



Proficy CIMPLICITY 11.1

Getting Started



Proprietary Notice

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

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

© 2021, General Electric Company. All rights reserved.

Trademark Notices

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

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

All other trademarks are the property of their respective owners.

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

doc@ge.com

Chapter 1. HMI/SCADA CIMPLICITY Introduction.....	4
About HMI/SCADA CIMPLICITY.....	4
Customer and Technical Support Contact Information.....	4
System Architecture Overview.....	5
System Architecture Overview.....	5
CIMPLICITY Server and Viewer Defined.....	7
Chapter 2. CIMPLICITY Applications Tour.....	9
CIMPLICITY Applications Tour.....	9
Part 1. CIMPLICITY Tour.....	9
Part 2. CIMPLICITY Tour.....	10
Part 3. CIMPLICITY Tour.....	11
Part 4. CIMPLICITY More Features.....	12
Part 5. CIMPLICITY Options.....	14
Chapter 3. Common Licensing.....	16
About Common Licensing.....	16
Installed License Issues.....	17
New License Steps.....	18
Update Licensed Options without Rebooting.....	21
Chapter 4. SCADA Web Configuration.....	23
About CIMPLICITY SCADA Web Configuration.....	23
Enable, Launch, and Log in to SCADA Web Configuration.....	23
Enable, Launch, and Log in to SCADA Web Configuration.....	23
Enable SCADA Web Configuration.....	24
Launch SCADA Web Configuration.....	25
Log in to SCADA Web Configuration.....	27
Select and Browse an OPC UA Device.....	28
Create SCADA Points.....	29
Generate SSL Certificate to secure SCADA Web Configuration.....	32
Generate SSL Certificate to secure SCADA Web Configuration.....	32
Using an External Certificate Authority.....	33
Update validity of SSL Certificate.....	35

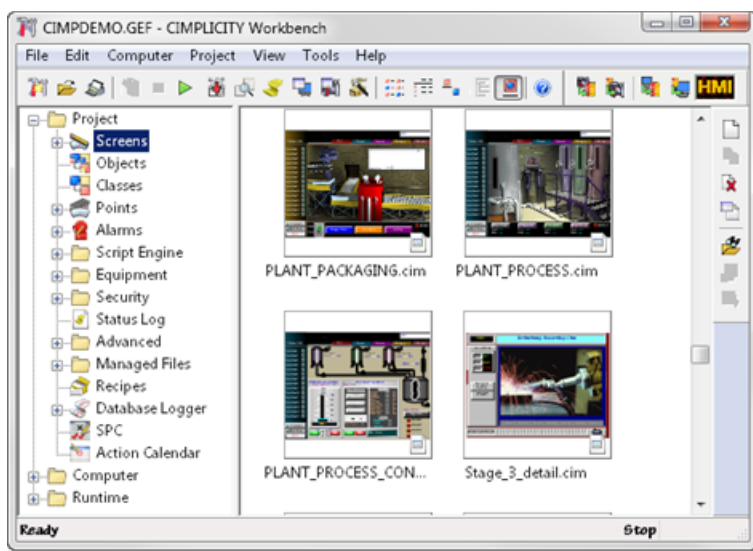
Advanced Configuration Options.....	36
Advanced Configuration Options.....	36
Configure SCADA Web Configuration Services.....	36
Configure Certificates from External Certificate Authorities for SCADA Web Configuration.....	38

Chapter 1. HMI/SCADA CIMPLICITY

Introduction

About HMI/SCADA CIMPLICITY

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



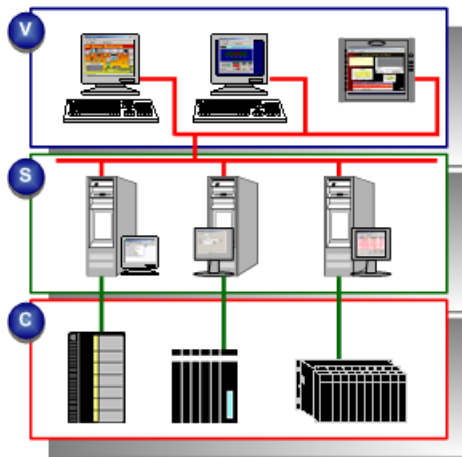
Customer and Technical Support Contact Information

For information on how to contact our Technical Support team, see digitalsupport.ge.com.

System Architecture Overview

System Architecture Overview

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



rect 3, 2, 273, 88 [\(page 6\)](#)

rect 6, 90, 273, 182 [\(page 6\)](#)

rect 4, 183, 274, 269 [\(page 6\)](#)

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.

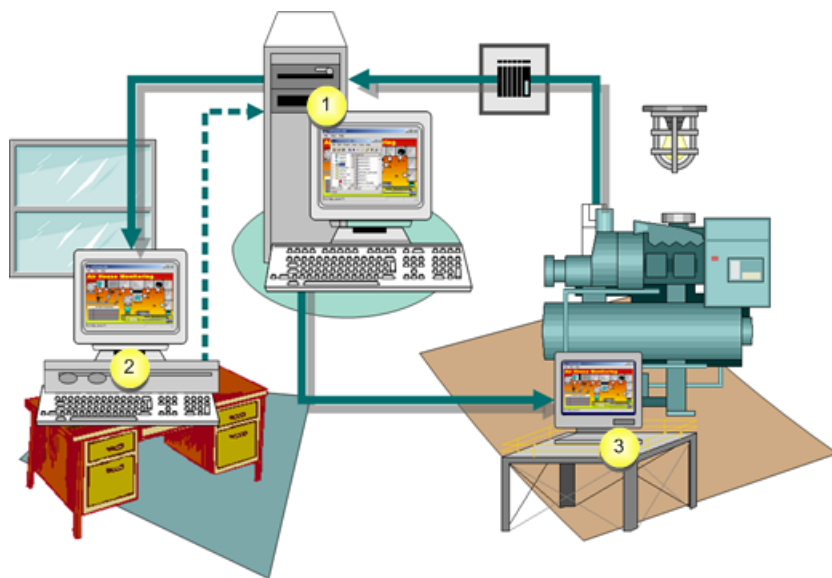
Servers and Viewers can be easily networked together to seamlessly share data without the need to replicate your point database from node to node. For example, points are configured once and only once on a server. Screens can be developed and stored in a single location on the network and accessed by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

i Tip: CIMPLICITY also provides numerous [options \(page 14\)](#) for remotely interacting with your CIMPLICITY projects.

Contact your [sales representative \(page 4\)](#) with questions about purchase options.

Chapter 2. 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 (page 9)	How to set up the foundation for your system goals.
Part 2 (page 10)	How to set up points and alarms.
Part 3 (page 11)	How to create powerful applications that can graphically deal with system data for whoever has access privileges.
Part 4 (page 12)	Many other powerful tools.
Part 5 (page 14)	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.
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.

Part 1 of CIMPLICITY Tour	
Step 4.	<p>Configure a device including:</p> <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.	<p>Define security and routing including:</p> <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.

Part 2 of CIMPLICITY Tour	
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. • 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: <ul style="list-style-type: none"> ◦ 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. ◦ 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. • 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. • XY Plot provides you with the ability to visually represent values in relation to each other. For example, you can plot real data vs. calculated date, or elements such pressure vs. temperature. • Remote Projects need to be defined when a project starts, the Point Bridge or Point Data Logger need to get points from projects on other computers running CIMPLICITY projects. • Recipes enable you to create and manage recipe data for your production processes. The Recipes interface consists of a spreadsheet format in which you enter the configuration data for each of your recipes. This format allows you to group similar products together.

Feature	Description
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. • 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.

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

Chapter 3. Common Licensing


About Common Licensing

The family of products provides you with hardware keys that are programmed with licenses for your selected products and options.

You simply:

1. [Buy \(page 18\)](#) your products and options.

Visit the GE Customer Center web site at <http://support.ge-ip.com> to obtain information about the latest GE product offerings.

 **Note:** If you visit this web site, click a topic on the HMI/SCADA CIMPLICITY documentation Contents tab to return to the documentation.

When you receive your DVD you will receive as many hardware keys as you need.

If you have any questions about licensing call the GE Intelligent Platforms [support line \(page 4\)](#). A GE representative will direct your call to the correct resource.

2. Install your products.
3. Plug one of the keys into each Server that requires one or more licenses.

You are ready to go.


You can choose either of two key types.

- One key can be plugged into a Server's parallel port.



- The other key can be plugged into a Server's USB port.



 **Note:** If you need to reboot a computer that requires a license, make sure the key is inserted in the computer before you reboot so any services that start up can read the key.

Installed License Issues

- Hardware key removal.
- License upgrades.
- License expiration.

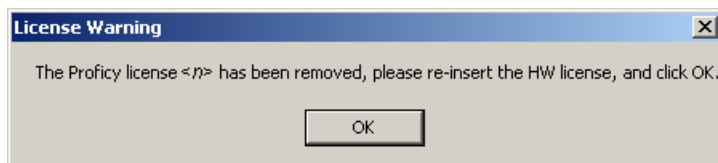
Hardware key removal

When the hardware key is removed from a Server:

- An Alert Message will display on the first Server, informing you that the hardware key has been removed; please plug it in.

When you click OK to close the message, it will display again in one minute.


The message will continue until the key is re-attached to the Server.



- If a project is running, it will continue running. However, if it is restarted before the key is re-attached, it will revert to demonstration mode.

License upgrades

If you buy additional options after you receive your hardware key(s) you will receive an email with an update .plic license file.


 **Important:** Before upgrading your license, shut down all of the applications on the computer you are working on. When you upgrade your licensing, the Licensing Service is automatically stopped and then restarted when the upgrade successfully completes.

1. Save the .plic file to a directory of your choice.
2. Double-click the file.

An update utility opens.

3. Click Update Now.

The utility validates your current license. If the validation is successful, the utility updates the license; if the validation is not successful, the upgrade is halted.

 **Note:** Contact your sales representative for information about obtaining the license file.

License expiration

When you purchase a product, it is licensed without an expiration date.

If a demonstration license is provided to you for you to try the software, it will be provided with an expiration date that will allow the software to run up until that date. You will receive notices on your screen alerting you to when the licenses will expire.

New License Steps

1. Obtain a hardware key for products and options.

Specify the following that you are ordering:

- Part number for each product and feature.
- Quantity of each product and feature.
- If the hardware should be parallel or USB port.
 - There can be only one hardware key per computer.
 - You can attach a parallel port printer cable to a parallel port hardware key.
- List of what products/options will be installed on each Server.

The default hardware key configuration is that each hardware key will contain the set of licenses for every product and option purchased.

You will receive a hardware key for each set of licenses.

If you order 4 CIMPLICITY licenses and 3 Historian licenses, you will receive the following:

No. of Keys	Key Contains Licensing for
3	CIMPLICITY and Historian
1	CIMPLICITY

Each key will contain that products/options according to your specifications.

If you order 4 CIMPLICITY licenses and 3 Historian licenses and plan to run each on a different server, you will receive the following:

No. of Keys	Key Contains Licensing for
4	CIMPLICITY
3	Historian


 **Important:** You can attach only one key to a Server.

When your order is fulfilled you will receive one or more CDs and hardware keys.

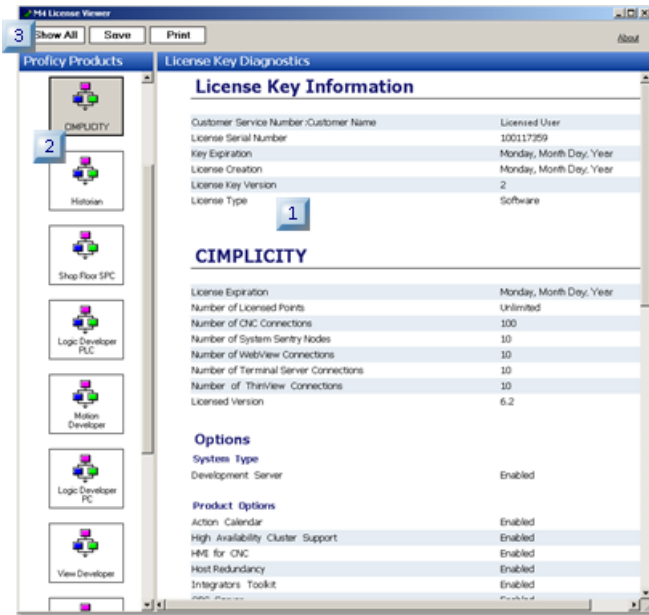
2. Install your products and options.
Follow the installation directions for each of your products.
3. Attach the hardware key to the server.

Attach one hardware key to either the parallel or USB port, depending on what you ordered.

Type of Key	Attach to a
Parallel port	Parallel port on the Server. You can then attach a parallel printer cable to the hardware key.
USB	USB port on the Server.


 **Important:** Attach the hardware key to the Server only after you install all of the licensed products.

4. Review the license report.
 - a. Click Start on the Windows task bar.
 - b. Select (All) Programs>Common>License Viewer on the Start menu.
The M4 License Viewer opens.



rect 0, 9, 23, 30 (page 20)
 rect 19, 78, 40, 99 (page 20)
 rect 170, 119, 191, 140 (page 20)

License report tools are as follows.

Tools	Description
1	The right pane in the M4 License Viewer displays the: <ul style="list-style-type: none"> • License key details. • Customer name • Serial number • Key expiration • License creation • License key version License type • License details for the selected product(s), including: <ul style="list-style-type: none"> • License expiration • Number of licensed points • Number of <option> nodes • Number of <option> connections • Enabled options.
2	The left pane displays icons for each of your licensed products. Click an icon to select it and the details display in the right pane that correspond to the selected product.  Note: You can click the Show All button on the M4 License Viewer toolbar to display details about all the licensed products on the same page
3	Click any of the buttons on the M4 License Viewer toolbar to do the following: <ul style="list-style-type: none"> • Show All - Displays all of the details about all of the licensed products on the same page. • Save - Saves. • Prints - Prints the report that displays.

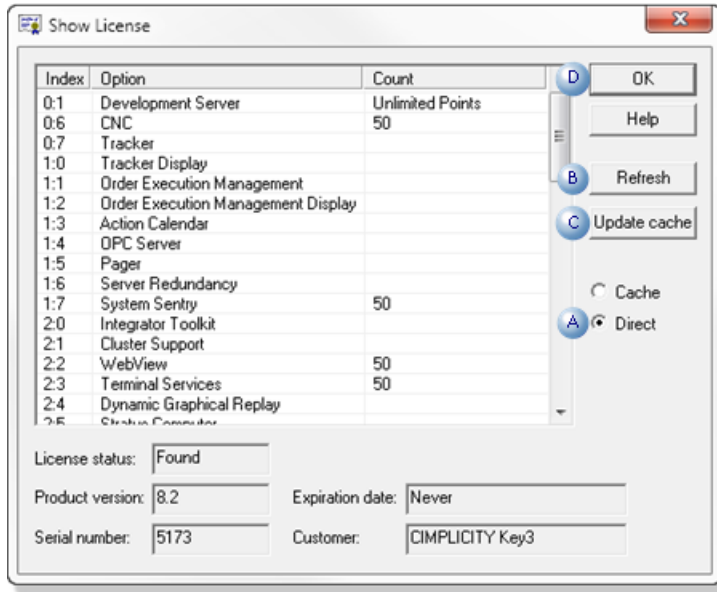
5. Run your project(s) on the licensed server. Start any project on the licensed server.

! **Important:** If you start a project on a Server that does not have a license a message may warn you that no license is present, and the project will run in demonstration mode. Demonstration mode provides you with limited functionality, including no networking. Demonstration mode runs for a maximum of two hours. The actual time depends on which product is unlicensed.

Update Licensed Options without Rebooting

1. Make sure the hard key is inserted in the computer on which the utility will be run.
2. Click Start on the Windows task bar.
3. Select Run on the Start menu.
4. Enter `ShowLicense` in the Run dialog box.
A Show License utility opens.
5. Select the following options on the **Show License** screen (shown below):

Option	Description
A	Check Direct to direct the report to what is on the new key.
B	Click Refresh to update the screen with updated licensing information when the licensing service reads the key. The key is read every 30 seconds.
C	Click Update cache .
D	Click OK when finished.



CIMPLICITY now recognizes the new option(s) as being licensed.

Chapter 4. SCADA Web Configuration

About CIMPPLICITY SCADA Web Configuration

You can use SCADA Web Configuration to discover the address space of an OPC UA Server and automatically create points from the address space.

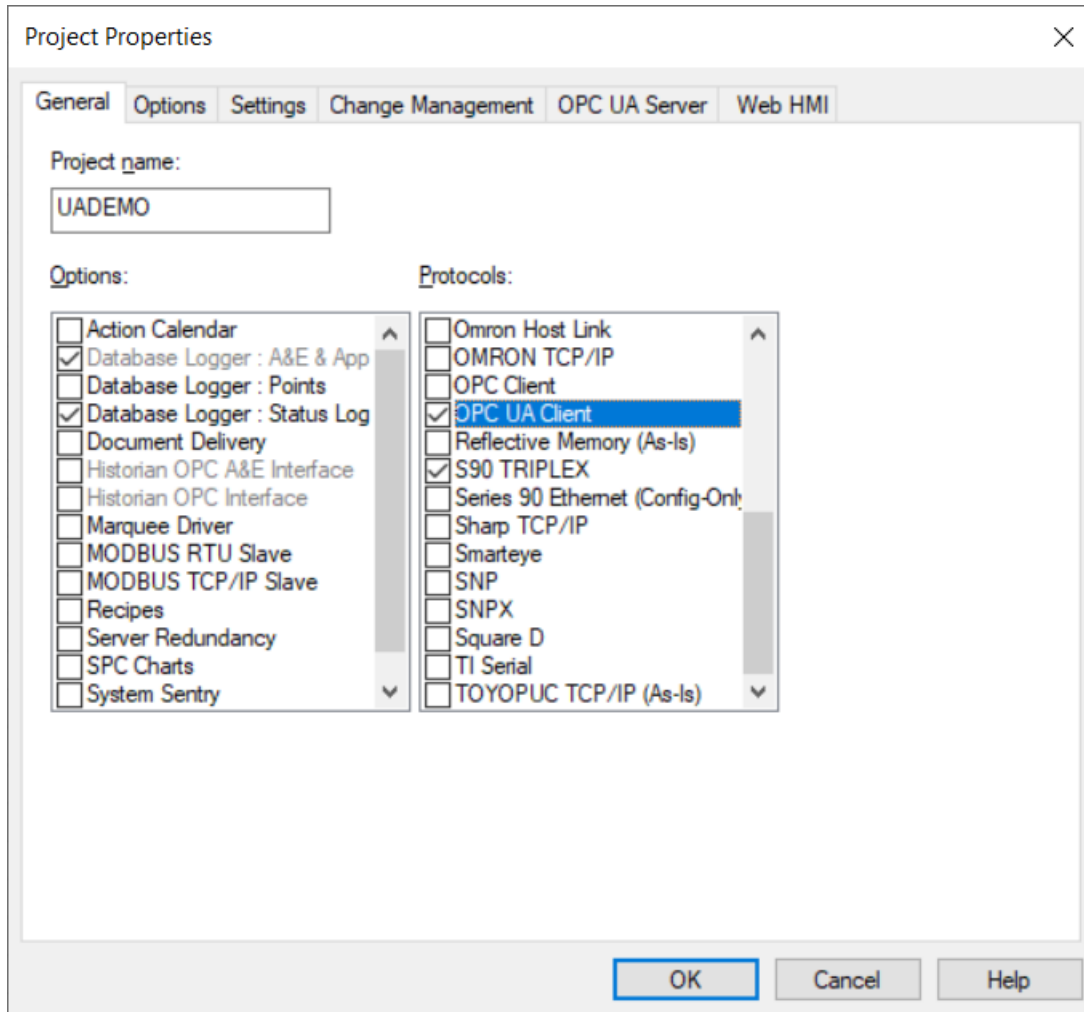
You are provided with access to a web application where you can browse through the OPC UA Servers configured in a project and create CIMPPLICITY points.

Enable, Launch, and Log in to SCADA Web Configuration

Enable, Launch, and Log in to SCADA Web Configuration

Before you enable, launch, and log in to SCADA Web Configuration, perform the following steps:

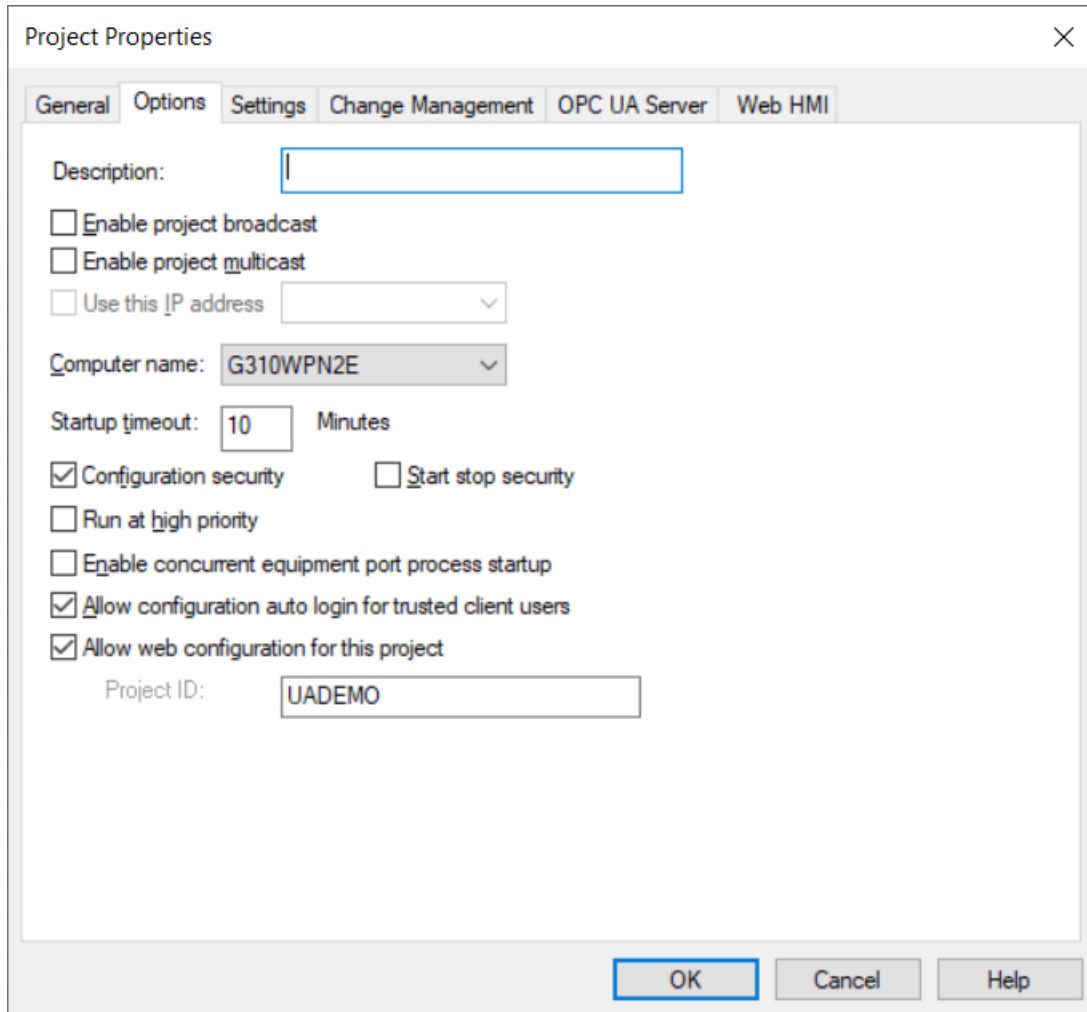
1. In Workbench, create a new project or access an existing project.
2. Access the Project Properties window, select the General tab, and under Protocols, select the OPC UA Client check box.



3. Select OK.
4. Create a device for each OPC UA Server and configure the device.

Enable SCADA Web Configuration


To enable web configuration for a project, in **Workbench**, access the **Project Properties** window, select the **Options** tab, and then select the **Allow web configuration for this project** check box.



The screenshot shows the 'Project Properties' dialog box with the 'Options' tab selected. The dialog has a title bar with a close button (X) and a tabbed interface with the following tabs: General, Options, Settings, Change Management, OPC UA Server, and Web HMI. The 'Options' tab contains the following settings:

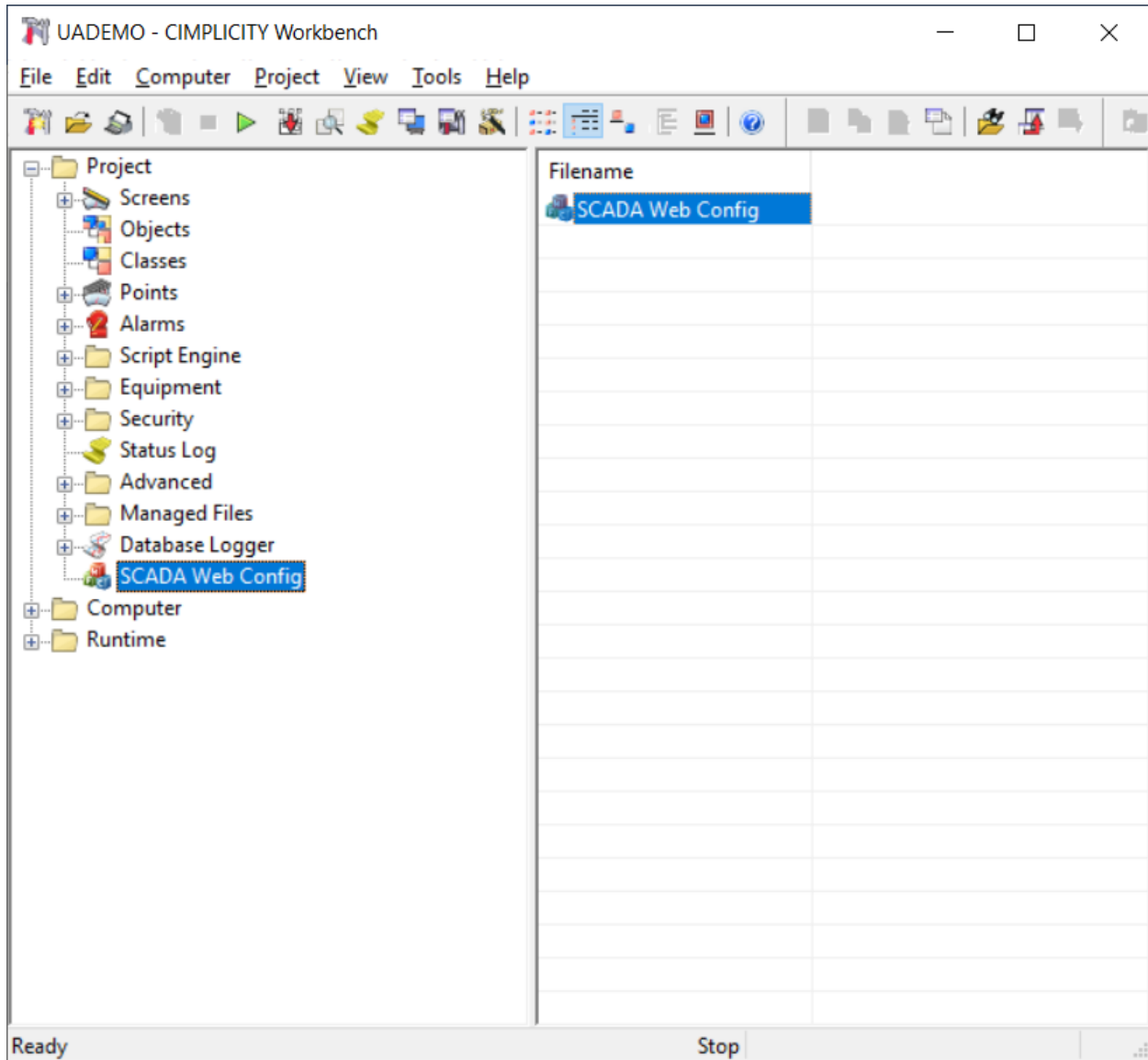
- Description: [Empty text box]
- Enable project broadcast
- Enable project multicast
- Use this IP address [Dropdown menu]
- Computer name: G310WPN2E [Dropdown menu]
- Startup timeout: 10 Minutes
- Configuration security Start stop security
- Run at high priority
- Enable concurrent equipment port process startup
- Allow configuration auto login for trusted client users
- Allow web configuration for this project
- Project ID: UADEMO [Text box]


At the bottom of the dialog are three buttons: OK, Cancel, and Help.

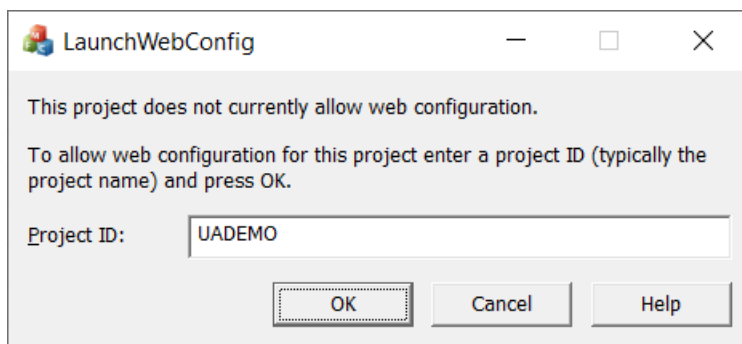
 **Note:** If you do not enable web configuration for a project as mentioned above, you can enable it when you launch SCADA Web Config.

Launch SCADA Web Configuration

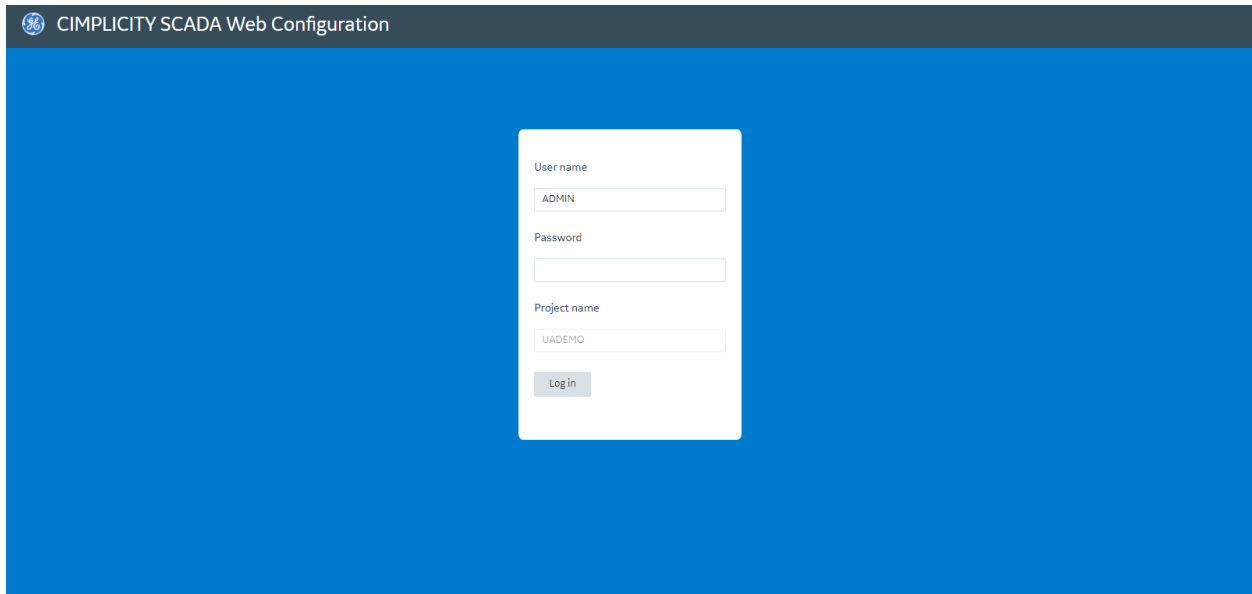
To launch SCADA Web Configuration, in **Workbench**, select **SCADA Web Config**, and double-click the SCADA Web Config file.



 **Note:** If web configuration was not enabled for the project, a **LaunchWebConfig** window appears, prompting you to enable web configuration for the project. Select **OK**.



The **CIMPLICITY SCADA Web Configuration** web page appears.



The screenshot shows the login page for CIMPLICITY SCADA Web Configuration. The page has a blue background and a white login form in the center. The form contains the following fields and buttons:

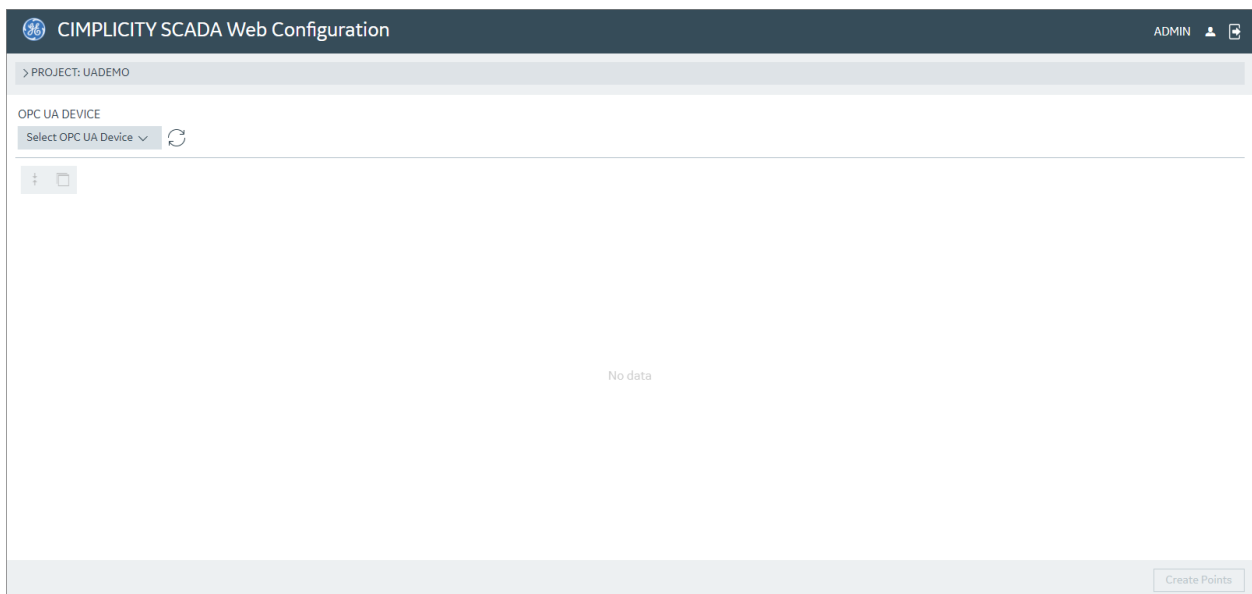
- User name:** A text input field containing the text "ADMIN".
- Password:** A text input field that is currently empty.
- Project name:** A text input field containing the text "UADEMO".
- Log in:** A button located below the Project name field.

To view the list of OPC UA Devices that your project contains, you must log in to SCADA Web Configuration.

Log in to SCADA Web Configuration

On the **CIMPLICITY SCADA Web Configuration** webpage, enter the username and password from the project configuration, and then select **Log in**.

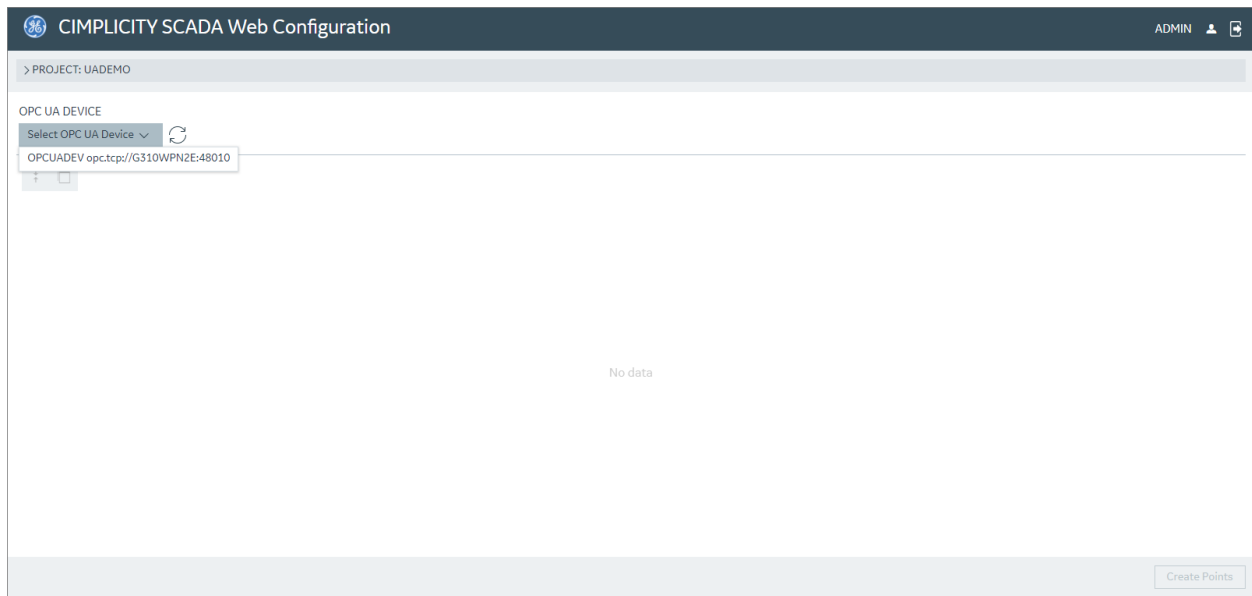
The **OPC UA Device** selection webpage appears.



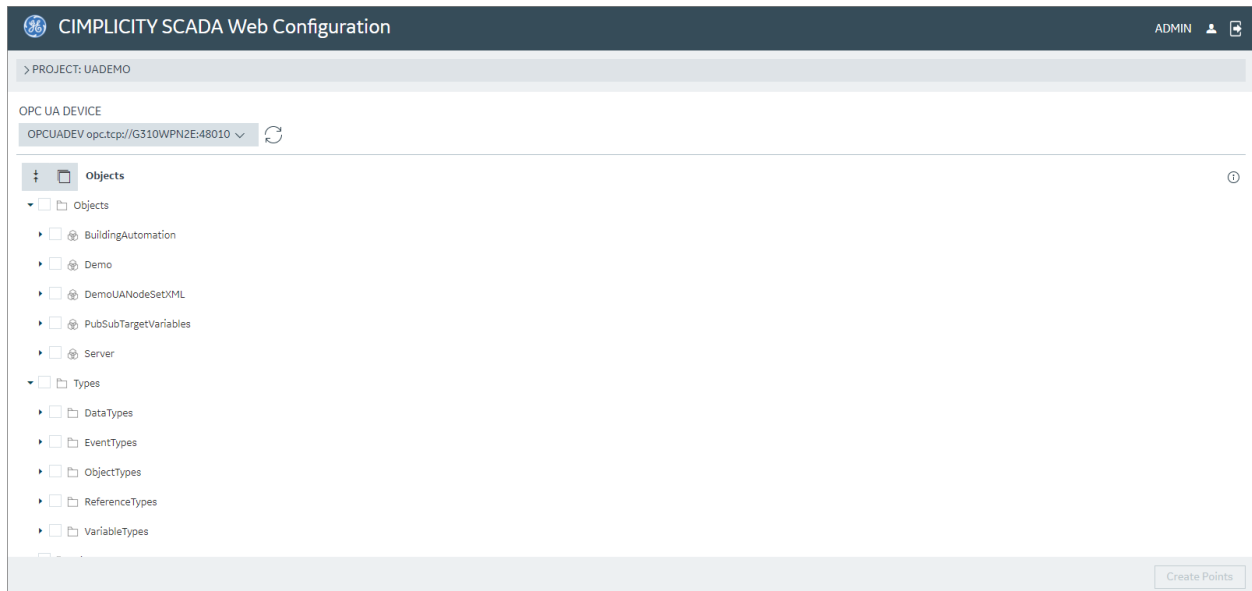
The screenshot shows the OPC UA Device selection webpage. The page has a light blue header with the text "CIMPLICITY SCADA Web Configuration" and "ADMIN" on the right. Below the header, there is a breadcrumb trail: "PROJECT: UADEMO". The main content area is titled "OPC UA DEVICE" and contains a dropdown menu labeled "Select OPC UA Device" with a refresh icon. Below the dropdown, there is a large empty area with the text "No data" centered. At the bottom right of the page, there is a button labeled "Create Points".

Select and Browse an OPC UA Device

The **Select OPC UA Device** list displays the list of devices that have been configured for OPC UA Servers in your project. Select an OPC UA Device.



All the nodes in the OPC UA Device are displayed. You can browse through them.



Create SCADA Points

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

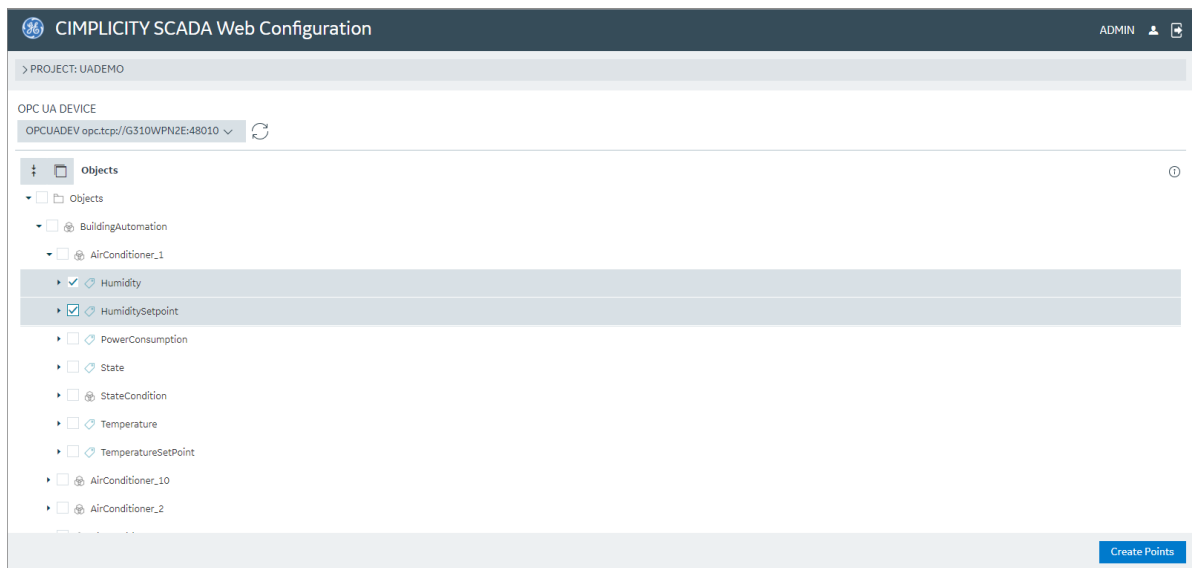
To create SCADA points:

1. Select the objects.

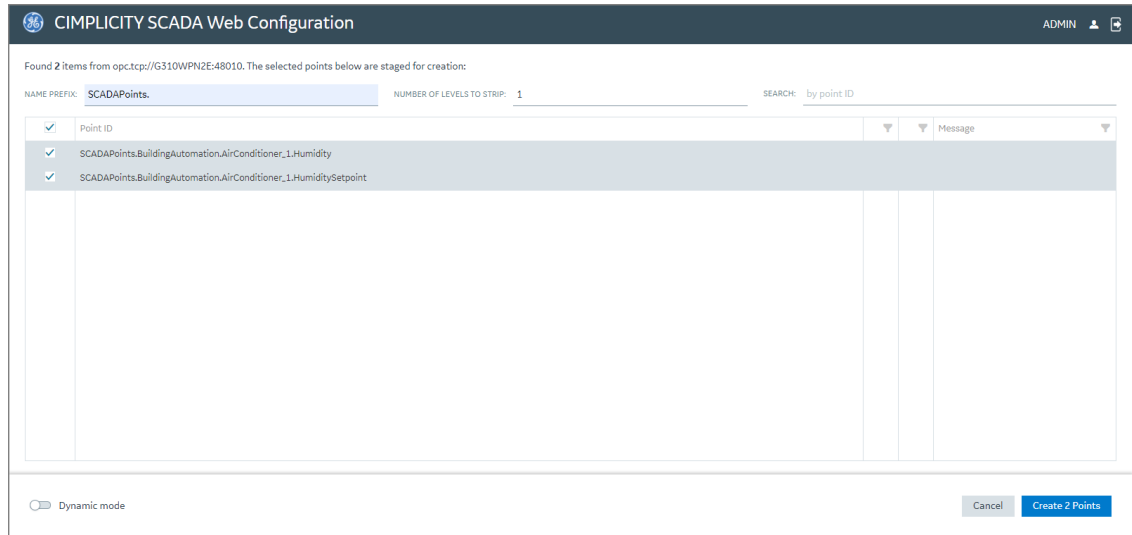
Note: To select the children of a node, right-click the node, and then select Select all children. Alternately, to select the children of a node, you can double-click the node.

To clear the children of a node, right-click the node, and then select Clear children selection. Alternately, to clear the children of a node, you can press and hold Alt, and double-click the node.

2. Select Create Points.



3. (Optional) You can use the following fields to perform specific actions:
 - **NAME PREFIX:** Enter a prefix to the name of the points that will be created.
 - **NUMBER OF LEVELS TO STRIP:** Enter the number of levels in the namespace to be stripped off from the beginning of the point IDs.
 - **SEARCH:** Enter text to display point IDs that contain the entered text.

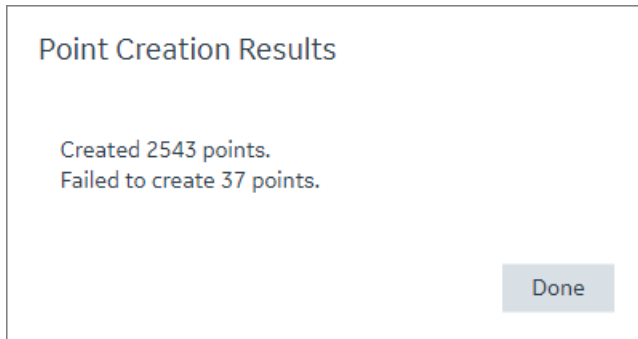


When the project is running, if you turn on the Dynamic mode toggle key, the points that are created will be available immediately. If you turn off the Dynamic mode toggle key, the points that are created will become available only after the project restarts.

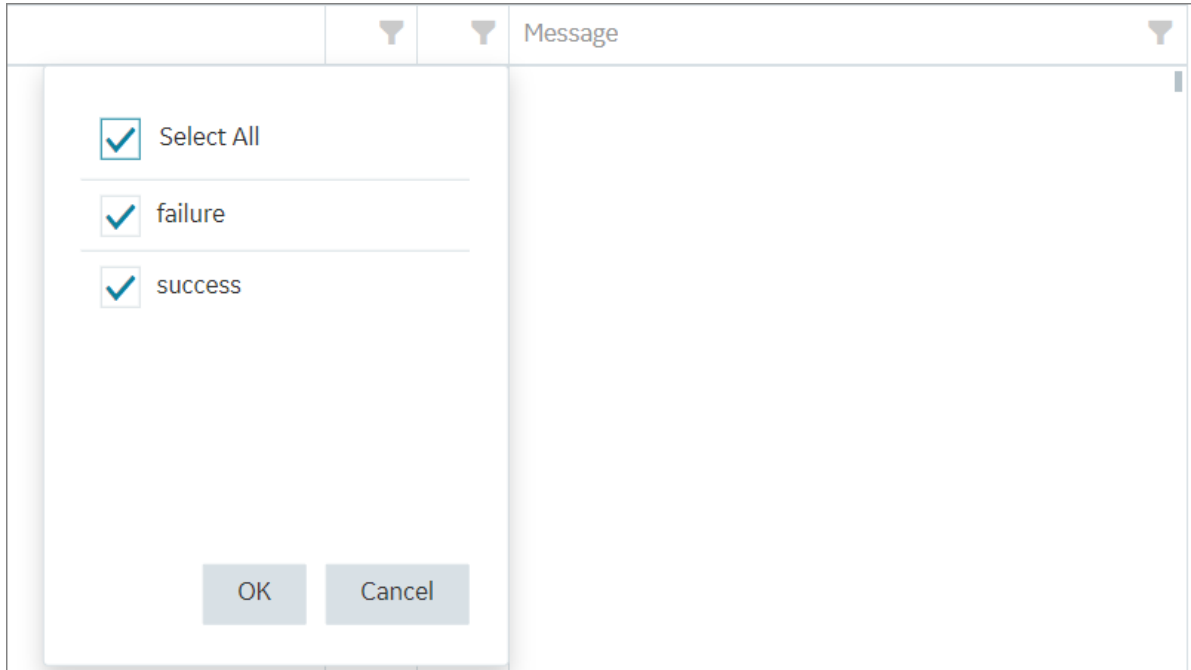
Note: In a redundant system, for dynamic configuration to work, the CIMPLICITY Configuration Microservice should run as the same user with the same password configured in the redundant pair of systems.

4. Select Create (number of points selected) Points.

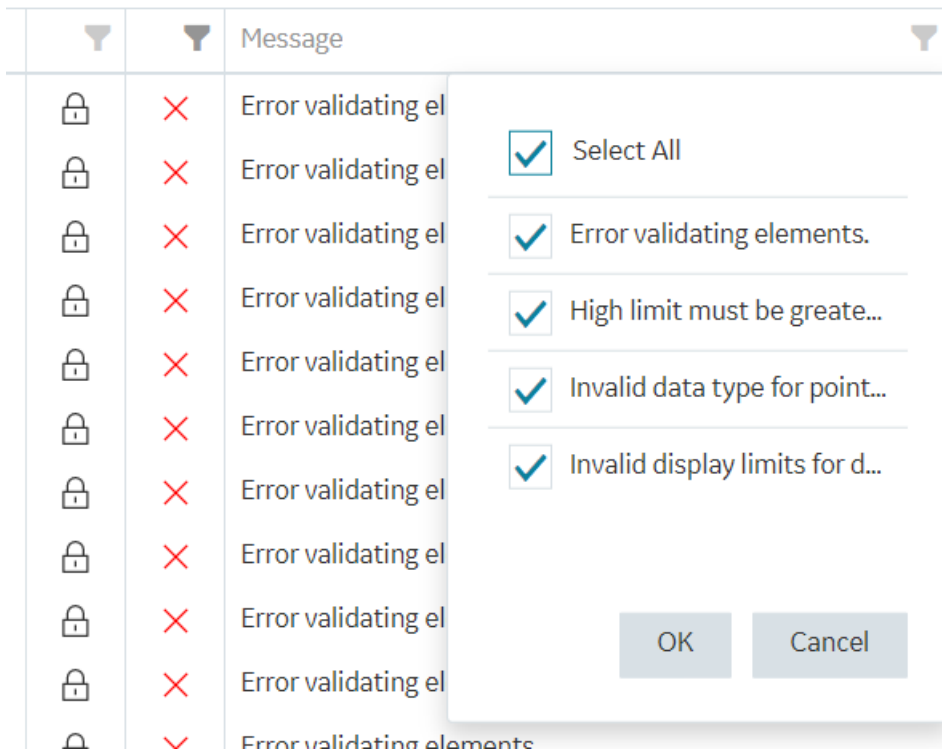
The points are created, and the results are displayed.



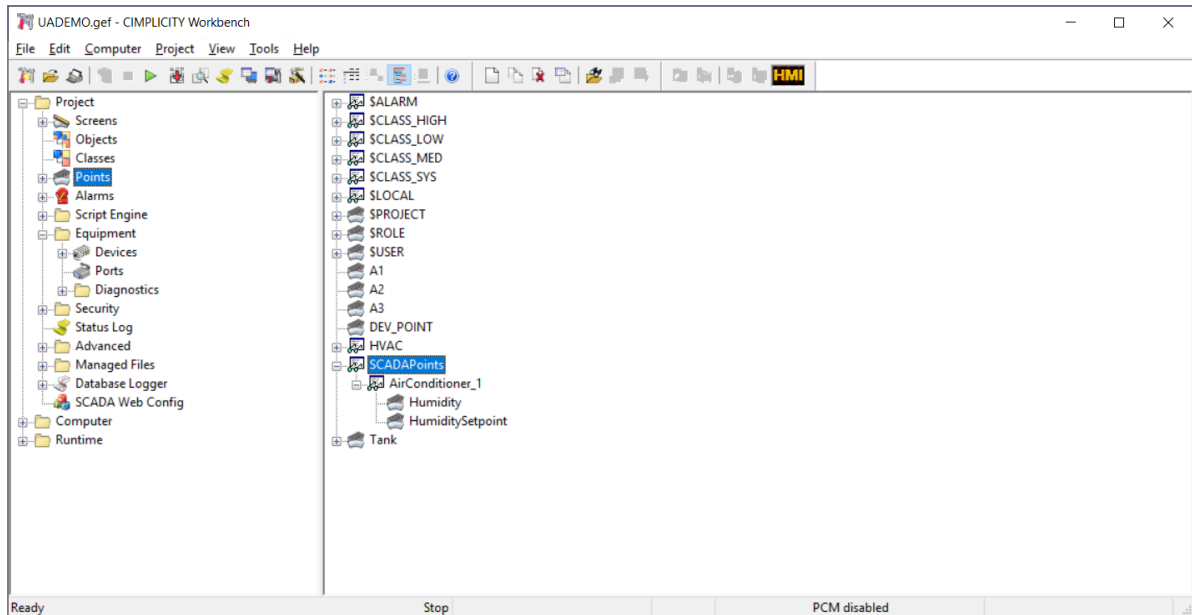
You can view the points that were not created by filtering the results based on the icon associated with the points.



You can filter the failed points based on the type of failure associated with each point.



Note: You can view the created points in Workbench under the Points section.



Generate SSL Certificate to secure SCADA Web Configuration

Generate SSL Certificate to secure SCADA Web Configuration

The SCADA Web Configuration is 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 SCADA Web Configuration, 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 SCADA Web Configuration is not secure. To make the connection secure, replace the domain name in the URL with the computer name.

This section provides information to help you to:

- [Using an External Certificate Authority \(page 33\)](#)
- [Update validity of SSL Certificate \(page 35\)](#)


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

To manually execute the batch files **Generate_CSR.bat** and **process_server_cert.bat**, the following parameters must be known:

- **InstallationPath** - The path where CIMPLICITY is installed.
- **ConfigServicePortNumber**, **UABrowseServicePortNumber**, and **WsmServicePortNumber** - The port numbers where micro services are running (WSM is the webspace-session-manager).
- **KeyPassPhraseFilePath(optional)** - The file path that contains a password that protects the private key (without the .crt/.key extension).
- **ServerCertificateName** - The name of the server certificate file (without the .crt/.key extension)..

 **Note:** The default value of **ServerCertificateName** is **server_cert**. To use a different file name, also update the variables **ssl_certificate** and **ssl_certificate_key** in **nginx.conf** file with the new values and restart the **CIMPLICITYNGINX** service.

- **PfxPassPhrase** - The password to protect the generated .pfx server certificate.

To regenerate the SSL certificate, perform the following steps:

1. Generate CSR

- a. In the command prompt, navigate to the path where **Generate_CSR.bat** is saved.
- b. Enter the following command in the command prompt.

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

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

- c. 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
CIMPLICITY" server_cert "c:\Passwords\password.txt"
```

- d. 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.
- e. Enter the following details:

Enter the required details Country Name (2 letter code) [AU]:

State or Province Name (full name) [Some-State]:

Locality Name (eg, 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 []:

Please enter the following 'extra' attributes to be sent with your certificate request

A challenge password []:

An optional company name []:

- f. 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. In the command prompt, navigate to the path where **process_server_cert.bat** is saved.
- b. Enter the following command in the command prompt.

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


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

Where:


- <CertFileName> is the name of the crt/key files without the .crt or .key extensions.
- <KeyPassPhraseFilePath> contains the pass phrase protected the .key file. This is the same pass phrase file used in the Generate_CSR.bat command.
- <PfxPassPhrase> is the pass phrase that will be used to protect the generated .pfx file. This is the pass phrase itself, not a path to a pass phrase file.

- <KeyPassPhraseFilePath> contains the pass phrase protected the .key file. This is the same pass phrase file used in the Generate_CSR.bat command.

4. Verify SSL certificate

- Launch Scada Web Config from CIMPLICITY Workbench.
- Select , and then select **Certificate**.
- Verify the CertificateInformation. It should match with the information provided at Step 1.

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

 **Note:** If the certificate is not updated, you may have to perform the following steps and re-launch Scada Web Config:

- Delete browser cache.
- Restart the following:
 - CIMPLICITY Configuration Microservice
 - OPC UA Browser Microservice
 - Webspace Session Manager Microservice
 - CIMPLICITY NGINX Server
- Update the proxy settings to exclude the server on which the SSL certificate is hosted.

Update validity of 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.

Advanced Configuration Options

Advanced Configuration Options


The default settings for the SCADA Web Configuration application is sufficient for most scenarios.

This section provides information on the following advanced configuration options for the SCADA Web Configuration application:

- [Configure SCADA Web Configuration Services \(page 36\)](#)
- [Configure Certificates from External Certificate Authorities for SCADA Web Configuration \(page 38\)](#)

Configure SCADA Web Configuration Services

You can configure various parameters for the SCADA Web Configuration application.

 **Note:** The default settings of the configuration files is sufficient for most scenarios. Update the configuration files only if absolutely necessary.

You can update the following configuration files:


- nginx.conf
- cim_config_service.json
- opcua-browse-config.json

nginx.conf


The SCADA Web Configuration application is hosted in the nginx web server. To update any parameter for nginx web server, you must edit the nginx.conf file.

You can update the following parameters in the nginx.conf file:

- **listen:** Enter the port number where you want to run your server.


 **Note:** The default port number is 9443.

- **client_max_body_size:** Enter the maximum size (in megabytes) of a client request that goes through the nginx server.

 **Note:** If this value is too low and the request is too big, a 413 Payload Too Large error will occur. If this value is too high, it could cause out-of-memory errors in the services and application, and could allow attackers to occupy the services for too long.

- **proxy_read_timeout:** Enter the maximum time that the nginx server will wait for a proxied response to be returned.

The nginx server proxies requests from a client to the CIMPLICITY Configuration service and the OPC UA Browse service. If a response isn't returned by the service within this amount of time, a 404 Not Found error will occur.


 **Note:** If this value is too low, when you browse or create points, 404 errors may occur. If this value is too high, it may take longer for issues with services to be discovered, and could allow attackers to occupy the services for too long.

cim_config_service.json

cim-config service is a microservice which is an intermediary between the web server and CIMPLICITY. To update any parameter in `cim_config_service`, you must edit the `cim_config_service.json` file.

You can update the following parameters in the `cim_config_service.json` file:

- **port:** Enter the port number on which the cim-config service is listening.

 **Note:** You must also update the port number for cim-config service under the reverse proxy section of the `nginx.conf` file.

- **maxWriteRequestObjects:** Enter the number of points that can be sent in a single request for point creation. If there are several points to create, multiple requests are sent.


 **Note:** If this value is too high, a 413 Payload Too Large or 404 Not Found error may occur. If this value is too low, the point creation performance will be affected.

opcua-browse-config.json

OPC UA browse service is a microservice which is an intermediary between the web server and CIMPLICITY. To update any parameter in OPC UA browse service, you must edit the `opcua-browse-config.json` file.

You can update the following parameters in the `opcua-browse-config.json` file:

- **port:** Enter the port number on which the OPC UA browse service is listening.

 **Note:** You must also update the port number for OPC UA browse service under the reverse proxy section of the `nginx.conf` file.


- **maxBrowseRequestObjects:** Enter the number of nodes that can be sent in a single request to the OPC UA Browse Service and the OPC UA server when browsing the OPC UA server.

 **Note:** If this value is too high, the 413 Payload Too Large error may occur. If this value is too low, the browsing and point creation performance will be affected.

- **maxBrowseResultObjects:** Enter the number of nodes that can be sent in a single response by the OPC UA Browse Service and the OPC UA server. If a request would return several nodes, multiple responses with OPC UA continuation points are returned.

 **Note:** If this value is too high, the 413 Payload Too Large error may occur. If this value is too low, the browsing and point creation performance will be affected.

maxReadRequestObjects: Enter the number of nodes that can be sent in a single request to the OPC UA Browse Service and the OPC UA server when reading node attributes from the OPC UA server.

 **Note:** If this value is too high, the 413 Payload Too Large error may occur. If this value is too low, the browsing and point creation performance will be affected.

404 and 413 Error Workaround

If you encounter a 404 error, perform either of the following actions:

- Decrease the service limits for these parameters - `maxReadRequestObjects`, `maxBrowseRequestObjects`, `maxBrowseResultObjects`, and `maxWriteRequestObjects`.
- Increase the `proxy_read_timeout` parameter in the `Web\exe\conf\nginx.conf` file.

If you encounter a 413 error, perform either of the following actions:

- Decrease the service limits for these parameters - `maxReadRequestObjects`, `maxBrowseRequestObjects`, `maxBrowseResultObjects`, and `maxWriteRequestObjects`.
- Increase the `client_max_body_size` parameter in the `Web\exe\conf\nginx.conf` file.


Configure Certificates from External Certificate Authorities for SCADA Web Configuration

You can configure certificates received from external Certificate Authorities (CA), such as VeriSign and DigiCert for the SCADA Web Configuration application.

Ensure that the certificate received from the CA can be used as an intermediate CA for signing other certificates.

To configure a certificate from an external CA:

1. Go to the path where CIMPLICITY is installed, and delete all the files in the ScadaConfigPki folder.

 **Note:** Before you delete the files in the ScadaConfigPki folder, prepare a backup of the files.

2. Copy the <RootCertificateName>.cert and <RootCertificateName>.key files from the CA and paste them into the ScadaConfigPki folder.
3. Access Command Prompt and enter the following command:

```
cd <InstallationPath>
```

For example:

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

4. Enter the following command by specifying the RootCertificateName received from the CA:

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

For example:

```
config_service_cert.bat "C:\Program Files (x86)\Proficy\Proficy
CIMPLICITY\" 4855 4865 RootCA1 server_cert cimplicity
```

A server certificate and private key is generated in the ScadaConfigPki folder and replicated to the nginx configuration folder.

5. Enter the names of the server certificate and private key in the server section of the nginx.conf file. For example:

```
server {
    .....
    .....
    ssl_certificate server_cert.crt;
    ssl_certificate_key server_cert.key;
}
```


The external CA is now used as the root authority for the SCADA Web Configuration application.