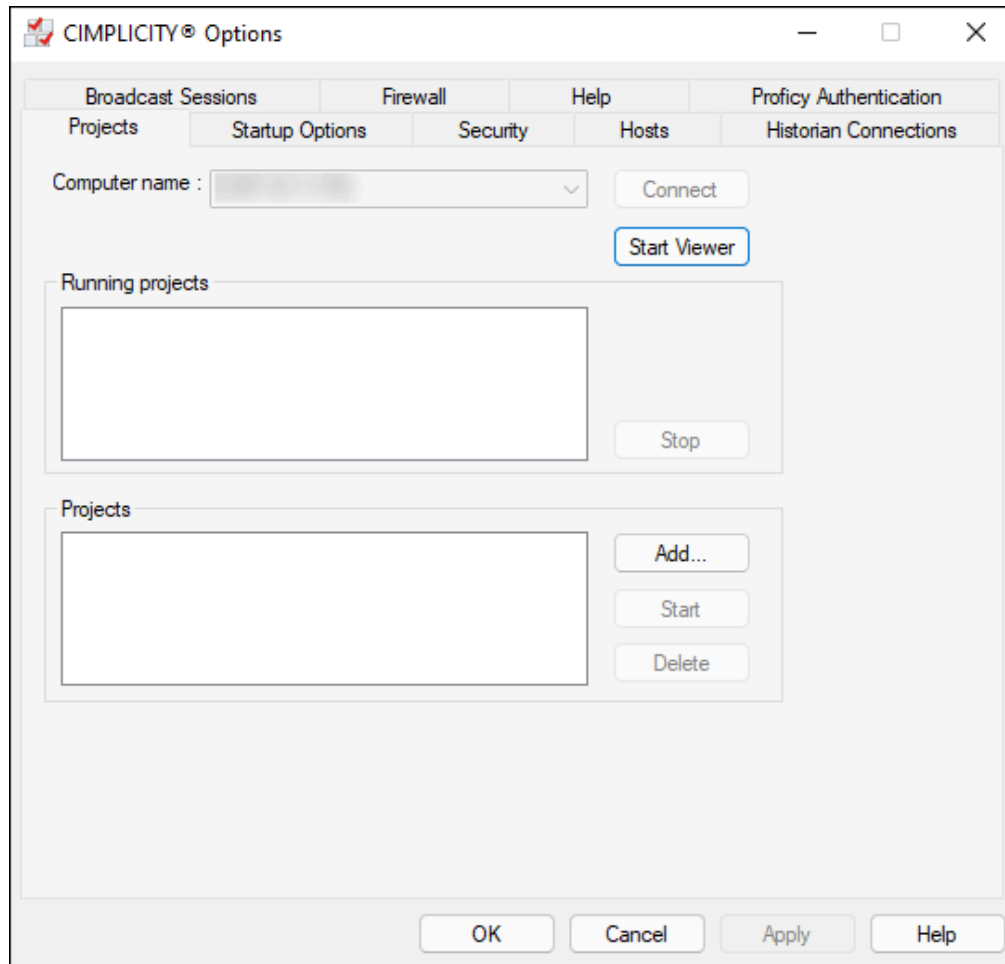
- [Configure Proficy Authentication Parameters in CIMPLICITY Options \(on page 67\)](#).
- [Enable and configure Proficy Authentication in Project Properties \(on page 71\)](#).

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 **CIMPLICITY Options**, see Access CIMPLICITY Options (on page).
The **CIMPLICITY Options** dialog box opens.

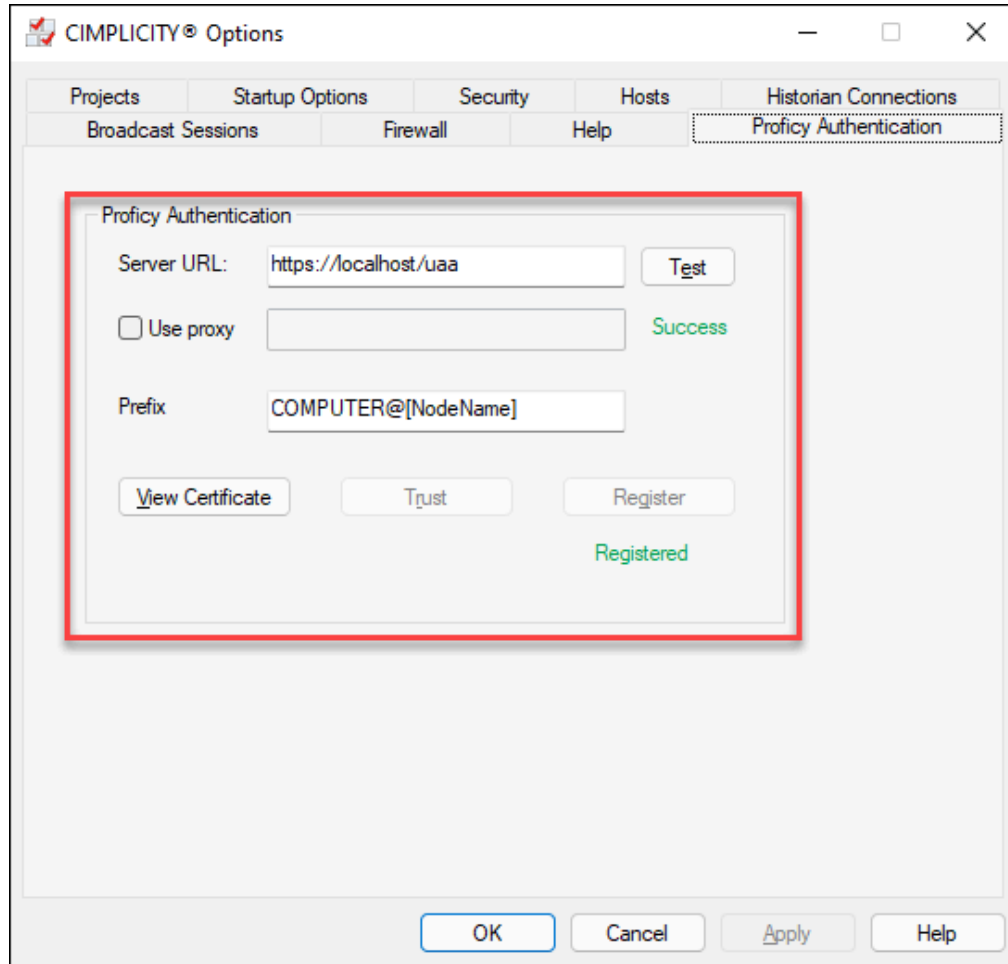


2. In the **CIMPLICITY Options** dialog box, click the **Proficy Authentication** tab.
The Proficy Authentication options are displayed.



Note:

To access this tab, you must be in administrator mode.



3. Enter the following details:

Options	Description
<p>Server URL</p>	<p>The URL of the Proficy Authentication server to which you want to register. In the <Fully qualified domain name> format.</p> <p>You can click the Test button to check the connection status of the Proficy Authentication server.</p> <p>If the connection to the Proficy Authentication server is successful, you will receive a success dialog. If your connection is unsuccessful, retry</p>

Options	Description
	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 \(on page 70\)](#).
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.

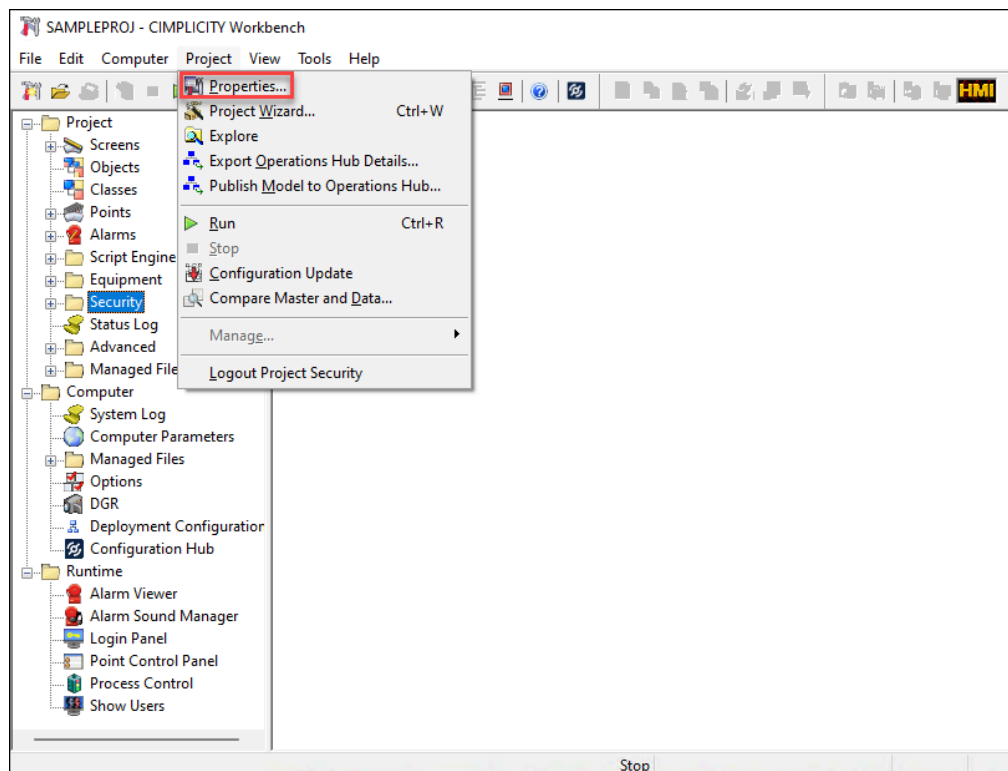
Enable and configure Proficy Authentication in Project Properties

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.

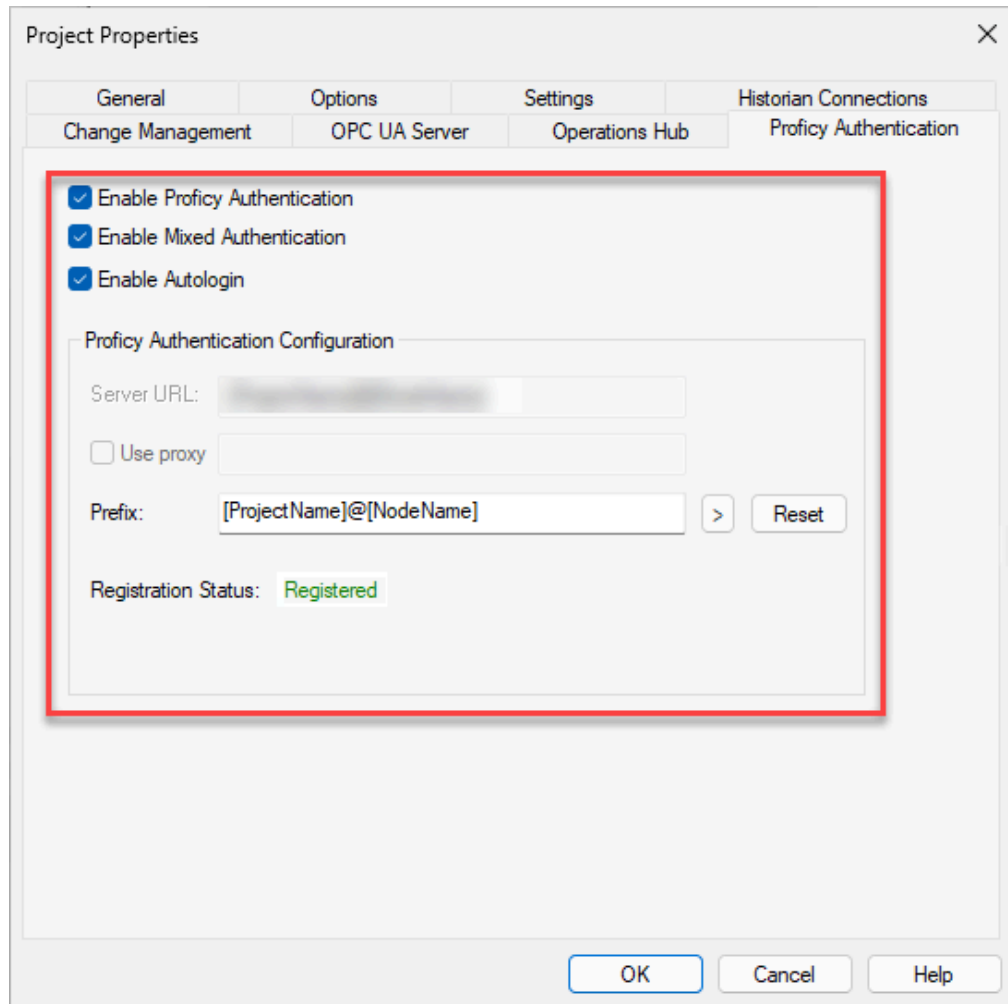


3. In the **Project Properties** dialog box, click the **Proficy Authentication** tab.
The Proficy Authentication options are displayed.



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.



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 Webspaces 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 \(on page 75\)](#).

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.SYSADMIN**. Where, **scada** is the default namespace. For more information on Groups, refer to [About Security Groups \(on page 75\)](#).

**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.

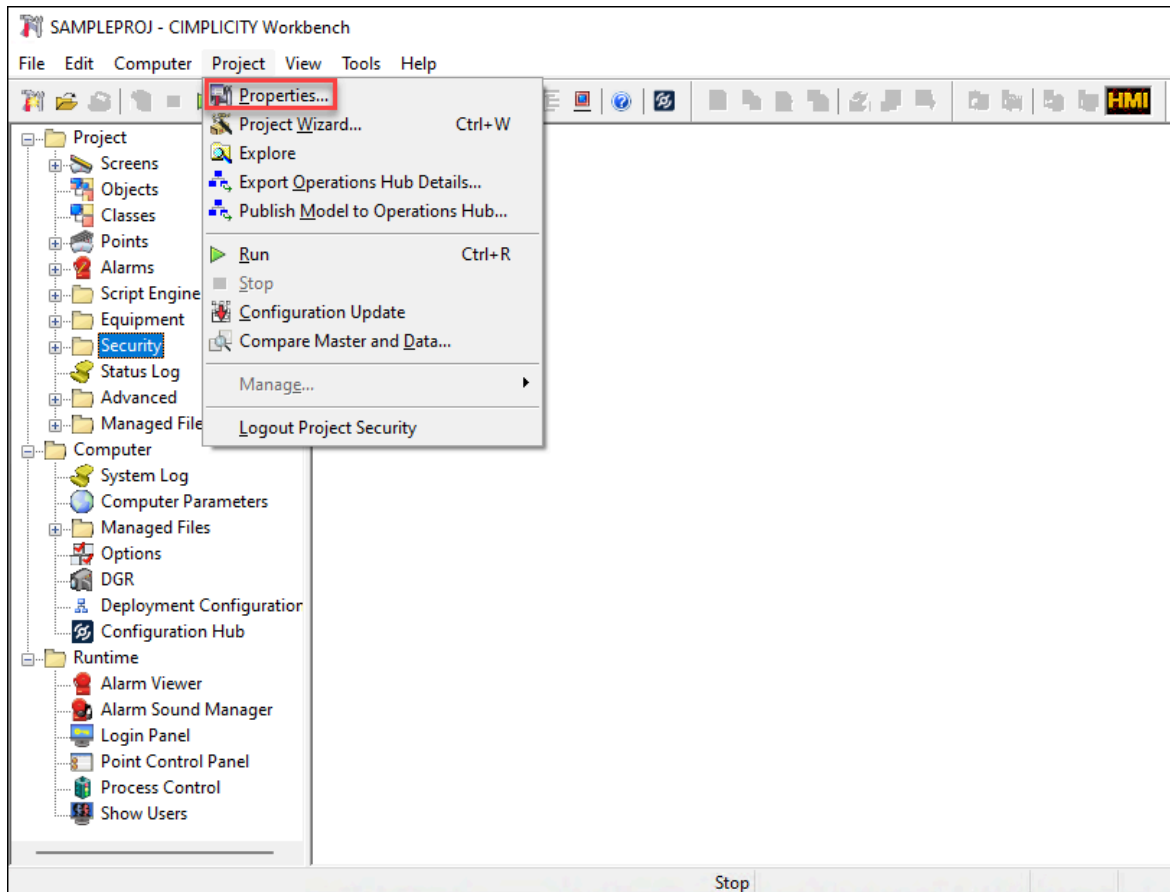
The configuration process is completed successfully. Now you can register CIMPLICITY with Proficy Authentication, and Configuration Hub.

Enable web configuration in Project Properties

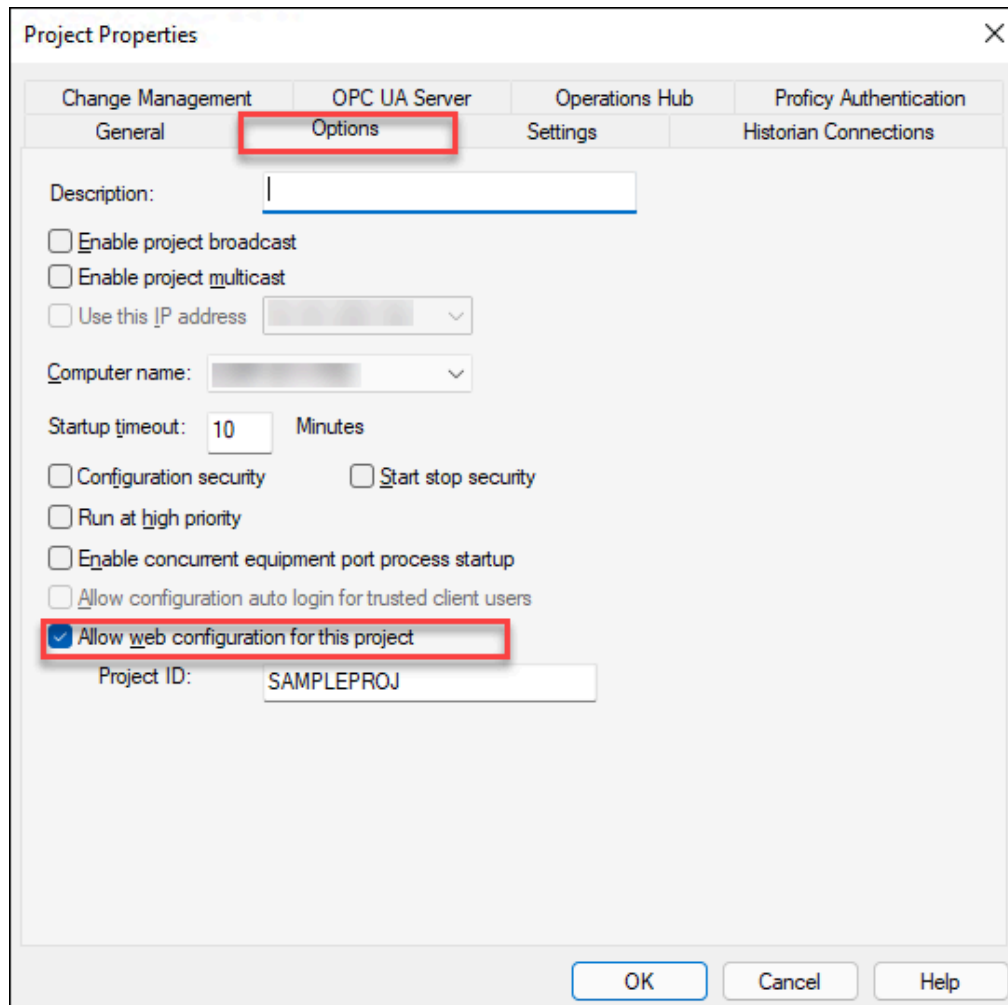
To host a project in Configuration Hub, you must enable the web configuration option for that project. When you configure and select the **Enable Proficy Authentication** check box in the **Project Properties> Proficy Authentication** tab, the **Allow web configuration for this project** check box in 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.



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:**

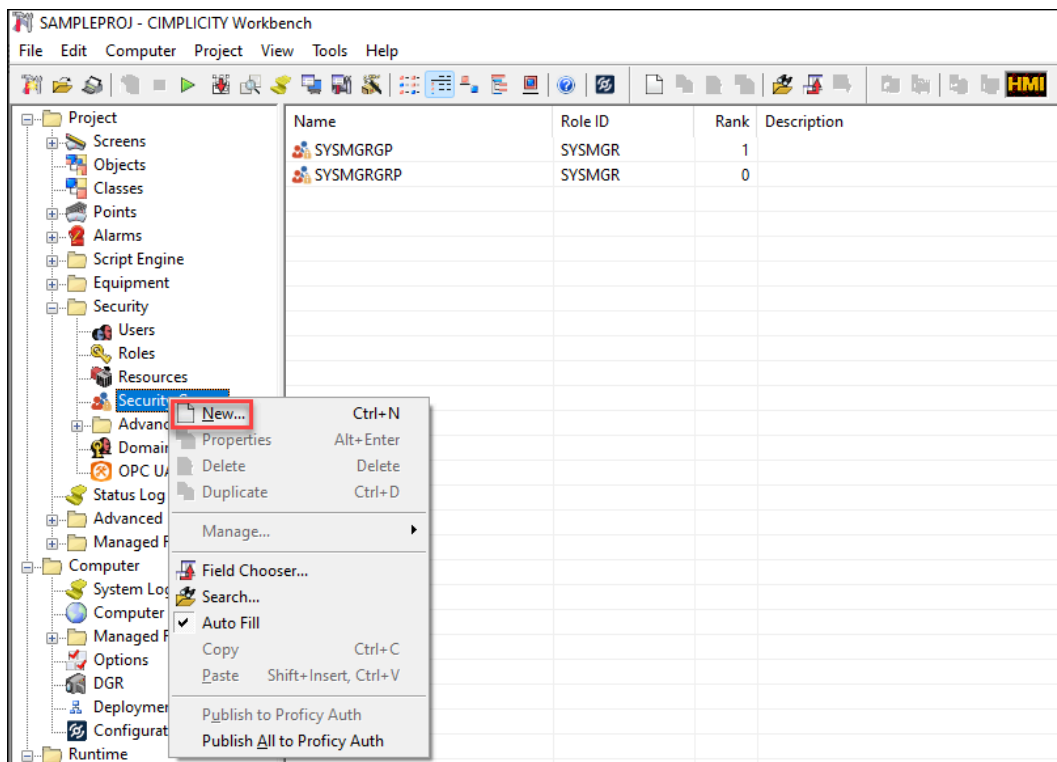
If you delete a group in CIMPLICITY, the Proficy Authentication users assigned to that group will not have the permission to use the assigned privileges.

You can [create \(on page 76\)](#), [edit \(on page 80\)](#), and [duplicate \(on page 81\)](#) a security group.

Create Security Groups in CIMPLICITY

To create a security group, do the following:

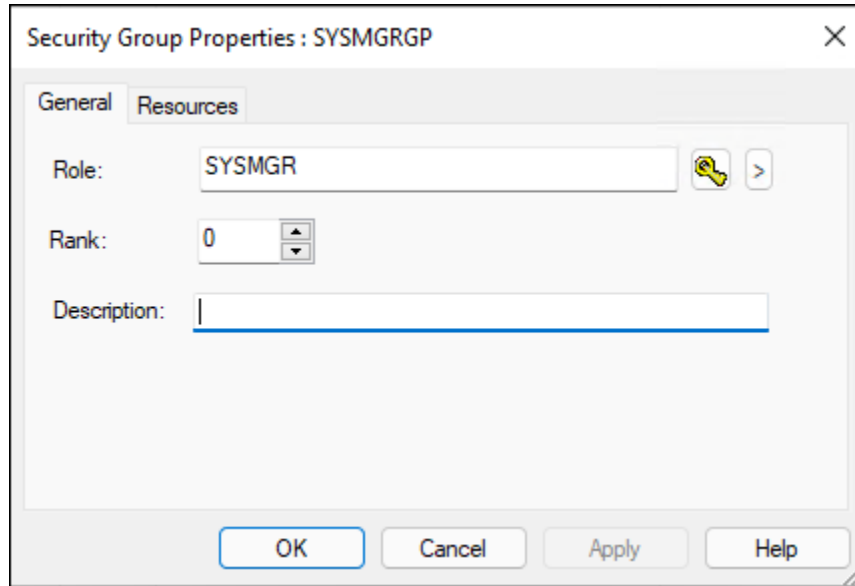
1. Open a project in **CIMPLICITY Workbench** as needed. For more information on Workbench, refer to the section About the CIMPLICITY Workbench. (on page).
2. In the top-level folders, click and expand **Project > Security**.
3. Right-click **Security Groups** and then click **New**.




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.



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** field, enter a description for the group.

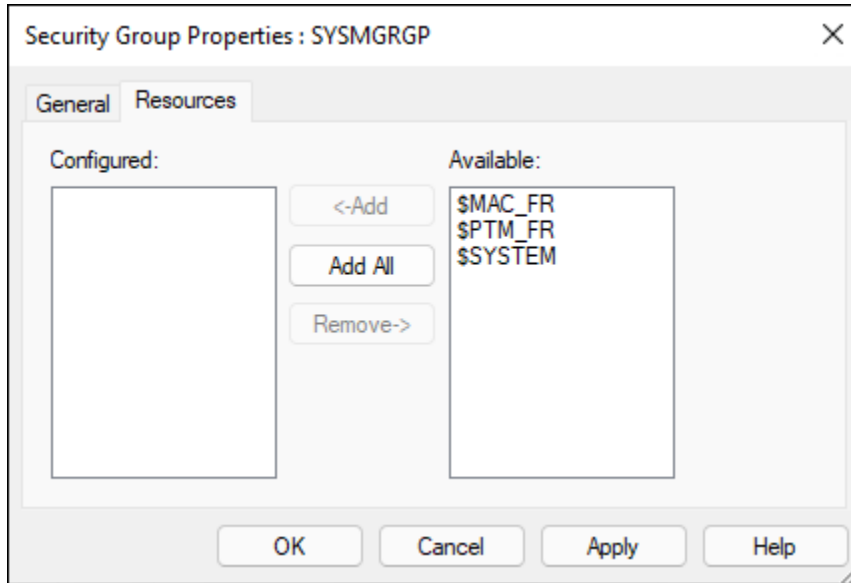
You can describe what a user is entitled if assigned to this group.

9. Click the **Resources** tab.

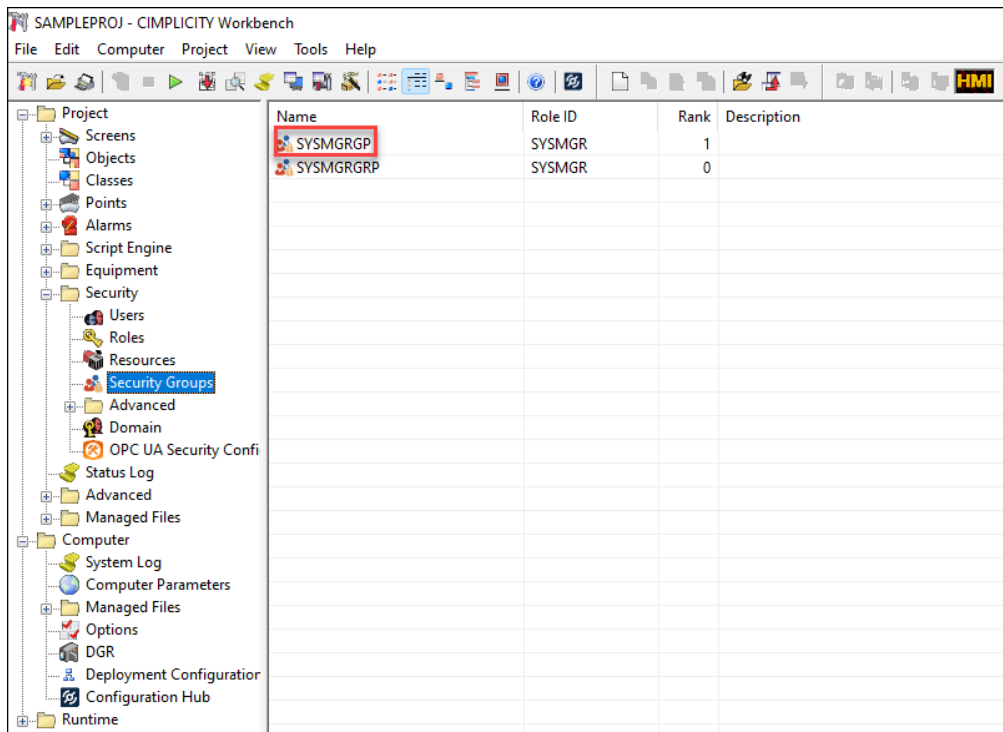
All the available resources are displayed.

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.



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:**

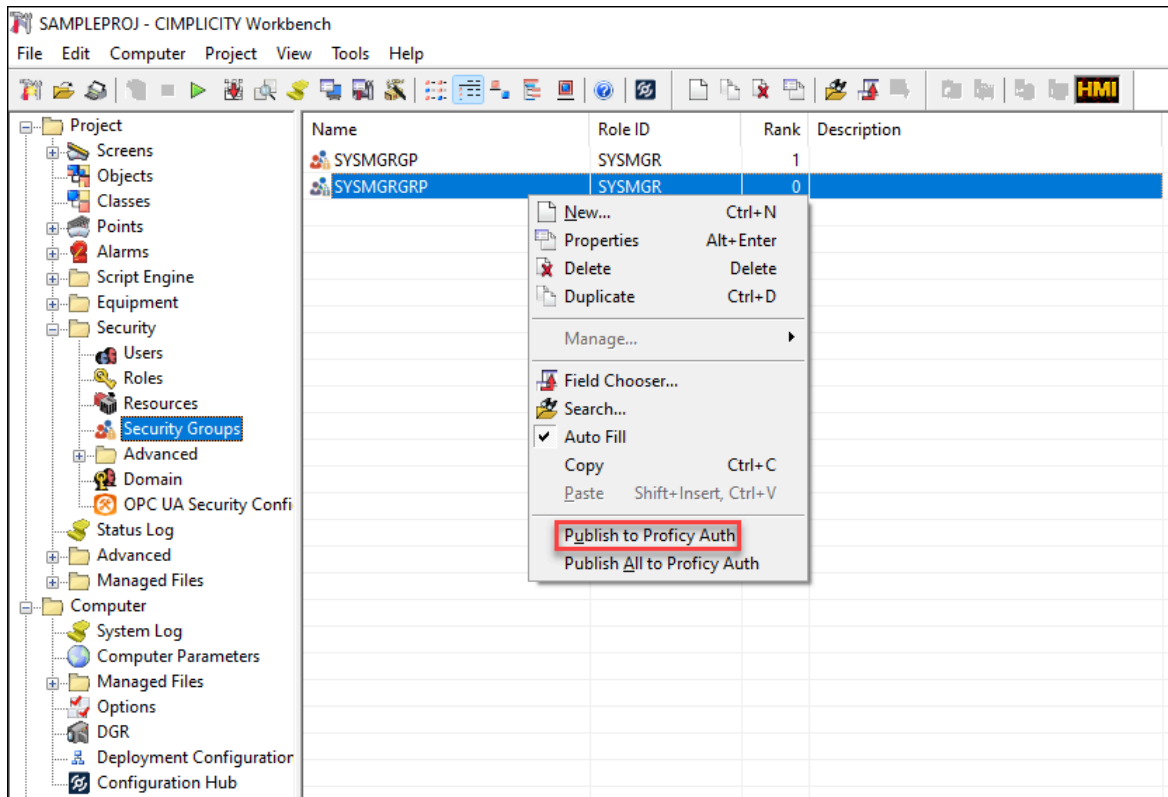
Ensure that the group names are unique.

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 \(on page 71\)](#).

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**.



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**.

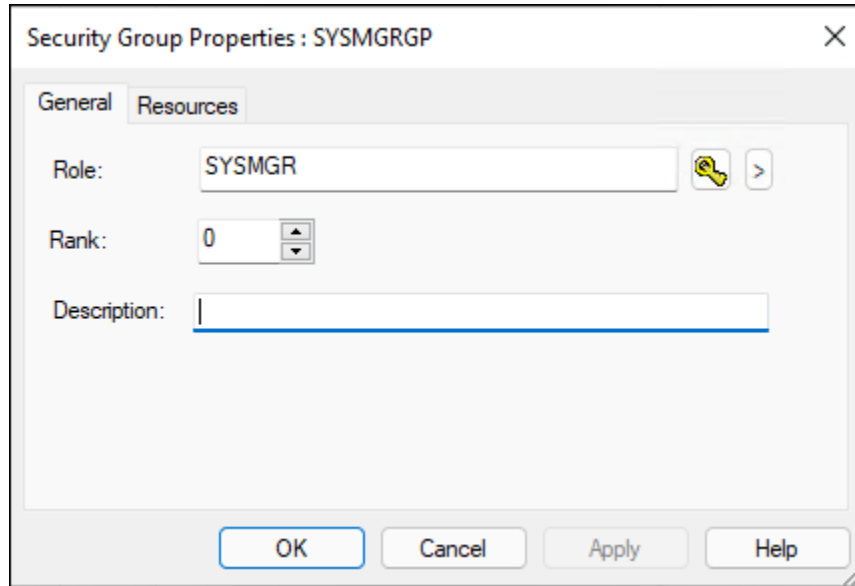


Note:

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 \(on page 71\)](#).

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 \(on page 68\)](#).
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.



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 8. CIMPLICITY Plug-in in Configuration Hub

About Registering CIMPLICITY Plug-in in Configuration Hub

What is a CIMPLICITY Plug-in?

A CIMPLICITY plug-in with Configuration Hub represents a CIMPLICITY server node. Using the CIMPLICITY plug-in, you can browse your CIMPLICITY project's OPC UA devices, and MQTT devices in Configuration Hub, which operates as a web-based application.

Configuration Hub allows you to register one or more CIMPLICITY nodes as plug-ins. To ensure secure interaction between Configuration Hub and a CIMPLICITY node, Proficy Authentication is used, which provides user account and authentication (UAA) service. Proficy Authentication provides identity-based security for applications and APIs. It supports open standards for authentication and authorization, including Oauth2.

Scopes Required to Access CIMPLICITY Plug-in in Configuration Hub

To access the plug-in, you must have the **SCADA.COMPUTER@[NodeName].\$CONFIGSECGRP** scope published to Proficy Authentication. By default, all the needed scopes are added to the ch_admin user.

Supported Setup for CIMPLICITY Plug-in Registration

Component	Version
CIMPLICITY	2024
Configuration Hub	2024
Proficy Authentication	2024



Note:

If you are using a previous version of Proficy Authentication and Configuration Hub, kindly upgrade to version 2024.

Supported Types of CIMPLICITY Plug-in Registration


- CIMPLICITY is installed on one machine, while Configuration Hub and Proficy Authentication are installed on another machine, provided that both CIMPLICITY and Configuration Hub are using the same Proficy Authentication.
- CIMPLICITY, Configuration Hub, and Proficy Authentication are installed on three different machines. Provided that both CIMPLICITY and Configuration Hub are using the same Proficy Authentication.
- CIMPLICITY, Configuration Hub, and Proficy Authentication are installed on the same machine.

If you have decided to follow the central registration method to register CIMPLICITY plug-in in Configuration Hub, or if you came to this topic directly, before you begin with the registration, for a very detailed information on different use cases, kindly refer to [CIMPLICITY plug-in registration use cases \(on page 83\)](#).

CIMPLICITY Plug-in Registration Use Cases

The following use cases provide detailed information on the different registration methods. You can use these uses cases as a reference to decide on the registration method.

First time Install: CIMPLICITY, Common components like Configuration Hub, and Proficy Authentication (Version 2024 or higher)



Scenario	Tasks to Perform
Common components installed before CIMPLICITY.	Perform install time registration (on page 10) during the CIMPLICITY installation. <div data-bbox="820 1291 1412 1606" style="border: 1px solid #00a0c0; border-radius: 10px; padding: 10px; margin-top: 10px;">  Note: If you skip providing Configuration Hub and Proficy Authentication details during the installation, then perform central registration (on page 86) after installing CIMPLICITY. </div>
Common components installed after CIMPLICITY installation.	Perform central registration (on page 86) after installing CIMPLICITY.

CIMPLICITY Upgrade from Version 2023 to 2024 or higher version



Important:

To upgrade your previous versions of CIMPLICITY, you must uninstall the previous version first and then install the latest CIMPLICITY, that is 2024 or later. If you have registered a CIMPLICITY plug-in in Configuration Hub, you must first unregister the plug-in and then uninstall the existing version of CIMPLICITY. For more information on how to unregister a plug-in from Configuration Hub, refer to the Unregister CIMPLICITY Plug-in from Configuration Hub section in the [CIMPLICITY 2023 online documentation](#).

Scenario	Tasks to Perform
Common components already upgraded to version 2024 or higher.	Perform install time registration (on page 10) during the CIMPLICITY upgrade, that is while installing CIMPLICITY 2024, after uninstalling the previous version of CIMPLICITY. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;">  <p>Note: If you skip providing Configuration Hub and Proficy Authentication details during the upgrade, then perform central registration (on page 86) method after the installing the latest CIMPLICITY.</p> </div>
Common components are installed later with version 2024 or higher.	Perform central registration (on page 86) after installing CIMPLICITY.
Common components installed but not upgraded to version 2024 or higher.	<div style="border: 1px solid #FFD700; border-radius: 10px; padding: 10px; margin-top: 10px;">  <p>Important: Upgrade common components to version 2024 or higher.</p> </div>

CIMPLICITY Unregistration

Scenario	Tasks to Perform
CIMPLICITY registered with version 2024 common components or higher.	Unregister CIMPLICITY centrally from Configuration Hub. Unregister CIMPLICITY plugin (on page 112) .

Scenario	Tasks to Perform
CIMPLICITY of version 2023 (registered conventionally) to common components of version 2024 or higher.	Unregister CIMPLICITY conventionally. Kindly refer to the CIMPLICITY Plug-in Registration with Configuration Hub section in the CIMPLICITY 2023 online documentation

Pre-2024 CIMPLICITY Registration

Scenario	Tasks to Perform
Older version of CIMPLICITY registration and unregistration with common components of version 2024 or higher.	Follow the conventional process for registration and unregistration. Kindly refer to the CIMPLICITY Plug-in Registration with Configuration Hub section in the CIMPLICITY 2023 online documentation .

Migration of Common Components (Version 2024 or later) Post-Registration

Scenario	Tasks to Perform
If you migrate to a new Proficy Authentication server.	<ol style="list-style-type: none"> 1. Unregister CIMPLICITY plugin (on page 112). 2. Unregister Configuration Hub with the old Proficy Authentication server and register with the new Proficy Authentication server. 3. Configure the CIMPLICITY node to use the new Proficy Authentication server (on page 87). 4. Register the CIMPLICITY plugin using the Configuration Hub Administration option (on page 89).

Scenario	Tasks to Perform
If you migrate to a new Configuration Hub server.	<ol style="list-style-type: none"> 1. Unregister CIMPLICITY plugin (on page 112) from the old Configuration Hub server. 2. Register the new Configuration Hub server with the existing Proficy Authentication server. 3. Register the CIMPLICITY plugin using the Configuration Hub Administration option (on page 89).
If you migrate both the new Configuration Hub server and the Proficy Authentication server.	<ol style="list-style-type: none"> 1. Unregister CIMPLICITY plugin (on page 112) from the old Configuration Hub server. 2. Register the new Configuration Hub server with the new Proficy Authentication server. 3. Configure the CIMPLICITY node to use the new Proficy Authentication server (on page 87). 4. Register the CIMPLICITY plugin using the new Configuration Hub Administration option (on page 89).

Central Registration of CIMPLICITY Plug-in with Configuration Hub

About Central Registration

Central registration method allows you to register your CIMPLICITY node as a plug-in with Configuration Hub after you have installed CIMPLICITY, Configuration Hub, and Proficy Authentication, either locally or remotely. This method is used to register your CIMPLICITY plug-in with Configuration Hub if you skipped registering the plug-in during the CIMPLICITY installation process.

What is a CIMPLICITY Plug-in?

A CIMPLICITY plug-in with Configuration Hub represents a CIMPLICITY server node. Using the CIMPLICITY plug-in, you can browse your CIMPLICITY project's OPC UA devices, and MQTT devices in Configuration Hub, which operates as a web-based application.

Supported Setup for CIMPLICITY Plug-in Registration

Components	Version
CIMPLICITY	2024
Configuration Hub	2024
Proficy Authentication	2024

**Note:**

If you are using previous version of Configuration Hub and Proficy Authentication, kindly upgrade to version 2024.

This setup can be on a same machine or can be installed on three different machines. However, both CIMPLICITY and Configuration Hub must connect to the same Proficy Authentication server.


What to do next:

Open the **Node Manager Configuration** utility on the machine where your CIMPLICITY node is located, and enter details of the Proficy Authentication server to which Configuration Hub is connected. This action will enable you to add your CIMPLICITY node in Configuration Hub, as both the CIMPLICITY node and Configuration Hub are configured to use the same Proficy Authentication server. For more information, refer to [Add CIMPLICITY node in Configuration Hub \(on page 87\)](#).

Configure the CIMPLICITY Node to use Proficy Authentication

Ensure that you have already installed [CIMPLICITY 2024 \(on page 10\)](#), [Configuration Hub 2024](#) and [Proficy Authentication 2024](#) or upgraded them to 2024.

This topic describes how to configure the CIMPLICITY node with the Proficy Authentication server used by Configuration Hub, with which you need to register the CIMPLICITY node. The following steps must be performed on the machine where the CIMPLICITY node is located.

1. From the desktop, open the **Node Manager Configuration**  utility as an administrator. The **Node Manager Configuration** utility appears.

Node Manager Configuration

Node manager details on this host


Host Name

Port

Note: Use these details to add plug-in through Configuration Hub

Proficy Authentication

Host Name

Port 

Client ID

Client Secret

Cancel

Node manager details on this host- This section displays the CIMPLICITY node's hostname and port number. Make a note of it as you will need these details while you add the node in Configuration Hub.

Proficy Authentication- This is the section where you must enter the details of the Proficy Authentication server that the CIMPLICITY node will use, as well as the one Configuration Hub is using. This will enable Configuration Hub to trust the CIMPLICITY node when you add it.

- In the **Proficy Authentication** section, enter the following details:

Field	Description
Host Name	The hostname of the Proficy Authentication server to which you want to connect the CIMPLICITY node.

Field	Description
Port	The port number of the Proficy Authentication server. By default, it is 443.
Client ID	The client ID of the Proficy Authentication server, provided during the Proficy Authentication server installation.
Client Secret	The client secret of the Proficy Authentication server, provided during the Proficy Authentication server installation.

If the root certificate of the Proficy Authentication server is not trusted, then click not trusted



, the **Certificate Details** page appears. Select **Trust** to trust the root certificate.

- After you enter the needed details, select **Configure**.

A success message appears stating that the Proficy Authentication was commissioned with Node Manager.

Add the CIMPLICITY node in Configuration Hub.

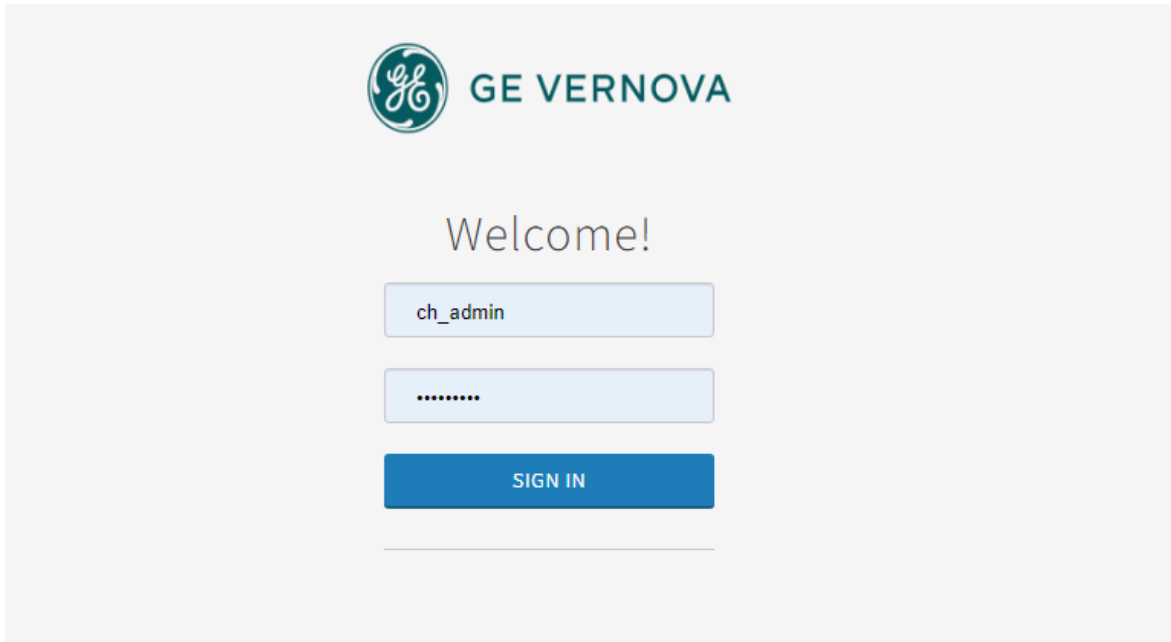
Add the CIMPLICITY Node and Register the Plug-in with Configuration Hub

Ensure that you have already [Configured the CIMPLICITY Node to use Proficy Authentication \(on page 87\)](#).

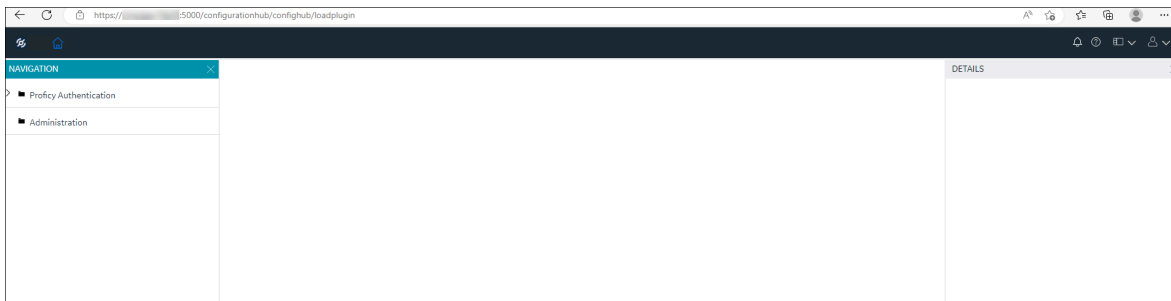
To use the CIMPLICITY plug-in in Configuration Hub, you must add the CIMPLICITY node in Configuration Hub.

To add the CIMPLICITY node in Configuration Hub, perform the following steps:

- In the machine that has Configuration Hub installed, in the desktop, double-click . The Proficy Authentication login page appears.

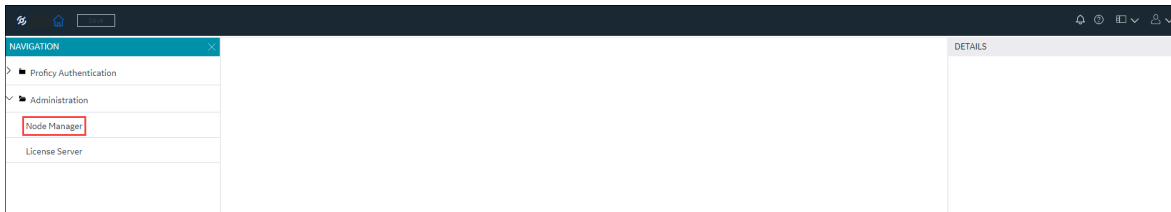


2. Log in using `ch_admin` as username and your Proficy Authentication secret as password. After a successful authentication, the Configuration Hub page appears.



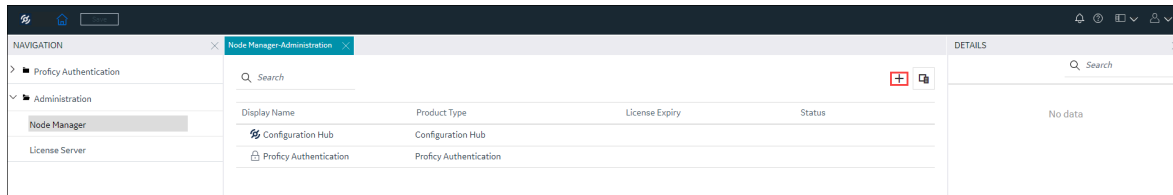
By default, in the **NAVIGATION** pane, the Proficy Authentication and Administration plug-in appear.

3. In the **NAVIGATION** pane, select **Administration**, and then expand it. **Node Manager** and **License Server** appear.



4. Select **Node Manager**.

The **Node Manager-Administration** panel appears, displaying the Configuration Hub and Proficy Authentication details.



5. Select



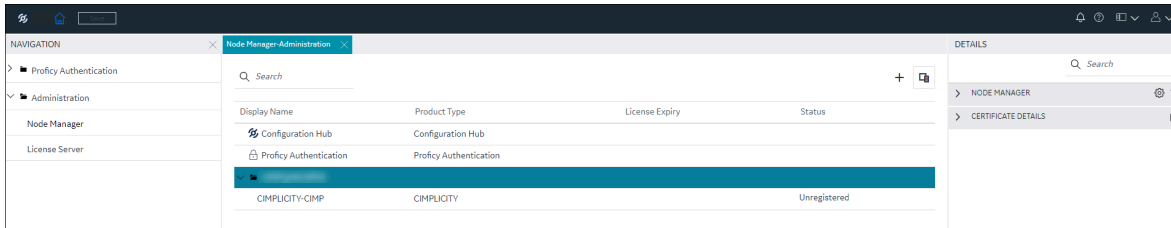
The **Add Node Manager** window appears.

6. Enter the **HOST NAME**. Here, it is the CIMPLICITY node. For example, testmachine123.
7. Enter the **DISPLAY NAME** for the CIMPLICITY node. By default, the hostname is added as the display name.
8. Enter the **PORT NUMBER** of the host that you entered.
9. You must trust the node manager certificate. To trust the certificate, select **Not Trusted**.
The **Certificate Details** window appears, listing the certificate information.
10. Read the certificate details and if you trust, select **Trust**.
In the **Add Node Manager** window, the certificate status changes to trusted.
11. Select **Test Connection**.

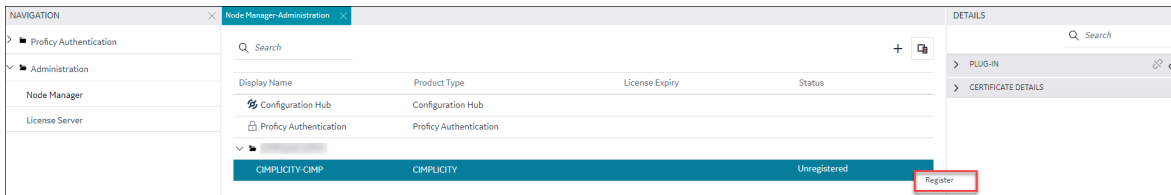
If the connection is successful, a success message appears. If not, check if the host name and the port are correct.

12. Select **Add**.

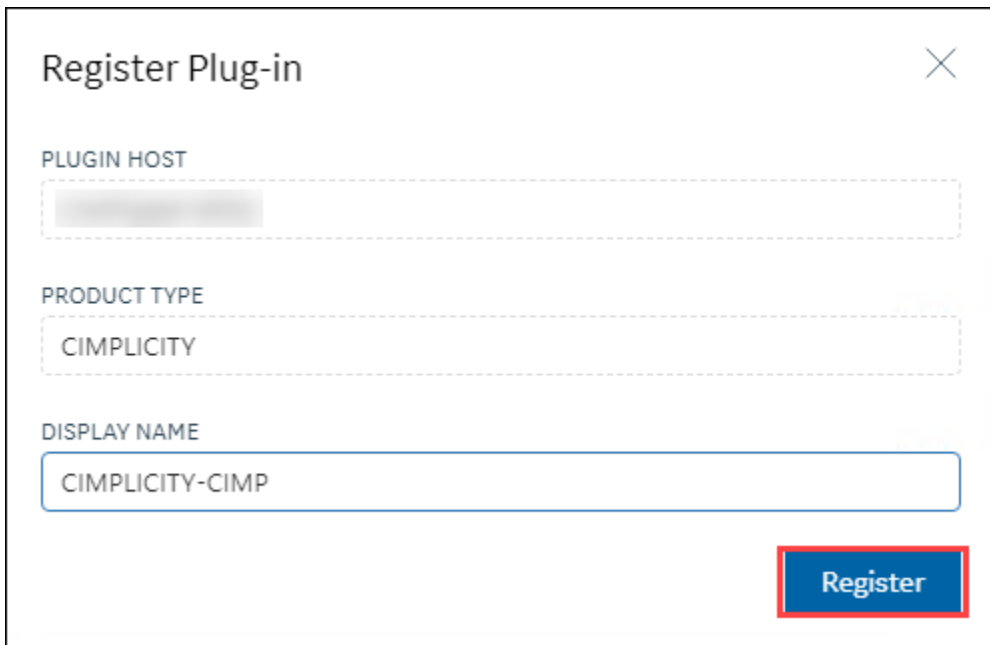
The CIMPLICITY node is added, along with the CIMPLICITY plug-in. However, the plug-in will be in an unregistered state because, it was just the CIMPLICITY node added in Configuration Hub, and the plug-in is yet to be registered with Configuration Hub.



13. Right-click the plug-in row, and then select **Register**.

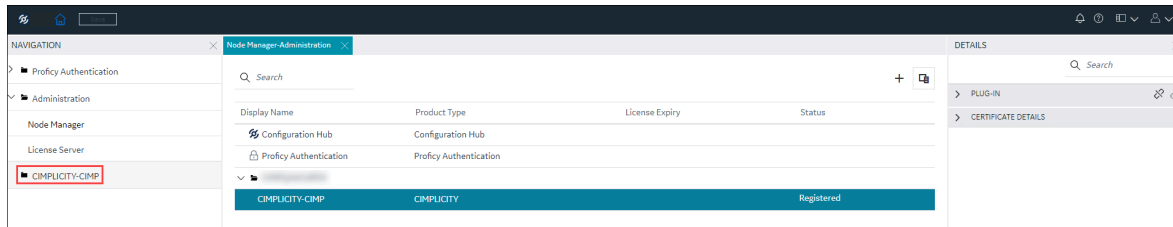



The **Register Plug-in** window appears, displaying the plug-in's host, product type, and display name.



14. If needed, modify the plug-in name, and then select **Register**.

The plug-in is registered with Configuration Hub, and displayed in the **NAVIGATION PANE**.



Alternatively, you can register a plug-in from the Plug-in **DETAILS** section by selecting  on the top-left corner in the **PLUG-IN** section.

-OR-

You can right-click the node, and then select **Manage Plug-ins**.


The **Manage Plug-ins** window appears, allowing you to select the plug-in in the node and register it.

- a. Select the plug-in as needed.
- b. Select **Register**.

The plug-in gets registered.

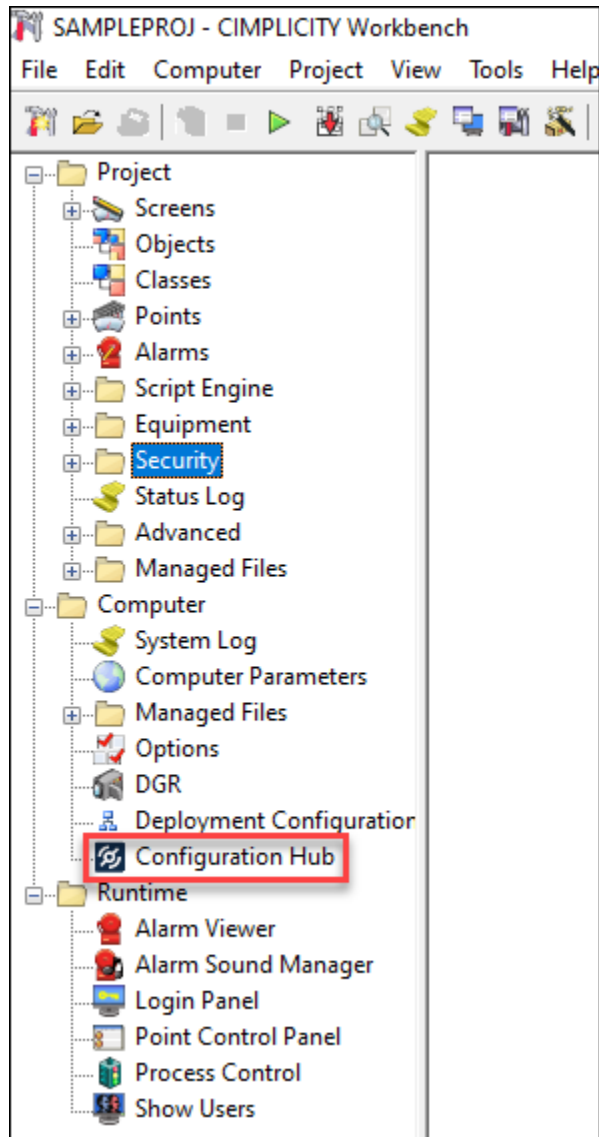
You can start to use the plug-in to browse your CIMPLICITY projects, start or stop the projects, browse devices like OPC UA, and MQTT, and create SCADA points. For more information, refer to [Overview of CIMPLICITY Plug-in within Configuration Hub \(on page 95\)](#).

Access Configuration Hub

After you register CIMPLICITY with Configuration Hub, you can access the Configuration Hub within CIMPLICITY Workbench, or from the desktop of the Configuration Hub machine, using the Configuration Hub shortcut .

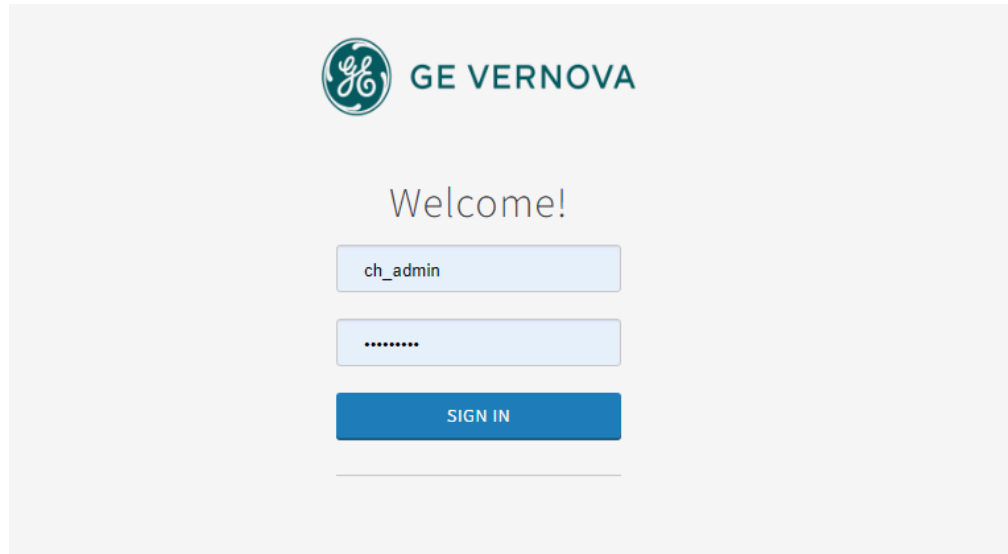
To access Configuration Hub from CIMPLICITY, do the following:

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 appears.



4. Log in using `ch_admin` as username and your Proficy Authentication secret as password.
After a successful authentication, the Configuration Hub page appears.

You can start to use the plug-in to browse your CIMPLICITY projects, start or stop the projects, browse devices like OPC UA, and MQTT, and create SCADA points. For more information, refer to [Overview of CIMPLICITY Plug-in within Configuration Hub \(on page 95\)](#).

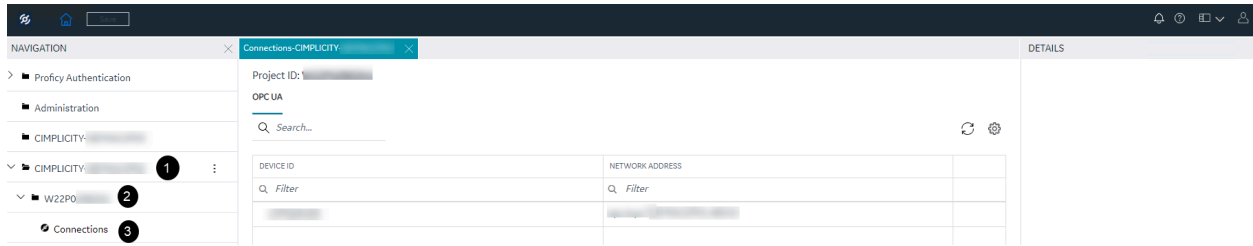
Overview of CIMPLICITY Plug-in within Configuration Hub


After registering CIMPLICITY plug-in with Configuration Hub, if you log in to Configuration Hub, either using the desktop shortcut on the Configuration Hub machine desktop, or from the CIMPLICITY Workbench, the CIMPLICITY plug-in will appear in the Navigation pane, along with its associated projects on the left-side panel as shown below.



Note:

To access the plug-in, you must have the **SCADA.COMPUTER@[NodeName].\$CONFIGSECGRP** scope published to Proficy Authentication. By default, all the needed scopes are added to the `ch_admin` user.



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. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note: Connections is displayed only if a Project is configured with devices. You can click Connections to browse (on page 99) devices and create (on page 106) points.</p> </div>

Managing CIMPLICITY Plug-in in Configuration Hub

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.

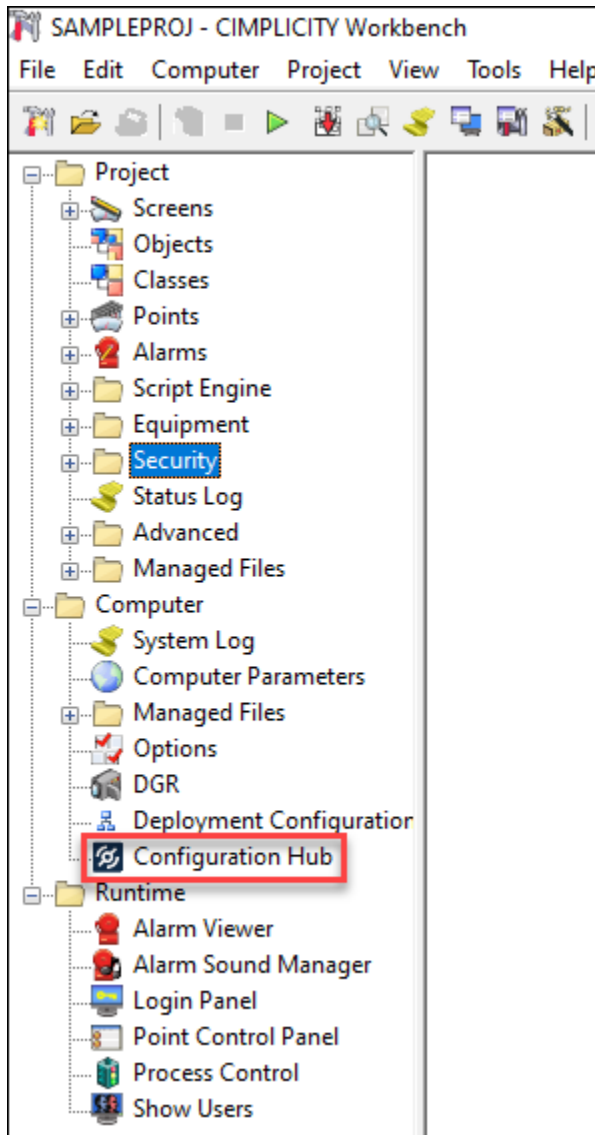


Note:

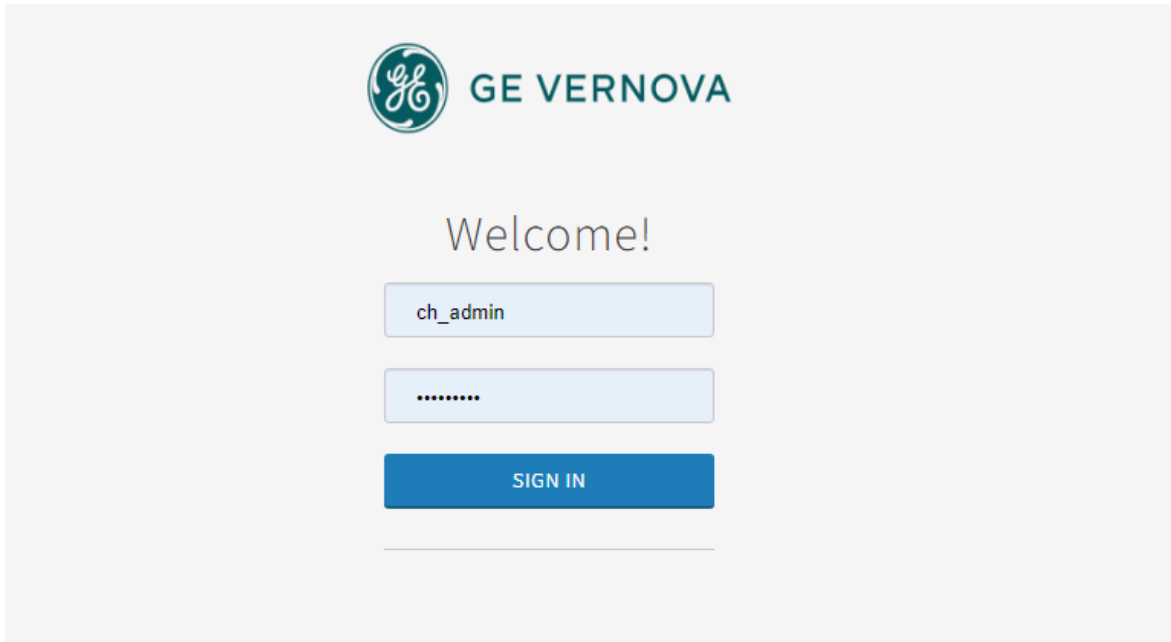
If you have set the CIM_SSL_STRICTPOLICY (on page) parameter to **Y** (recommended), it is important that the primary server trusts the secondary server's SSL certificate, and vice versa. For more information on SSL certificate exchange, refer to [SSL Certificate Exchange between the Primary Server and the Secondary Server \(on page \)](#).

To start a project, perform the following:

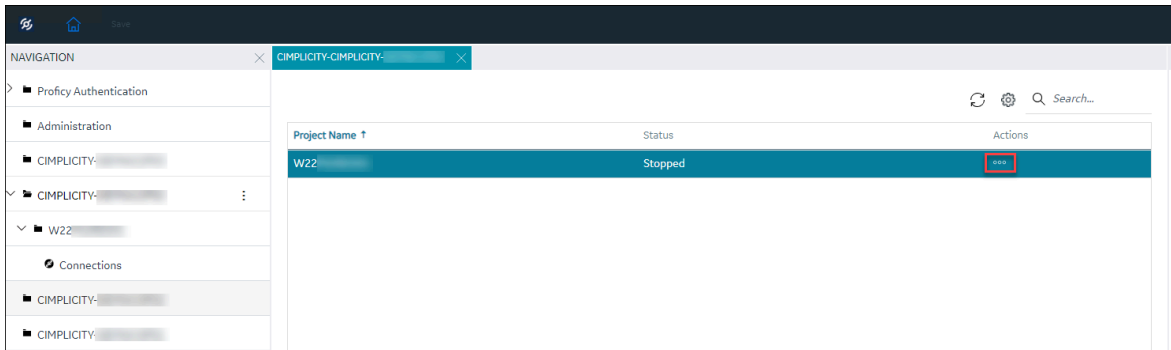
1. In the machine that has Configuration Hub installed, in the desktop, double-click . Alternatively, in the CIMPLICITY node machine, you can open Configuration Hub from the Workbench.



The Proficy Authentication login page appears.



2. In the **NAVIGATION** pane, select and expand the required node.
All the associate plug-in and its projects are listed.



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.

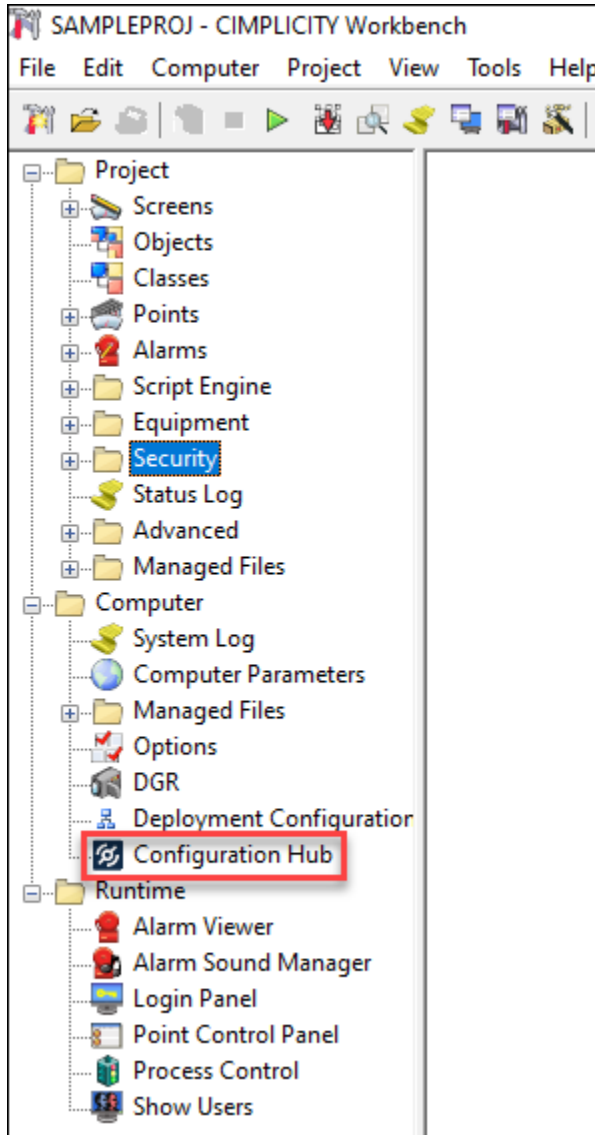
Option	Description
Start Primary and Secondary	Select this to start a stopped project in both primary and secondary servers.
Start Primary	Select this to start a stopped project in primary server only.
Start Secondary	Select this to start a stopped project in secondary server only.
Stop Primary and Secondary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

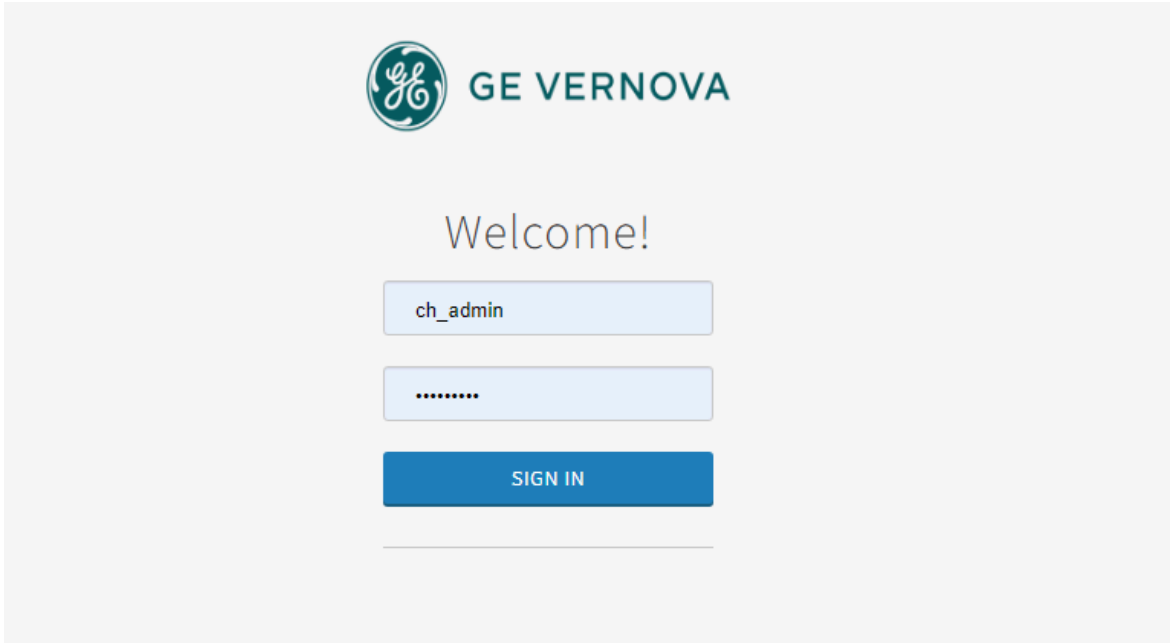
Select and Browse Devices

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

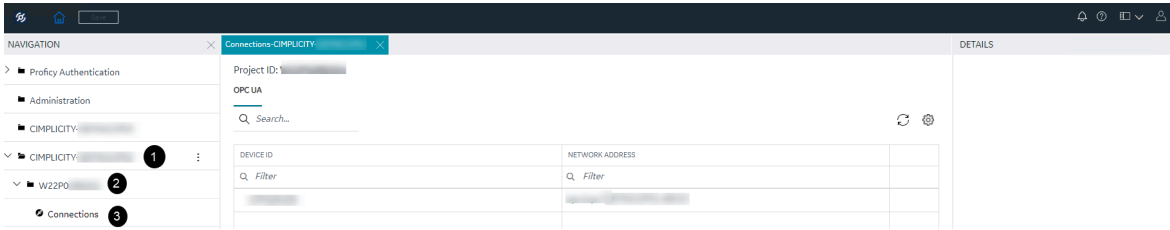
1. In the machine that has Configuration Hub installed, in the desktop, double-click . Alternatively, in the CIMPLICITY node machine, you can open Configuration Hub from the Workbench.



The Proficy Authentication login page appears.

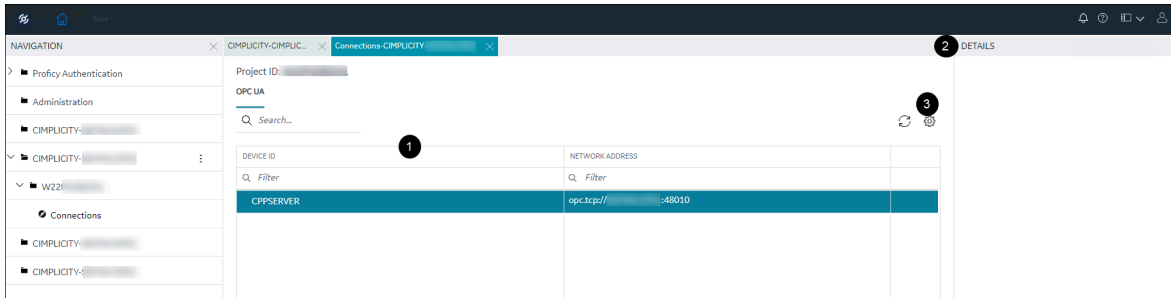



The Configuration Hub page appears, listing all the CIMPLICITY nodes and their associated plug-ins in the **NAVIGATION** pane.



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 Connections to browse all the available devices and create points.

- From the left pane, expand the required project and select **Connections**. The devices tab appears, listing all the associated devices.

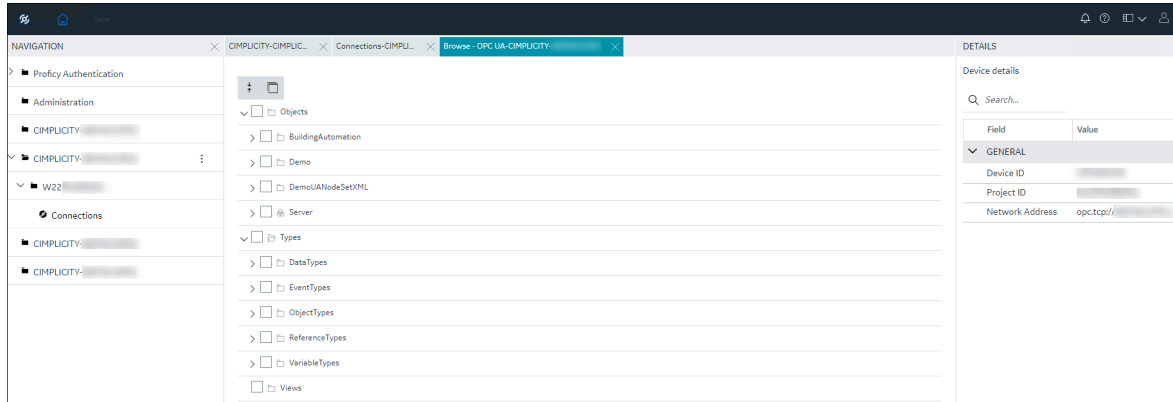


Marker	Description
1	List of all the OPC UA devices associated to the project.
2	<p>Details of the selected device.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;">  Note: This is read-only. </div> <p>In case of a redundancy project, you can see the details like node name, status, and path of the configured primary and secondary servers. For more information on configuring redundancy, refer to <i>Configuring Redundancy (on page)</i>.</p>
3	<p>Column chooser. You can select what all information of a device you want to view in the grid.</p> <p>Available options:</p> <ul style="list-style-type: none"> ◦ 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 appears, 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.



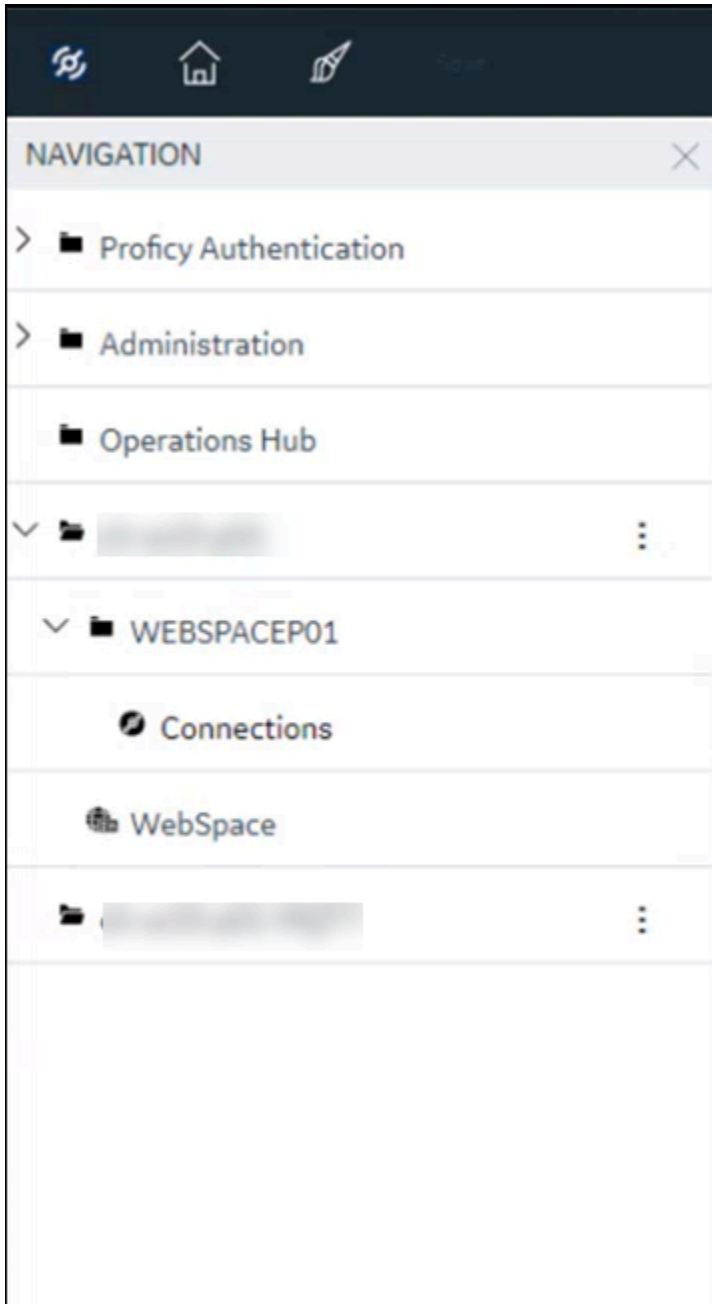
You can now create SCADA points from the objects displayed for the selected device.

Select and Browse Tags from an MQTT Device

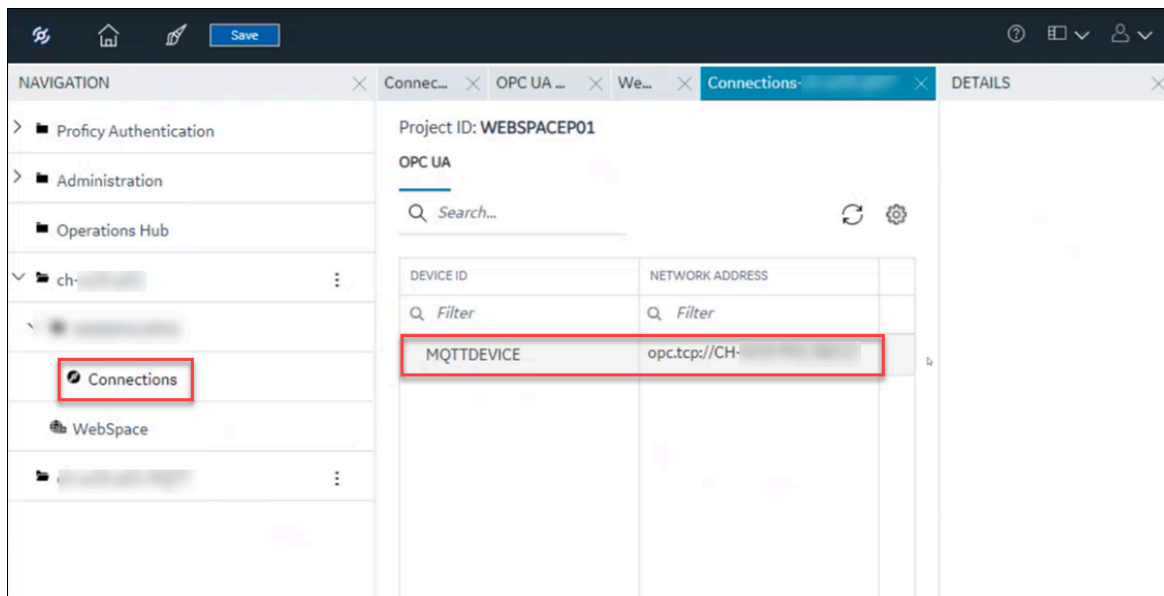
You can log in to Configuration Hub and browse through all the configured MQTT Devices and read the values. To browse an MQTT device using the CIMPLICITY plug-in, you must do the following configurations:

- 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 \(on page 93\)](#). The Configuration Hub page appears, listing all the CIMPLICITY nodes and their associated plug-ins in the **NAVIGATION** pane.



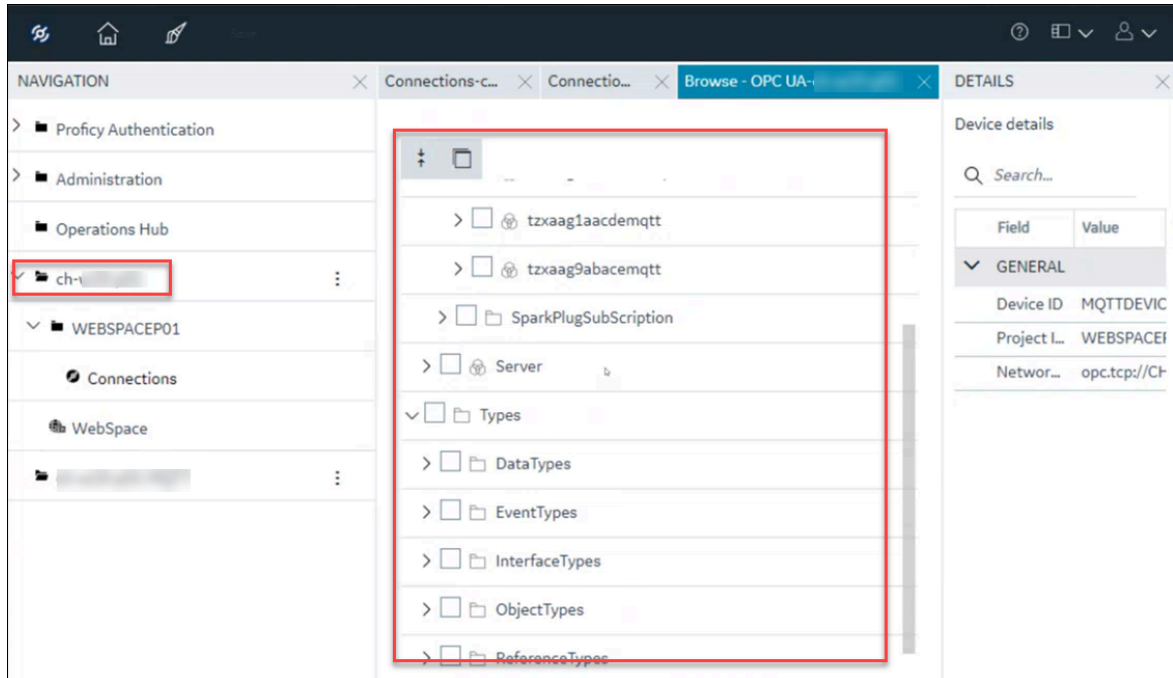
2. From the left pane, expand the required project and select **Connections**.
The devices tab appears, listing all the associated devices.



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 appears, 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 view the tags and their details from the MQTT device.

Create SCADA Points

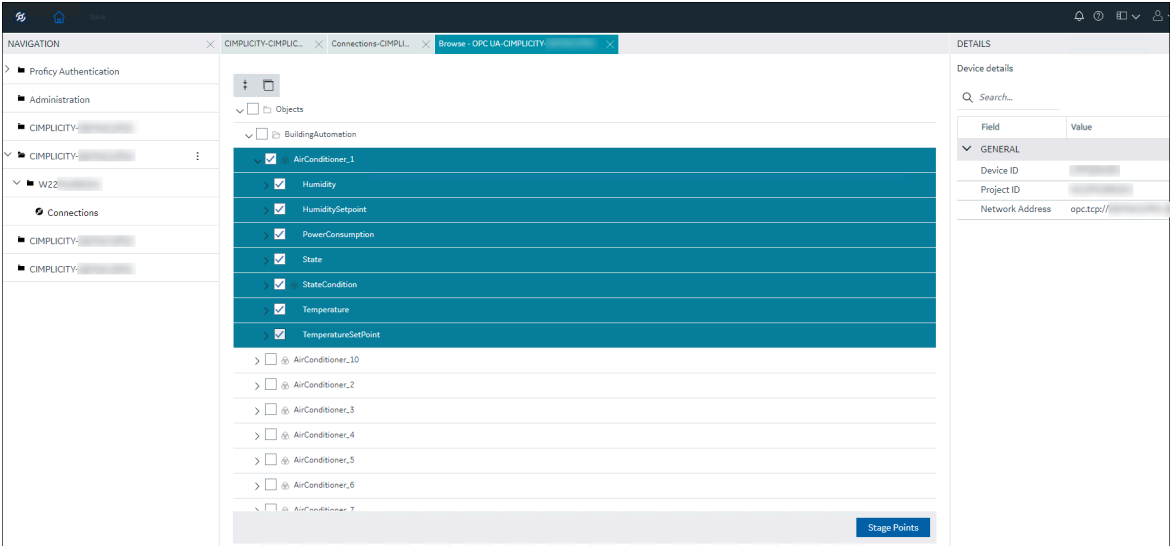
Create SCADA points from the objects. Ensure that you browsed a device to proceed with point creation.

To create points, perform the following:

1. Select the objects.

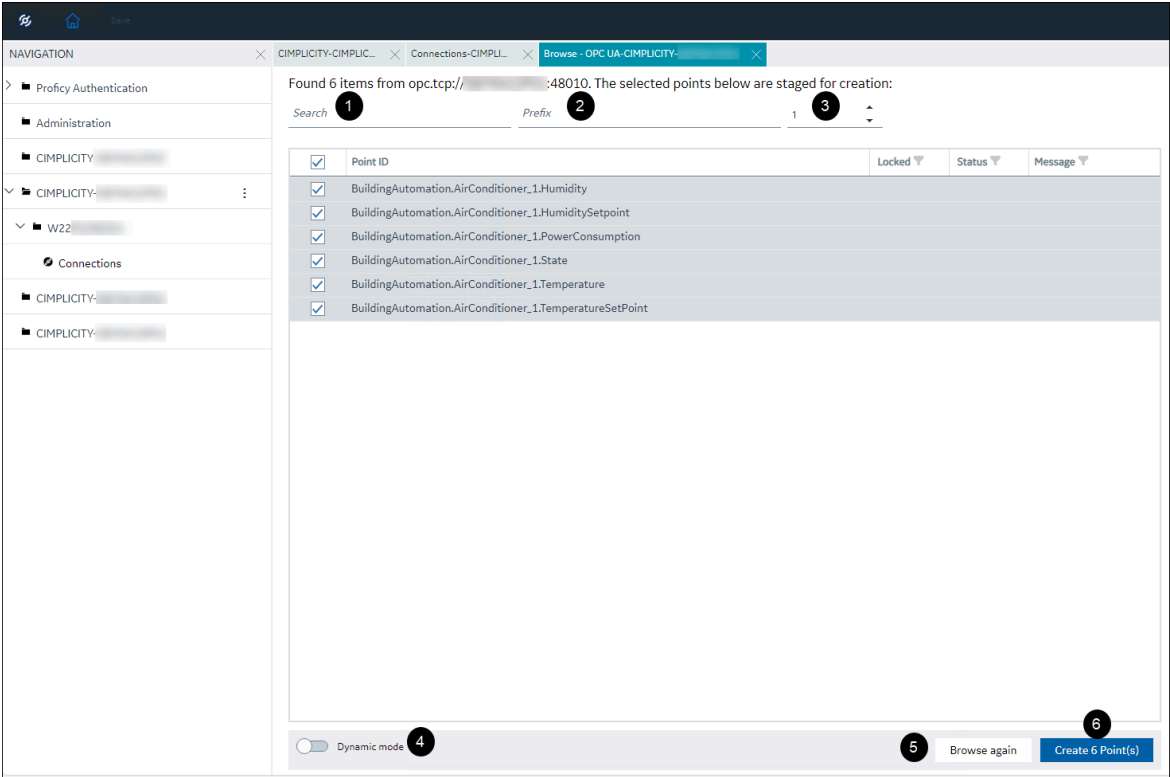
You can either right-click the node, and then select **Select all children**, or to select the children of a node, you can double-click the node.



Once you select objects, the **Stage Points** button is enabled.



2. Select **Stage Points**.

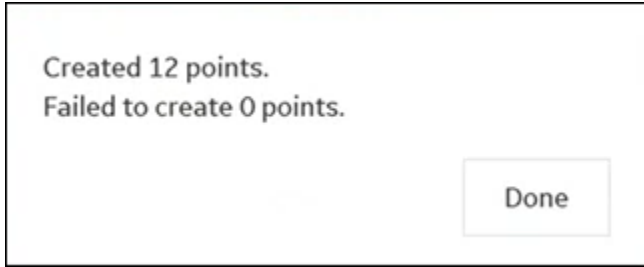
All the selected points are staged and listed.



Marker	Description
1	Enter text to display point IDs that contain the entered text.
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 removed from the beginning of the point IDs. For example, if you do not want AirConditioner_1 in the namespace, you must select 2.
4	<p>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</p> <div data-bbox="862 936 1419 1297" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> 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.</p> </div>
5	<p>Select this to browse the devices and objects again.</p> <div data-bbox="862 1430 1419 1608" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: This will be enabled only after you create points for the selected objects.</p> </div>
6	Select this to create points.

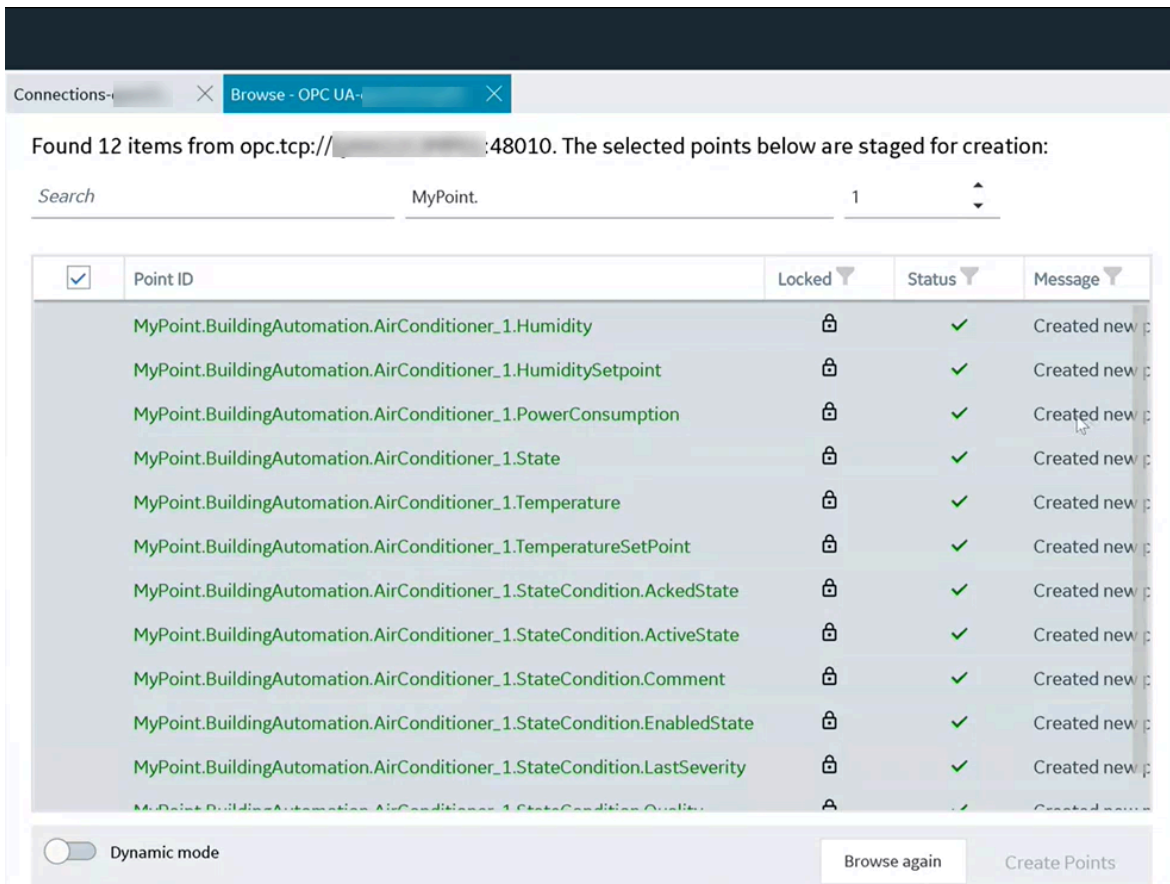
3. Select **Create** (number of points selected) **Points**.

The points are created, and the results are displayed.



4. Select **Done**.


All the created points and their status are listed.

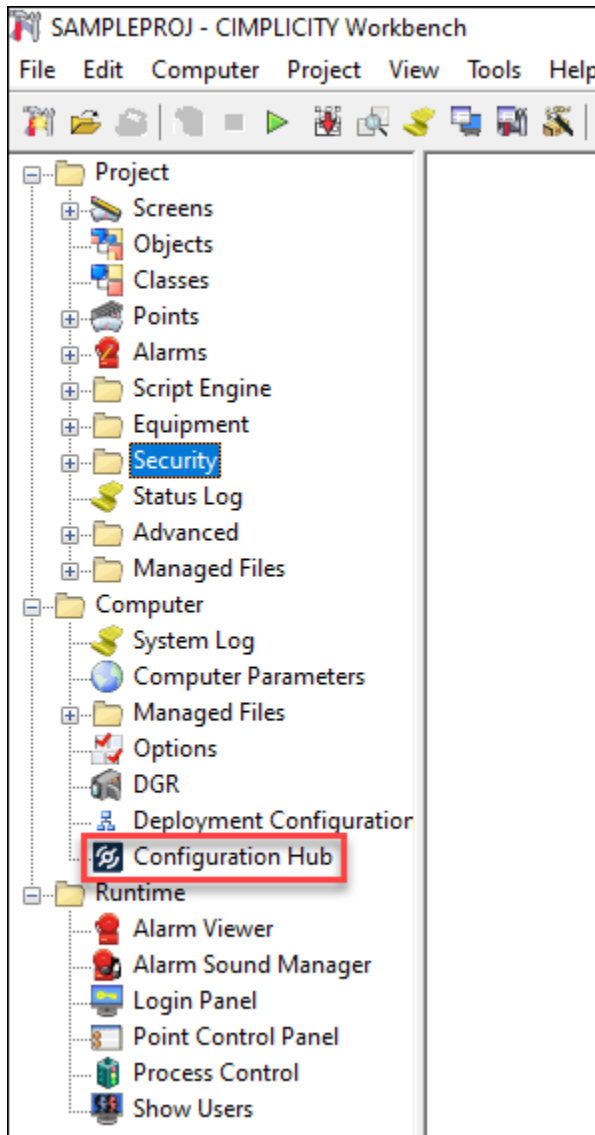


Update or Modify CIMPLICITY Node or Plug-in

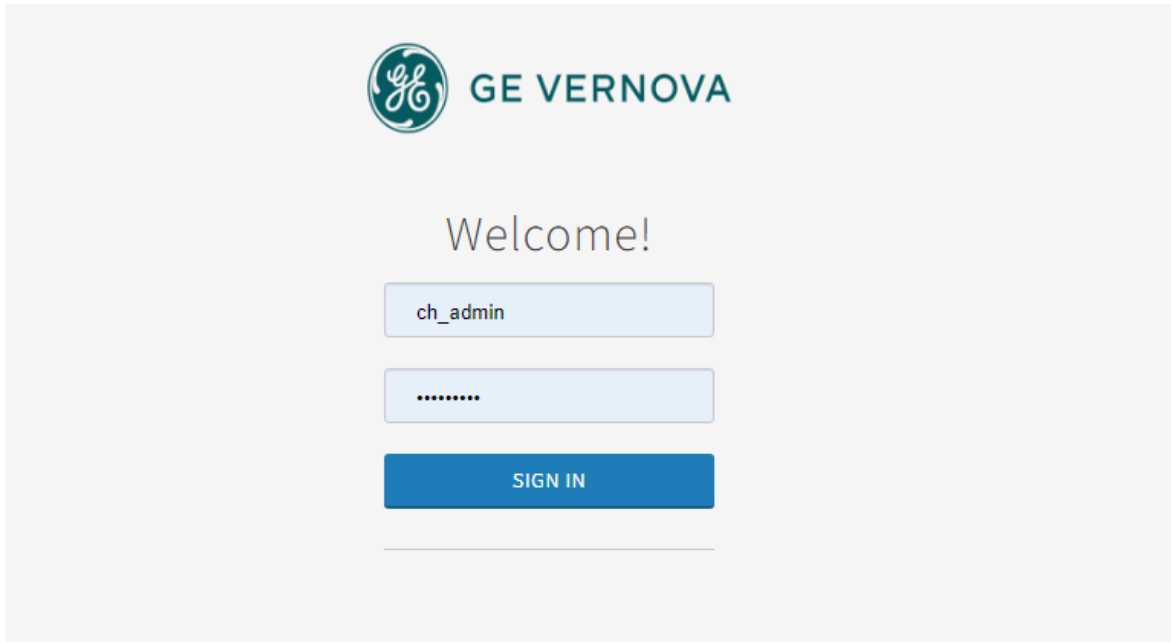
If you want to modify the alias name for the CIMPLICITY plug-in or the node that is registered with Configuration Hub, you can do that using the node manager in Configuration Hub.

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

1. In the machine that has Configuration Hub installed, in the desktop, double-click . Alternatively, in the CIMPLICITY node machine, you can open Configuration Hub from the Workbench.



The Proficy Authentication login page appears.



2. Log in using `ch_admin` as username and your Proficy Authentication secret as password. After a successful authentication, the Configuration Hub page appears.

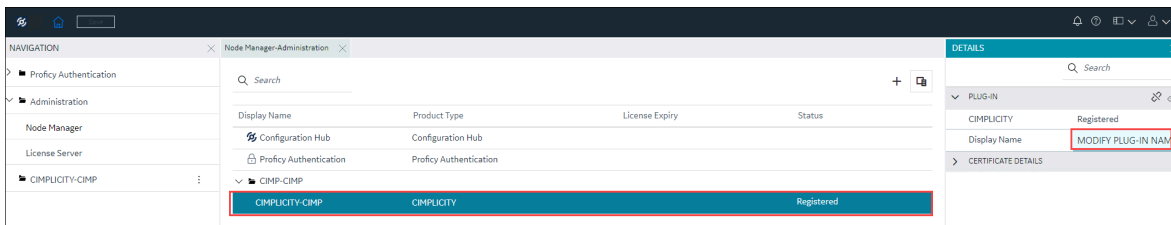
By default, in the **NAVIGATION** pane, the Proficy Authentication and Administration plug-in appear.

3. In the **NAVIGATION** pane, select **Administration**, and then expand it. **Node Manager** and **License Server** appear.

4. Select **Node Manager**.

The **Node Manager-Administration** panel appears.

5. To modify a plug-in display name, expand the node, and then select the plug-in.



6. In the right-side pane, in the **PLUG-IN** details, you can enter a new display name for the plug-in. The display name of the plug-in gets updated.

Alternatively, you can right-click the node, and then select **Manage Plug-ins**.

The **Manage Plug-ins** window appears, allowing you to select the plug-in in the node and modify the plug-in's display name.

- a. Select the plug-in as needed.
- b. In the **Plugin Display Name** column, modify the name of the plug-in.
- c. Select **Update**.


The plug-in name gets modified.

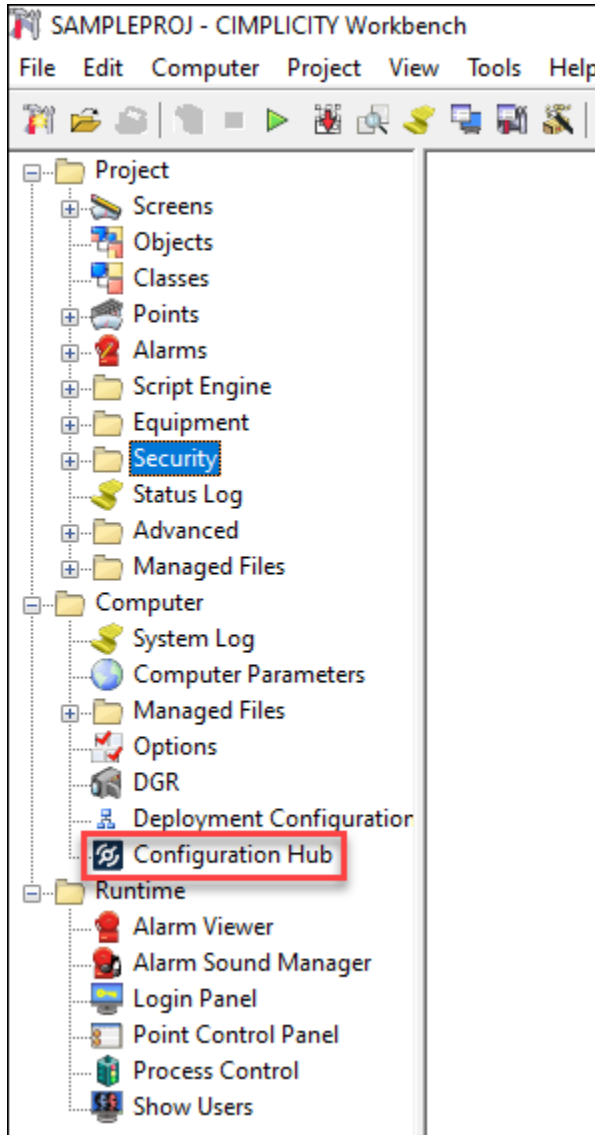
7. To modify a node's display name, select the node.
8. In the right-side pane, in the **NODE MANAGER** details, you can enter a new display name for the node.
The display name of the node gets updated.

Unregister CIMPLICITY Plug-in from Configuration Hub

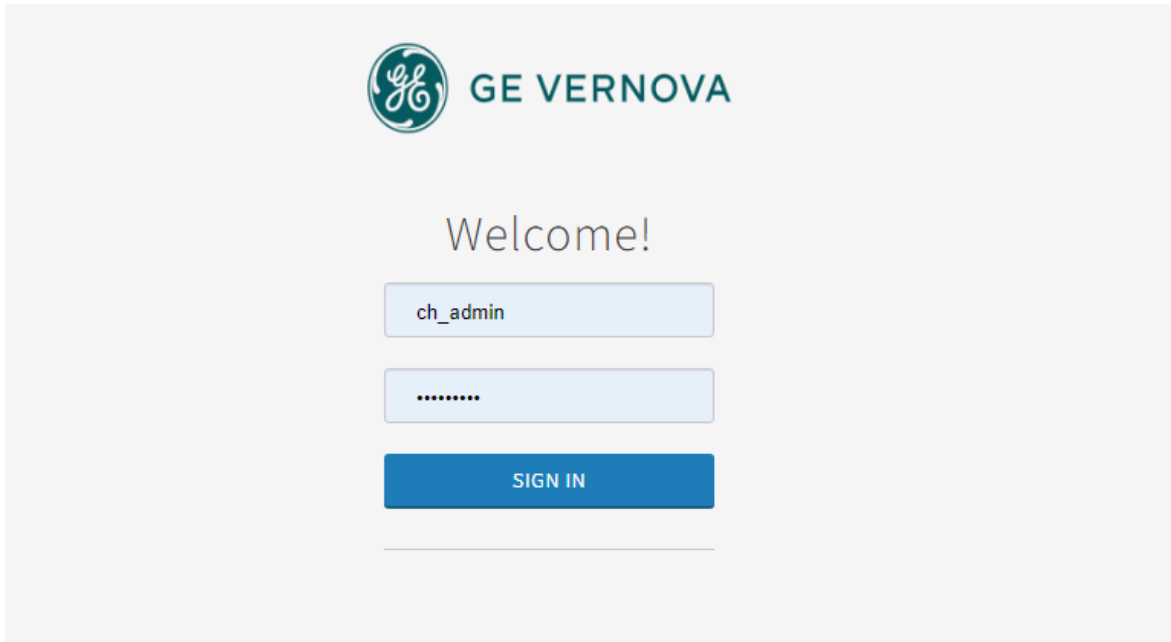
If you do not need a CIMPLICITY plug-in in Configuration Hub, you can unregister the plug-in completely from Configuration Hub. Once you unregister the plug-in, that plug-in's node is completely removed along with all the associated projects.

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

1. In the machine that has Configuration Hub installed, in the desktop, double-click .
Alternatively, in the CIMPLICITY node machine, you can open Configuration Hub from the Workbench.



The Proficy Authentication login page appears.



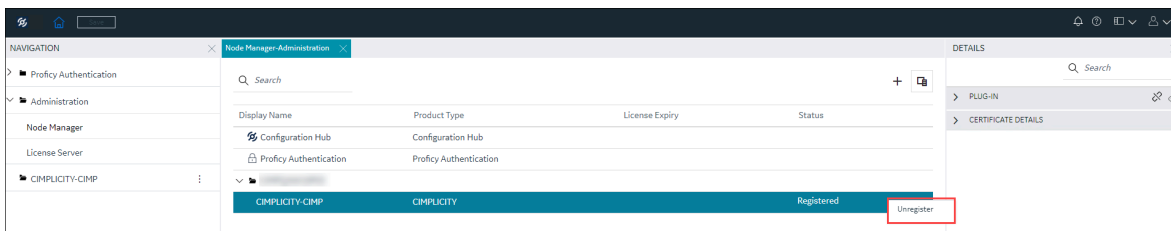
2. Log in using `ch_admin` as username and your Proficy Authentication secret as password. After a successful authentication, the Configuration Hub page appears.

By default, in the **NAVIGATION** pane, the Proficy Authentication and Administration plug-in appear.

3. In the **NAVIGATION** pane, select **Administration**, and then expand it. **Node Manager** and **License Server** appear.

4. Select **Node Manager**.

The **Node Manager-Administration** panel appears.



5. Expand the CIMPLICITY node, and right-click the plug-in, and then select **Unregister**.

The **Unregister Plug-in** confirmation window appears, prompting you to confirm whether to continue with the unregistration.


**Note:**

If you unregister the plug-in, it will be removed from the **NAVIGATION** pane, and any open or unsaved changes that belong to this plug-in will be discarded. However, the plug-in will remain intact but, in an unregistered state.

6. Select **Continue**.

The Plug-in is unregistered, and removed from the **NAVIGATION** pane.

If you need to register the same plug-in again, you can right-click the plug-in and select **Register**, and then provide the needed details.

Alternatively, you can unregister a plug-in from the Plugin **DETAILS** section by selecting  on the top-right corner in the **PLUG-IN** section.

-OR-

You can right-click the node, and then select **Manage Plug-ins**.

The **Manage Plug-ins** window appears, allowing you to select the plug-in in the node and unregister it.

- a. Select the plug-in(s) as needed.
- b. Select **Unregister**.

The plug-in(s) get unregistered.

Delete CIMPLICITY Node

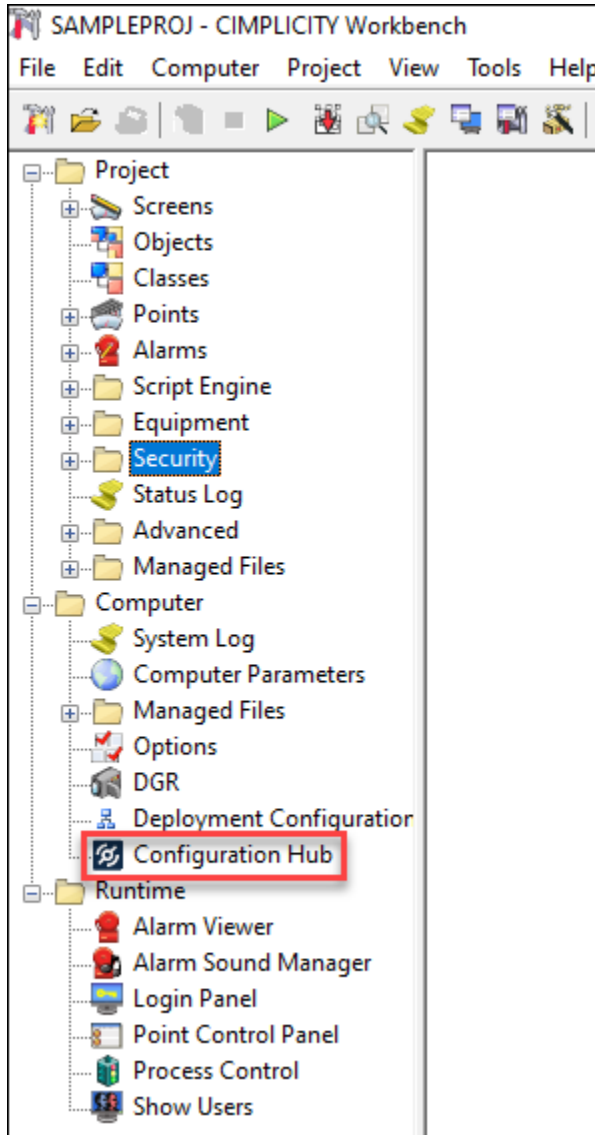
If you want to delete a CIMPLICITY node from Configuration Hub, you can delete it using **Node Manager-Administration**.

**CAUTION:**

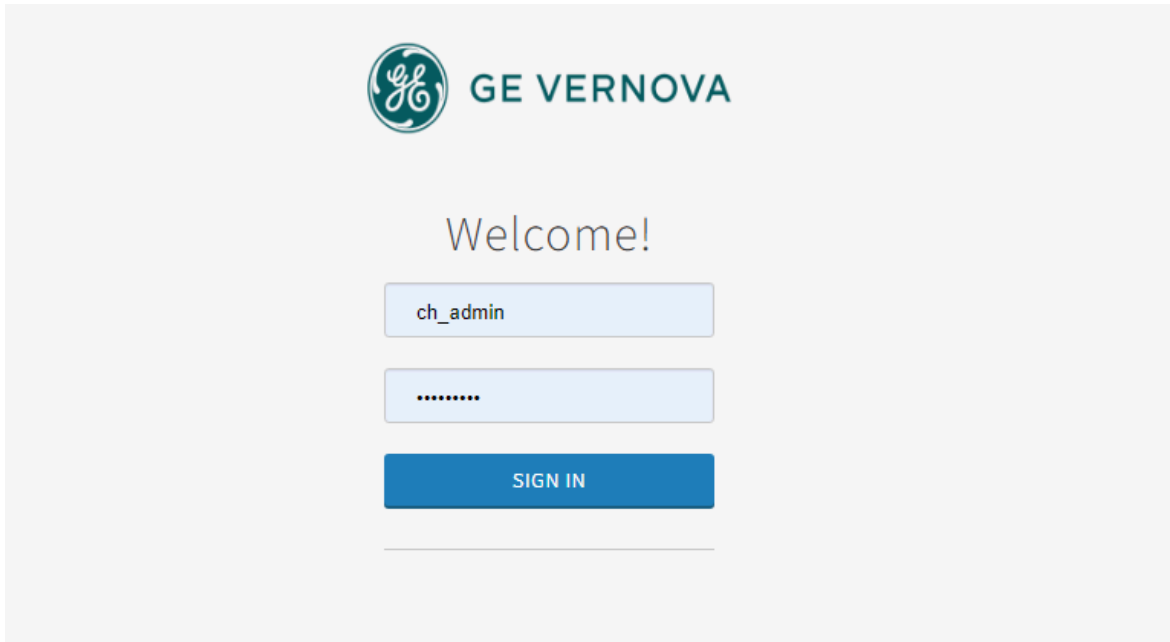
Be mindful before you delete a node, as it will completely remove the node, any plug-in in that node, and any open or unsaved changes that belong to that plug-in.

1. In the machine that has Configuration Hub installed, in the desktop, double-click .

Alternatively, in the CIMPLICITY node machine, you can open Configuration Hub from the Workbench.



The Proficy Authentication login page appears.

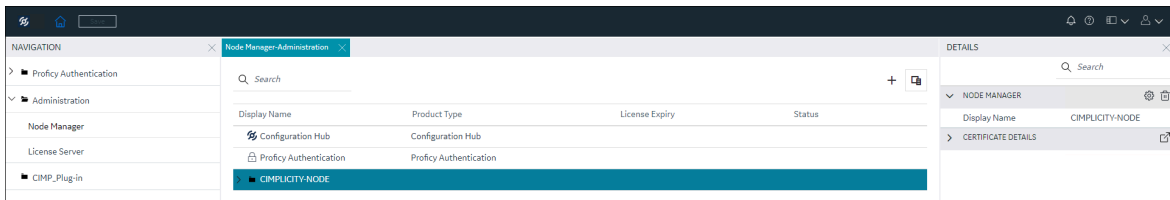


2. Log in using `ch_admin` as username and your Proficy Authentication secret as password. After a successful authentication, the Configuration Hub page appears.

By default, in the **NAVIGATION** pane, the Proficy Authentication and Administration plug-in appear.

3. In the **NAVIGATION** pane, select **Administration**, and then expand it. **Node Manager** and **License Server** appear.
4. Select **Node Manager**.

The **Node Manager-Administration** panel appears.



5. Right-click the CIMPLICITY node you want to delete, and then select **Delete**.

Alternatively, in **NODE MANAGER** details section, select .

The **Delete Node Manager** confirmation window appears, prompting you to confirm whether to continue with the delete. **Continue**.

Additionally, if you need to retain the CIMPLICITY plug-in as registered, you can leave the **Unregister all plug-ins on the selected node from Configuration Hub** check box cleared. So, when you add the node again in Configuration Hub, the plug-in also gets added, but it will remain registered, and you do not have to register it again with Configuration Hub.

6. Select **Continue**.

The Node Manager removes the CIMPLICITY node from the **NAVIGATION** panel. You will need to add the Node Manager again to use the CIMPLICITY node and the plugin.

Chapter 9. MQTT Client

Introduction

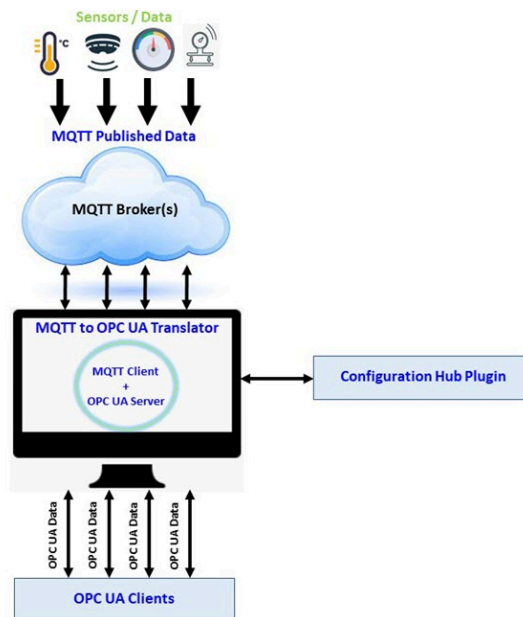
This document describes the importance of the MQTT Client application and its purpose in the GE Vernova Proficy product suite. The MQTT Client application can be installed along with the SCADA products using the CIMPLICITY Proficy installer.

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 Vernova 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.



Prerequisites

Ensure that you have already installed [CIMPLICITY 2024 \(on page 10\)](#), [Configuration Hub 2024](#) and [Proficy Authentication 2024](#) or upgraded them to 2024.

What to do next:

1. Install MQTT client. You can install the MQTT Client using the CIMPLICITY Proficy Installer. For more information on installing MQTT client, refer to https://www.ge.com/digital/documentation/mqtt/version2024/t_mqtt_install_time_registration.html.
2. To access MQTT devices in Configuration Hub using the CIMPLICITY plug-in, you must register the MQTT client with the Proficy Authentication and Configuration Hub server with which your CIMPLICITY plug-in is registered. For more information on registering MQTT client with Proficy Authentication and Configuration Hub, refer to https://www.ge.com/digital/documentation/mqtt/version2024/c_mqtt_overview_central_registration_and_install_time_registration.html.
3. Configure the MQTT client in Configuration Hub. For more information, refer to https://www.ge.com/digital/documentation/confighub/version2024/mqtt/g_mqtt_guide_mqtt_in_configuration_hub_mqtt_client_configuration.html.

For other management processes like changing admin credentials, port changes, and configuring OPC UA settings, refer to the MQTT Client documentation in the Configuration Hub documentation at <https://www.ge.com/digital/documentation/confighub/>.

Chapter 10. Licensing

Licensing

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 Vernova 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 Vernova support center web site at <https://digitalsupport.ge.com> to obtain information about the latest GE Vernova product offerings.

Table 1. 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

Central License Management in Configuration Hub

You can now centrally manage Proficy product from Configuration Hub. You can perform actions related to product license management such as viewing licenses, activating licenses, and returning licenses, and also manage product license expiration from the Node Manager in the Administration panel. And from the License Server-Administration panel, you can perform actions such as adding a new Local License Server, adding activation codes of the Proficy product(s) to the Local License Server, removing activation codes, reserving licenses, cleaning licenses, generate offline activation requests, generate response file, update licenses from response file, and other actions.

For more information, refer to [Central License Management](#).

Chapter 11. About Term Licensing in CIMPLICITY

About Term Licensing

In addition to the existing perpetual licensing model, CIMPLICITY 2024 supports Term licensing model.

What is a term licensing model in the context of CIMPLICITY?

As a CIMPLICITY user, you get the option to use the product on a subscription period, such as 3 years, or 5 years. After the subscription period, you have the option to renew your subscription and continue to use the product. Each term license contains a set of limited number of device tags (I/O) you can use as part of the license.

How am I benefited with term licensing?

- You have the flexibility to use or evaluate the complete product and all its features for a defined time and continue to renew the license as needed.
- You can run multiple projects with limited device tags (I/O).
- Unlike a trial or demo product, you still get the latest updates and support on the product throughout your license period.

Where can I see the license-specific information?

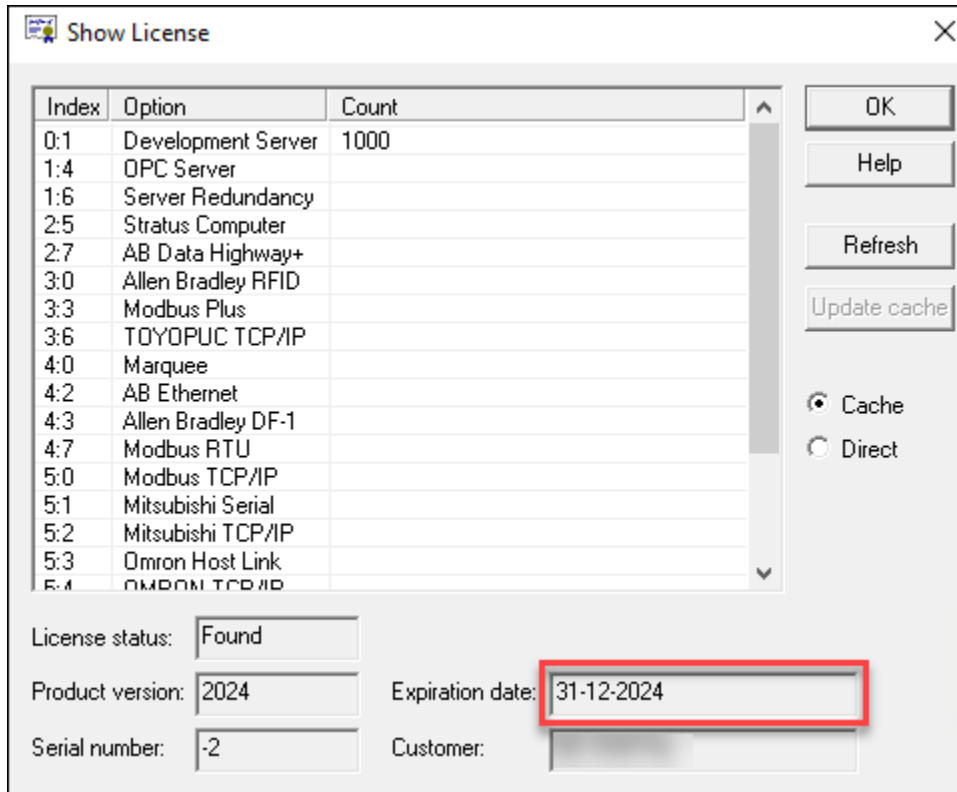
Once you activate your license and start to use the product, the necessary checks are periodically performed by the application in the background. When the product license nears the expiry date, a relevant information is logged in the CIMPLICITY system log (cor_log) only once, in the following sequence:

- 90 days before expiry.
- 60 days before expiry.
- 30 days before expiry.
- 15 days before expiry.
- On all the 7 days before expiry.

Date/Time	Status	Process	Procedure	Source	Code	Reference	Message
6/25/2024 12:59:55 AM	Warning	W32RTR	rtr_sub_lic_c...	COR_IPC_ERR	136	2725	License not found or expired, system will shutdown in 30 minutes.
6/24/2024 12:27:13 AM	Failure	CimProxy	cor_check_li...	COR_LIB_ERR	0	0	CIMPLICITY License will expire in 0 day(s). Please contact your GE Vernov...
6/23/2024 12:04:28 AM	Failure	CimProxy	cor_check_li...	COR_LIB_ERR	0	0	CIMPLICITY License will expire in 1 day(s). Please contact your GE Vernov...
6/22/2024 11:58:21 PM	Success	W32RTR	RtrStart	COR_IPC_ERR	0	0	CIMPLICITY Router V12.10.54247 (ENU) starting on QAW22IFIX01
6/22/2024 12:06:45 AM	Failure	CimProxy	cor_check_li...	COR_LIB_ERR	0	0	CIMPLICITY License will expire in 2 day(s). Please contact your GE Vernov...
6/21/2024 12:19:58 AM	Failure	CimProxy	cor_check_li...	COR_LIB_ERR	0	0	CIMPLICITY License will expire in 3 day(s). Please contact your GE Vernov...

Alternatively, you can search for **showlicense** in the Windows search, and check your license-specific information on the **Show License** utility, or if you have your license client installed, you can check your license-specific information on the license client, or if you have registered your CIMPLICITY node and plug-in with Configuration Hub, you can view the license-specific information in Configuration Hub's Administration plug-in > [License Server-Administration](#).

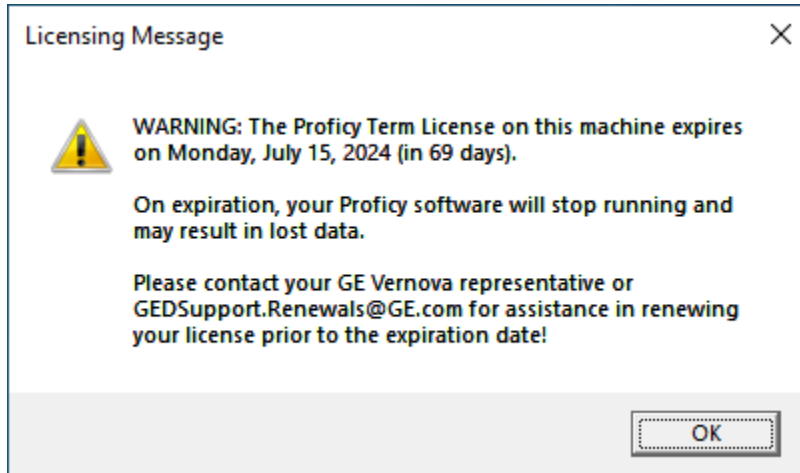
License Details on the Show License Utility



License Details on the License Client

You can see the license-specific information on the License Client UI.

Also, whenever you log in to your system, a licensing notification dialog will be displayed, notifying you about the license expiry date.



License Information on Configuration Hub

Activation Code	Description	Total	In Use	Available	Expiration
[Redacted]	Cimplicity v202...	5	0	5	No Expiration ...
[Redacted]	Cimplicity v202...	5	0	5	2024-03-07 23...
[Redacted]	Cimplicity v202...	5	1	4	No Expiration ...
[Redacted]	Cimplicity v202...	5	0	5	2024-03-18 23...
[Redacted]	SCADA Cimplic...	5	3	2	2092-12-31 23...
[Redacted]	SCADA Cimplic...	5	5	0	2092-12-31 23...
[Redacted]	Cimplicity v202...	5	0	5	No Expiration ...
[Redacted]	Cimplicity v202...	5	0	5	2092-12-31 23...
[Redacted]	Cimplicity v202...	5	0	5	No Expiration ...
[Redacted]	Cimplicity v202...	5	2	3	2092-12-31 23...

What happens if I dynamically renew my license (runtime)?

The license check is performed by the application in the background, and updates the license cache with the new license information. You will still be able to access your project without any downtime.

What happens if I forget to renew the license before it expires?

It is most unlikely that you would forget to renew the license as you can always check the expiry date and other license-specific information on different places like CIMPLICITY system log, or license client, or Configuration Hub's Node Manager. Despite that, if you forget to renew the license before it expires, the project will shutdown; however, you will be given 10 minutes before a project shuts down. Only after you renew the license, you will gain the access to the project back.



Important:

Please be mindful of the expiry date and renew the licenses on a timely manner.

What should I do to renew my license?

You can reach out to the GE Vernova's representative who enabled you with the license, or send an email to GEDSupport.Renewals@ge.com, or reach out to the support team at <https://digitalsupport.ge.com/>.

Best Practices

To effectively utilize term licensing, follow the below best practices:

- **Understand your requirements well:** Before subscribing or procuring the term licenses, understand your licensing requirements well. This will help you to procure what you need.
- **Check your license information frequently:** Unlike a perpetual license, term license has a validity, after which you will not be able to use the product till you renew your license. Ensure that you periodically check your license specific information such as, license expiry date, number of available licenses, and number of licenses that are distributed, and more. This will enable you to effectively manage the license renewal and distribution. For more information, refer to **Where can I see the license specific information?** in the [About Term Licensing \(on page 122\)](#) topic.
- **Be proactive in reaching out to the GE Vernova representative:** Ensure that you are mindful of the license expiry date and reach out to your GE Vernova representative proactively, or reach out to the support team at <https://digitalsupport.ge.com/>. This will help you to renew your licenses in a timely manner and continue to use the product seamlessly.