



Proficiency Web HMI

User Guide



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.

© 2022, 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

Contents

- Chapter 1. Release Notes..... 8**
 - Introduction..... 8
 - New in the Release.....8
 - Software Requirements..... 8
 - Hardware Requirements.....9
 - Compatibility Matrix..... 10
 - Kiosk Mode..... 10
 - Resolved Issues..... 11
 - Known Issues..... 12
- Chapter 2. Get Started with Cimplicity and Web HMI..... 15**
 - Get Started with CIMPLICITY and GE Web HMI..... 15
- Chapter 3. Get Started with iFIX and Web HMI..... 22**
 - Get Started with iFIX and Web HMI..... 22
- Chapter 4. Get Started with Workflow and Web HMI..... 27**
 - Get Started with Workflow and Web HMI..... 27
- Chapter 5. Install and Upgrade..... 31**
 - Prerequisites..... 31
 - Install Web HMI 32
 - Connections based on URLs..... 34
 - Run the Data Service Configuration Tool..... 34
 - Upgrade Web HMI..... 34
 - Back Up Customized Components..... 36
 - Restore Web HMI Databases..... 36
 - Import Extensions..... 37
 - Log in to Web HMI..... 37
 - Web HMI Environments..... 38
 - Uninstall Web HMI..... 38

Chapter 6. Certificate Management and Content Security	39
Certificate Management.....	39
Install CA Certificates.....	40
Apply Custom Certificates.....	41
Install Workflow Certificate in iPad Clients.....	41
Set up a Whitelist.....	42
Whitelists.....	42
Security Recommendations.....	43
Chapter 7. GE HMI Server Configuration Manager	45
GE HMI Server Configuration Manager.....	45
Secure Connections to OPC UA Endpoints.....	45
Create Self-Signed Certificates for Web HMI Clients.....	49
Use GDS Certificates for Web HMI Clients.....	49
Connect to Historian.....	51
Define Tracing and Logging.....	52
Chapter 8. Develop Runtime Content	53
Runtime Model.....	53
Model Editor.....	53
Supported Characters for the Model	53
Set Up Data Source Servers.....	55
Set Up the Model Structure.....	55
Define Objects.....	56
Duplicate Objects.....	57
Set Up Runtime Navigation.....	58
Change Server Details.....	59
Modify Object Types.....	59
Remove Contained Types	60
Replace Contained Objects.....	60
Modify Objects.....	61

Export the Model.....	62
Make Extensive Model Changes.....	62
Import the Model.....	62
Access the Model Template.....	63
Model Template Description.....	63
Layouts.....	69
Layout Cards.....	70
Import Mimics.....	71
Bind Mimics to Assets.....	72
Override Mimics.....	73
Set Up Mimic Target Zones.....	73
Define Mimic Control Views.....	75
Define Trend Data.....	76
Override Attributes at the Object Level.....	77
Chapter 9. Set Up User Security.....	78
User Account Overview.....	78
Access the Application Assembler	78
Create User Accounts.....	79
Assign Users to a Group.....	79
Change User Passwords.....	80
Define LDAP Settings.....	80
Create Users and Groups.....	81
Configure Active Directory Authentication.....	82
Set Up the AD Server Connection.....	83
Define the AD Schema Mappings.....	84
Map AD Groups with ThingWorx Groups.....	85
Enable User Provisioning.....	85
Set User Defaults.....	86
Exclude Users from Provisioning.....	88

Chapter 10. Reset Web HMI.....	89
Reset Web HMI.....	89
Chapter 11. Transfer Project Data.....	90
Overview.....	90
iFIX Prerequisites.....	92
CIMPLICITY Prerequisites.....	92
Bundle the Project Data	93
Copy the Project Data to the Target.....	93
Update the Server Alias File.....	93
Import the Workflow Project File.....	94
Deploy the Project Bundle	94
Command-Line Options.....	95
Error Messages.....	96
Chapter 12. Customize Components.....	98
Related Components.....	98
Alarm Gateway Configuration Tool.....	98
Alarm Microservice.....	99
Asset Microservice.....	100
Entity-Metadata Microservice.....	100
Server-Details Microservice.....	101
Tag-Source Microservice.....	101
Chapter 13. Customize the Web HMI Menu.....	102
Set the Default Layout.....	102
Add Menu Items.....	102
Hide Menu Items.....	103
Chapter 14. Interact with Runtime.....	104
Log in to Web HMI	104
Verify the Version Number.....	104
Select a Layout.....	104

View Alarm Cards.....	104
View Mimic Cards.....	106
Update Values on Mimic Cards.....	106
Edit Values on Mimic Control Views.....	107
View Trend Cards.....	108
Manipulate Trend Charts.....	110
View Task List Cards.....	112
Log out of Web HMI.....	113
Chapter 15. Troubleshoot.....	114
OPC UA Write Errors.....	114
Error Symbols.....	114
iFIX Issues.....	115
Workflow Task Lists Not Appearing in iPads.....	118
LDAP Settings for AD Authentication.....	118
How Does Historian Data Appear in the Model.....	121
Index.....	

Copyright GE Digital

© 2019 General Electric Company.

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

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

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

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

Chapter 1. Release Notes

Introduction

Web HMI from GE Digital enables you to monitor and control production equipment and processes through a web-based human machine interface (HMI) that securely communicates with your SCADA system via an on-premise web server.

Web HMI visualization consists of a series of animated process diagrams called mimics that simulate the equipment pieces and their properties in a production environment. The Web HMI navigation hierarchy provides real-time summary views that operators can drill down to see details about individual assets, enabling quick and effective analysis of issues.

New in the Release

The Web HMI 2.2 SP2 release provides the following:

The ability to retrieve data from more than one Historian server.

Software Requirements

Your software must meet the following minimum requirements to operate Web HMI.



Note:

Web HMI only supports the English version of the operating systems.

Browsers

- Safari 9.1 or higher on the iPad (runtime only)
- Google Chrome 51 or higher
- Microsoft Edge



Note:

Internet Explorer 11 is no longer supported.

Client (Browser) Operating Systems

- Microsoft® Windows® Server 2016
- Microsoft® Windows® Server 2012

- Microsoft® Windows® 10 Pro
- Microsoft® Windows® 8.1 Pro
- Microsoft® Windows® Server 8.0
- Microsoft® Windows® 7 Professional, SP1

Mobile Operating Systems

- iPad Tablet: iOS 11.0
- Android: version 6.0 or higher

For iPad tablets, you must install the CA certificates on the iPad clients to establish a trusted connection and to receive live data.

Server Operating Systems

- Microsoft® Windows® Server 2016 Standard
- Microsoft® Windows® Server 2012 R2 Standard
- Microsoft® Windows® Server 2008 R2 Standard, SP1
- Microsoft® Windows® Server 2008 R2 Enterprise, SP1
- Microsoft® Windows® 10 (64-bit only)
- Microsoft® Windows® 7, SP1 (64-bit only)

Hardware Requirements

Mobile devices, clients, and servers must meet the following hardware requirements to work with Web HMI.

Mobile Devices

- Android Tablet: Minimum Dual Core 1.7 GHz, 1 GB RAM
- iPad Tablet: Third generation or greater

Client Specifications

- 2.0 GHz Intel® Core™2 Duo Processor
- 4 GB (minimum), 8 GB (recommended)

Server Specifications

- Core i7: 4 Core Processor
- 8 GB (minimum), 16 GB (recommended)

Compatibility Matrix

Several GE Digital products work with Web HMI to provide real-time and historical data.



Important:

- It is recommended that you do not run another server on the same machine as Web HMI.
- When using multiple servers, such as iFIX, Workflow, and Web HMI, the time must be synchronized among the servers.

GE Digital Product	Required Version
CIMPLICITY	<ul style="list-style-type: none"> • CIMPLICITY 10.0 with SIM 3 • CIMPLICITY 10.0 with SIM 2 • CIMPLICITY 10.0 with SIM 1 • CIMPLICITY 10.0
iFIX	<ul style="list-style-type: none"> • iFIX 5.9 • iFIX 5.8 with iFIX58_SP2 and SIMs iFIX58_HPDynamicos_001, iFIX58_ExportJSON_002, and iFIX58_Blocks_001
Historian Client Tools	<ul style="list-style-type: none"> • Historian 7.0 SP5 • Historian 7.0 SP1 • Historian 6.0 SP1 with SIM 5 • Historian 5.5 with SIM 29
Workflow	<ul style="list-style-type: none"> • Workflow 2.6

Kiosk Mode

Kiosk mode is a Windows® operating system feature that allows only one application to run at a time. This mode locks down a device to be used for a particular task only.

In Web HMI, you can use kiosk mode to restrict user access within a web browser window to specific features, such as the toolbar and full-screen mode.

For information on implementing kiosk mode, see the online documentation of the related browser.

Resolved Issues


The following issues were resolved in Web HMI 2.2 SP2.

Issue	Description of Solution
DE44065: User and password checks shown in the bootstrapper logs require better formatting for usability.	The bootstrapper now logs user and password checks in an easy-to-read format.
DE49326: An unclear warning message appears during the Web HMI installation.	An accurate warning message now appears during the Web HMI installation.
DE61325: For Boolean editable fields on mimics, you must type a value.	You are now presented with a drop-down window to select values for Boolean editable fields on mimics.
DE62478: In Control Cards, you cannot select a separate HMI/SCADA data variable tag as a Control Point (Set-Point).	A Control Point can now be a separate variable tag. For example, TargetTemperature is the Control Point for ActualTemperature. If you modify the temperature of TargetTemperature, ActualTemperature gradually changes to that temperature.
DE66614: In Control Cards, the drop-down list window for the Attribute column does not work in Microsoft Edge.	The drop-down list window for the Attribute column is now working in Microsoft Edge.
DE82050: Assets deleted from the Model Editor remain in the Web HMI Runtime navigation hierarchy. As a result, the Runtime navigation hierarchy is out of synch with the Web HMI Asset Model.	The Runtime navigation hierarchy is now in synch with the Web HMI Asset Model. You no longer have to manually remove all assets from the Runtime navigation hierarchy that were deleted from the Model Editor.
DE89913: When Web HMI cannot reach a connected Workflow server, its responsiveness slows down considerably.	The timer intervals are now set to greatly improve the responsiveness of Web HMI.
US239904: A click zone on a mimic cannot relatively reference a child object.	Click zone navigation allows for both absolute and relative paths for click targets at the object type and the object level.

Known Issues

Review these limitations before installing and using Web HMI.

Issue	Description
DE25299: Cannot install Web HMI on Windows 7 and Windows 2008 R2, generates message "Microsoft .NET Framework required for Web HMI setup."	Your system requires Microsoft .NET Framework 3.5.1 and Microsoft .NET Framework 4.5.2. For installation instructions, see the Microsoft documentation.
DE16140: Mimic Card bindings cannot load.	When a mimic is bound to any asset type with child or descendant properties of that same asset type, Web HMI cannot load the mimic card bindings. For example, if you assign an asset type called "Area" to a child property with the same asset type (such as a contained "Area" within an "Area"), or assign a child property of any asset type with a child of type "Area," a failure to load message appears. Do not bind any asset type to child or descent properties with that same asset type.
DE40294: Real-time data for hard-coded enterprise points does not display in Web HMI.	The CIMPLICITY OPC UA server does not support enterprise points. As a result, the data for an enterprise point does not appear in any Web HMI Runtime displays.
DE41516: Unusual behavior when using the zoom functionality on iPad and Android tablets.	On mobile devices, the pinch gesture does not work on Trend charts.
DE42170: iFIX unable to write data or acknowledge alarms due to non-default Tomcat port.	If using Web HMI with iFIX and Web HMI does not use the default Tomcat port (8443), such as when Historian 7.0 is installed before Web HMI. In this scenario, iFIX cannot connect to the Web HMI authentication service to validate the user credentials required for data writes and alarm acknowledgements, causing all writes and acknowledgements to fail. To resolve this, see iFIX Issues (on page 115) .
DE42474: When iFIX is installed after Web HMI (not recommended), you may receive this message "iFIX not running! OPC AE Server unable to start."	Start iFIX so the Alarm Gateway can connect to the OPC AE server.

Issue	Description
DE43686: Real-time data type not plotting when range exceeds certain thresholds.	When the underlying CIMPLICITY point value exceeds certain thresholds, the Trend chart cannot plot the point. The valid range is approximately -2.064210e298 to 2.496796e306.
DE44401: Direct connect to an endpoint fails, receive Bad Security Checks Failed (cannot connect to server) error message.	When CIMPLICITY is configured to use a Global Discovery Server, you must register the Web HMI server to the same GDS.
DE45285: Upgrading to a different path fails.	To retain your model and configuration data, install Web HMI to the same location as the earlier version of Web HMI. If you installed Web HMI to a different location, do the following: <ol style="list-style-type: none"> 1. Uninstall Web HMI. 2. Install Web HMI to the same location as the earlier version. 3. Verify that data is flowing in the model.
DE46040: Incorrect alarms appearing for HMI/SCADA server (CIMPLICITY or iFIX).	When you change the server name (Uniform Resource Name (URN)) in Administration > Set Up > Server , this change is not reflected in alarm views. In Runtime, you continue to see alarms from the previous server source.
DE47669: When importing a model containing a second CIMPLICITY namespace table, it overwrites the values in the first namespace table.	Combine the server and namespace information from the two namespace tables in to one namespace table, and then import the model again.
DE47858: Alarm Card shows partial connection () to an iFIX alarm source that is no longer installed on the Web HMI server.	An artifact left from the iFIX installation results in the Alarm Gateway trying to connect to the iFIX OPC A&E server to retrieve alarms, and fails because it is not on the system. To resolve this, see iFIX Issues (on page 115) .
DE61322: Boolean labels from CIMPLICITY are not reflected on Web HMI Mimic Cards.	Boolean labels, such as open and close, display as 0 and 1 on mimics. When updating these CIMPLICITY values on mimics, you must specify 0 or 1.
DE62478: When upgrading from Web HMI 2.0 with a defined Control Point (SetPoint), the At-	In the Administration environment, you must configure the setpoint attribute and any other required attributes on the Control Card. To do

Issue	Description
tribute column on the Control Card defaults to none. As a result, the Mimic Control View does not display any attributes at Runtime.	this, navigate to Visualizations > Designer , and then select the Control Card settings for the object type.
DE65198: When you hover over a CIMPLICITY value that you can update on a Mimic Card, only some of its characters are highlighted in blue. Web HMI does not highlight the characters on the opposite side of the value's justification.	Hover over the highlighted characters and type the new value.
DE71418: A user removed from a Web HMI Admin group in an Active Directory Domain remains a member in a Administrator group.	After the administrative privileges are revoked for a user in an Active Directory Web HMI Admin group, that user should automatically be removed from its mapped Web HMI Administrator group.
DE76871: During a Windows installation, the Windows Defender Firewall blocks the erl and epmd apps.	Select Allow access to provide access to these apps.
DE79766: Web HMI 2.1>2.2 SP2 upgrade may fail on some systems because the PostgreSQL service is unable to start.	<p>The PostgreSQL service is not running but its processes are still executing. You must stop the main PostgreSQL service by following these steps:</p> <ol style="list-style-type: none"> 1. Read the number from the beginning of <code>C:\Program Files\PostgreSQL\9.4\data\postmaster.pid</code>, up to the file path, to determine the PID for the main PostgreSQL process. 2. Execute <code>pg_ctl kill INT <PID></code> in the command line, replacing the <code><PID></code> with the one found in step 1. 3. Restart the PostgreSQL service.
DE80295: Reimporting a model fails on first attempt.	In some systems, this can happen. Import the model again.

Chapter 2. Get Started with Cimplicity and Web HMI

Get Started with CIMPLICITY and GE Web HMI

When using the CIMPLICITY HMI/SCADA system as your data source, follow this quick walkthrough to successfully get data and alarms flowing for the first time into Web HMI.

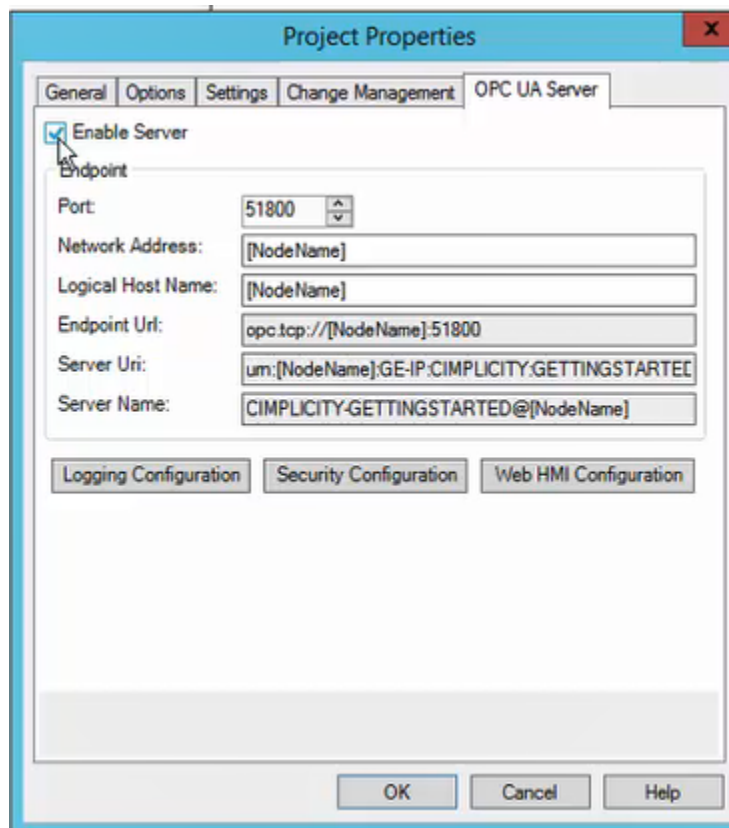
This procedure assumes you are familiar with creating CIMPLICITY projects and points as well as the fundamentals of building models and using mimics in Web HMI (as described in this help).



Note:

For detailed integration instructions, see *Integrating CIMPLICITY with Web HMI* in the CIMPLICITY help.

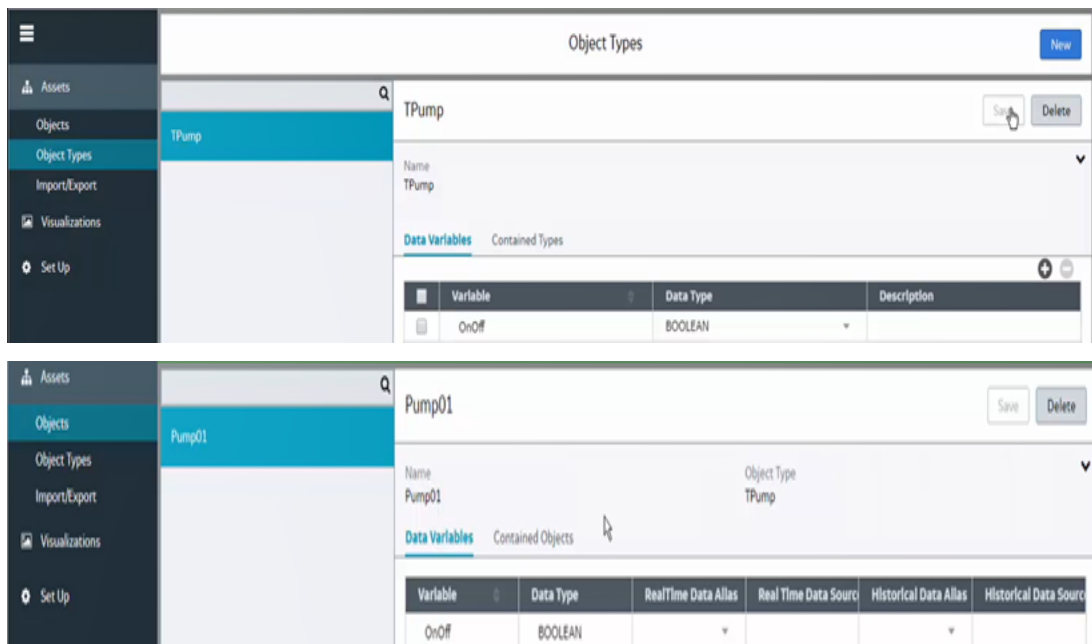
1. Install CIMPLICITY 10 and Web HMI on different servers or on the same server.
2. In CIMPLICITY, do the following:
 - a. Create a project.
 - b. Check **Enable Server** (OPC UA), as shown below:



- c. Verify there is a connection to the Web HMI server on **Web HMI Configuration**.
- d. Enable security on **Security Configuration**.
For this exercise only, select None.
- e. In the project, create a TPump class with an alarm enabled.
- f. Create a Pump01 object that corresponds to the class.
- g. Start the project.

3. In the Administration section of Web HMI, do the following:

- a. Define a model by creating a TPump object type with an OnOff variable and a Pump01 object to match the class and object created in CIMPLICITY, as shown below:



- b. Set up the Web HMI server to CIMPLICITY project connection by selecting **Set Up** and setting these values on the **Server Details Management** screen:

Server Alias	CIMPLICITY project name.
Server Type	OPCUA.
Server Name	CIMPLICITY Uniform Resource Name (URN) of the server. You find this URN in CIMPLICITY by selecting Export to Web HMI on the Project menu to generate a

CSV containing this value. The following shows a sample URN value in the last line:

```
#ServerDetails,ServerAlias,ServerName,ServerType
ServerDetails,GETTINGSTARTED,urn:CC-AUTO-CHADDEV:GE-IP:CIMPLICITY:GETTINGSTARTED,OPCUA
```



Note:

You can also find the URN on the **OPC UA** tab of the **Project Properties** screen.

- c. Return to the asset object that you created on the **Objects** screen and specify the CIMPLICITY project in **RealTime Data Alias** and the project's point in **RealTime Data Source**, which you can find in the CSV file. The following shows a sample CSV file highlighting the RealTime data source, followed by the **Objects** screen with the same data source value:

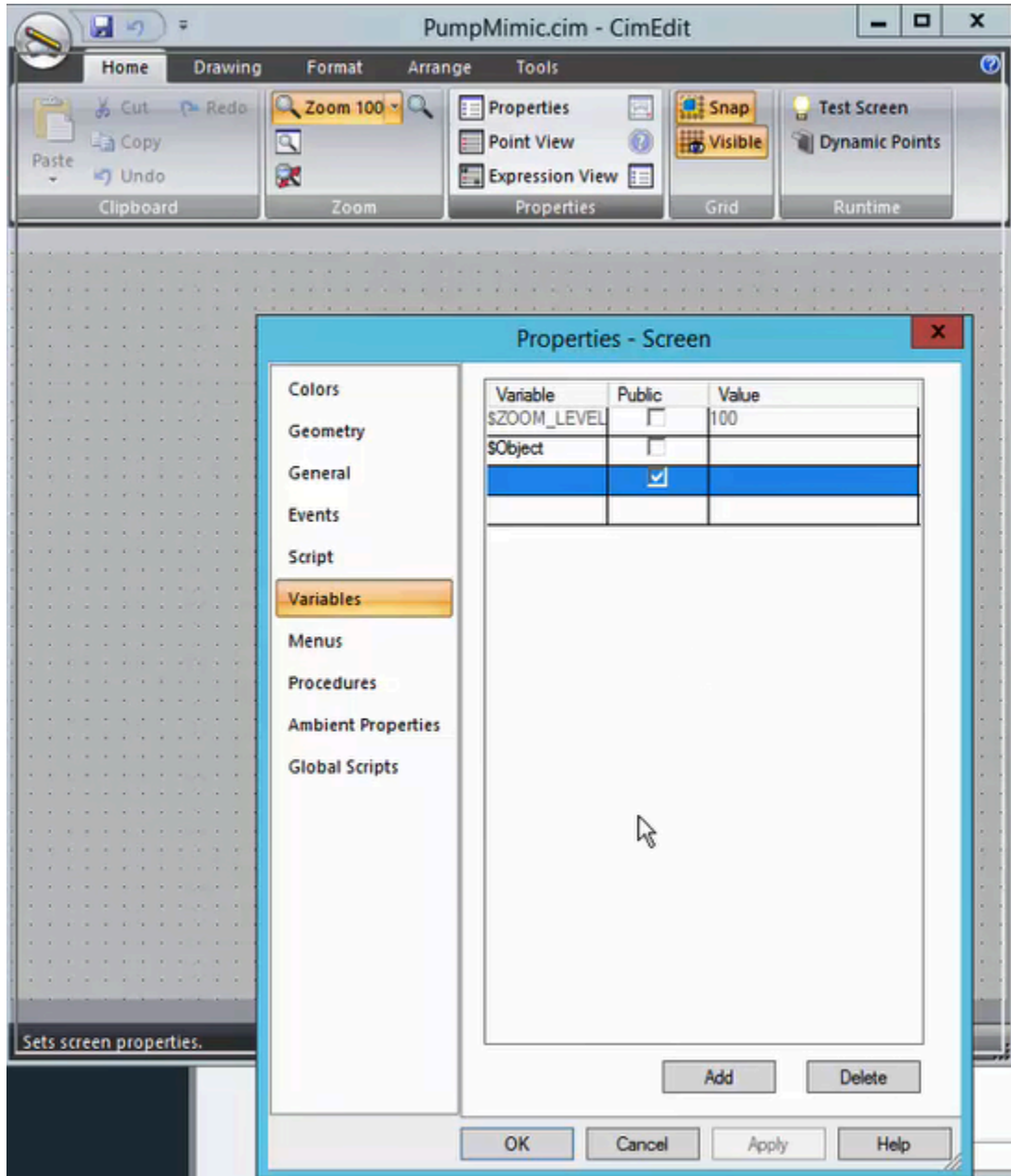
```
DateTime,2017-10-10T16:45:20.4639-07:00
TagGroupVersion,1

#ServerDetails,ServerAlias,ServerName,ServerType
ServerDetails,GETTINGSTARTED,urn:CC-AUTO-CHADDEV:GE-IP:CIMPLICITY:GETTINGSTARTED,OPCUA

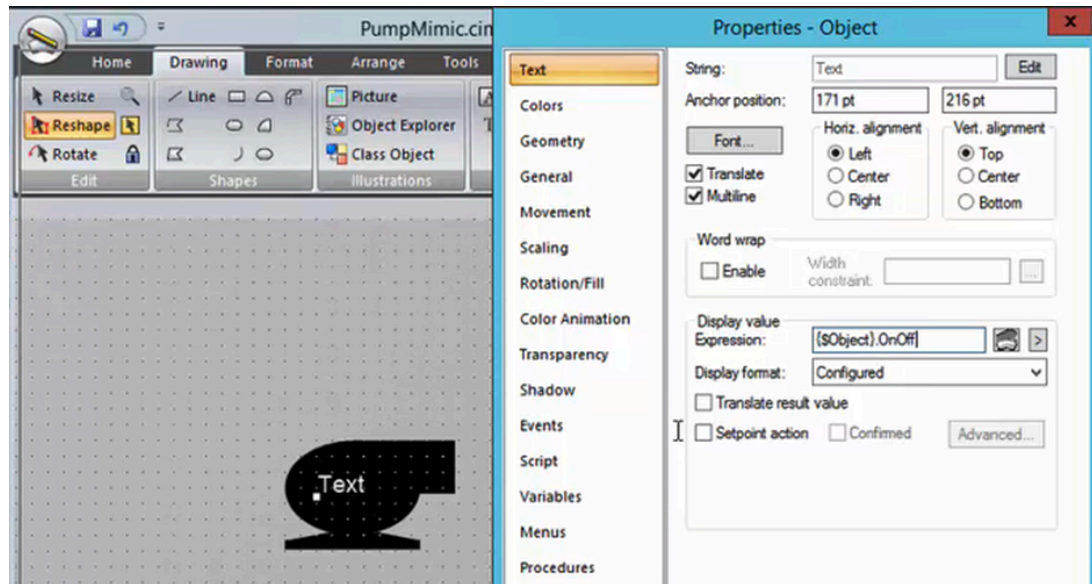
#NamespaceTableHeader,ServerAlias,NamespaceIndex,Namespace
NamespaceTable,GETTINGSTARTED,2,http://ge.com/ua/CIMPLICITY
NamespaceTable,GETTINGSTARTED,3,http://ge.com/ua/CIMPLICITY/GETTINGSTARTED
NamespaceTable,GETTINGSTARTED,4,http://ge.com/ua/CIMPLICITY/GETTINGSTARTED/project
#TagGroupHeader,TagGroupName,DataType,Description,RealtimeServerAlias,RealtimeDataSourceName,HistoricalServerAlias,HistoricalDataSourceName
TagGroup,PUMP01.OnOff,BOOLEAN,,GETTINGSTARTED,ns=3;s=PUMP01.ONOFF.Value,,
```

Variable	Data Type	RealTime Data Alias	Real Time Data Source	Historical Da	Historical Da
OnOff	BOOLEAN	GettingSta	ns=3;s=PUMP01.ONOFFValue		

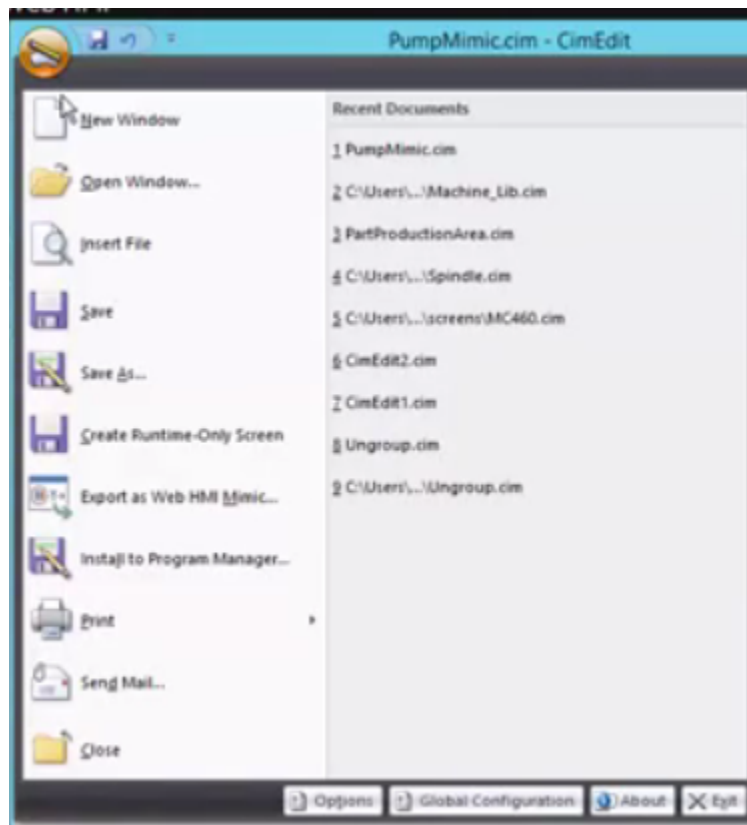
- 4. In CIMPLICITY, do the following:
 - a. Create a visual representation (PumpMimic) of the TPump on the CimEdit screen.
 - b. On **Properties**, type \$object in the **Variable** column. CIMPLICITY uses this value to reference the context in the Web HMI model, which is the TPump in this example.



- c. On **Text**, type `($Object).OnOff` in the **Display value Expression** field. This value represents the OnOff value on the TPump object type in the Web HMI model.

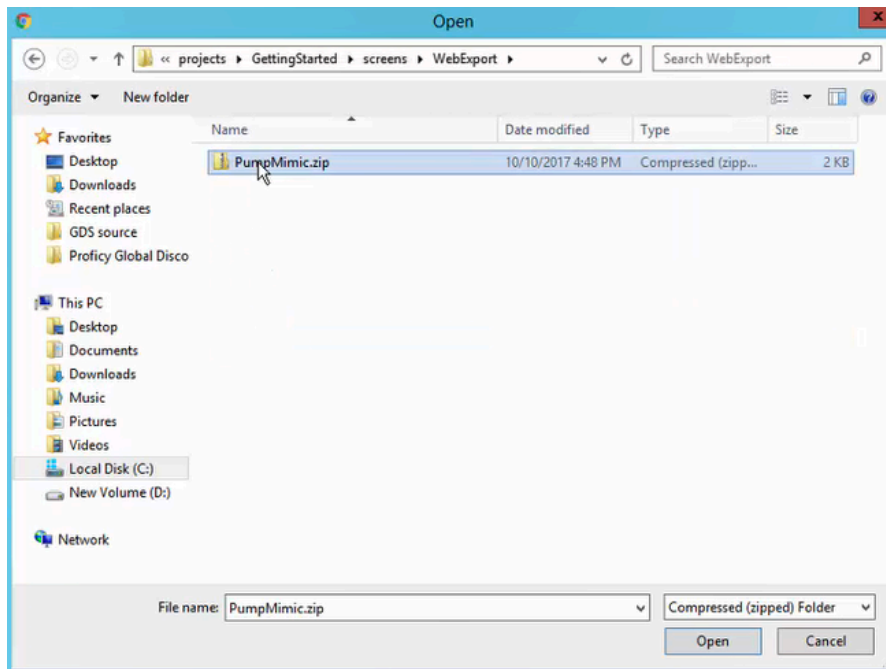


d. Export the mimic into a Web HMI format by selecting **Export as Web HMI Mimic**:

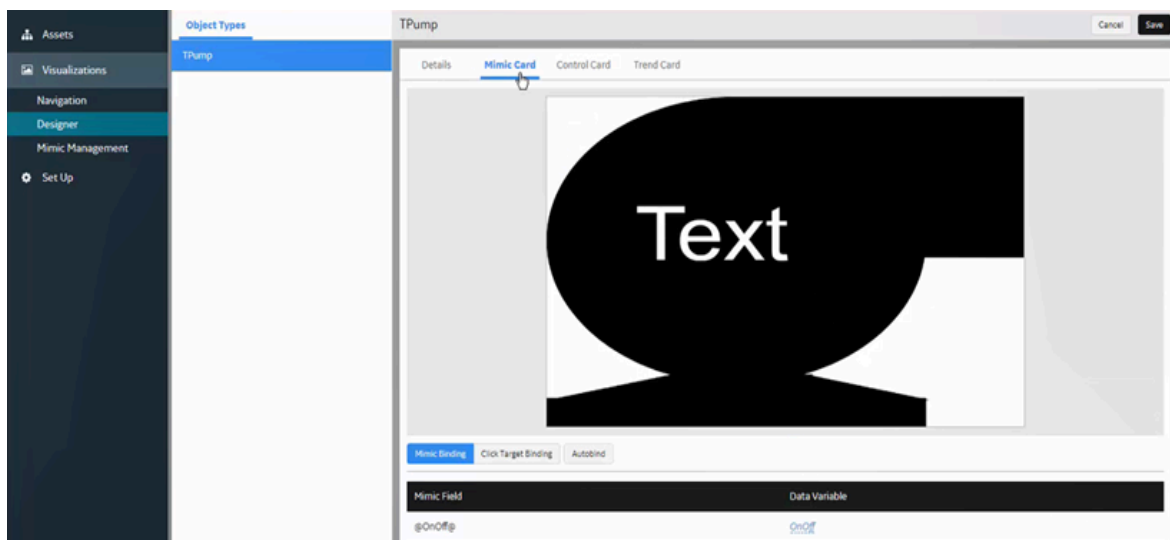



5. In the Administration section of Web HMI, navigate to **Visualizations > Mimic Management** to do the following:

a. Import the mimic:

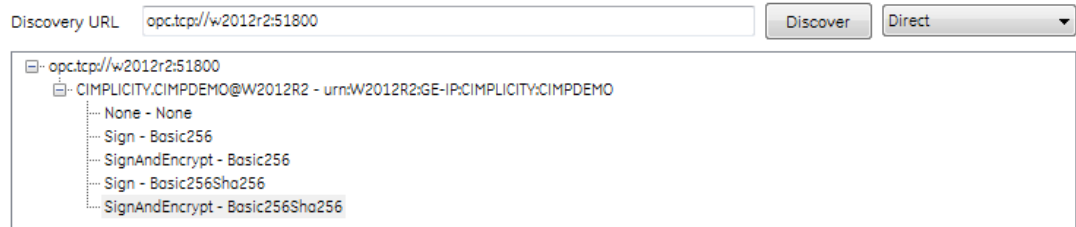


b. Under **Designer**, associate the mimic to the TPump object type:



6. Click  on your desktop to open the GE HMI Server Configuration Manager, and click the **OPC UA Endpoints** tab to do the following:

- a. Discover and select an OPC UA endpoint and its security. The following shows a CIMPLICITY endpoint with its available security options found at the w2012r2:51800 URL:



- b. and then configure its security connection to Web HMI. .

7. In the Runtime section of Web HMI, check to see if data and alarms are appearing in the correct context.

Chapter 3. Get Started with iFIX and Web HMI

Get Started with iFIX and Web HMI

When using the iFIX HMI/SCADA system as your data source, follow this workflow to successfully get data and alarms transferring in to Web HMI for the first time.

For a listing of iFIX objects supported by Web HMI, see the *Web HMI Element Support* section in the iFIX help.

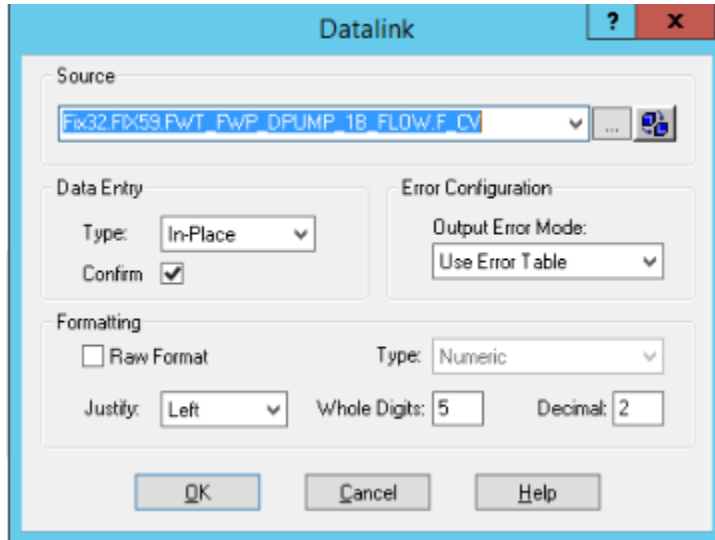
1. First install iFIX, and then install Web HMI on the same server.
2. Check the Task Configuration list of the iFIX System Configuration Utility (SCU) to verify these programs are installed on the Web HMI server:
 - a. AlarmGateway.exe: Subscribes to OPC alarm and event messages from the iFIX OPC AE server and posts them to the RabbitMQ service for the Alarm microservice to manage.
 - b. DataDistributor.exe: Routes data requests to the proper source and efficiently returns the requested data.



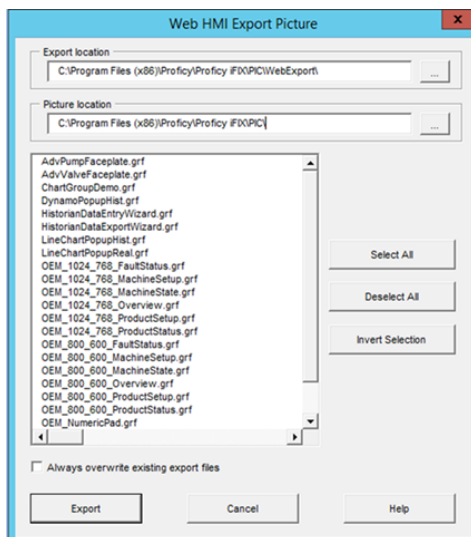
Note:

Scadastat.exe is deprecated. You may still see it running during a Web HMI upgrade as an iFIX task. This does not impact iFIX and you can safely remove it from the iFIX SCU.

3. Verify that iFIX SCU Network Configuration on the Web HMI server has networking enabled and the remote SCADA nodes (if any) display in its remote node list.
4. Launch the Web HMI shortcut on the desktop to load the default Web HMI URL in your browser and load Web HMI Runtime. If security warnings appear, verify that your browser meets the minimum requirements and the appropriate CA certificates are installed.
5. In iFIX, do the following:
 - a. Create pictures supporting the Web HMI objects. To make an object a click target in a Web HMI mimic, set its `is_selectable` property to `true`.
 - b. To enable a Web HMI operator to update an iFIX data source tag on a picture and answer an update confirmation question, access the **Datalink** screen and select the source tag. In the **Data Entry** section, select In-Place in the **Type** field, and then select the **Confirm** check box, as shown below.

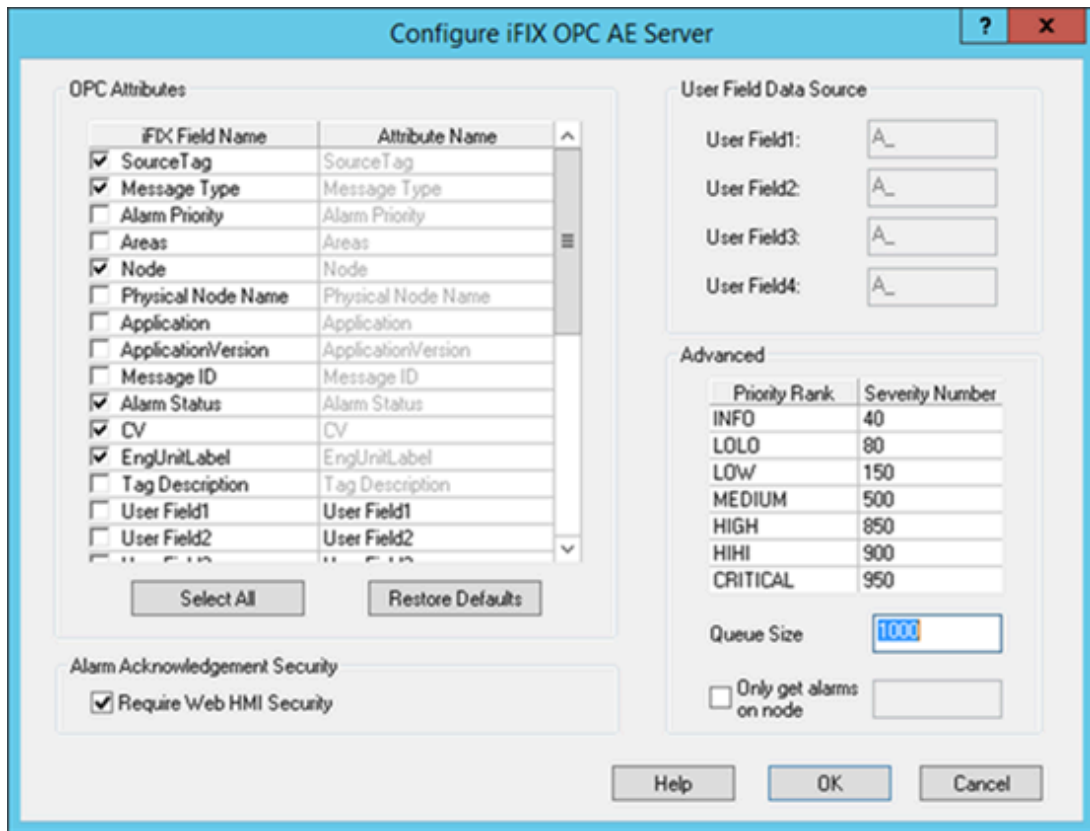


- c. In the iFIX Tools Ribbon, select **Web HMI Export Picture** to export selected pictures in GRF format in to a Picture folder as shown below. These GRF files are exported in to JSON ZIP files. These pictures become mimics (process diagrams) that you associate with asset object types in Web HMI.



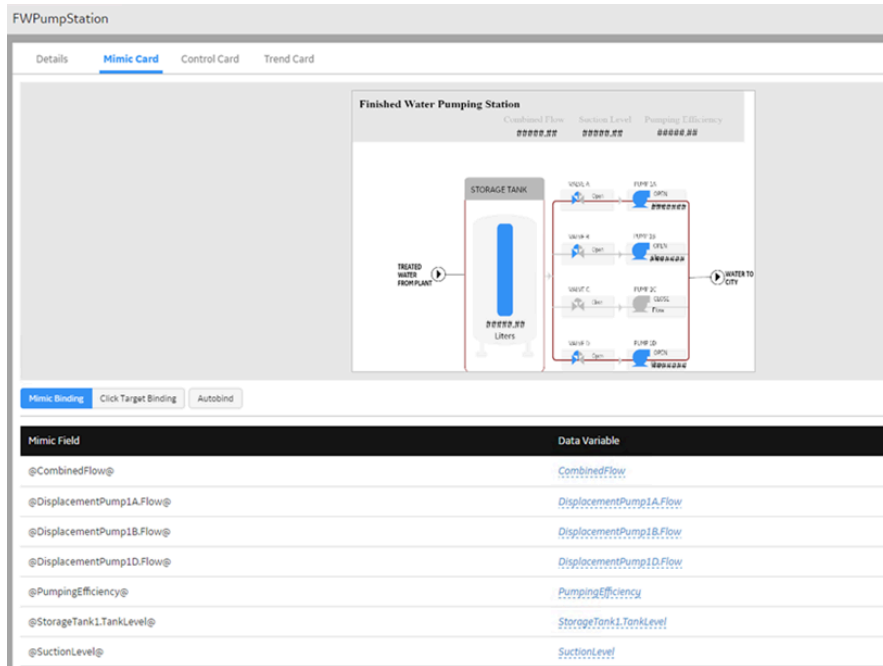
- d. Verify the values in the **Advanced** section of the **Configure iFIX OPC AE Server** screen conform to the OPC A&E specification guidelines and use the Web HMI default dividing point values to separate the alarm severity ranges, as explained in [Alarm Microservice \(on page 99\)](#).

The following provides a sample **Configure iFIX OPC AE Server** screen.

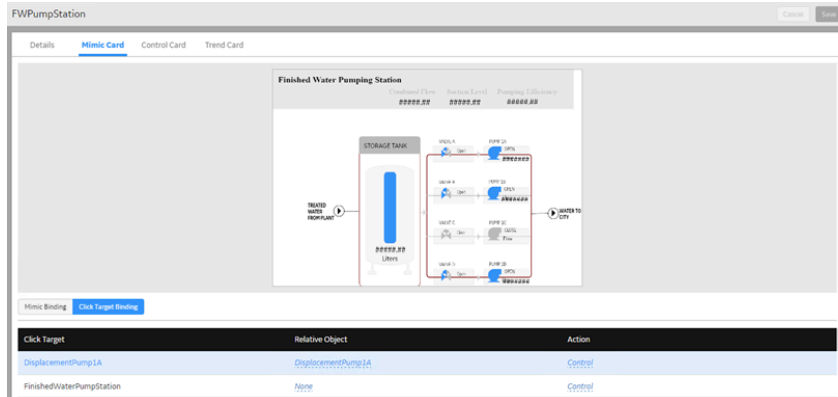


6. In the Web HMI Administration environment, perform the following tasks:

- a. Build the Runtime structure and navigation by creating a model.
- b. Import the pictures (mimics) in JSON format.
- c. Bind the imported mimics to asset object types in the model using the object type list. The following shows the mimic fields bound to the data variables of the Finished Water Pumping Station object type:

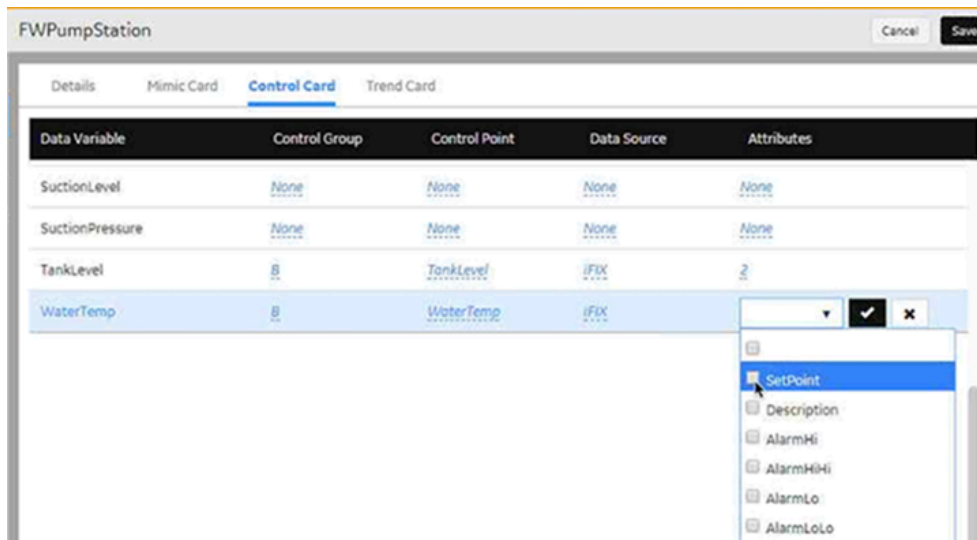


- d. Set up the navigation of mimic click targets. You define the click target to navigate to any asset in the model or to open a Control View where an operator can modify HMI/SCADA real-time values (if permitted in the HMI/SCADA source) and view historical data. In the following example, the FW Pump Station is set with a Control Action to open a Control View when an operator selects the DisplacementPump1A object in the mimic.

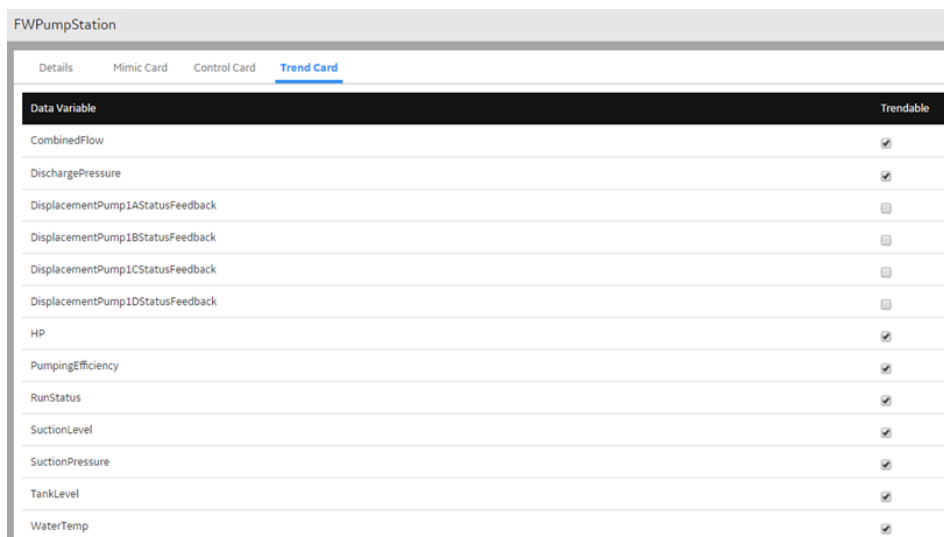


- e. Define the content for Control Views on the Control Cards. You can group related asset data variables together to appear in a Control View by specifying a group identifier in the Control Group column. In this example, the TankLevel and WaterTemp variables are grouped together, and both have Control Points that enable an operator to modify their current values in iFIX. Both TankLevel and WaterTemp are acting as their own Control Points, which means an operator is writing to and reading from the same variable tag. In some instances, a Control Point can be a separate variable tag. For example, TargetTemperature is the

Control Point for ActualTemperature. If you modify the temperature of TargetTemperature, ActualTemperature gradually changes to that temperature.



f. Select the data variables of an asset object type to appear as trend lines in a Trend Card, as shown below:



Note:

For detailed information about the above tasks, see *Develop Runtime Content*.

7. Switch to Runtime to view data and alarms appearing in the correct context and cards.

If iFIX is unable to write or acknowledge alarms, check the `secmgr.cclr.dll.config` file in the iFIX install folder on the SCADA node to verify it contains the correct host or port for the Web HMI server.

Chapter 4. Get Started with Workflow and Web HMI

Get Started with Workflow and Web HMI

When using Workflow, follow these steps to display interactive task lists in Web HMI Runtime for the first time.

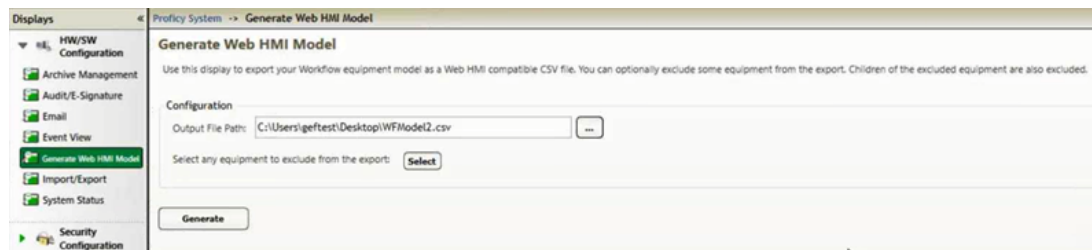
Verify the following:

- The administrator integrating Workflow must have the same credentials in both the Web HMI server and the Workflow server.
- The task lists using HTML5 forms were created in Workflow to appear in the Web HMI Task List Card.
- The time is synchronized among the servers being used.

1. Install Workflow 2.6 and Web HMI on different servers.

2. In the Workflow server, do the following:

- a. After creating the Workflow equipment model, you must convert it to the required .cvs file format before importing it to Web HMI. This model also includes the Workflow server information. To convert the model, navigate to **Proficy System > Proficy System > Generate Web HMI Model**, as seen in the following image.



- b. Set up access to the Web HMI server by selecting the **Web HMI Access** checkbox, and then entering the **Web HMI Host Name** in **General Electric > Configure Security > Security**, as seen in the following image.

Security

Name

Password

Confirm Password

Advanced user authentication settings:

Use SSO (Single Sign On)

Allow users to change password

Enforce user lockout

Enforce user password complexity rules

Web HMI Access

Web HMI Host Name

Save Exit

c. Select **Save**.

A message appears indicating that the configuration changes were successfully saved.

3. In the Workflow server, export the certificate required to communicate with the Web HMI server and clients by following these steps:
 - a. Select **General Electric > Workflow > Configuration > Export Certificates**.
 - b. In the **Export Folder** box, enter the path or navigate to the location in which to export the .zip file containing the certificate.
 - c. In the **Password** box, enter a password to secure the exported certificate, and to use when placing the certificate in a trust store.
 - d. Select **Save**.



A .zip file named `ExtensionServerCertificates.<WorkflowServerName>.zip` is created with the `ProficySelfSignedCA` certificate. You must place this certificate in the trust store of the Web HMI server and each Web HMI client, as explained in the following step.



Note:

Mobile iPad devices also require the `ProficySelfSignedCA` certificate, and have specific instructions to install this certificate. See [Install Workflow Certificate in iPad Clients \(on page 41\)](#).

4. Place the Workflow `ExtensionServerCertificates.<WorkflowServerName>.zip` file in the Web HMI server and each Web HMI client, and then follow these steps to add the certificate to each one of their trust stores:
 - a. Extract the the ProficySelfSignedCA certificate from the .zip file to a folder.
 - b. Open a Windows Command Prompt window, and then enter mmc.
The Microsoft Management Console appears.
 - c. Select **File > Add/Remove Snap-in...**
 - d. In the **Available snap-ins** pane, select **Certificates**, and then select **Add**.
 - e. Select **My user account**, then select **Finish**, and then select **OK**.
 - f. Select **Expand Certificates - Current User > Trusted Root Certificate Authorities > Certificates**.
 - g. Right click **Certificates**, then select **All Tasks**, and then select **Import**.
The Certificate Import Wizard appears.
 - h. Select **Next**.
 - i. In the **File Name** box, select **Browse**, and then select the ProficySelfSignedCA certificate that was extracted from the .zip file.
 - j. Select **Next**.
 - k. When prompted, enter the password set in step 3c to secure the certificate.
 - l. Select **Next**.
 - m. Select **Place all certificates in the following store**.
 - n. Select **Browse**.
 - o. Select **Trusted Root Certificate Authorities**.
 - p. Select **Next**, and then select **Finish**.
 - q. Close all browser instances.
 - r. Restart the browser.
5. In the Web HMI Administration environment, do the following:

- a. Import the Web HMI model file created in step 2a to Web HMI by navigating to **Assets > Import/Export**, as explained in [Import the Model \(on page 62\)](#).
 - b. Verify the Workflow server information was imported to Web HMI in **Set Up > Server > Server Details Management**, as explained in [Set Up Data Source Servers \(on page 55\)](#).
6. In Application Assembler, set up a few user accounts for testing purposes.
7. In the Web HMI Runtime environment, do the following:
 - a. Verify Web HMI is connected with the Workflow server. If not connected,  appears in the main navigation bar.
 - b. Verify tasks are assigned to the correct users within the equipment or process context. The number of tasks assigned to a user appears next to the task list icon in the main navigation bar. For example,  indicates there are two tasks for a user.

Chapter 5. Install and Upgrade

Prerequisites

Before installing or upgrading Web HMI, verify the following software is installed on your system.



Note:

Run Windows Update (including security updates) before installing or upgrading Web HMI.

- .NET Framework 3.5
- GE Historian Client tools (if using Historical data):
 - Historian 7.0 SP5 (for Historian 7.0)
 - Historian 7.0 SP1 (for Historian 7.0)
 - Historian 6.0 SP1 SIM 5 (for Historian 6.0)
 - Historian 5.5 SIM 29 (for Historian 5.5)

iFIX HMI/SCADA System



Important:

If using iFIX for your HMI/SCADA system, it is strongly recommended that you install it before installing Web HMI. If you do not, you must start the Data Service Configuration tool after installing iFIX, as explained in [Run the Data Service Configuration Tool \(on page 34\)](#).

Web HMI works with iFIX 5.9 or 5.8. If installing iFIX 5.8 on your system (HMI/SCADA or View Node, as required), install its software in this order:

- GE iFIX 5.8
- GE iFIX 5.8 SP2
- GE iFIX58_HPdynamos_001
- GE iFIX58_ExportJSON_002
- GE iFIX58_Blocks_001

Licensing

Read the following before installing or upgrading Web HMI:

- Some operating systems require that you install Microsoft KB2999226 before installing Common Licensing.
- If you are using Windows 7 and Windows Server 2008 R2, you must install SP1 before installing KB2999226.
- If you are using Windows Server 2012 R2, you must install KB2919442 and then KB2919355 before installing KB2999226.
- If you are using Windows 8.1, you must install KB2999226.
- Activating licenses from the GE Cloud Server onto Windows XP SP3 or Windows Server 2003 SP2 computers is no longer supported.

Install Web HMI

Follow this procedure if you are installing on a fresh Windows system.

- Only install Web HMI on operating systems supporting the English language.
- Run Windows Update (including security updates) before installing Web HMI.
- If using iFIX, verify that it is installed before installing Web HMI. Otherwise, you must run the Data Service Configuration tool.
- Do not install Web HMI on a host machine with a name containing underscores (_), percent signs (%), or pound symbols (#). Valid characters in the host name (up to 24 characters) can contain letters from the alphabet (A-Z), digits (0-9), the minus sign (-), and the period (.). For more information, see Microsoft KB article 149044. You cannot add a percent sign, pound sign, or underscore to the DNS Host Name.
- Install Web HMI on a Windows system without any applications already bundled with Web HMI. If applications, such as PostgreSQL and RabbitMQ, are installed, you must remove them before proceeding.



Note:

Some applications like PostgreSQL require you to manually remove the PostgreSQL folder in Program Files to completely uninstall it.

- If a VM screen appears frozen when installing Web HMI, click on it to view information about the installation. This typically occurs after 15 minutes of inactivity.
1. Start the installation program.
If the installation fails on Microsoft Windows 7 or Windows 10, right-click the installation program and select **Run as Administrator**.
 2. In the **Welcome** screen, select **Next**.

3. In the **License Agreement** screen, select **Accept**, and then **Next**.
4. In the **Configure Install Path** screen, select **Browse** to choose the installation directory path or accept the default path.
If you are not using the default installation path, make sure the path does not exceed 32 characters.
5. In the **Configure Host and Port** screen, define which URLs (host names or IP addresses) can be used by a browser to connect to Web HMI. For more information, see [Connections based on URLs \(on page 34\)](#).

Option	Description
IP address (required for mobile devices)	<p>You must use the IP address format of <servername>;<IP address>, where no spaces are in the servername or before or after the semicolon (;).</p> <p>Example: HMIWebServer;1.1.11.21</p> <p>You can add additional IP addresses known by the host using a semicolon, but these are not checked for accuracy.</p> <p>Example: HMIWebServer;1.1.11.21;2.2.12.22;3.3.13.33</p>
Host name	Example: w2012r2

For external Web HMI clients to connect to Web HMI, enable port number 443 or the port that you are using for the GE Web HMI installation in the incoming firewall rules.

6. Select **Next**.
7. In the **Configure PostgreSQL** screen, enter a new administrator password for PostgreSQL.
Record this new password, as you will need it to reinstall or upgrade.
8. In the **Configure GE Administrator User** screen, enter a user name and a password (10-character minimum) for your GE Administrator user.
A user name can contain alphanumeric characters (at least one), hyphens, periods, underscores, email addresses, and spaces. It cannot start or end with a space. You cannot create the following user names: Administrator, GEAdmin, GEUser, gePeMsUser, System, and SuperUser.
Record this user name and password, as you will use this user account to log in to Web HMI for the first time.
9. In the **Ready to Install** screen, select **Install**.
If a Progress screen appears, select **Next** and wait for the final screen to appear.
The program installs Web HMI and its associated software.
10. Select **Exit** when the installation completes.

Install the CA certificate, as explained in [Install CA Certificates \(on page 40\)](#).

Connections based on URLs

You define which URLs a browser can use to connect to Web HMI. This is particularly useful for mobile devices without access to DNS lookups.

You defined the list of acceptable URLs in the Host Name fields on the **Configure Host and Port screen** during installation. For example, if w2012r2 was entered as a host name, Web HMI will accept a connection request from `https://w2012r2/WebHMI/login.html`. The host values, which can also be IP addresses, are stored in the Reverse Proxy configuration file (default location: `C:\Program Files\Proficy\ProficyWebServer\ReverseProxy\serverConfig.json`). You can update this list in the host name field of the `serverConfig.json` file.



Note:

The HTTPS certificate for secure communication to Web HMI also uses these values.

Run the Data Service Configuration Tool

If you installed Web HMI before you installed iFIX, you must run the Data Service Configuration tool.

1. Navigate to `<install_path>\DataAcquisition\DataServiceConfig`.
2. To run the tool, type: `DataServiceConfig.exe --auto --dataexepath "C:\Program Files(x86)\Proficy\DataAcquisition\DataDistributor\DataDistributor.exe" --alarmexepath "C:\Program Files\Proficy\AlarmGateway\AlarmGateway.exe" --oauthport 8443`

This command assumes the default installation path, uses quotes because of spaces within the command, and uses the Tomcat server port, 8443.

Upgrade Web HMI

When installing Web HMI 2.2 SP2 on a machine that previously had an earlier version, the upgrade process automatically backs up existing PostgreSQL databases as well as the model and server data.

The Web HMI upgrade paths are:

- 2.0>2.2 SP2
- 2.1>2.2 SP2
- 2.2>2.2 SP2

 **Important:**

- To retain your model and configuration data, install Web HMI to the same location as the earlier version of Web HMI.
- If you modified any Web HMI components, such as mashups, and added menu links in Application Assembler (ThingWorx), these changes are overwritten during this upgrade. Any mashups that you added are not removed. Before upgrading, go to [Back Up Customized Components \(on page 36\)](#).

- Uninstall the earlier version of Web HMI.
- Run Windows Update (including security updates) before upgrading Web HMI.
- If using iFIX, do the following:
 - Start the iFIX System Configuration Utility (SCU).
 - Navigate to **Configuration > Tasks** to delete the tasks for Scadastat.exe, AlarmGateway.exe, and DataDistributor.exe, and then select **OK**.
 - Close the SCU and select **Yes** to save the changes.
 - If installing Web HMI on the same machine as iFIX, you must stop iFIX before installing Web HMI.
- Install all required software that is not already installed.
- Have your existing administrator passwords for Web HMI and PostgreSQL ready. You are asked for these during the upgrade.
- If a VM screen appears frozen when installing Web HMI, click on it to view information about the installation. This typically occurs after 15 minutes of inactivity.

1. Start the installation program.

If the installation fails on Microsoft Windows 7 or Windows 10, right-click the installation program and select Run as Administrator.

2. In the **Welcome** screen, select **Next**.

3. In the **License Agreement** screen, select **Accept**, and then **Next**.

4. In the **Configure Install Path** screen, select **Browse** to choose the installation directory path or accept the default path.

If you are not using the default installation path, make sure the path does not exceed 32 characters.

5. In the **Configure Host and Port** screen, define which URLs (host names or IP addresses) can be used by a browser to connect to Web HMI. For more information, see [Connections based on URLs \(on page 34\)](#).

For external Web HMI clients to connect to Web HMI, enable port number 443 or the port that you are using for the Web HMI installation in the incoming firewall rules.

6. Select **Next**.

7. In the **Configure PostgreSQL** screen, enter your existing Web HMI administrator password for PostgreSQL.

8. In the **Configure GE Administrator User** screen, select a user name and a password (10-character minimum) for your GE Administrator user.

A user name can contain alphanumeric characters (at least one), hyphens, periods, underscores, email addresses, and spaces. It cannot start or end with a space. You cannot create the following user names: Administrator, GEAdmin, GEUser, gePeMsUser, System, and SuperUser.

Record this user name and password, as you will use this user account to log in to Web HMI for the first time after the upgrade.

9. In the **Ready to Install** screen, select **Install**.

If a Progress screen appears, select **Next** and wait for the final screen to appear.

The program installs Web HMI and its associated software.

10. Select **Exit** when the installation completes.

Install the CA certificate, as explained in [Install CA Certificates \(on page 40\)](#).

Back Up Customized Components

Before you upgrade, back up any changes made to the Web HMI menu and components in Application Assembler (ThingWorx).

1. In Application Assembler, rename all new and customized Web HMI component content.

2. Upgrade Web HMI, as explained in [Upgrade Web HMI \(on page 34\)](#).

An upgrade does not remove any mashups that you added.

3. **Optional:** If you changed a component, such as a mashup, that was part of the Web HMI installation, you must rename it and incorporate it in to your own extension, and then import it, as explained in [Import Extensions \(on page 37\)](#).

4. **Optional:** If you modified the Web HMI menu to include links to custom mashups, you must recreate these links, as explained in [Add Menu Items \(on page 102\)](#).

Restore Web HMI Databases

During an upgrade, the Web HMI databases from PostgreSQL are automatically exported to the `<install_path>\ProficiencyWebServer\Backups\<Timestamp>\DatabaseExports` directory.

Use the files in the `<install_path>\ProficyWebServer\Backups\<Timestamp>\DatabaseExports` directory to manually restore the Web HMI databases to their previous states. Model and server data are also automatically backed up to `\Backups\<Timestamp>\Data`.

1. Stop the PostgreSQL service on Windows.
2. Replace the files in the `ProficyWebServer\Data` directory with the files in the `\Backups\<Timestamp>\Data` directory.
3. Restart the PostgreSQL service.

Import Extensions

Use the `webServerImport` batch file to import ThingWorx extensions (components) in to Web HMI.

1. As administrator, open a Windows Command Prompt window.
2. Navigate to the Proficy Web Server default installation directory: `C:\Program Files\Proficy\ProficyWebServer`.
3. Run the following command: `webServerImport.bat -twusername=<username> -twpassword=<twpassword> -filetoimport=<filename> -contenttype=extension`.

Command-line Option	Description
-twusername	ThingWorx GEAdministrator user name.
-twpassword	ThingWorx GEAdministrator password.
-filetoimport	Path and filename of the extension to import.
-contenttype	Value can only be an extension.

You can track the progress of this operation in the `importExtLog.txt` log file located in `\ProgramData\Proficy\WebHMI`.

Log in to Web HMI

As a GE administrator, you can access the Runtime environment, the Administration environment, and Application Assembler (ThingWorx).

1. Select the Web HMI icon on the desktop.
2. Enter the user name and password defined during installation.
3. Select **Log In**.

4. Select the user icon at the top right of the screen to choose a Web HMI environment. For more information, see [Web HMI Environments \(on page 38\)](#).

When you select Application Assembler, the application is launched in another browser window, where you can review and accept the customer agreement.

Web HMI Environments

Web HMI contains a Runtime environment, an Administration environment, and the Application Assembler.

Runtime Environment

Operators use the Runtime environment to interact with a HMI/SCADA system. Runtime content is linked directly to data sources, such as Historian.

Administration Environment

GE administrators configure the production runtime content for operators in the Administration environment. GE administrators perform the tasks needed to get data flowing and alarms appearing in the Runtime environment.

Application Assembler

GE administrators manage visualization, which includes creating and modifying mashups, masters, menus, style definitions, and state definitions in the Application Assembler. For information about managing visualization in Application Assembler, see ThingWorx documentation.

GE administrators also handle security, which includes creating and modifying users, user groups, organizational-level security, and Active Directory authentication in the Application Assembler.

Uninstall Web HMI

Follow these steps to uninstall Web HMI.

1. Navigate to **Control Panel > Programs > Uninstall a program**.
2. Select Web HMI and then **Uninstall**.
3. For iFIX, remove these tasks from the iFIX System Configuration Utility Startup Tasks list:
 - DataDistributor.exe
 - AlarmGateway.exe
 - ScadaStat.exe (upgrade only)

This eliminates any iFIX startup issues.

Chapter 6. Certificate Management and Content Security

Certificate Management

Certificate management is an integral part of securing communication between Web HMI and web browsers.

Certificates

Communication between Web HMI and a web browser over the HTTPS protocol uses the certificate of the Reverse Proxy component to encrypt messages. This certificate is signed by another certificate (which has a common name field set to ca) and is used as the Certificate Authority (CA) certificate. This CA certificate is generated at installation time, is self-signed, and is not trusted by web browsers. As a result, when a user tries to connect to Web HMI, the web browser prohibits access and displays the warning message: *Your connection is not private*. A user can then select **Advanced** to load the web page, but it is safer to import the CA certificate in to the user machine so the web browser can mark the connection as trusted.

Since you cannot force users to always use trusted HTTPS connections from the server side, Web HMI takes precautions to prevent content access to users with untrusted certificates.

The server side detects when the URL address does not match the host name or the IP address in the certificate. For example, the certificate only contains the host name by default but users may attempt to access Web HMI using an IP address in the URL, such as `https://10.0.0.10`. When Web HMI detects such a scenario, it blocks access to the content completely and returns this message:

Access Denied Please ensure you are using valid URL

You can disable this access restriction by setting the `denyIfAddressIsNotInCert` option to `false` in the Reverse Proxy configuration file. Alternatively, you can configure it to allow use of specific IP addresses by adding the desired IP addresses to the `proxy IPs` parameter of the Reverse Proxy configuration file, `serverConfig.json`. If defining multiple IP addresses in this file, separate each by a semicolon, such as `1.2.3.4;5.6.7.8`.

Custom Certificates

Since the CA certificate that signs the HTTPS certificate used by Web HMI is self-signed by default, you must import it in to each user machine for it to be trusted and recognized as safe by web browsers. This also applies to the server using a web browser to access Web HMI. If you purchased a valid CA certificate, you do not need to install this certificate on all clients. If you have your own infrastructure for generating

certificates, edit the serverConfig.json file to use your custom certificate, as explained in [Apply Custom Certificates \(on page 41\)](#).

Install CA Certificates

You must install Certificate Authority (CA) certificates on each client and server machine where Web HMI is installed.

1. Log in to the Web HMI server machine.
2. Navigate to C:\Program Files\Proficy\ProficyWebServer\SetCertificates\set-certificates-<version>\ca.
3. Copy the ca.cert.pem file to the client machine.
4. For iPad clients, do the following to install and trust the certificate in a configuration profile:
 - a. Click ca.cert.pem.
 - b. When asked to allow this website to open Settings to show a configuration profile, select **Allow**.
 - c. When the **Install Profile** screen appears, select **Install**.
 - d. If a warning message appears, select **Install**.
 - e. When another **Install Profile** screen appears, select **Install**.
 - f. When the **Profile installed** screen shows that the certificate is verified, select **Done**.
 - g. For iPads using iOS 10.3 or higher, you can trust the certificate by navigating to **Settings > General > About > Certificate Trust Settings**.
Each certificate installed via a profile is listed under **Enable Full Trust for Root Certificates**.
 - h. Under **Enable Full Trust for Root Certificates**, use the toggle button to trust the certificate, and then select **Continue** to store this certificate to the Trust store.
5. For Windows clients, do the following to install and trust the certificate:
 - a. Rename the ca.cert.pem file to ca.cert.cer.
 - b. Double-click ca.cert.cer and select **Install Certificate**.

- c. Select **Local Machine > Trusted Root Certification Authorities** to install the certificate to the Windows store.

A message appears confirming the import was successful.

6. Repeat this process on each client and server machine (if using the server machine as a client).

Apply Custom Certificates

Modify the Reverse Proxy configuration file to use custom certificates.

1. Navigate to the Reverse Proxy configuration file: `<install path>\ProficyWebServer\ReverseProxy\ssl\serverConfig.json`.
2. Define these field values in the serverConfig.json file:

Option	Description
sslCertFile	Location of the certificate file (PEM format).
sslKeyFile	Location of the private key (PEM format).
sslPassphrase	Password to access the private key.

3. Save the serverConfig.json file.
4. Navigate to the Windows Services menu to restart the GE Proxy service.

Install Workflow Certificate in iPad Clients

To interact with Workflow task lists through Web HMI on iPad devices, you must install the Workflow ProficySelfSignedCA certificate in each device.

1. Retrieve the ProficySelfSignedCA certificate in the Workflow server, as explained in step 3 of [Get Started with Workflow and Web HMI \(on page 27\)](#).
2. Place the ProficySelfSignedCA certificate in each iPad client.
3. For each iPad client, do the following to install and trust the ProficySelfSignedCA certificate in a configuration profile:
 - a. Click ProficySelfSignedCA.
 - b. When asked to allow this website to open Settings to show a configuration profile, select **Allow**.
 - c. When the **Install Profile** screen appears, select **Install**.

- d. If a warning message appears, select **Install**.
- e. When another **Install Profile** screen appears, select **Install**.
- f. When the **Profile installed** screen shows that the certificate is verified, select **Done**.
- g. For iPads using iOS 10.3 or higher, you can trust the certificate by navigating to **Settings > General > About > Certificate Trust Settings**.
Each certificate installed via a profile is listed under **Enable Full Trust for Root Certificates**.
- h. Under **Enable Full Trust for Root Certificates**, use the toggle button to trust the certificate, and then select **Continue** to store this certificate to the Trust store.

Set up a Whitelist

You create a whitelist of safe domains that Web HMI can load in to an iframe.

In Application Assembler, you can use the `Whitelist_Web_Frame(GE)` widget in a mashup to call any domain in that whitelist.

1. Open the Reverse Proxy configuration file located in `<install path>\ProficiencyWebServer\ReverseProxy\serverConfig.json`.
2. In the whitelist field, enter a list of comma-separated domain names surrounded by quotation marks. Always preface these names with https unless using a wildcard character. Use wildcards to allow the access of subdomains as well as all sources:
`"*.domain.com";https://www.domain.*";*`
3. Save the `serverConfig.json` file.
4. Navigate to the Windows Services menu to restart the GE Proxy service.
5. Refresh the browser clients.

Whitelists

The whitelist feature allows web content to load in to Web HMI.

Be aware that some websites programmatically ensure that their content does not appear inside of an iframe. Additionally, the Web HMI client only displays content loaded using the HTTPS protocol, which can prohibit the ability to host certain websites that store both HTTP and HTTPS content.

Web HMI conforms to the Content Security Policy (CSP) security to detect and mitigate attacks, such as cross-site scripting. CSP provides a standard method for website owners to declare approved origins of content that browsers can load on their websites. Web HMI returns each HTTPS response with a Content-Security-Policy field in its header containing a list of approved (as safe) domain names that web browsers

can load. You define this list in the whitelist field of the Reverse Proxy configuration file, as explained in [Set up a Whitelist \(on page 42\)](#).

Security Recommendations

To create a secure Web HMI environment, follow these recommendations.

Servers

The Web HMI server machines must not initiate outbound connections.

Low-level Privileges in Runtime

Use low-level privilege settings with no user logins for the Web HMI Runtime environment.

Configuration Files

Configuration files containing sensitive information must reside in a folder restricted to ACL access, limiting access to the application-context user.

Passwords

Passwords must consist of a minimum of 32 alphanumeric characters to prevent access through brute force.

Valid Certificate Authority Certificate

Instead of using a self-signed certificate, purchase a valid CA certificate to secure your SSL implementation.

Network Level Authentication (NLA)

Allow connections only from computers running Remote Desktop with Network Level Authentication (NLA), as set on **Control Panel > System and Security > System > Remote settings > Remote**. For more information, see <https://technet.microsoft.com/en-us/library/cc732713.aspx>.

NetBios Service

If not being used, disable the NetBios service. For more information, see https://msdn.microsoft.com/en-us/library/ff648653.aspx#c16618429_012.

If the Web HMI server requires an active NetBios service, restrict anonymous access to sensitive data using the Registry. For more information, see [https://msdn.microsoft.com/en-us/library/ms913275\(v=winembedded.5\).aspx](https://msdn.microsoft.com/en-us/library/ms913275(v=winembedded.5).aspx)

FIPS Compliance

Set the Remote Desktop Protocol (RDP) encryption level to FIPS compliant.

Autofill and Autocomplete

To reduce password security risks, turn off AutoComplete or AutoFill in the supported browsers:


- Chrome
- Safari
- Microsoft Edge

Chapter 7. GE HMI Server Configuration Manager

GE HMI Server Configuration Manager

The GE HMI Server Configuration Manager handles the connection configuration, certificate management, and logging settings required for Web HMI to successfully communicate with iFIX, Historian, and CIMPLICITY (OPC UA-enabled data source).

Accessing the GE HMI Server Configuration Manager

After you install Web HMI, the GE HMI Server Configuration Manager icon appears on the desktop. Select  to open the GE HMI Server Configuration Manager.

Configuration File

The values that you define in the GE HMI Server Configuration Manager are stored in a configuration file, which is located at `ProgramData\Proficy\WebHMI\DataServices\data-services-config.json`.

Secure Connections to OPC UA Endpoints

Use the GE HMI Server Configuration Manager to discover and configure CIMPLICITY OPC UA endpoints. An endpoint is the server found at the discovery URL (Uniform Resource Locator).

To establish a secure connection, an OPC UA endpoint and Web HMI client must be able to identify and accept each other's digital certificate. Use this procedure to check the authenticity of both certificates and test the connectivity to the OPC UA endpoint.

During this procedure, you enter a Discovery URL, select an endpoint (found at the Discovery URL), and then select the security settings for Web HMI to use when establishing a data connection with this endpoint.

In CIMPLICITY, verify the GE Web HMI server information was set up in **Project Properties > OPC UA Server > Web HMI Configuration**.



Note:

Web HMI supports standard OPC UA architecture and was qualified with a CIMPLICITY OPC UA server.

1. In the GE HMI Server Configuration Manager, select the **OPC UA Endpoints** tab.
2. Select **Add**.


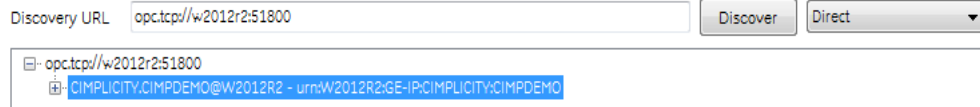
3. Select a discovery method for your OPC UA server endpoints from the top right drop-down menu:

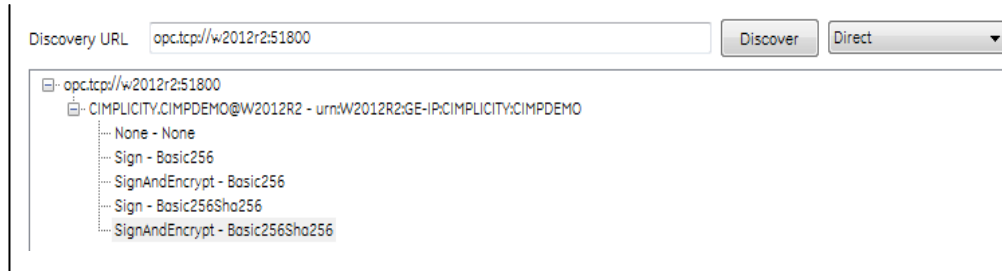
Option	Description
Direct	Discovers the endpoint of an OPC UA server (default, recommended). To use this discovery method, you must know the location of the OPC UA endpoint.
Local Network	Retrieves all OPC UA endpoints within your local network.
Directory	Retrieves all OPC UA endpoints that are registered with a Global Discovery Server (GDS).

4. Type the discovery URL in the **Discovery URL** field and select **Discover**.

- If you selected the Local Network discovery method, leave the Discovery URL entry as `opc.tcp://localhost`.
- If you selected the Directory discovery method, you may be prompted to trust the GDS certificate before continuing. If the **Server Certificate** window appears with the option to trust the certificate, click **Trust** and **Close**. Select **Discovery** again to continue with the discovery process.

The discovery results appear on the screen in a tree structure consisting of these three categories:

Discovery URL	<p>Entry that you typed in to the Discovery URL field. This shows an example of a Direct URL:</p> 
OPC UA Servers	<p>Endpoints found by the specified Discovery URL. Each endpoint entry consists of the application name and URN (Uniform Resource Name). This shows an example of the discovered CIMPLICITY endpoint found at the above URL:</p> 
Endpoint Security Configuration	<p>Each endpoint supports a combination of security configurations ranging from none (none-none) to encrypted and digitally signed (SignAndEncrypt - Basic256Sha256). This shows the security options you can define for the above CIMPLICITY endpoint:</p>



5. Expand the Discovery URL results and select the endpoint.

The security options appear for the selected endpoint.

6. Select the appropriate security policy and mode for this connection. The `None-None` option creates an unsecure connection.

7. Check the connectivity to the endpoint by selecting **Server Credentials**.

8. In the **Server Credentials** window, enter the user name and password for the server.

When you first enter a value in the password field, you can view the entry in plain text by selecting **Show**. The **Show** button is only enabled when a value is entered in to the password field. For security purposes, if you navigate away from this window, or if the GE HMI Server Configuration Manager has read a saved password from a configuration file, the **Show** button is disabled.

9. For Web HMI to use credentials of the logged-in user when writing values or acknowledging alarms, check the **Use logged-in Web HMI credentials for data writes and alarm acknowledgment** box. If unchecked, Web HMI uses the credentials specified here.

10. Select **Test**.

A Log window appears to the right of the application displaying diagnostic information for resolving connectivity issues between Web HMI and the OPC UA server. You can encounter these issues during a connection attempt:

<p>Certificate Validation Failed</p>	<p>When the Server Certificate window appears with the certificate information:</p> <ul style="list-style-type: none"> a. If satisfied with the authenticity of the certificate, select Trust to save the certificate in the <code>ProgramData\Proficiency\WebHMI\DataServices\pki\trusted\certs</code> file on the Web HMI client. b. Once the certificate is trusted, select Close. c. Select Test again to verify that the client accepted the endpoint certificate.
<p>Bad Security Checks Failed</p>	<p>If the log indicates a failed connection to the endpoint because the client certificate is in a rejected state:</p>

	<ol style="list-style-type: none"> a. From the endpoint's <project folder>\pki\rejected, copy the rejected client certificate into <project folder>\pki\trusted\cert. b. Select Test again to verify the endpoint accepted the client certificate.
<p>Bad Identity Token Rejected</p>	<p>If the log indicates a failed connection to the endpoint because of a bad identity token:</p> <ol style="list-style-type: none"> a. Verify that you entered the correct user name. b. Verify that you entered the correct password by selecting the Show button or re-entering the password. c. Confirm that the user account is enabled and exists in the OPC UA server user account list. d. Select Test again to verify the endpoint accepted the user name and password that you entered.

11. **Optional:** To use the Local Network filter:

- a. Select **Edit Filters**.
- b. In the **Max Records** field, define the limit for the number of endpoints returned when you select the **Discover** button. Note that the GE HMI Server Configuration Manager combines endpoints from the same server. As a result, the number of items appearing in the list may be less than expected given the specified **Max Records** value.

12. **Optional:** To use the Directory filters:

- a. Select **Edit Filters**.
- b. In the **Max Records** field, define the limit for the number of endpoints returned when you select the **Discover** button. Note that the GE HMI Server Configuration Manager combines endpoints from the same server. As a result, the number of items appearing in the list may be less than expected given the specified **Max Records** value.
- c. In the **Server Name** field, enter the human-readable name of the server to use in the endpoint search. You can use the % wildcard.
- d. In the **Server URI** field, enter the global unique identifier of the server instance to use in the endpoint search. You can use the % wildcard.
- e. In the **Product URI** field, enter the global unique product identifier to use in the endpoint search. You can use the % wildcard.
- f. Select the **Capabilities** box to select from a list of OPC UA features. These capabilities limit results to endpoints supporting the OPC UA feature selections. For example, the **provides historical alarms and events** selection returns endpoints only supporting alarms.

**Note:**

Not all endpoints publish their capabilities to the directory, and an NA (not available) is returned when endpoints do not provide this information.

13. Select **OK** and then **Save**.

Create Self-Signed Certificates for Web HMI Clients

Use the GE HMI Server Configuration Manager to create self-signed digital certificates for Web HMI clients to use when establishing a trusted relationship with OPC UA endpoints.

A new self-signed certificate generated by the GE HMI Server Configuration Manager overwrites the certificate you initially installed for the Web HMI client. Previously-configured OPC UA endpoints now require this new self-signed certificate. To reestablish this trust relationship, you must attempt to reconnect with the OPC UA server (using the **Test** button in the Server Credentials window). The OPC UA Server initially rejects the new client certificate (Bad Security Checks Failed). As a result, you must move the rejected client certificate in `<project folder>\pki\rejected\` to `<project folder>\pki\trusted\certs` of the OPC UA server host machine.

1. In the GE HMI Server Configuration Manager, select the **OPC UA Client** tab.
2. To create self-signed certificates, select **Enable Security**.

The **Task** panel shows the status of this step. The new self-signed certificates are stored in `ProgramData\Proficy\WebHMI\DataServices\pki\own\certs`.

Use GDS Certificates for Web HMI Clients

Use the GE HMI Server Configuration Manager to register with the Global Discovery Server (GDS) and use the certificates provided by GDS to establish a trusted relationship between Web HMI clients and OPC UA endpoints.

You must enable GDS security and register your project with a GDS in CIMPLICITY.

1. In the GE HMI Server Configuration Manager, select the **OPC UA Client** tab.
2. Set up the GDS server connection by selecting the **Use GDS** check box.
3. Enter the URL, user name, and password of the GDS server.

When you first enter a value in the password field, you can view the entry in plain text by selecting **Show**. The **Show** button is only enabled when a value has been entered in the password field. For

security purposes, if you navigate away from this window, or if the GE HMI Server Configuration Manager has read a saved password from a configuration file, the **Show** button is disabled.

4. Select **Test** to confirm a connection can be established with the GDS. A Log window appears to the right of the application displaying information relevant to diagnosing connectivity issues between Web HMI and GDS.

You can encounter these issues during a connection attempt:

Certificate Validation Failed	<p>When the Server Certificate window appears with the certificate information:</p> <ol style="list-style-type: none"> a. From the endpoint's <project folder>\pki\rejected, copy the rejected client certificate in to <project folder>\pki\trusted\cert . b. Once the certificate is trusted, select Close. c. Select Test again to verify that the client accepted the endpoint certificate.
Bad Security Checks Failed	<p>If the log indicates a failed connection to the endpoint because the client certificate is in a rejected state:</p> <ol style="list-style-type: none"> a. From the endpoint's <project folder>\pki\rejected folder, copy the rejected client certificate in to <project folder>\pki\trusted\cert. b. Select Test again to verify the endpoint accepted the client certificate.
Bad Identity Token Rejected	<p>If the log indicates a failed connection to the endpoint because of a bad identity token:</p> <ol style="list-style-type: none"> a. Verify that you entered the correct user name. b. Verify that you entered the correct password by selecting the Show button or re-entering the password. c. Confirm that the user account is enabled and exists in the OPC UA server user account list. d. Select Test again to verify the endpoint accepted the user name and password that you entered.

5. Select **Ok** on the **Configure GDS** window.

6. Select **Enable Security**.

This begins the process of registering the Web HMI client with GDS for the first time. After this first GDS registration, you can re-register the client by enabling **Use GDS** and selecting **Enable Security**.

The **Task** panel shows the status of the GDS registration and certificate creation process:

- a. Creates a self-signed certificate.
 - b. Authenticates Web HMI with GDS using the GDS URL, user name, and password.
 - c. If authentication is successful, registers Web HMI as an OPC UA application.
 - d. Creates a GDS signed certificate for Web HMI.
 - e. Generates a certificate trust list that contains all GDS trusted servers and clients.
7. Select **Save** to save the ID created by GDS during the above registration process.
This ID checks whether Web HMI was previously registered with GDS.

**Note:**

Every time you re-register with the same GDS, the GE HMI Server Configuration Manager asks you to re-trust the GDS certificate. For security purposes, the server certificate is removed at the end of the registration process.

Connect to Historian

Use the GE HMI Server Configuration Manager to set up the Historian server credentials used by the Data Distributor to connect Web HMI to one or more Historian servers.

1. In the GE HMI Server Configuration Manager, select the **Historian** tab.
2. Select **Add**.
3. In the **Server Name** box, you must enter the name of the Historian server as set in the **Server Name** column of the **Server Details Management** screen.
The **Server Name** box may be empty after an upgrade. In this case, you must enter a valid **Server Name** from the **Server Details Management** screen.
4. In the **Server Location** box, enter the host on which the **Historian** server runs, which can be the host name or the host IP address.
5. Enter the user name and password for the Historian server.
When you first enter a password, you can view the entry in plain text by selecting **Show**. The **Show** button is only enabled when a value is entered in to the password field. For security purposes, if you navigate away from this window, or if the GE HMI Server Configuration Manager has read a saved password from a configuration file, the **Show** button is disabled.
6. To check the Web HMI connection to the Historian server, select **Test**.
A window appears to indicate a successful connection or to provide diagnostic information for a failed connection.
7. To set up each Web HMI to Historian server connection, repeat the above steps.

Define Tracing and Logging

Use the GE HMI Server Configuration Manager to configure the tracing and logging settings for the Alarm Gateway and Data Distributor.

1. In the GE HMI Server Configuration Manager, select the **Alarm Gateway/Data Distributor** tab.
2. In the Alarm Gateway section, do the following:
 - a. In the **Application Trace Level** field, define the logging level for Alarm Gateway.
 - b. In the **OPC UA Trace Level** field, define the logging level for the messages used to communicate with an OPC UA server.
 - c. In the **Max Log File Backups** field, define the maximum number of log files to store in the log folder before overwriting the oldest log files with a newer one.
 - d. In the **Max Log File Entries** field, define the maximum number of log entries a log file can contain before creating a new log file.
 - e. To view the Alarm Gateway log files, select **Log Files**.
3. In the Data Distributor section, do the following:
 - a. In the **Trace Level** field, define the logging level for the Data Distributor.
 - b. In the **Enable Log Packets** field, indicate if you want to display the communication packet content, such as subscription requests, for the Data Distributor.
 - c. In the **Max Log File Backups** field, define the maximum number of log files to store in the log folder before overwriting the oldest log file with a newer one.
 - d. In the **Max Log File Entries** field, define the maximum number of log entries a log file can contain before creating a new log file.
 - e. To view the Data Distributor log files, select **Log Files**.

Chapter 8. Develop Runtime Content

Runtime Model

You create a model to build the Runtime structure and content. You set up the types of equipment to use, the instances of equipment to appear in the Runtime context, the information to display about the equipment, and the data sources for supplying both real-time and historical data to Web HMI.

Where to Begin

Web HMI provides a Model Editor user interface to help you create and modify your model. You can also use the model template to manually build and modify your model structure and then import it in to Web HMI. For information about the template, see [Model Template Description \(on page 63\)](#).

Model Editor

Web HMI provides an editor to help you create and modify asset object types and asset objects in your model.

To begin building a model, follow these tasks:

- [Set Up Data Source Servers \(on page 55\)](#)
- [Set Up the Model Structure \(on page 55\)](#)
- [Define Objects \(on page 56\)](#)
- [Setting Up Runtime Navigation \(on page 58\)](#)

Supported Characters for the Model

Before creating object types, objects and data variables, review the following tables to see which characters are supported as well as restricted.

Supported Characters

Character	Description
!	Exclamation Point
@	At sign
^	Caret
\$	Dollar Sign
()	Parentheses

Character	Description
	Pipe
.	Period
`	Grave Accent
~	Tilde
-	Hyphen
_	Underscore

**Note:**

A single space is allowed but a succession of spaces is not.

Unsupported Characters

Character	Description
#	Number Sign
%	Percent Sign
\	Backslash
,	Comma
?	Question Mark
;	Semicolon
+	Plus Sign
:	Colon
"	Quotation Marks
'	Apostrophe
< >	Greater than/Less than Symbols
{ }	Braces
/	Slash
=	Equal Sign

Character	Description
*	Asterisk
&	Ampersand

Set Up Data Source Servers

You set the data source servers used to populate data in your model.

You can set up multiple Historian servers.

1. In the Administration environment, select **Set Up** and then **Server**.

The **Server Details Management** screen appears.

2. To add each data source, do the following:

- a. Select **+** above the table.
- b. In **SystemAlias**, enter the alias for the server.
- c. In **SystemType**, select the data source type from where data originates.
- d. In **SystemName**, specify one of the following:
 - For iFIX, enter the logical node name.
 - For Historian, enter the server name.
 - For CIMPLICITY, copy the Uniform Resource Name (URN) from the CIMPLICITY Project Properties screen or from the .csv file containing the project server and namespace information exported from CIMPLICITY and paste it in to this field.
 - For Workflow, enter the server name. Workflow requires a refresh rate between 1 and 30 seconds to poll the server for new and updated tasks. The default is 5 seconds. You can only set up one Workflow server.

3. Select **Save**.

Set Up the Model Structure

Object types define the structure of the equipment pieces within your model. For each object type, such as a StorageTank, you set up all the data variable names, such as TankLevel, that any asset object associated with this type can reuse in its own definition. You also bind mimics to object types for use by their asset objects.

Using the **Contained Types** area, you set up the parent/child relationship of asset object types in the model. For example, StorageTank1 and SuctionValve2 are the children that comprise the FinishedWaterPumpStation. In Runtime, the children appear under the parent in the navigational context.

1. In the Administration environment, navigate to **Assets > Object Types > New**.
The **Object Type Information** screen appears.
2. Enter a unique name for the new object type and provide a description.
3. Select **Save**.
4. Select **Data Variables** to add variable names whose data will come from the HMI/SCADA system.
5. To add a variable name for this object type, do the following:
 - a. Select **+** above the table.
 - b. In **Variable**, enter the name of the data variable, such as Pressure.
 - c. In **Data Type**, select the type of data this variable stores: Boolean, String, Number, and Array (CIMPLICITY only).
For CIMPLICITY, Web HMI provides array support for monitoring purposes. For example, you can import CIMPLICITY screens that display array states, such as Idle, in Web HMI for viewing. You cannot control or trend data shown on these arrays.
 - d. In **Description**, explain the purpose of the data variable.
6. Repeat the above steps for each new object type.
7. To define an asset object type as a parent of other types, do the following:
 - a. Select **Contained Types**.
 - b. Choose the parent by selecting an object type on the left panel.
 - c. Select **+** above the table to add children to the parent.
 - d. Select the object type to become a child and provide an alias name.
8. Select **Save**.

Related information

[Bind Mimics to Assets \(on page 72\)](#)

Define Objects

Asset objects are the instances of equipment pieces, such as StorageTank1, to appear in the model. For each object, you determine which data variables derived from its object type to reuse, and then define them accordingly.

- Objects appear alphabetically.
 - Always use a unique object name.
1. In the Administration environment, navigate to **Assets > Objects**.
If objects are already defined, the left panel lists them.
 2. To add a new object, select **New**.
The **New Object** screen appears.
 3. Select the object type for this object.
The children of the object type appear under **Contained Objects** if defined. Web HMI automatically generates a contained object name from the alias and appends an instance number to it, such as DPump1_1. The next time another asset object reuses the object type with this contained object, the instance number is increased by one, which in this example is DPump1_2.
 4. Type a unique name for the new object and provide a description.
 5. Select **Save**.
The new object appears with the data variables of its object type.
 6. Define each data variable that you want to use for this object by doing the following:
 - a. For a real-time data source, select its **RealTime Data Alias**, and then enter the real-time data source tag or point ID that will feed data in to this variable. For an array data type, `ns=3;s=ARRAYPOINT.Value` is an example of a real-time data source point ID.
 - b. For a historical data source, select its **Historical Data Alias**, and enter the historical data source tag ID to retrieve data for this variable, which can appear on Trend charts and Control Views.
 7. Select **Save**.

Duplicate Objects

When an object uses similar data variables and contained objects as a configured object, you can duplicate the configured object to create new objects for your model.

1. In the Administration environment, navigate to **Assets > Objects**.
2. Select **Duplicate**.
The duplicated object appears highlighted in the left panel with Copy appended to its name.
3. Change the name in the **Name** field and select **Save**.
The renamed asset object appears in the left panel. You cannot rename the asset after selecting **Save**.
4. To duplicate more instances of the same object, continue to select **Duplicate** and repeat step 3.
The duplicated objects appear highlighted in the left panel with Copy and a number appended to their names, such as pump1_copy(1), pump1_copy(2), and so on.

Set Up Runtime Navigation

Use the Navigation app to visually structure the Runtime hierarchy of objects in Web HMI.

Changing the root of an existing Runtime navigation hierarchy requires that you clear the entire hierarchy and then rebuild it.

1. In the Administration environment, navigate to **Visualizations > Navigation**.

All objects appear in the left panel with check boxes.

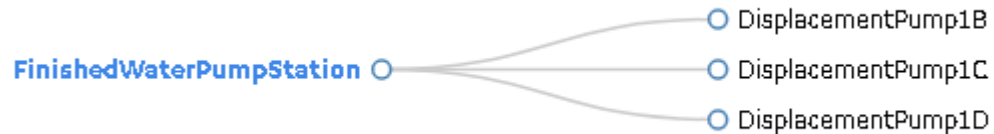
2. Select the parent check box and then select **+** at the top of the left panel.

The parent object instance appears in the app area. The following shows the FinishedWaterPumpStation parent.

FinishedWaterPumpStation

3. Select the parent object in the app area, select its children in the left panel and select **+**.
4. In the app area, expand the parent object to show its children by selecting its filled circle.

In this example, the FinishedWaterPumpStation has three DisplacementPump



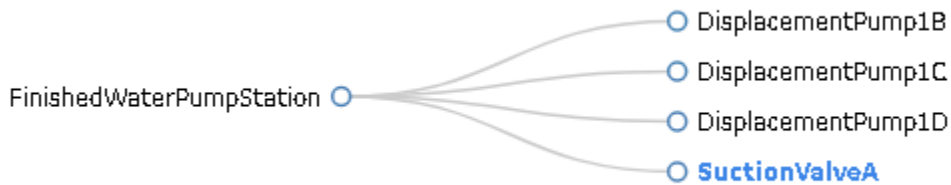
children.

5. To add object instances to a child, select the child in the app area and select its descendants in the left panel.

In this example, SunctionValveA is a descendant of DisplacementPump1D.



6. You can also drag and drop objects within the hierarchy to change their order, as shown in this example. SunctionValveA is now a child of FinishedWaterPumpStation.



7. **Optional:** To delete an object from the hierarchy, select its check box and then - at the top of the left panel.
8. **Optional:** At any time, you can remove the hierarchy and start with a blank app area by selecting **Clear Hierarchy**.
9. To save the Runtime hierarchy that you created, select **Save**.

Change Server Details

You can remove a server and change its system alias, type, and system name. When you change the server alias name, all objects using that alias are automatically updated.

1. In the Administration environment, select **Set Up**.
The **Server Details Management** screen appears listing the data source servers.
2. In the table, make the changes as needed.
3. To delete a server, select the check box next to it and select **Delete**.
4. Select **Save**.

Modify Object Types

You can remove an asset object type and delete and modify its data variable names but you cannot change the name of an object type. All changes made to an object type are reflected in its object instances.

You cannot delete an asset object type that has existing objects using its data structure.

1. In the Administration environment, navigate to **Assets > Object Types**.
The **Object Type Information** screen appears listing the object types.
2. In the left panel, select the object type to modify.
3. Make changes as needed and select **Save**.
4. To remove an object type, select it in the left panel, select **Delete**, and confirm the delete.

Remove Contained Types

When you delete a child from an asset object type, it is also removed from all objects using it.

1. In the Administration environment, navigate to **Assets > Object Types**.
The **Object Type Information** screen appears listing all the asset object types.
2. In the left panel, select the asset object type whose children you want to modify.
3. Select the **Contained Types** tab.
4. To remove children from a parent, select the check box next to each child you want to remove, and select - above the table.
5. Select **Save**.

Replace Contained Objects

You can quickly replace contained objects by browsing through a list of similar objects that are assigned to the same object type.

1. In the Administration environment, navigate to **Assets > Objects**.
2. Select the object type.
3. Select **Contained Objects**.
4. Select the arrow next to the contained object that you want to replace. A list appears with similar objects that are associated with the selected object type, as shown in the following image:

Data Variables		Contained Objects	
Name			
StorageTank1			▼
SuctionValveA			▼
SuctionValveB			▼
SuctionValveC			▼
SuctionValveD			▼
DisplacementPump1D			▲
		DisplacementPump1A DisplacementPump1B DisplacementPump1C DisplacementPump1D	

5. Select the object to replace the contained object. This selected object is now a contained object for the object type.
6. **Optional:** To view the details of a contained object, such as its data variables, select its hyper-linked name in the **Name** column.
7. Select **Save**.

Modify Objects

You can remove an asset object as well as change its real-time and historical data sources. You can select multiple SCADA nodes per object.


If an object has contained objects, you can change their auto-generated names but not their aliases.

1. In the Administration environment, navigate to **Assets > Objects**.
The **Object** screen appears.
2. In the left panel, select the object to modify.
3. Make the changes as needed and select **Save**.
You cannot modify data variables.
4. To remove an object, select it in the left panel, select **Delete**, and confirm the delete.

Export the Model

You can generate a file containing the required section headers to get you started if your model is not yet created. You can also export an existing model to make changes to it.


You cannot export the data source and the data variable attributes configured on a Control Card.

1. In the Administration environment, select the Model Import/Export icon, .
2. In the **Export** area, enter a model file name to generate in CSV format.
3. Select **Export**.
4. Retrieve the model file from the Windows Downloads folder.

Make Extensive Model Changes

If you want to make significant modifications to an existing model, you can export the model, make your changes, and then import the revised model in to Web HMI.


You cannot export the data source and the data variable attributes configured on a Control Card.

1. In the Administration environment, select the Model Import/Export icon, .
2. In the **Export** area, enter a model file name to generate in CSV format.
3. Select **Export**.
4. Retrieve the model file from the Windows Downloads folder.
5. Make the modifications to your model file.
6. Import the revised model file in to Web HMI.

Import the Model

After creating or modifying your model, you can import it in to Web HMI.


When replacing an existing model file containing different asset objects and object types, Web HMI does not remove the original asset objects and types from Application Assembler. Depending on your model requirements, you may need to delete these objects from the original model file before importing a new file.

1. In the Administration environment, select the Model Import/Export icon, .
2. Navigate to the model file and select **Import**.
Always check the log file if the import failed. You may find that some asset objects were successfully imported while others were not.
3. Follow these instructions to view and download the log file in these browsers:

Option	Description
Chrome	<ul style="list-style-type: none"> ◦ To view the log file, right-click [log] to open it in a new tab. ◦ To download and then view the log file, click [log]. You can view the file in the Downloads folder.
Microsoft Edge	<ul style="list-style-type: none"> ◦ To view the log file, click [log], and then Open. ◦ To download and view the log file, click [log], and then Save. You can then view the log file by selecting View downloads.

4. To view the model in Runtime, select **Runtime** from the user icon drop-down list at the top right of the screen.

By default, the highest asset point in the model hierarchy appears. If this is a new model, its HMI card is blank because you have not yet assigned mimics to any asset objects in the hierarchy.

5. To navigate through the asset objects in the hierarchy model, select the Asset Context Selector, . The model displays the relevant data in context to each asset object selected in the navigation scheme.

Access the Model Template

The model template, `ModelStarterTemplateSteps.xlsx`, provides a structure to help you create your model.

1. Navigate to `\Program Files\Proficy\ProficyWebServer\Tools`
`\ModelStarterTemplateSteps.xlsx`.
2. Follow the instructions in `ModelStarterTemplateSteps.xlsx`.
3. When done, select **Save Model to CSV** to save the model to a CSV file, which you can import in to Web HMI.

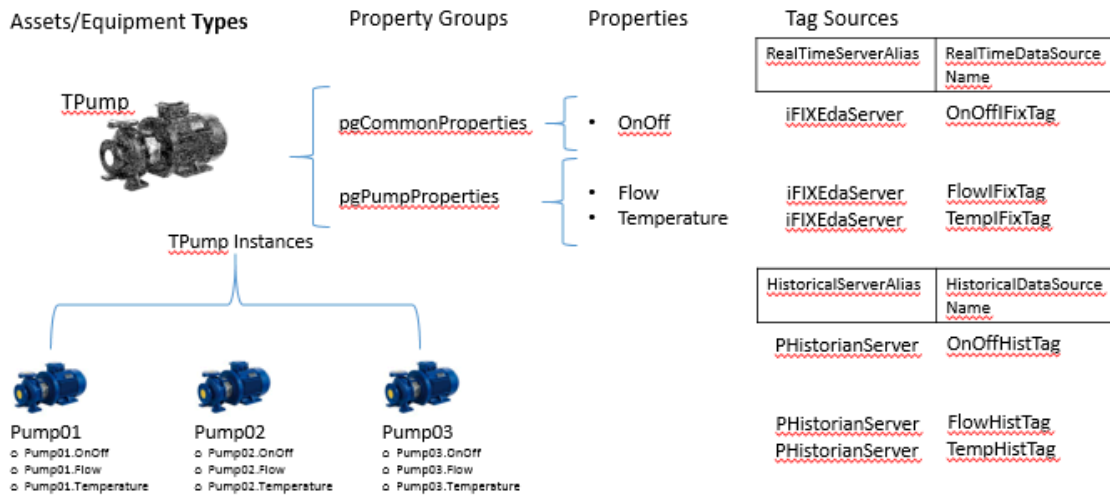
Model Template Description

The model template provides sections to help you build the Web HMI Runtime model structure.

Model Concepts

Review this illustration before creating your Runtime model.

Model Concepts



Concept Terminology Differences

The model template and Model Editor user interface use different concept terminology, as shown in the following table.

Model Template	Model Editor
Asset type	Object type
Asset	Object
Property	Data variable

Hierarchy

You must build an asset hierarchy to specify the hierarchical relationships of assets in Web HMI. Operators navigate through this hierarchy to select the equipment context for a given layout at Runtime.



Note:

Since only one root node is allowed in this hierarchy, do not define more than one asset to a root parent.

Property	Description
HierarchyFlagsHeader	Header column with the keyword <code>HierarchyFlags</code> .

Property	Description
HierarchyFlags	Specifies whether to update or overwrite the asset hierarchy when importing the model file in to Web HMI.
OverwriteHierarchy	<ul style="list-style-type: none"> • <code>True</code> creates a new hierarchy based on the exact content of the imported model file. • <code>False</code> updates any existing imported hierarchical relationships.
OverwriteAssetChildren	<ul style="list-style-type: none"> • <code>True</code> replaces existing child assets with child assets in the model template file. • <code>False</code> adds child assets from the model template file to the existing child assets.

Asset Types

Asset types define the structure of the equipment pieces within your model. For each asset type, such as a StorageTank, you set up all the property names, such as TankLevel, that any asset instance associated with this type can reuse in its own definition.

In Web HMI, you bind mimics to asset types for use by their asset instances.

Property	Description
AssetTypeHeader	Header column with the keyword <code>AssetType</code> .
Asset Type Name	Name of the asset type.
Description	Description of the asset type.
Property Groups of the Asset Type	Collection of properties associated with the asset type. Assets assigned to this asset type inherit these properties. An asset type can contain more than one property group.

Property Groups

Property groups assemble a set of properties for a piece of equipment. This enables you to create a common set of properties to reuse across multiple asset types.

Property	Description
PropertyGroupHeader	Header column with the keyword <code>PropertyGroup</code> .
Property Group Name	Name of the property group.
Description	Description of the property group.

Assets

Assets are the instances of equipment, such as StorageTank1, in the model. When you assign an asset to an asset type, it inherits all the properties created for that asset type.

You must arrange assets in to hierarchical relationships in the Hierarchy section to appear in the Runtime context selection. Each asset has a parent in the hierarchy.

Property	Description
AssetHeader	Header column with the keyword <code>Asset</code> .
Asset Name	Name of the asset instance.
Description	Description of the asset instance.
Asset Type Name	Name of its associated asset type.
Parent Asset Name	Name of the parent asset. One asset in the list must have a parent asset set to <code>\</code> (root).
Parent Property Name	Ties this asset instance to an asset property definition in the <code>Parent Asset Name</code> type definition. For example, the <code>TPumpStation</code> type contains the <code>InletTank</code> and <code>OutletTank</code> as properties of type <code>Asset</code> . When you create instances of the <code>TPumpStation</code> (for example, <code>PumpStation01</code> , <code>PumpStation02</code>), you must also create instances for <code>InletTank</code> (for example, <code>InletTank01</code> , <code>InletTank02</code>) and <code>OutletTank</code> (for example, <code>OutletTank01</code> , <code>OutletTank02</code>) and point them to the <code>InletTank</code> and <code>OutletTank</code> Properties of the <code>TPumpstation</code> type using this <code>Parent Property Name</code> column, as shown in the following example.

#AssetTypeHeader	Asset Type Name	Description	Property Groups of the Asset Type		
AssetType	TEnterpriseStation		TEnterpriseStationGroup		
AssetType	TPumpStation		TPumpStationPropertyGroup		
AssetType	TStorageTank		StorageTankShape	AssetType	
#PropertyDefinitionHeader	Property Group Name	Property Name	Property Type	AssetType (if the property type is Asset)	
PropertyDefinition	TPumpStationPropertyGroup	InletTank	Asset	StorageTank	
PropertyDefinition	TPumpStationPropertyGroup	OutletTank	Asset	StorageTank	
#AssetHeader	Asset Name	Description	Asset Type Name	Parent Asset Name (\ - root)	Parent Property Name
Asset	EnterpriseStation		TEnterpriseStation	\	
Asset	PumpStation01		TPumpStation	EnterpriseStation	
Asset	InletTank01		TStorageTank	PumpStation01	InletTank
Asset	OutletTank01		TStorageTank	PumpStation01	OutletTank
Asset	PumpStation02		TPumpStation	EnterpriseStation	
Asset	InletTank02		TStorageTank	PumpStation02	InletTank
Asset	OutletTank02		TStorageTank	PumpStation02	OutletTank

Property Definitions

Property definitions describe the actual pieces of data that come from a HMI/SCADA system or another data source. Among other things, it defines how to use a property in Web HMI views. For example, you

can define a property to appear as a trend line on Trend Card views or as a Control Point on Mimic Card views that an operator can modify. Properties comprise a property group.

Property	Description
PropertyDefinition-Header	Header column with the keyword <code>PropertyDefinition</code> .
Property Group Name	Property group name in which to associate this property.
Property Name	Name of the property.
Property Type	Property type: <code>Boolean</code> , <code>number</code> , <code>string</code> , or <code>asset</code> . Property definitions of an asset type can be contained types or child asset references. You must define the child asset type in the <code>AssetType</code> column.
AssetType	When the property type is <code>asset</code> , use this property definition. To assign an asset to a property, you must define this asset type. It allows you to nest child assets in the asset type.
Trendable	Property displays as a trend line on Trend Card views.
ControlGroupId	Unique ID of the control group, allowing you to group properties that can be modified. Any properties with a control group ID are grouped together in an auto-generated Control Card. If the control group has an associated Control Point, an operator can change its value on the Control View at runtime.
ControlPoint	Setpoint for the current HMI/SCADA property value. Both the current property and its control point must be in the same control group. A property can be controlled by itself or by another property in the asset type. To read and write to the same property, specify it as its own control point. A property without a control point is read-only.
HmiDataType	Data type from the underlying SCADA system. This is not required for this release.

Server Details

A server alias offers an indirect route between the model's data sources and the model itself, making it easier to transfer model data sources between servers. By using an alias to reference your data source (such as an iFIX node and OPC UA server) and associating it with your tag sources, you can change the node for a set of tag sources by changing the server name.

Property	Description
ServerDetailsHeader	Header column with the keyword <code>ServerDetails</code> .
Server Alias	Name of the server alias.
Server Name	Name of the server for the data source.
Server Type	Type of server from which data originates.

Tag Sources

A tag source defines where to retrieve asset property data, including real-time and historical data sources.

Property	Description
TagSourceHeader	Header column with the keyword <code>TagSource</code> .
Parent Asset Name	Name of the parent asset with a property with the tag source.
Property Name	Name of the property associated with the tag source.
Realtime Server Alias	Name of the real-time server alias to use with this tag source.
Realtime Data Source Name	HMI/SCADA data source tag ID that feeds data to this model property.
Historical Server Alias	(Optional) Name of the server alias to retrieve historical data for Trend Card views and the last known current value for Mimic Card views.
Historical Data Source Name	(Optional) Name of the historical tag ID to retrieve historical data for Trend Card views and the last known current value for Mimic Card views.

NameSpace Table

This table pertains to CIMPLICITY only. Populate this table using the project server and namespace information that was exported to a CSV file using the **Export to Web HMI** function on the CIMPLICITY Project menu.

Here is a sample NameSpace table:

#NameSpaceTable-Header	ServerAlias	NameSpaceIndex	NameSpaceUri
NameSpaceTable	<project-name>	2	http://ge.com/ua/CIMPLICITY

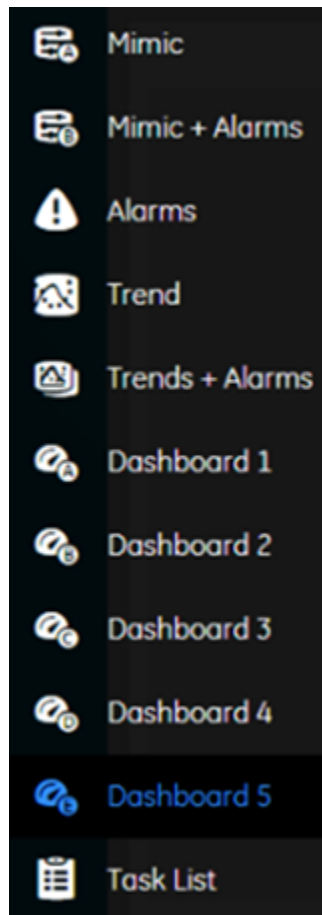
#NameSpaceTable-Header	ServerAlias	NameSpaceIndex	NameSpaceUri
NameSpaceTable	<project-name>	3	<a href="http://ge.com/ua/CIMPLICITY/<projectname>">http://ge.com/ua/CIMPLICITY/<projectname>
NameSpaceTable	<project-name>	4	<a href="http://ge.com/ua/CIMPLICITY/<project-name>/project">http://ge.com/ua/CIMPLICITY/<project-name>/project

Layouts

Web HMI provides a set of standard industry layouts that provide a window in to a running HMI/SCADA system. Layouts consist of cards that you can customize.

You can customize the following Runtime layouts and determine which ones to make available to operators. You can set one of these layouts as the default to appear each time Web HMI opens in a web browser, as explained in [Set the Default Layout \(on page 102\)](#). You can also set a custom menu as the default, as explained in [Add Menu Items \(on page 102\)](#).


Figure 1. Runtime Layouts






Layout Cards

A layout consists of cards that comprise the Web HMI Runtime system. Cards display data according to the context of their associated asset.

You can use the following Web HMI cards as well as build your own cards to view data from other sources, such as an external database, and then include them in custom layouts.

Card	Description
Trend Card 	Shows the trend-line analysis of an asset's property data in the HMI/SCADA system for a given time frame. If both real-time and historical data sources are available for a particular property, the card uses historical data source. If there are no historical data sources, then the card uses real-time data to show trend points of the latest incoming values.
Mimic Card	Displays a process diagram for monitoring and controlling production equipment and processes. When defined, an operator (with permission in the HMI/SCADA system)

Card	Description
	<p>can open a Control View on a Mimic Card to change an underlying HMI/SCADA value. The Control View can also display historical properties that show the last known current value returned from the Historian server.</p> <p>If a property has both real-time and historical data sources defined, the Mimic Card always displays data from the real-time data source, even when that tag is not available. To display values from a historical data source, you must configure those property values to use only a historical data source. To display both real-time and historical data for the same underlying tag, you must define separate properties in the model for the real-time tag and for the historical tag.</p>
<p>Alarm Card</p> 	<p>Displays the alarms occurring in the HMI/SCADA system.</p> <p>Web HMI provides these Alarm Card views:</p> <ul style="list-style-type: none"> • General view shows all active alarms in the underlying HMI/SCADA system by severity level. • Detail view displays all alarms for the selected model context. It displays the severity level of an alarm, date and time the alarm started, asset and its property causing the alarm, source where the alarm originated, subcondition of a property tag, and alarm description. An operator (with permission in the HMI/SCADA system) can acknowledge alarms and apply filters to alarms.
<p>Task List Card</p> 	<p>Displays a Workflow Task List that enables an operator to view the progress of tasks and act on the steps in the task.</p> <p>The Task List enforces authorization of specific Task List actions through Windows security and role definitions. For example, a user may have the ability to start a task but not skip a task, or delegate a task to someone else.</p>

Import Mimics

Mimics are the process diagrams that were created as pictures in the HMI/SCADA system. You import these pictures to use as mimics in the Web HMI layouts.

Verify the related iFIX pictures or CimEdit screens were exported for importing in to Web HMI.

1. In the Administration environment, navigate to **Visualizations > Mimic Management**.
2. Select **Import**.
3. In the **Import Mimics** dialog box, do the following:

- a. Browse to the JSON ZIP file containing the mimics.
 - b. To automatically create an asset object, object type, and group for the mimic based on its name and fields, select **Auto-Create Model Elements**.
To use **Auto-Create Model Elements**, a model must not exist in Web HMI, and your exported pictures must not contain symbolic addresses, such as @StorageTank1.TankLevel@.
 - c. Select **Import**.
 - d. Select the mimic in the left panel to view its mimic fields and associated data variables
4. To view the mimic as it would appear in real time (when connected to the related data source), navigate to the **Runtime** environment.

Bind Mimics to Assets

Asset objects can reuse the mimics that you bind to their object types. This enables Web HMI navigation to display the correct mimic in the HMI card in the context of the model.

Mimics are the pictures that contain animations and tag links for a selected asset object type. If the mimic animations follow the model structure, Web HMI can handle the bindings automatically.

1. In the Administration environment, navigate to **Visualizations > Designer**.
2. Select **Types**.
3. Select the asset object type in the left panel.
4. In the **Mimic** field on the **Details** tab, select a mimic from the drop-down list to associate with this asset object type.
5. Select **Save**.
6. Select **Mimic Card** for the selected asset object type.
The Mimic Fields display the animation sources within the mimic. For example, @Flow@ and @OpenClose@ are fields on a mimic for displaying data for the Suction Value asset object type.
7. To bind a mimic field with a data variable in the model:
 - Select **Mimic Binding** to choose a variable from the drop-down list for each mimic field.
 - To let Web HMI automatically perform the binding by matching the data variable and mimic field names, select **Autobind**. For example, a **TPump** asset object type with a variable named **Flow** automatically binds with a picture representing a pump with the @Flow@ animation.

**Note:**

If you add or remove properties in an asset object after binding a mimic to it, check the mimic field bindings to ensure they are correct.

8. Repeat these steps as needed to bind each mimic to an asset object type.
9. Select **Save**.

Override Mimics

Asset objects reuse the mimics that you bind to their object types in the model. If you want a different mimic to display for an asset object at Runtime, you can replace the mimic associated with the asset object type.

This mimic only appears with the asset object at Runtime.

1. In the Administration environment, navigate to **Visualizations > Designer**.
2. Select **Object Types**.
3. Select the object type and the asset object whose mimic you want to replace in the left panel.
4. Select **Details**.

The mimic appears for the asset object.

5. Select a different mimic from the drop-down list in the **Mimic** field.
6. Select **Save**.

The new mimic appears for the asset object and in the click target (if applicable). The original mimic appears in the list with Default before its name, such as Default - FWPS, Pump.

Set Up Mimic Target Zones

Target zones represent areas on a mimic that were set as selectable in the HMI/SCADA system. You set the navigation of these target zones for an operator.

You define a target zone to navigate to any asset in the model or to open a Control View where an operator can modify HMI/SCADA real-time values (if permitted in the HMI/SCADA source) and view historical data.

- In iFIX, set regions on a picture as Is Selectable to appear as clickable targets on the Mimic Card.
- In CIMPLICITY, only groups with the mouse-up or mouse-down event show as selectable targets on the Mimic Card. When defining a mouse-up or mouse-down event for a group, you must specify the script action, and then create an empty script.
- Assign the mimic to an asset type.

1. In the Administration environment, navigate to **Visualizations > Designer**.

2. Select the asset object type in **Object Types**.

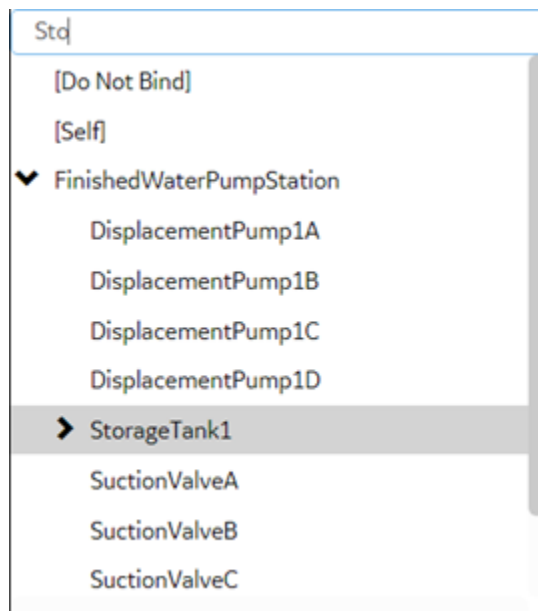
3. Select **Mimic Card**.

4. Select **Click Target Binding**.

By default, each target zone has a Control action that opens a Control View when an operator selects that target.

5. To enable an operator to navigate to a particular asset object in the model, do the following:

- In the **Relative Object** column and next to the target name, select or search for the asset object in the model hierarchy tree. You can do a partial search, such as `sto`, and Web HMI highlights all assets containing `Sto`, as shown in this example.



- Select the related **Action** field and then **Navigate**.

In Runtime, the background of a target zone changes to blue when an operator hovers over it. After an operator selects a target on the Mimic Card, the target asset becomes the active one, changing the mimic and content in the Trend and Alarm cards accordingly.

6. Select **Save**.

Define Mimic Control Views

Use Control Cards to specify which data variables to group together, and which data variables and their attributes to view and modify in auto-generated Control Views.

The Control Card variables were defined in the Model Editor or in a model file that was imported.

1. In the Administration environment, navigate to **Visualizations > Designer**.
2. Select the asset type in **Object Types**.
3. Select **Control Card**.
4. Group related asset data variables together to appear in a Control View by specifying a group identifier in the **Control Group** column of each related data variable.
Data variable values are limited to 15 digits of precision.
5. **Optional:** In the **Control Point** column, select the SetPoint for the current HMI/SCADA data variable from the list. Both the current data variable and its Control Point must be in the same Control Group.

You can set a Control Point as a separate data variable tag. For example, you can set PositionSetPoint as the Control Point for Position, as shown in the following sample screens. When you set a Control Point as a different data variable, be aware of the following attribute behavior:

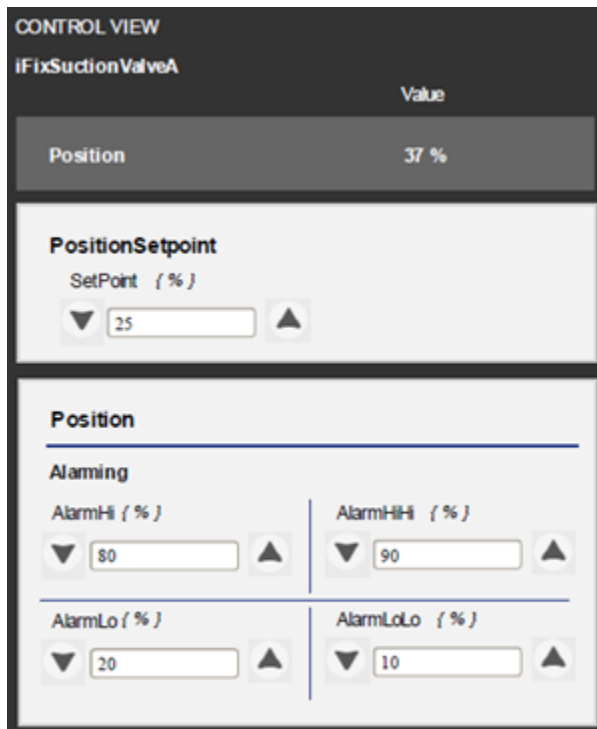
- If selected in the **Attributes** list, the SetPoint controls the data variable in the **Control Point** column.
- Any additional attributes that you select from the **Attributes** list pertain to the value in the **Data Variable** column, not the Control Point.

The following Control Card shows that PositionSetPoint is the Control Point for the Position data variable, and that the SetPoint, AlarmLo, AlarmLoLo, AlarmHi, and AlarmHiHi attributes are selected for the Position Control View.

Details Mimic Card **Control Card** Trend Card

Data Variable	Control Group	Control Point	Data Source	Attributes
ControlMode	None	None	None	None
Flow	None	None	None	None
Manufacturer	None	None	None	None
OpenClose	None	None	None	None
OperationMode	None	None	None	None
Position	ValveGroup2	PositionSetpoint	IFIX	5 <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>
PositionSetpoint	ValveGroup2	None	None	<input type="checkbox"/>
StatusFeedback	None	None	None	<input checked="" type="checkbox"/> SetPoint
isConnected	None	None	None	<input type="checkbox"/> Description
lastConnection	None	None	None	<input checked="" type="checkbox"/> AlarmHi
				<input checked="" type="checkbox"/> AlarmHiHi
				<input checked="" type="checkbox"/> AlarmLo
				<input checked="" type="checkbox"/> AlarmLoLo

Based on the above configuration, an operator can change the PositionSetPoint, AlarmLo, AlarmLoLo, AlarmHi, and AlarmHiHi attributes in the Position Control View, as shown below.



For an operator to modify the attributes of the PositionSetPoint in a Control View, you must select the attributes defined for the PositionSetPoint data variable on the Control Card.

- If you set a Control Point for a data variable, select its corresponding source from the list in the **Data Source** column.

The attributes, including the set point, for the selected data variable and its data source type appear in the **Attributes** column.

- In the **Attributes** column, select which attribute values of the data variable that you want an operator to view and modify on a Control View.

You can select the first check box to select or deselect all listed attributes.

- Select **Save**.

Define Trend Data

Trend Cards show trend-line analysis of variable data in an HMI/SCADA system for a selected time frame. Trend Card charts can display both real-time and historical data.

For real-time data to appear in Trend charts, you must have set the minimum and maximum data limits for viewing in your data source.

1. In the Administration environment, navigate to **Visualizations > Designer**.
2. Select **Types**.
3. In the left pane, select the asset object type containing the data variables to display in trend lines.
4. Select **Trend Card**.
5. Select the check box next to each variable containing the data to use as a trend point.
6. Select **Save**.

Override Attributes at the Object Level

Control Cards and Trend Cards are available at the object level to allow you to override the attribute values set at the object type level.

If you make changes in the **Control Card** and **Trend Card** sections at the object type level, every instance of that object type is affected. If an object instance has set overrides, the overrides are removed, and then replaced with the changed values from the object type.

This procedure explains how to override attribute values in the Control Card.

1. In the Administration environment, navigate to **Visualizations > Designer**.
2. In the pane, in the **Objects** section, select the asset.
3. Select the **Control Card** tab.
4. Modify the attribute values as needed.
5. Select **Save**.

A blue dot appears next to each changed attribute value. The following sample screen shot shows that two attribute fields were overwritten for CombinedFlow at the object level.

The screenshot shows the 'FinishedWaterPumpStation' object selected in the 'Objects' pane. The 'Control Card' tab is active, displaying a table of attributes. A note indicates that 2 fields have been overridden. The table below shows the overridden attributes.

Data Variable	Control Group	Control Point	Data Source	Attributes
CombinedFlow	7	CombinedFlow	None	None
DischargePressure	None	None	None	None
DisplacementPump1AStatusFeed...	None	None	None	None
DisplacementPump1BStatusFeed...	None	None	None	None
DisplacementPump1CStatusFeed...	None	None	None	None
DisplacementPump1DStatusFee...	None	None	None	None
HP	None	None	None	None

6. **Optional:** You can hide or show the blue dots by selecting .

Chapter 9. Set Up User Security

User Account Overview

Users consist of both operators and GE administrators. In Application Assembler (ThingWorx), a GE administrator creates and maintains user and group accounts for access to Web HMI environments.

How User Security Works

Web HMI combines its own user security with your system's user security.

To avoid user access issues, such as a user not being able to acknowledge an alarm or write to a Control Point on a Control View from Web HMI, make sure all user accounts match (exact names) in your system, Windows, and Web HMI.

You can set up [Active Directory Authentication \(on page 82\)](#), which provides user provisioning.

GE Administrators

Members of the GEAdministrators group have default access to the following:

- Administration environment to create Runtime content for operators.
- Runtime environment to check its content.
- Application Assembler to manage user security and visualizations, which include creating and modifying mashups, masters, menus, style definitions, and state definitions.

GEAdmin is a member of the GEAdministrators group.


Users

GEUser is an operator with permissions to view and interact with content models in the Runtime environment. These members cannot access the Administration environment or the Application Assembler.

GEUser is a member of the GEUsers group.

Access the Application Assembler

Set up security for Web HMI users and groups in the Application Assembler.


1. In Web HMI, select **Application Assembler** from the user icon box.
The Application Assembler is launched in a different browser tab.
2. Select  to open the Application Assembler home page.
3. Select the **SECURITY** section to view the selections.

Create User Accounts

You create user accounts by duplicating the default user templates, GEAdmin and GEUser. All settings are inherited from these default user templates except for the password and group membership.

For each user account, specify a unique password that follows these guidelines:

- Contains a minimum of 8 characters
- Contains at least one uppercase letter.
- Contains at least one lowercase letter.
- Contains at least one special character (such as @, #, \$).
- Does not match the user ID.
- Does not contain the user ID.


1. In the **SECURITY** section of the Application Assembler  page, select **Users**.
The **Users** configuration panel appears.
2. Select the check box that is next to the user to duplicate.
3. In the main navigation bar, select **Duplicate**.
The **General Information** panel appears.
4. In the **Name** box, enter the new user name.
5. In the **Password** box, select **Change Password**.
6. In the **Change Password** dialog box, enter the new password twice and select **Change Password**.
7. Select **Save**.

Assign the user to the appropriate group.

Assign Users to a Group

As a GE administrator, you assign users duplicated from the GEUser or GEAdmin user template to the appropriate group.

Users in the GEUsers group can access the Runtime environment. Users in the GEAdministrators group can access the Runtime environment, the Administration environment, and the Application Assembler.


1. In the **SECURITY** section of the Application Assembler  page, select **User Groups**.
2. Select the check box next to the target group.
3. In the main navigation bar, select **Edit Members**.
4. In the **Edit Members** panel, select and drag the users from the left column to the right column.
5. Select **Save**.

Change User Passwords

GE administrators can change existing user passwords when needed.

User passwords must be unique, following these guidelines:

- Contains a minimum of 8 characters
- Contains at least one uppercase letter.
- Contains at least one lowercase letter.
- Contains at least one special character (such as @, #, \$).
- Does not match the user ID.
- Does not contain the user ID.


1. In the **SECURITY** section of the Application Assembler  page, select **Users**.
2. Select the user whose password you want to change.
3. In the **General Information** panel, select *Change Password* in the **Password** field.
4. In the **Change Password** dialog box, enter a new password twice and select **Change Password**.
5. Select **Save**.

Define LDAP Settings

Use the LDAP Directory Services in Application Assembler (ThingWorx) to manually edit Web HMI users to exactly match the user names in Active Directory, and then assign them to groups.

In previous versions of Web HMI, this was the way to use AD authentication. You can now set up dynamic user provisioning for AD authentication, as explained in [Configure Active Directory Authentication \(on page 82\)](#).

Application Assembler provides the LDAP Directory Services template for you to duplicate and configure your LDAP settings. This template uses a nonstandard organizational unit (OU) named WebHMI in the Windows Active Directory instead of the default Users OU.

1. In the **SECURITY** section of the Application Assembler  page, select **LDAP Directory Service**.
2. Select the **Active Directory** check box.
3. In the main navigation bar, select **Duplicate**.
A new entity is created, and the **General Information** page appears.
4. In the **Name** box, enter a new name for this entity, such as GE_WebHMI_LDAP.
5. In the **Description** box, explain this type of authentication, such as LDAP Directory Service.
6. Select the **Enabled** check box.
7. Select **Save**.

8. In the Active Directory entity that you just created, select **Configuration** under **ENTITY INFORMATION**.

The **Configuration for DirectoryServices** page appears.

9. Define the following LDAP settings:

If you need help finding these LDAP values in Windows AD, see [LDAP Settings for AD Authentication \(on page 118\)](#).


Option	Description
server	The name of the computer where the Active Directory resides. Example: WIN2008
userIdAttribute	Do not modify the default value of sAMAccountName.
LDAP	Do not modify the default value of LDAP.
port	The Active Directory server port. Do not change the default value of 389 unless another port was set.
adminBindDN	The login of the administrative user with permission to run the Active Directory lookup. This is the distinguished name (DN) in the Active Directory. For example, for the Support administrative account residing in the default Users organizational unit, the DN for this setting is: CN=support,CN=Users,DC=support,DC=webhmi,DC=com
userBaseDN	The Active Directory lookup for the user group or base organizational unit. This is the distinguished name in the Active Directory. For example, for all users residing in the WebHMI organizational unit, the DN for this setting is: OU=WebHMI,DC=support,DC=webhmi,DC=com
adminPassword	The password of the user with permission to run the Active Directory lookup, which is the above adminBindDN user. Using the above adminBindDN example, this is the password for the Support administrative account on the Users OU.

10. Select **Save**.

Create Users and Groups

When using LDAP Directory Services for AD authentication, you manually create users in Application Assembler to match existing users in AD, and then assign them to groups.

You create Web HMI users for AD authentication by duplicating the GEUser or GEAdmin user templates, and then edit them to exactly match the user names in the Active Directory. These names are case-sensitive.


1. In the **SECURITY** section of the Application Assembler  page, select **Users**.
2. Select the check box next to an existing user, and then select **Duplicate**.
3. In the **General Information** panel, enter a Web HMI user name that exactly matches an AD user.
Since this user is being authenticated against the Active Directory, do not specify a password.
4. Repeat this for each Web HMI user to be authenticated against the AD.
5. Select **User Groups**.
6. Select the GEUsers group or the GEAdministrators group.
7. Select **Edit** and then **Edit Members**.
8. Drag each new user from the left pane to the right pane.
9. Select **Save**.

Add each Web HMI user that was created for AD authentication to your HMI/SCADA system.

Configure Active Directory Authentication

Application Assembler (ThingWorx) provides the ActiveDirectory template for you to duplicate to create a directory service for each one of your AD domain servers.

You can set up user provisioning for each domain server.

1. In the **SECURITY** section of the **Application Assembler**  page, select **Directory Services**.
2. Select the **ActiveDirectory** check box.
3. In the main navigation bar, select **Duplicate**.
A new entity is created, and the **General Information** page appears.
4. In the **Name** box, enter a new name for this entity, such as GE_WebHMI_AD_DomainX.
5. In the **Description** box, enter a description for the type of authentication, such as Active Directory Service for Domain X.
6. Select the **Enabled** check box.
7. Set the priority domain order for authenticating users. If an AD directory service with the lowest priority setting, such as 1, fails to authenticate a user, the next AD directory service in the priority order is used to authenticate a user, and so on.
8. Select **Save**.
9. In the Active Directory entity that you just created, select **Configuration** in the **ENTITY INFORMATION** section.

The **Configuration for DirectoryServices** page appears, displaying sections for completing the following tasks:

- a. [Set Up the AD Server Connection \(on page 83\)](#)
- b. [Define the AD Schema Mappings \(on page 84\)](#)
- c. [Map AD Groups with ThingWorx Groups \(on page 85\)](#)
- d. [Enable User Provisioning \(on page 85\)](#)
- e. [Set User Defaults \(on page 86\)](#)
- f. [Exclude Users from Provisioning \(on page 88\)](#)

Set Up the AD Server Connection

Use the **Connection Settings** section in the **DirectoryServices** page to define how to communicate with the AD server.


Define the following connection settings:

Option	Description
URI Scheme	The protocol to communicate with the AD server. The default is LDAP.
Server FQDN or IP Address	The AD server name or IP address that is targeted for directory queries. The default is localhost. Example: W2012R2
Server Network Port	The AD server port. Do not change the default value of 389 unless another port was set.
Domain Distinguished Name	The domain distinguished name of the top-level directory used for user group lookup. Example: DC=ge,DC=local
Administrative Principal Name	The user name with administrative read access to the specified domain. This name is dependent on the specified User ID Attribute Name in the Schema Mappings section (on page 84) of the DirectoryServices page. Example: CN=John Smith,CN=Users,DC=ge,DC=local
Administrative Password	The password for the above Administrative Principal Name.

Define the AD Schema Mappings

Use the **Schema Mappings** section in the **DirectoryServices** page to manage the mappings of the user and group objects used in the Active Directory authentication.

1. Define the following schema mappings settings:

Option	Description
User ID Attribute Name	<p>The attribute name containing the user name to match against the Web HMI login user name. The default is cn.</p> <p>Example: sAMAccountName</p>
User Base Distinguished Name	<p>The distinguished name of the top-level directory that is used to validate user credentials. The default is ou=people.</p> <p>Example: CN=Users,DC=ge,DC=local</p>
Group Object Class Name	<p>The value of the object class attribute indicating the object is a group. The group objects are queried and presented for the Active Directory and ThingWorx group mapping in the Group Mappings (on page 85) section in the DirectoryServices page. The default is group.</p>
Group LDAP Filter to filter domain groups	<p>Enables the filtering of a large number of domain groups.</p> <div data-bbox="526 1129 1422 1352" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note:</p> <p>Do not leave this field blank when there are a substantial number of domain groups because performance may be significantly impacted.</p> </div>
Group Membership Attribute Name	<p>The attribute name that indicates a user or group is a member of another group. For each memberOf entry within a user in the Active Directory, that user is added as a member to the ThingWorx group mapped with the Active Directory group named in the memberOf entry. The default is memberOf.</p>
Group Attribute Name	<p>The attribute name that retrieves the group display name from the ThingWorx UI, specifically in the Group Mappings (on page 85) section in the DirectoryServices page. The default is cn.</p>
User Flags Attribute Name	<p>The default is userAccountControl. For information about this setting, see https://msdn.microsoft.com/en-us/library/cc223145.aspx.</p>

Option	Description
User Control Attribute's Disabled Bit	The default is 2. For information about this setting, see https://msdn.microsoft.com/en-us/library/cc223145.aspx .
User Control Attribute's Lockout Bit	The default is 16. For information about this setting, see https://msdn.microsoft.com/en-us/library/cc223145.aspx .

2. Select **Save**.

Map AD Groups with ThingWorx Groups

Use the **Group Mappings** section in the **DirectoryServices** page to associate Active Directory groups with ThingWorx groups. Permissions are set by the ThingWorx groups and are used at Web HMI runtime.

When a user is auto-provisioned to an AD group, that user is automatically added to its mapped ThingWorx group.


You must have created and configured the ThingWorx groups to use for AD authentication.

1. Select **Add**.
2. In the **Active Directory Group Name** box, select the AD group, such as WebHMIAdmins, that you want to map with a ThingWorx group.



Note:

If a red circle with a line through it appears when selecting an AD group (not connected to AD domain), select **Save**, and then try closing and reopening the **DirectoryServices** page. You should now be connected.

3. In the **ThingWorx Group Name** box, select  to choose the ThingWorx group, such as WebHMIAdmin, to map with the specified AD group.

Enable User Provisioning

Use the **User Provisioning** section in the **DirectoryServices** page to enable the AD domain server to dynamically create, modify, and delete users in Web HMI. For example, by enabling user creation, the Active Directory automatically creates new users on first login to Web HMI.

For user provisioning to occur, the AD groups must be mapped to the appropriate ThingWorx groups, as explained in [Map AD Groups with ThingWorx Groups \(on page 85\)](#).

1. To enable user provisioning, select the check box next to the following settings:

Option	Description
User Creation Enabled	Users are created with the specified Web HMI login user name and any specified default values, as explained in Set User Defaults (on page 86) . If a user is in the User Provisioning Exclusion List (on page 88) , the user is not created.
User Modification Enabled	Users are updated upon each Web HMI login attempt with any default values specified in the User Default Settings section. Users must exist in ThingWorx for updates to succeed. If a user is in the User Provisioning Exclusion List (on page 88) , the user is not created.
User Deletion Enabled	Users removed from the domain are deleted upon a Web HMI login attempt. Users must exist in ThingWorx for deletes to succeed. If a user is in the User Provisioning Exclusion List (on page 88) , the user is not created.

2. Select **Save**.


Set User Defaults

Use the **User Defaults** section in the **DirectoryServices** page to define settings to help you manage and identify provisioned users.

1. Set these user defaults as needed:

Option	Description
Provisioned User's Default Domain Prefix	A domain prefix for user names to use when provisioning users. For example, if you connected this directory service to the mycompany.com domain, enabled user provisioning, and set this prefix to mycompany.com@, the first time a user, such as john, logs in to Web HMI as mycompany.com@john, the login request goes to the directory service to authenticate john, and then automatically creates mycompany.com@john as a new Web HMI user. AD views this user as john, but Web HMI identifies this user as mycompany.com@john.

Option	Description				
	Setting a domain prefix allows you to explicitly control the domain server for users to log in to when these users may exist in several domains.				
Provisioned User's Default Description	A description generated for all provisioned users, such as Auto-provisioned by domain server ge.local.				
Provisioned User's Default Home Mashup	The name of a home mashup to appear when provisioned users log in.				
Provisioned User's Default Mobile Mashup	The name of a mobile mashup to appear when provisioned users log in.				
Provisioned User's Default Tags	<p>A set of model tags that are set on all users provisioned by this directory service. When Workflow is integrated with Web HMI, you must add the domain as a tag term in the geActiveDirectoryDomain vocabulary, and then select this term in the Provisioned Users Default Tag box. Web HMI checks this vocabulary to see which domain a user is logged in to, and then passes the domain name to the Workflow server.</p> <p>For example, if your domain is mycompany.com, add the mycompany.com term to the geActiveDirectoryDomain vocabulary, as shown below.</p> <div data-bbox="521 1220 1424 1564" style="border: 1px solid #ccc; padding: 10px; background-color: #f9f9f9;"> <p>New Term</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #212121; color: white;">Choose a Vocabulary:</th> <th style="background-color: #212121; color: white;">New Term:</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px;">geActiveDirectoryDomain ▼</td> <td style="padding: 5px; border: 1px solid #ccc;">mycompany.com</td> </tr> </tbody> </table> <div style="text-align: right; margin-top: 10px;"> Cancel Add Term </div> </div> <p>Then add the new mycompany.com term to the Provisioned Users Default Tag box, as shown below.</p> <div data-bbox="521 1705 1424 1768" style="border: 1px solid #ccc; padding: 5px; background-color: #e8f5e9;"> <p>Provisioned User's Default Tags</p> <div style="float: right; border-bottom: 1px solid #ccc; padding-bottom: 5px;"> geActiveDirectoryDomain mycompany.com ✕ </div> <div style="clear: both; margin-top: 5px;"> <input style="width: 90%; border: none; border-bottom: 1px solid #ccc; padding: 2px 5px;" type="text" value="Search Model Vocabulary"/> </div> </div>	Choose a Vocabulary:	New Term:	geActiveDirectoryDomain ▼	mycompany.com
Choose a Vocabulary:	New Term:				
geActiveDirectoryDomain ▼	mycompany.com				

Option	Description
	 Note: Use this setting for a single domain server. If a user exists in multiple domain servers, use the above Provisioned User's Default Domain Prefix setting.

2. Select **Save**.

Exclude Users from Provisioning

Use the **User Provisioning Exclusion List** section in the **DirectoryServices** page to specify which Web HMI users to exclude from all the user provisioning features.

The Administrator user is automatically added to the exclusion list. Do not modify or remove this user.

1. Select the user that you want to add to the list, and then select **Add**.
2. Enter the user name.
3. For each user that you want to add to the list, repeat steps 1 and 2.
4. Select **Save**.

Chapter 10. Reset Web HMI

Reset Web HMI

Use the `webServerReset` command to delete all user-created data, restoring Web HMI to a ready, clean state. Use this operation to remove a model and its mimics as well as all users and any user-defined content that was added to the system.

When this command completes, the following occurs:

- Drops and recreates ThingWorx (Application Assembler) and the microservice databases.
 - Recreates ThingWorx storage folders.
 - Deletes ThingWorx extensions and imports them again.
 - Restarts Tomcat and RabbitMQ services.
1. Open a Windows Command Prompt window with administrator privileges.
 2. Navigate to the Proficy Web Server installation directory: `<install_path>\ProficyWebServer\.` Example: `D:\General Electric\Web HMI\ProficyWebServer\.`
 3. Run the following command: `webServerReset.bat -hmiusername=<username> -hmipassword=<twpassword> -pgpassword=<pgpassword>.`

Command-line Option	Description
-hmiusername	(Required) ThingWorx GEAdministrator user name (and matching password) account is used to verify that an administrator is resetting Web HMI. When the reset completes, it recreates this account.
-hmipassword	(Required) ThingWorx GEAdministrator password.
-pgpassword	(Required) PostgreSQL Administrator password defined during installation.
-help	Displays the help menu on how to use <code>webServerReset.bat</code> .

You can track the progress of this operation in `\ProgramData\Proficy\WebHMI\resetLog.txt`.

Chapter 11. Transfer Project Data

Overview

Use the Project Deployment Tool to bundle and deploy Web HMI project data from one node to another. This tool is particularly useful when moving from a test to a production environment.

Web HMI project data builds the Runtime environment, including the asset model structure and content, mimic definitions, and their associations to assets.

This process requires that you complete these tasks:

1. Complete the prerequisite tasks for your system if required.
2. Bundle the project data to a .zip file in the source node.
3. Copy the bundle .zip file and the sever alias file from the source node to the target node.
4. Update the server alias file in the target node.
5. Deploy the project data in the target node.

Before you begin, review the following:

- To use the Project Deployment Tool, you must be running the same version of Web HMI in the source and target systems.
- If the source system and target system are in the same node, you do not need to use this tool.
- Do not use the Project Deployment Tool for disaster recovery.

Server Alias

Web HMI projects interact with external servers (for example, Historian, iFIX, and Workflow) and CIMPLICITY projects. To facilitate project deployment, each server is represented by the following entries:

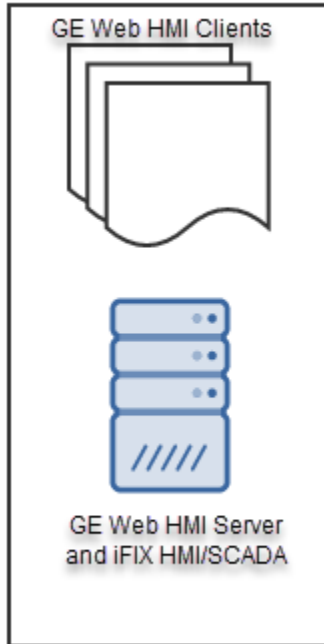
- system-alias – alias for that server (same across different setups of the same project).
- system-name – actual physical name of the server or the CIMPLICITY project.

For example, the Historian server in your source system may have the physical name SOURCE-HOST, and may be represented by the alias HIST-SERVER.

After you copy the server alias file to the target node, you must update the original source server alias entries with the new target server alias names before deploying the project on that target node.

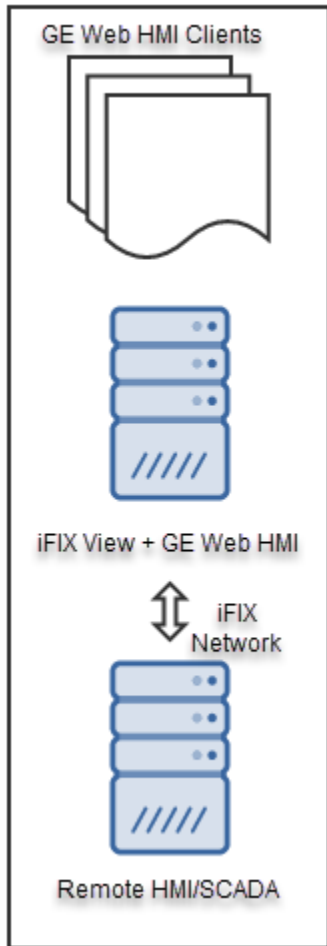
Example of Single-Node Systems

In a single-node system, your Web HMI server and the HMI/SCADA system reside in one node, as shown in the following iFIX sample illustration.



Example of Multi-Node Systems

In a multi-node system, your Web HMI server and HMI/SCADA system reside in separate nodes that communicate with each other. The client (view node) is remotely connected to a server (HMI/SCADA node). In the following sample illustration, the Web HMI server is installed in the same node as the iFIX view node and is connected to a remote HMI/SCADA node.



To deploy the HMI/SCADA content of remote or redundant systems, use the iFIX backup and restore tool or copy the CIMPLICITY project to the target system.

iFIX Prerequisites

When you have set Web HMI to connect with an iFIX HMI/SCADA, use the GE HMI Server Configuration Manager in the target system to complete the following prerequisite tasks before proceeding.

Open the GE HMI Server Configuration Manager to complete these tasks:

- a. [Connect to Historian \(on page 51\)](#).
- b. [Define tracing and logging \(on page 52\)](#).

CIMPLICITY Prerequisites

When you have configured Web HMI to connect with CIMPLICITY, complete the following prerequisite tasks in your target system before proceeding.

1. Copy the CIMPLICITY project to the target system.
2. Run the CIMPLICITY project.
3. Open the GE HMI Server Configuration Manager to complete these tasks:
 - a. **Optional:** Use GDS certificates for GE Web HMI clients ([on page 49](#)).
 - b. Secure connections to the OPC UA endpoints ([on page 45](#)).
 - c. Connect to Historian ([on page 51](#)).
 - d. Define tracing and logging ([on page 52](#)).

Bundle the Project Data

Create the bundle containing the project data to copy to the target.

1. Open a Windows Command Prompt window with administrator privileges.
2. Navigate to `<Web HMI Install Location>\ProficyWebServer\Tools`.
3. Enter `project-deployment-tool.bat --bundle --file=<bundleName>.zip --webserver --server=https://<Computer Name> --username=<Web HMI Username> --password=<Web HMI password>`
For iFIX, you can specify additional [options \(on page 95\)](#) in the above command. In the following example, the option `--iFix="/s /BackupSec"` includes iFIX security files for the bundle:

```
project-deployment-tool.bat --bundle --file="<bundleName>.zip" --webserver --scada --
server=https://<Computer Name> --username=<Web HMI Username> --password=<Web HMI
password> --iFix="/s /BackupSec"
```

The `<bundleName>.zip` and `serverAlias.txt` files are created in the `<Web HMI Install Location>\ProficyWebServer\Tools` folder in the source node.

Copy the Project Data to the Target

When the bundle is created, you must copy the `<bundleName>.zip` and `serverAlias.txt` files in the source node to the target node.

1. Navigate to `<Web HMI Install Location>\ProficyWebServer\Tools` folder in the source node.
2. Copy the `<bundleName>.zip` and `serverAlias.txt` files to the `<Web HMI Install Location>\ProficyWebServer\Tools` folder in the target node.

Update the Server Alias File

After you copy the `serverAlias.txt` file to the target node, you must update its original source server alias entries with the new target server alias names.

Verify that you copied the serverAlias.txt file to the <Web HMI Install Location> \ProficiencyWebServer\Tools folder in the target node.

1. Open the serverAlias.txt file in the target node.
2. Update the relevant server alias entries in serverAlias.txt, as explained in this table.

Original Source Server Alias	New Target Server Alias
Web HMI	Replace {INSERT SYSTEM NAME} with the target computer name.
OPC UA Server	In the CIMPLICITY Project Workbench, do the following: <ol style="list-style-type: none"> a. Select Project. b. Select Export to Web HMI. c. Save the file to a known location. d. Open the project and copy the CIMPLICITY Uniform Resource Name (URN). e. Replace {INSERT SYSTEM NAME} with this URN.
Historian Server	Replace {INSERT SYSTEM NAME} with the Historian server name.
SCADA Server	Replace {INSERT SYSTEM NAME} with the corresponding HMI/SCADA server found in the target system.
Workflow Server	Replace {INSERT SYSTEM NAME} with the Workflow server name.

Import the Workflow Project File

When using a different Workflow server in the target environment, you can import the project file from the original source Workflow server.

1. Log in to Workflow in the target server that will receive the project file from the source server.
2. Follow the instructions in *Deploy a project to import its contents* in the Workflow help.

Deploy the Project Bundle

Use the Project Deployment Tool to deploy the bundle containing the project data on the target node.

When a bundle is deployed, it overwrites the data in the target node.

1. Open a Windows Command Prompt window with administrator privileges.
2. Navigate to <Web HMI Install Location>\ProficiencyWebServer\Tools.
3. Enter project-deployment-tool.bat --deploy --file=<bundleName>.zip --webserver --server=https://<Computer Name> --username=<Web HMI Username> --password=<Web HMI password>
For iFIX, you can specify additional [options \(on page 95\)](#) in the project-deployment-tool.bat command. In the following example, the option --iFix="/S /RestoreSec" includes iFIX security settings for the iFIX and Web HMI deployment:
project-deployment-tool.bat --deploy --file=<bundleName>.zip --webserver --scada --server=https://<Computer Name> --username=<Web HMI Username> --password=<Web HMI password> --iFix="/S /RestoreSec"
4. Enter `Yes` to confirm deployment.
The deployment.tool.log file is located in <Web HMI Install Location>\ProficiencyWebServer\Tools.

Command-Line Options

Use the Project Deployment Tool command-line options to bundle and deploy a Web HMI project to another node.

The following Project Deployment Tool command-line options are case-sensitive.

Option	Description
--bundle	Creates a bundle containing project data.
--deploy	Deploys a bundle in the target, overriding the current project data.
--scada	Bundles or deploys the HMI/SCADA contents. Used in conjunction with the bundle and deploy options.
--webserver	Bundles or deploys the Web HMI contents. Used in conjunction with the bundle and deploy options.
--server	Specifies the web server instance URL in which to create or deploy a bundle.
--username	Specifies your Web HMI user name for authentication.
--password	Specifies your Web HMI password for authentication.
--file	Specifies a file name for your bundled content. If you do not specify a file name, the tool generates a name that includes the server name and time stamp.

Option	Description
--overwrite	Without prompting, automatically overwrites the target files with your source files.
-iFix	<p>Allows you to pass in non-default parameters to the iFIX backup and restore tool, which bundles and deploys iFIX content. The supplied parameters overwrite the default parameters.</p> <p>The default parameters are:</p> <ul style="list-style-type: none"> • Bundling – "/S /BackupSec", which performs a full backup with security files in silent mode. • Deployment: – "/S /RestoreSec", which restores <xxxxx>, replacing the current security settings with those in the bundle file. <p>To pass in more than one parameter, surround the parameter value in double quotes, such as: -iFix="/F /S"</p> <p>Unsupported parameters (/B, /R, /FactoryDefaults):</p> <ul style="list-style-type: none"> • /B and /R – The Project Deployment Tool determines the right operation based on the --bundle or --deploy options. • /FactoryDefault parameter – You cannot use the Project Deployment Tool to bundle or deploy iFIX factory defaults. <p>For more information on the iFIX backup and restore tool, see the iFIX online documentation.</p>
-help	Displays the supported command-line options.

Error Messages

You may receive the following messages after executing Project Deployment Tool commands in the command prompt window.

Message	Description
0 - SUCCESS	The operation was successful and no errors were found.
1 - INVALID_ARGUMENT	<p>A missing, incomplete, incompatible, or incorrect argument has been entered.</p> <p>Example: A file does not have a file name.</p>
2 - INVALID_BUNDLE_FILE	A bundle file argument is invalid.

Message	Description
	Deployment Example: A ZIP file is missing or invalid. Bundling Example: A ZIP file already exists.
3 - SERVER_NOT_FOUND	You cannot connect to a web server. Example: You may have entered an incorrect URL, or the connection attempt timed out.
4 - AUTHENTICATION_FAILURE	You entered invalid authentication credentials.
9 - FATAL_EXCEPTION	An exception occurred for an unknown reason.
101 - BUNDLING_FAILED	A bundling operation started, but a failure occurred before the operation completed. As a result, the bundled file is probably incomplete.
200 - MISSING_CONTENT	The bundle that you are trying to deploy is missing content.
201 - DEPLOYMENT_FAILED	The deployment started, but a failure occurred before the operation completed. As a result, not all data in the bundle was deployed to the target system.

Chapter 12. Customize Components

Related Components

You can customize certain settings of the components used by Web HMI.

These components include:

- [Alarm Gateway Configuration Tool \(on page 98\)](#)
- [Alarm Microservice \(on page 99\)](#)
- [Asset Microservice \(on page 100\)](#)
- [Entity-Metadata Microservice \(on page 100\)](#)
- [Server-Details Microservice \(on page 101\)](#)
- [Tag-Source Microservice \(on page 101\)](#)



Important:

The configuration files of these components may contain additional configurable settings. Do not modify these values. Changing any settings other than the ones specified in this section can cause software to stop working.

Where to Find the Microservices

Each microservice has a folder under the `\ProficiencyWebServer\Tomcat\apache-tomcat\webapps` folder.

To apply microservice configuration changes, restart the microservice and the GE Tomcat service.

Alarm Gateway Configuration Tool

The Alarm Gateway Configuration Tool is an OPC Alarms & Events (OPC AE) client application that subscribes to OPC alarm and event messages from the data source OPC AE server, and posts them to the RabbitMQ service for the Alarm Microservice to manage.

Where to Find the Alarm Gateway Configuration Tool

The Alarm Gateway Configuration Tool is located in `\Program Files\Proficiency\AlarmGateway`. When running this program as an administrator, the following three tabs appear with configurable settings.

A&E OPC Server Tab

Use this tab to view the ProgID, the available OPC AE servers, and the logical name of the server.

RabbitMQ Tab

Use this tab to perform the following tasks:

- Change the RabbitMQ server name.
- Specify an SSL or a client certificate.
- Specify the path to the certificate.
- Specify the logical name of the alarm gateway, which is used as the RabbitMQ topic name.
- Change the password of the client certificate.
- Change the maximum alarms per message.
- Test the connection.



Important:

Always consult with a GE Technical Support representative before making any changes on the RabbitMQ tab. Improper changes to RabbitMQ settings can affect alarms.

Logging Tab

Use this tab to configure logging details, the maximum size of the log file, and the logging destination.

Alarm Microservice

The Alarm microservice receives messages from one or more Alarm Gateways, and manages the current alarm states in the context of the equipment model, including the alarm lists associated with each asset.

The `rabbitMQ.server`, `rabbitMQ.alarm.logicalNames`, `hierarchyService.NetworSkName`, and `rank.ranks` settings are in `application.properties`.

The Web HMI dividing point values between the different alarm severity ranges are defined in the `rank.ranks` setting of the Alarm Microservice. The default dividing points are 200, 800, 950, resulting in these default alarm severity ranges.

Low Severity Value	High Severity Level	Description	Alarm Icon
950	1000	Alarm is critical.	
800	949	Alarm is high severity.	
200	799	Alarm is medium severity.	
1	199	Alarm is low severity.	

Configurable Settings	Purpose	Default Values	Internal Settings
logging.file=\${service.name}- .log logging.level.com.ge.ente- prise=DEBUG	Specifies the log loca- tion and logging level.	Same as config- urable settings.	None
rabbitMQ.server	RabbitMQ server host.	localhost	
rabbitMQ.alarm.logicalNames	Comma-separated list of RabbitMQ topics. Each entry represents an alarm.	alarms	
hierarchyService.NetworSkName	Name of the TW net- work.	/AssetHierarchy_geAsset	
rank.ranks	Comma-separated list of dividing point values for the alarm severity levels.	200, 800, 950	None

Asset Microservice

The Asset microservice is the interface to the model and performs all its create, read, update and delete operations.

The Administration environment uses the Asset microservice to configure the model. The Runtime environment uses it to retrieve the asset hierarchy and other model information.

For the Asset microservice, the default values are the same as the configurable settings and there are no internal settings.

Configurable Settings	Purpose
logging.file=\${service.name}.log logging.level.com- .ge.enterprise=DEBUG	Specifies the log location and logging level.

Entity-Metadata Microservice

The Entity-Metadata microservice stores and serves model asset data required by clients to make decisions. For example, it determines whether you can write to a property/tag.

For the Entity-Metadata microservice, the default values are the same as the configurable settings and there are no internal settings.

Configurable Settings	Purpose
logging.file=\${service.name}.log logging.level.com-ge.enterprise=DEBUG	Specifies the log location and logging level.

Server-Details Microservice

The Server-Details microservice manages the Server Alias table that enables you to set up connection information to different data sources.

By changing which computers the server aliases point to, you can use the same model file for a test environment and a production environment.

For the Server-Details microservice, the default values are the same as the configurable settings and there are no internal settings.

Configurable Settings	Purpose
logging.file=\${service.name}.log logging.level.com-ge.enterprise=DEBUG	Specifies the log location and logging level.

Tag-Source Microservice

The Tag-Source microservice stores and provides the details of where an asset data variable retrieves its data. For example, Pump01.Flow gets its data from iFIX point FIX32.FLOW_TAG.

For the Tag-Source microservice, the default values are the same as the configurable settings and there are no internal settings.

Configurable Settings	Purpose
logging.file=\${service.name}.log logging.level.com-ge.enterprise=DEBUG	Specifies the log location and logging level.

Chapter 13. Customize the Web HMI Menu

Set the Default Layout

In Application Assembler, you can set one of the existing layouts to appear each time Web HMI opens in a web browser.

For information about the Web HMI layouts, see [Layouts \(on page 69\)](#).

1. In Application Assembler, navigate to **Visualization > Menus > CustomMenu_geWebHmiCore**.
2. Select **Add Menu Item**.
3. Select **Menu Definition**.
4. Add the following information to set the default layout:
 - a. **Type:** Hyperlink
 - b. **Title:** Title of an existing menu item to set as the default layout, such as Mimic or Mimic + Alarms, from ModuleMenu_geWebHmiCore
 - c. **Target:** Replace Page
 - d. **Link:** Leave blank
5. If you want to make this the default layout, select **Default**.
6. Select **Save**.
7. In the Runtime environment, verify this layout appears when you open Web HMI in a web browser.

Add Menu Items

Use the CustomMenu_geWebHmiCore menu in the Application Assembler to append items to the existing layouts in the Web HMI menu. You can also set a custom menu as the default layout to appear when Web HMI opens in a web browser.

You cannot use the CustomMenu_geWebHmiCore menu to reorder or replace existing layouts in the Web HMI menu.



Note:

You can no longer edit the ModuleMenu_geWebHmiCore menu.

1. In Application Assembler, navigate to **Visualization > Menus > CustomMenu_geWebHmiCore**.
2. Select **Menu Definition**.
3. Select **Add Menu Item**.
4. Add the following information for the new menu item:

- a. **Type:** Hyperlink
 - b. **Title:** <user defined>
 - c. **Target:** Replace Page
 - d. **Link:** <IconName>:<MashupName>
5. If you want to make this the default layout, select **Default**.
 6. Select **Save**.
 7. In the Runtime environment, verify the new item appears in the Web HMI menu.

Hide Menu Items

Use the `HiddenMenuThing_geWebHmiCore` thing in the Application Assembler to hide items, such as the Dashboard 1 layout, in the Web HMI menu.

1. In Application Assembler, select **All** on the left panel.
2. Search for **HiddenMenuThing_geWebHmiCore** and select **View**.
3. Navigate to **Properties** on the left panel.
4. In the table that appears, find the **HiddenMenus** row and select the **Set** button next to Infotable in the **Value** column.
5. Select **Add**.
6. Type the name of the item to hide, such as `Dashboard1Layout_geWebHmiCore`, in **MashupName**.
The name of the item to hide is the mashup name of an item in `ModuleMenu_geWebHmiCore`, which you can find by browsing the mashups in the Application Assembler.
7. To hide the item, select the check box in the **Hidden** column.
8. Select **Set**.
9. In the Runtime environment, verify the item does not appear in the Web HMI menu.

Chapter 14. Interact with Runtime

Log in to Web HMI

As an operator, you can log in to the Web HMI Runtime user interface with the credentials given to you by your administrator.

1. Select the Web HMI icon on the desktop.
2. Enter your user name and password.
3. Select **Log In**.

The Web HMI Runtime user interface appears.

Verify the Version Number


After you log in, make sure you are using the correct Web HMI version number.

Select the GE logo.

The Web HMI version number appears along with the installed components and credits.

Select a Layout

Layouts consist of cards that provide a specific view of the HMI/SCADA system and are asset-context aware. You select which layout to use to monitor and control production equipment and processes.

1. Select , the Asset Context Selector, to choose your context.
This displays the relevant data in context to each asset selected in the navigation scheme.
2. Select the optimal layout for monitoring data.





View Alarm Cards

An Alarm Card provides details of the active alarms by their severity levels in the HMI/SCADA system for the selected asset. You can acknowledge alarms and apply filters to display specific information about alarms.

You can acknowledge alarms from the Alarm Card if you have permission to do so in the supporting HMI/SCADA system.

The severity of an alarm is based on the priorities set in the underlying HMI/SCADA system. Each alarm icon is color-coded and contains a specific number of dots to indicate its severity level, as shown in the following table. Each icon has a corresponding number to indicate the number of alarms currently active

for that severity level. The UI banner shows the number of alarms per severity level for all assets in the model, whereas the Alarm Card displays the number of alarms per severity level for the selected context.


Icon	Description
	Alarm is critical.
	Alarm is high priority.
	Alarm is medium priority.
	Alarm is low priority.




A summary of alarms by each severity level icon for the selected context appears at the top of the Alarm Card. The summary reflects unfiltered alarm counts that cannot be modified by applying a filter. Below this summary data is a table showing details about each alarm associated with the selected asset, as shown in the following example:

0	0	0	1	Total Alarms: 1			
Ack.	Severity	Start Time	Source	Current Value	Asset	State	
		09/07/2017 9:55:02 AM	FIX:FWT_FWP_SVALVEC_STATUSFE...	RUNNING	SuctionValveC		<input type="button" value="CFN"/>



Note:

When Web HMI cannot connect to one or more alarm sources, the connection status icon appears orange on the Alarm Card. Hover over  to see which alarm sources are not connected. This icon becomes red when Web HMI cannot connect to ANY alarm sources, and these sources are not listed in the tooltip.

1. Select , the Asset Context Selector, to choose your context.
This displays the relevant data in context to each asset selected in the navigation scheme.
2. Select , the Alarm Card icon.
The Alarm Card displays the alarms for that asset and its descendants' assets.
3. **Optional:** To view data in a column in ascending or descending order, select the heading column name.
4. **Optional:** To define specific column criteria for viewing alarms in the table, such as displaying only critical alarms, select  and set the criteria accordingly.
Filters do not persist after you close your browser.
5. **Optional:** To acknowledge an alarm, do the following:

a. Select the check box next to it.

b. Select **Acknowledge**.

A check mark appears next to the alarm icon if the alarm was successfully acknowledged in the HMI/SCADA system.

View Mimic Cards


A Mimic Card provides a specific view of a process diagram associated with a selected asset, allowing you to monitor and control production equipment and processes.

When configured, you can click a target zone on a Mimic Card that navigates you to its asset or opens a Control View for modifying real-time HMI/SCADA values and viewing historical data. For more information on Control Views, see [Edit Values on Mimic Control Views \(on page 107\)](#).

When you hover over an asset on a Mimic Card and its background changes to blue, it is a target zone.

1. Select , the Asset Context Selector, to choose your context.

This displays the relevant data in context to each asset selected in the navigation scheme.

2. Select , the Mimic icon.

The Mimic Card displays the data using the mimic associated with the selected asset.

3. **Optional:** Select a target zone to navigate to its asset.

The asset defined for the target becomes the active asset, changing the mimic and content of any other cards that appear.

4. **Optional:** You can use the breadcrumb trail at the top left of the screen to navigate upwards through an asset's hierarchy.

Update Values on Mimic Cards

When configured, you can modify values in the HMI/SCADA data source directly on Mimic Cards.

You must have permissions in the HMI/SCADA data source to perform this task.

1. Hover over the value you want to update on the Mimic Card.

If the background of the value changes to blue, you can update the value.

2. Enter the new value in its entirety and press **Enter** or select the value from a drop-down list.

If you specify an invalid value in any entry box on the Mimic Card, the box becomes outlined in red.

3. **Optional:** For mobile devices:

- a. Select the entry field whose value you want to update. If its background changes to blue, you can edit this value, as shown below:



- b. Select the entry field again and specify the new value or select it from a drop-down list.
- c. **Optional:** Click outside the field if you do not want to update the current value.
- d. If an update confirmation window appears, answer accordingly.
4. If an update confirmation window appears, answer accordingly.
- An error can occur when you are not connected to the data source, you do not have permissions to write to your data source, or you entered a numeric value not within the acceptable minimum and maximum range for that value.

Edit Values on Mimic Control Views

When configured, a Mimic Card provides a Control View that lets you update the current data values and their attribute values in your HMI/SCADA system as well as view historical data.

You must have permissions in the HMI/SCADA system to modify real-time values.

1. To access the Control View on a Mimic Card, select .

A card appears with the variable names, targets, and values, as shown in this example.

	Target	Value	
CombinedFlow	5,089.952	5,089.952	
WaterTemp	0.999	0.999	
TankLevel	252.998 Gallons	252.998 Gallons	

An icon displays next to each value that represents the following:

	Real-time value that you can update. If defined, you can also edit the attribute values of this value, including the setpoint. If this gear does not appear next to a real-time value, you cannot change it.
	Last known current value returned from Historian that you cannot edit.

- For each real-time variable value you want to update, select .
- Edit the real-time values as needed.

Real-time values and their attribute values are limited to 15 digits of precision, such as 12345678901234500000. You can include underscores, hyphens, dashes, and at signs in the body of these values but not as the first character.

- Change the attribute values of the real-time values as needed.

If you specify an invalid value in any entry box on the Control View card, the box becomes outlined in red. Select **Confirm** to generate an error message at the top of this view.

- After making valid updates, select **Confirm**.
- Close the Control View.

View Trend Cards

Trend Cards provide a trend-line analysis view of selected data variables for an asset within a selected time period. Trend Card charts can display both real-time and historical data.


You can choose up to 20 data variables at a time per asset. These selections persist for the duration of the browser session. The selection persists for an asset even if you navigate to another asset and return.

**Note:**

Boolean and string tags from real-time data sources are not supported in the Trend Card.



1. Select , the Asset Context Selector, to choose your context.

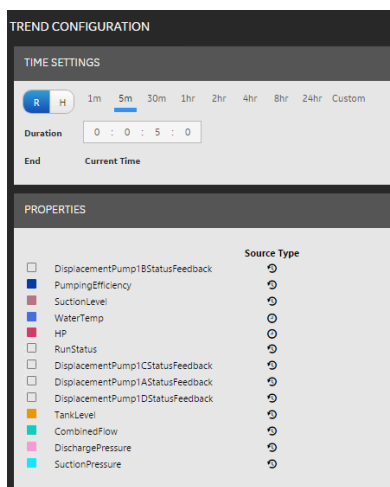
This displays the relevant data in context to each asset selected in the navigation scheme.

2. Select , the Trend icon.

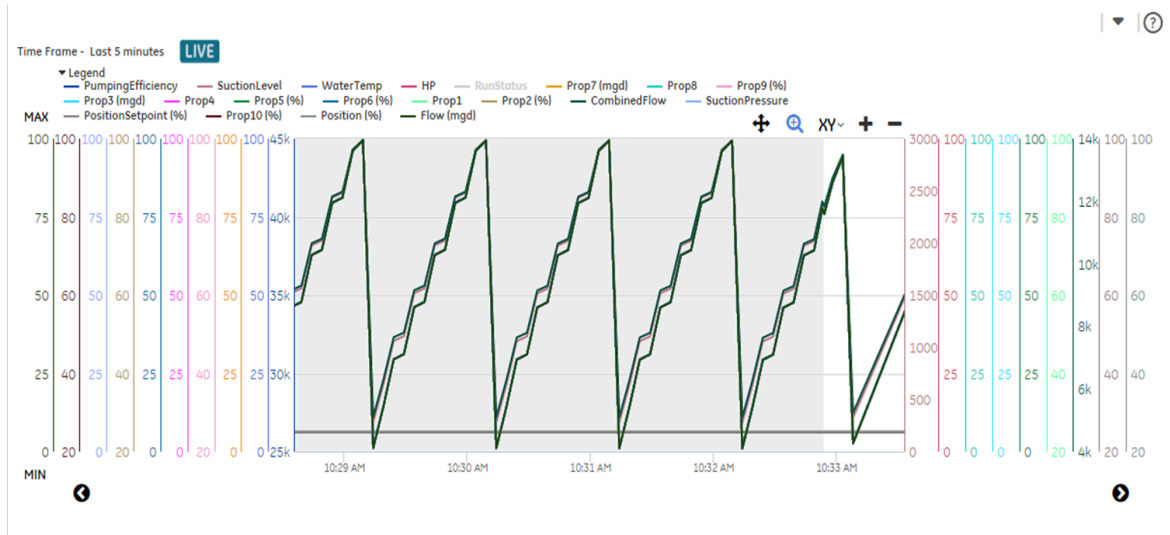
3. Select the down arrow at the top right of the Trend Card.

The **TREND CONFIGURATION** window appears showing the time settings as well as the asset's data variables with their associated data source type icons, as shown in the following example.

The  icon represents a historical data source and the  icon indicates a real-time data source.



4. Select **Real-time (R)** or **Historical (H)**. In the **Real-time (R)** view, you can see both real-time and historical data that is charted from the current time. The initial view shows a gray background, indicating the time period before opening the Trend Card. Only values coming from historical data sources will appear during this time frame. Subsequent real-time data appears with a white background, as shown in the following chart. In the **Historical (H)** view, you can see historical data charted on a start time and a duration.



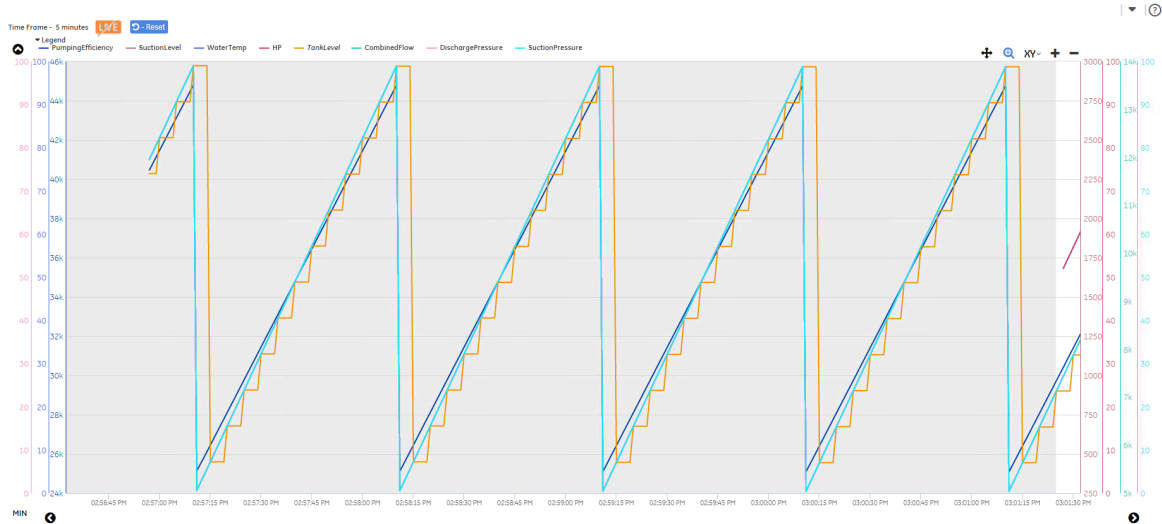
5. To view real-time trend data, do the following:
 - a. Select or deselect the asset's data variables.
A color is assigned to each selected data variable.
 - b. In **Duration**, select the time span to view past data activity from the current time. For example, to display the last hour of activity trends, select one hour.
 - c. In the field below the duration selector, you can specify a custom duration using the format of days:hours:minutes:seconds.

6. To view historical trend data, do the following:
 - a. Select or deselect the asset's data variables.
A color is assigned to each selected data variable.
 - b. Select the start time to begin viewing historical data trends.
 - c. In **Duration**, select the time span to view data activity beginning at the start time. For example, to display 12 hours of activity trends from the start time, select 12 hours.
 - d. In the field below the duration selector, you can specify a custom duration using the format of days:hours:minutes:seconds.

Manipulate Trend Charts

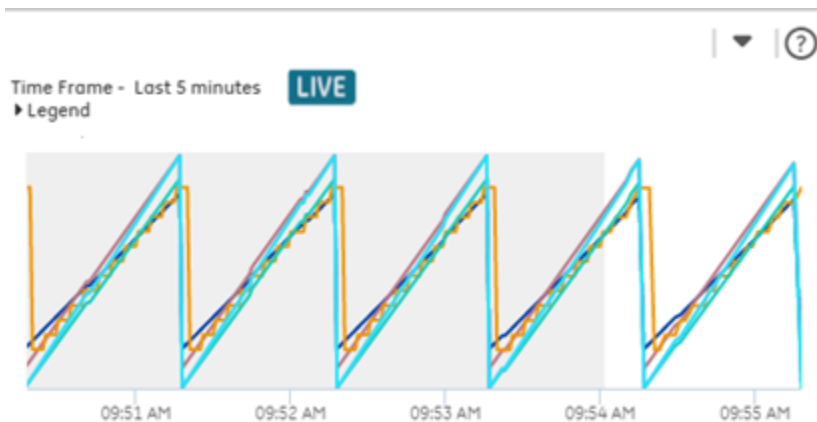
You can pause live data flow, display areas outside the area you are currently viewing, and use various zoom options to view and analyze trends on live and historical charts.

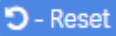
1. Click anywhere in a live chart to pause its data flow while it still collects data. The following shows a paused chart, indicated by a line through the **LIVE** icon.



2. Use the following zoom options to get a closer look at trend values:
 - a. To zoom in and out on the center of a chart (both XY axes), use **+** and **-** on the toolbar.
 - b. To view a specific area on the chart, hover over the chart with the **Q** cursor, and then click and drag to form a box over that area.
 - c. To isolate an axis for zooming, select **XY** on the toolbar, and then select **X** or **Y** from the drop-down list. When you zoom on the y-axis, the chart remains in live mode with data flowing.
3. Use the following pan options to adjust the chart axis for viewing:
 - a. Select **+** from the toolbar, and click and drag to view different values and time periods on the chart.
 - b. Use the pan arrows at the ends of each axis.
The up and down arrows are replaced with min and max if all data is within the value range.
4. **Optional:** Select the arrow next to **Legend** to show or hide the data variables of the selected asset. In the smaller view of the Trend chart, these variables are hidden by default.
5. **Optional:** To use the y-axis line toggle:
 - a. Select a variable name in the legend and its name becomes italicized and its y-axis line disappears.
 - b. Select the italicized variable name and its name becomes grayed out and its trend line disappears.
 - c. Select the grayed-out variable name and its y-axis line and trend line reappear.

In the smaller Trend chart view, the y-axis does not appear by default, as shown in the following example. To show the y-axis, select the arrow next to **Legend**, and then select the data variable to display.




6. After making changes to a chart, select  - Reset to revert the chart to its original duration and axis preferences.


This is the best way to return to live mode after manipulating the chart. You can also return to live mode by using the right pan arrow to shift to the current time.




View Task List Cards

Use a Task List Card to monitor and act on the steps in a running workflow that is assigned to you.

If Workflow is not integrated with Web HMI, information about Workflow appears in this card.

When connected with the Workflow server, the task list icon at the top of the card shows you the number of tasks assigned to you. For example,  indicates you have two tasks.

- Access the Task List documentation from the Workflow server, which you can find in C:\Program Files (x86)\Proficy\Proficy Workflow\Help\TaskListWebHMI.pdf.
- Verify Web HMI is connected to the Workflow server. If not connected,  appears in the main navigation bar.

1. Select , the Asset Context Selector, to choose your equipment or process context.
2. Select , the Task List Card icon.
3. **Optional:** You can also display a task list with its alarm view and mimic view by selecting .
4. Interact with the task list.

Log out of Web HMI

When you are done with working in Web HMI, you can log out.

1. Select the user icon.
2. Select **Logout**.

Chapter 15. Troubleshoot

OPC UA Write Errors

The following explains errors that can occur when Web HMI performs data writes to data sources.

Error	Description
BadCommunicationError Opc-Ua_BadServerNotConnected	There is a problem with the connection to the HMI/SCADA system.
BadOutOfService	The tag or point is not currently enabled or available.
BadNotWritable	The tag or point does not allow writes.
BadOutOfRange	The value being written exceeds the range of the tag or point. In the case of text data, the text exceeds the maximum length.
BadIdentityTokenInvalid	There was a problem with the security token used to authenticate the Web HMI user with the HMI/SCADA system.
BadIdentityTokenRejected	The user is not authorized to connect to the HMI/SCADA system. Verify there is an account for that user on the HMI/SCADA system.
BadResourceUnavailable	A required resource is not available. For iFIX, this specifically means that iFIX cannot connect to the Web HMI authentication service to validate the user. In some cases, this can happen if the <code>secmgr.cclr.dll.config</code> file in the iFIX install folder on the SCADA node contains an incorrect host or port for the Web HMI server.
BadNodeIdInvalid	The data source name that was specified as the source for the asset's property is incorrect. This pertains to CIMPLICITY OPC UA data sources.
BadTypeMismatch	The value being written does not match the data type of the tag or point.
BadUserAccessDenied	The user name does not have permissions to write to the point in the CIMPLICITY project.

Error Symbols

The following explains the error symbols that may appear in Web HMI.

Error Symbol	Type	Description
****.**	Configuration	Mimic fails to receive data because its data source cannot be found.
####	Configuration/Communication	Mimic fails to subscribe to data from this data source. If all data in the mimic shows this symbol, then the connection to the data server probably failed. If only some data items show this, then those data items may have incorrect syntax.
&&&&.&&	Unknown	Mimic receives an undefined error.
@@@@@.@@	Communication	Mimic receives a network error.
?????.??	Out of Service	Mimic cannot receive data because the specified I/O point is off scan.
%%%%.%%	Uncertain	Mimic receives questionable data, such as out-of-range data.
xxxxx.xx	Device	Mimic cannot receive data because an OPC device is unresponsive.

iFIX Issues

DE42170: iFIX unable to write data or acknowledge alarms due to non-default Tomcat port

The secmgr.cclr.dll.config file contains an incorrect host or port.

Do the following to resolve this issue:

1. In the Registry, find the Tomcat port in use by opening the 'Environment' value and looking for the TOMCAT_LOCATION line. The following shows that **8444** is the Tomcat port in use:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\
GETomcat8\Parameters 'Environment' value,
TOMCAT_LOCATION contains the port at the end (TOMCAT_LOCATION=https://127.0.0.1:8444)
```

2. Record this port number. For this example, the Tomcat port is 8444.
3. Open the secmgr.cclr.dll.config file in the C:\Program Files (x86)\GE\iFIX folder.
4. Type the Tomcat port in the "oauthPort" value setting, as shown below:

```

?xml version="1.0" encoding="utf-8" ?>

<configuration>

  <appSettings>

    <add key="oauthHost" value="127.0.0.1"/>

    <add key="oauthPort" value="8444"/>

    <add key="oauthEndPoint" value="oauth"/>

    <add key="strictCertificatePolicy" value="false"/>

  </appSettings>

</configuration>

```

5. Restart iFIX for this change to take effect.

DE47858: Alarm Card shows partial connection () to an iFIX alarm source that is no longer installed on the Web HMI server

On systems where iFIX was uninstalled or where iFIX is installed but it is not being used as the alarm source for Web HMI, perform these steps to prevent the Alarm Gateway from trying to connect to iFIX and report a connection failure:

1. Navigate to C:\ProgramData\Proficy\WebHMI\DataServices.



Note:

The ProgramData folder is hidden by default in Windows. You may need to change the Windows Folder Options, or type this folder directly in to the address bar of the File Explorer to navigate to it.

2. Open the data-services-config.json configuration file in a text editor.
3. Find the following section in this file and delete the text in bold.



Note:

Be sure to delete the comma preceding "comServers" or Web HMI cannot read the data-services-config.json file, and data and alarms will not flow in Web HMI.

```

"alarmGateway": {
  "logFilePath": "%ProgramData%\Proficy\Logs\",
  "traceLevel": 3,
  "stackTraceLevel": 1,
  "maxLogFileEntries": 100000,

```

```

    "maxLogFileBackups": 5,
    "logicalName": "alarms",
    "brokerHost": "localhost",
    "brokerExchange": "alarms",
    "brokerRequiresSsl": true,
    "brokerCertificate": "C:\\Program Files\\Proficy\\AlarmGateway\\ssl\\alarmGateway.p12",
    "brokerPassword": "K9Umpz3btpQlB9n6AsUOm7qvKSoE2nwpdGjQ3m4G4HIbwKkca+JiQ/m05B3kELAE",
    "maxAlarmsPerMessage": 1000,
    "loggingFlagsForCom": 0,
    "comServers": [
      {
        "logicalName": "alarms",
        "hostName": "localhost",
        "progId": "Proficy.OPCiFIXAE.1"
      }
    ]
  }
}

```

4. Verify the section looks like this:

```

"alarmGateway": {
  "logFilePath": "%ProgramData%\Proficy\\Logs\\",
  "traceLevel": 3,
  "stackTraceLevel": 1,
  "maxLogFileEntries": 100000,
  "maxLogFileBackups": 5,
  "logicalName": "alarms",
  "brokerHost": "localhost",
  "brokerExchange": "alarms",
  "brokerRequiresSsl": true,
  "brokerCertificate": "C:\\Program Files\\Proficy\\AlarmGateway\\ssl\\alarmGateway.p12",
  "brokerPassword": "K9Umpz3btpQlB9n6AsUOm7qvKSoE2nwpdGjQ3m4G4HIbwKkca+JiQ/m05B3kELAE",
  "maxAlarmsPerMessage": 1000,
  "loggingFlagsForCom": 0
}

```

5. Save the file. If using Notepad, ensure data-services-config.json is not saved with a .txt extension.
6. Restart the Alarm Gateway and GE Tomcat Server Windows services for this change to take effect.

Workflow Task Lists Not Appearing in iPads

iPad Cannot Resolve the Workflow Host Name

Use the Workflow IP address instead of the host name by following these steps:

1. In the Administration environment of Web HMI, navigate to **Set Up > Server**.
2. In the **Server Details Management** screen, change the Workflow server name to its IP address. For example, change MyWorkflowServer:8447 to 3.87.64.57:8447.
3. Refresh the Web HMI browser to see the Workflow task count and tasks.

Workflow Server is Untrusted

Because the Workflow ProficySelfSignedCA certificate is a self-signed certificate, the Workflow server displays as an untrusted site. As a result, you must follow these steps:

1. Navigate to https://<workflowserverip>:<workflowport>. When you arrive at this URL, your browser may warn you that the source is untrusted.
2. Continue to proceed to this URL, which enables your browser to trust the Workflow domain.
3. Refresh the Web HMI browser to see the Workflow task count and tasks.

LDAP Settings for AD Authentication

Use this troubleshooting topic to help you retrieve required information from the Windows Active Directory to use when setting up the LDAP settings for AD authentication.

Retrieving Distinguished Names from the Windows Active Directory

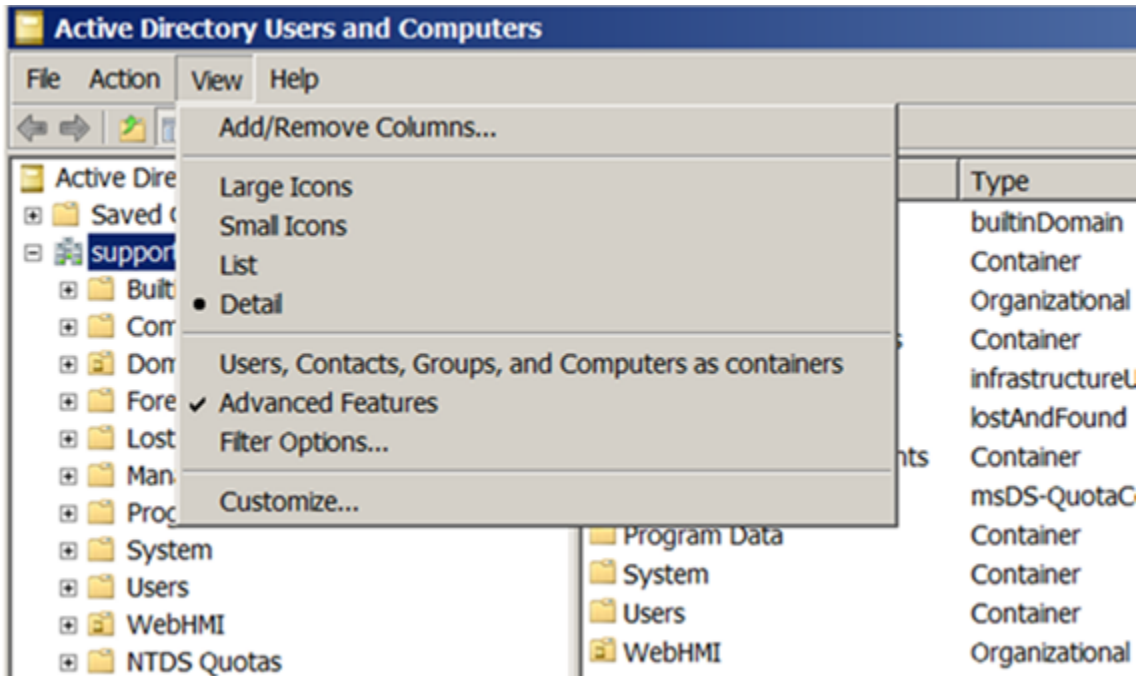
The Web HMI Application Assembler provides a template for defining the LDAP settings for DirectoryServices. This template uses a nonstandard organizational unit (OU) named WebHMI in the Windows Active Directory instead of the default Users OU.

Before you can fill out this template, you must first search for certain values in the Active Directory and then record them. This template requires these values from the Active Directory:

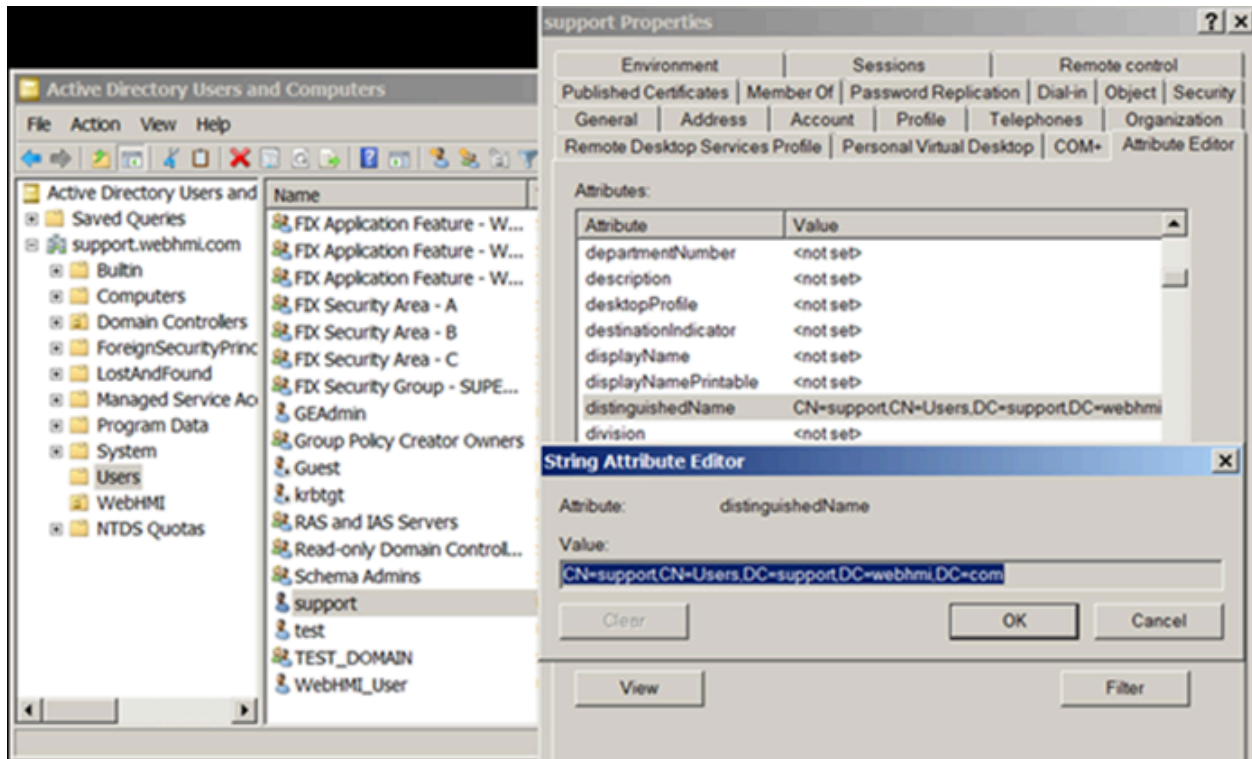
Active Directory Value	Description
server	The name of the computer where the Active Directory resides.
adminBindDN	The login of the administrative user with permission to run the Active Directory lookup. This is the distinguished name (DN). For example, for the Support administrative account residing in the default Users organizational unit, the DN is:

Active Directory Value	Description
	CN=Support,CN=Users,DC=Support,DC=webhmi,DC=com
userBaseDN	The Active Directory lookup for the user group or base organizational unit. This is the distinguished name. For example, for all users residing in the WebHMI OU, the DN is: OU=WebHMI,DC=support,DC=webhmi,DC=com
adminPassword	Password for the above adminBindDN user.

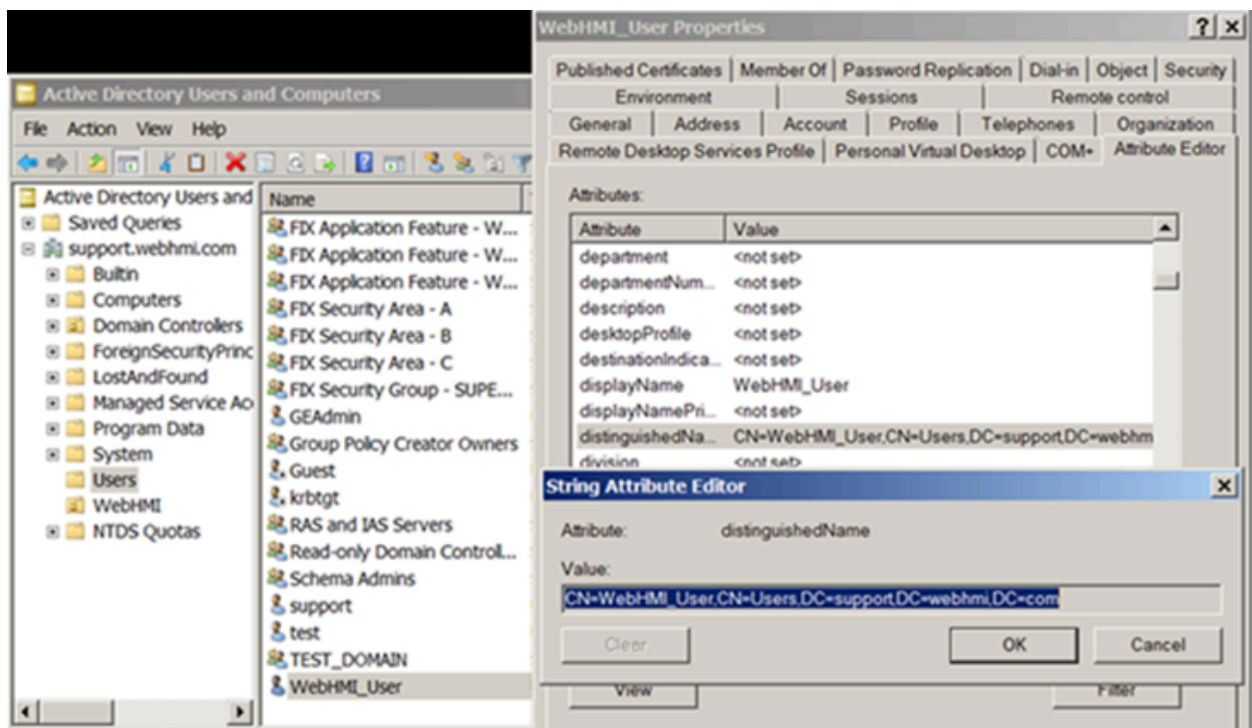
First enable **Advanced Features** under **Active Directory Users and Computers > View**. This displays the **Attribute Editor** where you can find the required distinguished names.



The following sample screens show how to retrieve the distinguished name for an adminBindDN setting. In this example, the Support administrative account resides in the default Users organizational unit.



The following sample screens show how to retrieve a distinguished name for the userBaseDN setting. In this example, the distinguished name uses the WebHMI organizational unit.



Finding the name and IP address of the AD domain controller

Use nslookup, a network administration command-line tool, to retrieve the name and IP address of the AD domain controller on your network, and other information for diagnosing the Domain Name System (DNS) infrastructure.

1. In nslookup, select **Start** and then **Run**.
2. In the Open box, enter `cmd`.
3. Enter `nslookup`, and press **Enter**.
4. Enter `set type=all`, and press **Enter**.
5. Enter `_ldap._tcp.dc._msdcs.Domain_Name`, where `Domain_Name` is the name of your domain, and then press **Enter**.

Retrieving data about AD Users

To generate information about a specific AD user, use the Windows Get-ADUser cmdlet, as shown in this example.

```
C:\Users\Administrator.ANIMAL> get-aduser "-svc-TEST"

DistinguishedName : CN=Test User,OU=Test,OU=Groups,DC=Animal,DC=farm
Enabled           : True
GivenName        : Test
Name             : Test User
ObjectClass      : user
ObjectGUID       : 7b5bc454-5b2a-4317-8df0-bbdee05b5435
SamAccountName   : -svc-TEST
SID              : S-1-5-21-2742514831-3001338947-4026583061-1618
Surname         : User
UserPrincipalName : -svc-TEST@Animal.farm
```

How Does Historian Data Appear in the Model

Review the following to understand how the Historian data source names display in the Web HMI model for CIMPLICITY and iFIX.

CIMPLICITY Example

In CIMPLICITY, the `BLUE.ANIDPYVAL_DATATYPES_UFT_CL_INSTANCE00.dt_INT` data source tag name represents the following:

- BLUE = Project Name
- ANIDPYVAL_DATATYPES_UFT_CL_INSTANCE00 = Class ID
- dt_INT = Point

In the Historian **Source Address** field, this tag appears as:

```
\\BLUE\ANIDPYVAL_DATATYPES_UFT_CL_INSTANCE00.dt_INT
```

In the Web HMI model, this tag appears as:

```
BLUE_ANIDPYVAL_DATATYPES_UFT_CL_INSTANCE00.dt_INT
```

iFIX Example

In iFIX, the IFIX58S1.HWT_FWP_DPUMP_1A_FLOW.F_CV data source tag name represents the following:

- IFIX58S1 = Node
- HWT_FWP_DPUMP_1A_FLOW = Tag
- F_CV = Field

In the Historian **Source Address** field, this tag appears as:

```
IFIX58S1.HWT_FWP_DPUMP_1A_FLOW.F_CV
```

In the Web HMI model, this tag appears as:

```
IFIX58S1.HWT_FWP_DPUMP_1A_FLOW.F_CV
```