



GE VERNOVA

DIGITAL

PROFICY CONFIGURATION HUB 2023

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.

© 2023, 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

Configuration Hub Documentation

Contents

- Chapter 1. Getting Started..... 15**
 - Introduction to the Configuration Hub Framework..... 15
 - Sample Deployment Architectures..... 16
 - Install and Uninstall Options..... 20
 - Available Product Plugins..... 27
 - Common Panels..... 28
 - Common Panels..... 28
 - Application Bar 29
 - Navigation Panel..... 30
 - Details Panel..... 32
 - Concurrency Management..... 35
 - Server Certificates for Configuration Hub 36
 - Client Certificates for Configuration Hub..... 39
 - Proficy Authentication Certificate..... 48
 - Known Issues and Limitations 48
 - High Availability for Configuration Hub..... 50
 - Overview..... 50
 - Configure High Availability for Configuration Hub..... 51
 - Install Failover Clustering Feature..... 54
 - Create Failover Cluster..... 55
 - Create Role..... 58
 - Create Client Access Point (Virtual IP)..... 60
 - Add Dependencies to Role..... 62
 - Create Network Attached Storage..... 63
 - Install Configuration Hub on Cluster Nodes..... 65
 - Handling Silent Installation..... 67
- Chapter 2. Proficy Authentication 70**

About Proficy Authentication.....	70
Set up Proficy Authentication.....	70
Navigation in Proficy Authentication.....	75
Manage Identity Providers.....	76
Add LDAP Identity Provider.....	76
Enable SAML.....	79
Add SAML Identity Provider.....	88
Enable Multi-Factor Authentication.....	90
Modify LDAP Identity Provider.....	92
Modify SAML Identity Provider.....	94
Delete Identity Provider.....	95
Manage Groups.....	96
Overview of iFIX Groups in Proficy Authentication.....	96
Overview of Historian Groups in Proficy Authentication.....	97
Create Groups.....	97
Modify Groups.....	98
Map Groups.....	99
Add/Remove Users in a Group.....	102
Add/Remove Sub-Groups in a Group.....	103
Delete Group.....	104
Manage Users.....	105
Create Users.....	105
Add/Remove Groups for a User.....	107
Reset User Password.....	109
Delete User.....	110
Windows Integrated Authentication / Auto-login.....	110
Configure Security Policy.....	113
Create Service Principal Name.....	115
Generate Keytab File.....	118

Proficy Authentication Service Configuration.....	121
Configure Browser.....	122
Troubleshooting Error Logs.....	123
High Availability.....	128
Configure High Availability for Proficy Authentication.....	128
Configure iSCSI Target.....	129
Configure iSCSI Initiator.....	130
Create a Virtual Disk.....	131
Initialize a Virtual Disk.....	133
Create a Cluster.....	135
Configure Role.....	138
Configure Proficy Authentication Installation.....	142
Prerequisites for Installing Operations Hub with External Proficy Authentication.....	146
Customize Login Screen.....	150
Chapter 3. iFIX.....	152
Overview	152
Introduction to iFIX Web Configuration.....	152
Integrated Development Environment.....	154
Prerequisites to Use Configuration Hub with iFIX.....	154
Configuration Information.....	155
Access iFIX Web Configuration.....	169
Connections	171
Connections Overview.....	171
OPC UA Connections	171
IGS Connections.....	183
Drivers.....	191
Network Connections.....	193
Special Considerations for SCADA Enhanced Failover.....	198
SQL Connections.....	200

Model	203
Model Overview.....	203
Model Panel.....	204
Type Creation.....	206
Type Variables	208
Template Overview.....	211
Template Management.....	211
Substitutions.....	214
Expression Builder.....	216
Object Creation.....	216
Model Import and Export.....	217
Model Tags in iFIX.....	218
Database.....	221
Database Overview.....	221
Database Management.....	227
Tag Management.....	279
Validations.....	281
Custom Editors.....	282
Tag Properties.....	283
Project Security	823
Overview of Project Security.....	823
Add or Modify Users.....	824
Add or Modify Groups for Proficy Authentication.....	827
Add or Modify Security Areas.....	828
Auto Login Configuration.....	830
Alarms	832
Defining Alarm Areas.....	832
Alarm Services.....	834
Alarm Printers.....	839

Alarm Events.....	841
Alarm Queue Configuration.....	843
Common Message Format Configuration.....	845
Common Alarm Areas Configuration.....	846
Alarm Clients.....	847
Project Settings	848
Overview of Project Settings.....	848
Starting and Stopping iFIX Projects.....	851
Add a New Project.....	853
Add an Existing Project.....	855
General Settings.....	856
Startup Options.....	858
Startup Schedules.....	861
Startup Pictures.....	862
Historian.....	863
SCADA Failover.....	864
Task Configuration.....	868
Deployment.....	872
Project Deployment.....	872
Save and Publish.....	874
Chapter 4. Historian.....	877
Overview of Historian with Configuration Hub.....	877
About Historian in Configuration Hub.....	877
Configuration Hub Workflow for Historian.....	878
Setting up Configuration Hub for Historian.....	879
About Setting up Configuration Hub with Historian.....	879
Install the Historian Server.....	880
Install Web-based Clients.....	885
Install Collectors.....	898

Perform Post-Installation Tasks.....	901
Upgrade.....	902
Access Configuration Hub.....	902
Common Tasks.....	906
Setting up a Stand-Alone System.....	907
About Setting up a Stand-Alone Historian System.....	907
Add a Collector.....	909
Add Tags for the Data Store Using Configuration Hub.....	909
Setting up a Horizontally Scalable System.....	911
About Setting up a Horizontally Scalable System.....	911
Add a Server.....	913
Add a Collector.....	914
Add Tags.....	915
Setting up High Availability.....	917
About Data Mirroring	917
Create.....	918
Create a Data Store.....	920
Creating a Model.....	921
About a Historian Model.....	921
About Object Templates.....	927
Workflow for Creating a Historian Model.....	930
Create an Object Type.....	931
Include a Contained Type.....	936
Create an Object Instance.....	939
Provide Data for a Static Variable.....	941
Collect Data for a Direct Variable.....	944
Collect Data for an Indirect Variable.....	947
Export an Object Type/Instance.....	951
Import an Object Type/Instance.....	953

Copy an Object Type.....	954
Delete a Template.....	959
Delete an Object Instance.....	961
Delete an Object Type.....	962
Managing Historian Systems.....	963
Access a System.....	963
Access the Collectors in a System.....	971
Access Offline Configuration Collectors.....	973
Access the Tags in a System.....	976
Add a System.....	978
Add a Server.....	979
Set Up a Mirror of Mirror.....	980
Remove a Server.....	990
Set a Default Location.....	990
Modify a System.....	991
Configure Advanced Settings.....	992
Configure Labels of Spare Fields.....	995
Set a Default System.....	996
Delete a System.....	996
Managing Mirror Locations.....	997
Create.....	997
Rename.....	998
Add a Machine.....	1000
Remove a Machine.....	1001
Delete.....	1002
Managing Data Stores.....	1003
About Data Stores	1003
Create a Data Store.....	1004
Access a Data Store.....	1005

Rename a Data Store.....	1009
Set as Default.....	1013
Access Archives.....	1014
Access Activity Logs.....	1015
Access Tags.....	1015
Specify Tags for Data Collection.....	1016
Add a Tag Manually.....	1018
View Performance.....	1021
Delete.....	1023
Adding a Collector Instance.....	1024
The Calculation Collector.....	1024
CygNet Collector.....	1027
The File Collector.....	1031
The HAB Collector.....	1035
Collection Definitions of a HAB Collector.....	1041
About Adding an iFIX Collector Instance.....	1047
The iFIX Collector.....	1051
The MQTT Collector.....	1056
The ODBC Collector.....	1062
The OPC Classic Alarms and Events Collector.....	1067
The OPC Classic DA Collector.....	1070
The OPC Classic HDA Collector.....	1076
The OPC UA DA Collector.....	1080
The OSI PI Collector.....	1084
The OSI PI Distributor.....	1088
The Server-to-Server Collector.....	1093
The Server-to-Server Distributor.....	1098
The Simulation Collector.....	1102
The Windows Performance Collector.....	1106

The Wonderware Collector.....	1110
Collector Configuration - Common Fields.....	1114
Sending Data to Cloud.....	1122
Alibaba Cloud.....	1122
AWS Cloud.....	1127
Azure Cloud (Key-Value Format).....	1134
Azure Cloud (KairosDB Format).....	1142
Google Cloud.....	1148
Predix Cloud.....	1154
Protocols and Port Numbers.....	1159
Managing Collector Instances.....	1160
Managing Collectors Using Configuration Hub.....	1160
Access a Collector.....	1161
Access Tags.....	1164
Add a Collector.....	1165
Modify a Collector.....	1166
Add a Comment.....	1168
Access Comments.....	1169
Start a Collector.....	1170
Stop a Collector.....	1172
Restart a Collector.....	1173
Pause Data Collection.....	1175
Resume Data Collection.....	1176
Clear Buffer.....	1177
Move Buffer.....	1179
Change Destination.....	1180
Configure Collector Redundancy.....	1182
Delete a Collector.....	1184
Managing Offline Configuration Collector Instances.....	1186

Access Offline Configuration Collectors.....	1186
Manage Offline Configuration Collectors.....	1188
Access Tags.....	1189
Managing Tags.....	1189
About Tags.....	1189
About Array Tags.....	1190
About Collector and Archive Compression.....	1190
About Scaling.....	1197
About Condition-Based Collection.....	1197
Specify Tags for Data Collection.....	1198
Add a Tag Manually.....	1200
Access a Tag.....	1204
Access Trend Chart.....	1218
Access Last 10 Values.....	1219
Access a Tag Alias.....	1222
Rename a Tag.....	1224
Copy a Tag.....	1226
Stop Data Collection.....	1228
Resume Data Collection.....	1230
Remove a Tag.....	1230
Delete a Tag.....	1232
Managing Enumerated Sets.....	1234
About Enumerated Sets.....	1234
Create an Enum Set.....	1235
Assign to Tag.....	1236
Delete an Enum Set.....	1237
Managing User-Defined Data Types.....	1238
About UDTs.....	1238
Create UDT.....	1238

Assign to Tag.....	1239
Delete UDT.....	1240
Managing Archives.....	1241
About Archives.....	1241
Guidelines for Archive Sizing.....	1242
Access an Archive.....	1243
Create Archives Automatically.....	1245
Create Archives Manually.....	1247
Back up an Archive.....	1249
Back up Archives with Volume Shadow Copy Service.....	1250
Restore an Archive.....	1252
Close an Archive.....	1253
Remove an Archive.....	1253
Reading/Writing Data.....	1253
Query Data.....	1253
Write Data.....	1257
Managing Alarms and Events.....	1259
About Alarms and Events.....	1259
Requirements.....	1260
Create an Alarm.....	1260
Access/Filter Alarms.....	1261
Back up Alarms.....	1262
Restore Alarms.....	1263
About Purging Alarms.....	1264
Accessing Activity Logs.....	1266
Troubleshooting Historian and Configuration Hub	1268
Chapter 5. Operations Hub.....	1272
Operations Hub and the Integrated Installer.....	1272
Install Common Components.....	1273

Install Operations Hub for SCADA.....	1277
Install Operations Hub from a Dedicated Installer.....	1282
Register Operations Hub with Configuration Hub.....	1289
Getting Started with Operations Hub.....	1290
Operations Hub (New Layout).....	1291
Panels Layout.....	1291
Navigation Panel.....	1292
Components Panel.....	1294
Display Panel.....	1305
Details Panel.....	1310
HMI Graphics.....	1325
Chapter 6. WebSpace	1348
Overview of WebSpace with Configuration Hub.....	1348
Sample WebSpace Deployment Architecture.....	1349
How to Install a WebSpace Server.....	1350
Exporting the Root Certificate for WebSpace Setup.....	1351
Importing the Certificate for WebSpace Setup.....	1353
Registration with Configuration Hub for WebSpace.....	1355
WebSpace Settings in Configuration Hub.....	1358
iFIX WebSpace Plugin in Operations Hub.....	1359
Troubleshooting WebSpace with Configuration Hub.....	1363
Chapter 8. MQTT Client.....	1378
Getting Started.....	1378
Introduction.....	1378
Prerequisites and Hardware Requirements.....	1379
Sample Deployment Architectures.....	1380
Installation.....	1384
Registration and Proficy Authentication.....	1390
Utilities.....	1397

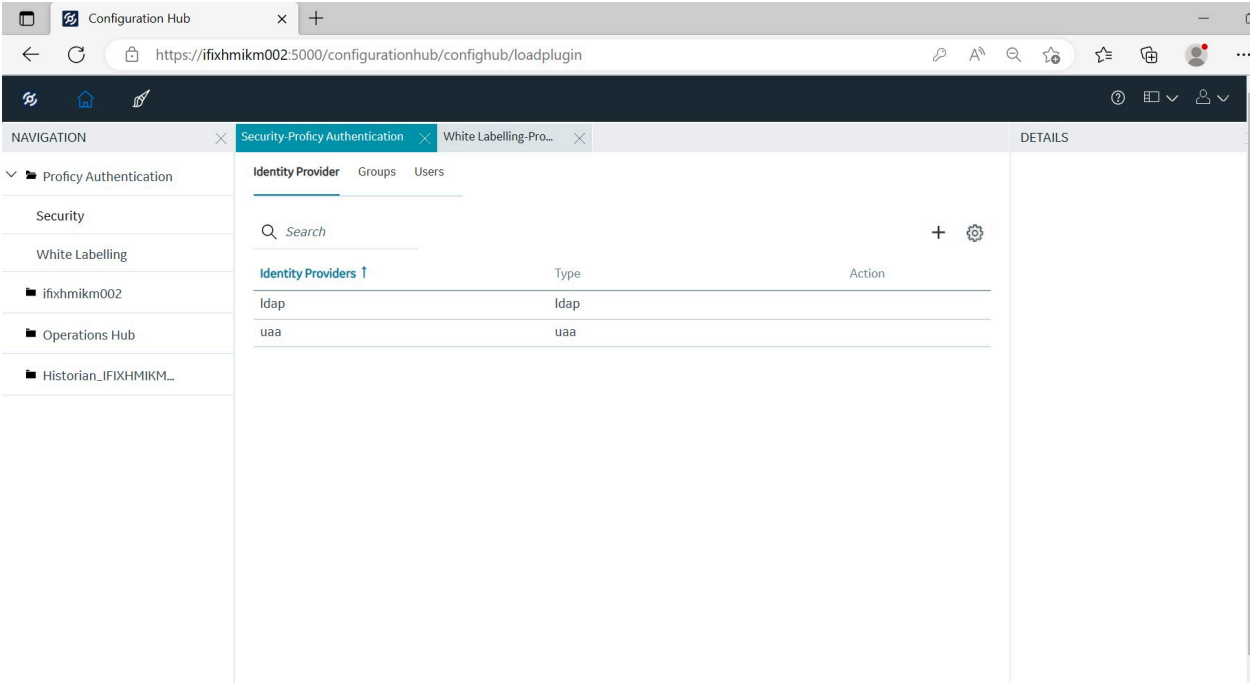
Changing Admin Credentials.....	1397
Port Changes.....	1398
Configuration.....	1399
MQTT Client in Configuration Hub.....	1399
Chapter 9. Settings.....	1442
Switch Users.....	1442
Modify Layout.....	1442
Host Name Changes.....	1442
Port Changes for Configuration Hub.....	1445
Chapter 10. Troubleshooting.....	1447
Log Files.....	1447
Frequently Asked Questions.....	1450

Chapter 1. Getting Started

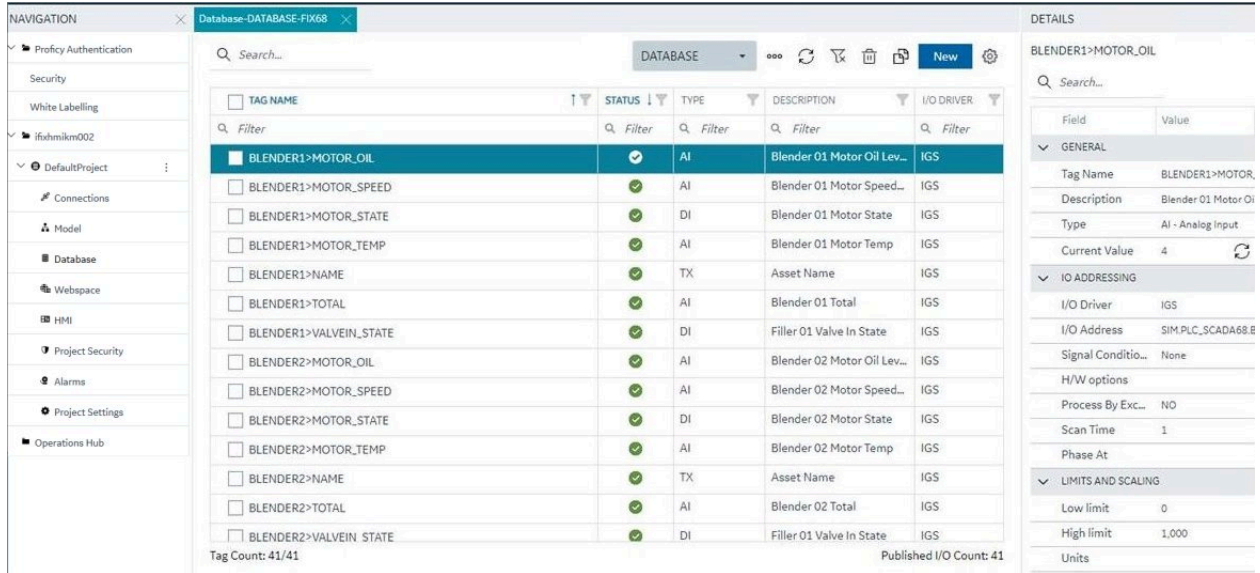
Introduction to the Configuration Hub Framework

Configuration Hub allows you to configure your Proficy products all together in one place, and access and configure them from anywhere. You can view multiple Proficy applications from within Configuration Hub. For example: Proficy Authentication, iFIX, Historian, and Operations Hub.

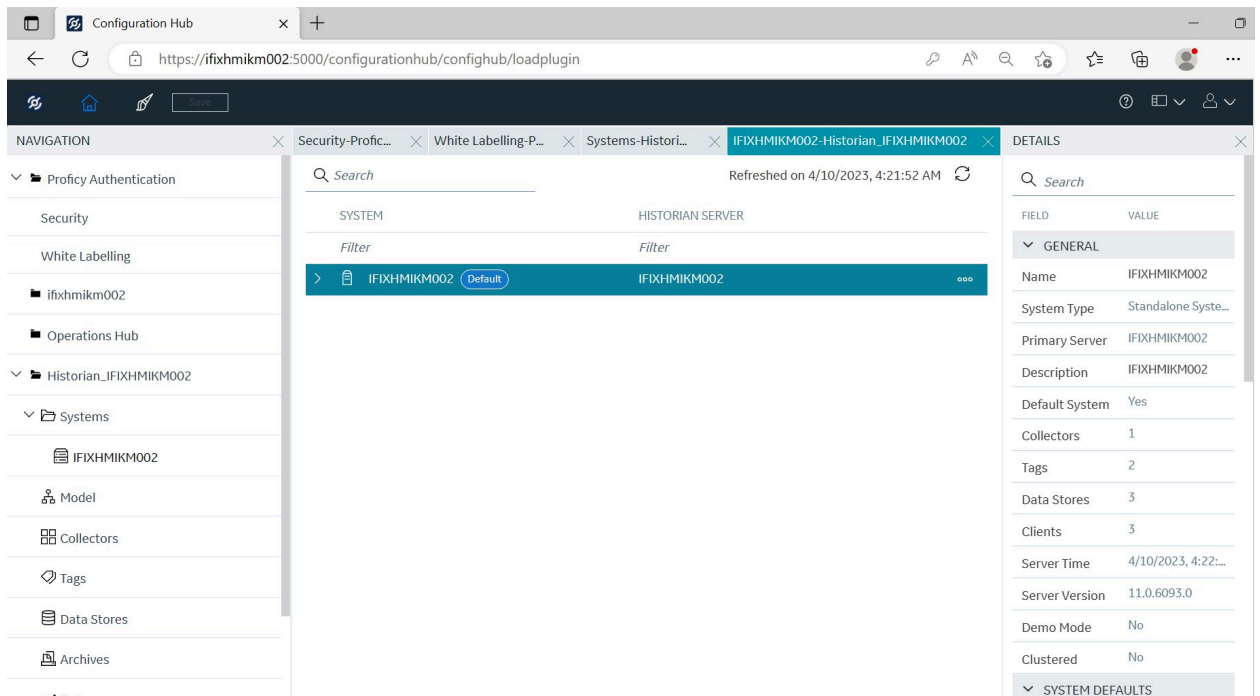
The following graphic shows an example of Configuration Hub with Proficy Authentication selected:



The following graphic shows an example of Configuration Hub with the iFIX Database panel selected:



The following graphic shows an example of Configuration Hub with Historian and a Server selected from the Historian Systems panel:

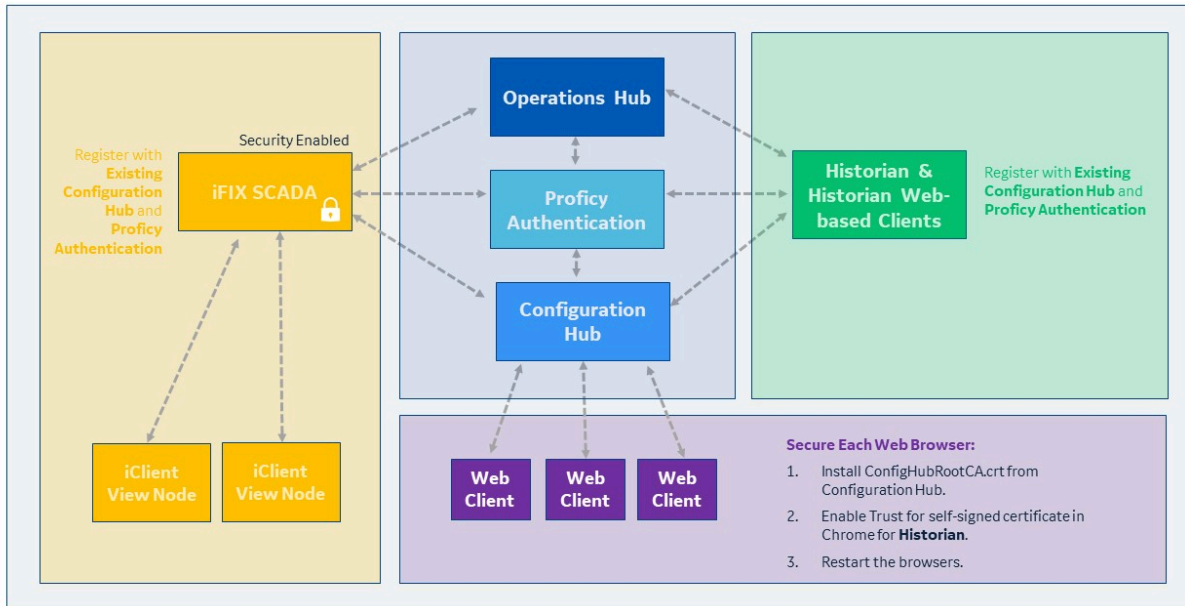


Sample Deployment Architectures

The following examples show different types of deployment architectures you may choose to use with Configuration Hub.

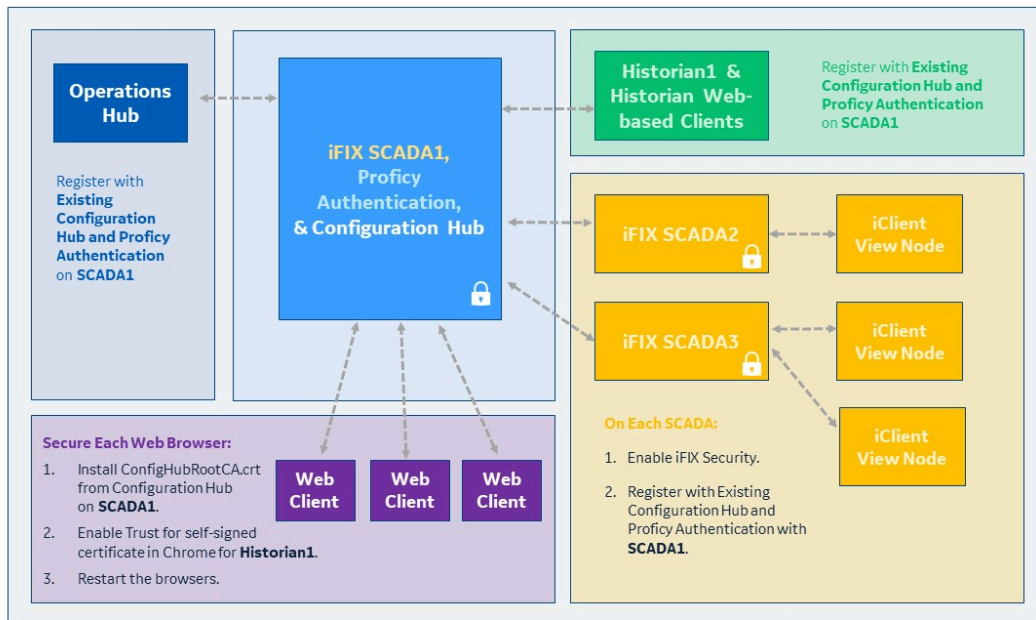
Example 1

The following example shows Configuration Hub, Proficy Authentication, and Operations Hub installed on one central computer, with iFIX (SCADA), View nodes, and Historian all on different computers. This diagram represents a highly recommended deployment architecture.



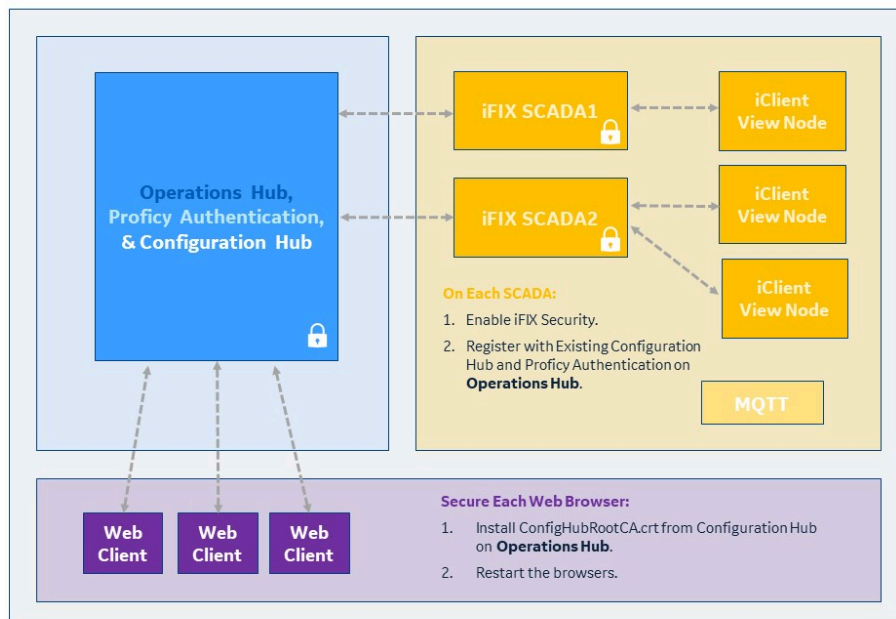
Example 2:

The following example shows an iFIX SCADA (SCADA1) with Configuration Hub and Proficy Authentication installed. Operations Hub, the Historian Server (Historian1), and additional SCADAs (SCADA1 and SCADA2) are on different computers connecting to that existing SCADA1 node.



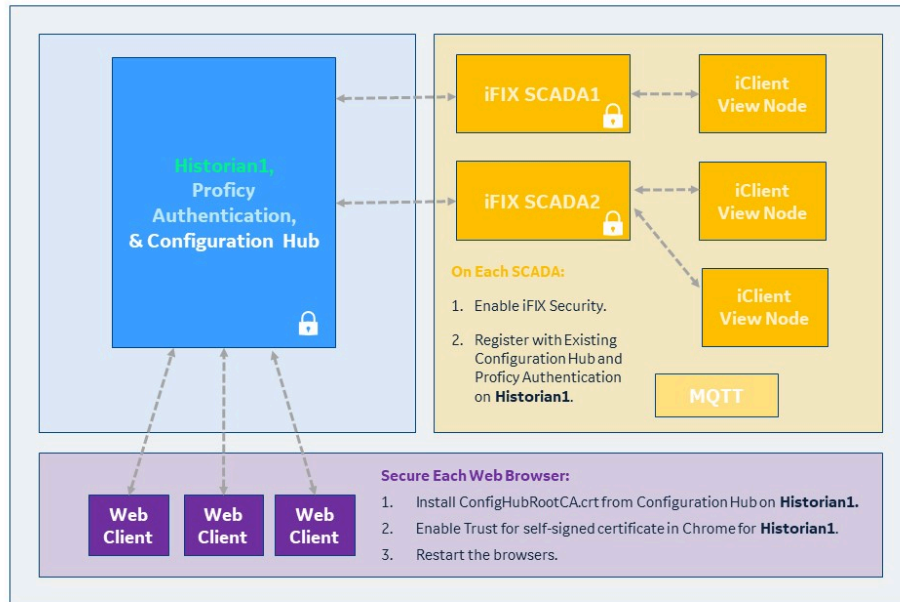
Example 3

The following example shows a computer with Operations Hub, Proficy Authentication, and Configuration Hub all on the same box, with other computers with iFIX (SCADA1 and SCADA2) connecting to that existing node, along with web-based clients.



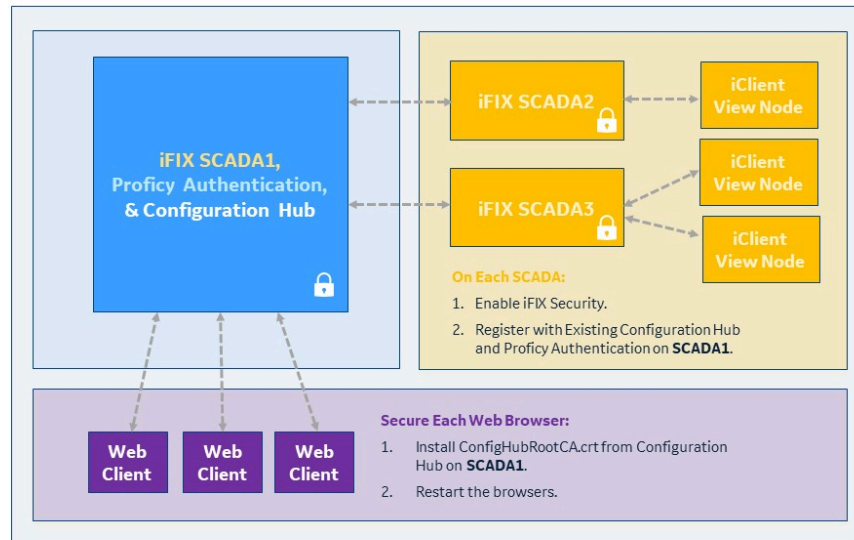
Example 4

The following deployment architecture illustrates Historian (Historian1), Proficy Authentication, and Configuration Hub all on the same box, with the iFIX SCADAs (SCADA1 and SCADA2) connecting to the existing Historian1 server, along with web-based clients.



Example 5

The following example shows iFIX SCADA (SCADA1) with Proficy Authentication and Configuration Hub installed with other SCADAs (SCADA2 and SCADA3) on different computers connecting to the existing node with SCADA1, along with web-based clients.



Install and Uninstall Options

Configuration Hub, along with the iFIX SCADA, Historian, and Operations Hub products are all installed using Integrated Installer experience.

Integrated Installer

To install Configuration Hub, use the Integrated Installer Common Components option, as shown in the following figure. This figure shows the SCADA version of the Integrated Installer. Configuration Hub only needs to be installed once. It should not be installed on a computer with the Webspace Server or a Enhanced Failover pair.



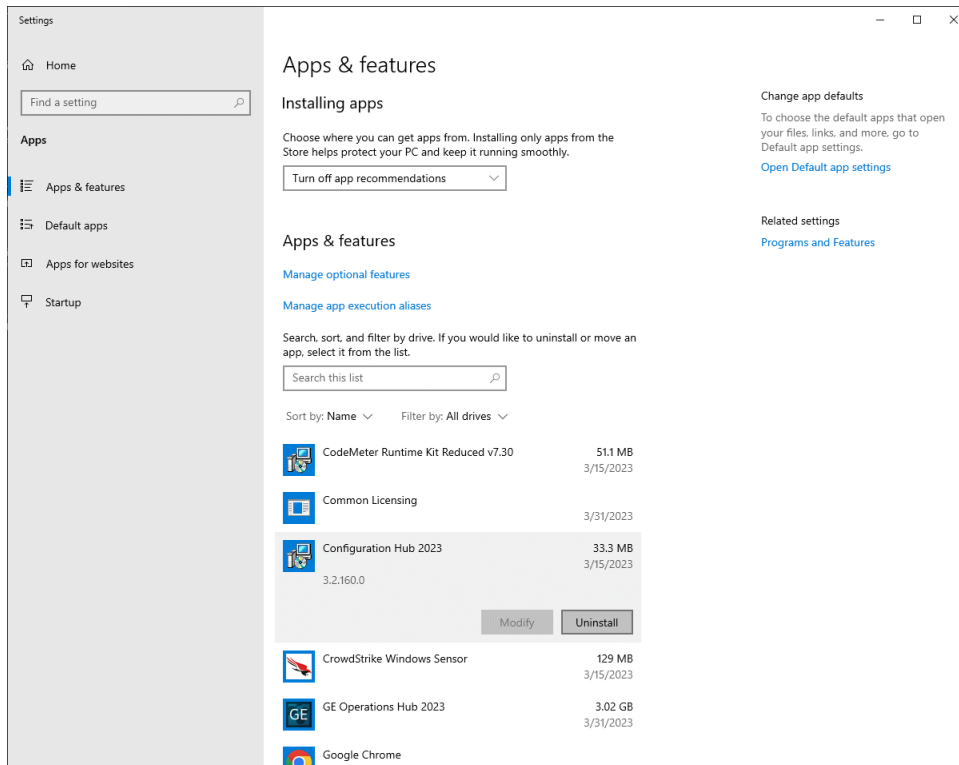
Important:

In order to access Historian from Configuration Hub when using iFIX, you need to manually install the Web Components by browsing the folders on the Integrated Installer to this location: Historian \WebComponents, and then right-clicking the install.exe > Run as Administrator, and install Historian Web-based Clients. Currently, there is not an option to install Web Components from the iFIX Integrated Install experience. You will need to make sure that the [Historian security groups \(on page 97\)](#) are added to your admin user in order to view Historian from Configuration Hub. Restart the browser, after [modifying your user \(on page 107\)](#), and then you can access Proficy Historian from within Configuration Hub, along with iFIX.



Uninstall

To uninstall Configuration Hub, or any of its associated plug-ins (Historian, Webspaces, Operations Hub, for instance), use the **Add Remove Programs** feature in Microsoft Windows. Locate the app you want to uninstall, and select **Uninstall** to remove it. After uninstalling, you can then choose to reinstall with the Integrated Installer again, or through one of the individual installers found in the subfolders on the Integrated Installer.



Installing from a Command

A response file named SilentInstallResponseFile.json is saved to the install folder with the settings you selected for the install – each time you run the integrated install. This response file can be used to run the integrated installer from a command line or programmatically. This can be helpful, for instance, if you have several computers on your network that you need to run the installer on.

You can make your own SilentInstallResponseFile.json using any of the full list of options in detailed in the sections that follow, or modify the one created for you when you installed your products with the integrated install. You can find this autogenerated file in the install folder, which is by default: C:\Program Files (x86)\Proficy.

To run the integrated installer from a command line, use the following command line:

```
D:\Setup\setup.exe -response SilentInstallResponseFile.json
```

where *D:* is the drive where the integrated installer is located.



Note:

In addition to the options provided in the following sections, you can further customize the options selected for the iFIX install by using the [scadaconfig.ini](#) for SCADA installs or the



[installconfig.ini](#) for iClient (View node) installs. Refer to the [iFIX Documentation](#) for more information.

Common Components

```
{
  "packageSelected": "CommonComponents",
  "installLocation": "C:\\Program Files (x86)\\Proficy",
  "configHubClientId": "admin",
  "configHubClientSecret": "*****",
  "uaaClientId": "admin",
  "uaaClientSecret": "*****",
  "selectedPackageProducts": [
    {
      "productName": "Configuration Hub",
      "installType": "installText"
    },
    {
      "productName": "Proficy Authentication",
      "installType": "installText"
    },
    {
      "productName": "Local License Server",
      "installType": "installText"
    },
    {
      "productName": "License Server Tool",
      "installType": "installText"
    }
  ]
}
```

SCADA Client

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

```

    "productName": "iClient",
    "installType": "installText"
  },
  {
    "productName": "Productivity Tools",
    "installType": "installText"
  },
  {
    "productName": "Historian Client Tools",
    "installType": "installText"
  },
  {
    "productName": "Proficy Webspaces",
    "installType": "installText"
  }
],
"nodeName": "FIXVIEW"

"historianServerLocation": "10.10.01.10",
}

```

SCADA Standalone Server

```

{
  "packageSelected": "ScadaStandAloneServer",
  "installLocation": "C:\\Program Files (x86)\\Proficy",
  "nodeName": "FIX",
  "selectedPackageProducts": [
    {
      "productName": "SCADA",
      "installType": "installText"
    },
    {
      "productName": "Industrial Gateway Server [IGS]",
      "installType": "installText"
    },
    {
      "productName": "Productivity Tools",
      "installType": "installText"
    }
  ]
}

```

```

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

```

SCADA with Remote Historian

```

{
  "packageSelected": "ScadaWithRemoteHistorian",
  "installLocation": "C:\\\\Program Files (x86)\\\\Proficy",
  "selectedPackageProducts": [
    {
      "productName": "SCADA",
      "installType": "installText"
    },
    {
      "productName": "Industrial Gateway Server [IGS]",
      "installType": "installText"
    },
    {
      "productName": "Productivity Tools",
      "installType": "installText"
    },
    {
      "productName": "Historian Client Tools",
      "installType": "installText"
    }
  ]
}

```

```

    "productName": "Historian Collectors",
    "installType": "installText"
  }
],
"nodeName": "FIX",
"dataPathFolder": "C:\\\\Proficy Historian Data",
"historianServerLocation": "HIST1",
"historianUserName": "admin",
"historianPassword": "*****"
}

```

Historian Server

```

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

```

Operations Hub

```

{
  "packageSelected": "productOpsHub",
  "installLocation": "C:\\\\Program Files (x86)\\\\Proficy",
  "opshubusername": "ch_admin",
  "opshubpassword": "*****",
  "ophub": {
    "useLocalUaa": false,
    "uaaBaseUrl": "https://server/uaa",
    "adminClientId": "admin",
    "adminClientSecret": "admin",

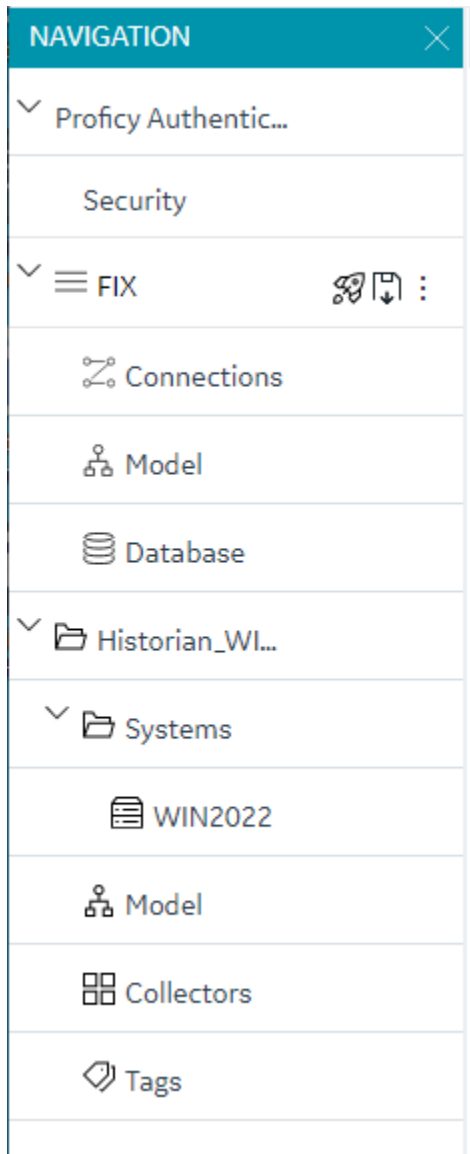
```

```
"configHubRegClientId": "admin",  
"configHubRegClientSecret": "admin",  
"deferConfigHubRegistration": true  
},  
"opshubdrivelocation": "C:",  
"selectedPackageProducts": [  
  {  
    "productName": "Operations Hub",  
    "installType": "installText",  
    "opshubinstalltype": "Silent Install"  
  }  
]
```

Available Product Plugins

Overview

Configuration Hub is a framework where more than one Proficy product can be configured. Currently, you can register Proficy Authentication, iFIX, Historian, and Operations Hub "plugins" with Configuration Hub. When you log in to Configuration Hub, you will see the registered products in the navigation pane. For example, here is the navigation pane showing Proficy Authentication, iFIX, and Historian.



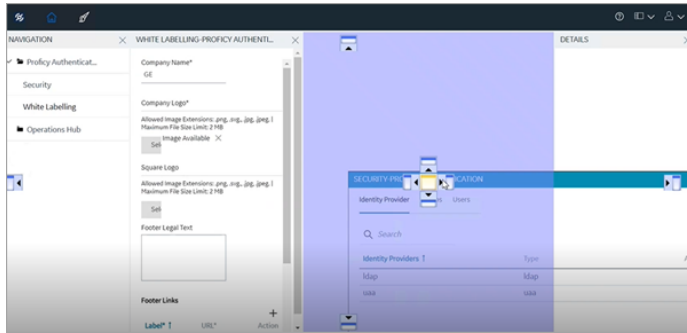
Common Panels

Common Panels

In the Configuration Hub IDE, there are two panels and a toolbar that are common across all products and instances. These panels are the Navigation panel and the Details panel. These panels are always available to re-open via the toolbar. For more information, refer to the following topics:

- [Application Bar \(on page 29\)](#)
- [Navigation Panel \(on page 30\)](#)
- [Details Panel \(on page 32\)](#)

You can make the panels float, and dock them either to the left, right, top, or bottom of the application window.



Application Bar

Configuration Hub has a common toolbar always at the top of the IDE. From this toolbar you can close and open the common panels (Navigation and Details) as well as access the Help and the User actions like Logout.



When configuring an iFIX node, a Home and Save button also appear on this toolbar.

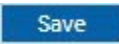


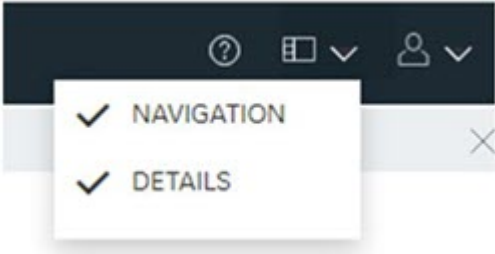



When working with Operations Hub, the paintbrush icon appears between the Home and Save button on the toolbar, so that you can switch between the following application modes appear on the toolbar:

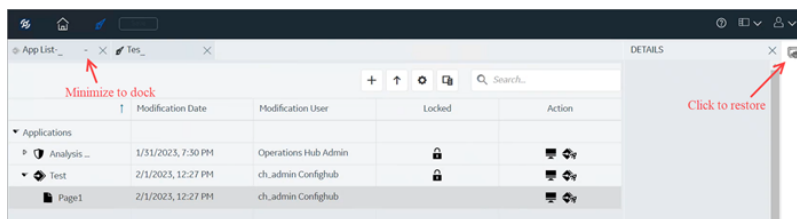
- Designer Mode
- Configure Mode



Item	Description
	Use this button to return to the home view (Configure mode). In Configure mode, you remain connected to the Configuration Hub panels: Navigation and Details.
	When Operations Hub is used with Configuration Hub, use this button to enter Design mode for Operations Hub. In Designer mode, the Configuration Hub panels are disconnected to allow more work area for Op-

Item	Description
	<p>erations Hub designer. The panels appear in this mode while designing pages.</p> <p>In Designer mode, a ribbon bar appears on the left side, wherein you can minimize and dock your items. To restore minimized items on the ribbon bar, click their respective icons. See figure below.</p>
	<p>Click to save your changes locally. These changes will not get pushed to the iFIX server until you publish them.</p>
	<p>Click to access the online help.</p>
	<p>Use this button to open or close a Navigation or Details panel.</p> 
	<p>Click to select Logout. This will end the current user session and load the launch page to select another plug-in. From a single browser session, a user can log into only one plugin at a time. For example, a user can log in to an iFIX node or Historian one.</p>

The following figure shows an example of Design mode, with Operations Hub installed:



Navigation Panel

The Navigation panel contains the plugin instance of the name that you are currently logged into and the associated details. Examples are as follow:

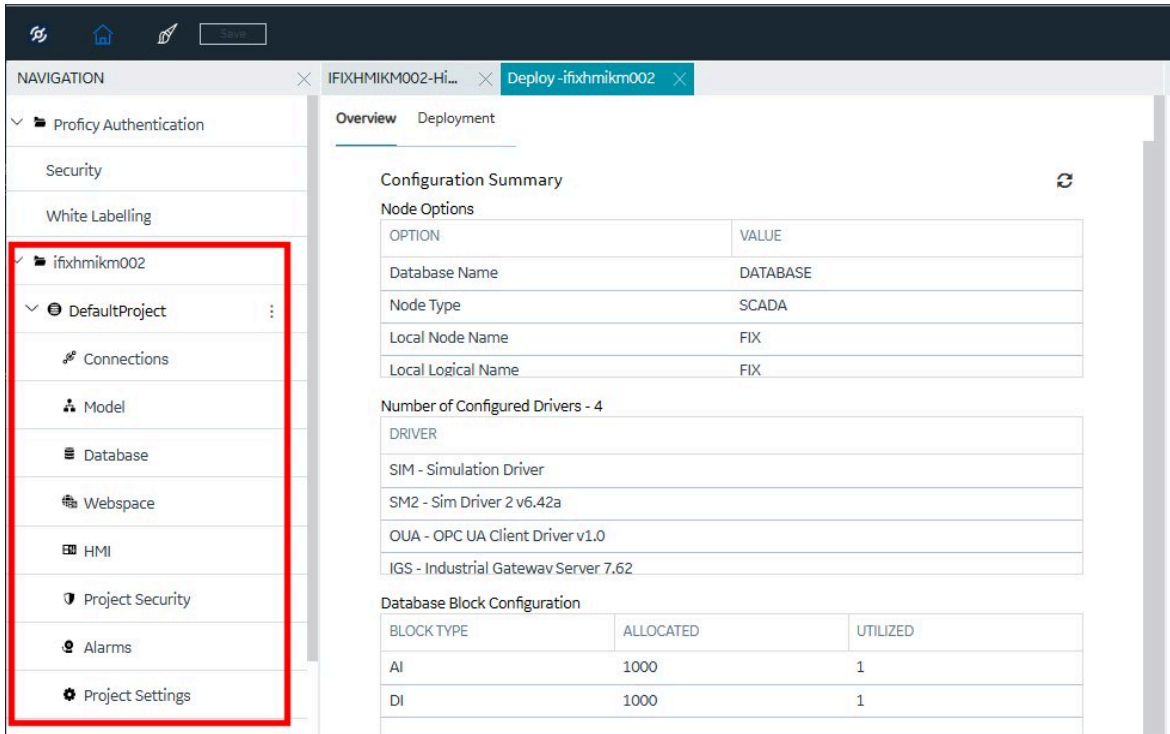
- For Historian, the Navigation panel includes the Systems configured by user. Systems will have Server details displayed. By default, there will be one system created. It also includes the Model, Collectors, Tags, Data Stores, Archives, Data, Alarms, and Activity Logs.

The screenshot displays the Configuration Hub interface for a Historian system. The NAVIGATION panel on the left shows a tree view with 'Historian_IFIXHMIK...' selected and highlighted with a red box. The SYSTEM panel in the center displays a table of servers for the selected system, with one server named 'ifixhmik002' shown as 'Connected'. The DETAILS panel on the right shows various system parameters such as Name, System Type, Primary Server, Description, Default System, Collectors, Tags, Data Stores, Clients, Server Time, Server Version, Demo Mode, and Clustered status.

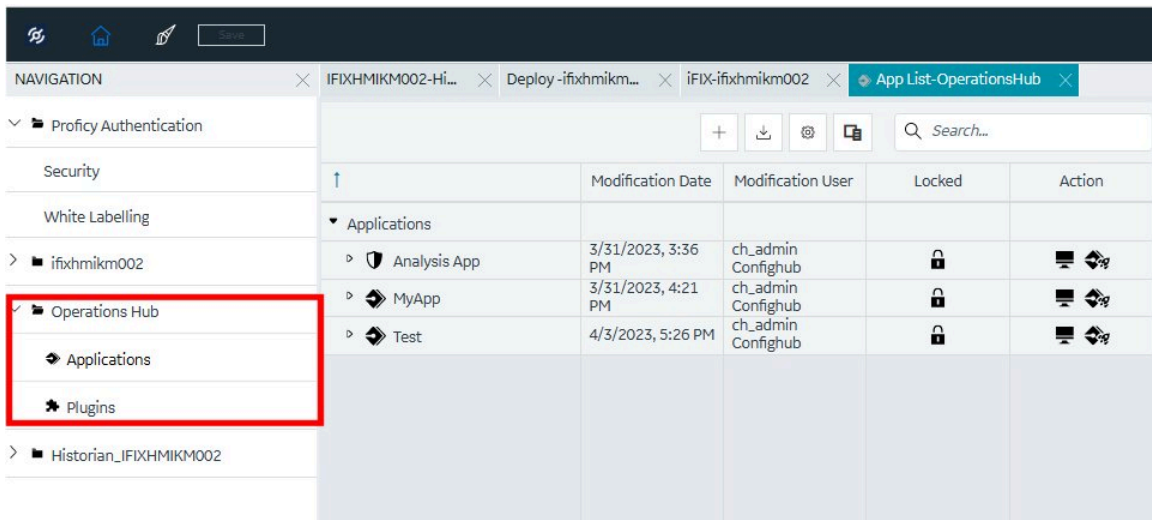
MACHINE NAME	STATUS	ARCHIVE CO..	WRITE CACH..	CONSUMPTL..
ifixhmik002	Connected	36.3	0.75	0.47

FIELD	VALUE
GENERAL	
Name	IFIXHMIK002
System Type	Standalone Syste...
Primary Server	IFIXHMIK002
Description	IFIXHMIK002
Default System	Yes
Collectors	1
Tags	2
Data Stores	3
Clients	3
Server Time	4/5/2023, 2:23:5...
Server Version	11.0.6093.0
Demo Mode	No
Clustered	No

- In the case of iFIX, the plugin name is the node name of your iFIX node. Under the node name, you will see a Default Project and Connections, Model, Database, WebSpace (if WebSpace is installed and configured), HMI (if Operations Hub is installed and configured), Project Security, Alarms, and Project Settings panels.



- In the case of Operations Hub, you will see an Applications and Plugins panels.



Depending on the product, the Navigation panel will have different options available to open and configure.


Details Panel


The Details panel is a companion panel that responds and works with the currently active panel in the IDE.

For example, if you are configuring the iFIX Database panel, the Details panel will show the tag property grid for the currently selected tag.

DETAILS

ABLAST992

 *Search...*

FIELD	VALUE	
<div style="display: flex; align-items: center;"> ▼ GENERAL </div>		
Tag Name	ABLAST992	
Description	I/O ADDRESS RE	
Type	AI - Analog Input	
Current Value	93	
<div style="display: flex; align-items: center;"> ▼ IO ADDRESSING </div>		
I/O Driver	SIM	
I/O Address	RE	
Signal Conditioning		
H/W options		
Process By Excepti...	NO	
Scan Time	0.05	
Phase At		

For Historian, the Details panel will show the various details pertaining to Collectors and Servers at this point of time. You will be able to take some actions from this pane as well.



The image shows a 'DETAILS' panel with a close button (X) in the top right corner. The panel contains a table of configuration properties. The first row is 'Collector Type' with the value 'OPC UA DA Collector'. The second row is 'Status' with a red dot icon and the value 'Unknown'. The third row is 'Description'. The fourth row is 'Compression' with the value 'Off'. The fifth row is 'Debug Level' with the value '0 - Debug off'. The sixth row is 'Destination' with the value 'historian'. The seventh row is 'Configuration Type' with the value 'Historian'.

DETAILS	
Collector Type	OPC UA DA Collector
Status	● Unknown
Description	
Compression	Off
Debug Level	0 - Debug off
Destination	historian
Configuration Type	Historian

For Proficy Authentication, the Details panel will show properties for identity providers, groups, and users. The following example shows the details of the default user, ch_admin:

DETAILS	
ch_admin	
<input type="text" value="Search"/>	
Field	Value
GENERAL	
Name	ch_admin
First Name	Confighub
Last Name	ch_admin
Email	ch_admin@test....
Active	<input checked="" type="checkbox"/>
Origin	uaa
GROUP MEMBERSHIP	
historian_visuali...	
ih_unaudited_wr...	
historian_rest_a...	
confighub.access	
ih_archive_admi...	
zones.write	
scim.invite	
historian_visuali...	
clients secret	

Concurrency Management

One of the advantages to a browser-based tool is that more than one user can access the system at the same time. Configuration Hub supports this generally with some of the following considerations:

Generally

- Working on one plugin has no overlap with working on a different plugin in terms of different users overwriting each other's work.

iFIX

- An iFIX node can only ever have one active database, so changes resulting from the Publish operation to the running database will be reflected across every browser session.
- The Unpublished changes on any given node are common to all browser sessions accessing that node. So, a user on one browser adding tags, importing tags, modifying, and adding to the model and so on will affect what a user in a different browser session working on the same node will see. For example, if one user imports 1000 tags into the database, a second user looking at the same Database panel will see those tags appear in their panel even though they have not yet been published to the running iFIX SCADA system.
- If a user is in the middle of changing anything in iFIX that requires a "Save" operation, they will be prompted to save and refresh if the database is changed from any other source.
- Generally, you should avoid importing from more than one session at the same time. Though this is supported from the Data panel, it will slow down performance drastically to have multiple imports happening simultaneously.

Historian

- Changes resulting from a Publish operation will be reflected across every browser session.
- If an item is changed from any other source while a user is in the middle of making a change in Historian that requires a "Save" operation, the user will be prompted to save and refresh.

Server Certificates for Configuration Hub

Server-side certificates allow for secure connections between the REST services running and the Configuration Hub web server. The SSL certificate for Configuration Hub is valid for two years and must be regenerated after it expires. If you need to regenerate your certificates use the following steps.

Self-Signed Certificates for Configuration Hub

Use the following steps to update your self-signed certificates for Configuration Hub:

1. Either remove or backup the certificate files in C:\Program Files (x86)\Proficy\ConfigurationHub\ConfigHubPki folder.
2. Open a command prompt as an administrator in the C:\Program Files (x86)\Proficy\ConfigurationHub directory.
3. Enter the following command to create new self-signed certificates:

```
restart_confighub.bat "C:\Program Files (x86)\Proficy\ConfigurationHub" "C:\Program Files  
(x86)\Proficy\ConfigurationHub\Web" 5678 4890 htclab.ge.com
```

where "C:\Program Files (x86)\Proficy\ConfigurationHub" is the Configuration Hub install directory, C:\Program Files (x86)\Proficy\ConfigurationHub\Web is the directory where the Configuration Hub server resides, 5678 is the Configuration Hub authentication service port (Not used any more), and 4890 is the Configuration Hub server port.

4. Copy the server_cert.crt and server_cert.key files the from C:\Program Files (x86)\Proficy\ConfigurationHub\ConfigHubPki folder to the C:\Program Files (x86)\Proficy\ConfigurationHub\Web\conf folder.
5. Restart the computer.

Self-Signed Certificates for iFIX with Configuration Hub

Use the following steps to update your self-signed certificates for iFIX:

1. Open iFixConfigServiceCertTool.exe as an administrator. This tool is found in the C:\Program Files (x86)\Proficy\iFIX\ folder. The iFIX Configuration Service Certificate Tool appears.
2. Click Delete Certificates, and then click Delete Certificate Binding.
3. From the Windows File Explorer, remove or backup the certificate files in C:\Program Files (x86)\Proficy\iFIX\CFG\iFIX_OpcuaConfigService\pki directory.
4. From iFIX Configuration Service Certificate Tool, create the new certificates by clicking on the Create Certificates button.
5. After the new set of certificates are created, ensure that the certificate thumbprint is different in the iFIX Configuration Service Certificate Tool. If they are not different, the new certificates are not created.
6. Copy the iFIX_OpcuaConfigServer.crt and iFIX_OpcuaConfigServer.key files from C:\Program Files (x86)\Proficy\iFIX\CFG\iFIX_OpcuaConfigService\pki into the C:\Program Files (x86)\Proficy\iFIX\web\conf directory.
7. Restart the computer.

External Certificates for Configuration Hub and iFIX

Use the following steps to configure an externally issued server certificate for Configuration Hub and iFIX.

1. Obtain the private key, server certificate, and the CA bundle that contains the certificates for the issuers. Typically, the private key is generated by you or someone in your organization, and the certificate vendor provides you with the server certificate and the CA bundle.
2. If you received the certificates and the private key in other formats (such as PFX), consult your vendor on how to obtain them as or convert them into PEM files.
3. In a text editor, open the PEM file and locate the multiple certificates mentions; each certificate is enclosed by an opening line:

```
-----BEGIN CERTIFICATE-----
```

and a closing line:

```
-----END CERTIFICATE-----
```

4. Confirm that the server certificate appears first in this certificate PEM file, followed by the CA certificates in the CA bundle.
5. For Configuration Hub, copy the root and server certificates and key files into the C:\Program Files (x86)\Proficy\ConfigurationHub\ConfigHubPki folder, and the server certificate and key files to the C:\Program Files (x86)\Proficy\ConfigurationHub\Web\httpd\conf folder. (In Configuration Hub the HTTPD server certificate files are named: server.crt and server.key.)



Note:

If there is a name change, then the httpd.conf file in the C:\Program Files (x86)\Proficy\ConfigurationHub\Web\httpd\conf\httpd.conf folder also must be updated with the correct file names.

6. If iFIX is used with Configuration Hub, copy the root and server certificates and key files into the C:\Program Files (x86)\Proficy\iFIX\CFG\iFX_OpcuaConfigService\pki folder, and the server certificate and key files to the C:\Program Files (x86)\Proficy\iFIX\web\httpd\conf folder. (In iFIX, the HTTPD server certificate files are named: iFIX_OpcuaConfigServer.crt and iFIX_OpcuaConfigServer.key.)



Note:

If there is a name change, then the httpd.conf file in the C:\Program Files (x86)\Proficy\ConfigurationHub\Web\httpd\conf\httpd.conf folder also must be updated with the correct certificate file names.

7. Also for iFIX, edit the ifix_config_service.json file (found in the C:\Program Files (x86)\Proficy\iFIX\CFG folder) with the correct certificate file names. The following fields must be updated in this file:


```
"rootCertificateName": "iFIX_OpcuaConfigRoot",
"serverCertificateName": "iFIX_OpcuaConfigServer",
"serverCertificatePassPhrase": "75D43CAAC1E440F08080D7E4A58AE941",
"generateSSLCerts": false
```



Important:

The "generateSSLCerts" field must be set to false if external certificates are used.

Client Certificates for Configuration Hub

For a browser to have a secure connection to Configuration Hub, the Configuration Hub certificate must be copied to the remote machine and added to the trusted root folder. Client-side certificates validate the client's identity to the Configuration Hub web server.

Configuration Hub Root Certificate

To install the Configuration Hub root certificate:

1. Copy the ConfigHubRootCA.crt file on the server machine. By default, this file can be found in the C:\Program Files (x86)\Proficy\ConfigurationHub\ConfigHubPki folder.
2. Paste the ConfigHubRootCA.crt file to the destination computer.
3. Double-click ConfigHubRootCA.crt to install the certificate. The Install Certificate screen appears.
4. Click the Install Certificate button. The Import Certificate screen appears.
5. Select Local Machine, and then Next. A message appears requesting if you want to proceed.
6. Click Yes. The Certificate Store Screen appears.
7. Select Place All Certificates in the Following Store.
8. Click Browse, and then select Trusted Root Certificate Authorities and then click OK.
9. Click Next. The final screen appears.
10. Click Finish. A message should appear indicating the import was successful.
11. Click OK.
12. Restart the browser.

iFIX Configuration Hub Client Root Certificate

To install the iFIX OPC UA Client root certificate:

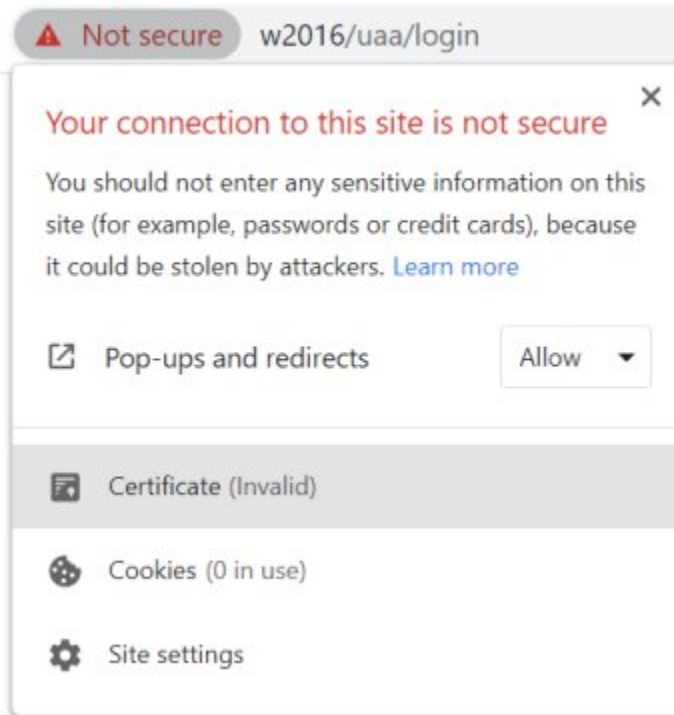
1. Copy the iFIX_OpcuaConfigRoot.crt file on the server machine. By default, this file can be found in the C:\Program Files (x86)\Proficy\iFIX\CFG\ iFIX_OpcuaConfigService folder.
2. Paste the iFIX_OpcuaConfigRoot.crt file to the destination computer.
3. Double-click iFIX_OpcuaConfigRoot.crt to install the certificate. The Install Certificate screen appears.
4. Click the Install Certificate button. The Import Certificate screen appears.
5. Select Local Machine, and then Next. A message appears requesting if you want to proceed.
6. Click Yes. The Certificate Store Screen appears.
7. Select Place All Certificates in the Following Store.
8. Click Browse, and then select Trusted Root Certificate Authorities and then click OK.
9. Click Next. The final screen appears.
10. Click Finish. A message should appear indicating the import was successful.
11. Click OK.
12. Restart the browser.

Enable a Trust with Historian with a Self-Signed Certificate in Chrome

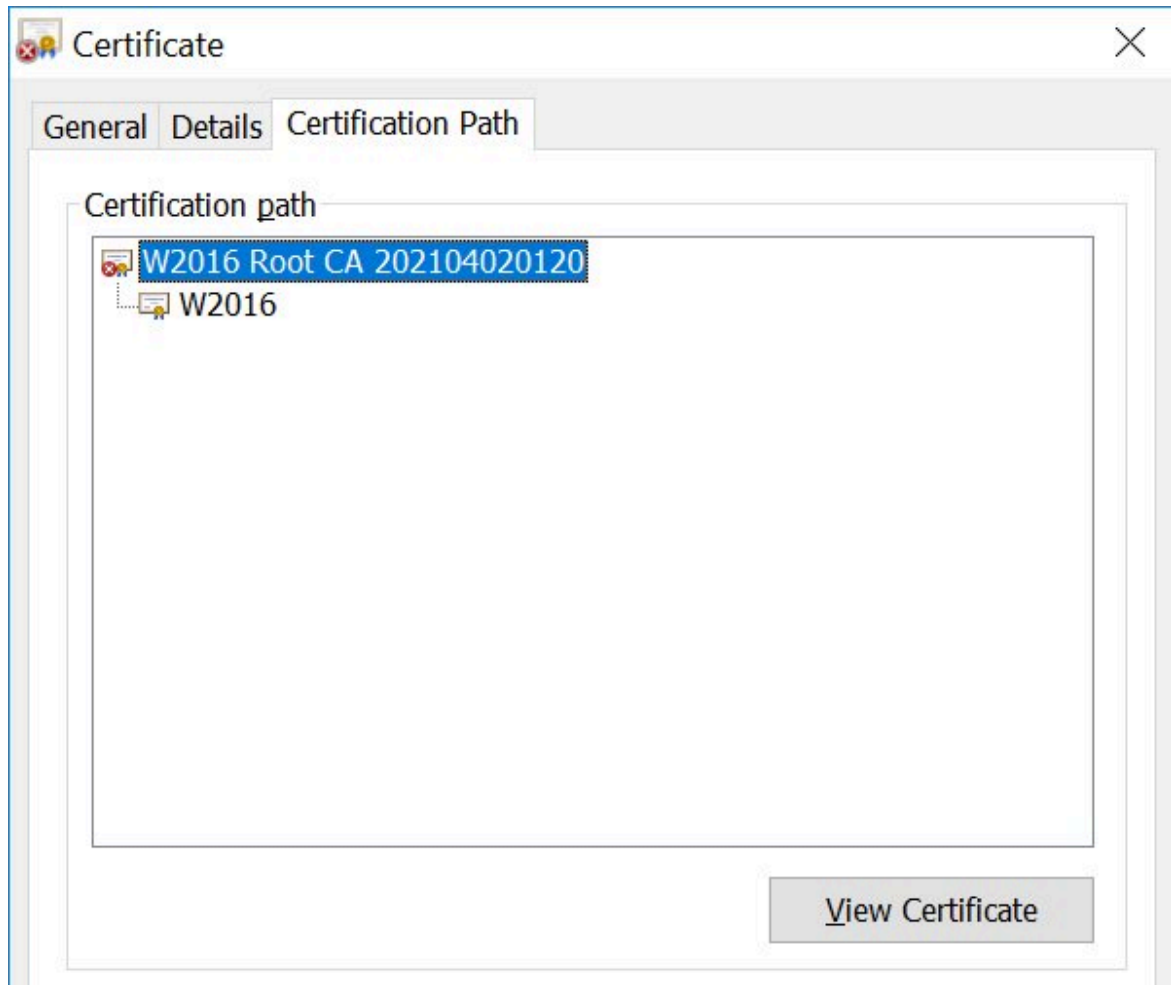
During Historian installation, a self-signed certificate is generated for use with Historian web applications. A self-signed certificate is a certificate that is signed by itself rather than signed by a trusted authority. Therefore, a warning appears in the browser when connecting to a server that uses a self-signed certificate until it is permanently stored in your certificate store. These steps describe how to ensure that Google Chrome trusts the self-signed certificate.

To enable a trust with Historian using a Self-Signed Certificate in Chrome:

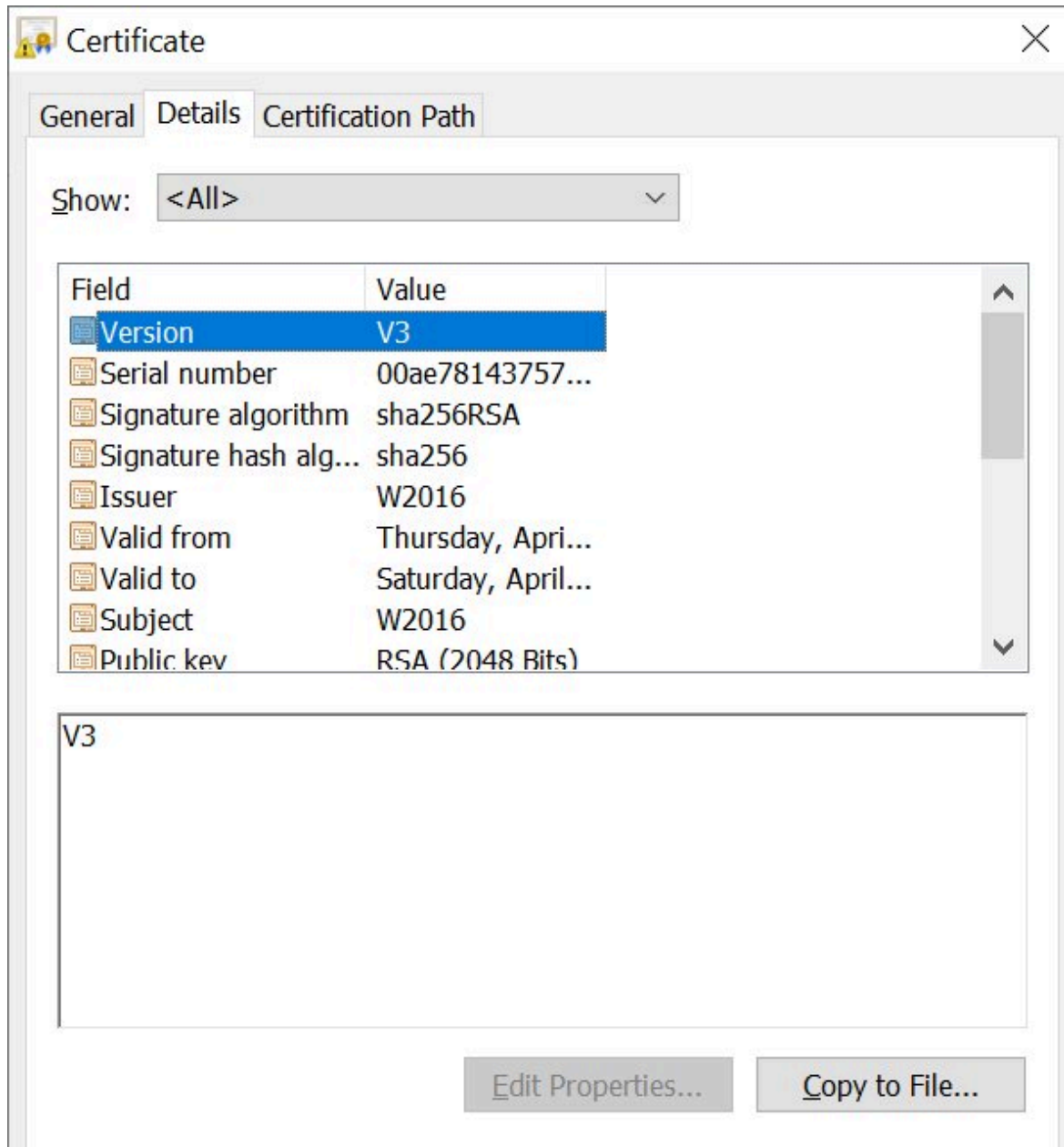
1. Using Google Chrome, access the site to which you want to connect. A message appears to inform you that the certificate is not trusted by the computer or browser.
2. Select **Not Secure** in the URL, and then select **Certificate**. The Certificate window appears.



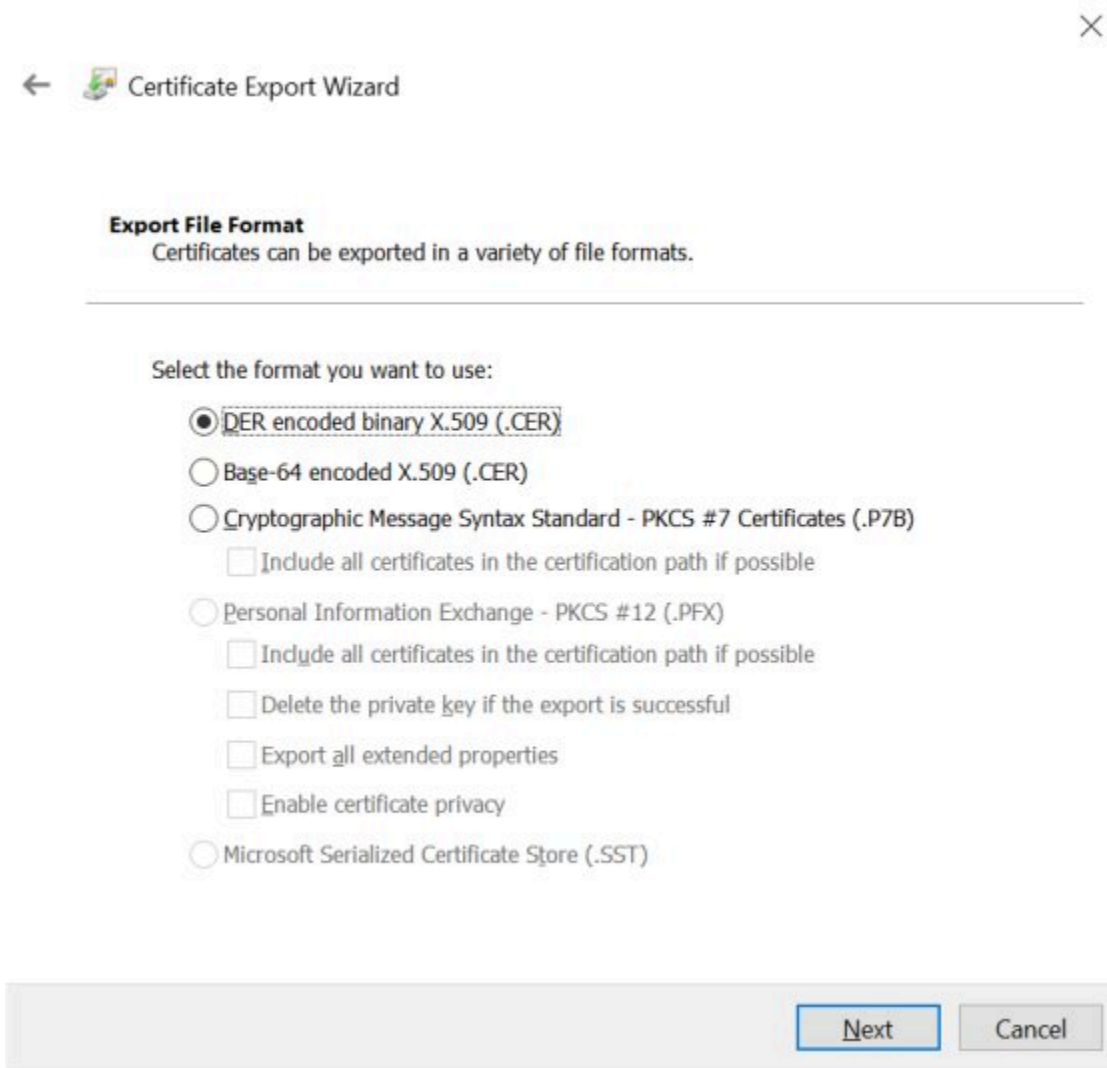
3. Select the **Certification Path** tab, and then select the **root certificate**.



4. Select **View Certificate**. The Certificate window appears, displaying the General, Details, and Certification Path sections. Select Details, and then select Copy to Files.



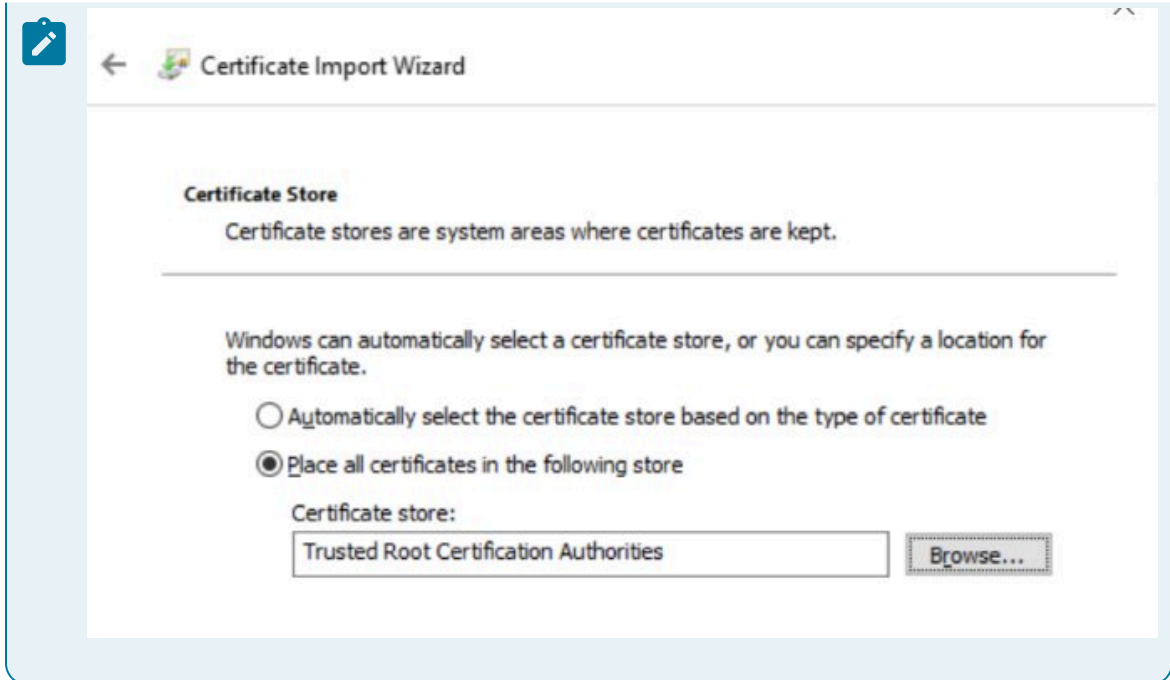
5. Follow the on-screen instructions to save the certificate to a local file. Use the default format: DER encoded binary X.509 (.CER).



6. Right-click the .CER file that you have exported, and select **Install Certificate**. The Certificate Import Wizard window appears.
7. Select **Local Machine** and click Next.
8. Select **Trusted Root Certificate Authorities**, and then select OK.

**Note:**

Do not let the wizard select the store for you.



A Security Warning window may appear. If it does, ignore the message by selecting Yes. The certificate is installed.

9. Restart the browser, and connect to the server.
10. Open the URL authenticated by the certificate. If error messages do not appear, the certificate is successfully imported.

Import an Issuer Certificate in Chrome for Historian

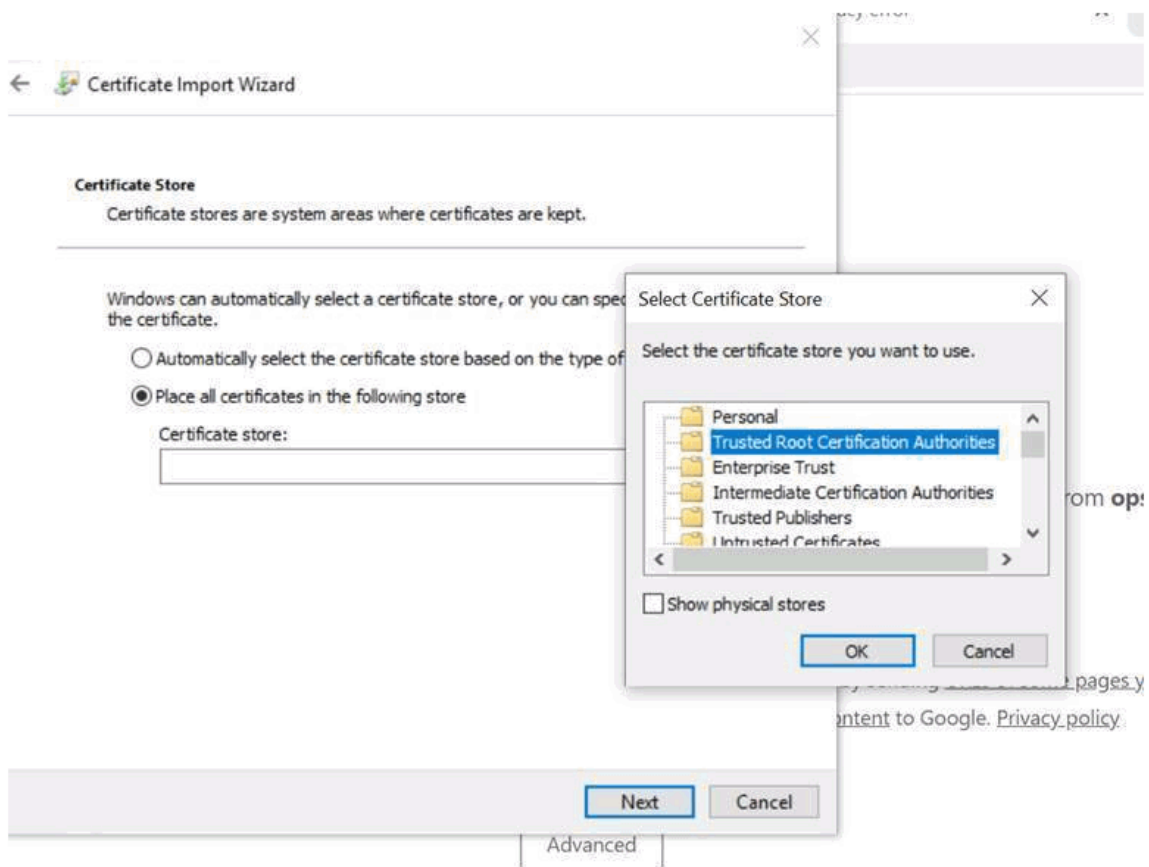
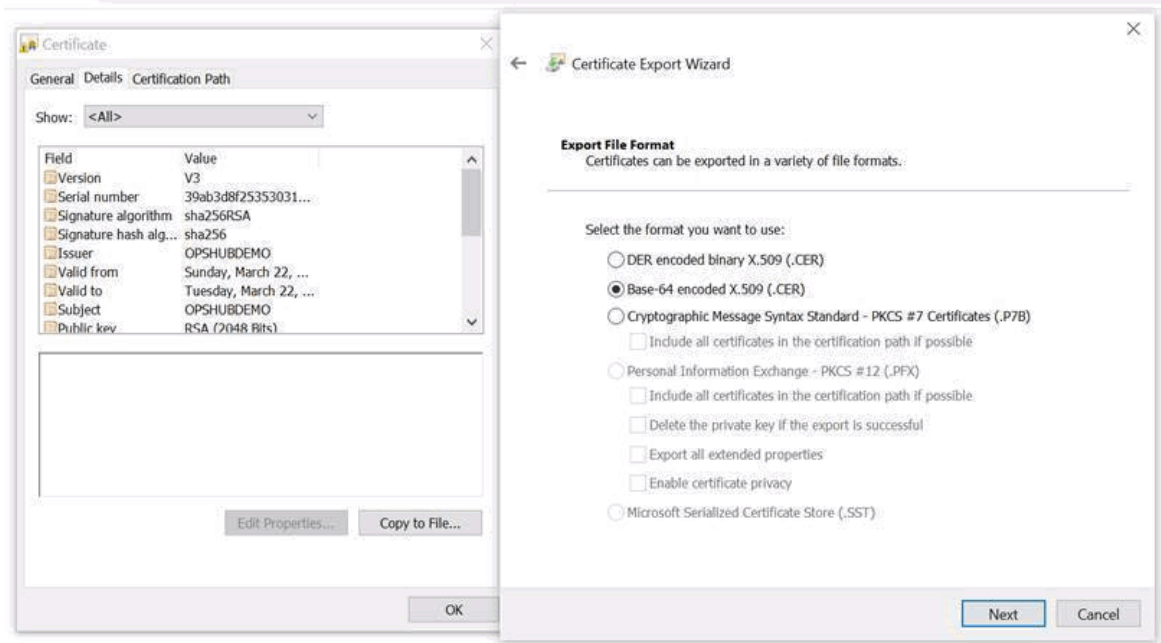
If you want to use an external UAA, you must import an issuer certificate.

1. Copy the issuer certificate from the machine on which UAA is installed.
2. Access the Certificate Management tool. The GE Operations Hub Certificate Management Tool page appears, displaying the Server Certificate section.
3. In the External Trust subsection, next to the Certificate File box, select Select.
4. Navigate to and select the certificate file, and then select Open.
5. Select Import. A message appears, asking you to confirm that you want to import a certificate.
6. Select Yes. You are now ready to use Configuration Hub.

For more information on Historian, security, and certificates, refer to the [Historian online documentation](#).

Operations Hub Client Certificates

1. On the client machine, open a browser such as Google Chrome and access the Operations Hub server using the url. For example: `https://opshubservername/iqp`. The browser should display a "Not secure" icon.
2. Right-click the Not Secure icon, which should lead you to a Certificate dialog box.
3. Find the issuer in the **Certificate Path** tab.
4. On the issuer, select **View Certificate**.
5. In the **Certificate** dialog box, on the issuer certificate, select the **Details** tab and then **Copy To File**.
6. Right-click that exported certificate file, and choose to import it into the Trusted Root Certificate Authorities store.



Proficy Authentication Certificate

The location of the Proficy Authentication certificate is, by default:

```
C:\Program Files (x86)\Proficy\ConfigurationHub\UaaCert\uaa_cert.crt
```

During iFIX registration with Proficy Authentication, this certificate is automatically imported for you. However, if there is error or you want to reinstall the certificate, you can browse to the folder above on the installed product folder, and then copy it and register it manually.

Proficy Authentication Certificate

To install the Proficy Authentication certificate:

1. Copy the uaa_cert.crt file from the C:\Program Files (x86)\Proficy\ConfigurationHub\UaaCert folder.
2. Paste the uaa_cert.crt file to the destination computer.
3. Double-click uaa_cert.crt to install the certificate. The Install Certificate screen appears.
4. Click the Install Certificate button. The Import Certificate screen appears.
5. Select Local Machine, and then Next. A message appears requesting if you want to proceed.
6. Click Yes. The Certificate Store Screen appears.
7. Select Place All Certificates in the Following Store.
8. Click Browse, and then select Trusted Root Certificate Authorities and then click OK.
9. Click Next. The final screen appears.
10. Click Finish. A message should appear indicating the import was successful.
11. Click OK.
12. Restart the browser.

Known Issues and Limitations

The following limitations apply to using Configuration Hub:

- Multiple users can log into the same server and make changes, but they must be different browser sessions.
- Only the following browsers were tested for use with Configuration Hub and iFIX: Google® Chrome, Microsoft® Edge based on Chromium, Mozilla® Firefox, or Apple® Safari (MAC OS only).

**Note:**

Sometimes the MAC OS cannot resolve the system name. In this case, update the hosts file. Also, on the MAC OS, you will be required to manually install the Configuration Hub root certificate.

- From a single browser session, a user can log into only one plugin at a time. For example, an iFIX node or Historian one.
- For iFIX, you can only run Configuration Hub from a running SCADA node. View nodes/iClients will not be able to login to Configuration Hub.
- For Historian, if only one machine remains in a mirror group, you cannot remove it.
- If you install Configuration Hub and the Historian Web Admin console on the same machine, and use self-signed certificates for both of them, the login page for Configuration Hub does not appear. To prevent this issue, disable the domain security policies:
 1. Access the following URL: `chrome://net-internals/#hsts`
 2. In the **Domain Security Policy** section, in the **Delete domain security policies** field, enter the domain name for Configuration Hub, and then select **Delete**.
- Configuration Hub cannot be installed on computers with machine names containing non-English characters.
- For German, French, and Polish languages, when using Configuration Hub, the iFIX database name can only be in lower case letters. Do not use capital letters for the iFIX database file name in these languages; capital letters in an iFIX database file name are not supported for German, French, or Polish.
- Configuration Hub will display the number formats and strings as they appear on SCADA or Historian Server node. Changing the browser language will not have impact on the appearance of this data.
- In the Connections Panel, group parameters do not support regional number formatting.
- Only English alphanumeric characters values and the following symbols are supported in the client ID and client secret fields:


```
"-<>$~!@#%^&*?!"
```
- When iFIX and Configuration Hub are on different computers and an error displays that the iFIX SCADA is not active or unable to retrieve locale information, ensure that iFIX is started and that SCADA is enabled. (If iFIX has Failover enabled, then only the Primary Node in Maintenance Mode can connect to Configuration Hub.) Also, make sure that both systems have same date and time.
- Spaces are not supported in the model or iFIX tag names in Configuration Hub.

- If Historian and iFIX are registered with the same Configuration Hub, the Historian Model editor will be disabled. In this case, you can use the iFIX model to create your model.
- When multiple iFIX and Historian plugins are registered to Configuration Hub, all plugins should use same Proficy Authentication (UAA) Server Name. If the Configuration Hub or Proficy Authentication Server are part of a domain system, then Fully Qualified Domain Name (FQDN) name should be used for Server Name.
- When iFIX is upgraded from a previous version of iFIX, sometimes the iFIX Register to Configuration link shows as non-trusted. You will need to delete the certificates and binding, and then recreate them using the iFixConfigServiceCertTool.exe tool (as an Administrator). As a final step to establish the trust, you would need to copy the certificate files (iFIX_OpcuaConfigServer.crt and iFIX_OpcuaConfigServer.key files) from the C:\Program Files (x86)\Proficy\iFIX\CFG\iFIX_OpcuaConfigService\pki folder into the C:\Program Files (x86)\Proficy\iFIX\web\conf directory, and restart iFIX.
- For Configuration Hub, it is recommended to use a display setting at 1920x1080 or better, with scaling set to 100%.
- Be aware that if you want to publish a model from iFIX 2023 to Operations Hub, you must use Operations Hub 2023.
- Alarm name, tag name, model object instance names should not be same.
- iFIX entities like the database name, tag names, alarm areas, model types, and model instances must be unique. Ensure you use unique names when creating these items.
- Computers connected in a Work Group environment is not supported in iFIX 2023 with shared drive Security Paths (using Configuration Hub).
- The iFIX Registration page does not function when the Client ID or Client Secret for Configuration Hub or Proficy Authentication include any characters other than the alphanumeric character set from the English keyboard. This is currently a known limitation. There is no workaround.

High Availability for Configuration Hub

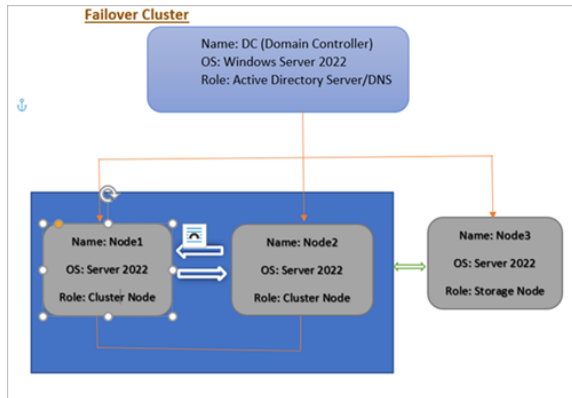
Overview

This topic provides an overview of a clustered environment for high availability for Configuration Hub. It does not cover SCADA Enhanced Failover. iFIX Failover should not be used on a node participating in this High Availability configuration. See [Special Considerations for SCADA Enhanced Failover \(on page 198\)](#) for details on SCADA Enhanced Failover with Configuration Hub.

High availability (HA) is the ability of a system to operate continuously without failing for a designated period of time. HA works to ensure a system meets an agreed-upon operational performance level. The following sections describe how high availability works with Configuration Hub.

About Failover Cluster

In a cluster environment, multiple servers are installed, which share the same data. Each of these servers is called a node. One of them acts as the primary node, while the others are standby nodes. If the primary node is down, one of the standby nodes is used.



For example, if Configuration Hub on the primary node is unable to connect to the server, then the user session on the standby node is activated. Therefore, you will still be able to connect to the server using Configuration Hub installed on the standby node.

Configuration Hub works with Microsoft Failover Cluster Manager to ensure high availability of web-based clients. The following services are shared between the primary and standby nodes in a cluster. Using Failover Cluster Manager, you must add these services to the cluster.

- `ConfighubContainerService`
- `ConfigHubHttpdService`

Refer to [Configure High Availability for Configuration Hub \(on page 51\)](#).

For additional information on Windows failover clustering, visit the following links:

- <https://docs.microsoft.com/en-us/windows-server/failover-clustering/create-failover-cluster#install-the-failover-clustering-feature>
- <https://www.papercut.com/support/resources/manuals/ng-mf/common/topics/cluster-server-2012-2016.html#Create>

Configure High Availability for Configuration Hub

This topic describes how to set up a highly available server for Configuration Hub using Windows failover cluster.

You need:

- Two Windows Server 2022 virtual machines to serve as nodes in a cluster:
 - Primary node (Node1)
 - Secondary node (Node2)

Ensure that both the nodes (primary and secondary) have the same domain name, and are installed with the same version of Windows Server.

- One Windows Server 2022 virtual machine (Node3) in the same domain.

Create a shared drive on this node, which both the nodes in the cluster can access.

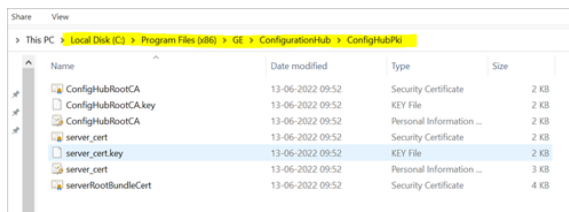
- During installation, provide the same Configuration Hub credentials in both the nodes. Use the same cluster name created in the Windows failover cluster manager.

Perform the following tasks to set up high availability for Configuration Hub using a two-node failover cluster.

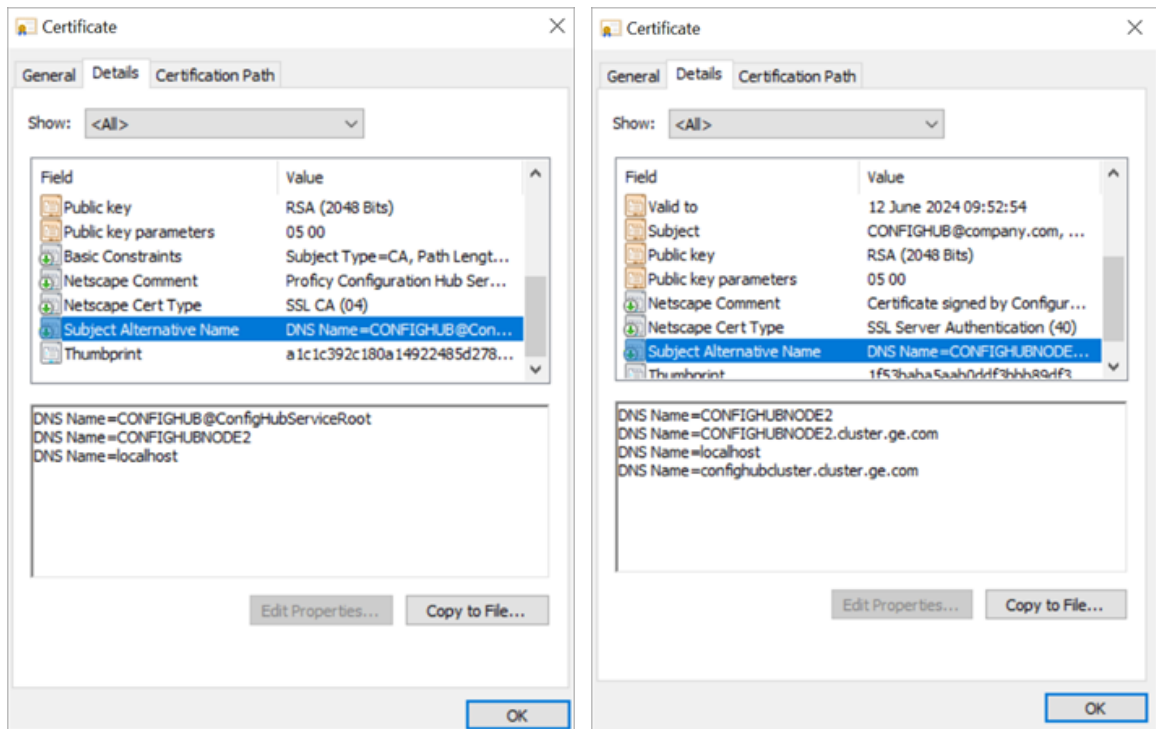
1. [Install Failover Clustering Feature \(on page 54\)](#)
2. [Create Failover Cluster \(on page 55\)](#)
3. [Create Role \(on page 58\)](#)
4. [Create Client Access Point \(Virtual IP\) \(on page 60\)](#)
5. [Add Dependencies to Role \(on page 62\)](#)
6. [Create Network Attached Storage \(on page 63\)](#)
7. [Install Configuration Hub on Cluster Nodes \(on page 65\)](#)
8. [Handling Silent Installation \(on page 67\)](#)

When Configuration Hub is installed on a node server (for example, Node1):

- `ConfigHubRootCA.crt` and `ConfigHubRootCA.key` files are created in the `ConfigHubPki` folder using Node1 DNS name Configuration Hub ports.
- Using the above root certificates, `server_cert.crt` and `server_cert.key` files are created to access the application.



- The Configuration Hub cluster name parameter is sent to the `RegisterConfighub_httpd.bat` for creating certificate 'subject alternative names' using the cluster name.



- Two extra parameters are introduced to capture 'cluster name' and 'domain name' if high availability is set up for Configuration Hub. The root certificates and server certificates are created using the extra parameter like 'cluster name'. All cluster nodes certificates have the same 'cluster name' so users can access all the nodes without any certificate issues.

```

RegisterConfigHub_httpd.bat - X
1 REM Parameters
2 REM %1 httpd root directory
3 REM %2 full path to httpd.exe
4 REM %3 confighub root directory
5 REM %4 storage service port
6 REM %5 container service port
7 REM %6 full qualified domain name
8 REM %7 Dns Name 1
9 REM %8 Dns Name 2
10
11 ECHO %1 %2 %3 %4 %5 %6 %7
12
13 cd /d %3
14 REM call config_service_cert.bat %3 %4 %5 ConfigHubRootCA server_cert proficy %6
15 IF [%7] == [] (
16 call config_service_cert.bat %3 %4 %5 ConfigHubRootCA server_cert proficy %6 ) ELSE (
17 IF NOT [%8] == [] (
18 call config_service_cert.bat %3 %4 %5 ConfigHubRootCA server_cert proficy %6 %7 %8 ) ELSE (
19 call config_service_cert.bat %3 %4 %5 ConfigHubRootCA server_cert proficy %6 %7 ) )
20
21 cd /d %1
22 set HTTPD_PATH=%1
23 nssm install "ConfigHubHttpdService" %2
24 nssm set "ConfigHubHttpdService" ObjectName Network Service
25 REM PAUSE
26 REM nssm set "ConfigHub Httpd Service" Start SERVICE_AUTO_START
27 REM nssm set "ConfigHub Httpd Service" AppDirectory %HTTPD_PATH%
28 nssm set "ConfigHubHttpdService" Description "WebServer for Configuration hub."
    
```

- Configuration Hub installer copies `ConfigHubRootCA.crt` and `ConfigHubRootCA.key` files into shared configuration. These are used in the other nodes for creating `server_cert.key` and `server_cert.key` files and maintains a trust between both nodes.

- While installing Configuration Hub on other cluster nodes, the system checks if any root certificates exist in the given shared configuration path or not. If certificates exist, then copies both `ConfigHubRootCA.crt` and `ConfigHubRootCA.key` into the local machine `ConfigHubPki` folder of Configuration Hub, and then creates server certificates using the root certificates.

Install Failover Clustering Feature

This topic describes how to install the failover clustering feature on the nodes.

Perform these steps on both the server nodes (Node1 and Node2).

1. Log in to the node server.
2. Go to **Start > Administrative Tools > Server Manager**.
3. From the Server Manager dashboard, select **Manage > Add roles and features**.
4. Complete **Add Roles and Features Wizard** with these options:

Section	What To Do
Before You Begin	Skip to the next section.
Installation Type	Select Role-based or feature-based installation .
Server Selection	<ol style="list-style-type: none"> Choose the option Select a server from the server pool. Under the server pool section, select your Node1 server. This means you will be installing the role/feature on this server.
Server Roles	In the roles list box, select the check box for File and Storage Services .
Features	<p>To allow the installation of Failover Cluster Manager:</p> <ol style="list-style-type: none"> In the features list box, select the check box for Failover Clustering. <p>The Add features that are required for Failover Clustering? screen appears, which shows the dependencies that are installed with this feature.</p> <ol style="list-style-type: none"> Select Add Features.
Confirmation	Select Install .

The selected role and feature is installed on the server node.

5. When the installation is complete, restart the machine.

After completing the steps in this topic, the failover clustering feature is installed on all the server nodes you want to include in the failover cluster.

[Create Failover Cluster \(on page 55\)](#)

Create Failover Cluster

This topic describes how to create a failover cluster.

[Install Failover Clustering Feature \(on page 54\)](#)

You can perform these steps on either Node1 or Node2. Suppose you perform these steps on Node1, they are automatically applied to Node2.

1. Log in to the server node.
2. Go to **Start > Administrative Tools > Failover Cluster Manager**.
3. In Failover Cluster Manager, select **Validate a Configuration**.

Before starting to create a cluster of nodes, you should validate whether the nodes that you are adding to the cluster are compatible with the cluster hardware requirement. For more information, refer to [Microsoft documentation](#).

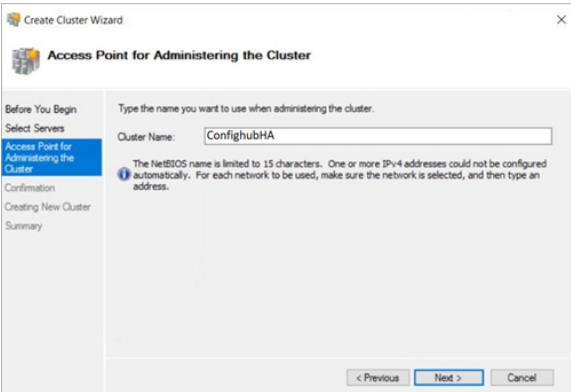
4. Complete **Validate a Configuration Wizard** with these options:

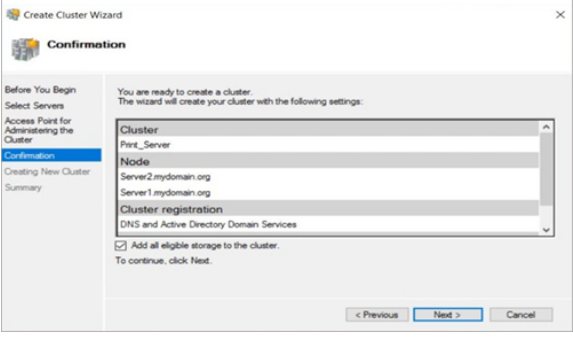

Section	What To Do
Before You Begin	Skip to the next section.
Select Servers or a Cluster	<p>Browse and locate the nodes you want to add to the cluster.</p> <p>For example, <code>confighubnode1.cluster.ge.com</code> and <code>confighubnode2.cluster.ge.com</code></p> <p>For resolving server related issues, see Troubleshooting (on page 55).</p>
Testing Options	Select Run all tests (recommended) .
Confirmation	Review the list of tests run on the selected servers. The number of tests run are based on the roles installed on the server nodes.
Validating	This process may take several minutes depending on your network infrastructure, and the number of server nodes selected for validation.

Section	What To Do
Summary	<p>a. Select View Report.</p> <p>b. Review Failover Cluster Validation Report and fix any failed validations. You can ignore expected warnings. The validation report should be free of any errors, otherwise the cluster setup will not be successful.</p> <p>c. Select Finish.</p>

5. In Failover Cluster Manager, select **Create a Cluster**.

6. Complete **Create Cluster Wizard** using these options:

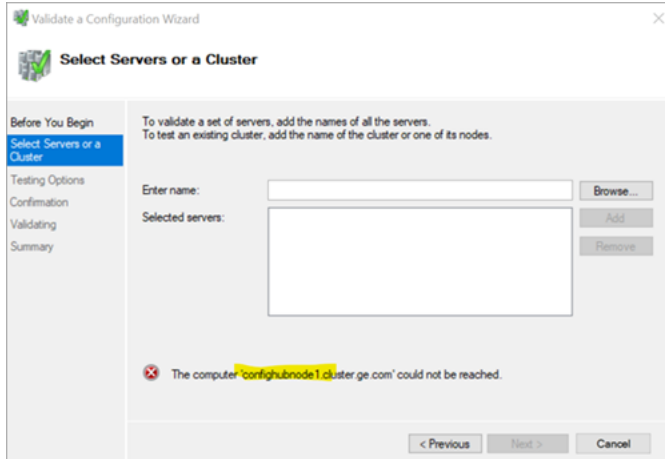
Section	What To Do
Before You Begin	Skip to the next section.
Select Servers	Nodes were already added during validating the configuration process. Skip to the next section.
Validation Warning	Select No . We already validated the nodes in the previous steps.
Access Point for Administering the Cluster	<p>Enter a unique name for your cluster.</p> 
Confirmation	<p>This screen lists the settings to be applied to your new cluster. Select the check box for Add all eligible storage to the cluster. The system will now try to assign any storage it can find.</p>

Section	What To Do
	
<p>Creating New Cluster</p>	<p>This process may take a while as there are several checks that must be run, and tests that are conducted while the system is configured.</p> <div data-bbox="605 745 1419 1134" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note:</p> <p>You may receive node cleanup failed errors at this stage (not detected during validation stage). Run the following command in all the cluster nodes, and then attempt to create the cluster. You need to execute this command in the administrative mode of Windows power shell.</p> <pre style="background-color: #FFF9E6; padding: 5px; margin-top: 10px;">> Clear-ClusterNode -Name confihubnode1.cluster.ge.com -Force</pre> </div>
<p>Summary</p>	<p>When the process is complete, select Finish.</p>

After completing the steps in this topic, a new cluster is created in your network domain.

To verify that the cluster is configured correctly, navigate to **Nodes** in the Failover Cluster Manager. Check that all nodes in the cluster are online. If they are not, go to the server that is offline, and bring the system online to join the cluster.

Troubleshooting Errors:



While adding the cluster nodes, if you get the above error, you need to do the following and attempt to add the clusters again:

- Disable the firewall on both the nodes.
- Add DNS name in the `hosts.conf` file.

```
# localhost name resolution is handled within DNS itself.
#          ::ffff:0:0:0:0:0:0:0:1   localhost
#          ::1                   localhost
#          htclab.ge.com
#          htclab.ge.com
#          confighubnode1.cluster.ge.com
#          confighubcluster
```

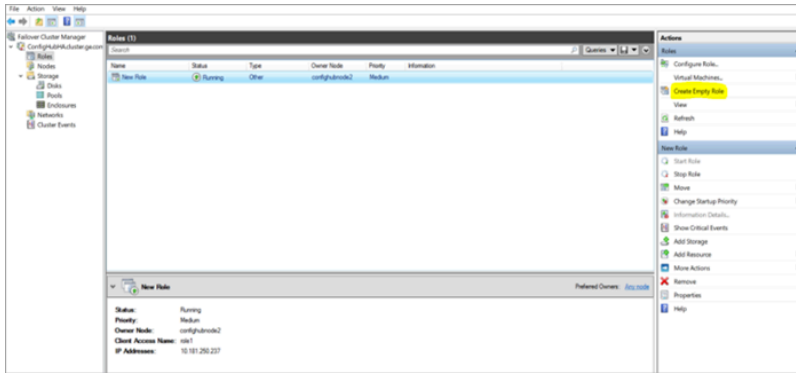
[Create Role \(on page 58\)](#)

Create Role

This topic describes how to create a role.

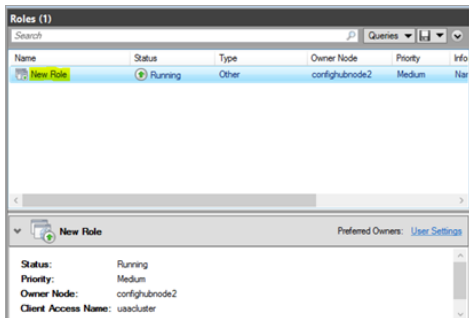
[Create Failover Cluster \(on page 55\)](#)

1. In Failover Cluster Manager, expand your cluster name and select **Roles**.
2. Right-click **Roles** and select **Create Empty Role**, (or) select under **Actions** as shown here:



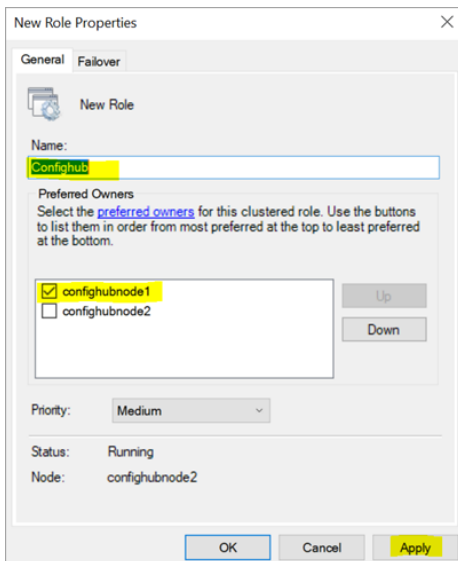
An empty role is created with primary node pointing to the active cluster node. The newly created empty role appears in the Roles pane with the name `New Role`.

3. Right-click `New Role` and select **Properties**.



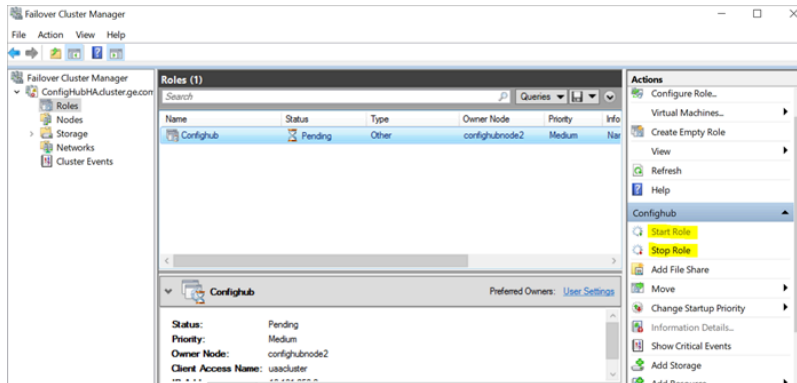
The **New Role Properties** screen appears.

4. Enter a valid name, and select the primary node to access the application, and then apply the changes.



After completing the steps in this topic, the newly created empty role is renamed.

If the role is in offline mode, you can manually start this role using the failover cluster. Use the options **Start Role** and **Stop Role** to start or stop the cluster roles.



See also [Move Role \(on page 60\)](#).

[Create Client Access Point \(Virtual IP\) \(on page 60\)](#)

Move Role

This topic describes how to move a role from one node to another.

[Create Role \(on page 58\)](#)

When you shut down a server node in a cluster, the role automatically moves to the next available node. You can also move the role manually (without shutting down the current node) to another node with these steps.

1. In Failover Cluster Manager, select the (renamed) empty role, and from the right pane, select **Move**. The **Move Clustered Role** screen appears.
2. Select the node to which you want to move the role and select **OK**.
The cluster now points to the selected node and serve the results from selected node

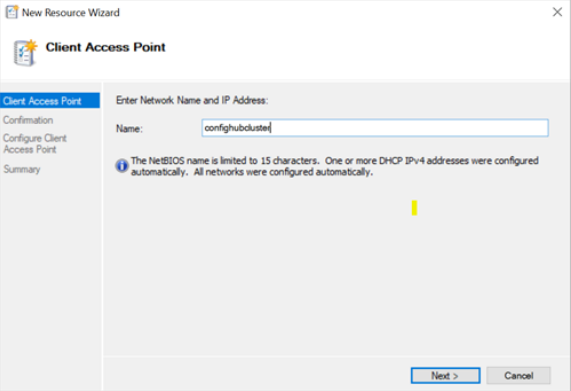
Create Client Access Point (Virtual IP)

This topic describes how to create a client access point.

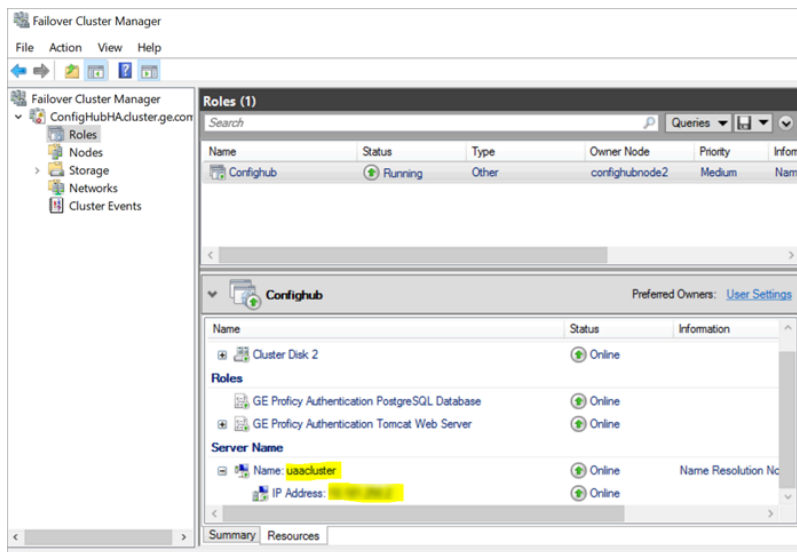
[Create Role \(on page 58\)](#)

The client access point is a virtual IP address and a corresponding DNS name that allows to access the Configuration Hub application.

1. In Failover Cluster Manager, right-click the (renamed) empty role and select **Add Resource > Client Access Point**.
2. Complete **New Resource Wizard** with the following options.

Section	What To Do
Client Access Point	Enter a name. This name (DNS) will be used to access the Configuration Hub application. 
Confirmation	The network name and IP address are displayed for confirmation.
Configure Client Access Point	Verifies the validity of the client access point settings and creates a new resource.
Summary	Select Finish .

After completing the steps in this topic, a virtual IP address is created to access the application.



[Add Dependencies to Role \(on page 62\)](#)


Add Dependencies to Role

This topic describes how to add dependency services to a role.

[Create Client Access Point \(Virtual IP\) \(on page 60\)](#)

On adding dependency services to a role, services restart whenever the role is switched to a different node (failover condition).

1. In Failover Cluster Manager, right-click the (renamed) empty role and select **Add Resource > Generic Service**.
2. Complete **New Resource Wizard** with the following system options:

Section	What To Do
Select Service	In the services list, select the dependency service to add to the role. 
Confirmation	Skip to the next section.
Configure Generic Service	Skip to the next section.
Summary	Select Finish .



Note:

Windows failover cluster starts the generic services in whichever node is currently active. It stops these generic services on all other nodes. When you switch the cluster nodes, then automatically Windows failover cluster starts the services in the new active node, and stops in all other nodes.

After completing the steps in this topic, dependency services are added to the role. See also [Move Role \(on page 60\)](#).

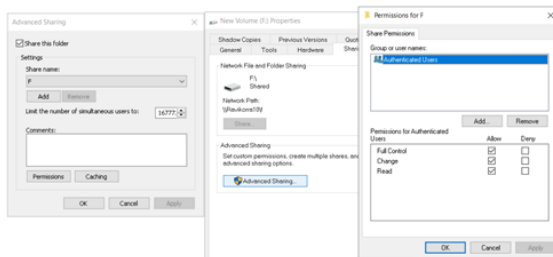
[Create Network Attached Storage \(on page 63\)](#)

Create Network Attached Storage

This topic describes how to create a Network Attached Storage (NAS).

Log in to the Node3 Windows server machine.

1. Create a shared folder on Node3.
2. To make the shared folder a central storage location, give full permission to the drive.
 - a. Right-click the drive and select **Give access to > Advanced sharing....**
The **Properties** dialog appears.
 - b. Select **Advanced Sharing....**
The **Advanced Sharing** dialog appears.
 - c. Select the check box for **Share this folder**, and then select **Permissions**.
The permissions dialog for the drive appears.
 - d. Select the group/user, and then select the check box for **Full Control**.



During Configuration Hub installation, we will select this drive to store common data across the nodes in a cluster.

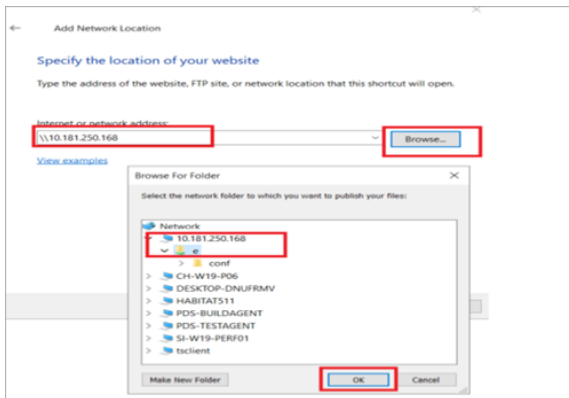
3. Add cluster nodes IP address and FQDN in the shared VM `hosts.conf` file. Also add shared VM IP address and FQDN to the hosts file.

```

hosts - Notepad
File Edit Format View Help
Copyright (c) 1993-2009 Microsoft Corp.
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       192.168.1.100    rhino.acme.com    # source server
#       192.168.1.101    x.acme.com      # x client host
#
# localhost name resolution is handled within DNS itself.
#
#       ::1             localhost
#       fe80::          localhost
#
10.181.250.100    ravigorral0
10.181.250.101    confighubnode2.cluster-ge.com
10.181.250.102    confighubnode2
10.181.250.103    confighubnode1.cluster-ge.com
10.181.250.104    confighubnode1
10.181.250.105    htclab.ge.com
10.181.250.106    htclab.ge.com
10.181.250.107    ravigorral1.htclab.ge.com
10.181.250.108    :confighubha1.cluster-ge.com
    
```

4. Log in to Node1 and Node2 servers and attach the shared drive.

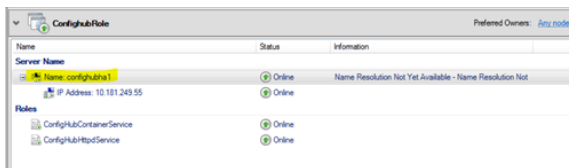
Here we can give either the IP address or FQDN to access the shared drive.



5. Access the Configuration Hub application using the virtual IP address.

In the following example screenshot, Configuration Hub cluster virtual IP address is DNS name.

FQDN: `confighubha1.cluster-ge.com`



You can either access with virtual IP address or domain name.

For example, access the Configuration Hub application with `https://confighubha1.cluster-ge.com:5200/` from any network.

Install Configuration Hub on Cluster Nodes

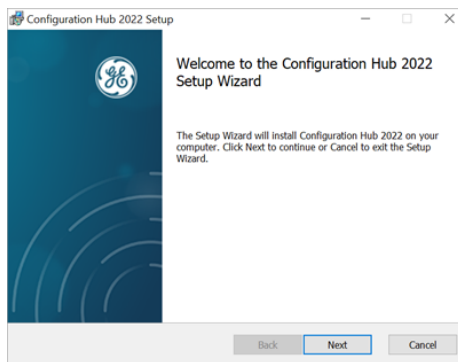
This topic describes how to install Configuration Hub in a high available environment.

Log in to a cluster node.

Follow these steps to install Configuration Hub on all the cluster nodes. You can access the application using the virtual IP address.

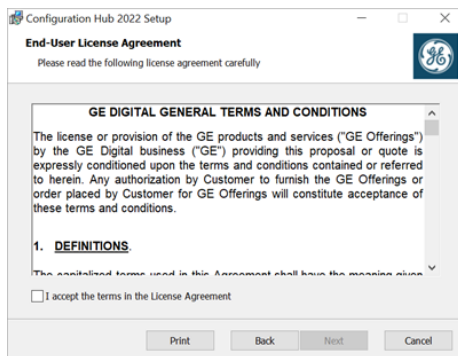
1. Run the Configuration Hub installation setup.

The welcome screen appears.



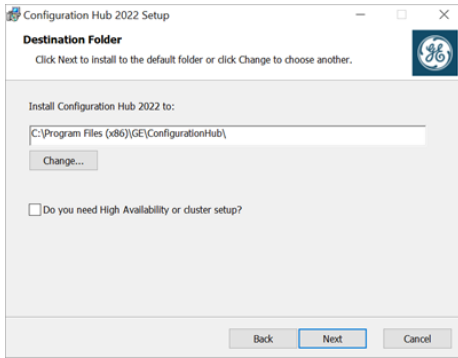
2. Select **Next**.

The license agreement screen appears.



3. Select the check box for **I accept the terms in the License Agreement**, and then select **Next**.

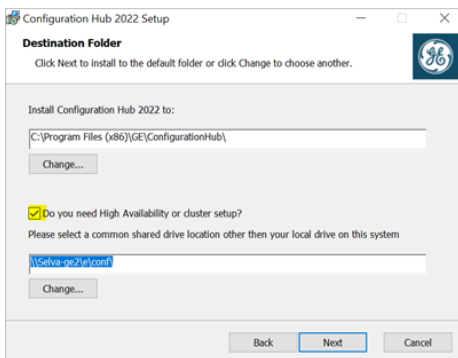
The destination folder selection screen appears.



4. Complete the following and select **Next**.

Field Name	What to do
Install Configuration Hub <version> to:	Proceed with the default install location, (or) select Change... to specify a different location path for installation.
Do you need High Availability or cluster setup?	Select the check box.

Options to set destination folder for shared configuration appears.



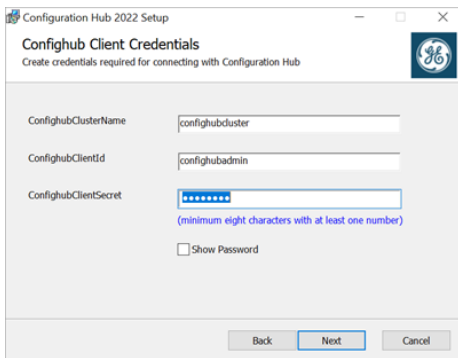
5. Enter the mapped shared network folder path, and then click **Next**.

The application client credentials screen appears.

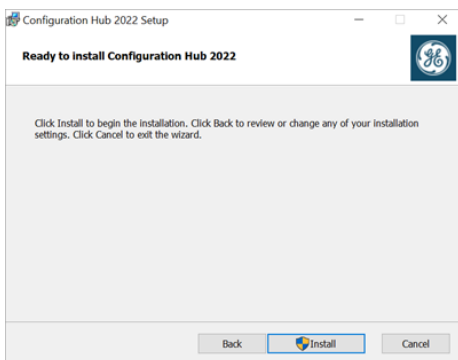
6. Complete the following and select **Next**.

Field Name	What to do
ConfighubClusterName	Enter the cluster name created for high availability.
ConfighubClientId	Enter the client ID to log in to the Configuration Hub application.

Field Name	What to do
ConfighubClientSecret	Enter the secret password to authenticate the client for logging in to the Configuration Hub application.



7. Select **Install**.



All binaries are installed on to the selected node. The shared configurations are installed on to the shared configuration path. Configuration Hub application shortcuts are created on all the cluster nodes using the virtual DNS name.

Handling Silent Installation

This topic describes how to perform a silent install of Configuration Hub in a high available environment.

These are the prerequisites for an HA silent install:

1. All the cluster VMs should have Windows server with any version.
2. Windows Failover cluster is setup on all the cluster nodes.
3. Provide a full access to shared drive on any other VM, and mount that drive in all cluster nodes manually as per the network attached storage drive setup.

4. Create a client access point under Windows failover cluster role. Use this as the cluster name or virtual DNS name to access to the Configuration Hub application. Give the same name for silent install command parameter.
5. Provide the port for the Configuration Hub web server.

You need to run the command on all the cluster nodes.

1. Open Windows command prompt as an administrator.
2. Run the following command for fresh installs of Configuration Hub:

```
ConfigHubInstaller.msi /quiet WIXUI_CHB_CLIENTSECRET=admin123 ISINSTALLHASHAREDRESOURCE=1
WIXUI_CHB_CLUSTERNAME=confighubcluster SHAREDCONFINSTALLFOLDER="\\Selva-ge2\e\conf"
```

These are the required command parameters for silent installation in high availability:



Note:

To achieve Configuration Hub high availability, the following parameter values must match on all the nodes.

Parameter	Description
<code>ISINSTALLHASHAREDRESOURCE=1</code>	Check box value to select Configuration Hub run on HA environment.
<code>WIXUI_CHB_CLUSTERNAME=confighubcluster</code>	Enter the name of your Windows failover cluster.
<code>SHAREDCONFINSTALLFOLDER="\\Selva-ge2\e\conf"</code>	Enter the shared configuration path, which contains Configuration Hub authentication and reverse proxy configuration. This configuration is shared by all cluster nodes and used when switching the nodes.

These are optional command parameters:

- `WIXUI_CHBHTTPD_PORT = 5000`
- `WIXUI_CHBCON_PORT = 4890`
- `WIXUI_CHB_CLIENTSECRET = " "`
- `WIXUI_CHB_CLIENTID = "confighubadmin"`
- `INSTALLFOLDER = "C:\Program Files (x86)\Proficy\ConfigurationHub"`

3. After installing Configuration Hub on all the cluster nodes, do the following:

- a. Add Configuration Hub services like `ConfigHubHttpdService` and `ConfigHubContainerService` to Windows failover cluster nodes.

These services will restart whenever nodes are switched in Windows failover cluster.

- b. Perform a setup authentication on any node (in a cluster).

Once the authentication is set up on one node, it automatically applies to all the cluster nodes since they share the configuration.

Any plug-in registered on the primary node will also load on other stand by nodes as well.

Chapter 2. Proficy Authentication

About Proficy Authentication

Proficy Authentication (UAA) provides identity-based security for Proficy based applications and APIs. It supports open standards for authentication and authorization, including OAuth2. You can configure Proficy Authentication from Configuration Hub.

When a user is created or deleted in a product that uses Proficy Authentication, the associated user account is created or deleted in the Proficy Authentication instance, respectively.

Several Proficy products use Proficy Authentication, including Historian, Plant Applications, and Operations Hub. To use Proficy Authentication, you must install one of these products. Each product can install an independent instance of Proficy Authentication, or it can reuse an existing instance of Proficy Authentication which was previously installed by another Proficy product. When more than one product uses the same instance of Proficy Authentication, this is called a shared or common Proficy Authentication.


Shared Proficy Authentication (UAA) means that if you have a Proficy product installed that uses Proficy Authentication, additional Proficy products installed after that initial product can also share that existing, already configured Proficy Authentication architecture.

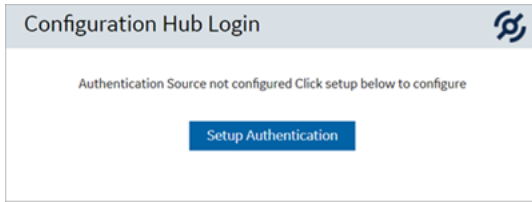
Proficy Authentication can additionally be configured to use an external identity provider. This includes identity providers which use Lightweight Directory Access Protocol (LDAP) or Security Assertion Markup Language (SAML). When you integrate Proficy Authentication with an external identity provider, you can provide the users and groups from that identity provider with access to Proficy products and their features.

Set up Proficy Authentication

This topic describes how to set up Proficy Authentication in Configuration Hub.

The following steps describe how to set up Proficy Authentication in Configuration Hub. Setting up authentication provides access to all the products (Historian, iFIX) registered with Configuration Hub. You use the same Proficy Authentication server to authenticate.

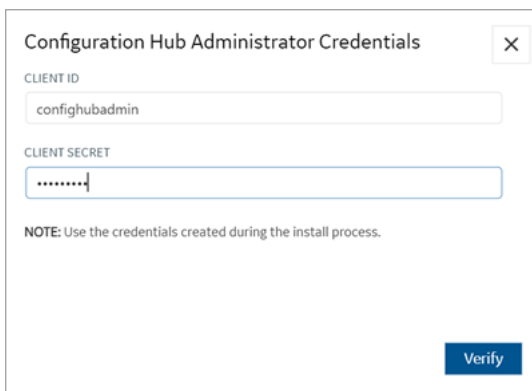
1. Double-click  desktop icon to launch the Configuration Hub application.
2. Select **Setup Authentication**.



The **Configuration Hub Administrator Credentials** screen appears.

3. Enter the details for logging in to the Configuration Hub application.

Field	Description
Client ID	The client ID provided during installing Configuration Hub. Example: <code>confighubadmin</code>
Client Secret	The client secret provided during installing Configuration Hub.



4. Select **Verify**.

If the credentials are correct, the **Register with Proficy Authentication** screen appears.

5. Provide these details to configure the Proficy Authentication application.

These fields are populated automatically if you opted for installing Proficy Authentication along with Configuration Hub. You have the option to edit and update the details.

Field	Description
Server Name (Fully Qualified Name)	The host name of the machine where Proficy Authentication is installed. Enter a fully qualified domain name. For example, <code>desktop-sahfg5f.logon.ds.ge.com</code>

Field	Description
	Refer to step 6 to establish a trust with this server connection.
Server Port	<p>The port number to communicate with the host machine. The default port where UAA is installed is 443.</p> <p>The server connection is automatically tested on entering the port. You can also select Test to test the connection.</p>
Use Configuration Hub Administration credentials for Proficy Authentication	<p>Select this check box to populate the same login credentials you entered for Configuration Hub Admin account.</p> <p>If you want to use unique login credentials for Proficy Authentication, clear the check box and enter CLIENT ID and CLIENT SECRET.</p>
Proficy Authentication Client ID	The administrator client identifier that has permission (authority) to log in to Proficy Authentication.
Proficy Authentication Client Secret	The administrator client secret to log in to Proficy Authentication.

Register with Proficy Authentication ✕

SERVER NAME (FULLY QUALIFIED NAME)
 Not trusted

SERVER PORT

Proficy Authentication Credentials

Use Configuration Hub Administration credentials for Proficy Authentication

CLIENT ID

CLIENT SECRET

NOTE: Use the credentials created during the install process.

6. Select **Not trusted** to establish a trust connection between Configuration Hub and Proficy Authentication.

The **Certificate Details** screen appears.


Certificate Details

Attribute Name	Root Certificate
Subject	CN=SACHINAUTHGUARD Root CA 202112241544, OU=Operations Hub Site, O=GE Customer
Thumbprint	0B8B85FDA172C1DCF7A6C48F127085EF1338119C
Serial Number	3F678CC3732C8A69
Issuer	CN=SACHINAUTHGUARD Root CA 202112241544, OU=Operations Hub Site, O=GE Customer
Valid From	2021-12-24 00:00:00 GMT
Valid To	2026-12-23 00:00:00 GMT

7. Select **Trust**.

The trusted certificate(s) are added to the windows store on the machine where Configuration Hub is installed.

Register with Proficy Authentication

SERVER NAME (FULLY QUALIFIED NAME)
sachinauthguardianvm01.htclab.ge.com 

SERVER PORT
443

Test Server Connection

Proficy Authentication Credentials

Use Configuration Hub Administration credentials for Proficy Authentication

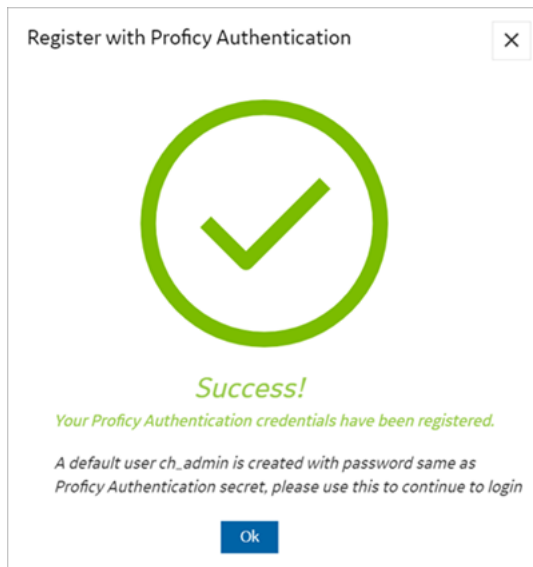
CLIENT ID
confighubadmin

CLIENT SECRET

NOTE: Use the credentials created during the install process.

Register

8. Select **Register**.



9. Select **Ok**.

The **Configuration Hub Login** screen appears.

Configuration Hub is set up as a client for Proficy Authentication. The following default user is created to log in to the Configuration Hub application.

User ID	Password
ch_admin	The client secret you entered for Proficy Authentication.

Log in to Configuration Hub and perform operations related to Proficy Authentication.

Navigation in Proficy Authentication


Proficy Authentication provides identity-based security for Proficy based applications and APIs.

You can perform the following tasks in Proficy Authentication:

- Configure UAA/LDAP/SAML identity providers
- Create new user accounts
- Create new group accounts and add users/other groups as members
- Perform UAA/LDAP/SAML group mapping



Displaying Data Columns

You can show or hide columns within the Proficy Authentication application.

1. Select  for the respective data. The **Column Chooser** dialog appears with a list of available columns.
2. Select the check box for the column you want to show. To hide a column, clear its check box.
3. Close the dialog to apply the changes.


Sorting Data

The sorting option appears when you select a data column.

- Select  to sort data in an ascending order.
- Select  to sort data in a descending order.

Filtering Data

The filtering option appears next to each data column.

1. Select  for the data you want to filter. A screen appears with a list of existing data in that column.
2. Select the check box for the data you want to filter. To undo filtering, you can **Select All**.
3. Select **OK** to apply.

Searching Data

Use the search option to search for existing accounts in Proficy Authentication. You can also filter account details using search keywords.


Manage Identity Providers

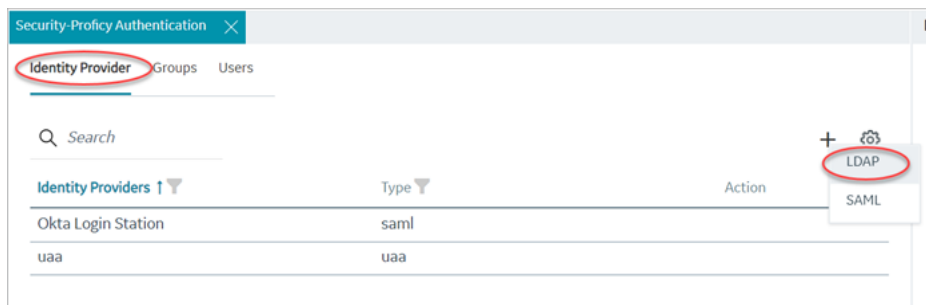
Add LDAP Identity Provider

This topic describes how to add a LDAP account in Proficy Authentication.

Log in to Configuration Hub with user/client having write access for admin and clients.

You can add multiple LDAP connections.

1. Go to **Proficy Authentication > Security > Identity Provider**.
2. Select  and then select **LDAP**.



The **LDAP Identity Provider** screen appears.

3. Enter the following details:

Field	Description
Name	A unique name to help identify your LDAP connection.
URL	The URL of the LDAP server. The trailing slash (/) must be included at the end of the URL.

Field	Description
	<p>You can use LDAP with or without secure authentication in the following format:</p> <ul style="list-style-type: none"> ◦ Insecure port: <code>ldap://100.100.100.2:389/</code> ◦ Secure port: <code>ldaps://100.100.100.2:636/</code> <p>You can also use a fully qualified domain name instead of an IP address.</p> <p>For a secure port, provide user credentials.</p>
Bind User Distinguished Name	<p>Distinguished LDAP user name.</p> <p>Describes the part of the hierarchy the user belongs to on the active directory network. CN=Common Name. DC=Domain Component. OU= Organization Unit Name.</p> <p>CN and DC are typically required, while OU is optional.</p> <p>Example: <code>CN=John Smith,OU=Factory,DC=Company,DC=COM</code></p>
Password	<p>The password to log in to the LDAP server if you choose secure authentication.</p>
Test	<p>Tests the connection to the LDAP server. If the URL and login details are correct, you will receive a test successful message.</p>
Skip SSL Verification	<p>This option appears only when you choose a secure port for LDAP.</p> <p>Select this check box if you want to skip establishing a secure connection between client and server for exchanging LDAP data.</p> <p>Clear the check box to allow SSL verification. Refer to step 4.</p>

LDAP Identity Provider

Name*
DSFREE50KFORUM

URL*
ldap://10.181.215.2:389/

Bind User Distinguished Name *
CN=spcuser1,CN=Users,DC=pa,DC=com

Password *

4. If you choose to secure LDAP, select for SSL verification.
A message appears when the security certificate is trusted and added to the store.

In case the certificate is not added automatically, the following message appears.

Certificate cannot be retrieved
Please use the browse button below to select the server certificate

Select **Browse** to navigate and choose the server certificate from your local system.

5. **Optional:** Select next to the lock icon to view the certificate.

certAttributeName	Root Certificate
certSubject	CN = CWARIRSSVR2K19.pa.com
certThumbprint	4723FC64421BB6A13846CBF5A65EE812B5602A7E
certSerialNumber	5800000002F700D88850581AFD000000000002
certIssuer	DC = com.pa CN = CWARIRSSVR2K19.pa.com
certValidFrom	Jun 21 18:28:08 2021 GMT
certValidTo	Jun 21 18:28:08 2022 GMT

6. Select **Save**.

The LDAP identity provider is created.

Enable SAML

This topic describes how to configure SAML identity providers for Proficy Authentication.

You should enable SAML prior to [adding SAML IDP accounts \(on page 88\)](#) in Proficy Authentication.

To enable SAML, you will need to download the Proficy Authentication service provider's metadata file.

1. Visit `https://enter FQDN of the machine where Proficy Authentication is installed/uaa/saml/metadata` to download the `saml-sp.xml` file.
2. To configure any SAML identity provider, gather information from the downloaded `saml-sp.xml` file.
3. Generate a metadata XML file from the configured identity providers, and use the file to [add a SAML IDP account \(on page 88\)](#) in Proficy Authentication.

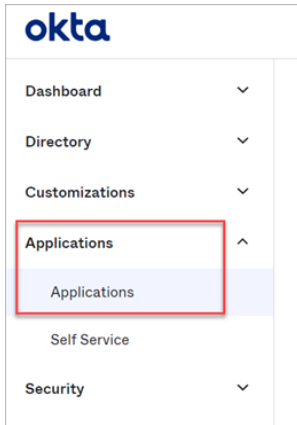
Refer to the following examples on how to set up SAML identity providers for Proficy Authentication:

- [Configure Okta as SAML IDP \(on page 79\)](#)
- [Configure Azure AD as SAML IDP \(on page 83\)](#)

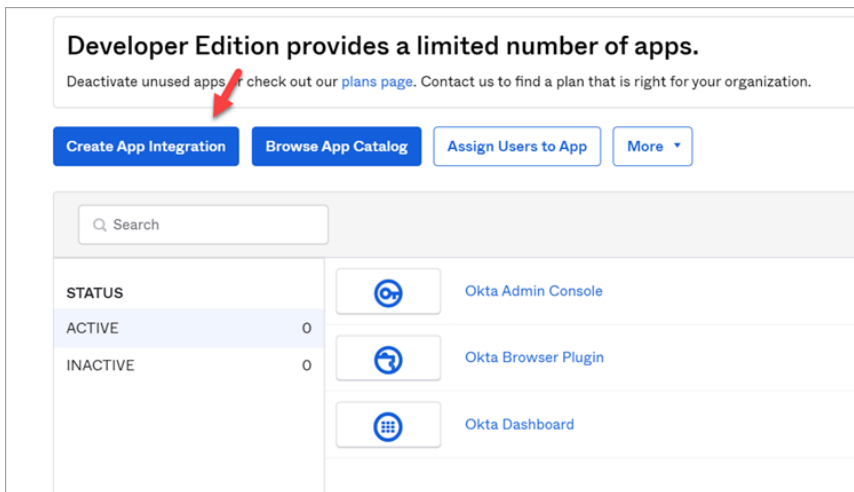
Configure Okta as SAML IDP

This topic describes SAML configuration with Okta.

1. Create an account in Okta.
 - a. Visit <https://developer.okta.com/>.
 - b. Sign up for an Okta account using your email address.
2. Log in to your newly created Okta account.
3. Navigate to **Applications > Applications**.

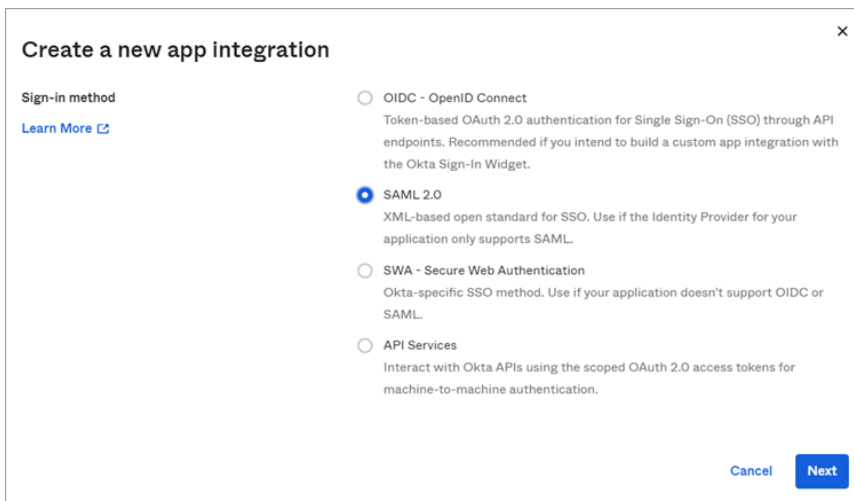


4. Select **Create App Integration**.



The **Create a new app Integration** screen appears.

5. Select **SAML 2.0**, then select **Next**.



The **Create SAML Integration** screen appears.

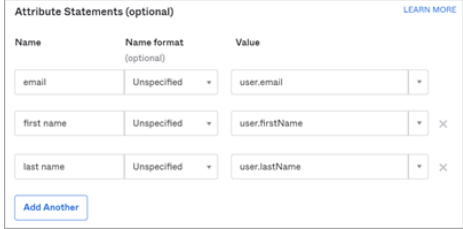
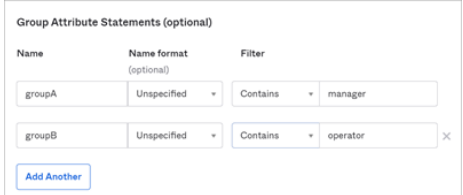
6. Under **General Settings**, provide a name and logo for your application, then select **Next**.


The screenshot shows a two-step process. Step 1, 'General Settings', is active. It contains the following elements:

- App name:** A text input field containing 'Multiverse Paradigm'.
- App logo (optional):** A large image placeholder containing the GE logo. To the right of the image are two small icons: an upload icon and a trash icon.
- App visibility:** A checkbox labeled 'Do not display application icon to users', which is currently unchecked.
- Navigation:** A blue 'Next' button is located at the bottom right, and a blue 'Cancel' link is at the bottom left.

7. Under **Configure SAML**, fill out these details:

<p>Single sign on URL</p>	<p>Use the downloaded Proficy Authentication metadata file (on page 79) <code>saml-sp.xml</code> to get the URL for this field. It should look something like this:</p> <pre><md:AssertionConsumerService Location="https://ghldz593e.logon.ds.ge.com/uaa/saml/SSO/alias/ophubSamlSp" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" isDefault="true" index="0"/> <md:AssertionConsumerService Location="https://ghldz593e.logon.ds.ge.com/uaa/oauth/token/alias/ophubSamlSp" Binding="urn:oasis:names:tc:SAML:2.0:bindings:URI" index="1"/></pre>
<p>Audience URI (SP Entity ID)</p>	<p>Refer to <code>saml-sp.xml</code> to get the logout URL. It should look something like this:</p> <pre><?xml version="1.0" encoding="UTF-8"?> - <md:EntityDescriptor entityID="https://ghldz593e.logon.ds.ge.com/uaa/saml/metadata" ID="https://ghldz593e.logon.ds.ge.com/uaa_saml_metadata" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" > - <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" ></pre>
<p>Enable Single Logout</p>	<ol style="list-style-type: none"> Select Show Advanced Settings. Select the check box for Allow application to initiate Single Logout.

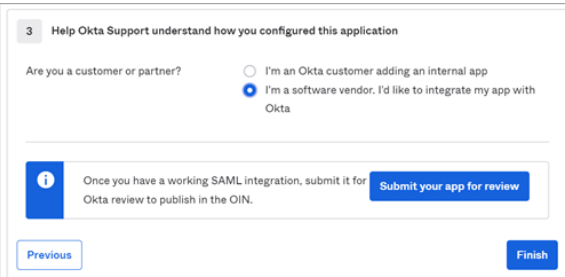
	<p>c. Enter Single Logout URL. Refer to <code>saml-sp.xml</code> to get the logout URL. It should look something like this:</p> <pre></md:KeyDescriptor> <md:SingleLogoutService Location = "https://ghldz593e.logon.ds.ge.com/uaa/saml/SingleLogout/alias/ophubSamlSp" Binding = "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/> <md:SingleLogoutService Location = "https://ghldz593e.logon.ds.ge.com/uaa/saml/SingleLogout/alias/ophubSamlSp" Binding = "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/></pre>
<p>Attribute Statements (optional)</p>	<p>Add user attribute statements such as email, first name, and last name as shown here:</p> 
<p>Group Attribute Statements (optional)</p>	<p>Add group attribute statements such as groupA and groupB as shown here:</p> 

 **Note:**

The setting option mentioned in this topic is the minimum requirement for setting up the SAML identity provider. Refer to the [Okta documentation](#) for information on using additional settings.

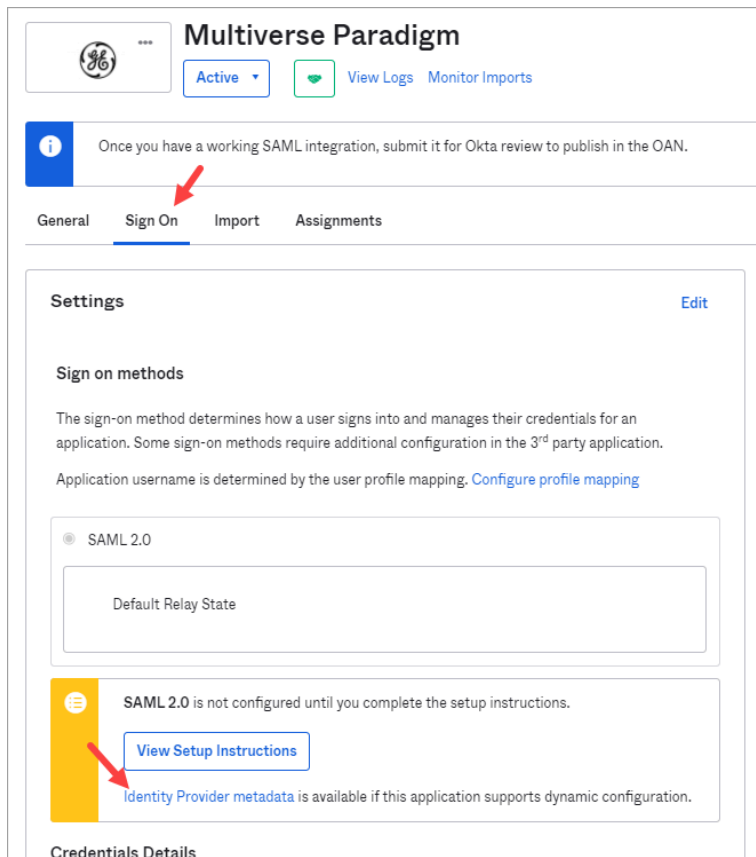
8. Select **Next**.

9. Provide your feedback and select **Finish**.



Your application is created.

10. Under **Sign On**, select **Identity Provider metadata**.



The metadata opens in a new tab.

11. Save the metadata as an .xml file.

Use the metadata xml file to [configure a SAML identity provider \(on page 88\)](#) in Proficy Authentication.

12. Under **Assignments**, you can assign the app to groups and individual users.

If there are no users/groups, navigate to **Directory > People** to create and activate new users/groups in Okta.

Configure Azure AD as SAML IDP

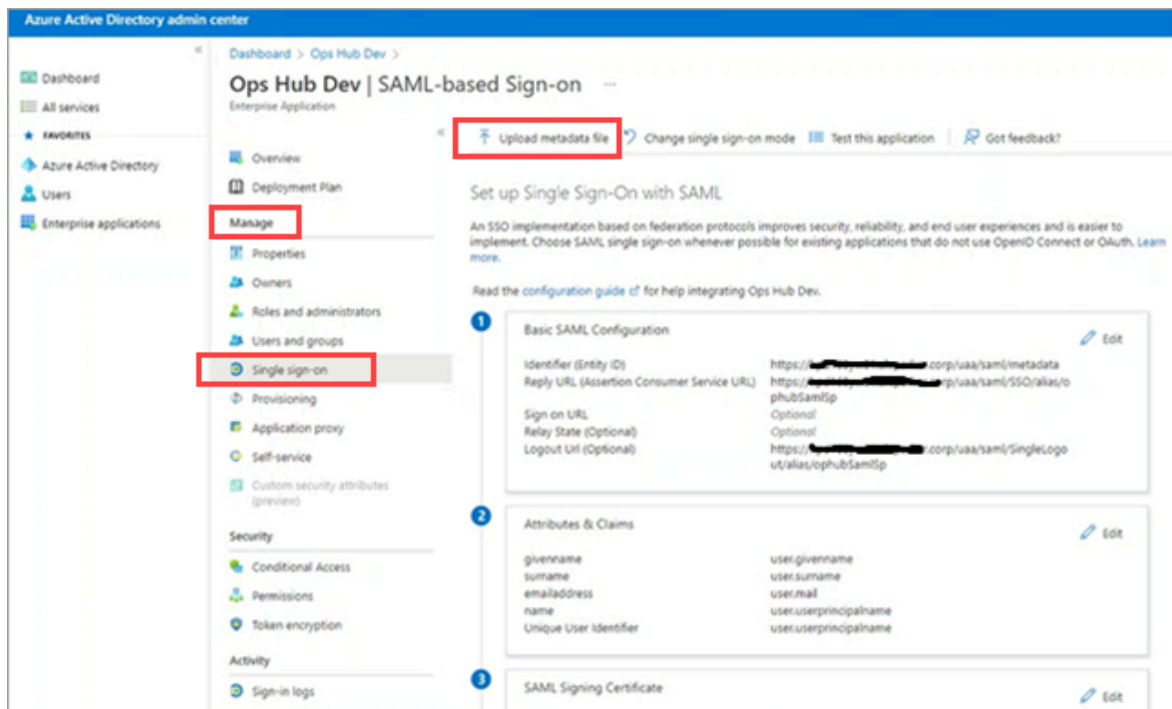
This topic describes SAML configuration with Azure AD (Active Directory).

1. Visit <https://azure.microsoft.com/en-us/free/> and create an account.
2. Add an enterprise application. For more information, refer to [Microsoft Azure documentation](#). `Ops Hub Dev` is the example enterprise application used in the procedural steps (refer to the figure in step 2).
3. Create at least one user and group.

The following steps include:

- Creating a SAML app in Azure (steps 1-5).
- Configuring Azure metadata xml in Proficy Authentication (steps 6-7).

1. Download Proficy Authentication `saml-sp.xml` metadata file. Refer to [Enable SAML \(on page 79\)](#) on how to download the file.
2. Sign in to the Azure portal, and upload `saml-sp.xml`.
 - a. From left menu, select **Manage > Single sign-on**.
 - b. Select **Upload metadata file**.

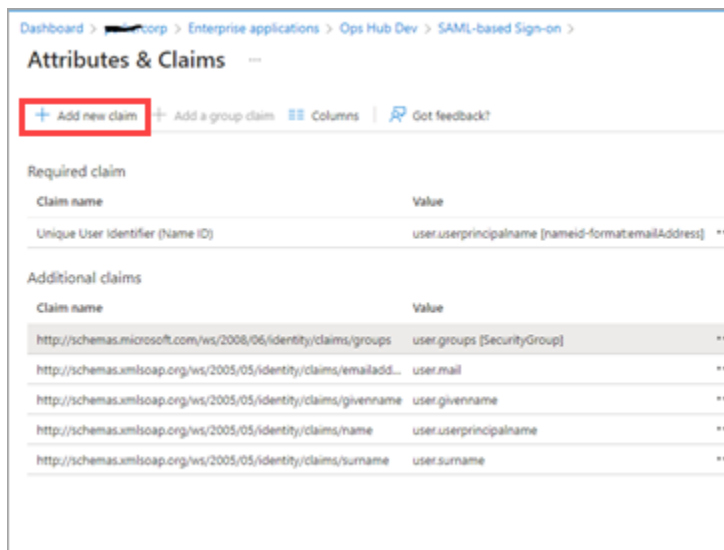


3. Perform user and group attribute mapping in Azure.

- a. Under the **User Attributes & Claims** section, select **Edit** and add claims.



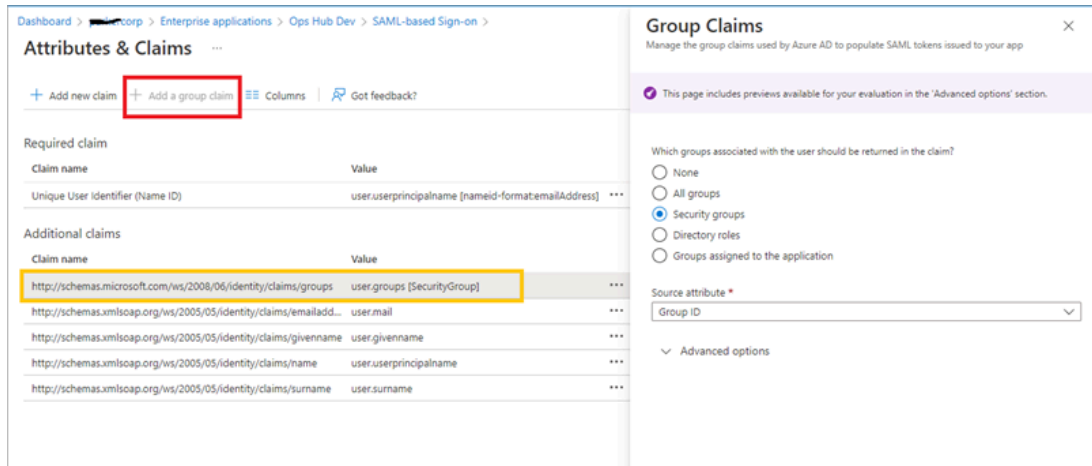
- b. Select **Add new claim** and save entered details to set up claims.



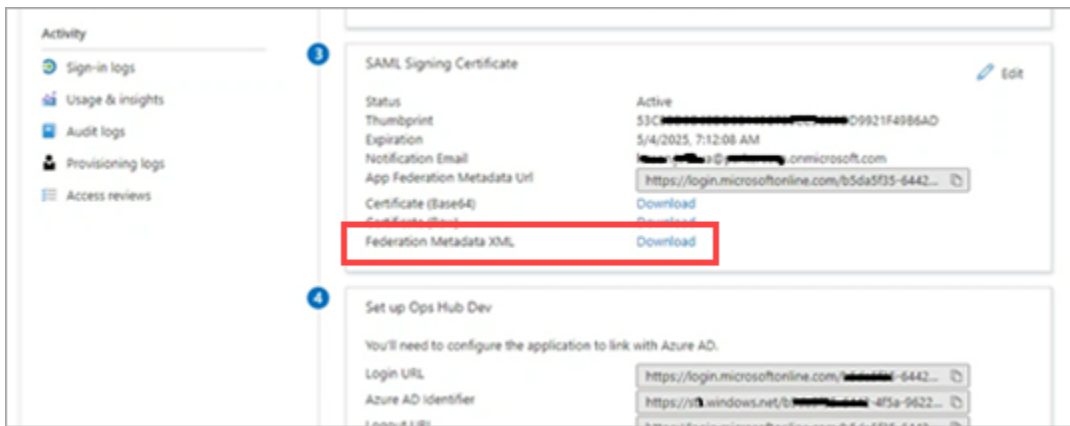
Note:

Make a note of the claim name value (for example `user.groups`). You need to provide this value in the **Attribute Name** field when adding a SAML identity provider in [step 6a \(on page 87\)](#).

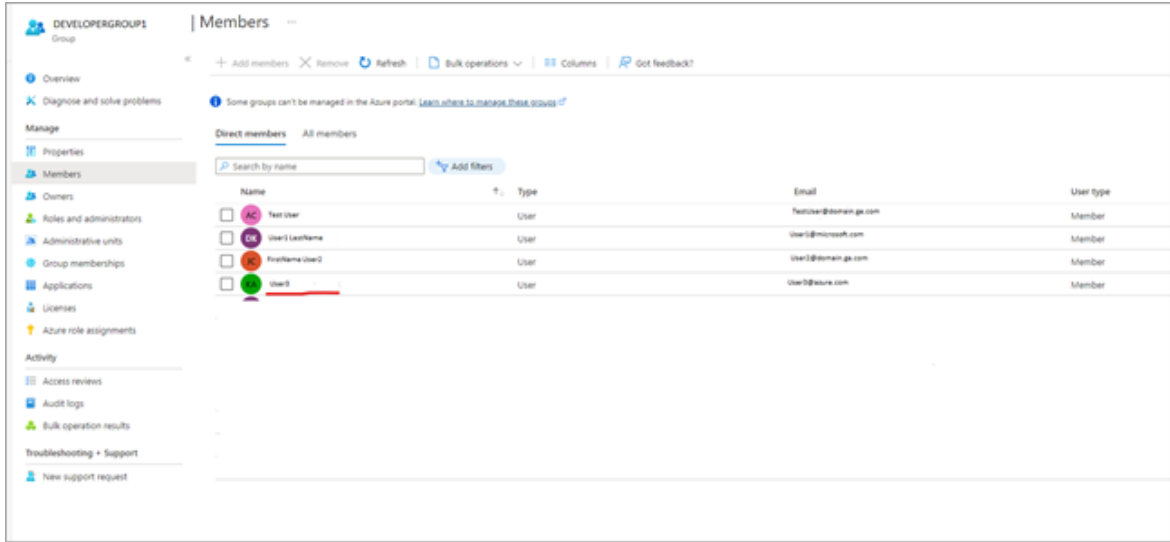
c. Select **Add a group claim** and set up group claims.



4. Under the **SAML Signing Certificate** section, download the **Federation Metadata XML** file.



5. Perform user group mapping in Azure.



6. Log in to Proficy Authentication and do the following:

a. Upload the **Federation Metadata XML** file downloaded from the Azure portal in [step 4 \(on page 86\)](#).

For step-by-step instructions, refer to [Add SAML Identity Provider \(on page 88\)](#).

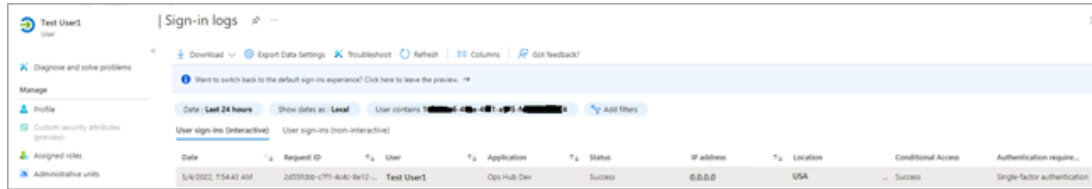
b. Add and map SAML groups.

For step-by-step instructions, refer to [Map Groups \(on page 99\)](#).

7. To test SAML authentication, visit Operations Hub login page, and select **Sign In With Azure**.



- You should login successfully. In Azure portal, you can access the logs to verify successful logins:

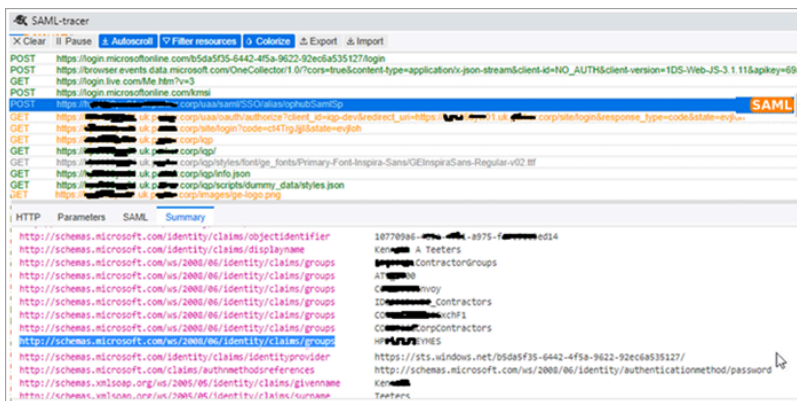


- If login access is denied, then verify the group attribute name and group name from SAML Azure (see troubleshooting below). Clear the cache and login again.

Troubleshooting: For troubleshooting, add [SAML-tracer](#) extension to Chrome.

1. Open SAML-tracer from your browser extensions.
2. Log in to Operations Hub to reproduce the SSO login issue.
3. In SAML-tracer, look for `POST` messages, and select the **Summary** tab.

In the following screenshot, incorrect SAML group attribute names were detected, and replaced with the correct ones to fix the login issue.



Add SAML Identity Provider

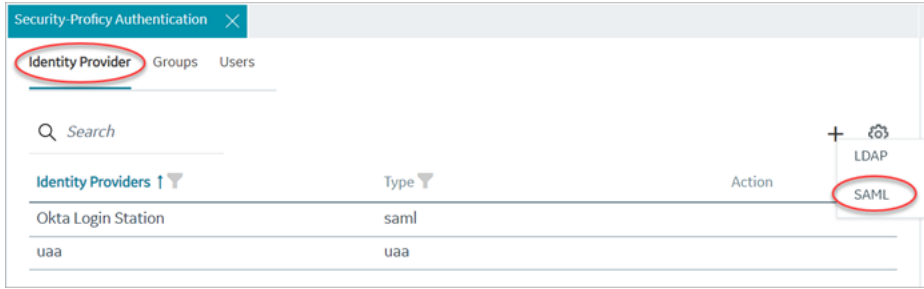
This topic describes how to add multiple SAML accounts in Proficy Authentication.

[Enable a SAML identity provider \(on page 79\)](#). For example, Okta or Azure AD or any other IDP.

You can add multiple SAML connections.

1. Log in to Configuration Hub as an administrator.
2. Go to **Proficy Authentication > Security > Identity Provider**.

3. Select **+**, then select **SAML**.



The **SAML Identity Provider** screen appears.

4. Enter the following details:



Note:

The XML file contains the metadata to interact with SAML enabled identity providers (Azure, ADFS, or Okta). Refer to [Configure Okta as SAML IDP \(on page 79\)](#).

Field	Description
Upload XML File	Choose this option if you want to upload an XML document. Select Upload XML File to browse and locate the XML document from your local system. The uploaded data appears in a text box, and is read-only.
Provide File Location	Choose this option if you want to provide an external URL to the XML document. Enter the URL in the text field, and select Load . The data from the URL appears in a text box, and is read-only.
Name	Name of the SAML identity provider. You can provide any name. For example, <code>okta_123</code> or <code>demo_mach_azure</code> .
Attribute Name	The attribute that contains the group membership information about a user in a SAML assertion.

Field	Description
Name ID	SAML Name identifier and associated fields that you want to use in a link test.
Enable SAML Link	Select the check box.

5. Select **Save**.

The SAML identity provider is created.

Enable Multi-Factor Authentication

This topic describes how to enable multi-factor authentication for users.

Install the [Google Authenticator](#) app on your mobile device.

Only administrators can enable multi-factor authentication (MFA) for users.

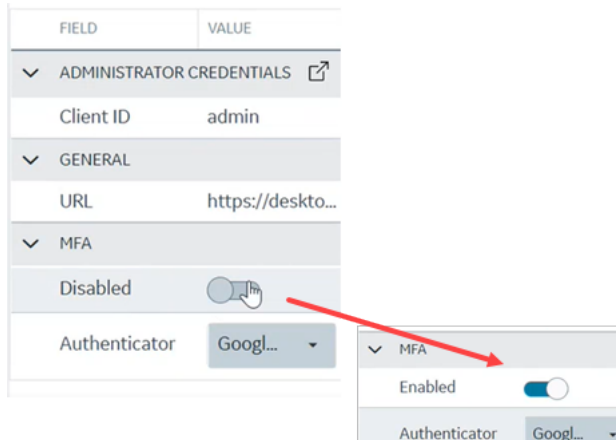


Note:

Enabling MFA also enables two-factor authentication for UAA and LDAP users as both the identity providers have a common login entry point.

1. Log in to Configuration Hub as an administrator.
2. Go to **Proficy Authentication > Security > Identity Provider**.
The existing list of identity providers appear.
3. Select the **UAA** record for which you want to enable the multi-factor authentication.
The option to enable MFA appears on the **DETAILS** panel under the **MFA** section.
4. Enable the toggle switch for MFA.

By default, MFA is disabled.



The multi-factor authentication for UAA is enabled.

5. Select **Authenticator**.

Currently, Google authenticator is the only available authenticator.

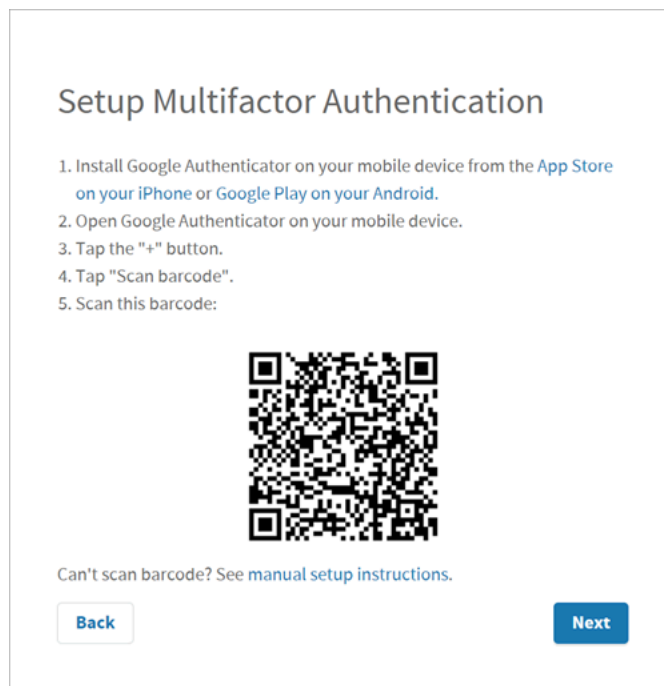
6. Restart the `GE Proficy Authentication Tomcat Web Server` service.

7. Activate multi-factor authentication for user logins.

You need to perform the following steps only for the first time for every user login.

a. Log in to Configuration Hub with UAA user credentials.

The MFA setup screen appears with a barcode.



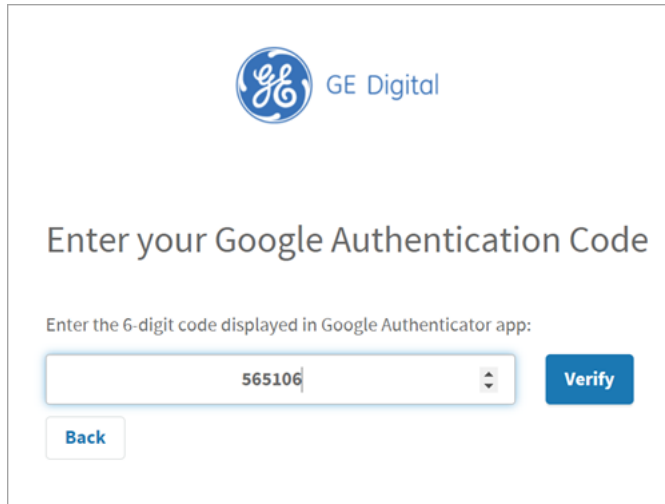
b. Open the Google Authenticator app on your mobile device and scan the barcode.

The authentication app validates the user login and displays a 6-digit code. Barcode scanning appears only for the first time validation for every user login.

c. On your browser, select **Next** on the MFA setup screen.

The code verification screen appears.

d. Enter the 6-digit code in the passcode field and select **Verify**



You are logged in successfully.

Multi-factor authentication is enabled for both UAA and LDAP users.

Modify LDAP Identity Provider

This topic describes how to modify the existing details for the LDAP account.

[Add LDAP Identity Provider \(on page 76\)](#)


1. Log in to Configuration Hub as an administrator.

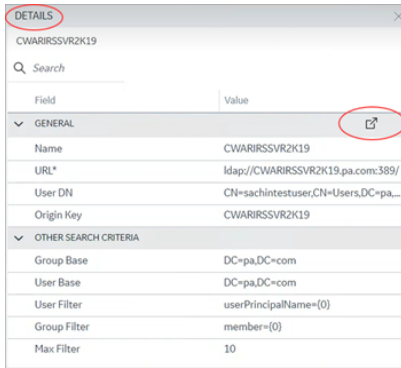
2. Go to **Proficiency Authentication > Security > Identity Provider**.

The existing list of identity providers appear.

3. Select the LDAP identity provider.

The existing information for the identity provider appears on the **DETAILS** panel.

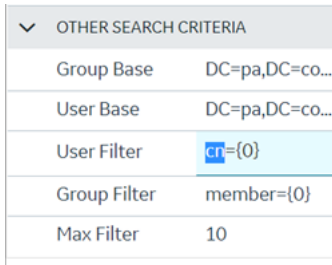
4. To modify the **GENERAL** details, select  to open a pop-up screen with the existing information.




5. If you modify any existing information, save the changes.


The general details are required to configure LDAP authentication.

6. To modify **OTHER SEARCH CRITERIA** details, place your cursor and enter the new value for the respective criteria.



Use these settings to enable the sub-directories in your search criteria.

Search Criteria	Example Value	Description
Group Base	OU=Sales,OU=Groups,OU=Enterprise,DC=company,DC=com	<p>Defines the starting point for the LDAP group search in the active directory tree.</p> <ul style="list-style-type: none"> ◦ CN is Common Name (required) ◦ DC is Domain Component (required) ◦ OU is Organization Unit Name (optional) <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note: If you use only <code>DC=Ge,DC=com</code>, timeout may occur due to slow system response. Use the exact <code>ou</code> to avoid timeout.</p> </div>

Search Criteria	Example Value	Description
User Base	<code>OU=Sales,OU=Users,OU=Enterprise,DC=company,DC=com</code>	<p>Defines the starting point for the LDAP group user search in the active directory tree.</p> <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p> Note: If you use only <code>DC=Ge,DC=com</code>, timeout may occur due to slow system response. Use the exact <code>ou</code> to avoid timeout.</p> </div>
User Filter	<code>userPrincipalName={0}</code>	Allows the LDAP user (active directory user) to login into Configuration Hub with their email address.
User Filter	<code>cn={0}</code>	Allows the LDAP user (active directory user) to login with their display name. This field is populated by default.
User Filter	<code>sAMAccountName={0}</code>	Allows the LDAP user (active directory user) to login with their account name (Windows login name). This field is populated by default.
Group Filter	<code>memberOf={0}</code>	Retrieves the <code>memberOf</code> attribute values for the specific user. This field is populated by default.
Max Filter	<code>10</code>	<p>Defines the maximum depth for searching the LDAP groups. The default value is <code>10</code>.</p> <p>For very large systems, set the value to <code>2</code> as it may impact system performance.</p>

Modify SAML Identity Provider

This topic describes how to modify the existing details for a SAML account.


[Add SAML Identity Provider \(on page 88\)](#)

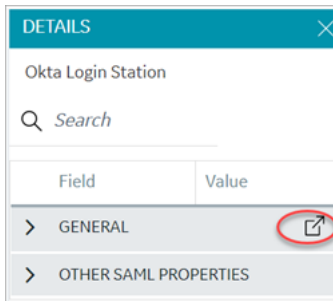
1. Log in to Configuration Hub as an administrator.
2. Go to **Proficy Authentication > Security > Identity Provider**.

The existing list of identity providers appear.

3. Select the SAML identity provider you want to modify.

The existing information for the identity provider appears on the **DETAILS** panel.

4. Select  to display the details in a pop-up screen.



The **SAML Identity Provider** screen appears.

5. You can modify the existing information and save the changes.
6. You can also modify items under **OTHER SAML PROPERTIES** section. Enter a new value to replace the existing value.

Delete Identity Provider

This topic describes how to delete identity providers.

[Add SAML Identity Provider \(on page 88\)](#)

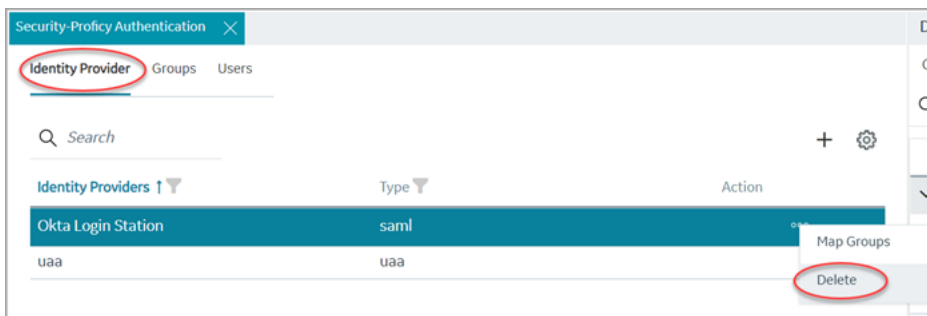
1. Log in to Configuration Hub as an administrator.
2. Go to **Proficy Authentication > Security > Identity Provider**.

The existing list of identity providers appear.

3. Select the identity provider you want to delete.

Additional options appear under the **ACTION** column.

4. Select , then **Delete**.



A message appears to confirm the delete action.

5. Select **Delete**.

The identity provider record is deleted from the Proficy Authentication database.

Manage Groups

Overview of iFIX Groups in Proficy Authentication

Proficy Authentication provides access to the following security groups for iFIX access:

`scada.fix.shared_IFIX_PROFICY_AUTH_ADMIN`, `scada.fix.shared.APPLICATION_DESIGNER`,
`scada.fix.shared.OPERATORS`, `scada.fix.shared.SUPERVISORS`, and `scada.proficy.admin`.

The following descriptions explain the access provided for iFIX groups in Proficy Authentication.

- `scada.fix.shared_IFIX_PROFICY_AUTH_ADMIN`: This group allows access to all iFIX application features. Any Proficy Authentication user who is a member of this group will have privileges similar to a native iFIX ADMIN user (except the access to security areas). Proficy Authentication users who want to directly log in to iFIX can use this group.

This group is not available by default when you upgrade from iFIX 6.1 or 6.5. You must manually create this group with all the iFIX application features as needed.

- `scada.fix.shared.APPLICATION_DESIGNER`: This group allows a user to access Configuration Hub and provides use of iFIX features such as iFIX connection, database, and model management.



Important:

Be aware that the `scada.fix.shared.APPLICATION_DESIGNER` group is not available by default when you upgrade from iFIX 6.1 or 6.5. You must manually create the group with the required iFIX application features, or update your existing groups to include the following iFIX application features (if you want users in these groups to have access to and use Configuration Hub).

- Database Block Add-Delete
- Database Manager
- Database Reload
- Database Save
- Security Configuration
- System Configuration

To create a new group or modify an existing group, use the iFIX Security Configuration application.

- `scada.fix.shared.OPERATORS`: This group provides run mode only access for a user in iFIX.
- `scada.fix.shared.SUPERVISORS`: This group provides access to WorkSpace run and configure mode, as well as access to background task exit, iFIX system shut down, and iFIX system user login.
- `scada.proficy.admin`: This group allows the Proficy Authentication user access to the iFIX Projects panel and to the Deploy operations from Configuration Hub. This group is for Proficy Authentication only; this group is not linked to any iFIX group and has no permissions in iFIX.

Overview of Historian Groups in Proficy Authentication

Proficy Authentication provides access to the following security groups for Historian access:

`historian_enterprise.admin`, `historian_enterprise.user`, `historian_rest_api.admin`, `historian_rest_api.read`, `historian_rest_api.write`, `historian_visualization.admin`, `historian_visualization.user`, `ih_archive_admins`, `ih_audited_writers`, `ih_collector_admins`, `ih_readers`, `ih_security_admins`, `ih_tag_admins`, `ih_unaudited_logins`, and `ih_unaudited_writers`.

The following descriptions explain the access provided for Historian groups in Proficy Authentication:

- `historian_enterprise.admin`: Provides read/write access to Configuration Hub APIs.
- `historian_enterprise.user`: Allows access to Configuration Hub APIs.
- `historian_rest_api.admin`: Provides read/write access to public REST API.
- `historian_rest_api.read`: Provides read access to public REST API.
- `historian_rest_api.write`: Provides write access to public REST API.
- `historian_visualization.admin`: Provides access to Trend Client and the Web Admin console.
- `historian_visualization.user`: Allows access to Trend Client.
- `ih_archive_admins`, `ih_audited_writers`, `ih_collector_admins`, `ih_readers`, `ih_security_admins`, `ih_tag_admins`, `ih_unaudited_logins`, `ih_unaudited_writers`: Provides access to tables for the Historian OLE DB provider.

Create Groups

This topic describes how to create new groups in Proficy Authentication.

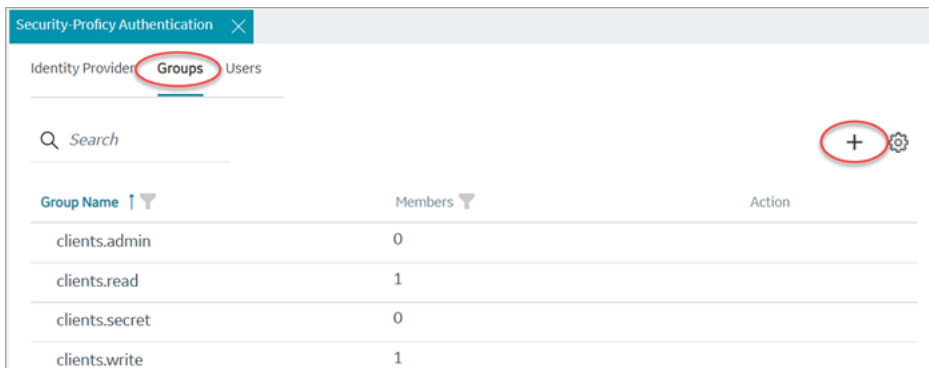
Log in to Configuration Hub as an administrator.

For example, you can create a group for users who perform the same task on the same resource.

You can have a group of supervisors for each line such as, `Supervisors_LineA`, `Supervisors_LineB`, `Supervisors_LineC`.

1. Go to **Proficy Authentication > Security > Groups**.

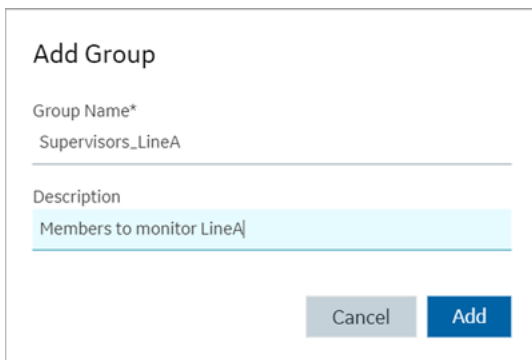
2. Select **+**



The **Add Group** screen appears.

3. Enter the following details for the new group.

Field	Description
Group Name	A unique name of the group that does not match with any existing Proficy Authentication groups. For example, <code>Supervisors_LineA</code>
Description	A brief description of the group.



4. Select **Add**.

The group is created successfully.

The newly created group is added to the list of groups on the **Groups** tab.

Modify Groups

This topic describes how to modify existing groups in Proficy Authentication.

Log in to Configuration Hub as an administrator.


You can modify a group to:

- [Add/Remove Users in a Group \(on page 102\)](#)
- [Add/Remove Sub-Groups in a Group \(on page 103\)](#)
- [Map Groups \(on page 99\)](#)

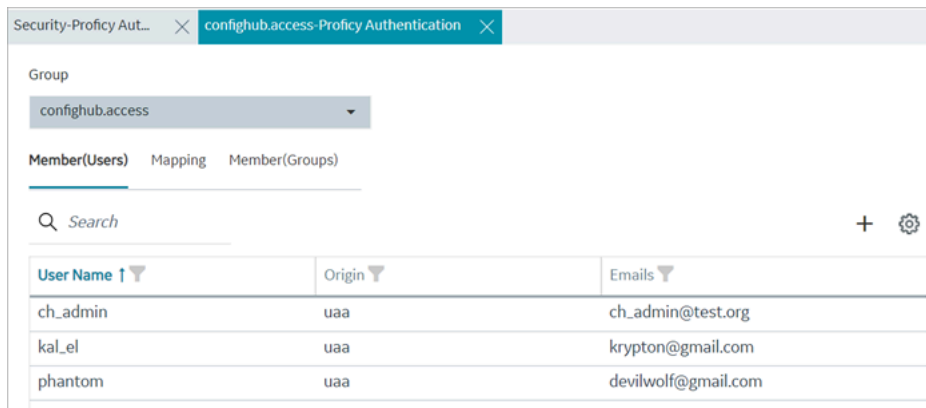
1. Go to **Proficy Authentication > Security > Groups**.

The existing list of Proficy Authentication groups appear.

2. Use any of these options to open a group.

- Double-click the group name you want to modify.
- For the group you want to modify, from its **ACTION** column, select , then **Edit**.

The group opens in a new tab.



3. You can modify the following:

Tab	Description
Member (Users)	Displays the list of users added to this group. Add/Remove Users in a Group (on page 102) .
Mapping	Displays the list of mapped groups for this group. You can add/remove mapped groups (on page 99) .
Member (Groups)	Displays the list of sub-groups added to this group. Add/Remove Sub-Groups in a Group (on page 103) .

Map Groups

This topic describes how to perform group mapping.

Log in to Configuration Hub as an administrator.

You can map any of the following to a Proficy Authentication group. The users belonging to these groups gain access to Proficy Authentication, and become a member of the target group.

- UAA groups
- LDAP
- SAML groups

1. Go to **Proficy Authentication > Security > Groups**.

The existing list of Proficy Authentication groups appear.

2. Double-click and open the group you want to map to UAA/LDAP/SAML groups.


3. Select the **Mapping** tab.

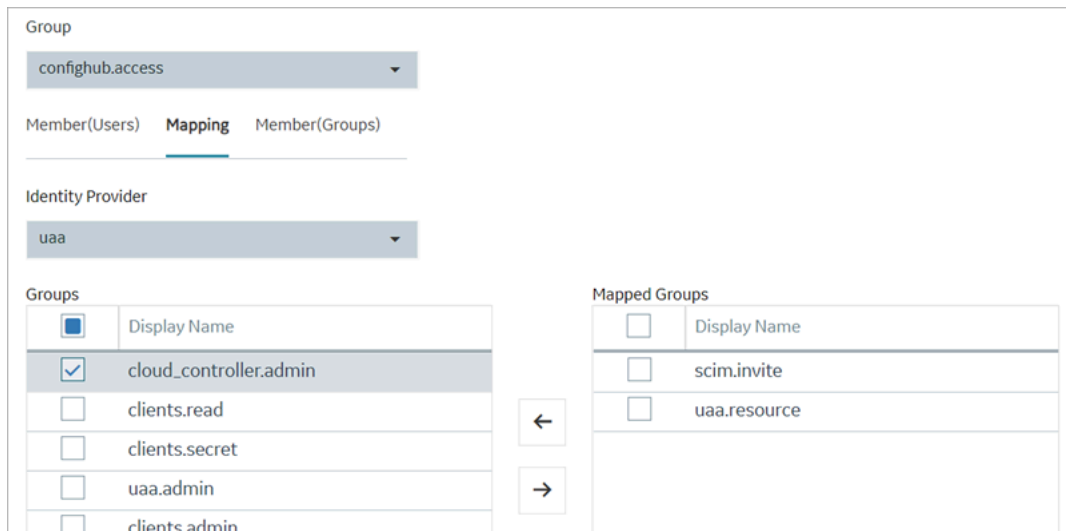
4. Map UAA groups.

a. From the **Identity Provider** drop down list, select the UAA record.

The groups from the UAA record appear.

b. Select the check box for the groups you want to map to the Proficy Authentication group selected in step 2.

c. Select  to move the selected items from **Groups** to **Mapped Groups**.



The screenshot shows the 'Mapping' tab for a group named 'confighub.access' under the 'uaa' identity provider. On the left, a table lists available groups from the UAA record. The 'cloud_controller.admin' group is selected with a checked checkbox. On the right, a table shows the 'Mapped Groups' which currently includes 'scim.invite' and 'uaa.resource'. A left-pointing arrow is positioned between the two tables, indicating that the selected group from the left will be moved to the mapped groups on the right.

Group	
confighub.access	

Member(Users) **Mapping** Member(Groups)

Identity Provider



uaa

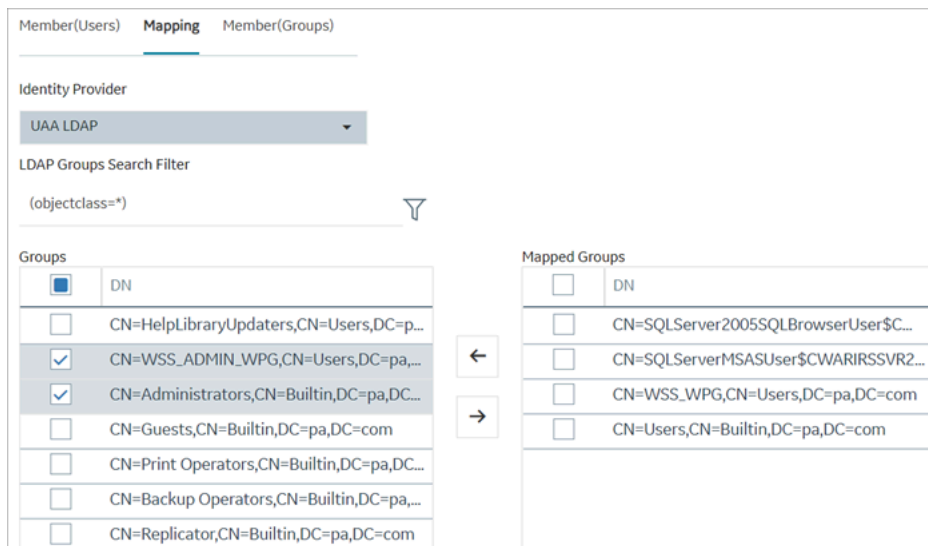
Groups	
<input type="checkbox"/>	Display Name
<input checked="" type="checkbox"/>	cloud_controller.admin
<input type="checkbox"/>	clients.read
<input type="checkbox"/>	clients.secret
<input type="checkbox"/>	uaa.admin
<input type="checkbox"/>	clients.admin

Mapped Groups	
<input type="checkbox"/>	Display Name
<input type="checkbox"/>	scim.invite
<input type="checkbox"/>	uaa.resource

The users belonging to the mapped UAA groups are now a member of the Proficy Authentication group selected in step 2.

5. Map LDAP groups.

- a. From the **Identity Provider** drop down list, select the LDAP record.
The groups from the LDAP server appear.
- b. Select the check box for the groups you want to map to the Proficy Authentication group selected in step 2.
- c. **Optional:** To search for an LDAP group, enter the keyword in the **LDAP Groups Search Filter** field and select .
- d. Select  to move the selected items from **Groups** to **Mapped Groups**.



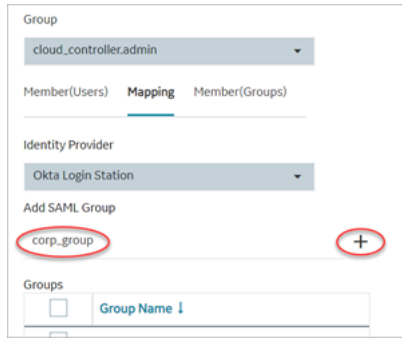
The screenshot shows the 'Mapping' tab in the configuration interface. It features a dropdown menu for 'Identity Provider' set to 'UAA LDAP' and a search filter field containing '(objectclass=*)'. Below these are two columns: 'Groups' and 'Mapped Groups'. The 'Groups' column contains a list of LDAP groups with checkboxes. Two groups are selected: 'CN=WSS_ADMIN_WPG,CN=Users,DC=pa,DC=com' and 'CN=Administrators,CN=Builtin,DC=pa,DC=com'. The 'Mapped Groups' column is currently empty. Between the columns are two arrow buttons: a left-pointing arrow and a right-pointing arrow.

Groups	Mapped Groups
<input checked="" type="checkbox"/> CN=WSS_ADMIN_WPG,CN=Users,DC=pa,DC=com	
<input checked="" type="checkbox"/> CN=Administrators,CN=Builtin,DC=pa,DC=com	
<input type="checkbox"/> CN=HelpLibraryUpdaters,CN=Users,DC=p...	
<input type="checkbox"/> CN=Guests,CN=Builtin,DC=pa,DC=com	
<input type="checkbox"/> CN=Print Operators,CN=Builtin,DC=pa,DC...	
<input type="checkbox"/> CN=Backup Operators,CN=Builtin,DC=pa,...	
<input type="checkbox"/> CN=Replicator,CN=Builtin,DC=pa,DC=com	
	<input type="checkbox"/> CN=SQLServer2005SQLBrowserUser\$C...
	<input type="checkbox"/> CN=SQLServerMSASUser\$CWARIRSSVR2...
	<input type="checkbox"/> CN=WSS_WPG,CN=Users,DC=pa,DC=com
	<input type="checkbox"/> CN=Users,CN=Builtin,DC=pa,DC=com


The users belonging to the mapped LDAP groups are now a member of the Proficy Authentication group selected in step 2.

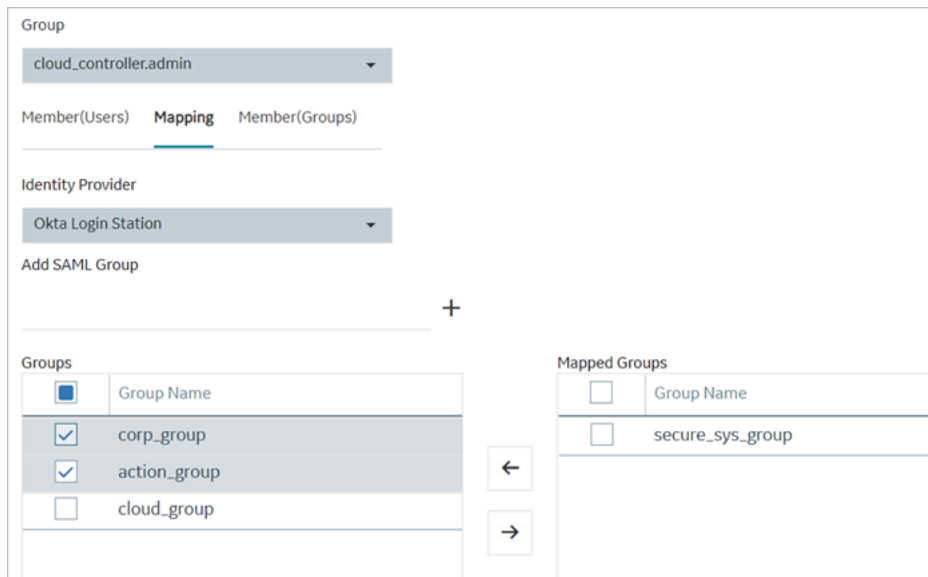
6. Map SAML groups.

- a. From the **Identity Provider** drop down list, select the SAML record.
- b. To create SAML groups, enter the valid SAML group name in the **Add SAML Group** field and select the plus icon.



c. Select the check box for the groups you want to map to the Proficy Authentication group selected in step 2.

d. Select  to move the selected items from **Groups** to **Mapped Groups**.



If the mapped SAML groups are valid, then all their users become a member of the Proficy Authentication group selected in step 2.

7. To unmap any of the mapped groups, select and move them back to **Groups**.

UAA/LDAP/SAML groups are successfully mapped.

Add/Remove Users in a Group

This topic describes how to add or remove users from a group.

[Modify a group \(on page 98\)](#) to add or remove users.

1. Select the **Member (Users)** tab.

2. Select **+**.

The **Map User** screen appears.

3. Select the check box for the user account you want to add to the group.

To remove user from a group, clear the check box.

<input type="checkbox"/>	User List 1
<input checked="" type="checkbox"/>	ch_admin
<input checked="" type="checkbox"/>	kal_el
<input type="checkbox"/>	mandrake_01
<input checked="" type="checkbox"/>	phantom

NOTE: Mapping supported for UAA users only.

Cancel Apply

4. Select **Apply**.

The users are added to (or removed from) the group.

Add/Remove Sub-Groups in a Group

This topic describes how to add or remove sub-groups from a group.

[Modify a group \(on page 98\)](#) to add or remove sub-groups.

1. Select the **Member (Groups)** tab.

2. Select **+**.

The **Group Membership** screen appears.

3. Select the check box for the group/s you want to add as a sub-group.

To remove a sub-group from a group, clear the check box.

Group Membership

Q Search

<input checked="" type="checkbox"/>	GROUPNAME ↑
<input type="checkbox"/>	clients.admin
<input type="checkbox"/>	clients.read
<input checked="" type="checkbox"/>	clients.secret
<input type="checkbox"/>	clients.write
<input checked="" type="checkbox"/>	cloud_controller.admin
<input type="checkbox"/>	confighub.admin

Cancel Apply



Important:

Do not select the check box for `icp.studioAdmin` group for any users or groups. As this group is for reserved purposes, make sure no user accounts or groups are assigned to this group to avoid runtime errors.

4. Select **Apply**.

The groups are added (or removed) as sub-groups in the group.

The users added to the sub-groups are automatically associated to the main group.

Delete Group

This topic describes how to delete Proficy Authentication groups.

Log in to Configuration Hub as an administrator.

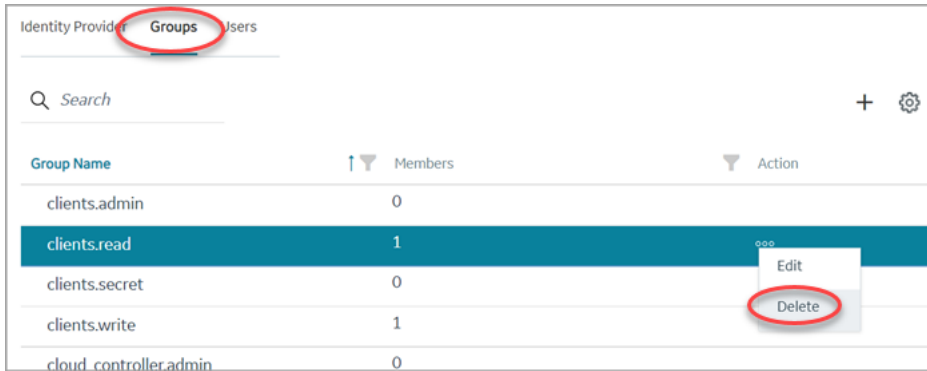
1. Go to **Proficy Authentication > Security > Groups**.

The existing list of groups appear.

2. Select the group you want to delete.

Additional options appear under the **ACTION** column.

3. Select , then **Delete**.



A message appears to confirm the delete action. The message also informs if users are associated to the group being deleted.

4. Select **Delete**.

The group account is deleted from the Proficy Authentication database.

Manage Users

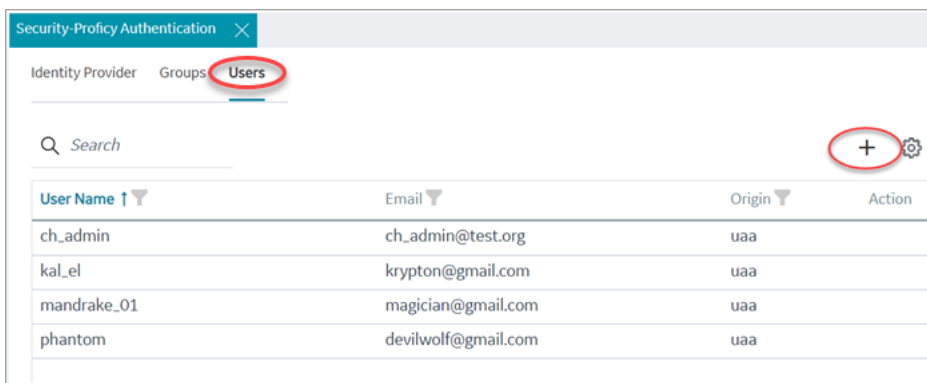
Create Users

This topic describes how to create new users in Proficy Authentication.

Log in to Configuration Hub as an administrator.

1. Go to **Proficy Authentication > Security > Users**.

2. Select **+**




The **Add User** screen appears.


3. Enter the following details for the new user account.

Field	Description
User Name	The user name to log in to Proficy Authentication.
Password	The password to log in to Proficy Authentication.
Confirm Password	Enter the password again for confirmation.
Email	User's email address.

Add User

User Name*
sys_admin

Password*
..... 

Confirm Password*
..... 

Email*
pacman@gmail.com


4. Select **Add**.

The user is created and added to the list of user accounts on the **Users** tab.

The new user is associated to default Proficy Authentication groups. These default groups cannot be deleted or modified: `approvals.me`, `cloud_controller.read`, `cloud_controller.write`, `cloud_controller_service_permissions.read`, `oauth.approvals`, `openid`, `password.write`, `profile`, `roles`, `scim.me`, `scim.userids`, `uaa.offline_token`, `uaa.user`, `user_attributes`.

Every user/client must possess the following three scopes to access the Security plug-in via Configuration Hub. If these scopes are not added, then a warning message alerts the user to contact Admin.

Scope	Description
<code>uaa.admin</code>	This scope indicates that this is a superuser.

Scope	Description
<code>clients.write</code>	This scope resets the Security plug-in's admin client secret.
<code>password.write</code>	This admin scope enables to change the user password. <div data-bbox="820 493 1421 714" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: This scope is assigned to all the UAA/ LDAP/SAML users by default without the need to assign manually. </div>

Default `ch_admin` has all the three scopes.

For user accounts originating from LDAP or SAML, refer to [Add LDAP/SAML Users \(on page 107\)](#).

Add LDAP/SAML Users

This topic describes how to add LDAP/SAML users to Proficy Authentication.

You must have an LDAP or SAML user account.

Only user accounts created in Proficy Authentication are immediately visible in the users list. LDAP or SAML users must perform the following steps to create user accounts in Proficy Authentication.

Log in to Proficy Authentication with LDAP/SAML user credentials.

A shadow user is created in Proficy Authentication, and can be subsequently seen in the Proficy Authentication users list.

The LDAP/SAML user account is added to the list of accounts on the **Users** screen.

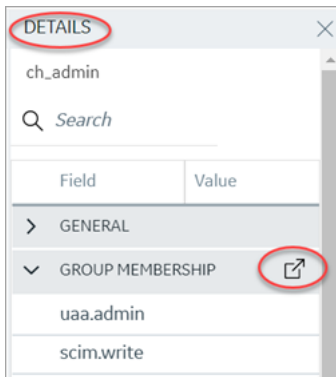
Add/Remove Groups for a User

This topic describes how to modify group membership for existing user accounts.

[Create Users \(on page 105\)](#)

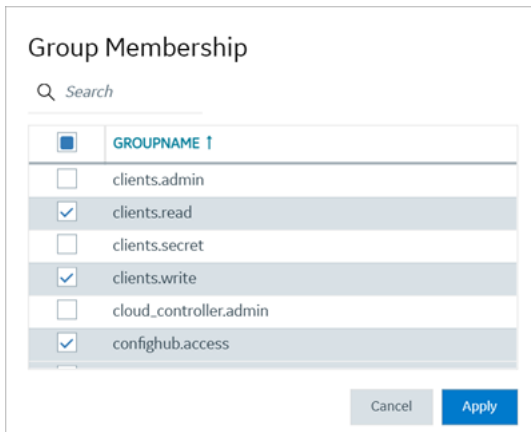
1. Go to **Proficy Authentication > Security > Users**.
The existing list of user accounts appear.
2. Select the user account for which you want to modify group membership.
The existing information for the user appears on the **DETAILS** panel.

3. Select  next to the **GROUP MEMBERSHIP** section.



The **Group Membership** screen appears.

4. Select the check box for the groups you want to add the user as a member.
To remove a group, clear the check box.



Important:

Do not select the check box for `iqp.studioAdmin` group for any users or groups. As this group is for reserved purposes, make sure no user accounts or groups are assigned to this group to avoid runtime errors.

5. Select **Apply**.

The groups are added (or removed from) for the user.



Note:

If a logged-in user attempts to remove his/her own scopes/groups, the remove operation may fail and result in an error: `Error while assigning the group`. In such instances, the user should log



out of the Configuration Hub application and log-in again. We recommend that logged-in users should avoid removing their own scopes.

Reset User Password

This topic describes how to reset passwords for Proficy Authentication users.

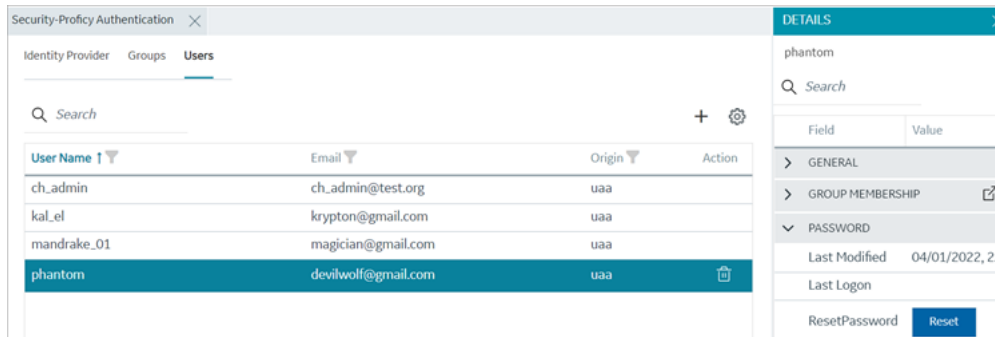
Log in to Configuration Hub as an administrator.

1. Go to **Proficy Authentication > Security > Users**.

The existing list of user accounts appear.

2. Select the user account for which you want to reset the password.

The option to reset password appears on the **DETAILS** panel under the **PASSWORD** section.



3. Select **RESET**.

The **Password Reset** screen appears.

4. Enter the new **Password** and **Confirm Password** for the user account.

The screenshot shows the 'Password Reset' form. It has three input fields: 'User Name*' (with 'phantom' entered), 'Password*' (with masked characters and a toggle icon), and 'Confirm Password*' (with masked characters and a toggle icon). At the bottom, there are 'Cancel' and 'ResetPassword' buttons.

5. Select **Reset Password** to apply the changes.

The password is reset for the user.

Delete User

This topic describes how to delete Proficy Authentication user accounts.

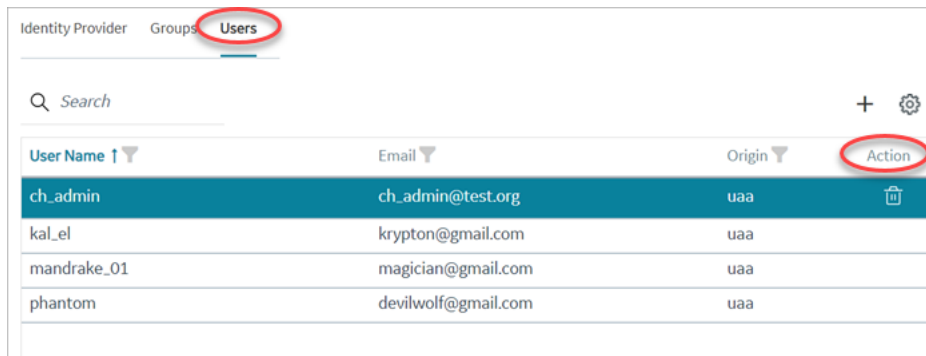
Log in to Configuration Hub as an administrator.


1. Go to **Proficy Authentication > Security > Users**.

The existing list of user accounts appear.

2. Select the user you want to delete.

Delete option appears in the **ACTION** column.



User Name	Email	Origin	Action
ch_admin	ch_admin@test.org	uaa	
ka_l_el	krypton@gmail.com	uaa	
mandrake_01	magician@gmail.com	uaa	
phantom	devilwolf@gmail.com	uaa	

3. Select .

A message appears to confirm the delete action.

4. Select **Delete**.

The user account is deleted from the Proficy Authentication database.

Windows Integrated Authentication / Auto-login

Windows Integrated Authentication is a new capability added to Proficy Authentication Service from version 2.5.

When Windows Integrated Authentication or Auto-login is enabled, users logged into any Windows machine in a domain are able to access Operations Hub and/or hosted Proficy applications without the need to type in their Windows credentials again. The same Windows logged-in user context is used for authenticating the user. Based on the user's privileges, access is provided to Operations Hub and/or its hosted applications.

This document describes the steps to configure the 'Windows Integrated Authentication' functionality in an instance of Proficy Authentication service. After configuring auto-login, when you attempt to log into Operations Hub / hosted Proficy applications, the **Select Authentication** screen appears (see figure

below) to choose between `Standard Proficy Authentication Login` Or `Active Directory (Windows) Integrated Login`.

If you choose `Active Directory (Windows) Integrated Login`, the authentication option will follow the new flow and you will not be prompted for providing credentials. Whereas choosing `Standard Proficy Authentication Login` will take you through the normal authentication flow and prompt for your credentials.



Note:

- The auto-login capability is only for authenticating the users. For authorization or access permissions, you have to configure LDAP IDP. To accomplish this, select the same active directory service / LDAP server, which brings the authentication service node, application accessing nodes in the network, and the users seeking auto-login, into the same Windows scope.
- For configuring LDAP IDP, refer to [Add LDAP Identity Provider \(on page 76\)](#).

Select Authentication

Standard Proficy Authentication Login

Active Directory (Windows) Integrated Login

Don't ask me again.

Standard Proficy Authentication Login	<p>Choose this option if you want to use the standard login (username/password or SAML).</p> <p>This is a regular login, which is based on username/password, including LDAP, or SAML.</p>
Active Directory (Windows) Integrated Login	<p>This option appears only if Windows auto-login is configured.</p> <p>This allows to automatically log into Operations Hub using the user's domain login session that was used to log in to Proficy Authentication.</p>
Don't ask me again	<p>Select this check box, if you don't want to display the Select Authentication screen every time you login.</p>

	<p>The system remembers the last selected authentication (between regular and autologin) and applies it for future logins.</p> <p>With Don't ask me again enabled, you can clear the last selected authentication only during logout.</p> <div data-bbox="537 411 1118 793" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>You have logged out</p> <hr/> <p>You should now close the browser, or click here to login again.</p> <p>You may also click here to clear the previously selected authentication option.</p> </div> <p>Select You may also click here to clear the previously selected authentication option to clear the saved selection. Once cleared, the clearing option is hidden from the logout screen.</p> <p>Select click here to login again to return to the login page.</p>
<p>Defer</p>	<p>Select to dismiss this screen, and skip selecting an authentication. You have the choice to select authentication next time you login.</p>

To configure Windows Auto-login, an administrator performs the following tasks only for the first time. The first task is performed on all the participating nodes (Active Directory service node, Proficy Authentication service node, and the client nodes). The second and third are performed on the Windows Active Directory Server machine. The fourth task is performed on the machine where Proficy Authentication is installed.

1. [Configure Security Policy \(on page 113\).](#)
2. [Create a service principal for your user account \(on page 115\).](#)
3. [Generate the Kerberos keytab file \(on page 118\).](#)
4. [Update the Proficy Authentication .yml file \(on page 121\).](#)
5. [Add LDAP Identity Provider \(on page 76\)](#) for the Active Directory service used in Steps 2 and 3.



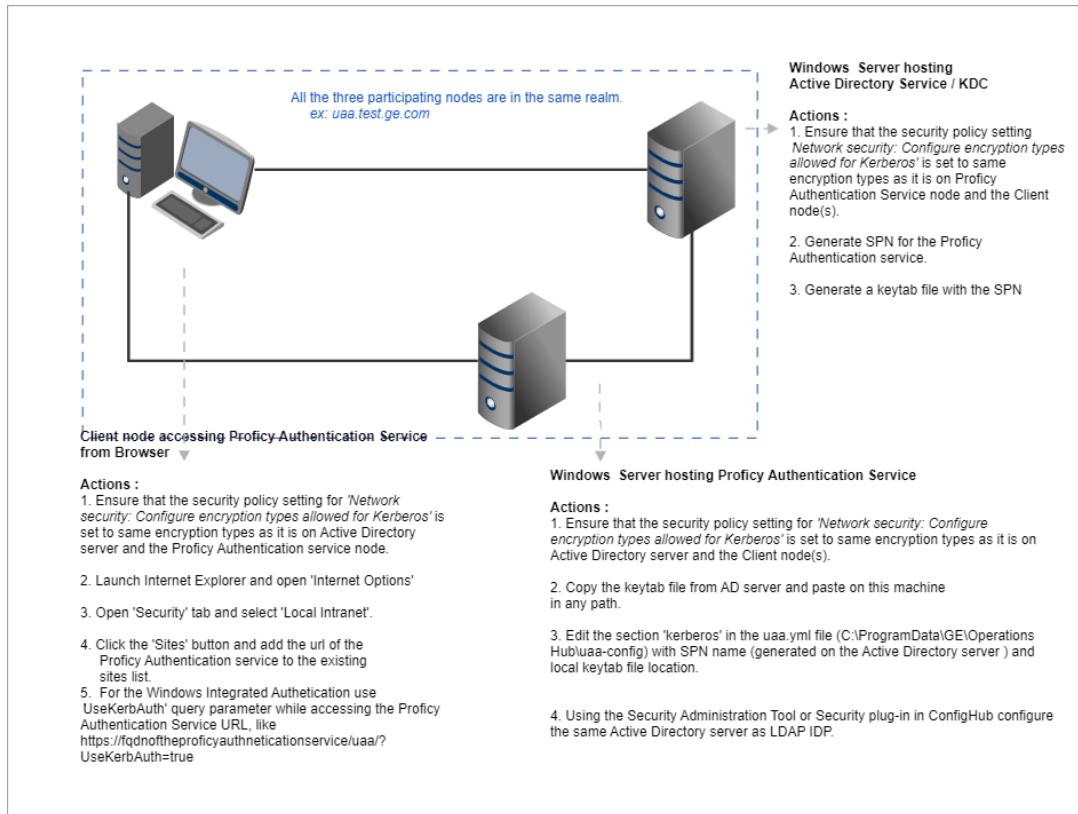
Note:

Users logging into DPM products using Windows Auto-login are authorized / get the scopes based on the LDAP configuration performed in Step 5.

To configure the browser settings for Windows Auto-login, the following task is performed on the end-user machine.

- [Configure the browser settings for Kerberos authentication \(on page 122\).](#)

Figure 1. Windows Auto-login - Deployment Topology and Configuration



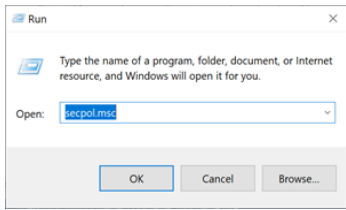
Configure Security Policy

This topic describes how to configure security policy setting associated to Kerberos authentication.

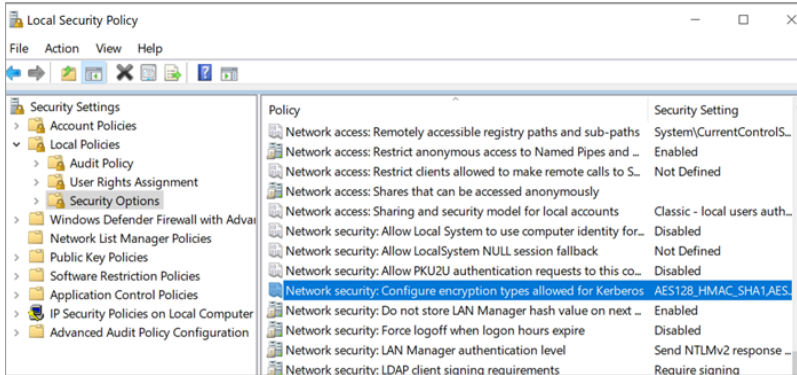
It is possible that you may not have access to your computer's local security policy settings, if it is governed by a group policy (controlled by your domain administrator). In any case, make sure that these security options are enabled for your computer.

If your environment is not governed by a group policy, then follow these steps to configure local security policy:

1. To access Local Security Policy, enter `secpol.msc` in Windows Run dialog and select **OK**.

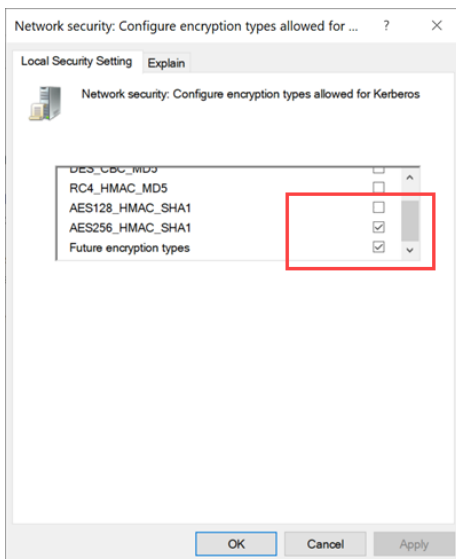


2. Navigate to **Security Settings > Local Policies > Security Options**.



3. Double-click and open `Network security: Configure encryption types allowed for Kerberos` security policy setting.
4. Select the valid encryption types that you want to use as shown in the figure. Ensure that the selection is same across all the participating nodes.

You can select either `AES128_HMAC_SHA1` or `AES256_HMAC_SHA1` as the encryption type. Also select the `Future encryption types` option.





Note:

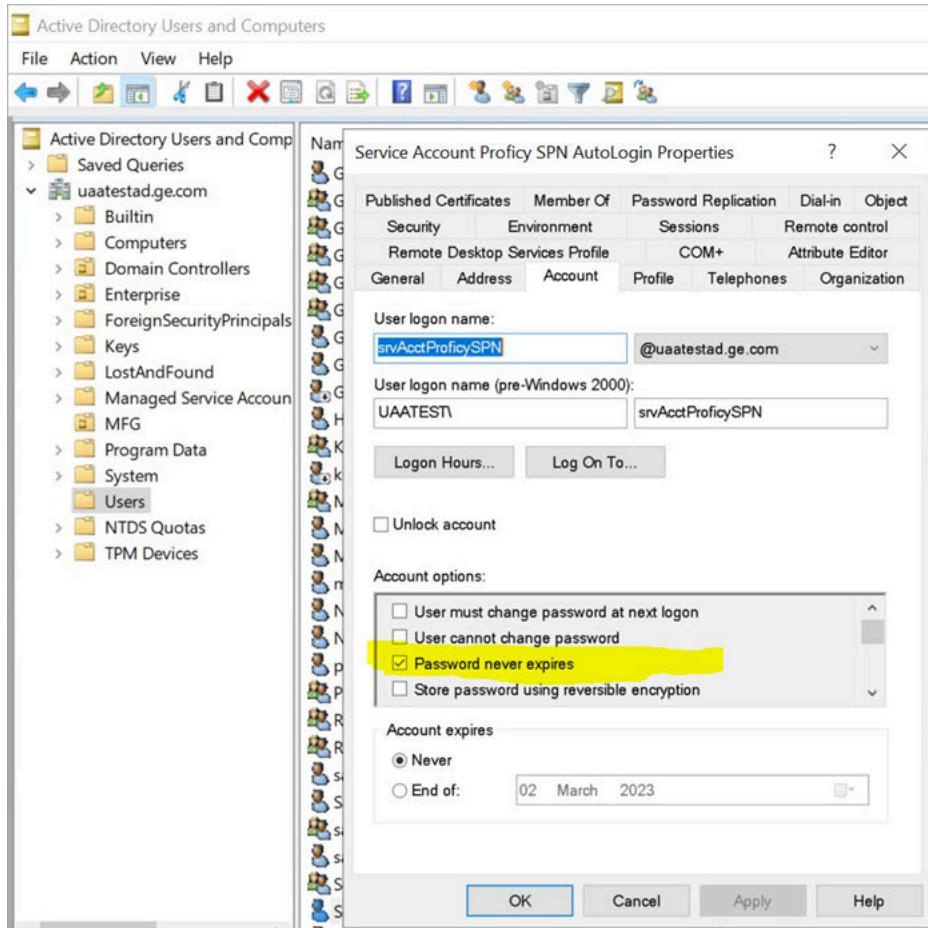
In our current documentation, we use `AES256_HMAC_SHA1` encryption type in our example code to [generate the keytab file \(on page 118\)](#).

For more information refer to [Microsoft documentation](#) on security policy settings.

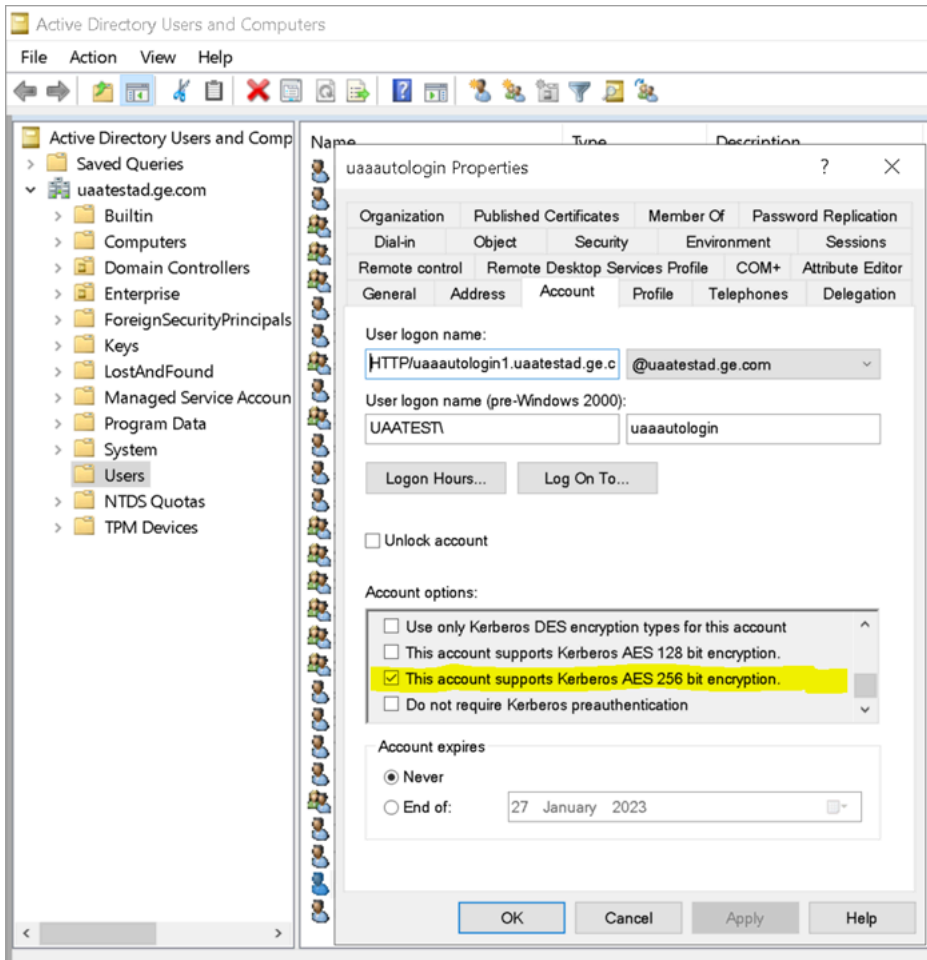
Create Service Principal Name

This topic describes how to create a service principal name.

- Create a dummy user account on the Active Directory Server node to represent the Proficy Authentication application in the active directory registry. Make sure to implement these settings for the account:
 - It is mandatory user is a member of the domain user group. Refer to [Microsoft documentation](#) for more information.
 - Set the account password to never expire. To do so, access the domain user account properties dialog: **Account > Account options > Password never expires**.



- [Configure Security Policy \(on page 113\)](#)




Note:

Delete existing SPNs, if any. Refer to [Useful SPN commands \(on page 127\)](#).

You must be an administrator to perform this task.

1. Log in to your Active Directory machine.
2. Open the Windows Command Prompt application.
3. Run the following command replacing with the appropriate code: `setspn -S HTTP/<FQDN> <user account>`

Code	Replace With
<FQDN>	Fully Qualified Domain Name (FQDN) of the server on which Proficy Authentication service is running.

Code	Replace With
	<p>For example, HTTP/win16-phantomhost.uaatestad.ge.com@UAATESTAD-.GE.COM</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: These should be in capital letters:</p> <ul style="list-style-type: none"> ◦ HTTP ◦ UAATESTAD.GE.COM (the domain name that follows @) </div>
<p><user account></p>	<p>Dedicated dummy user account created for Proficy Authentication service.</p> <p>For example, ghost1.</p>

Based on the above examples, your code should look like this: `setspn -S HTTP/win16-phantomhost.uaatestad.ge.com@UAATESTAD.GE.COM ghost1`

The service principal name (SPN) is created.

[Generate Keytab File \(on page 118\)](#)


Generate Keytab File



Generate the Kerberos keytab file.

[Create Service Principal Name \(on page 115\)](#)

You must be an administrator to perform this task.

1. Log in to your system and open the Windows Command Prompt application.
2. Run the following command replacing with the appropriate code: `ktpass -out <filename> -princ HTTP/<service principal name> -mapUser <user account> -mapOp set -pass <password> -crypto AES256-SHA1 -pType KRB5_NT_PRINCIPAL`

Code	Replace With
<p><filename></p>	<p>Name of the keytab file.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Keytab file name can be any given name.</p> </div>

Code	Replace With
	The file is created at the default location. You also have the option to specify an absolute path for file creation. For example, <code>-out c:\Documents\myskullcave.keytab</code> .
<service principal name>	Enter the service principal name that was created in the following format: <code>HTTP/win16-phantomhost.uaatestad.ge.com@UAATESTAD.GE-.COM</code>
<User account>	Enter the same dummy user account that was used during creating the service principal name. For example, <code>ghost1</code> . <div data-bbox="634 758 1419 978" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;"> Note: If you want to use a different user account, delete the existing user account, (or) rename the logon name in the user account.</div>
<password>	Proficy Authentication dummy user account password.
AES256-SHA1	Encryption algorithm you want to use. <div data-bbox="634 1136 1419 1310" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;"> Note: GE recommends <code>AES256-SHA1</code>. But you can also use <code>AES128-SHA1</code>.</div>
KRB5_NT_PRINCIPAL	Encryption type you want to use.

If the keytab is successfully created, the log should look something like this:

```
C:\Users\Administrator>ktpass -out c:\Temp\SACHINJOHUB21VM.uaatestad.ge.com.keytab -princ
HTTP/SACHINJOHUB21VM.uaatestad.ge.com@UAATESTAD.GE.COM -mapUser Mark -mapOp set -pass Gei321itc -crypto
AES256-SHA1 -pType KRB5_NT_PRINCIPAL
Targeting domain controller: uaatestad.uaatestad.ge.com
Using legacy password setting method
Successfully mapped HTTP/SACHINJOHUB21VM.uaatestad.ge.com to Mark.
Key created.
Output keytab to c:\Temp\SACHINJOHUB21VM.uaatestad.ge.com.keytab:
Keytab version: 0x502
```

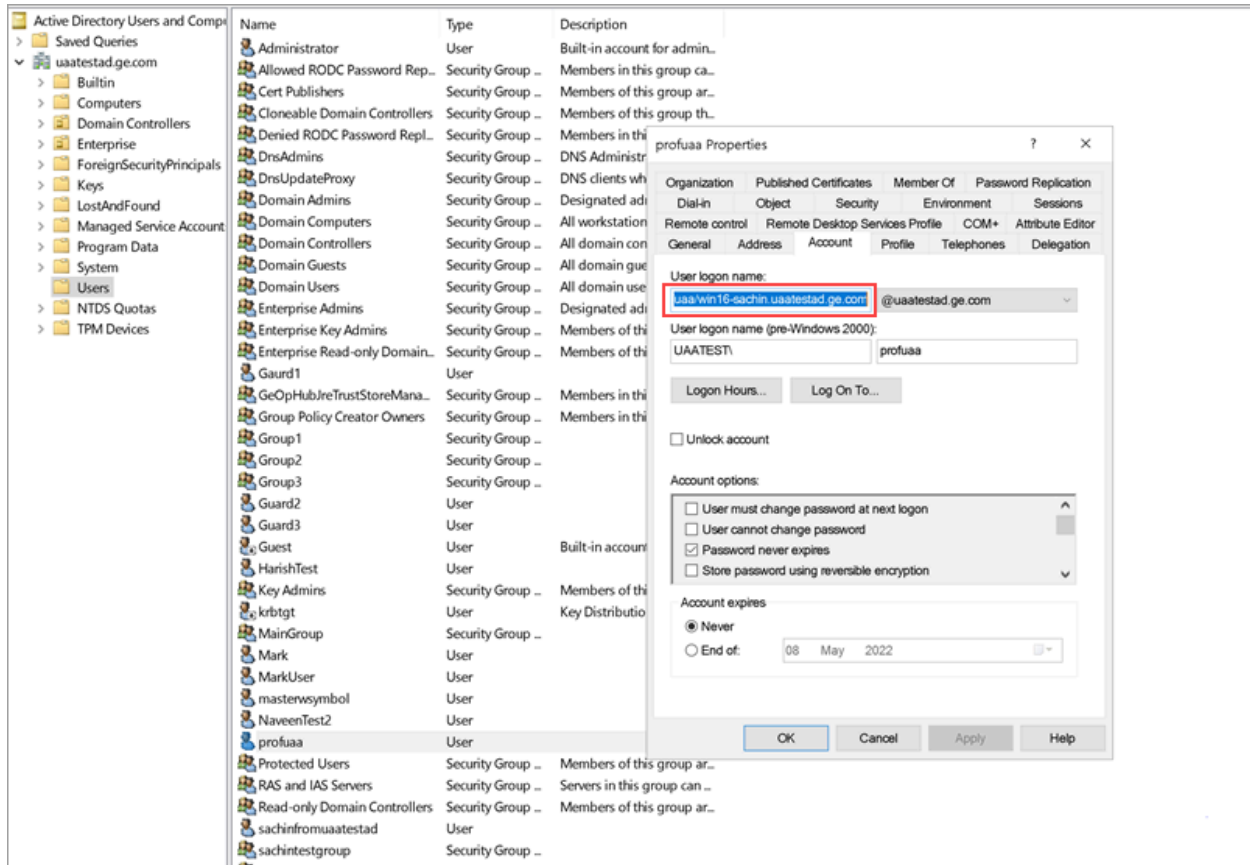
```
keysize 105 HTTP/SACHINJOHUB21VM.uaatestad.ge.com@UAATESTAD.GE.COM ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etype 0x12
(AES256-SHA1) keylength 32 (0x3fb2a2824864a6b3617bfa4a6458af83534efdb8a3eac08b02316cce9c4ee7fc)
```

Example of a failed log:

```
C:\Windows\system32>ktpass -out c:\Temp\win16-sachin.uaatestad.ge.com.keytab -princ
HTTP/win16-sachin.uaatestad.ge.com@UAATESTAD.GE.COM -mapUser John -mapOp set -pass Gei32litc -crypto
AES256-SHA1 -pType KRB5_NT_PRINCIPAL
Targeting domain controller: uaatestad.uaatestad.ge.com
Using legacy password setting method
Failed to set property 'userPrincipalName' to 'HTTP/win16-sachin.uaatestad.ge.com@UAATESTAD.GE.COM' on Dn
'CN=John,CN=Users,DC=uaatestad,DC=ge,DC=com': 0x13.
WARNING: Failed to set UPN HTTP/win16-sachin.uaatestad.ge.com@UAATESTAD.GE.COM on
CN=John,CN=Users,DC=uaatestad,DC=ge,DC=com.
kinits to 'HTTP/win16-sachin.uaatestad.ge.com@UAATESTAD.GE.COM' will fail.
Successfully mapped HTTP/win16-sachin.uaatestad.ge.com to John.
Key created.
Output keytab to c:\Temp\win16-sachin.uaatestad.ge.com.keytab:
Keytab version: 0x502
keysize 102 HTTP/win16-sachin.uaatestad.ge.com@UAATESTAD.GE.COM ptype 1 (KRB5_NT_PRINCIPAL) vno 9 etype 0x12
(AES256-SHA1) keylength 32 (0x8b551a22050935e9ace848cacbcc86a4eb845e63b6461d4f31b7d815158cf6c)
```

You can also do the following to verify if the service principal is mapped to the dummy account, and a keytab is created:

1. Go to **Active Directory Users and Computers > Users**.
2. Access the properties of the user account for which you created the keytab file.
3. On the **Account** tab, verify **User logon name**. is pointing to your service principal name.



- Copy the keytab file on the machine, where Proficy Authentication is installed.
- [Update the Proficy Authentication uaa.yml file \(on page 121\).](#)

Proficy Authentication Service Configuration

This topic provides steps to update the Proficy Authentication `uaa.yml` file.

Make sure you have completed the following tasks:

- [Generate Keytab File \(on page 118\).](#)
- Copy the keytab file from the Active Directory server, and paste it anywhere on the Proficy Authentication machine.
- Make a note of the keytab file location on the Proficy Authentication machine.

You must be an administrator to perform this task.

1. Log in to the computer machine where Proficy Authentication is installed.
2. Access the `uaa.yml` file.

The file is located at `C:\ProgramData\Proficy\Operations Hub\uaa-config\uaa.yml`

3. To modify, open `uaa.yml` in any text editor.

Example: Notepad++

4. Search for `kerberos` and enter values for the following keys:

service-principal	Enter the service principal name. For more information, refer to Create Service Principal Name (on page 115) .
keytab-location	Enter the location path where you copied the keytab file on this machine.

For example:

```
kerberos:
  service-principal: HTTP/win16-phantomhost.uaatestad.ge.com@UAATESTAD.GE.COM
  keytab-location: 'file:///C:/ProgramData/GE/Proficy Authentication/uaa-config/myskullcave.keytab'
```

5. Save and close the modified file.
6. Restart the `GE Proficy Authentication Tomcat Web Server` service.
 - a. Access the Windows Run dialog.
 - b. Enter `services.msc` to open the **Services** screen.
 - c. Right-click `GE Proficy Authentication Tomcat Web Server` and select **Restart**.

The Proficy Authentication service configuration is updated .

Configure Browser

Configure the browser settings for Kerberos authentication.

Windows Auto-login works if the following tasks are accomplished.

- [Create Service Principal Name \(on page 115\)](#)
- [Generate Keytab File \(on page 118\)](#)
- [Proficy Authentication Service Configuration \(on page 121\)](#)

The steps describe how to configure the browser settings on Internet Explorer (IE). Since IE settings are shared by Chrome, you do not have to configure it separately for the Chrome browser.



Important:

Windows Auto-login is not supported on the node where the Proficy Authentication service is running. To enable auto-login, configure the browser settings on a node different from the Proficy Authentication service node.

1. Go to **Control Panel > Internet Options**

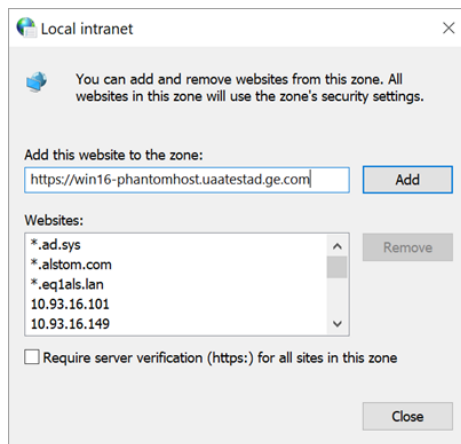
The **Internet Properties** dialog appears.

2. On the **Security** tab, select **Local intranet > Sites**.

The **Local intranet** window appears.

3. Select **Advanced**.

4. In **Add this website to the zone**, enter the URL of the Proficy Authentication service, and then select **Add**.



5. Select **Close**.

6. Select **OK** to close the open windows.

Kerberos supported SPNEGO authentication is enabled on your IE browser.

For Windows Auto-login, use `UseKerbAuth` query parameter while accessing the Proficy Authentication service URL. For example, `https://FQDN of the Proficy Authentication Service Node/uaa/?UseKerbAuth=true`

Troubleshooting Error Logs

This topic describes Windows Auto-login success/failure scenarios.

User logs in successfully

Verify the `uaa.log` if the TGT/Kerberos token is generated properly. It should start with **YII**. You can ignore the lengthy token value in the log entries.

```
[2022-02-22 19:29:41.949] cloudfoundry-identity-server - 14188 [http-nio-9480-exec-8] ...
DEBUG --- SpnegoAuthenticationProcessingFilter: Received Negotiate Header for request
https://win16-sachin.uaatestad.ge.com/uaa/: Negotiate YIIHVQYGKwY*****
```

A local Windows (non-domain) user attempts Windows Auto-login (using query parameter in the URL) from a domain member machine

Browser displays an error. The error message also appears in `uaa.log`. The following error appears when attempting to login with domain name in the URL.

HTTP Status 500 – Internal Server Error

Type Exception Report

Message Servlet.init() for servlet [spring] threw exception

Description The server encountered an unexpected condition that prevented it from fulfilling the request.

Exception

```
javax.servlet.ServletException: Servlet.init() for servlet [spring] threw exception
org.apache.catalina.authenticator.AuthenticatorBase.invoke(AuthenticatorBase.java:5
org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:92)
org.apache.catalina.valves.AbstractAccessLogValve.invoke(AbstractAccessLogValve.jav
org.apache.catalina.valves.RemoteIpValve.invoke(RemoteIpValve.java:769)
org.apache.catalina.valves.rewrite.RewriteValve.invoke(RewriteValve.java:289)
org.apache.catalina.valves.RequestFilterValve.process(RequestFilterValve.java:378)
org.apache.catalina.valves.RemoteAddrValve.invoke(RemoteAddrValve.java:56)
org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:357)
org.apache.coyote.http11.Http11Processor.service(Http11Processor.java:382)
org.apache.coyote.AbstractProcessorLight.process(AbstractProcessorLight.java:65)
org.apache.coyote.AbstractProtocol$ConnectionHandler.process(AbstractProtocol.java:
org.apache.tomcat.util.net.NioEndpoint$SocketProcessor.doRun(NioEndpoint.java:1722)
org.apache.tomcat.util.net.SocketProcessorBase.run(SocketProcessorBase.java:49)
org.apache.tomcat.util.threads.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java
org.apache.tomcat.util.threads.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.jav
org.apache.tomcat.util.threads.TaskThread$WrappingRunnable.run(TaskThread.java:61)
java.base/java.lang.Thread.run(Unknown Source)
```

Root Cause

```
java.lang.IllegalStateException: Listeners cannot be added to context [/uaa] as the context
org.cloudfoundry.identity.uaa.impl.config.YamlServletProfileInitializer.initialize(
org.cloudfoundry.identity.uaa.impl.config.YamlServletProfileInitializer.initialize(
org.springframework.web.servlet.FrameworkServlet.applyInitializers(FrameworkServlet
org.springframework.web.servlet.FrameworkServlet.configureAndRefreshWebApplicationC
org.springframework.web.servlet.FrameworkServlet.createWebApplicationContext(Framew
org.springframework.web.servlet.FrameworkServlet.createWebApplicationContext(Framew
org.springframework.web.servlet.FrameworkServlet.initWebApplicationContext(Framewor
org.springframework.web.servlet.FrameworkServlet.initServletBean(FrameworkServlet.f
org.springframework.web.servlet.HttpServletBean.init(HttpServletBean.java:170)
javax.servlet.GenericServlet.init(GenericServlet.java:158)
org.apache.catalina.authenticator.AuthenticatorBase.invoke(AuthenticatorBase.java:5
org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:92)
org.apache.catalina.valves.AbstractAccessLogValve.invoke(AbstractAccessLogValve.jav
org.apache.catalina.valves.RemoteIpValve.invoke(RemoteIpValve.java:769)
org.apache.catalina.valves.rewrite.RewriteValve.invoke(RewriteValve.java:289)
org.apache.catalina.valves.RequestFilterValve.process(RequestFilterValve.java:378)
org.apache.catalina.valves.RemoteAddrValve.invoke(RemoteAddrValve.java:56)
```

The following error appears when attempting to login with non-domain name in the URL.

HTTP Status 500 – Internal Server Error

Type Exception Report

Message Servlet.init() for servlet [spring] threw exception

Description The server encountered an unexpected condition that prevented it from fulfilling the request.

Exception

```

javax.servlet.ServletException: Servlet.init() for servlet [spring] threw exception
    org.apache.catalina.authenticator.AuthenticatorBase.invoke(AuthenticatorBase.java:540)
    org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:92)
    org.apache.catalina.valves.AbstractAccessLogValve.invoke(AbstractAccessLogValve.java:687)
    org.apache.catalina.valves.RemoteIpValve.invoke(RemoteIpValve.java:769)
    org.apache.catalina.valves.rewrite.RewriteValve.invoke(RewriteValve.java:289)
    org.apache.catalina.valves.RequestFilterValve.process(RequestFilterValve.java:378)
    org.apache.catalina.valves.RemoteAddrValve.invoke(RemoteAddrValve.java:56)
    org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:357)
    org.apache.coyote.http11.Http11Processor.service(Http11Processor.java:382)
    org.apache.coyote.AbstractProcessorLight.process(AbstractProcessorLight.java:65)
    org.apache.coyote.AbstractProtocol$ConnectionHandler.process(AbstractProtocol.java:895)
    org.apache.tomcat.util.net.NioEndpoint$SocketProcessor.doRun(NioEndpoint.java:1722)
    org.apache.tomcat.util.net.SocketProcessorBase.run(SocketProcessorBase.java:49)
    org.apache.tomcat.util.threads.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1191)
    org.apache.tomcat.util.threads.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:659)
    org.apache.tomcat.util.threads.TaskThread$WrappingRunnable.run(TaskThread.java:61)
    java.base/java.lang.Thread.run(Unknown Source)

```

Root Cause

```

java.lang.IllegalStateException: Listeners cannot be added to context [/uaa] as the context has been initialised
    org.cloudfoundry.identity.uaa.impl.config.YamlServletProfileInitializer.initialize(YamlServletProfileInitializer.java:86)
    org.cloudfoundry.identity.uaa.impl.config.YamlServletProfileInitializer.initialize(YamlServletProfileInitializer.java:54)
    org.springframework.web.servlet.FrameworkServlet.applyInitializers(FrameworkServlet.java:764)
    org.springframework.web.servlet.FrameworkServlet.configureAndRefreshWebApplicationContext(FrameworkServlet.java:701)
    org.springframework.web.servlet.FrameworkServlet.createWebApplicationContext(FrameworkServlet.java:716)
    org.springframework.web.servlet.FrameworkServlet.initWebApplicationContext(FrameworkServlet.java:591)
    org.springframework.web.servlet.FrameworkServlet.initServletBean(FrameworkServlet.java:530)
    org.springframework.web.servlet.HttpServletBean.init(HttpServletBean.java:170)
    javax.servlet.GenericServlet.init(GenericServlet.java:158)
    org.apache.catalina.authenticator.AuthenticatorBase.invoke(AuthenticatorBase.java:540)
    org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:92)
    org.apache.catalina.valves.AbstractAccessLogValve.invoke(AbstractAccessLogValve.java:687)
    org.apache.catalina.valves.RemoteIpValve.invoke(RemoteIpValve.java:769)
    org.apache.catalina.valves.rewrite.RewriteValve.invoke(RewriteValve.java:289)
    org.apache.catalina.valves.RequestFilterValve.process(RequestFilterValve.java:378)
    org.apache.catalina.valves.RemoteAddrValve.invoke(RemoteAddrValve.java:56)
    org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:357)

```

Bad or missing keytab file (or) Bad SPN in `uaa.yml` file

The following errors appear in `uaa.log`.

```

[2022-02-21 19:09:21.839] cloudfoundry-identity-server - 13956 [http-nio-9480-exec-8] .... ERROR ---
DynamicKerberosAuthenticationManager: Kerberos validation not successful. Encountered Bad Credentials Exception :
Kerberos validation not successful
[2022-02-21 19:09:21.839] cloudfoundry-identity-server - 13956 [http-nio-9480-exec-8] .... ERROR ---
DynamicKerberosAuthenticationManager: Kerberos validation not successful. Encountered Bad Credentials Exception :
Kerberos validation not successful
[2022-02-21 19:09:21.839] cloudfoundry-identity-server - 13956 [http-nio-9480-exec-8] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : null

```

```
[2022-02-21 19:09:21.839] cloudfoundry-identity-server - 13956 [http-nio-9480-exec-8] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : null

[2022-02-21 19:09:21.839] cloudfoundry-identity-server - 13956 [http-nio-9480-exec-8] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Defective token detected (Mechanism
level: GSSHeader did not find the right tag)

[2022-02-21 19:09:21.839] cloudfoundry-identity-server - 13956 [http-nio-9480-exec-8] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Defective token detected (Mechanism
level: GSSHeader did not find the right tag)

[2022-02-21 19:09:21.839] cloudfoundry-identity-server - 13956 [http-nio-9480-exec-8] ....
WARN --- SpnegoAuthenticationProcessingFilter: Negotiate Header was invalid: Negotiate
TlRMTVNTUABAAAAA14II4gAAAAAAAAAAAAAAAAAAAAAAAAAKADk4AAAAADw==
org.springframework.security.authentication.BadCredentialsException: Bad Credentials excption. It could be due to
keytab file and the SPN configuration.
```

Crypto Mismatch

A crypto mismatch occurs if the encryption algorithm specified while using `ktpass.exe` to generate keytab does not match what is supported by the service account.

```
[2022-02-22 11:39:18.326] cloudfoundry-identity-server - 6084 [http-nio-9480-exec-3] .... ERROR ---
DynamicKerberosAuthenticationManager: Kerberos validation not successful. Encountered Bad Credentials Exception :
Kerberos validation not successful

[2022-02-22 11:39:18.326] cloudfoundry-identity-server - 6084 [http-nio-9480-exec-3] .... ERROR ---
DynamicKerberosAuthenticationManager: Kerberos validation not successful. Encountered Bad Credentials Exception :
Kerberos validation not successful

[2022-02-22 11:39:18.326] cloudfoundry-identity-server - 6084 [http-nio-9480-exec-3] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : null

[2022-02-22 11:39:18.326] cloudfoundry-identity-server - 6084 [http-nio-9480-exec-3] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : null

[2022-02-22 11:39:18.326] cloudfoundry-identity-server - 6084 [http-nio-9480-exec-3] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Failure unspecified at GSS-API
level (Mechanism level: Invalid argument (400) - Cannot find key of appropriate type to decrypt AP-REQ - RC4 with
HMAC)

[2022-02-22 11:39:18.326] cloudfoundry-identity-server - 6084 [http-nio-9480-exec-3] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Failure unspecified at GSS-API
level (Mechanism level: Invalid argument (400) - Cannot find key of appropriate type to decrypt AP-REQ - RC4 with
HMAC)
```



```
[2022-02-22 11:39:18.326] cloudfoundry-identity-server - 6084 [http-nio-9480-exec-3] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Invalid argument (400) - Cannot
find key of appropriate type to decrypt AP-REQ - RC4 with HMAC

[2022-02-22 11:39:18.326] cloudfoundry-identity-server - 6084 [http-nio-9480-exec-3] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Invalid argument (400) - Cannot
find key of appropriate type to decrypt AP-REQ - RC4 with HMAC
```

Clock skew between client and server

The following errors appear in `uaa.log`.

```
[2022-02-19 13:14:55.556] cloudfoundry-identity-server - 14532 [http-nio-9480-exec-9] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : null

[2022-02-19 13:14:55.556] cloudfoundry-identity-server - 14532 [http-nio-9480-exec-9] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : null

[2022-02-19 13:14:55.556] cloudfoundry-identity-server - 14532 [http-nio-9480-exec-9] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Failure unspecified at GSS-API
level (Mechanism level: Clock skew too great (37))

[2022-02-19 13:14:55.556] cloudfoundry-identity-server - 14532 [http-nio-9480-exec-9] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Failure unspecified at GSS-API
level (Mechanism level: Clock skew too great (37))

[2022-02-19 13:14:55.556] cloudfoundry-identity-server - 14532 [http-nio-9480-exec-9] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Clock skew too great (37)

[2022-02-19 13:14:55.556] cloudfoundry-identity-server - 14532 [http-nio-9480-exec-9] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Clock skew too great (37)
```



Note:

Make sure the clocks on all the three systems are synchronized.

Useful SPN commands

<p>To view existing SPNs</p>	<pre>setspn -F -Q HTTP/<FQDN></pre> <p>Example: <code>setspn -F -Q HTTP/win16-phantomhost.uaatestad.ge.com@UAATESTAD- .GE.COM</code></p>
<p>To delete SPN</p>	<pre>setspn -D HTTP/<FQDN> <user account></pre> <p>Example: <code>setspn -D HTTP/win16-phantomhost.uaatestad.ge.com@UAATESTAD.GE- .COM ghost1</code></p>

High Availability

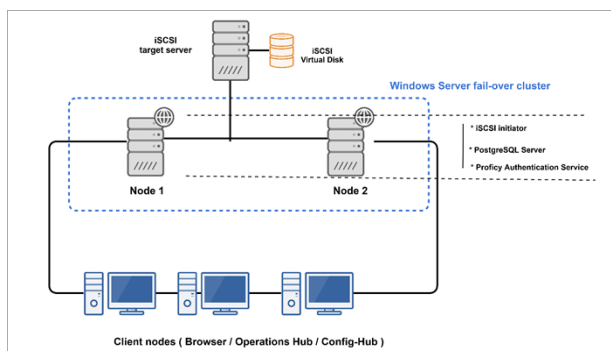
Configure High Availability for Proficy Authentication

This topic describes how to set up a highly available server for the Proficy Authentication service that is based on the Windows failover cluster and iSCSI technologies.

You need:

- One Windows Server 2019 virtual machine to serve as iSCSI Target.
- Two Windows Server 2019 virtual machines to serve as iSCSI Initiators:
 - A primary node (Node1) server
 - A secondary node (Node2) server

The following image illustrates the simplest form of deploying the Windows failover cluster and iSCSI technology-based high available solution for the Proficy Authentication Service.



In failover cluster technology, a group of independent computers work together to increase the availability and scalability of clustered roles (identified as nodes in a cluster). Nodes are clustered server machines running applications and services.

Failover cluster feature and file server roles are installed on the Node1 and Node2 servers (also called iSCSI initiators). A virtual disk is created on the iSCSI target server for shared storage. Failover clustering technology arranges for a backup server whenever the primary server has failed for any reason. So, if the primary server Node1 is down, then the backup server Node2 is automatically activated to replace the role of the primary server. This ensures uninterrupted access to shared storage and continuity of services even during failure of the primary server.

1. Set up the iSCSI Target.
 - a. [Configure iSCSI Target \(on page 129\)](#)
 - b. [Create a Virtual Disk \(on page 131\)](#)
2. Set up the iSCSI initiators: Node1 and Node2.

- a. [Configure iSCSI Initiator \(on page 130\)](#)
- b. [Initialize a Virtual Disk \(on page 133\)](#)
3. Open Failover Cluster Manager on any of the iSCSI initiator nodes in a cluster (Node1 or Node2), and [create a cluster \(on page 135\)](#).
4. Create and configure a role for the failover cluster. See [Configure Role \(on page 138\)](#).
5. Install Proficy Authentication on both the nodes.
See [Configure Proficy Authentication Installation \(on page 142\)](#).

If you are installing Operations Hub in a highly available cluster, follow the steps as described in [Prerequisites for Installing Operations Hub with External Proficy Authentication \(on page 146\)](#).

6. Restart the services on both the nodes.

Configure iSCSI Target

This topic describes how to configure an iSCSI target server.

You can configure an external storage using Windows 2019.

1. Log in to the virtual machine where you want to set up the iSCSI target server.
2. Go to **Start > Administrative Tools > Server Manager**.
3. From the Server Manager dashboard, select **Manage > Add roles and features**.
4. Complete **Add Roles and Features Wizard** with these options:

Section	What To Do
Before You Begin	Skip to the next section.
Installation Type	Select Role-based or feature-based installation .
Server Selection	<ol style="list-style-type: none"> a. Choose the option Select a server from the server pool. b. Under the server pool section, select your target server. You will be installing the role/feature on this server.
Server Roles	In the roles list box: <ol style="list-style-type: none"> a. Expand File and Storage Services > File and iSCSI Services. b. Select the check box for iSCSI Target Server.
Confirmation	Select Install .

When the installation is complete, restart the machine.

Log in to the same server again and [create a virtual disk \(on page 131\)](#).

Configure iSCSI Initiator

This topic describes how to configure an iSCSI initiator and connect to the target server.

[Configure iSCSI Target \(on page 129\)](#).

You must perform these steps on all the initiator server nodes you want to add to a cluster. Let us assume you are setting up a basic two-node cluster, where there are two iSCSI initiators:

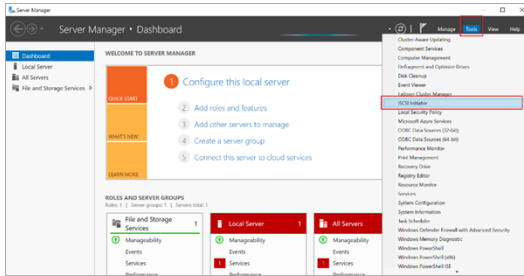
- A primary server called Node1
- A secondary server called Node2

1. Log in to the Node1 server.
2. Go to **Start > Administrative Tools > Server Manager**.
3. From the Server Manager dashboard, select **Manage > Add roles and features**.
4. Complete **Add Roles and Features Wizard** with these options:

Section	What To Do
Before You Begin	Skip to the next section.
Installation Type	Select Role-based or feature-based installation .
Server Selection	<ol style="list-style-type: none"> a. Choose the option Select a server from the server pool. b. Under the server pool section, select your Node1 server. You will be installing the role/feature on this server.
Server Roles	In the roles list box: <ol style="list-style-type: none"> a. Expand File and Storage Services > File and iSCSI Services. b. Select the check box for iSCSI Target Server.
Features	To allow the installation of Failover Cluster Manager: <ol style="list-style-type: none"> a. In the features list box, select the check box for Failover Clustering. The Add features that are required for Failover Clustering? screen appears, which shows the dependencies that are installed with this feature. b. Select Add Features.
Confirmation	Select Install .

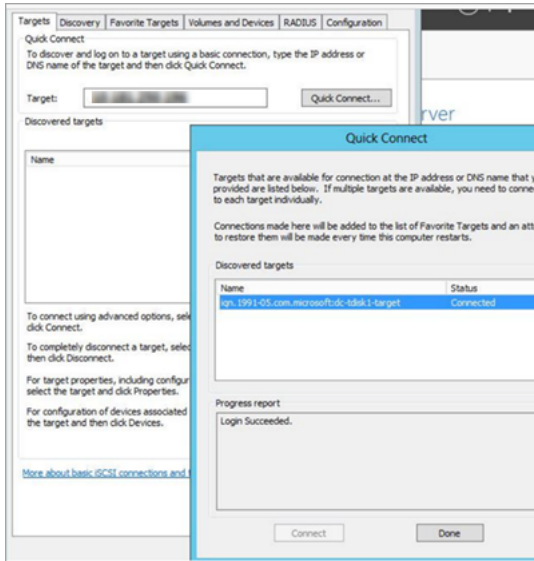
The selected role and feature is installed on the Node1 server.

5. When the installation is complete, restart the machine.
6. Log in to the same server again and launch **Server Manager**.
7. From the **Tools** menu, select **iSCSI Initiator**.



8. In the **Target** field, enter the iSCSI target server address.
9. Select **Quick Connect**.

If connected, the login success appears as shown in the following figure:



10. Select **Done**, then **OK** to exit.
11. Log in to the Node2 server and repeat steps 1-9.

Initialize a Virtual Disk (on page 133)

Create a Virtual Disk

This topic describes how to create an iSCSI virtual disk and configure the access server.

You must first [configure the iSCSI target server \(on page 129\)](#).

1. Log in to the iSCSI target server.
2. Go to **Start > Administrative Tools > Server Manager**.

3. Go to **File and Storage Services > iSCSI**.
4. From the **TASKS** drop-down menu, select **New iSCSI Virtual Disk**.
5. Complete **New iSCSI Virtual Disk Wizard** with these options:

Section	What To Do
iSCSI Virtual Disk Location	The iSCSI target server and volume details are displayed.
iSCSI Virtual Disk Name	Enter a name for the virtual disk. For example, <code>sharedDisk</code>
iSCSI Virtual Disk Size	<ol style="list-style-type: none"> a. Enter the disk size. For example, <code>10GB</code>. The disk size depends on your database utilization and number of users. b. Select Dynamically expanding.
iSCSI Target	<p>Select New iSCSI target.</p> <p>If the target is new, then it should be assigned later as described in step 8.</p>
Target Name and Access	Enter a name for the iSCSI target server. For example, <code>hauaatarget</code>
Access Servers	<p>Add the iSCSI initiators (Node1 and Node2) and enable them to access the iSCSI virtual disk. Follow these steps to add the servers one at a time:</p> <ol style="list-style-type: none"> a. Select Add. The Add initiator ID screen appears. b. Select Enter a value for the selected type. c. From the Type drop-down menu, choose any of the following options to enter a value: <ul style="list-style-type: none"> ▪ If you select DNS Name, enter the DNS name of the computer where the iSCSI initiator is installed. ▪ If you select IP Address, then enter the IP address of the computer where the iSCSI initiator is installed. ▪ If you select Mac Address, then enter the MAC address of the computer where the iSCSI initiator is installed. d. Select OK to exit. e. To add Node2, repeat the above steps.
Enable authentication	Skip to the next section.
Confirmation	Select Create .

When the iSCSI virtual disk is created successfully, select **Close** to exit the wizard.

- In Server Manager, go to **File and Storage Services > iSCSI** and verify the newly created virtual disk is listed under iSCSI virtual disks.

The virtual disk status appears as `Not Connected`. This occurs when a new iSCSI target is selected during iSCSI virtual disk creation.

- Right-click the `Not Connected` iSCSI virtual disk and select **Assign iSCSI Virtual Disk**.
- Complete **Assign iSCSI Virtual Disk Wizard** with these options:

Section	What To Do
iSCSI Target	Select Existing iSCSI target and select the target server to connect.
Confirmation	Select Assign .

When the iSCSI virtual disk is assigned successfully, select **Close** to exit the wizard.

Initialize a Virtual Disk

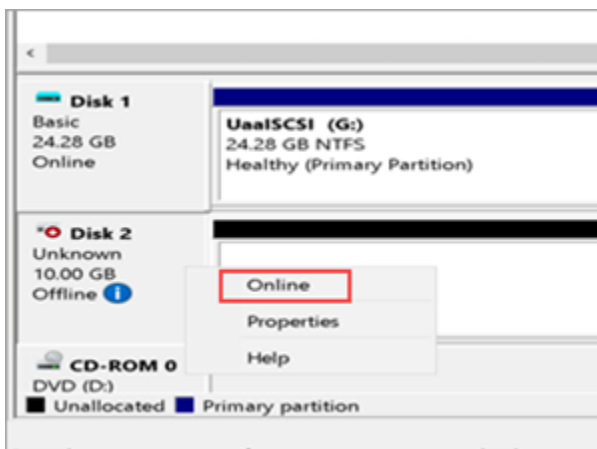
This topic describes how to initialize a disk and create a volume.

[Create a Virtual Disk \(on page 131\)](#).

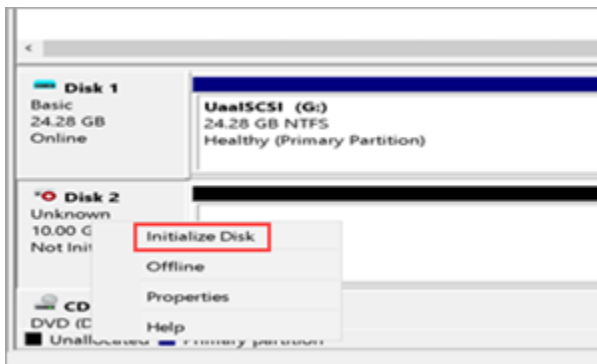
You need to perform the following tasks only once on any of the iSCSI initiator nodes and it applies to the other nodes in a cluster. Suppose there are two nodes in a cluster, Node1 and Node2. If you initialize a virtual disk on the Node1 server, then you don't need to do it again on the Node2 server.

- Log in to any of the server nodes in a cluster (Node1 or Node2).
- Go to **Control Panel > Administrator Tools > Computer Management > Storage > Disk Management**.
- Look for the unknown disk, right-click and select **Online**.

If the unknown disk is offline, you must bring it online.

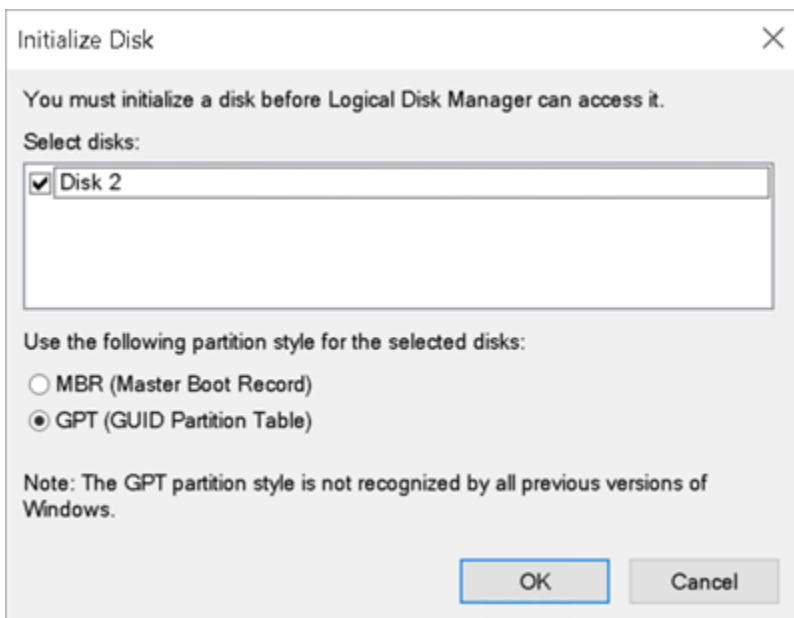


4. Right-click the unknown disk again and select **Initialize disk**.

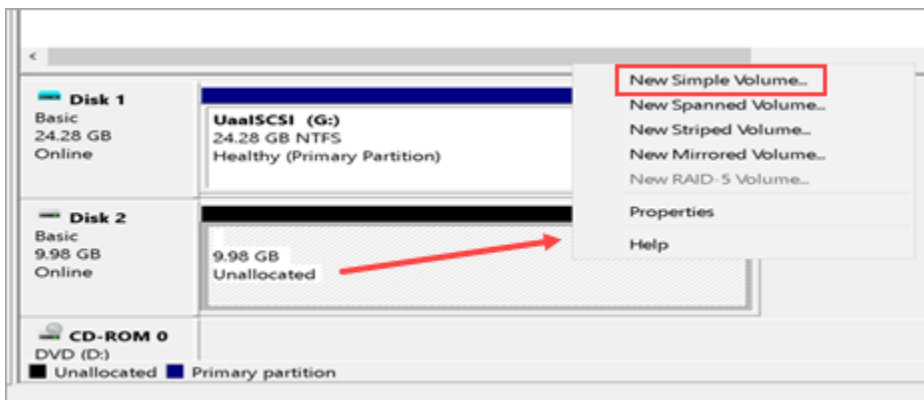


The **Initialize Disk** screen appears.

5. Select **OK**.



6. Right-click the unallocated space on the disk, and select **New Simple Volume**.



The **New Simple Volume Wizard** screen appears.

7. Complete the steps in the wizard to create a new volume.

You need to:

- Specify the size of the volume you want to create in megabytes (MB).
- Assign a drive letter to identify the partition.
- Format the volume with default settings.

The newly created volume should appear under **This PC** on the logged-in machine.

Create a Cluster

This topic describes how to create a failover cluster.

Install Failover Cluster Manager on the iSCSI initiator nodes. Refer to steps 1-4 in [Configure iSCSI Initiator \(on page 130\)](#).

You can perform these steps on either Node1 or Node2. Suppose you perform these steps on Node1, they are automatically applied to Node2.

1. Log in to the iSCSI initiator node.
2. Go to **Start > Administrative Tools > Failover Cluster Manager**.
3. In Failover Cluster Manager, select **Validate a Configuration**.

Before starting to create a cluster of nodes, you should validate whether the nodes that you are adding to the cluster are compatible with the cluster hardware requirement. For more information, refer to the [Microsoft documentation](#).

4. Complete **Validate a Configuration Wizard** with these options:

Section	What To Do
Before You Begin	Skip to the next section.
Select Servers or a Cluster	Browse and locate the servers you want to add to the cluster. Refer to Add Server Nodes for Validation (on page 136) .
Testing Options	Select Run all tests (recommended) .
Confirmation	Review the list of tests run on the selected servers. The number of tests run are based on the roles installed on the server nodes.
Validating	This process may take several minutes depending on your network infrastructure, and the number of server nodes selected for validation.

Section	What To Do
Summary	<ul style="list-style-type: none"> a. Select View Report. b. Review Failover Cluster Validation Report and fix any failed validations. You can ignore expected warnings. The validation report should be free of any errors, otherwise the cluster setup will not be successful. c. Select Finish.

5. In Failover Cluster Manager, select **Create a Cluster**.

6. Complete **Create Cluster Wizard** using these options:

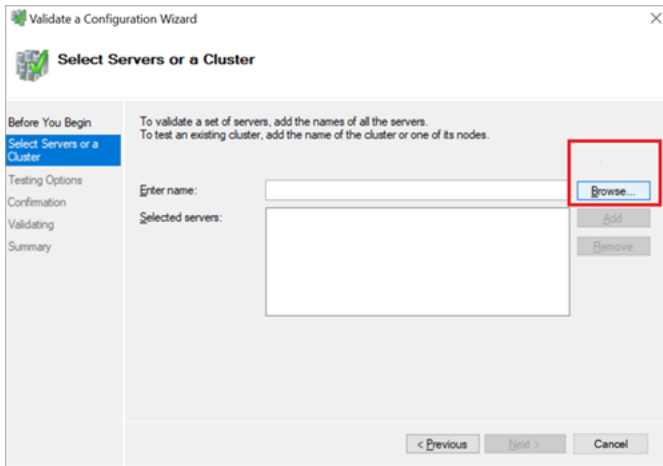
Section	What To Do
Before You Begin	Skip to the next section.
Select Servers	Nodes were already added during validating the configuration process.
Validation Warning	Select No .
Access Point for Administering the Cluster	Enter a unique name for your cluster. For example, <code>hauaacluster</code>
Confirmation	Clear the check box for Add all eligible storage to the cluster .
Creating New Cluster	This process may take a while as there are several checks that must be run, and tests that are conducted while the system is configured.
Summary	Select Finish .

Add Server Nodes for Validation

This topic describes how to select computers during validating a cluster configuration.

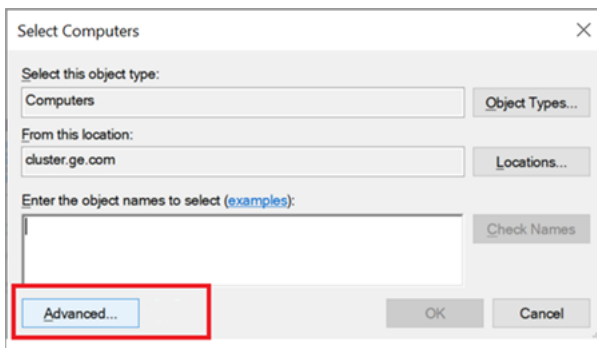
In the following steps, `UAAHANODE1` (Node1 server name) and `UAAHANODE2` (Node2 server name) are used as example server nodes in a cluster.

1. On the **Select Servers or a Cluster** tab, select **Browse**.

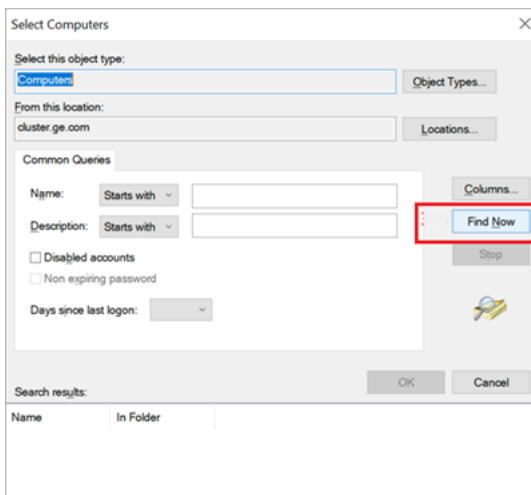


The **Select Computers** screen appears.

2. Select **Advanced**.

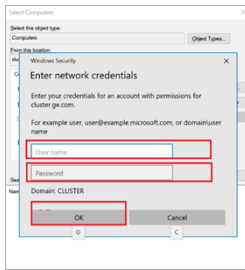


3. Select **Find Now**.



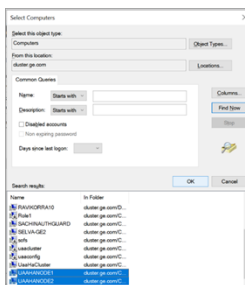
A screen appears prompting to enter the network credentials.

4. Enter the user name and password of the domain where the cluster validation is being performed, and select **OK**.



After successful login, you can see the associated nodes.

5. Select **UAAHANODE1** and **UAAHANODE2**, and select **OK**.



6. Select **OK** to exit.



Configure Role

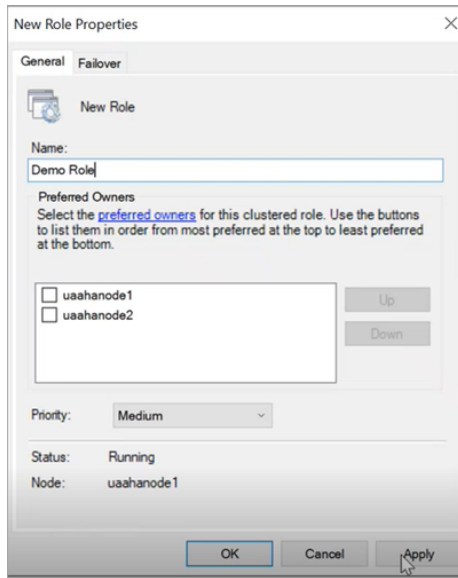
This topic describes how to configure a highly available virtual machine.

In failover cluster technology, each highly available virtual machine is considered to be a role.

You can perform the following steps on either Node1 or Node2. Suppose you perform these steps on Node1, they are automatically applied to Node2.


1. Log in to any of the iSCSI initiator nodes.
2. Go to **Start > Administrative Tools > Failover Cluster Manager**.
3. In Failover Cluster Manager, expand your cluster name and go to **Storage > Disks**.
The cluster name is the unique name entered when creating your cluster. Refer to step 6 in [Create a Cluster \(on page 135\)](#).
4. Right-click **Disks** and select **Add Disk**.
The **Add Disks to a Cluster** screen appears.

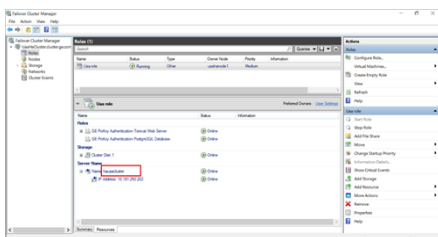
5. Select the disk you want to add, and select **OK**.
6. In Failover Cluster Manager, expand your cluster name and select **Roles**.
7. Right-click **Roles** and select **Create Empty Role**.
The newly created role appears in the Roles pane with the name `New Role`.
8. Right-click `New Role` and select **Properties**.
The **New Role Properties** screen appears.
9. Enter a name for the new role, and select **Apply**.
You can assign the role to multiple node servers and set an order of preference.
For example, the new name is `Demo Role`.



10. Right-click `Demo Role` and select **Add Storage**.
The **Add Storage** screen appears.
11. Select the storage that is already associated to the cluster, and select **OK**.
12. Right-click `Demo Role` and select **Add Resource > Client Access Point**.
13. Complete **New Resource Wizard** with the following options.

Section	What To Do
Client Access Point	<p>Enter a name. For example, <code>hauaacluster</code></p> <p>Make a note of this name. You need to provide the fully qualified domain name while installing Proficy Authentication. See step 3a in Configure Proficy Authentication Installation (on page 142). For example, <code>hauaacluster.cluster.ge.com</code> wherein <code>cluster.ge.com</code> is the domain where cluster is installed. Make sure all the initiator nodes are in the same domain name.</p>

Section	What To Do
Confirmation	<p>The network name and IP address are displayed for confirmation.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: After creating this resource, the IP address and the name should be added to the <code>hosts</code> file on the node servers configured for high availability.</p> </div>
Configure Client Access Point	Verifies the validity of the client access point settings and creates a new resource.
Summary	Select Finish .



On the node servers configured for high availability, go to `..\Windows\System32\Drivers\etc\hosts` and open the file in a text editor to add the network IP address and name as follows.

```
<ipaddress>  haaacluster.cluster.ge.com
<ipaddress>  haaacluster
```

In the above example, `<ipaddress>` should be replaced with the actual ip address of your machine.

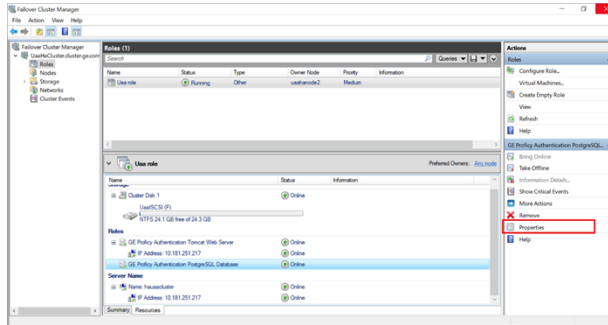
14. Right-click `Demo Role` and select **Add Resource > Generic Service**.
15. Complete **New Resource Wizard** with the following options:

Section	What To Do
Select Service	In the services list, select <code>GE Proficy Authentication Tomcat Web Service</code> .
Confirmation	Skip to the next section.
Configure Generic Service	Skip to the next section.
Summary	Select Finish .

16. Add the dependency service to role using properties of the added service, so that services restart when switching the node (failover condition).

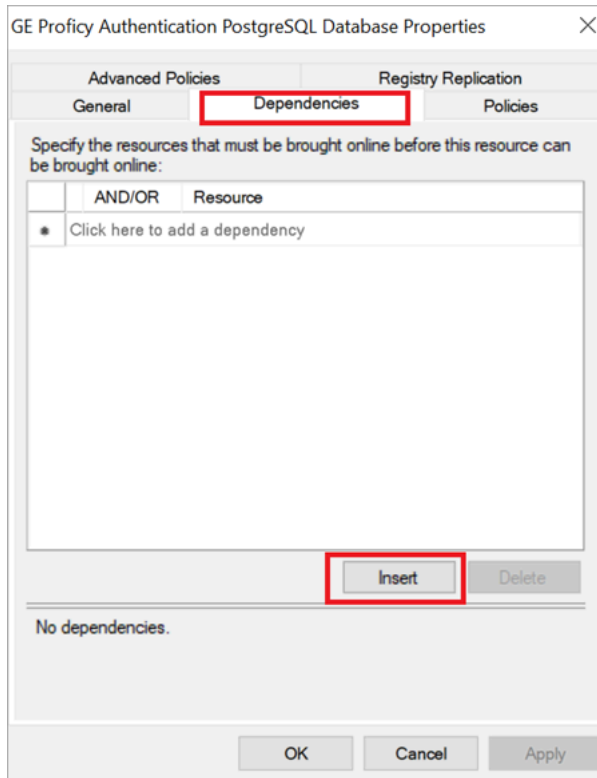
a. In Failover Cluster Manager, select the added service.

b. Select **Properties**.



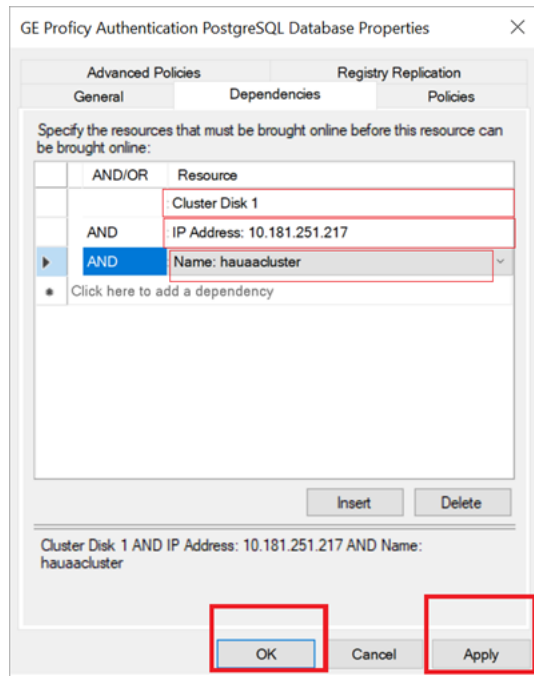
The properties screen for that service appears.

c. Select the **Dependencies** tab, and select **Insert**.



A row is added to specify our required dependencies.

d. From the drop-down, select the required resource one by one to be added as part of dependencies.



e. After inserting the resource, select **Apply** and then **OK**.

Configure Proficy Authentication Installation

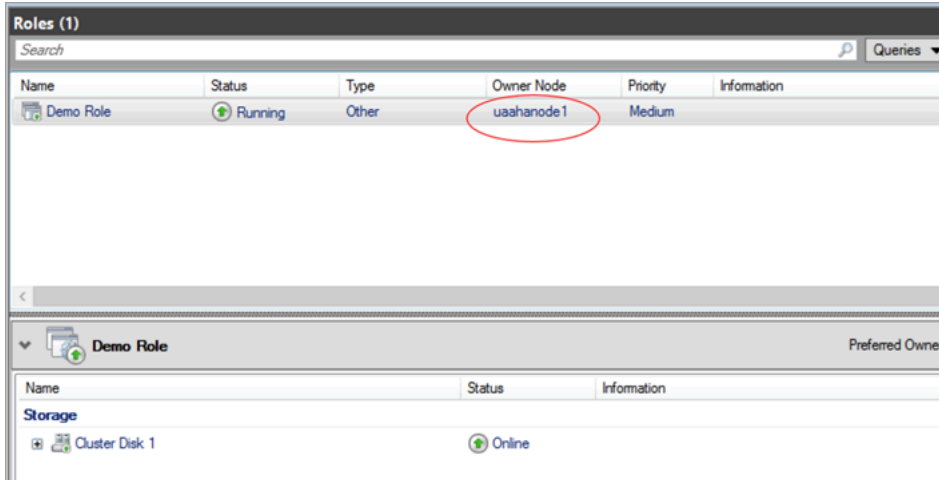
This topic describes Proficy Authentication installation setup in a high available environment.

For fresh installation, you can straightaway proceed with the procedural steps in this topic. But, if you want to use an existing database, do the following before you start with the procedural steps:

1. Copy your Proficy Authentication existing database (found in the Postgress database location) from wherever installed to the shared drive created using the iSCSI server. When you copy, make sure the cluster is pointing to the drive before copying the database. For example, if the cluster is pointing to Node1, then copy the database to Node1.
2. Make a note of the location path where you copied the database in the iSCSI server. For example, `F:\UaaConf`. You need to provide this path for installing Proficy Authentication on Node1 and Node2 machines.

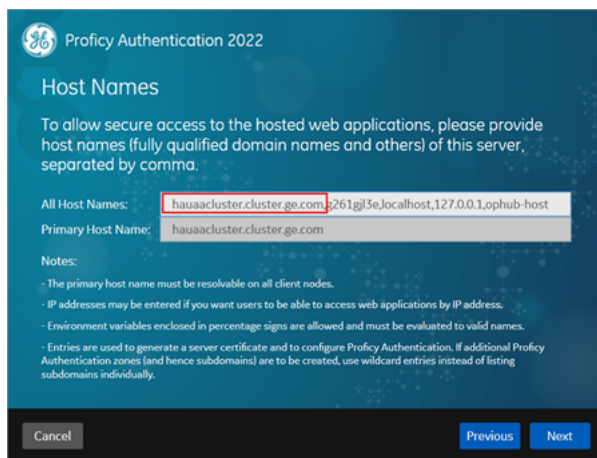
To install Proficy Authentication on the iSCSI initiators (Node1 and Node2), make sure the shared drive is available on the node where you want to run the installation.

1. Log in to the iSCSI initiator Node1 server.
2. Open Failover Cluster Manager and verify that the cluster role is associated to the node where you want to install Proficy Authentication.



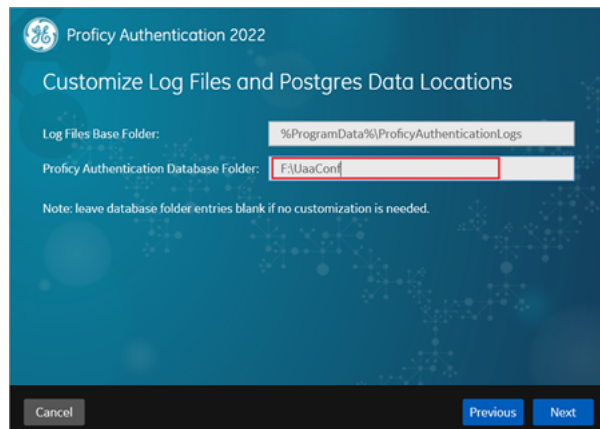
If not, then follow these steps to associate the node server:

- a. Right-click your cluster role and select **Select Node**.
The **Move Clustered Role** screen appears.
 - b. Select the Node1 server, and select **OK**.
Once the cluster is mapped to Node1, the shared drive is available on Node1.
3. Run Proficy Authentication installation setup, and provide these details for the respective screens:
- a. In **All Host Names** field, enter `hauaacluster.cluster.ge.com` as the leading hostname, followed by any other hostname/s.



- b. This step applies for associating existing database. Enter the iSCSI server shared drive location path where you copied the Proficy Authentication database. Refer to the [steps at the beginning of this topic \(on page 142\)](#).

For example, `F:\UaaConf`

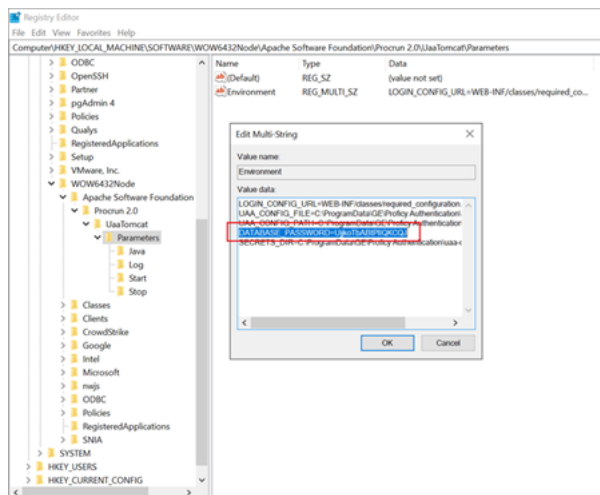


4. Log in to the iSCSI initiator Node2 server, and repeat the above steps to install Proficy Authentication on Node2.
5. After installing Proficy Authentication on both the nodes, copy the `DATABASE_PASSWORD` registry key from the last installed node to overwrite the registry key in the first installed node.

For example, in the following scenario:

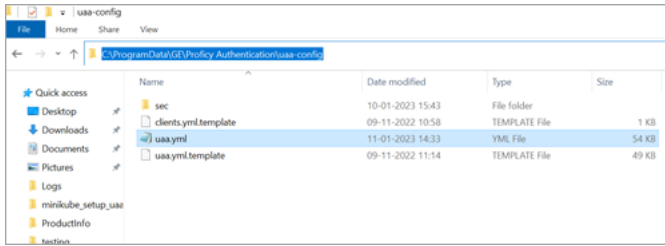
- a. First Proficy Authentication is installed successfully on the Node1 machine.
- b. Next Proficy Authentication is installed successfully on the Node2 machine.

Node2 is considered as the latest installation. Node1 is considered as the first installation. So, copy the Node2 registry key and overwrite the Node1 registry key.



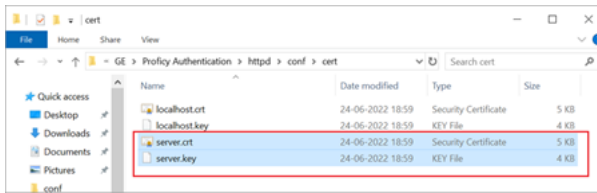
6. Copy and replace the `UAA.yaml` file from Node 2 (latest installation) to Node 1 (first installation).

The file is located here `C:\ProgramData\Proficy\Proficy Authentication\uaa-config`



7. Copy `server.crt` and `server.key` from Node 2 (latest installation) to Node 1 (first installation).

The certificates are located here: `C:\Program Files\Proficy\Proficy Authentication\httpd\conf\cert`

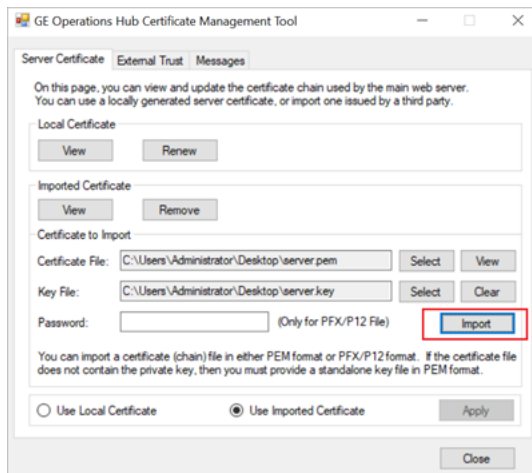


8. After copying the certificates (to Node1), rename `server.crt` to `server.pem`.



9. Open **Certificate Management Tool** on Node1 from the desktop shortcut, and import the certificates as follows:

- a. For **Certificate File**, select the `server.pem` file created in the earlier step.
- b. For **Key File**, select the `server.key` file.
- c. Select **Import**.



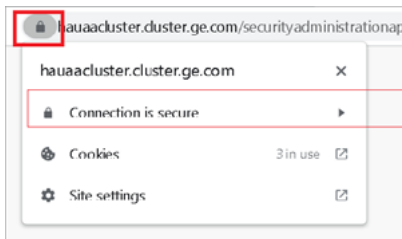
Prerequisites for Installing Operations Hub with External Proficy Authentication

This topic describes how to install Operations Hub with external Proficy Authentication in a high available environment.

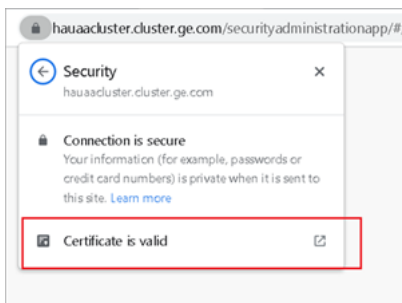
Set up a high available environment. See [Configure High Availability for Proficy Authentication \(on page 128\)](#).

These steps apply for installing Operations Hub with external Proficy Authentication. The steps include mandatory changes prior to installing Operations Hub on any highly available server.

1. Log in to the node server where you want to install Operations Hub.
2. Open a browser and enter `https://hauacluster.cluster.ge.com /securityadministrationapp/`
3. Select the lock icon next to the web address, and then select **Connection is secure**.

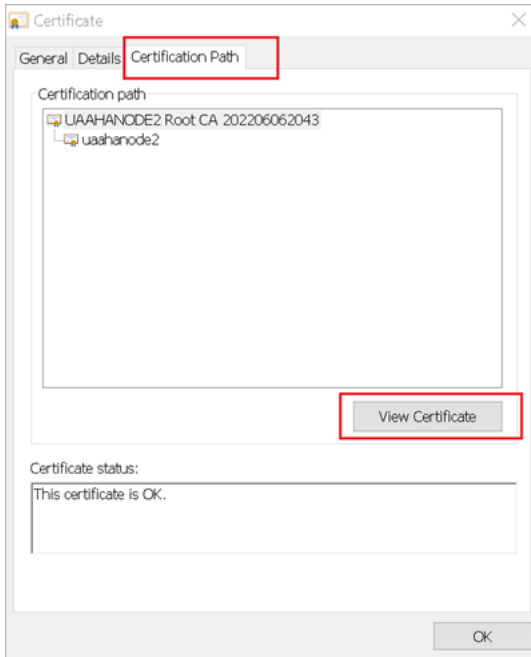


4. Select **Certificate is valid**.

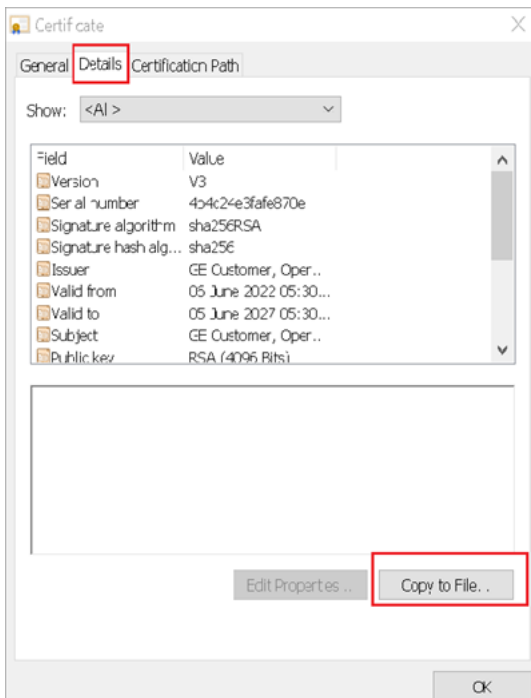


The issued certificate appears.

5. Select **Certificate Path > View Certificate**.

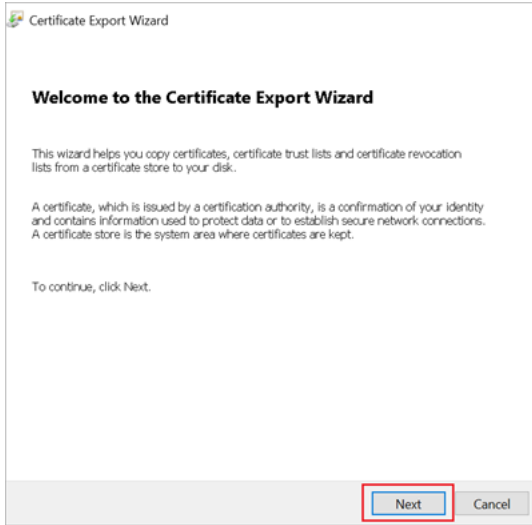


6. Select **Details > Copy to File**.

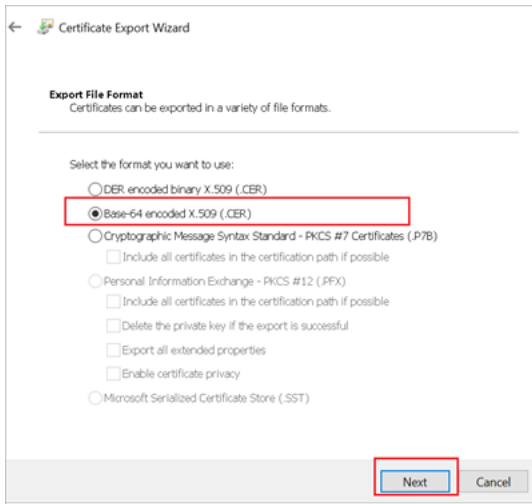


The **Certificate Export Wizard** appears.

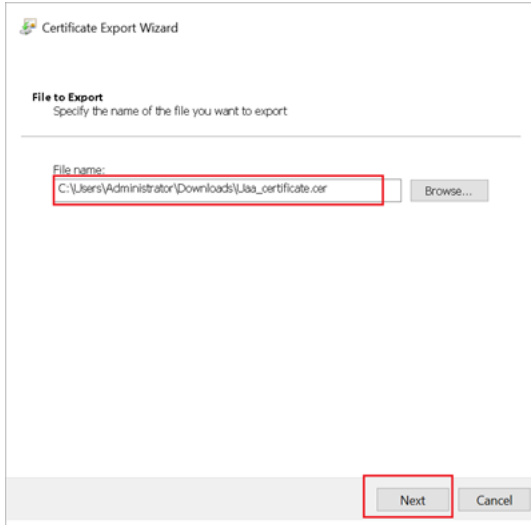
7. Select **Next**.



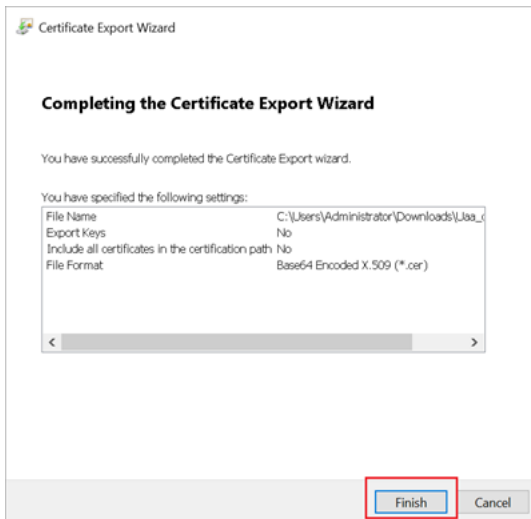
8. Select **Base-64 encoded X.509 (.CER)**, and select **Next**.



9. Browse and specify the file location, and select **Next**.



10. Select **Finish**.

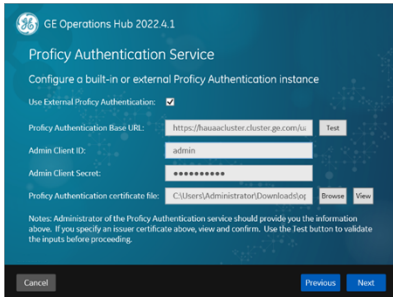


11. Rename `Uaa_certificate.crt` to `Uaa_certificate.pem`.

12. Run Operations Hub installation setup, and provide these details for external Proficy Authentication fields:

Proficy Authentication Base URL	<code>https://hauaacluster.cluster.ge.com/uaa</code>
Admin Client ID	<code>admin</code>

Admin Client Secret	<code>Gei@321itc</code>
----------------------------	-------------------------





Operations Hub is installed successfully.



Customize Login Screen

This topic describes how to customize the Proficy Authentication login screen.

You can customize the company name, logo, favicon, and include additional text/links to appear on the login screen.

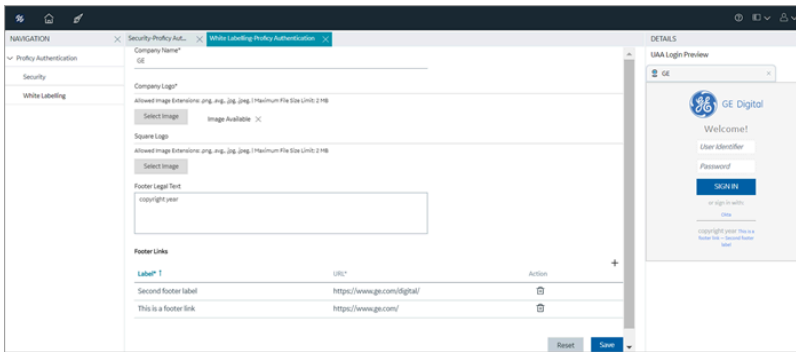
1. Log in to Configuration Hub.
2. Go to **Proficy Authentication > White Labelling**.
The default login screen details appear.
3. Use the following fields to customize your login screen.
A quick preview appears on the **DETAILS** tab.

Field	Description
Company Name	Name of the company that appears on the login homepage.
Company Logo	Select an image from your local system to upload as company logo. Select  to remove an existing image.
Square Logo	Select an image from your local system to upload as a favicon, which appears on the browser tab. Select  to remove an existing image.
Footer Legal Text	Use this space to enter any legal information.
Footer Links	To add hyperlinks, create a label and provide a URL to connect.

Field	Description
	<p>a. Select  to add a row.</p> <p>b. Enter a label name.</p> <p>c. Enter a URL for the label name.</p> <p>Select  to delete existing labels.</p>

4. Select **Save** to save the updates you made to the login screen appearance.

To undo the saved changes, select **Reset**. The login screen is reset to the previously saved appearance.



5. Restart **GE Proficy Authentication Tomcat Web Server** to apply the changes.

Chapter 3. iFIX

Overview

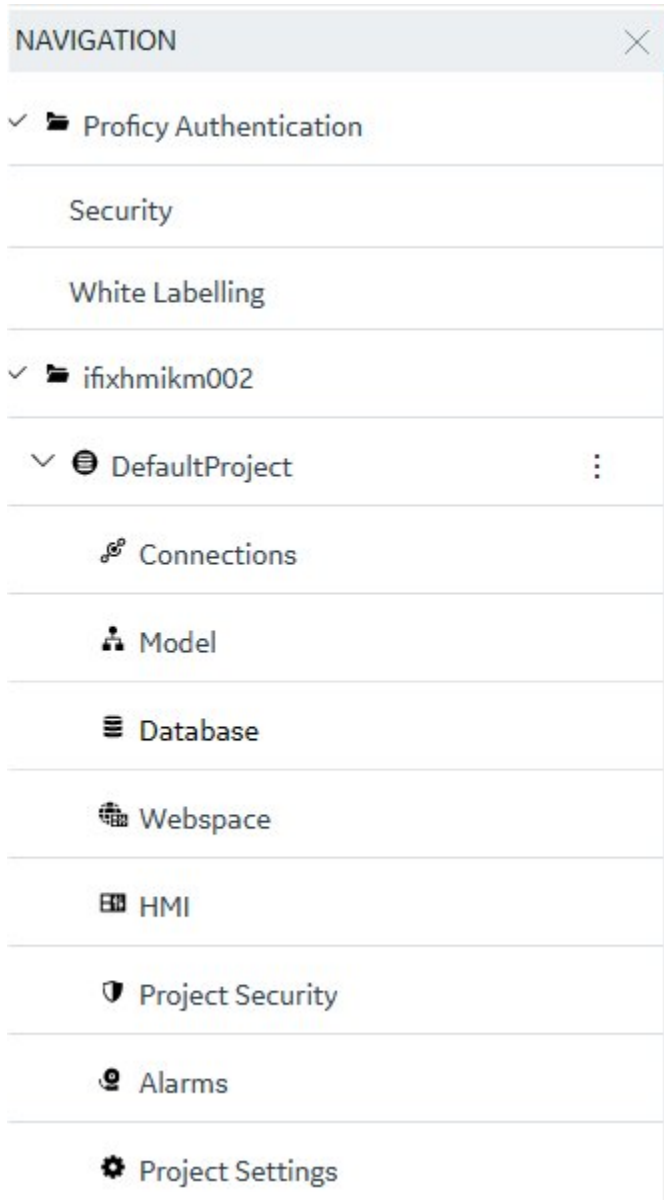
Introduction to iFIX Web Configuration

For iFIX, you can launch Configuration Hub from the Applications ribbon bar in the iFIX WorkSpace.

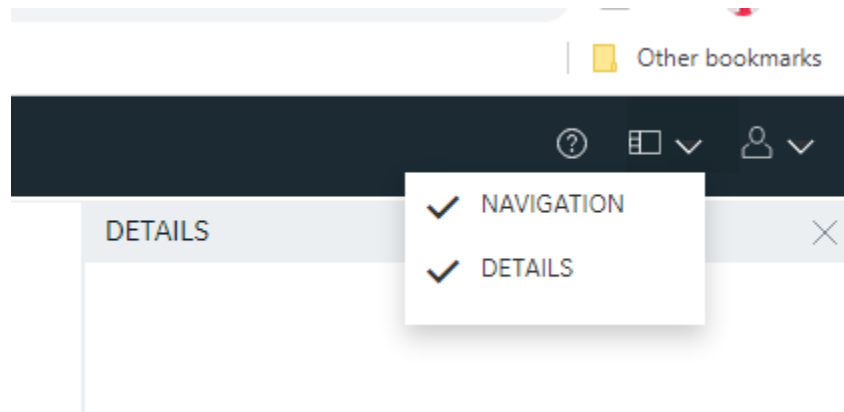


You can also launch Configuration Hub from the icon on your desktop, but be aware that you will get an error message unless you have a running iFIX project.

Use the Navigation panel to open any of the configuration panels.



The Navigation panel can be closed to give you more real estate in your IDE and can be re-opened again from the common toolbar on the top right.



Integrated Development Environment

Integrated Development Environments or "IDE's" are configuration tools that provide flexibility in how you layout a number of panels and tools that work together in building a system. Popular development tools that are IDEs include Microsoft Visual Studio and Jupyter Notebook.

Configuration Hub leverages web technologies to create a panel-based experience for configuring Proficy products that allows you to move, open, close and resize panels in such a way as to reflect the most convenient and efficient way for you to work on your configuration.

The screenshot displays the Configuration Hub interface. On the left is a 'NAVIGATION' sidebar with categories like Security, White Labelling, and Database. The main area shows a table of tags from a database. The table has columns for TAG NAME, STATUS, TYPE, DESCRIPTION, and I/O DRIVER. The first row is selected and highlighted in blue.

TAG NAME	STATUS	TYPE	DESCRIPTION	I/O DRIVER
BLENDER1>MOTOR_OIL	✓	AI	Blender 01 Motor Oil Lev...	IGS
BLENDER1>MOTOR_SPEED	✓	AI	Blender 01 Motor Speed...	IGS
BLENDER1>MOTOR_STATE	✓	DI	Blender 01 Motor State	IGS
BLENDER1>MOTOR_TEMP	✓	AI	Blender 01 Motor Temp	IGS
BLENDER1>NAME	✓	TX	Asset Name	IGS
BLENDER1>TOTAL	✓	AI	Blender 01 Total	IGS
BLENDER1>VALVEIN_STATE	✓	DI	Filler 01 Valve In State	IGS
BLENDER2>MOTOR_OIL	✓	AI	Blender 02 Motor Oil Lev...	IGS
BLENDER2>MOTOR_SPEED	✓	AI	Blender 02 Motor Speed...	IGS
BLENDER2>MOTOR_STATE	✓	DI	Blender 02 Motor State	IGS
BLENDER2>MOTOR_TEMP	✓	AI	Blender 02 Motor Temp	IGS
BLENDER2>NAME	✓	TX	Asset Name	IGS
BLENDER2>TOTAL	✓	AI	Blender 02 Total	IGS
BLENDER2>VALVEIN STATE	✓	DI	Filler 01 Valve In State	IGS

At the bottom of the table, it says 'Tag Count: 41/41' and 'Published I/O Count: 41'. On the right side, a 'DETAILS' panel for the selected tag 'BLENDER1>MOTOR_OIL' is shown, displaying various fields and values such as Tag Name, Description, Type, Current Value (4), I/O Driver (IGS), I/O Address (SIM.PLC_SCADA68.B), and Limits (Low limit: 0, High limit: 1,000).

Prerequisites to Use Configuration Hub with iFIX

The following prerequisites are required in order to use iFIX with Configuration Hub:

1. You must enable security before you can log in to Configuration Hub through the browser.
2. You must use a Proficy Authentication user to login to Configuration Hub. The default user is `ch_admin`, and the default password is your client secret entered at install.
3. The `ch_admin` user should have access to all of the iFIX application features. In Proficy Authentication, include these groups include: `scada.fix_shared_IFIX_PROFICY_AUTH_ADMIN` and `scada.proficy.admin`.
4. You can use either a user's login name or the Full Name to login to Configuration Hub.
5. Configuration Hub can only be run with iFIX SCADA or Historian Server nodes.
6. An iFIX node configured to use Configuration Hub should be registered using the Registration tool (available from Applications menu in Workspace) if Configuration Hub is not installed along with iFIX. See the [iFIX Plugin Registration \(on page 158\)](#) topic for more details.
7. Multiple users can log into the same server and make changes, from different browser sessions.
8. If using Enhanced Failover with iFIX, you must be in Maintenance Mode before you log in to Configuration Hub. (When you enter Maintenance Mode, SCADA synchronization temporarily stops; synchronization between the SCADA pair is suspended.) After Maintenance Mode is enabled, you can make changes to the database on the primary node.
9. The time on Configuration Hub server and the iFIX SCADA node should be synchronized.
10. Use any of the following browsers tested for use with Configuration Hub: Google® Chrome, Microsoft® Edge based on Chromium, Mozilla® Firefox, or Apple® Safari (MAC OS only).

**Note:**

Sometimes the MAC OS cannot resolve the system name. In this case, update the hosts file. Also, on the MAC OS, you will be required to manually install the Configuration Hub root certificate.

Configuration Information

Local and Remote Installations

Configuration Hub supports product registrations local to the same machine as Configuration Hub and as remote plugins. For a remote plugin registration, you do NOT need to install Configuration Hub on the remote computer. Instead, simply use the registration tool on the Application tab in the iFIX WorkSpace. If on a domain, be sure to use the fully qualified domain name in the server name fields.

For example, say you choose to install Configuration Hub on the same machine as iFIX and Historian. Subsequent iFIX and Historian installations on different servers in the same network can be registered with the originally installed Configuration Hub instead of installing Configuration Hub again. This allows

you to open Configuration Hub centrally from a browser and be able to see and configure multiple product instances from that one installed instance of Configuration Hub.

iFIX – When you use the integrated installer to install Configuration Hub, during installation you provide Client ID and Client Secret. You will need to take some additional steps after installation to complete the process, which includes registering the plug-in from the Applications tab on the iFIX WorkSpace ribbon bar. iFIX Security will also need to be enabled. Refer to the [iFIX Plugin Registration \(on page 158\)](#) for more details.

Historian – To register with an existing Configuration Hub during the [Historian Web-based Clients install](#), when prompted, enter the client IDs & client secrets supplied during the original Configuration Hub install. Historian Web-based Clients can be installed on the iFIX node or separately.

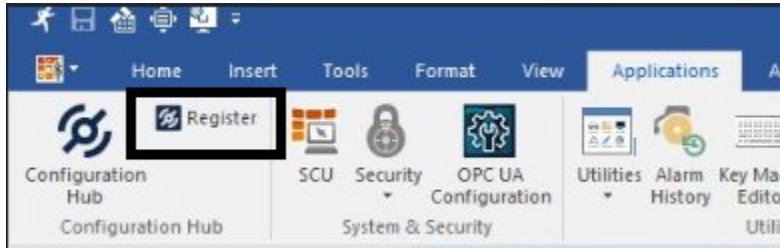
Installation Overview

Use the Common Components option on the integrated installer to install Configuration Hub. Configuration Hub only needs to be installed only once. It does not need to be installed on remote nodes.



iFIX Registration Overview

After installing, you can register the iFIX SCADA with Configuration Hub using the Register option on the Applications toolbar in the iFIX WorkSpace.



Enter the Server name and port and click Test Server Connection to continue. Click the Trusted link to enable the trust between the computers. Enter the Client ID and Client Secret supplied during installation of Configuration Hub to complete the registration.

Configuration Hub Server Registration

Configuration Hub

SERVER NAME



SERVER PORT

Test Server Connection

Create User Friendly Plug-in Name

PLUG-IN ALIAS NAME

Configuration Hub Administration Credentials

CLIENT ID

CLIENT SECRET

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

Proficy Authentication

SERVER NAME



SERVER PORT

Test Server Connection

Proficy Authentication Credentials

Use Configuration Hub Authentication Credentials for Proficy Authentication.

CLIENT ID

CLIENT SECRET

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

Register

Remote Registration Overview

Before you register a remote Configuration Hub, be sure that the latest Microsoft Updates are installed. Remote registration uses the same iFIX Registration process. However, you will most likely need to enter the Server names for Configuration Hub and Proficy Authentication. Use the fully qualified domain name if on a domain.

iFIX Plugin Registration

A registration tool is installed during the iFIX install. This tool allows you to register (in the case of an existing Configuration Hub), or re-register your iFIX product plugin with Configuration Hub when and if your setup changes. iFIX security must be enabled before you can register Configuration Hub.

The following sections describe how to access the Registration Tool and the fields available.

Before you can Register Configuration Hub

- Make sure that users have been added in Windows, and that security is enabled on all of the iFIX SCADAs.
- Be aware that the Configuration Hub web server and the iFIX plugin ports must be allowed in the firewall exception rules during installation. If you do not do this during installation, you will need to add these applications manually to the firewall rules.
- If you are using Configuration Hub on a domain, you may need to update the HOSTS files on your network with the name of the Configuration Hub server, the iFIX SCADA Server, and Historian Server (if applicable).

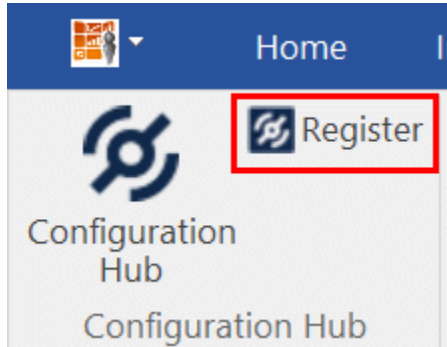


Tip:

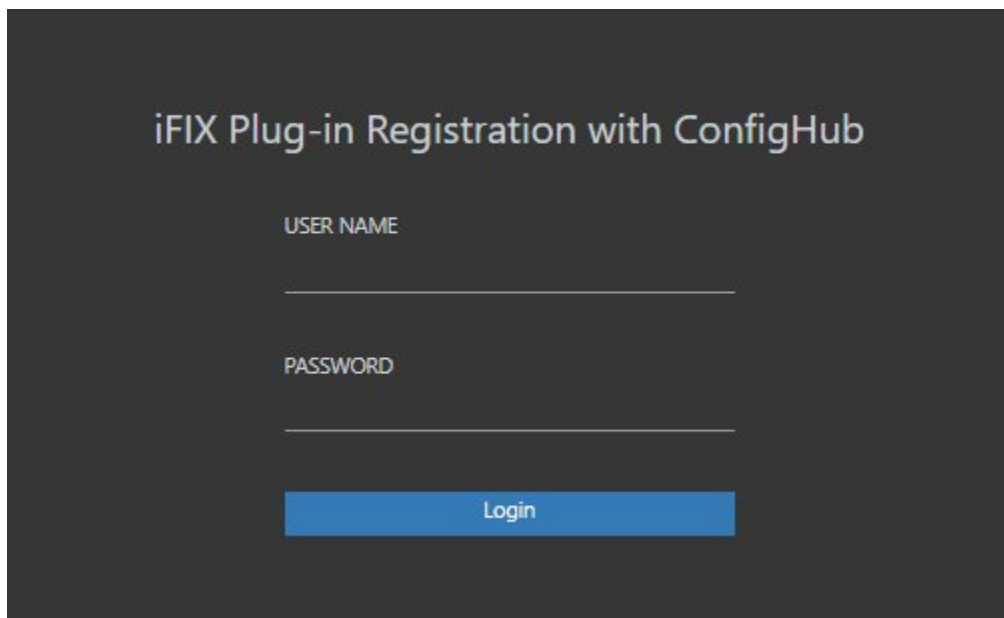
- You can find the HOSTS file in the C:\WINDOWS\system32\drivers\etc folder.
- Depending upon your permissions, you may need to copy this file to another folder, edit it, and then copy it back to the etc folder after your edits are complete.
- Use a text editor such as Notepad to edit the HOSTS file. To prevent Notepad from automatically adding a .TXT file extension when you save the file, in the Save as Type field, select "All Files."
- An example entry in the HOSTS file is as follows: 198.212.170.4 SCADA01. If SCADA1 was the iFIX SCADA Server node name, but the computer name where the iFIX SCADA Server was installed was AREA1, you would need to add a second line to the HOSTS file for AREA1: 198.212.170.4 AREA1.
- If you do not know the TCP/IP address of a computer, run the IPCONFIG command on the SCADA Server to obtain it.
- The contents of the HOSTS file should be identical on each node in your network.
- If your iFIX SCADA Server node name is different from the computer name where iFIX is installed, you also need to add this name to each HOSTS file.
- For Historian, you may need to use the fully qualified domain name (FQDN) in the hosts file of the Web client's machine so it can connect properly to the Configuration Hub machine.

Access the Registration Tool

You can access the Configuration Hub Registration tool from the Windows Desktop, or from the iFIX WorkSpace, on the Applications tab, in the Configuration Hub area. Click **Register** to open the tool.



After you launch it, the following login screen appears.



Enter your iFIX user name and password for authentication. The Registration the tool appears, as shown in the following figure.

Configuration Hub Server Registration

Configuration Hub

SERVER NAME



SERVER PORT

Create User Friendly Plug-in Name

PLUG-IN ALIAS NAME

Configuration Hub Administration Credentials

CLIENT ID

CLIENT SECRET

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

Proficy Authentication

SERVER NAME



SERVER PORT

Proficy Authentication Credentials

Use Configuration Hub Authentication Credentials for Proficy Authentication.

CLIENT ID

CLIENT SECRET

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


Test the Connection

For both Configuration Hub and Proficy Authentication, first test the connection. Enter the server's name and port number (if required). If on a domain, use the fully qualified domain name. Click **Test Server Connection**. Confirm that you can connect to both servers.

Trust the Certificates

If the server certificate shows as **Not Trusted** (in blue next to the server's name), click the Not Trusted link next to the server name to establish the trust. Here is an example of what the Not Trusted link looks like next to the Proficy Authentication Server Name field:

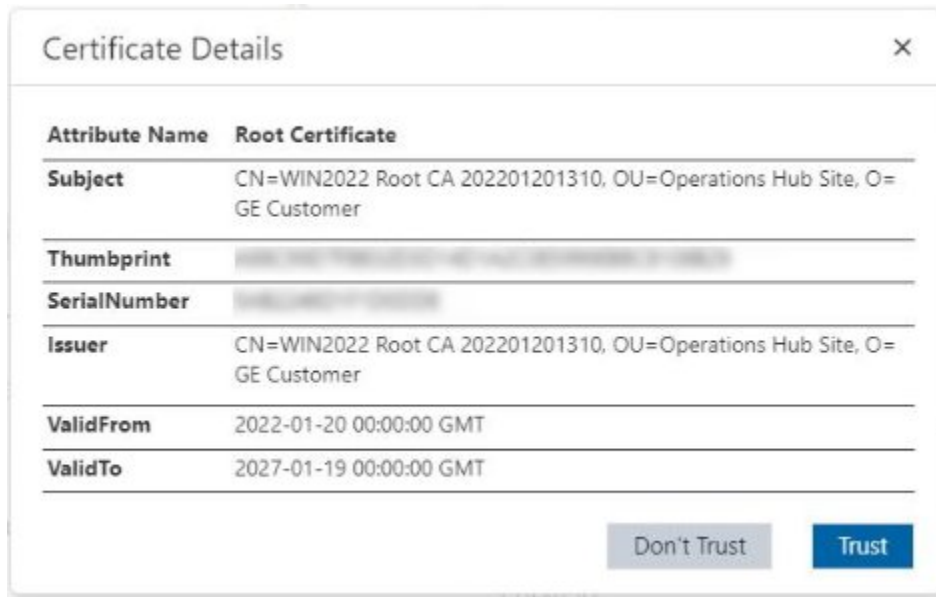
Proficy Authentication

SERVER NAME
win2022  [Not trusted](#)

SERVER PORT
443

Test Server Connection

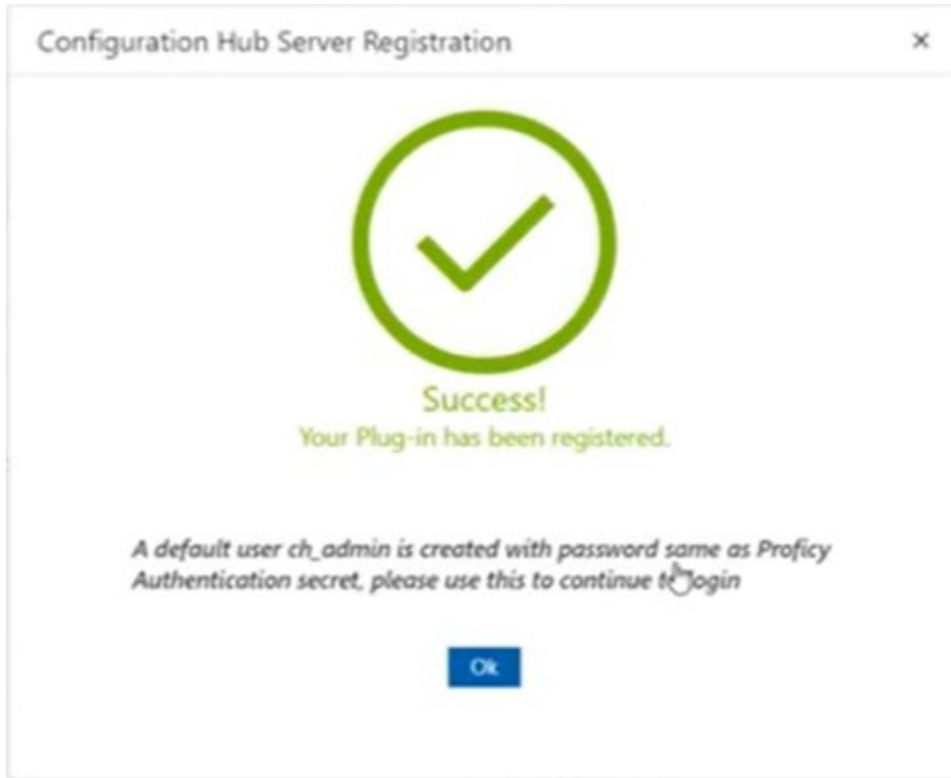
After clicking Not Trusted, the Certificate Details window appears. From the Certificate Details window, click **Trust** to trust the certificate.



Both Configuration Hub and Proficy Authentication must have Trusted certificates before proceeding to register.

Complete the Registration

To complete the registration for Configuration Hub and Proficy Authentication, for both servers, supply the client IDs and client secrets entered during the common component install, and then click **Register**. When registration is complete, the following screen appears.



Login to Configuration Hub and Configure the User

You can now login to Configuration Hub with the **ch_admin** user. Use the client secret supplied when you installed Proficy Authentication as the password.


Add the **scada.fix.shared.APPLICATION_DESIGNER** group to the user for iFIX access in Configuration Hub access, and the **scada.fix_shared_IFIX_PROFICY_AUTH_ADMIN** group to provide access for to all iFIX features (iFIX administrator access).

Logout of Configuration Hub and log back in to start using iFIX features in Configuration Hub.

Descriptions of Fields Available in Registration Tool

The following fields appear in the Configuration Hub Registration tool:

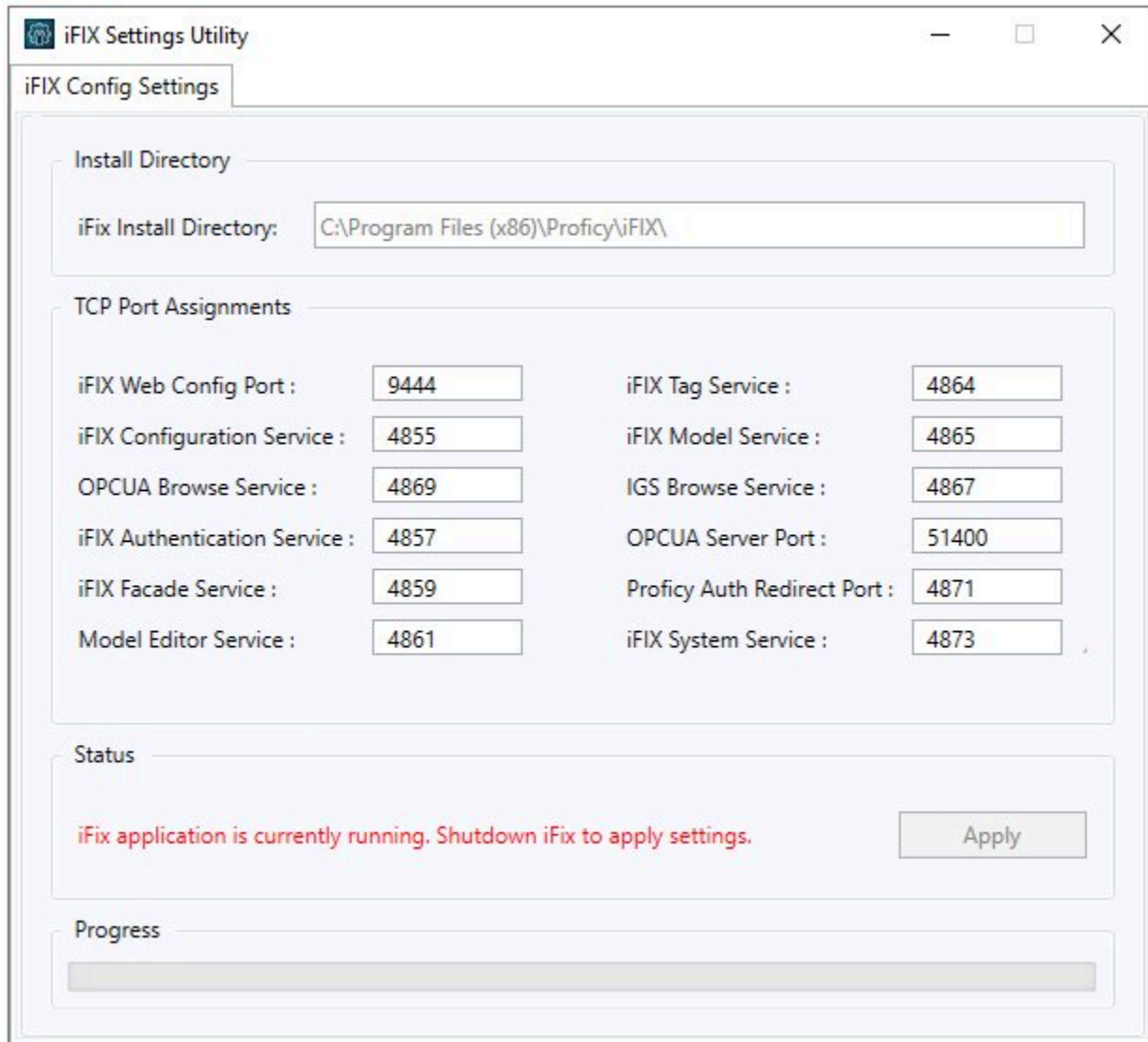
Field	Description
Server Name	The server's name for the Configuration Hub or Proficy Authentication server. When using a network domain, provide the full domain name.

Field	Description
	You must supply valid current credentials (Client ID and secret) to register.
Server Port	Displays the port associated with the Configuration Hub or Proficy Authentication server.
Client ID	Displays the Client ID for your Configuration Hub or Proficy Authentication server. The Client ID and Client Secret was created when you installed the Configuration Hub product.
Client Secret	<p>The client secret associated with the Configuration Hub or Proficy Authentication server. The Client ID and Client Secret was created when you installed the product.</p> <p>You will need to enter the Client Secret if you want to change the server's name (update), unregister, or register your Configuration Hub web server.</p> <div data-bbox="820 1031 1421 1434" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: If you forget your client ID or secret, you will not be able to register/unregister plug-ins with Configuration Hub or Proficy Authentication. In this case, you would need to reinstall Configuration Hub and/or Proficy Authentication and register all of all the plug-ins again in order to change them.</p> </div>
Use Configuration Hub Authentication Credentials for Proficy Authentication check box	Select this check box if you had entered same credentials (Client ID and Client Secret) for both Configuration Hub and Proficy Authentication during installation.
Update button	Click this button to save changes entered in this wizard. To save your changes, You must enter the Client ID and Client Secret information that you entered when you installed the product.

Field	Description
Register button	<p>Click to register your Configuration Hub and Proficy Authentication server. This button is only available if the Configuration Hub or Proficy Authentication web server is in an unregistered state.</p> <p>To register Configuration Hub and Proficy Authentication , you'll need the Client ID and Client Secret information that you entered when you installed the product.</p>
Unregister button	<p>Click to unregister your Configuration Hub web server. This button is only available if the Configuration Hub or Proficy Authentication web server is in a registered state.</p> <p>To unregister Configuration Hub, you'll need the Client ID and Client Secret information that you entered when you installed the product.</p>

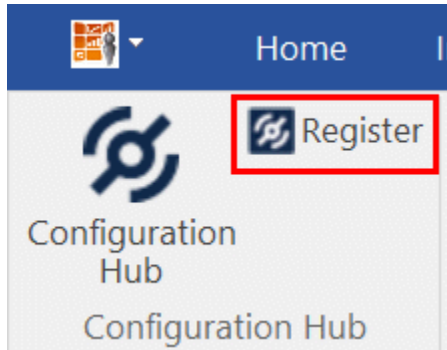
Port Changes for iFIX after Configuration Hub Install

If you need to change the ports used by iFIX after install, use the **iFIXConfighubSettingsUtility.exe** utility found in the iFIX folder (by default this folder is: C:\Program Files (x86)\Proficy\iFIX) to reset them. This change must be done only when iFIX is NOT running.



Note:

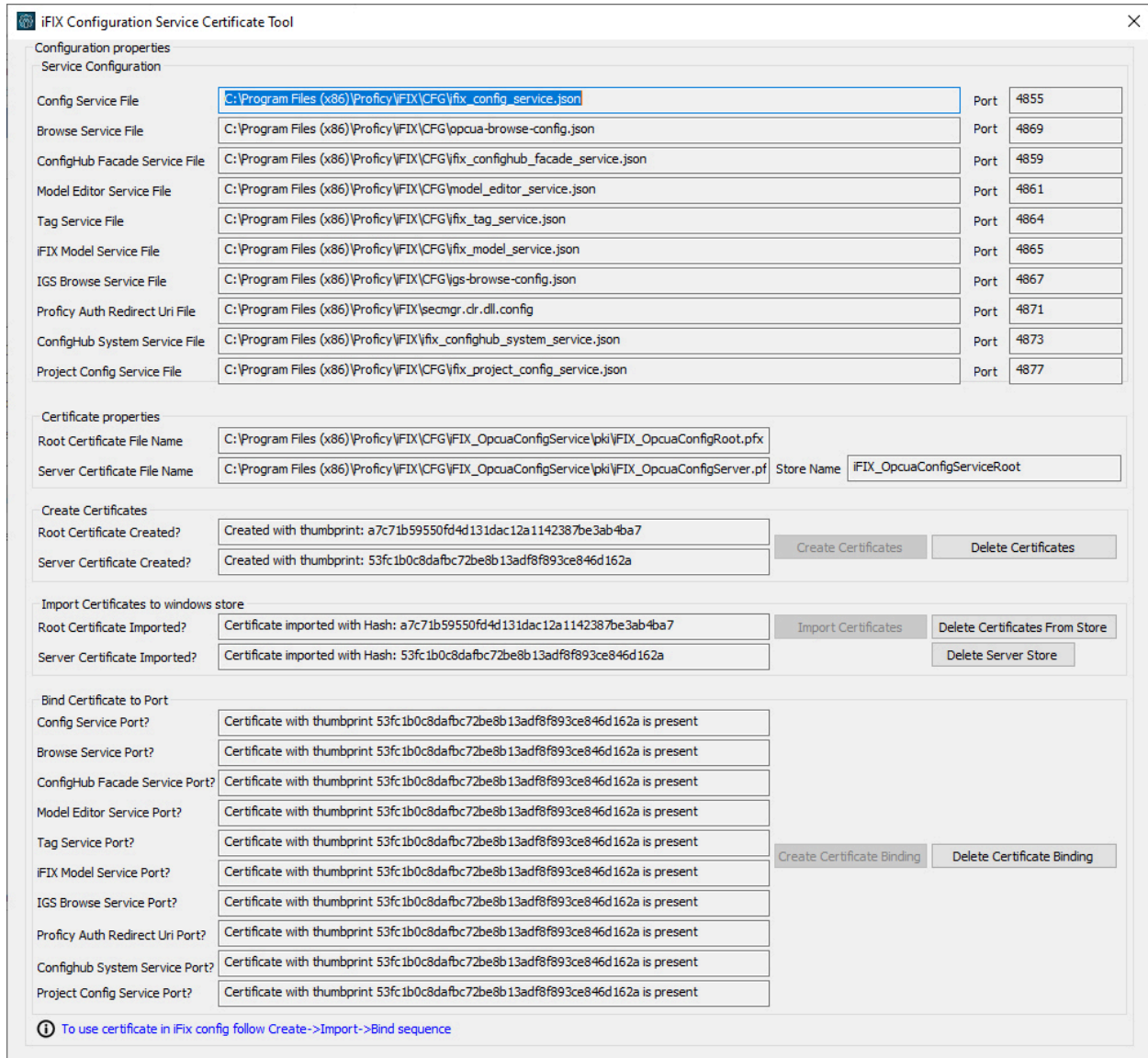
If you are planning to update iFIX Web Config Port, you must first unregister the iFIX Plugin with ConfigHub. If any of the other service ports are changed, then there is no unregister/register needed.



If the iFIX Web Config Port changed, then you must register the iFIX plugin again with Configuration Hub using the Register button in the iFIX WorkSpace. See the [iFIX Plugin Registration \(on page 158\)](#) for more details.

With the exception of the iFIX Web Config and OPCUA Service ports, if any other service ports are changed, then you must run the **iFixConfigServiceCertTool.exe** tool (shown in the following figure) to bind the certificates to the changed ports found in C:\Program Files (x86)\Proficy\iFIX. Please note that this utility must be run as an administrator only.

If any ports are changed, the iFIX Configuration Service Certificate tool shows the updated ports as “No certificate binding is not present.” Click the Create Certificate Binding button to add the necessary port binding.



After the binding is complete, close the utility and restart iFIX. The changed ports then will be used by the iFIX.

Upgrading Configuration Hub

If upgrading from a previous version of Configuration Hub, be sure to clear your browser cache and re-register the iFIX Plugin (click the Register iFIX Plugin on the desktop). Be aware that iFIX Security must be enabled to access. For steps, refer to [iFIX Plugin Registration \(on page 158\)](#).


Also, be aware that the `scada.fix.shared.APPLICATION_DESIGNER` group is not available by default when you upgrade from iFIX 2022 or earlier. You must manually create the group with the required iFIX

application features, or update your existing groups to include the following iFIX application features (if you want users in these groups to have access to and use Configuration Hub):

- Database Block Add-Delete
- Database Manager
- Database Reload
- Database Save
- Security Configuration
- System Configuration

If you create a new user in Proficy Authentication Security, be sure to add these two groups in order to get full access to iFIX in Configuration Hub: `scada.project.admin` and `iFIX_PROFICY_AUTH_ADMIN`.

Access iFIX Web Configuration

1. In the iFIX WorkSpace, select the Applications ribbon and click Configuration Hub Or, on the desktop, click the Configuration Hub icon ()



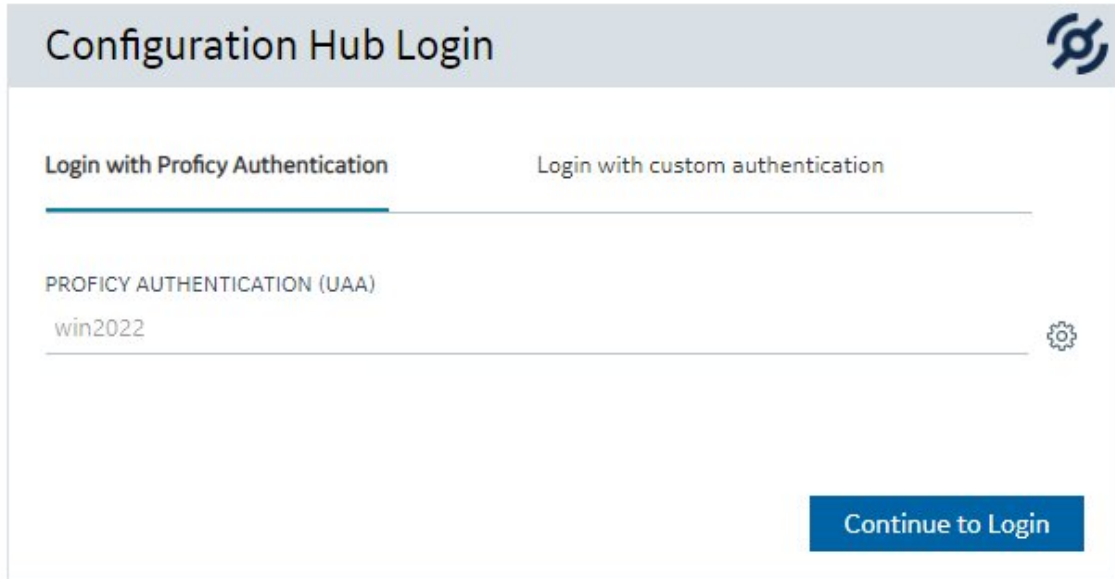
Note:

If using the desktop icon, confirm that iFIX is running, and you are logged into iFIX.

When using the iFIX plugin, the login page expects credentials that are configured for Proficy Authentication. The user should be a member of the **scada.fix.shared.APPLICATION_DESIGNER** group in Proficy Authentication to have all the permissions necessary to use Configuration Hub.

The Configuration Hub Login screen appears.

2. Select **Continue to Login**.



The iFIX Authentication screen appears.

3. Enter the Proficy Authentication user name and password, and click Sign In.



**Note:**

If this is your first time logging in, use the **ch_admin** login with the client secret that you entered during install as the password. The ch_admin is the default user.

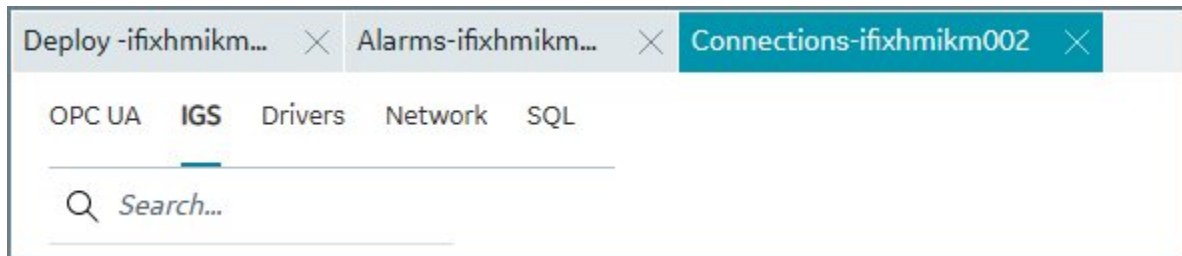
After a successful authentication, the Configuration Hub screen appears.

Connections

Connections Overview

Connections are where you establish connections to the data you want to collect and bring into iFIX. Current available options are OPC UA, IGS, Driver, Network, and SQL.

In the Navigation panel, select your iFIX node, and then Connections, and then select the option at the top of the main panel.



For more detailed information, see:

- [OPC UA Connections \(on page 171\)](#)
- [IGS Connections \(on page 183\)](#)
- [Drivers \(on page 191\)](#)
- [Network Connections \(on page 193\)](#)
- [SQL Connections \(on page 200\)](#)

OPC UA Connections

OPC UA Connections

iFIX offers an OPC UA Client Driver option that allows you to connect to OPC UA Servers.

Overview of OPC UA Connections

If you want to connect to an OPC UA server from a newly created project in Configuration Hub, make sure that the certificate is to the server is validated, else the test connection with the OPCUA server will fail.

To use this feature in Configuration Hub:

- Your running iFIX SCADA node must be licensed for this option.
- You must have valid certificate for iFIX to act as an OPC UA server or as OPC UA client.

Steps to Add a Certified Connection

To create a new connection with a valid certificate:

1. Start iFIX.
2. Open the **SCU app** and verify that the OPC UA Client was added in the SCADA Configuration. If not, add the OPC UA Client Driver to SCADA node (in the SCADA Configuration dialog box).
3. Save the SCU file and restart the iFIX.
4. From the iFIX WorkSpace, on the Applications tab, select the **OPC UA Configuration** tool.
5. Click the **Certificate** tab.
6. Select the **Generate Self-Signed** certificate button.
7. Click **Save and Exit**.
8. From Configuration Hub, in the Navigation panel select the node, the project, and then **Connections**.
9. Select the **OPC UA** connection option.
10. Click **New** to create a new connection. Type in the unique server name and the end point URL of your OPC UA Server. For example: `opc.tcp://myserver:51400/`.



Note:

If you do not know this path and port, you can obtain it by opening the iFIX WorkSpace, selecting the Application tab, and clicking OPC UA Configuration. When the tool opens, on the Server tab, you can find the Endpoint URL and copy it so that you can paste it in the Endpoint URL field in The New OPC UA Server Connection dialog box in Configuration Hub.

11. Click **Test** to test the connection. The connection should succeed.
12. After you get a successful connection, click **Create** to add the connection.

Working with OPC UA Connections

After your connection is created, it appears in the table. Click the ellipsis (...) to the right of your entry to interact with the server.

The screenshot displays the 'Connections' tab in the Configuration Hub. The main area shows a table with the following data:

SERVER NAME	STATUS	END POINT	
unified_auto	✓	opc.tcp://WIN10:48010	⋮
<ul style="list-style-type: none"> Groups 			

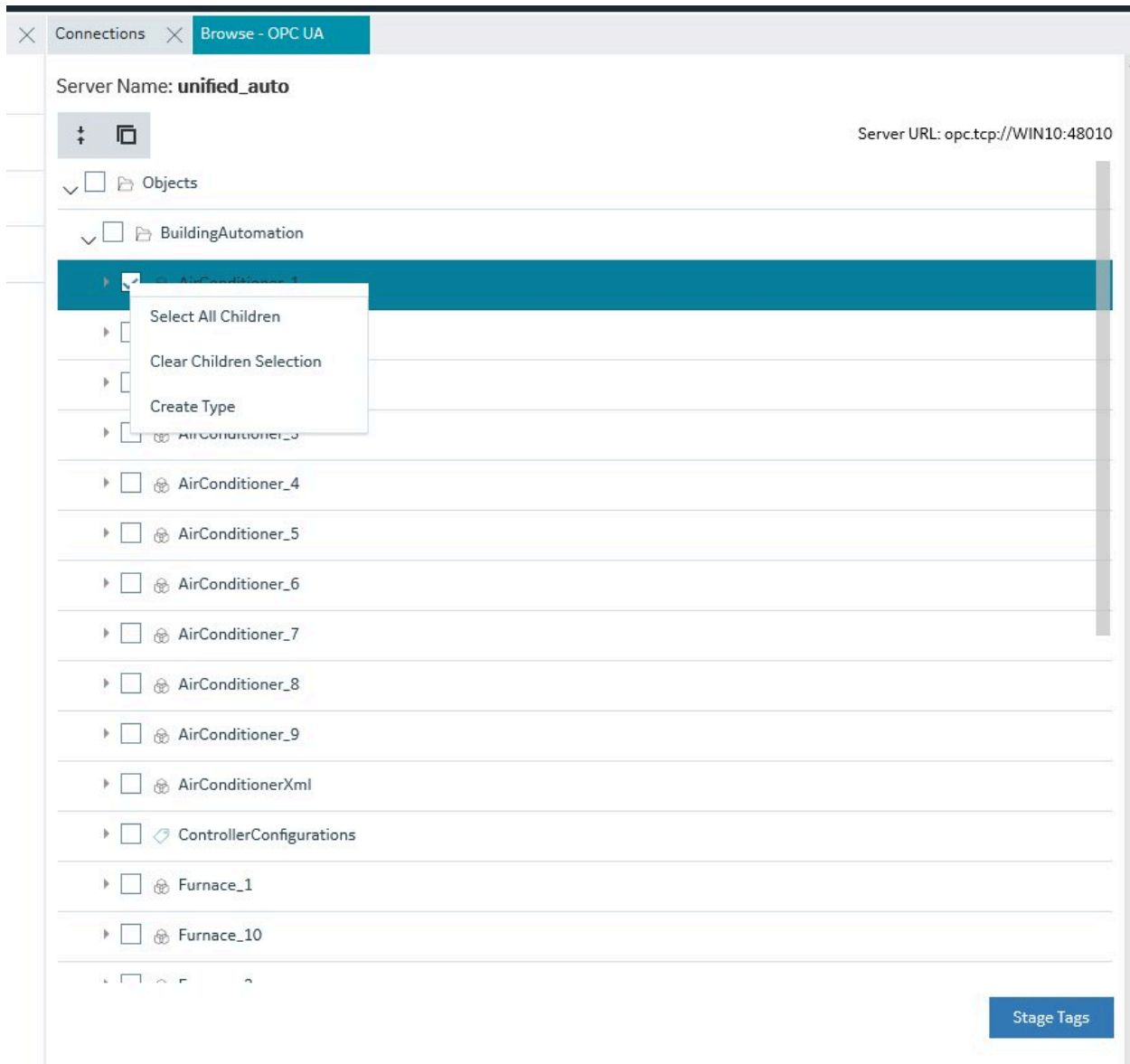
The context menu for the 'unified_auto' connection includes the following options:

- Browse
- Delete
- Create Group
- Refresh
- Driver Tags

The right sidebar shows the 'DETAILS' for the selected connection, including a search bar and sections for 'AUTHENTICATION' (User Credentials) and 'CONNECTION DE' (server Name, endpoint Urls, security Mode, security Policy Ur, disabled, REDUNDANCY, Redundancy Supr).

From the popup menu, select Browse to browse the hierarchy available in the OPC UA Server.

From here you can select individual tags to populate your iFIX Database, or select higher level object and create a new object type for your iFIX model. For example, you can right-click on an Object row to bring up a sub-menu, and then select Create Type.



Server Management

OPC UA Server connections can be edited using the Details panel. After selecting a server configuration in the Connections panel, the Details panel populates the server connection information.

The ENDPOINT URL field takes the host name or IP address and port used to connect with the OPC UA Server. For example: `opc.tcp://MyServer:51400/`. The format of this URL (with the machine name, IP address, or fully qualified domain name) is defined on the OPC UA Server.

The authentication type can be set to Anonymous or UserName/Password. It is recommended that you select UserName/Password to provide the highest level of security. Anonymous does not provide any protection for accessing data or logging.

If the UserName/Password option is selected, enter the user name and password to connect to the OPC UA Server.

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

In addition to editing a server connection, the connections panel supports creating groups under the server connections and deleting them. When an OPC UA server connection is created, a default group is created.

Groups under a server connection allows you to configure the publishing interval, and sampling interval. Any application requesting data from the OPC UA Server uses group names to access items in the group. Group names can be up to 19 alphanumeric characters including underscores (_) and hyphens (-).

The screenshot shows the 'Connections' panel with a table of server connections and a 'DETAILS' panel for a selected group.

SERVER NAME	STATUS	END POINT
UACPPServer	✔	opc.tcp://DESKTOP-AKOV2NU:48010
Group_1		
UADefaultServer	✔	opc.tcp://DESKTOP-AKOV2NU:48010

The 'DETAILS' panel for 'Group_1' shows the following configuration:

FIELD	VALUE
Name	Group_1
PublishingInterval	250
SamplingInterval	1000

Testing Connections



Test Connection function is provided on the OPC UA server connection's Details panel. The test

connection function is initiated from the toolbar button




The test makes an attempt to reach to the end point URL provided in the Connection Details panel and on successful connection comes back with the test status and populates into the end point URL field with a check mark; on failure to connect the same field is highlighted in red with failure a reason.

The following figure displays a successful test.

DETAILS ✕	
UACPPServer	
<input type="text" value="Search..."/>  	
FIELD	VALUE
<div style="background-color: #f2f2f2; padding: 2px;"> ▼ AUTHENTICATION </div>	
User Credentials	Anonymous
<div style="background-color: #f2f2f2; padding: 2px;"> ▼ CONNECTION DETAILS </div>	
Server Name	UACPPServer
Endpoint Urls	✓ opc.tcp://DESKTOP-AK0V2NU:48010
Security Mode	None
Security Policy Uri	None
Disabled	false
<div style="background-color: #f2f2f2; padding: 2px;"> ▼ REDUNDANCY </div>	
Redundancy Support	None
Redundant EndPoint1	
Redundant EndPoint2	
Redundant EndPoint3	

Policy Browse

OPC UA servers are configured with specific security mode and policy. The Details panel of a server connection provides a toolbar button to browse policies  .

On execution of this function, the configured Security mode and Policies from the server are browsed and populated into the respective fields in the Details panel.

Select a Security Model and Security Policy to apply to this connection: Basic128Rsa15, Basic256, Basic256Sha256, Aes128_Sha256_RsaOaep, or Aes256_Sha256_RsaPss.



Note:

If you are not sure what to select for Security Mode and Security Policy or simply want to test a connection, select None. Be sure that you go back and change this setting later, however, to ensure you have adequate security enabled for your connections.

DETAILS
✕

UACPPServer

🔍 *Search...* 🌐 🔗

FIELD	VALUE
▼ AUTHENTICATION	
User Credentials	Anonymous
▼ CONNECTION DETAILS	
Server Name	UACPPServer
Endpoint Urls	opc.tcp://DESKTOP-AK0V2NU:48010
Security Mode	None
Security Policy Uri	None
Disabled	None
▼ REDUNDANCY	
Redundancy Support	Basic256Sha256
Redundant EndPoint1	Aes128_Sha256_RsaOaep
Redundant EndPoint2	Aes256_Sha256_RsaPss
Redundant EndPoint3	

**Note:**

For the connection to work for any other security policy other than None, you will have to ensure the certificates are properly trusted between the iFIX client and the OPC UA server you are communicating to. See the iFIX help for use of the OPC UA tool in iFIX.

Redundancy Configuration

You can specify the redundancy settings for your OPC UA Server connection, if you have this feature enabled on your OPC UA Server. Scroll to view the Redundancy settings on the Details panel for selected OPC UA server Connection tab, as show in the following figure. You can configure Cold, Warm, or Hot redundancy.

DETAILS	
W2019KMM	
<input type="text" value="Search..."/>	
FIELD	VALUE
▼ AUTHENTICATION	
User Credentials	Anonymous
▼ CONNECTION DETAILS	
Server Name	W2019KMM
Endpoint Urls	opc.tcp://W2019KMM:51400/
Security Mode	None
Security Policy Uri	None
Disabled	false
▼ REDUNDANCY	
Redundancy Support	Hot
Redundant EndPoint1	opc.tcp://W2019D:48010/
Redundant EndPoint2	opc.tcp://W2019E:48010/
Redundant EndPoint3	opc.tcp://W2019F:48010/

According to the OPC Foundation: Cold redundancy requires an OPC UA Client to reconnect to a backup server after the initial server has failed. Warm redundancy allows a client to connect to multiple servers, but only one server will be providing data values. In Hot redundancy, subscriptions are created in multiple servers but only 1 server is active and providing data to the client at a time.

You can configure up to 3 backup servers (endpoint URLs).

Browse and Create iFIX Tags for OPC UA

An OPC UA server connection can be browsed to navigate through the address space and select content to create tags into the active iFIX database.

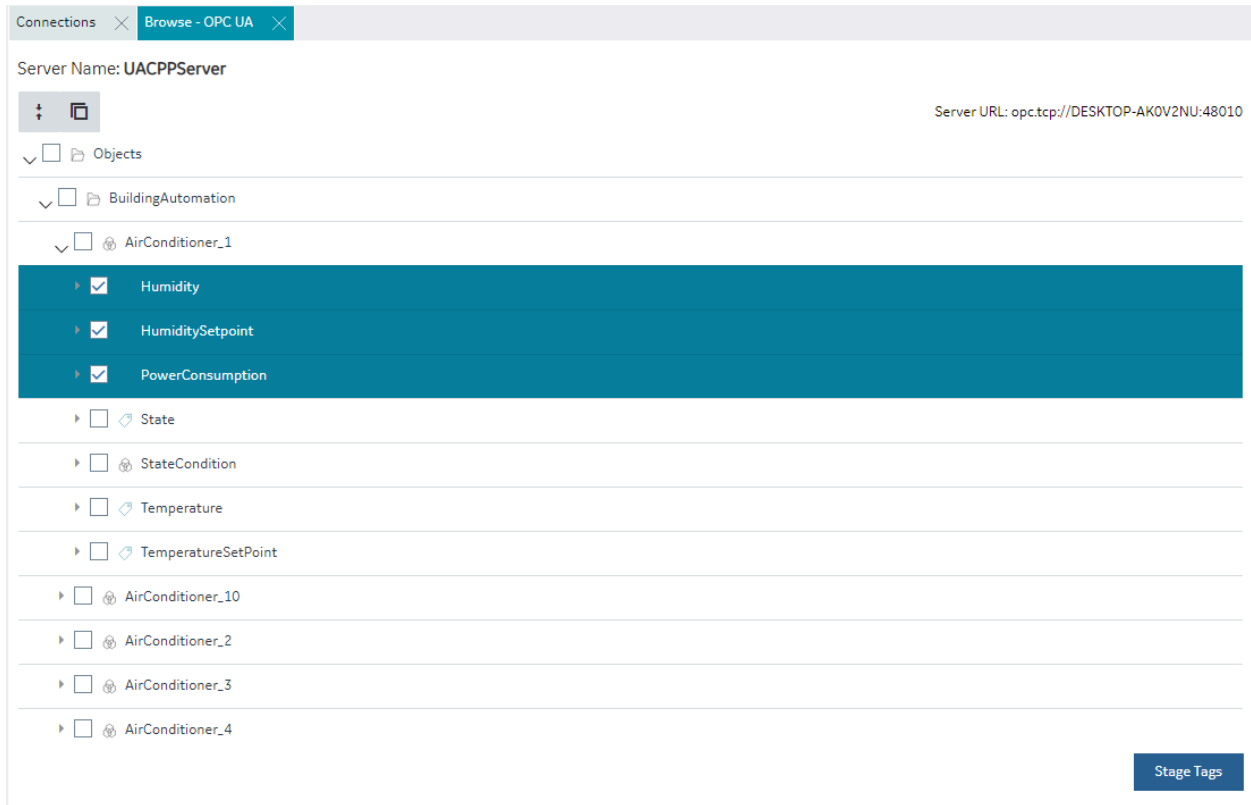
The OPC UA server connection browse is provided through the context menu on the selection of the server connection row.

The screenshot shows the OPC UA configuration interface. At the top, there are navigation tabs: OPC UA, IGS, Drivers, Network, and SQL. Below the tabs is a search bar labeled "Search...". The main area contains a table with the following columns: SERVER NAME, STATUS, and END POINT. The table has two rows: UACPPServer and UADefaultServer. The UACPPServer row is selected and highlighted in blue. A context menu is open over the UACPPServer row, showing options: Browse, Delete, Create Group, Refresh, and Driver Tags. To the right of the table, there is a sidebar with a search bar labeled "Search" and a tree view showing a hierarchy of nodes: FIELD, AUTHI, User C, and CONN. The CONN node is expanded, showing a list of server connections: UACPPServer, dpc, curi, curi, sabl, DUJ, and Redur.

SERVER NAME	STATUS	END POINT
UACPPServer	✓	opc.tcp://DESKTOP-AK0V2NU:48010
UADefaultServer	✓	opc.tcp://DESKTOP-AK0V2NU:48010

The first step in the tag creation process is to browse the OPC UA Server device and select the tags from the browse content. A parent node's right-click menu can be used to selected bulk child tags for creation.



The next step is to stage the tags and preparing the tags for creation into the iFIX database.



The staging environment allows for modifications to tag names, selection of iFIX block type (default mapped on staging) and selecting a tag for Historian collection.

Connections × Browse - OPC UA ×

Staging Area for Tag Creation

Search _____ Name prefix _____ 1  

<input checked="" type="checkbox"/>	IFIX TAG NAME	BLOCK TYPE	GROUP NAME	HISTORIAN	STATUS	RESULT
<input checked="" type="checkbox"/>	BuildingAutomation_AirConditioner_1_Humidity	AI	Group_1	<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/>	BuildingAutomation_AirConditioner_1_HumiditySetpoint	AI	Group_1	<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/>	BuildingAutomation_AirConditioner_1_PowerConsumption	AI	Group_1	<input checked="" type="checkbox"/>		

Browse again Create (3) Tags

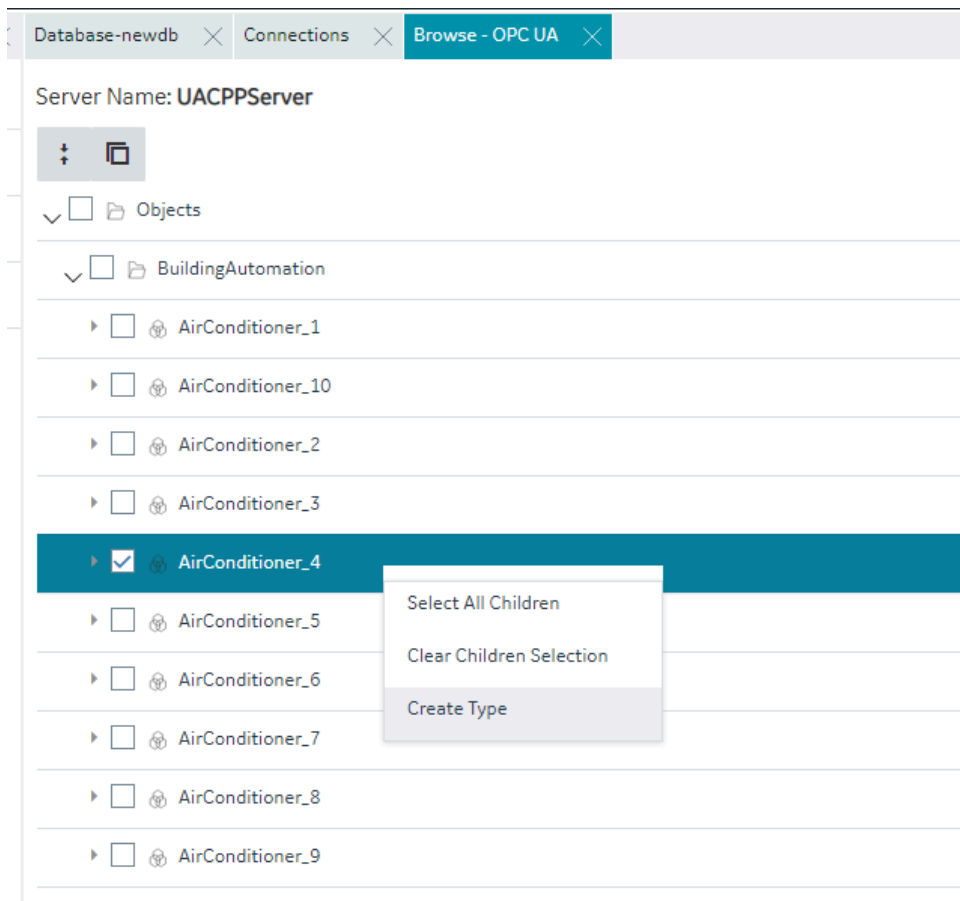
You can automatically generate one or more tags at a time by browsing the OPC UA Server device.

Browse and Create Types for OPC UA

Using the browse functionality on an OPC UA server, you can create new model types from existing types, replicating their variables and if required, any child objects or variable groupings. This allows you to quickly populate the properties of an object type, without having to configure them separately.

To create a new model type based on an existing type:

1. Right-click the existing model type from the **Browse** tab and select **Create Type** from the menu that appears. The **Create Object Type** dialog will appear.



Create Object Type

NAME
AirConditionerControllerType

DESCRIPTION

Include Hierarchy

STATUS:

2. Enter a unique **NAME** for the model type.
3. Enter a **DESCRIPTION** for the model type (optional).
4. The **Include Hierarchy** checkbox provides two options:
 - If left unchecked, only the variables at the level directly below that of the object type would be copied. Any contained assets (child objects or variable groupings) will be ignored when the new model type is created.
 - If the box is checked, all contained assets from all sub-levels, will also be created in the new model type.
5. Click **Create**.
 - If there is a conflict with one of the copied types (that is, it already exists within another asset), the **Create Type Hierarchy** dialog appears.

Create Type Hierarchy

The following types are conflicting. Please select an appropriate action to proceed.

TYPE	ACTION	NEW TYPE NAME
Pump	<input checked="" type="radio"/> Use Existing <input type="radio"/> Create New	

Cancel Continue

At this point you must choose to either:

- **Use Existing:** reuse the type in the new model.
 - **Create New:** if the existing type does not represent the new asset (for example if it has different variables), give it a new, unique name in the **NEW TYPE NAME** field.
- Click **Continue**.
 - Click **Close** in the **Create Object Type** dialog.

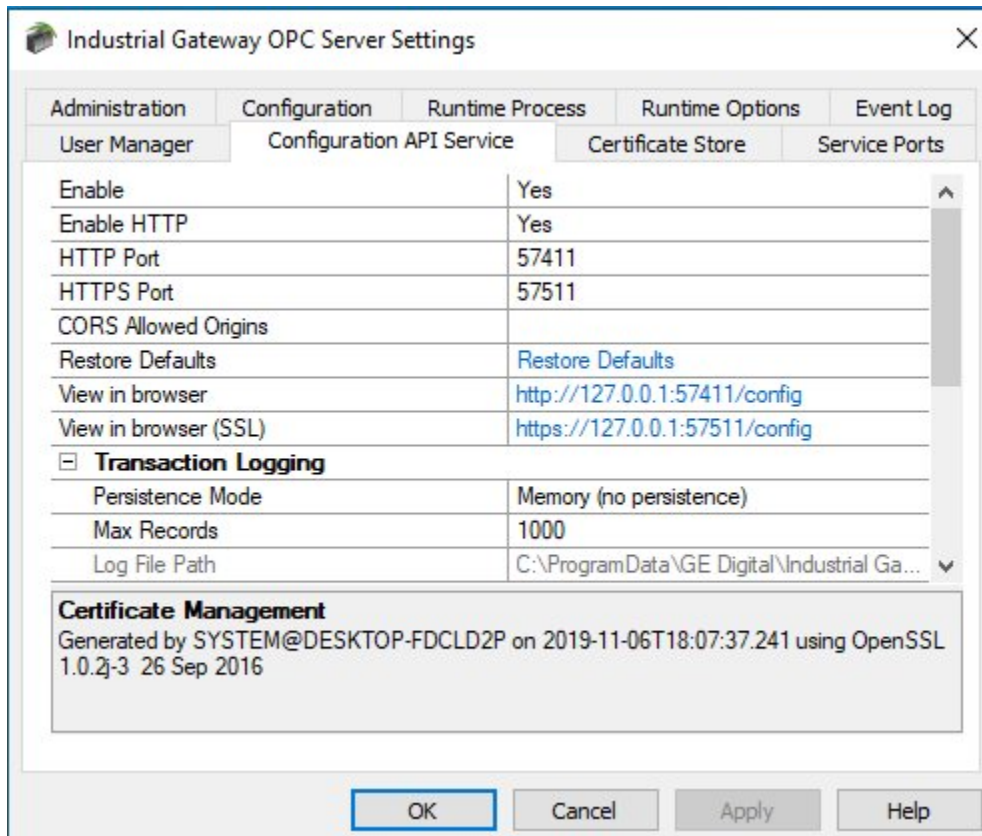
IGS Connections

IGS Connections

Overview

To use the IGS feature in Configuration Hub, you must:

- Have a license for IGS: Industrial Gateway Server - Basic or 100.
- Have the IGS driver added to the iFIX SCU.
- Have the correct settings for the IGS Configuration API Service: both the **Enable** and **Enable HTTP** fields are set to Yes. Restart the driver after you configure these settings.



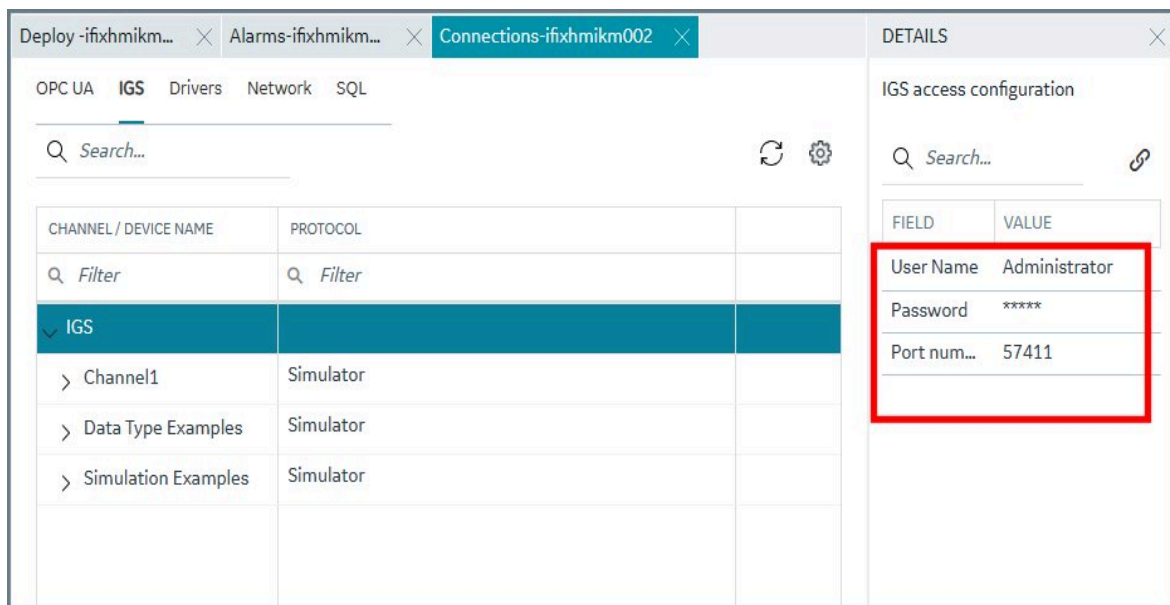
Steps to Add the IGS to the iFIX SCU

Start iFIX.

1. From the iFIX WorkSpace ribbon, select Applications and then select the SCU (System Configuration Utility) option. The SCU appears.
2. On the Configure menu, select SCADA. The SCADA Configuration dialog box appears.
3. In the I/O Driver Name field, click the browse (...) button. The available driver dialog box appears.
4. Select the IGS driver, and click OK.
5. Click Add to add the driver.
6. Click OK. A message appears that the database named "DATABASE" does not currently exist.
7. Click Yes to continue.
8. On the File menu, click Save to save the SCU file.
9. Restart iFIX.

Steps to Enable IGS Settings

1. In the Windows system tray, select the IGS Server icon.
2. Right-click and select Settings. The Industrial Gateway OPC Server Settings dialog box appears.
3. Select the Configuration API Service tab.
4. Set the 'Enable' and 'Enable http' fields to YES.
5. Restart the IGS Driver.
6. Open Configuration Hub.
7. From the Navigation panel, click FIX and then Connections.
8. Select the IGS option, and then inspect the settings.
9. If the IGS is configured with a user name and password, select the IGS connection, and then enter the user name and password for your IGS server (as shown in the fields displayed in the following figure) and then click **Save**. (If you do not configure a user name and password, the default user name is Administrator and the password is left blank.)



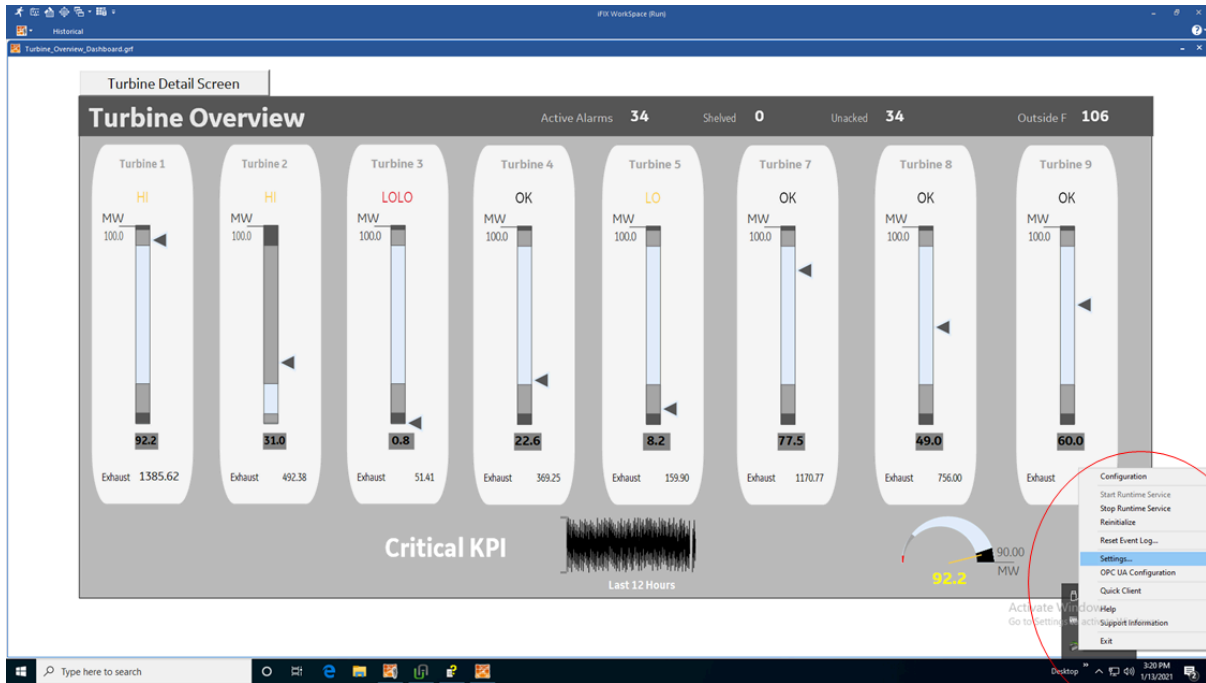
Tip:

If you need to troubleshoot IGS issues, you can find the IGS log file (igs-browse-config.log) located in the C:\Program Files (x86)\Proficy\iFIX\ folder, by default.

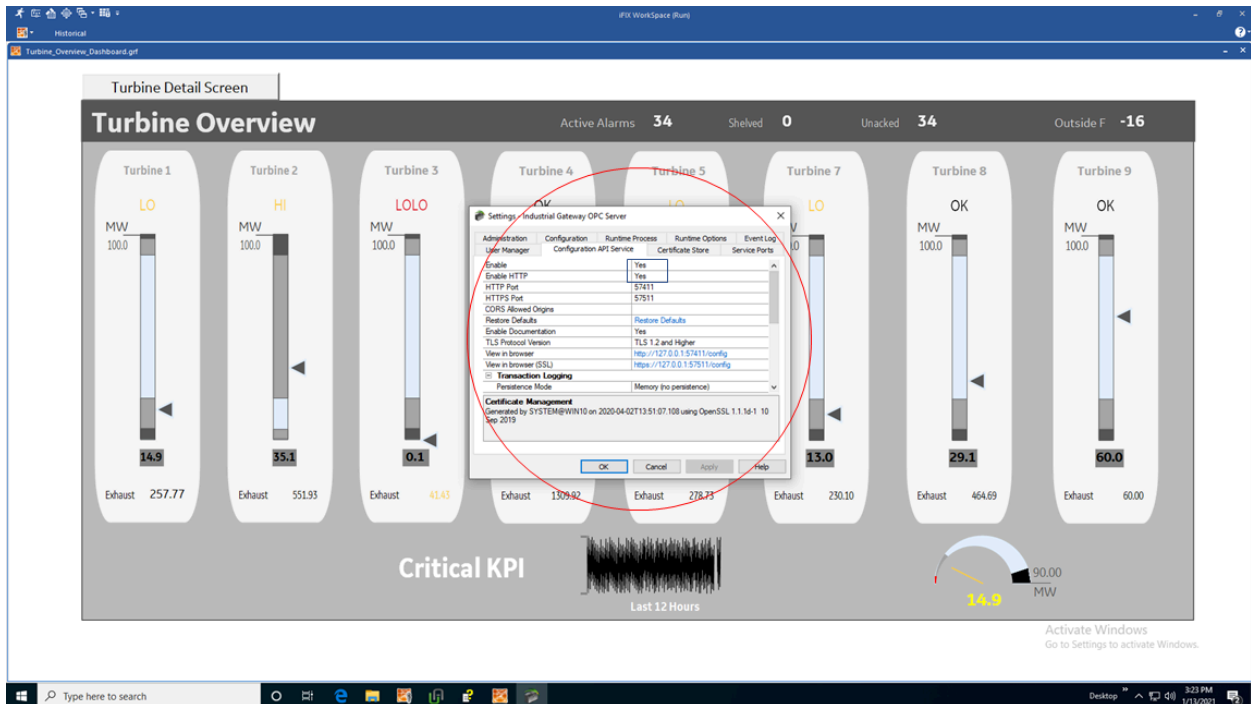
You can now configure channels/devices in the IGS (devices must be added to show Server details), and then Configuration Hub should display the configured channels/devices.

Configuration Example

The following example shows how to access the Settings for the IGS.



This is the Settings screen for the IGS driver:



Prerequisites for IGS

Prerequisites for the IGS driver include:

- Only IGS version 7.6 and onwards will be supported.
- Your license must be for IGS: Industrial Gateway Server - Basic or 100.
- In the IGS Administrator on the Configuration API Service, both Enable and Enable HTTP must be set to Yes.
- You must specify the proper user name and password in the Details panel of the IGS Connection screen in Configuration Hub in order to make the connection.
- The IGS driver must be added to iFIX in the SCU.

Getting Started with the Browse Tree for IGS

If you have an active IGS Project, it will appear in the table.

Select Browse to browse the hierarchy of channels and devices available in the IGS Server.

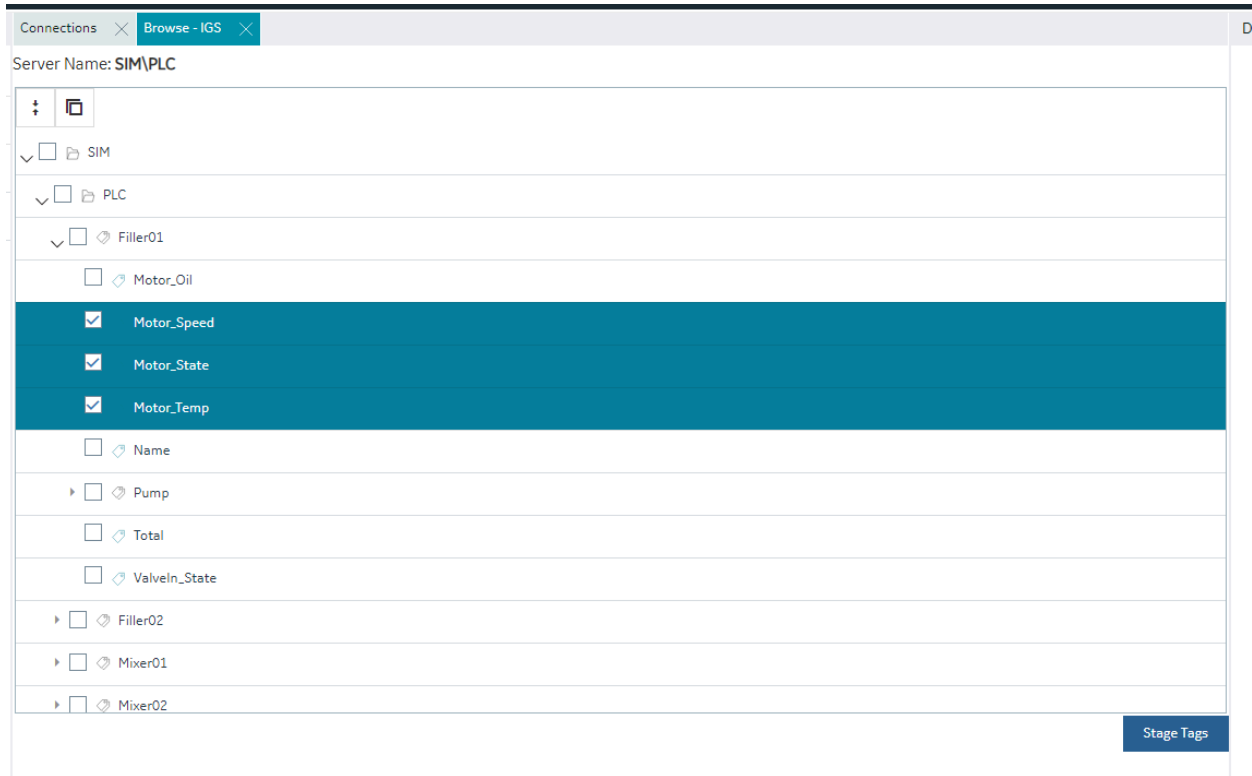
The screenshot shows the Configuration Hub interface. The main panel is titled 'Connections' and has tabs for 'OPC UA', 'IGS', 'Drivers', 'Network', and 'SQL'. The 'IGS' tab is active. Below the tabs is a search bar and a table with columns 'CHANNEL / DEVICE NAME' and 'PROTOCOL'. The table contains a row for 'SIM' (Simulator) and a row for 'PLC' (PLC). The 'PLC' row is highlighted, and a 'Browse' button is visible next to it. To the right of the table is a 'DETAILS' panel for the selected 'PLC' device. The details panel includes a search bar and a table with the following data:

FIELD	VALUE
Description	
Channel N...	SIM
Protocol	Simulator
Device Des...	
Device ID	1
Device Na...	PLC

Browsing IGS Channels and Devices

The IGS tab in the connections panel displays the configured channels in the table. The channel can be expanded to access the devices configured under the channels. On selection of a device, the menu offers a browse command.

The configuration content of a device is populated into a new panel, the panel displays the selected channel/device and shows the tags/tag groups configured in the device. The tag groups can be expanded to navigated to the further levels of hierarchy.



Browse and Create Tags for IGS

The IGS browse panel shows the content of the IGS channel/device. Individual tags or a tag group can be selected to create as iFIX tags. Right-click menu on the tag groups provides a bulk selection option to select all the tags under the tag group. On selection of the tags and clicking of the Stage Tags option, the tags are staged for the next step in tag creation process.

The staging environment allows for selection of iFIX block type (default mapped on staging) and selection of Historian collection option for the tag. Additionally, you can add a prefix and reduce the hierarchical levels of the tag names.

Connections × Browse - IGS ×

Staging Area for Tag Creation

Search Name prefix 0 ↑ ↓ 📄

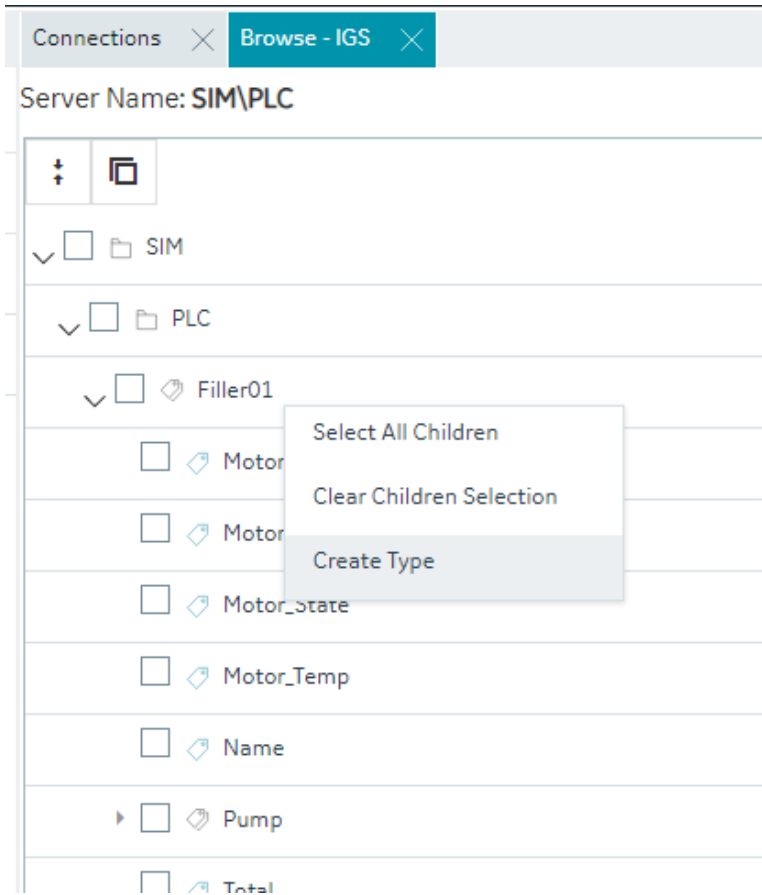
<input checked="" type="checkbox"/>	IFIX TAG NAME	BLOCK TYPE	HISTORIAN	STATUS	RESULT
<input checked="" type="checkbox"/>	SIM_PLC_Filler01_Motor_Speed	AI	<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/>	SIM_PLC_Filler01_Motor_State	DI	<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/>	SIM_PLC_Filler01_Motor_Temp	AI	<input checked="" type="checkbox"/>		

Browse and Create Types for IGS

Using the browse functionality on an IGS server, you can create new model types from existing types, replicating their variables and if required, any child objects or variable groupings. This allows you to quickly populate the properties of an object type, without having to configure them separately.

To create a new model type based on an existing type:

1. Right-click the existing model type from the **Browse** tab and select **Create Type** from the menu that appears. The **Create Object Type** dialog will appear.



Create Object Type

NAME
AirConditionerControllerType

DESCRIPTION

Include Hierarchy

STATUS:

2. Enter a unique **NAME** for the model type.
3. Enter a **DESCRIPTION** for the model type (optional).
4. The **Include Hierarchy** checkbox provides two options:
 - If left unchecked, only the variables at the level directly below that of the object type would be copied. Any contained assets (child objects or variable groupings) will be ignored when the new model type is created.
 - If the box is checked, all contained assets from all sub-levels, will also be created in the new model type.
5. Click **Create**.
 - If there is a conflict with one of the copied types (that is, it already exists within another asset), the **Create Type Hierarchy** dialog appears.

TYPE	ACTION	NEW TYPE NAME
Pump	<input checked="" type="radio"/> Use Existing <input type="radio"/> Create New	

At this point you must choose to either:

- **Use Existing:** reuse the type in the new model.
 - **Create New:** if the existing type does not represent the new asset (for example if it has different variables), give it a new, unique name in the **NEW TYPE NAME** field.
- Click **Continue**.
 - Click **Close** in the **Create Object Type** dialog.

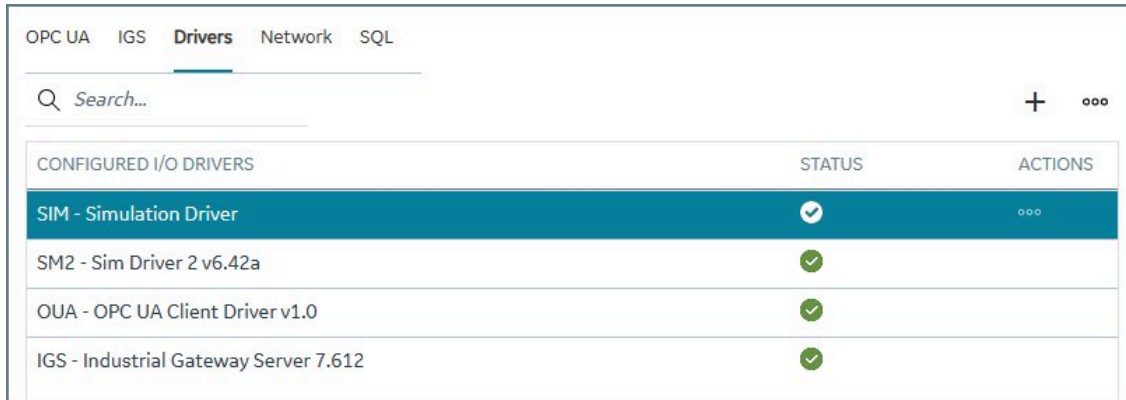
Drivers

The Drivers area lists the available drivers that you can add to your SCADA configuration.

View the Configured Drivers

To view the configured drivers for your SCADA system:

1. On the Configuration Hub Navigation panel, select your iFIX node, and then **Connections**.
2. Click **Drivers**. The following screen appears in the Connections panel. The grid displays a list of I/O drivers configured on this node, and their status.



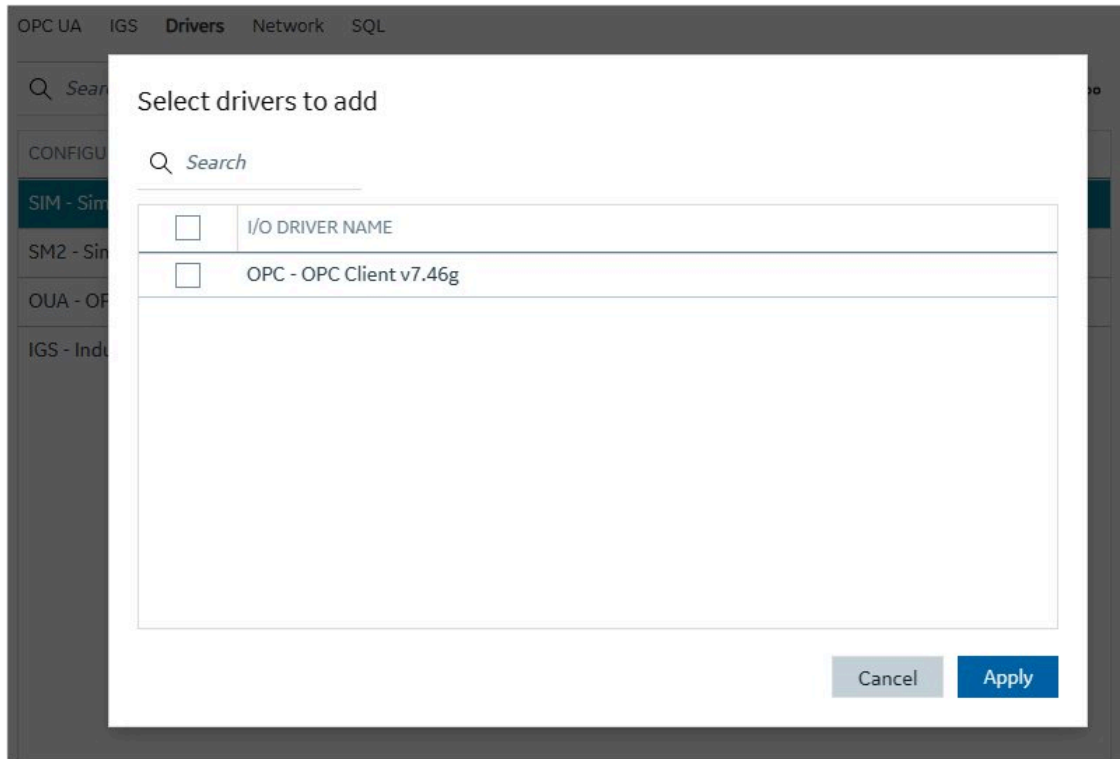
The screenshot shows the 'Drivers' tab in the Configuration Hub interface. At the top, there are navigation tabs for 'OPC UA', 'IGS', 'Drivers', 'Network', and 'SQL'. Below the tabs is a search bar with the placeholder text 'Search...'. To the right of the search bar are a plus sign (+) and a three-dot menu icon (⋮). The main content is a table with the following structure:

CONFIGURED I/O DRIVERS	STATUS	ACTIONS
SIM - Simulation Driver	✓	⋮
SM2 - Sim Driver 2 v6.42a	✓	
OUA - OPC UA Client Driver v1.0	✓	
IGS - Industrial Gateway Server 7.612	✓	

Add a Driver

To add a driver in Configuration Hub:

1. Click the plus (+) icon at the top of the Configured I/O Drivers grid. The Select Drivers to Add dialog box appears. Only the drivers that are available to add (and have previously been added through the iFIX SCU application) appear in this list.
2. Select the check box of the driver that you want to add.
3. Click **Apply**.



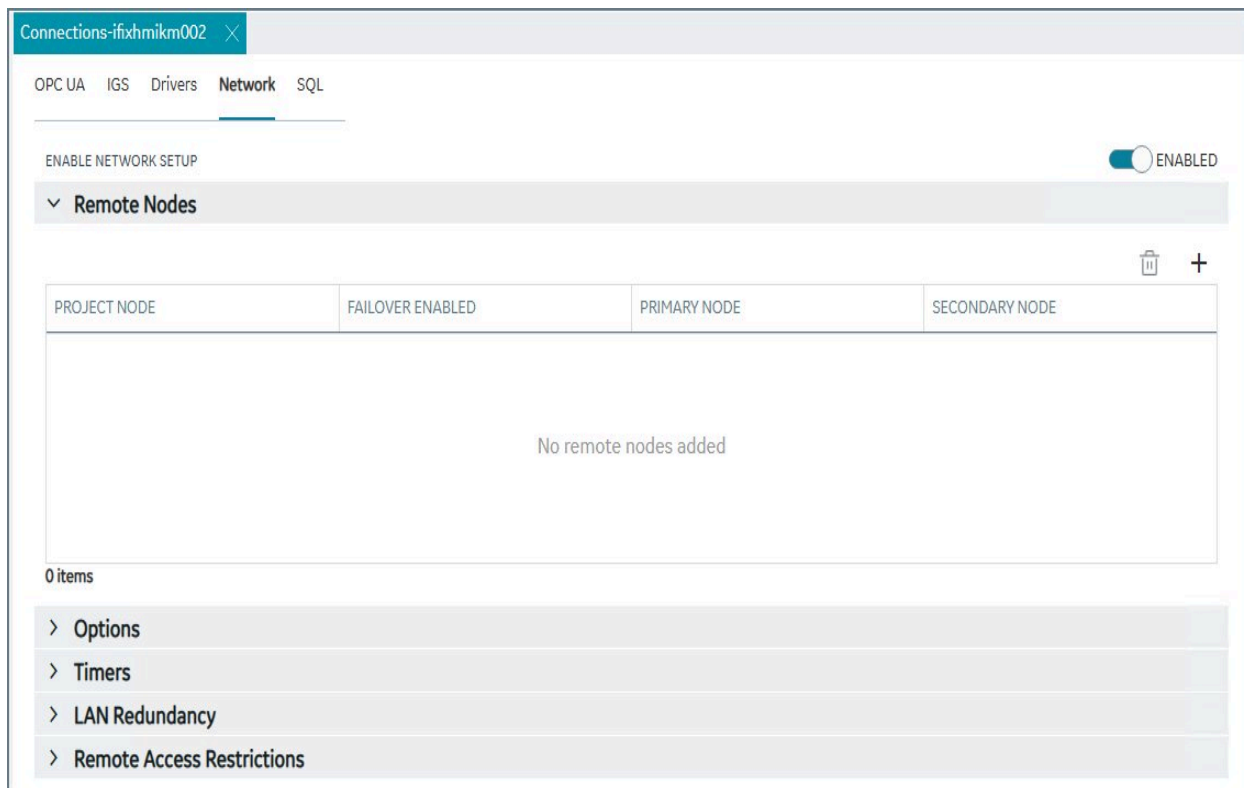
Network Connections

The Network Connections area allows you to view and control network communications for this node.

Overview

To access the Network Connections:

1. In the Navigation panel, select your iFIX node, project, and then **Connections**.
2. Click **Network**. The following screen appears in the Connections panel.



Network Connections Details

The tables that follow describe the details that you can configure or view.

Table 1. Remote Nodes

Field	Description
Project Node	Displays the iFIX project node name.
Description	Provides the description of the node.
Primary Node	Specifies the name of the primary node. The node name you enter cannot already be listed in the Configured Remote Nodes list box. You also cannot enter the name of a node that is already entered as a primary node.
Secondary Node	Allows you to specify the name of the standby node. The node name you enter cannot already be listed in the Configured Remote Nodes list box.

Table 1. Remote Nodes (continued)

Field	Description
	You also cannot enter the name of a node that is already entered as a standby node.
Failover Enabled	Describes whether iFIX Enhanced Failover is enabled. The default is No.
Reset to Defaults button	Allows you to reset the remote node network timers to their default values.
Use Network Timers	Allows you to enable the use of network timers on the remote node. The default is Yes.
Keep Alive	Allows you to specify the amount of time that, if no activity has occurred over an established connection, a View client waits before sending a heartbeat message. The default value for this field is 20 seconds.
Send	Allows you to specify the amount of time that a View client waits for a request to the SCADA server to be acknowledged. If this timer expires, the session ends. The default value for this field is 30 seconds.
Receive	Allows you to specify the amount of time that a View client waits for a reply from the SCADA server. When running iFIX over TCP/IP, the effective session timeout values is either the Send timer or the Receive timer, whichever is greater. If this timer expires, the session ends. The default value for this field is 60 seconds.
Inactivity	Allows you to specify the amount of time that, if no data activity has occurred over an established connection, a View client waits before removing the dynamic connection from the list of outgoing con-

Table 1. Remote Nodes (continued)

Field	Description
	<p>nections. If this timer expires, the session ends. The default value for this field is 300 seconds.</p>

Table 2. Options

Field	Description
Resolve Dynamic Connections	<p>Allows you to establish dynamic connections on this node. Disable this option if you want to connect only to nodes configured in the Configured Remote Nodes list. This feature is not available if you are setting up a stand-alone node.</p> <p>The default is Disabled.</p>
Enforce Trusted Computing	<p>Allows you to establish trusted computing on this node. Disable this option if you want to use legacy network computing. This feature is not available if you are setting up a stand-alone node.</p> <p>When Trusted Computing is enabled, a valid password must be configured and confirmed before the changes will be saved.</p> <p>The default is Disabled.</p>
Set Up Network Password	<p>Allows you to set a password to create a site-specific certificate for network security. The default password (INETWORK) allows legacy network security to continue. This field is not available if you are setting up a stand-alone node.</p>

Table 3. Timers

Field	Description
Keep Alive	<p>Allows you to specify the amount of time that, if no activity has occurred over an established connection, a View client waits before sending a heartbeat message.</p>

Table 3. Timers (continued)

Field	Description
Range (10-129 seconds)	The default value for this field is 20 seconds.
Send	Allows you to specify the amount of time that a View client waits for a request to the SCADA server to be acknowledged. If this timer expires, the session ends.
Range (5-120 seconds)	The default value for this field is 30 seconds.
Inactivity	Allows you to specify the amount of time that, if no data activity has occurred over an established connection, a View client waits before removing the dynamic connection from the list of outgoing connections. If this timer expires, the session ends.
Range (50-32000 seconds)	The default value for this field is 300 seconds.
Receive	Allows you to specify the amount of time that a View client waits for a reply from the SCADA server. When running iFIX over TCP/IP, the effective session timeout values is either the Send timer or the Receive timer, whichever is greater. If this timer expires, the session ends.
Range (5-120 seconds)	The default value for this field is 60 seconds.

Table 4. LAN Redundancy

Field	Description
Reset to Defaults button	Allows you to reset the network timers to their default values.
Enable LAN Redundancy	Allows you to enable the LAN redundancy feature on the node. The default is Disabled.
Available Paths list	Displays a list of available network paths, and their network status.

Table 5. Remote Access Restrictions

Field	Description	Default
Accept Unknown Host	Select this option to allow the SCADA node to accept connections from any computer. When the parameter is disabled, access is restricted to the iClients (View) you specify.	Disabled
Remote Viewers list	The list of remote viewers that can Accept Unknown Hosts.	None
Accept Unauthorized Writes	Select this option to allow the SCADA node to log all unauthorized write attempts from the iClients.	Disabled
Remote Viewers list	The list of remote viewers that can Accept Unauthorized Writes.	None
Log Unauthorized Writes	Select this option to enable the logging of failed writes.	Disabled

Special Considerations for SCADA Enhanced Failover

This topic covers iFIX Enhanced Failover special considerations. It does not cover High Availability for Configuration Hub servers. iFIX Enhanced Failover should not be used on a node participating in a [High Availability \(on page 50\)](#) setup.

If using Enhanced Failover, you must be in Maintenance Mode to make changes to your Database or Model in Configuration Hub. Maintenance Mode allows you to temporarily suspend synchronization between the two SCADA nodes in an Enhanced Failover pair. This allows you to add or modify groups and tags in your iFIX database while the Scan, Alarm, and Control (SAC) program is running. When you enter Maintenance Mode, SCADA synchronization temporarily stops; synchronization between the SCADA pair is suspended. After Maintenance Mode is enabled, you can make changes to the database on the primary node.

Additionally, all changes to a Failover pair's Database or Model must be made on the Primary node. Changes made to a Failover pair's Database or Model on the Secondary node cannot be published.

Every time you make a change in the configuration and publish, the data is reloaded in the configuration and the driver is restarted. This is important to know if you are making changes on a live system. You will NOT need to restart iFIX after you make any changes in the Configuration Hub. However, after you exit Maintenance Mode, you will need to stop and restart the driver from Mission Control on the secondary in order to pick up the configuration changes.

Using Configuration Hub with iFIX Enhanced Failover

In an Enhanced Failover setup, both the Primary and Secondary Nodes can register and login to Configuration Hub. See [iFIX Plugin Registration \(on page 158\)](#).

1. Once registered, you can login and work with Configuration Hub on the Primary and Secondary nodes.
2. When making changes to the Database or Model you must be in Maintenance Mode, and those changes must be made on the Primary node.
3. Changes made while in Maintenance Mode need to be published in Configuration Hub to the iFIX node.
4. Once all changes to the Database or Model have published, disable Maintenance Mode in the Primary Node. This will allow the Primary Node to synchronize changes with the Secondary Node.

Deleting Servers or Groups

Be aware that when the iFIX SCADA Enhanced Failover pair has the OPC UA Driver configured, any server or group delete operation in the Configuration Hub UI on the Primary will not be deleted on Secondary after the maintenance mode synchronization happens. The Secondary SCADA continues to retrieve data since the server and/or group still exist on the Secondary. As a workaround, manually delete the server and group files from the secondary SCADA, since you cannot run Configuration Hub on the Secondary SCADA. The UA client will continue to receive data from these servers/groups until the OUA driver is restarted (via Mission Control or iFIX restart) on the Secondary SCADA, forcing the driver to reload the configuration from disk, which will no longer have those servers/groups.

Server and Group configuration files are found in the PDB\iFixUaClient folder, in Servers and Groups folders, respectively. Each server and group have its own file. In each of these folders, compare the contents on the Primary node to those on the Secondary. If a file exists on the Secondary but not on the Primary then open the file in a text editor and verify that it is a server or group that was deleted from the Primary. If so, delete that file from the Secondary.

For all other operations, the synchronization works as expected such as: Server Create, Driver tag deletions or updates, Group updates, and so on.

Notes on Certificate Management

When the iFIX SCADA is part of an Enhanced Failover pair and we have enabled the OPC UA Driver on the SCADA, each physical SCADA needs to establish trust with the configured OPC UA Server separately. After both SCADAs can communicate to a remote OPC UA Server individually using their certificates, you can then bring the iFIX SCADAs up as failover pair. Be sure to confirm that you can communicate individually first.

Special I/O Addresses

There are special I/O addresses in iFIX that are very helpful in a Redundancy Configuration for the OPC UA Client. Using the `ConnectionStatus` and `EndpointUrl` addresses, you can see the overall connected status of a (logical) server, and the endpoint it is currently using for data.

SQL Connections

The SQL Connections area in Configuration Hub allows you to control how the iFIX SQL option communicates with a server containing a relational database.

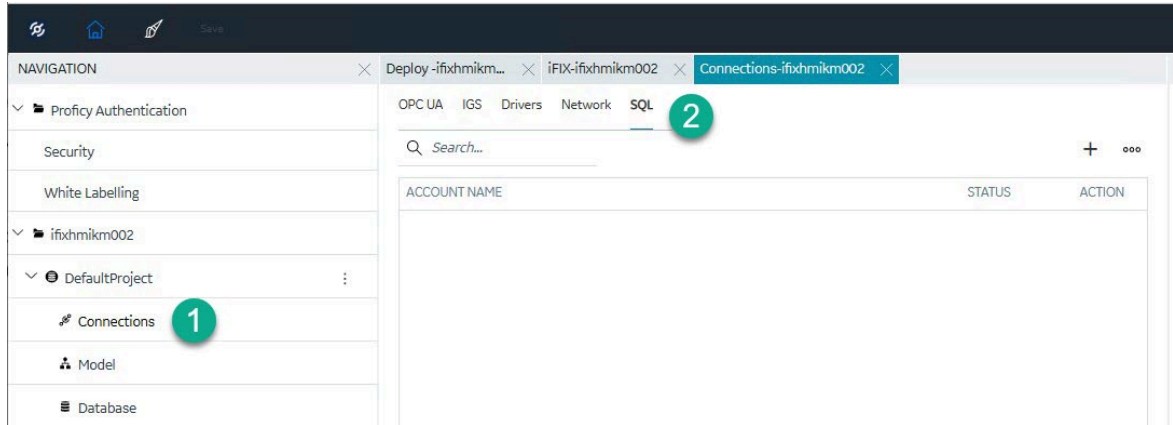
Overview

The SQL Connections let you identify the:

- Type of database to which the SQL option connects (for example, Oracle, or Access).
- User name for the account to which you log into on the relational system.
- Password for the account.
- ODBC data source name.

Add a SQL Connection

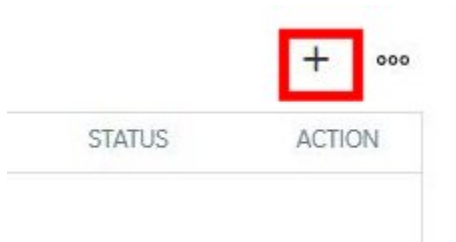
1. In Configuration Hub, in the Navigation panel, select your iFIX node, and then Connections.
2. Next, click SQL. The following screen appears in the Connections panel.



Note:

To refresh the list, click the ellipsis (...) button, and then select **Refresh SQL Accounts**.

3. To add a SQL connection, click the plus (+) icon at the top of the grid.



The Add accounts dialog box appears as shown in the following figure.

4. Enter the information described in the following table.
5. Click **Add**.

Table 6. Add Accounts Dialog Box Fields

Field	Description
Database Type	Allows you to display a list of supported relational databases.
User	Allows you to specify the name of the user's account on the server. This name is usually the same one you use to log onto the server. This field can be left blank or can contain a name with up to 31 characters.
Password	Allows you to specify the password used to log onto the server. This field can be left blank or can contain a password with up to 31 characters.

Table 6. Add Accounts Dialog Box Fields (continued)

Field	Description
	If you enter a user name, then most likely you are required to enter a password. As each character is entered, an asterisk appears in the Password field. This protects your password.
Database Identifier	Allows you to specify the ODBC data source name to which the SQL option can connect. Click the drop-down list to display a list of ODBC data sources.

Model

Model Overview

The iFIX model allows you to create a blueprint or template of the assets in your system and quickly and easily create and maintain instances generated from the Type definition.

The model in iFIX consists of the following components:

- **Object Types:** An object type is a blueprint. A blueprint is something tangible in your plant that you want to replicate, such as mixer, furnace, or pump, that will have a common structure (common variables and contained types) shared across all mixers, furnaces, and pumps. Object Types will have Variables, Contained Types, and Templates.
- **Variables** - Individual tags or measurements that are common across all Objects of a certain type, like temperature, pressure, flow, and so on. Variables represent tags that will hold values retrieved via iFIX drivers like IGS and OPC UA client from the devices in your system.
- **Templates:** Templates provide the capability to have one or more translations of an Object Type into an Object Instance. If you have two different types of pumps that have some commonly shared variables but a subset that are unique, you would create two templates for a single pump type.
- **Substitutions** - Substitutions allow you to parametrize your Type definition such that you can modify the Object Instances created from the Type and Templates to be unique.
- **Contained Types** - Contained types allow you to create a hierarchical blueprint of assets that will be instantiated together.

- **Object Instances** - An instance created from the Object Type. The instance represents an asset in the application and the variables are either created as iFIX tags (direct variables) or point to existing iFIX tags (indirect variables) or are static to the type (static variables).

Model Panel

The Model panel is where you go to navigate and initiate actions on your model. To configure the model, click on Model entry under your iFIX node in the Navigation panel. You will see a table of Types and Instances in the main panel.

Model ✕

↓
↑
↻
⚙️
🔍
New

∨ Types		
∨ 📁 Mixer	✔	
∨ 📁 Variables		
🔑 Motor_Oil		
🔑 Motor_SP		
🔑 Motor_Speed		
🔑 Motor_State		
🔑 Motor_Temp		
🔑 Name		
🔑 Tank_Level		
🔑 ValveIn_State		
🔑 ValveOut_State		
∨ 📁 Templates		
📄 Default_Template_Mixer		
∨ Instances		
∨ 📁 PaintMixer	+	
∨ 📁 Variables		
🔑 Motor_Oil		
🔑 Motor_SP		
🔑 Motor_Speed		
🔑 Motor_State		
🔑 Motor_Temp		

ⓘ
Active Database: NEWDB

Note:

Be aware that the panel should not be floating, and must be docked before performing any operation.

The Details panel will provide additional information about your selections in the Model panel. The Object types show variables and contained types on expansion and the contained types can be further expanded to navigate through the containment hierarchy. You can also see the hierarchy of templates that will be created for a given parent template. Similarly, the object instances tree provides navigation to the instance containment hierarchy.

The Model panel lets you configure the model in the following ways.

- Create Types
- Edit types (in a separate panel)
- Create Object Instances from Types

**Warning:**

In the Model panel, when Object Instances or variables under an Object Instance are selected, the properties are populated on the Details panel. When changes are made to the properties of an instance or variable, these changes are saved on a selection change in the model tree.

Type Creation

Object Types provide a powerful mechanism for creating and managing Object Instances and variables for your iFIX SCADA. In conjunction with Type Templates, you can generate and update multiple Object Instances from one location.

To create a type, click the "New" button on the top right of the Model panel. This will prompt you for the type name and description.

New Object Type

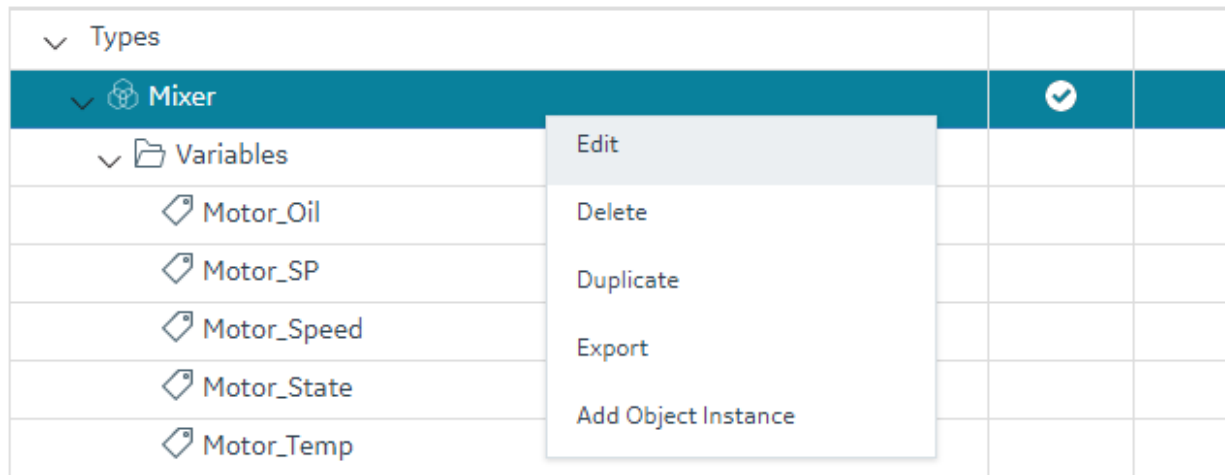
NAME
FillerType

DESCRIPTION
Blueprint for the plants fillers.

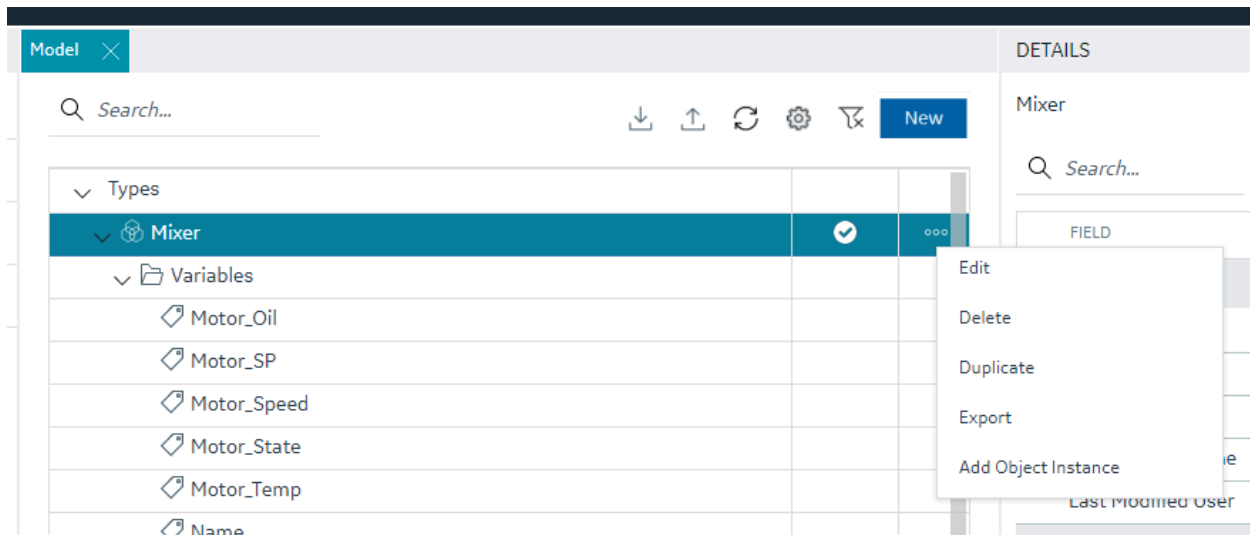
Cancel Create

Creating or editing a type will open that type into a separate IDE panel. Currently, there is only one Type Edit panel, so as you edit multiple types, the Type Edit panel will be replaced with the Type currently selected for editing.

After the type is created and saved, the model panel gives you capabilities to manage that type include editing, deleting, duplicating, exporting, or creating an instance of the type.



This can be accessed from the context menu in the Type's row in the grid or the Right-Click menu. Double-clicking the Type's row will open the Type Edit panel.



**Note:**

When saving a type, any updates will be automatically pushed to existing Object Instances of type. Depending on the number of instances associated with the type, it could take a long time to update. This may result in the save taking a long time.

Type Variables

Type Variables

Type Configuration

When configuring your type, the most important component is the list of variables that define the asset type characteristics or measures.

In the type edit panel, you can add new variables using the New button. You can configure some simple tag details in Type mode including tag type. Switching to template mode allows you to configure the majority of the variable details.

The type of a variable (Number/String/Boolean) can be defined differently between templates. iFIX block types can be mapped differently between templates.

Supported Tag Types for Variable Configuration

The iFIX model supports the following tag types for variable configuration:

- [Direct Variables \(on page 209\)](#) - Direct variables when instantiated, become tags in your iFIX database.
- [Indirect Variables \(on page 209\)](#) - Indirect variables allow you to reference an existing iFIX tag in the tag database. This can be useful to create a model structure on top of an existing flat tag database.
- [Static Variables \(on page 210\)](#) - Static variable store static value for the variables, these variables are not created as iFIX tags, they take the value through an object instance and do not change the value during the runtime.

Details Panel

The Details panel shows the properties of variable type. Setting or changing property values for variables in template mode will translate into any Object Instances that will or are created from this type's templates when you save those changes.

Direct Variables

Direct variables are variables that directly communicate to iFIX drivers. Direct variables are created as iFIX tags in the iFIX database when Object Instances are created. You can configure variable properties in Object Template mode.

Currently, model variables support a subset of the tag types available in the iFIX system. This subset includes:

- Numeric types supported - AI, AA, AR, AO, DA, DT, DC, TM
- Boolean types supported - DI, DA, DR, DO, BL
- Text types supported - TX

Indirect Variables

Indirect variables give you the capability to build a model on top of an existing flat tag database. When you create an indirect variable in a Type, for each template, you can use the Details panel to specify a tag or a substitution to generate a tag reference when Object Instances are created.

By using a substitution value in the Template Tag Name property, you can dynamically change the name of the variable per Object Instance.

Details panel

DETAILS
✕

Indirectvar

🔍 Search...

FIELD	VALUE
▼ GENERAL	
Variable Name	Indirectvar
Data Type	NUMBER
Description	
Variable Type	INDIRECT
Template Tag Name	Paint_Mixer_{Mixer#}

Static Variables

Static variables are variables meant to hold static data in your Object Type and Instance. They are read-only variables that are set only at the model instance level and do not create iFIX tags. Static variables can be browsed for and used in your iFIX pictures. An example of a static variable could be a serial number of an Asset.

DETAILS ×	
Static_Var	
<input type="text" value="Search..."/>	
FIELD	VALUE
▼ GENERAL	
Variable Name	Static_Var
Variable Type	Static
Static Value	123456

Template Overview

Templates describe how Object Instances will be created from an Object Type. All Types are created with a default template and require at least one template to work. Creating multiple templates is useful if you have a number of Asset definitions that are similar and have majority of overlapping variables, but have some exceptions.

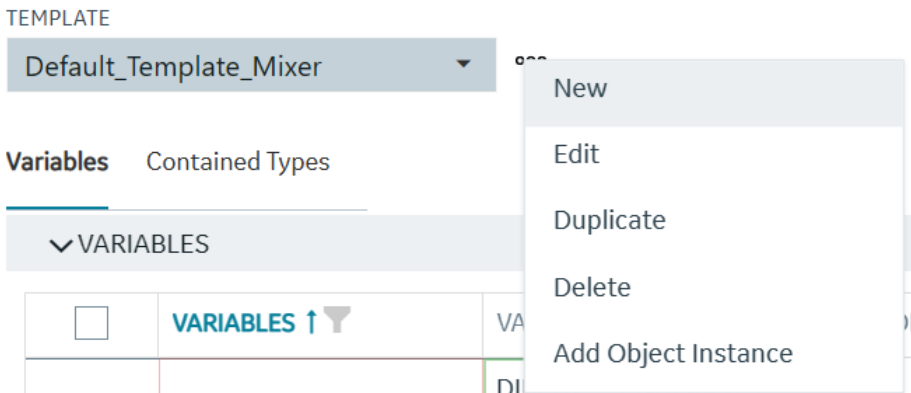
Default Template

A type must always contain at least one Template. By default, when you create a Type, a default template is created for you. If you do not need to account for slight variations in the Object Instances that will be created from your type, then you do not need to configure anything further with the template.

Template Management

Overview

You can manage templates from the Template drop-down in the Type edit panel.

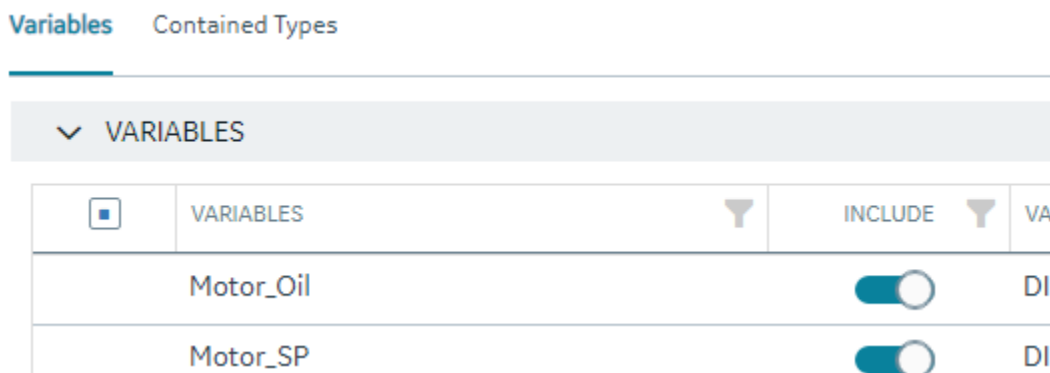


What's Stored in a Template

Each template stores a number of details about a type that are unique from other templates in the type. Specifically, the template stores:

- **Substitutions** - are unique per template.
- **Include/Exclude variable** - at the template level, you can choose which variables to include or exclude when an instance is created from that template.
- **Variable property changes** - All property changes you make in template mode, for example the IO address or alarm limits, are stored in the template. They can be different if you create a new template.
- **Contained Type template specification** - for each template, you can specify the template to use when creating an instance from that template for each of your Contained type aliases. Contained types can be included or excluded between templates.

Variables



All property changes you make in template mode, for example the IO address or alarm limits, are stored in the template. They can be different if you create a new template.

DETAILS

TextView

🔍 *Search...*

FIELD	VALUE
▼ GENERAL	
Variable Name	TextView
Tag	
Description	
▼ IO ADDRESSING	
I/O device	SIM
I/O address	{MixerNumber}

Substitutions

▼ SUBSTITUTIONS			
	PARAMETER NAME	DATA TYPE	DEFAULT VALUE
<input type="checkbox"/>	MixerNumber	NUMBER	1

Substitutions provide a mechanism to create placeholders in the variable property definitions through the templates. When the variable property value needs to vary between object instances, substitutions can help define a placeholder and provide unique values for each instance. For example, if the I/O address of a variable is defined in the variable template, providing I/O address of a particular tag would bring the same value across all instances. Instead, if we use a substitution in parts of or the full I/O address value, this value can be replaced differently for different instances.

A substitution can be defined and managed as part of a template definition. To use substitutions in template variable properties, use the substitution name surrounded by curly braces within a property. A numeric type property needs to have the full value substituted whereas a string value can have a part substituted or multiple substitutions can be used. Substitutions cannot currently be used for enumerated properties.

For example, a description property for a variable can be defined with substitutions as "This is the serial number \{Asset_Number\} of this \{Asset_Name\}" where Asset_Number and Asset_Name are substitutions and their values are provided per object instance.

**Note:**

Formulas are not currently supported within substitution strings used in the Model.

Contained Types

Contained types help define asset containment and provide a hierarchy relationship that can be used to make a multi-level instance as well as utilize this hierarchy during the model consumption in the iFIX picture definitions.

Contained types refer to other existing type definitions and are organized under a parent type. For example, an asset type definition for a pump can contain a shaft type, this can be accomplished by creating a type definition for pump and shaft separately and in the pump type definition, the contained types tab provides options to add a new containment by providing an alias name and selecting the shaft type from the drop-down.

Aliasing

When including contained types under a parent type, you must specify an alias name for that contained type. When the parent type is instantiated, the aliased contained types will be automatically created as instances with the alias name under the Parent instance. Aliasing enables differentiating multiple containments of the same type. You can have more than one alias contained under a parent type and the contained types can also contain other types making up a hierarchy. For example, a pump could contain two bearing units, one for inboard and one for outboard. The bearing type can be added as contained type to the pump with alias names Bearing_Inboard and Bearing_Outboard.

Substitutions

iFIX model type and template variable properties (mapped to tag fields based on block type selected) take input values as numerics, string constants, and substitutions, and offer placeholders for these inputs. You can use substitutions to enable assigning values at instance level for these properties.

You can insert substitutions directly into value cells by browsing. To use this feature, click on the property's cell value. A browse button displays in the value cell. Click this browse button to displays list of substitutions, click on the desired substitution to insert at the cursor position. Substitutions can also be used in expressions along with other value constants to finally evaluate to a final value substitution.



Note:

You refer to parent substitutions using the special character “@” from a contained child object. The value from the parent object instance is substituted to the contained object.

DETAILS
✕

Vibration

🔍 Search...

FIELD	VALUE
GENERAL	
Variable Name	Vibration
Tag Name	
Description	Filler 01 Pump Vibration
IO ADDRESSING	
I/O Driver	IGS
I/O Address	Filler0{FillerNum}.Pump.Vibration ⋮
Signal Conditioning	None
H/W options	None
Scan Time	1.00
LIMITS AND SCALING	
Low limit	0.15
High limit	0.18
Units	
Scale Enabled	NO
Scale Clamping	NO
Raw low	0.00

Expression Builder >

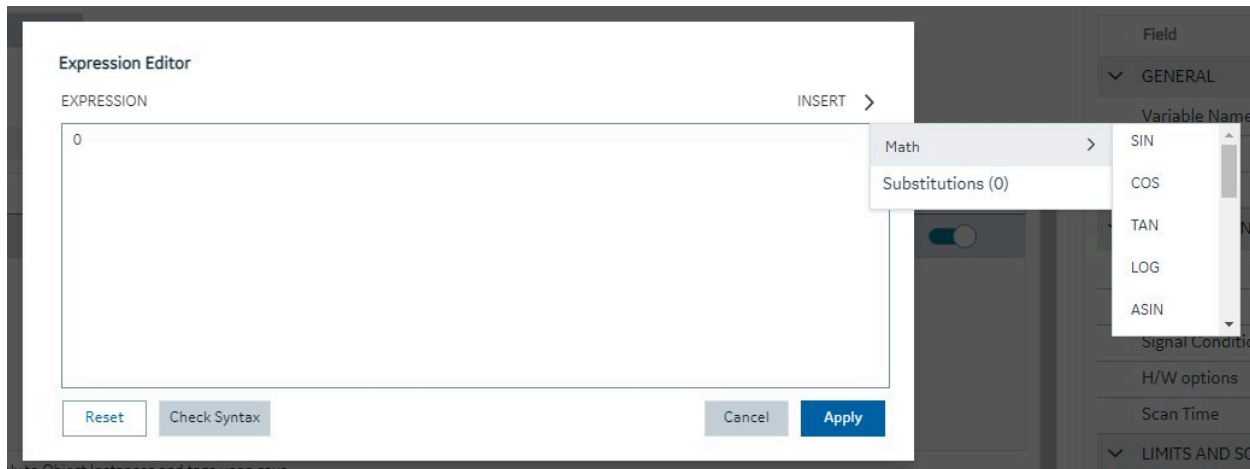
Substitutions (1) ▼

FillerNum

Expression Builder

Expression Builder

Another placeholder mechanism is enabled for the type variable property values: using an expression to define the value for a property. Expressions can be built using simple mathematical operators and functions. You can also insert substitutions into expressions.



You could also launch expression editor from the property value cell to build the expression.

For example, if you were defining a Pump type and create a variable called RPM, you could create a substitution for High Limit called "RPM_HighLimit" to define alarm limit values for this variable, and you could use an expression like Alarm Hi – "{RPM_HighLimit – 20}". The substitution value can be set at an instance level and automatically the alarm limits are adjusted based on the High Limit.

Object Creation

When you create a new object, a dialog box appears requesting a name, description, type, and template.

NEW OBJECT

Active Database

NEWDB

NAME

PaintMixer

DESCRIPTION

Mixer used for the truck line paintshop.

TYPE

Mixer

TEMPLATE

Default_Template_Mixer

Substitution Values

Any substitution values from the template that an Object Instance was created from can be edited in the Details panel by selecting the Object Instance in the Model Panel.

Model Import and Export

Use the model import and export to help you move the model from one node to another, to make bulk changes to the model itself, or to use your model in Operations Hub.

Overview

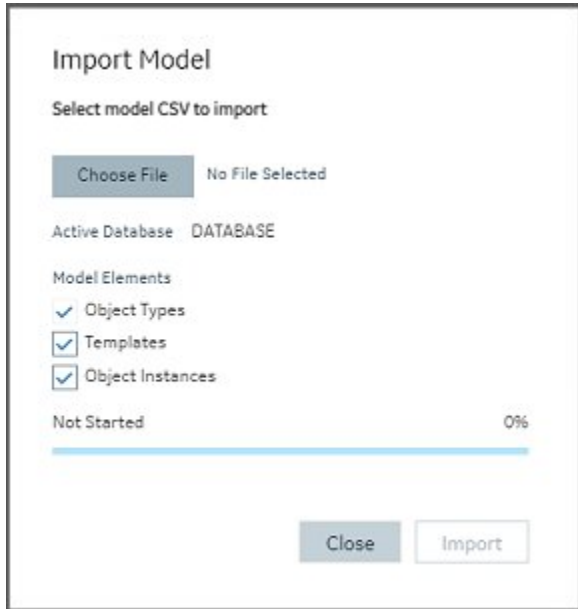
The Model can be exported or imported for working on outside of Configuration Hub. The Model export is compatible and can be imported into Operations Hub.

To import or export the model, use the first two buttons on the model toolbar:



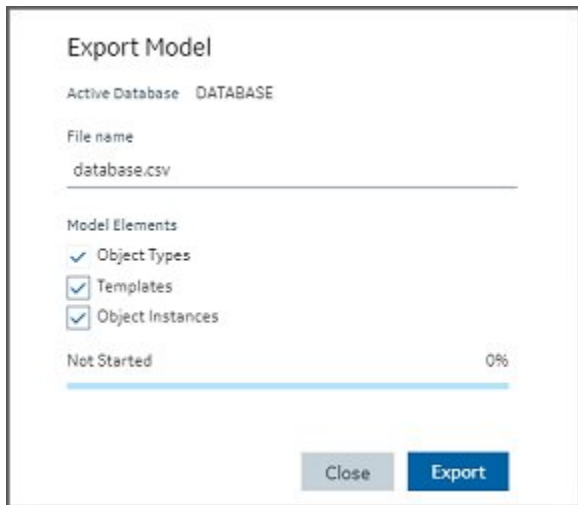
Importing a Model

To import a model, click the import button (↓). The Import Model dialog box appears where you can choose a file and specify what you want to import.



Exporting a Model

To export a model, click the export button (↑). The Export Model dialog box appears where you can specify



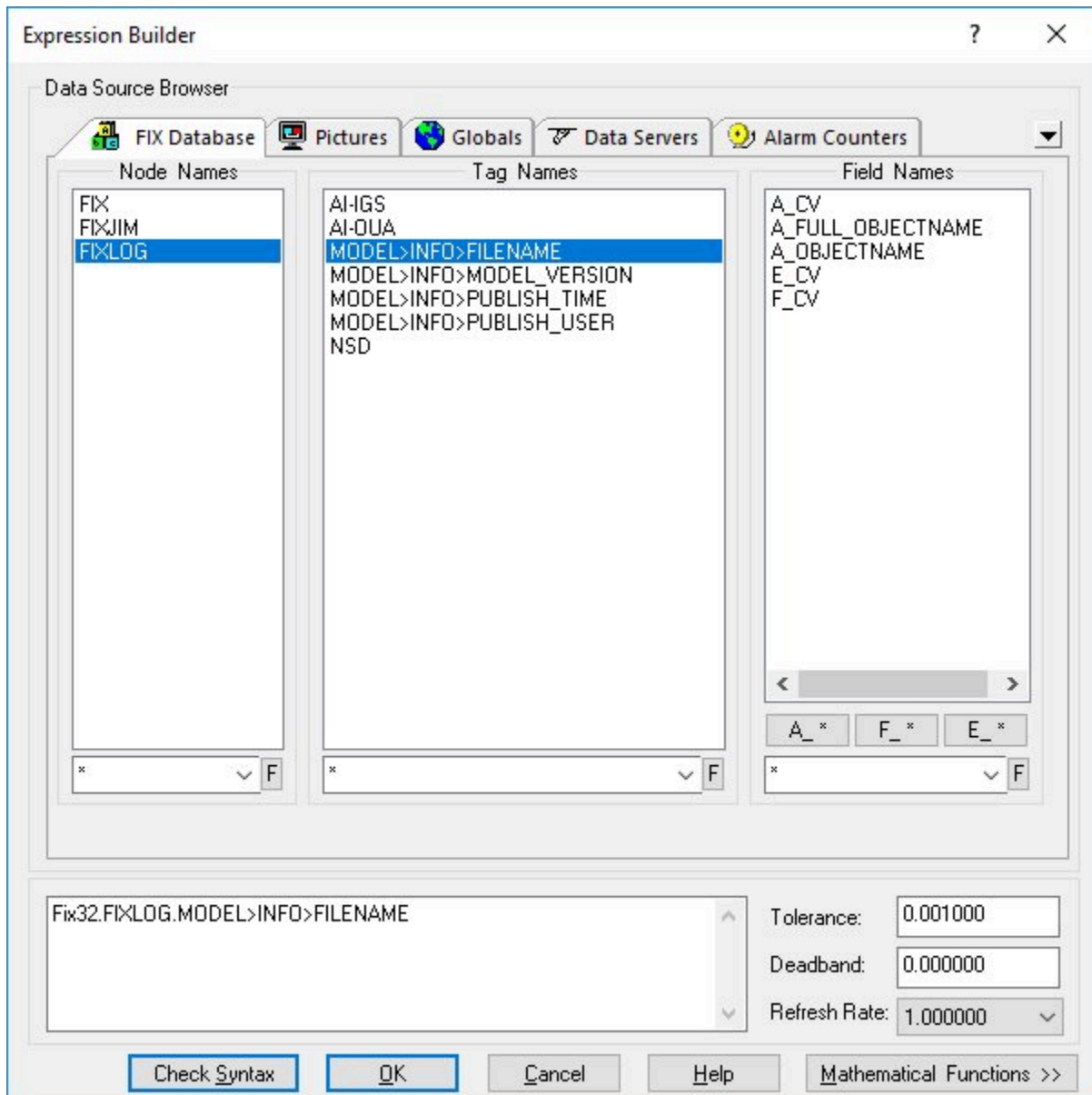
Model Tags in iFIX

Overview

Model-defined tags are also viewable from the iFIX Workspace. These include Indirect and Static variables defined in the model, as well as pre-defined tags that show model-related information. When viewing tags in the iFIX Expression Builder, you can see Indirect and Static variables listed alongside iFIX tags, as well as the pre-defined Model Info tags. Their values can be used in animations in the WorkSpace (such as in data links) just like any other iFIX tag.

Tag	Description
MODEL>INFO>FILENAME	The full file name with path of the model file from which the model was loaded.
MODEL>INFO>MODEL_VERSION	The version of the published model.
MODEL>INFO>PUBLISH_TIME	The time of the last publish.
MODEL>INFO>PUBLISH_USER	The iFIX user who performed the last publish.

Example of Expression Builder with Model Tags Displayed



Notes on the Example

The A_OBJECTNAME and A_FULL_OBJECTNAME fields shown in the previous figure will not have a value for the pre-defined Model Info tags. If iFIX tags are not associated with a variable in the model, they will not display values for these fields.

The Expression Builder does not display the A_OBJECTNAME and A_FULL_OBJECTNAME fields when browsing a tag that exists in the iFIX database – these fields only display when browsing Indirect or Static variables. However, this field can be manually entered for any iFIX database tag, and if that tag

is associated with a variable in the currently published model then the owning object's name will be displayed.

Database

Database Overview

Database Overview

The Database panel provides similar functionality to the iFIX Database Manager, but in a completely different interface: a web one. That interface that should be natively intuitive to those familiar with web-based grid objects. The Database in Configuration Hub has off-line storage where you do your work.

Click on the Database panel to connect to the database running on your iFIX SCADA node. All the tags appear into the off-line database. Interact with your iFIX tags in a web container where you can easily sort, filter, and interact with your iFIX tags.

After you are finished, you can Publish your changes to the running iFIX node. A filterable status column in the database shows the publish status of each tag. A log file is generated every time you Publish providing information about the operation.

**Note:**

iFIX supports up to 65534 tags per block type depending on the composition of the database in relation to available contiguous shared memory and process memory space.

The currently active iFIX database is what will show in Configuration Hub and is what will receive all operations. This is true regardless of how many users are connected to and configuring the same database. Changes to the database, both published and unpublished, are shared across users and browser sessions.

Refer to the following sections for more information about the iFIX Database panel:

- [Grid Features \(on page 222\)](#)
- [Searching, Filtering, Sorting, and Column Reordering \(on page 222\)](#)
- [Database Toolbar \(on page 224\)](#)
- [Database Column Choosing \(on page 225\)](#)
- [Database Details Panel \(on page 226\)](#)

Grid Features

The database grid provides many great features to allow you to easily and efficiently work with your iFIX data. The grid will always show and configure the currently active iFIX database for the node you are connected to. An example of the grid is displayed in the following figure.

<input type="checkbox"/> TAG NAME	↑ STATUS ↓	TYPE	DESCRIPTION
<input type="checkbox"/> MIXER01>MOTOR_OIL	✓	AI	Mixer 01 Motor Oil Level
<input type="checkbox"/> MIXER01>MOTOR_SP	✓	AI	Mixer 01 Motor SP
<input type="checkbox"/> MIXER01>MOTOR_SPEED	✓	AI	Mixer 01 Motor Speed R...
<input type="checkbox"/> MIXER01>MOTOR_STATE	✓	AI	Mixer 01 Motor State
<input type="checkbox"/> MIXER01>MOTOR_TEMP	✓	AI	Mixer 01 Motor Temp

When the active database changes from anywhere, the grid should notify you and ask you to refresh. If at any time you believe it is out of date due to concurrent changes from other locations, the toolbar contains a refresh icon to re-fetch the latest updates. The database grid panel works closely with the Details panel.

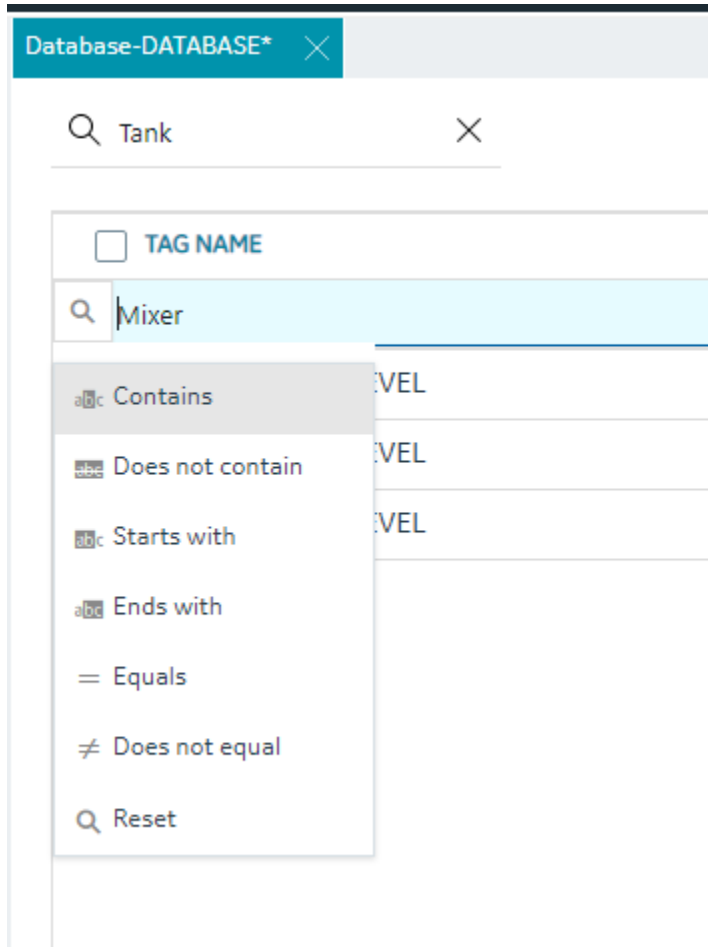
Ensure you have the Details panel open and visible as you work in this panel. As tag rows are selected within the grid, the tag details are displayed and are editable inside the Details panel.

Searching, Filtering, Sorting, and Column Reordering

The following sections provide more details on this functionality.

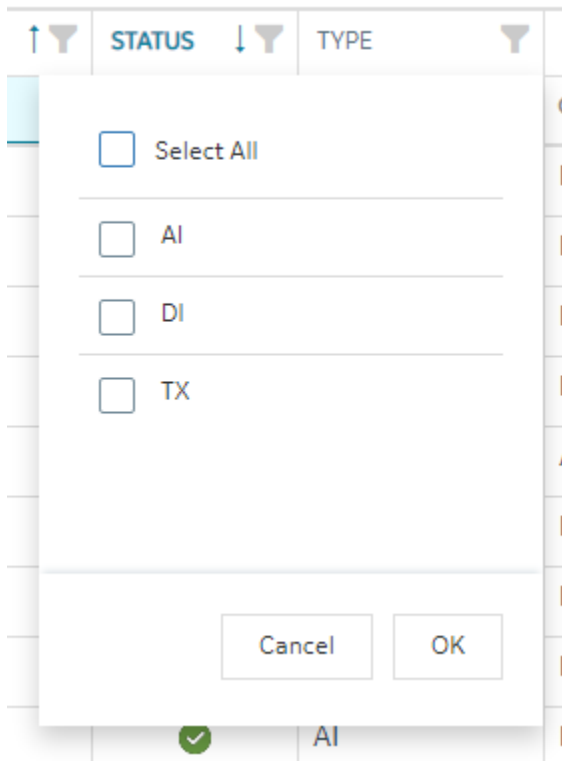
Searching

There are two main search options when using the database grid. A global search that searches the whole grid for the typed in text and a column search that searches a particular column and provides multiple search parameters. Especially for large datasets, using these search options helps to quickly find the tags and data you want to work with.



Filtering

Each column can filter by the current contents of the grid. For example, you can quickly and easily search for all the instances of a particular tag type, status, or IO Driver:



Sorting

Sorting is easy to do by clicking the header of any column to toggle between ascending and descending sort. For more advanced sorting, you can hold down the shift key and select more than one column to sort by.

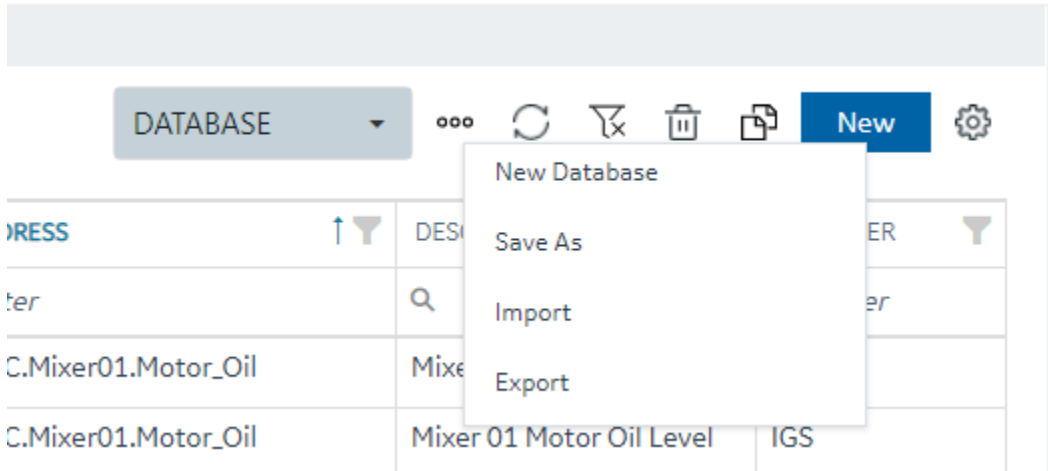


Column Re-Ordering and Resizing

The Tag Name is locked at the left position, but the rest of the columns in the database grid can be re-ordered via drag and drop of the column header with your mouse. Any column can be resized to optimally fit the data you are working on.

Database Toolbar

The toolbar for the Database Details screen contains the following icons:



For more information on these icons, refer to the following table.

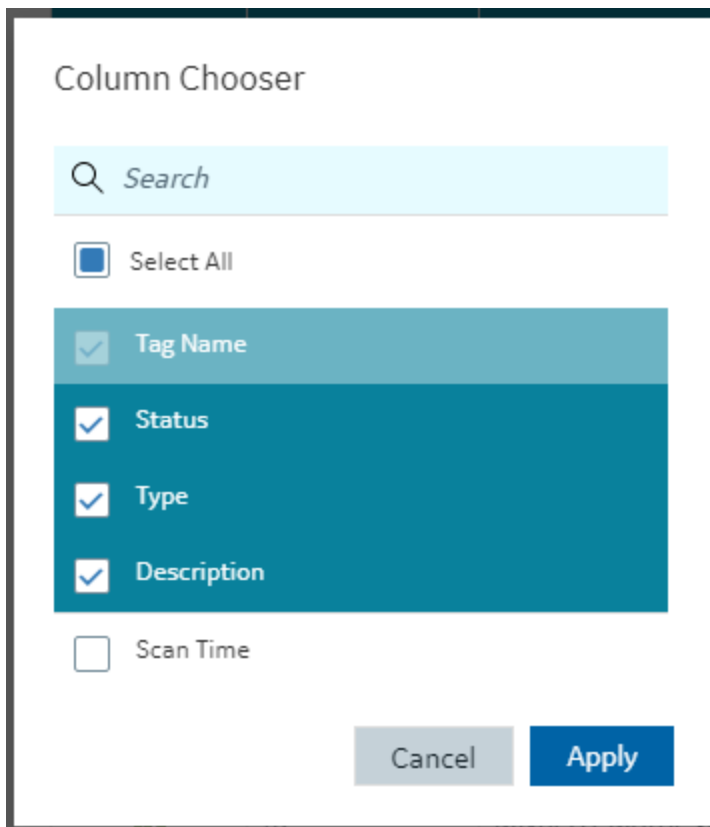
Item	Description
	Click the drop-down to switch to another database.
	Use this button to open a menu that you can use to create a new database, save a database under another name, import, or export a database.
	Use this to refresh your grid view.
	Click here to clear all filters currently applied to the grid.
	Select one or more tags and click this button to delete a tag(s).
	Select a tag and click this button to duplicate an existing currently selected tag. You will be prompted to enter a new name.
	Click the New button to add a new tag to the database.
	Use the settings icon to pick the columns you want to display on the Database view.

Database Column Choosing

The Database panel by default shows the following columns:

- Tag Name (Fixed and always visible)
- Status - This column shows the publish status of the tag (Published, Unpublished, Modified)
- Type - Displays the block type abbreviation (for example: AI, AA, MDI, and so on)
- Description - Tag description
- I/O Driver - The driver configured for the tag
- I/O Address - The IO address of the tag.

Other columns are available to show in the grid by using the column chooser available when you click on the gear settings icon on the far right of the database toolbar.



Database Details Panel

Editing database tags is done via the Details panel after selecting a particular tag in the Database panel.

DETAILS ✕

MIXER01>TANK_LEVEL

🔍 *Search...*

FIELD	VALUE
GENERAL	
Tag Name	MIXER01>TANK_LEVEL
Description	
Type	AI - Analog Input
Current Value	111 ↻
IO ADDRESSING	
LIMITS AND SCALING	
ALARMS OPTIONS	
Alarm Areas	ALL
Enable Alarm	ENABLE
Priority	LOW

- MIXER01>MOTOR_OIL
- MIXER01>MOTOR_SP
- MIXER01>MOTOR_SPEED
- MIXER01>MOTOR_STATE
- MIXER01>MOTOR_TEMP
- MIXER01>NAME
- MIXER01>TANK_LEVEL**
- MIXER01>VALVEIN_STATE
- MIXER01>VALVEOUT_STATE
- MIXER02>MOTOR_OIL
- MIXER02>MOTOR_SP
- MIXER02>MOTOR_SPEED
- MIXER02>MOTOR_STATE
- MIXER02>MOTOR_TEMP
- MIXER02>NAME

The Details panel for the database is made up of property rows with names and values grouped by area. These areas are expandable and collapsible. At the top of the grid is the name of the tag for easy viewing and a search box for filtering and finding the tag property you want to view or configure. The 'Field' and 'View' columns are resizable.

There are different types of properties in the Details panel depending on the type of value being shown or edited. Some are enumerated values with drop down lists, some are text edit boxes and others are numeric edit boxes. Some properties are read only depending on the values of other properties in the grid.

As you make changes on tags, their published status changes to "Modified" and will be applied to the active databases after Publish.

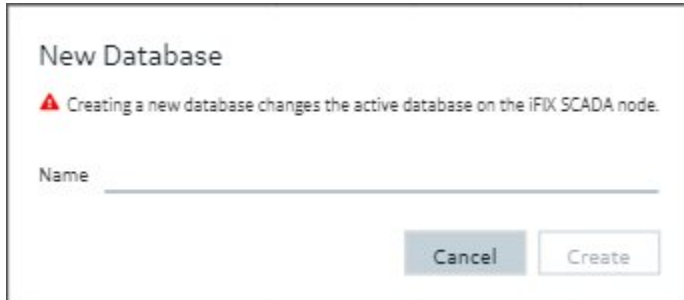
Database Management

Database Management

You can manage your database operations from the Database panel. This includes adding, copying, importing, and exporting your databases.

New Database

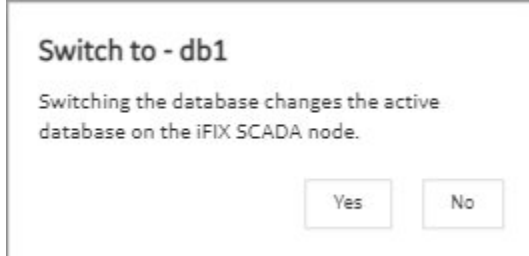
When you create a new database, you will be prompted for a new database name (up to 8 characters). After you choose to create a new database, the currently active database switches to this new empty database.



The dialog box titled "New Database" contains a warning icon and the text "Creating a new database changes the active database on the iFIX SCADA node." Below this is a text input field labeled "Name" with a horizontal line underneath. At the bottom right, there are two buttons: "Cancel" and "Create".

Switching Databases

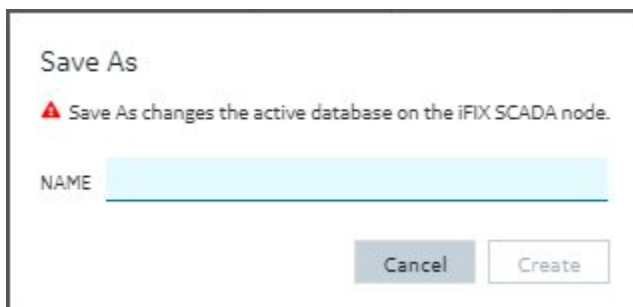
The drop down in the toolbar lets you quickly switch your currently active iFIX database.



The dialog box titled "Switch to - db1" contains the text "Switching the database changes the active database on the iFIX SCADA node." At the bottom, there are two buttons: "Yes" and "No".

Save as Database

The Save As command lets you take your existing active database and save it as a newly named database. This operation will also switch the active database to the newly copied database.



The dialog box titled "Save As" contains a warning icon and the text "Save As changes the active database on the iFIX SCADA node." Below this is a text input field labeled "NAME" with a light blue background and a horizontal line underneath. At the bottom right, there are two buttons: "Cancel" and "Create".

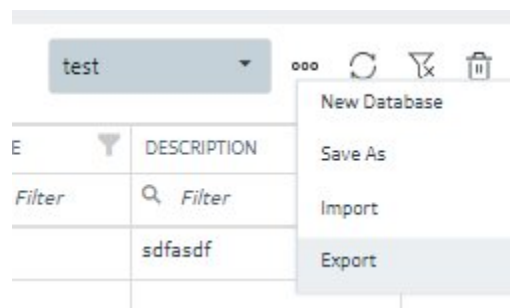
Import or Export a Database

See [Import a Database \(on page 230\)](#) or [Export a Database \(on page 229\)](#).

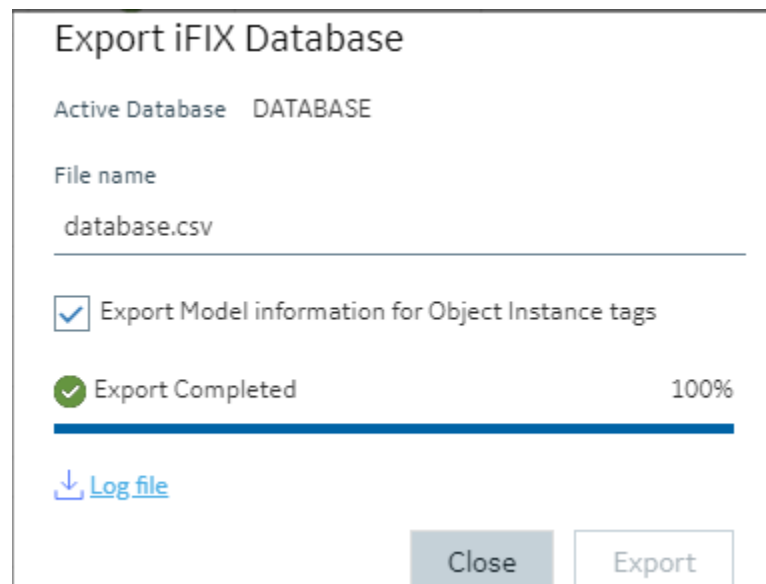
Export a Database

Use the database export when you want to export iFIX tags into a spreadsheet format. These tags can be regular tags (non-model), or both model and non-model tags. Your database is exported in CSV format. You can edit that CSV file in a spreadsheet program and then later import it back into iFIX again.

To export your database, from the Database panel, click the ellipsis (...) icon, and use the drop-down beside the database selector in the toolbar.



When you select the Export option, the Export iFIX Database dialog box appears where you select the options you want and click Export.



The exported file will be automatically downloaded to your browsers in the specified download folder with "export.csv" as the name.

A progress bar keeps you informed of the export progress, especially for larger exports.

After export, you can see the results of the export by clicking on the Log file link to download the log file.

Including/Excluding Model

Exporting your currently active database provides you with an option to export any associated model artifacts that are tied to tags in the database.

Selecting the **Export Model Information for Object Instance Tags** check box (the default) will export the model and associated types and template details. This is most useful when exporting the database to move it to another node or project. Other uses include when you want to back up your model changes, when you want to make bulk changes to the model itself, or to re-import or when you want to use your model in Operations Hub.

Clearing the Export Model Information for Object Instance Tags check box will export just the database tags and their details.

Backwards compatibility

Exports from databases of previous versions of iFIX will import into the new Database Manager.

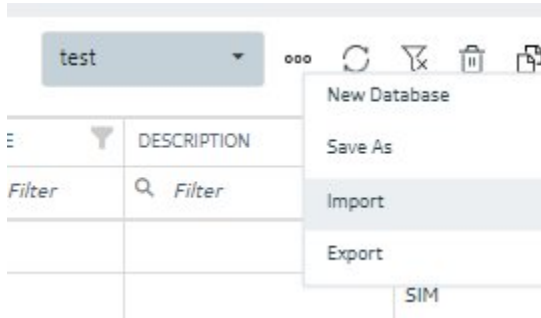
Exporting from the Database panel and importing into older versions of iFIX will also work, however if you choose to export the model associations, these sections will not import and will generate errors.

Import a Database

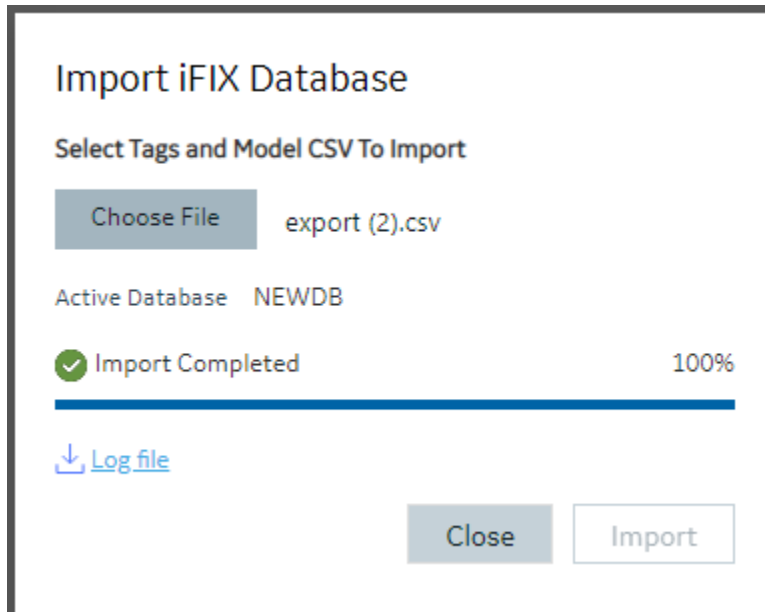
Use the database import when you want to import tags to your iFIX database. These tags can be regular tags (non-model), or both model and non-model tags.

Be aware that Configuration Hub supports only UTF-8 encoded files. The iFIX Database Manager uses ANSI encoding. Prior to importing files into Configuration Hub's Model or Database panel, ensure that the CSV file is in UTF-8 encoding. To do so, open the CSV file in the Windows Notepad editor and perform a SAVE AS with UTF-8 encoding selected, and then save the file as a CSV. Likewise, if you want to import a file from Configuration Hub into the iFIX Database Manager, save as ANSI encoding before importing the file into the Database Manager.

1. Configuration Hub, on the Database panel, click the ellipsis (...) icon to open the shortcut menu.



2. Click Import.



The Import iFIX Database dialog box appears.

3. Click Choose File to select a file to import.
4. Click Import.

Configuring Custom Blocks

For custom blocks to function properly within Configuration Hub, two supporting files are required.

- `block-name.gov`
- `block-name_details.json`

In the above examples, *block-name* is the name of the custom block (e.g., for the D16 block, the files would be named `D16.gov` and `D16_details.json`).

When using the block tool kit to create custom blocks, the utility creates the .gov file; it is up to the user to create the .json file and save it in the C:\Program Files (x86)\Proficy\iFIX\PDB\ folder.

The basic structure of the .json file is:

- `type_name`: the name of the custom block (e.g., `"type_name": "D16"`)
- *Category* elements outline the logical groupings of items in the details display. Using the D16 block as an example, its categories are `General`, `IO_Addresssing`, `Device_States`, `Alarms_Options`, `E-Signature`, and `Advanced_Options`. Within each of these elements, there is a *Rank* entry that specifies the display order. For example:
 - `"rank": 1` will display at the top of the details pane
 - `"rank": 2` will display next, etc.

Within each of the categories are individual listings of the block fields to be displayed under that heading. For example, the fields listed under the `General` heading of the D16 block are:

```
"General": [
  {
    "A_TAG": {
      "default": "",
      "enum": "",
      "datatype": "string",
      "validators": [
        "TagCommonValidators.maxLength",
        "TagCommonValidators.tagName"
      ]
    }
  },
  {
    "A_DESC": {
      "default": "",
      "enum": "",
      "datatype": "string",
      "validators": [
        "TagCommonValidators.maxLength"
      ]
    }
  },
  {
```

```
"rank": 2
}
```

The behavior of display and input is controlled by these entries. In this example, the tag name ("A_TAG") and description ("A_DESC") are listed in the `General` category. These must correspond to actual field names available in the block. A complete list of field names and their descriptions can be obtained by creating the custom blocks in the iFIX Database Manager and exporting the resulting PDB file to a CSV file, which can be opened (e.g., using Excel) to list the field names and their corresponding descriptions.

Elements are assigned a `datatype`, such as `string` or `number`, and can be given an enumeration set to limit the values entered to those defined in the enumeration set. The possible values will display as a drop-down list for the field. A sample of this is demonstrated in the E-Signature section of the `D16_details.json` file (at the bottom of this page).

```
"enum": [
    "YES",
    "NO"
]
```

- Additionally, validation criteria can be provided to stipulate allowable entries for each field. This behavior is controlled by the "validators" section for the tag field. Some commonly used validators are:
 - `TagCommonValidators.maxLength`: Verifies that the value does not exceed the field's maximum length, which is obtained from the .gov file. For example, `field_length` is used to determine the length (for `tagname` it will be 256).
 - `TagCommonValidators.tagName`: Checks for the tag name characters and matches the validation to that in the iFIX Database Manager. It also checks for duplicates in the current database. For example, the following special characters cannot be in the iFIX tag name - `~ ` + ^ : ? " * = { } . , ; ? @`
 - `TagCommonValidators.ioAddress`: This validator applies only to the SIM driver. The value cannot be more than 2000; if a bit value is used, it cannot be more than 15.
 - `TagCommonValidators.isIntegerValidation`: Checks if it is a numeric value, otherwise the input is rejected.
 - `TagCommonValidators.minValue`: Based on the value of `field_min` in the .gov file.
 - `TagCommonValidators.maxValue`: Based on the value of `field_max` in the .gov file.
 - `TagCommonValidators.isEmpty`: Checks if the value is empty.
 - `TagCommonValidators.scanTime`: Matches to the iFIX Database Manager input for scan time.
 - `TagCommonValidators.blockName`: Similar to `tagName`, but does not check for a duplicate tag name in the database.

- `TagCommonValidators.maxPrecision`: Based on the value of `field_precision` in the `.gov` file.
- `TagCommonValidators.eguValuesNotEqual`: This validator checks if the value is within EGU limits. If the value matches EGU limit values, it is rejected.
- `TagCommonValidators.invalidNumericFormat`: Confirms that the number format matches the locale. Only default number formats for a given locale are supported.

**Note:**

Depending on the complexity of your custom block, it is recommended to use the `TXT_details.json` (simpler) or `D16_details.json` (more complex) as a template.

TXT_details.json

```
{
  "tag_type": [
    {
      "type_name": "TXT",
      "category": {
        "General": [
          {
            "A_TAG": {
              "default": "",
              "enum": "",
              "datatype": "string",
              "validators": [
                "TagCommonValidators.maxLength",
                "TagCommonValidators.tagName"
              ]
            }
          },
          {
            "A_DESC": {
              "default": "",
              "enum": "",
              "datatype": "string",
              "validators": [
                "TagCommonValidators.maxLength"
              ]
            }
          }
        ]
      }
    }
  ]
}
```

```

    },
    {
        "rank": 1
    }
],
"IO_Addressing": [
    {
        "A_IODV": {
            "default": "SIM",
            "enum": [
                ""
            ],
            "datatype": "string"
        }
    },
    {
        "A_IOAD": {
            "default": "0",
            "enum": "",
            "datatype": "string",
            "validators": [
                "TagCommonValidators.maxLength",
                "TagCommonValidators.ioAddress"
            ]
        }
    },
    {
        "A_IOSC": {
            "default": "None",
            "drivers": [],
            "enum": [
                ""
            ],
            "datatype": "string"
        }
    },
    {

```

```

    "A_IOHT": {
        "default": "None",
        "enum": [
            "None"
        ],
        "datatype": "string"
    }
},
{
    "rank": 2
}
],
"Limits_and_Scaling": [
    {
        "A_ELO": {
            "default": "0.00",
            "field_min": "-3.4E+38",
            "field_max": "3.4E+38",
            "field_precision": "16",
            "enum": "",
            "datatype": "number",
            "validators": [
                "TagCommonValidators.minValue",
                "TagCommonValidators.maxValue",
                "TagCommonValidators.maxPrecision",
                "TagCommonValidators.isEmpty",
                "TagCommonValidators.eguValuesNotEqual"
            ]
        }
    },
    {
        "A_EHI": {
            "default": "100.00",
            "field_min": "-3.4E+38",
            "field_max": "3.4E+38",
            "field_precision": "16",
            "enum": "",

```

```

        "datatype": "number",
        "validators": [
            "TagCommonValidators.minValue",
            "TagCommonValidators.maxValue",
            "TagCommonValidators.maxPrecision",
            "TagCommonValidators.isEmpty",
            "TagCommonValidators.eguValuesNotEqual"
        ]
    }
},
{
    "A_EGUDESC": {
        "default": "",
        "enum": "",
        "datatype": "string",
        "validators": [
            "TagCommonValidators.maxLength"
        ]
    }
},
{
    "rank": 3
}
],
"Text Strings": [
    {
        "TR0": {
            "default": "1",
            "field_min": "1",
            "field_max": "65535",
            "enum": "",
            "datatype": "number",
            "validators": [
                "TagCommonValidators.maxLength",
                "TagCommonValidators.isIntegerValidation",
                "TagCommonValidators.minValue",
                "TagCommonValidators.maxValue"
            ]
        }
    }
]

```

```

    ]
  }
},
{
  "A_TS0": {
    "default": "",
    "enum": "",
    "datatype": "string",
    "validators": [
      "TagCommonValidators.maxLength"
    ]
  }
},
{
  "TR1": {
    "default": "2",
    "field_min": "1",
    "field_max": "65535",
    "enum": "",
    "datatype": "number",
    "validators": [
      "TagCommonValidators.maxLength",
      "TagCommonValidators.isIntegerValidation",
      "TagCommonValidators.minValue",
      "TagCommonValidators.maxValue"
    ]
  }
},
{
  "A_TS1": {
    "default": "",
    "enum": "",
    "datatype": "string",
    "validators": [
      "TagCommonValidators.maxLength"
    ]
  }
}

```



```
},  
{  
  "TR2": {  
    "default": "4",  
    "field_min": "1",  
    "field_max": "65535",  
    "enum": "",  
    "datatype": "number",  
    "validators": [  
      "TagCommonValidators.maxLength",  
      "TagCommonValidators.isIntegerValidation",  
      "TagCommonValidators.minValue",  
      "TagCommonValidators.maxValue"  
    ]  
  }  
},  
{  
  "A_TS2": {  
    "default": "",  
    "enum": "",  
    "datatype": "string",  
    "validators": [  
      "TagCommonValidators.maxLength"  
    ]  
  }  
},  
{  
  "TR3": {  
    "default": "8",  
    "field_min": "1",  
    "field_max": "65535",  
    "enum": "",  
    "datatype": "number",  
    "validators": [  
      "TagCommonValidators.maxLength",  
      "TagCommonValidators.isIntegerValidation",  
      "TagCommonValidators.minValue",
```

```
        "TagCommonValidators.maxValue"
    ]
}
},
{
    "A_TS3": {
        "default": "",
        "enum": "",
        "datatype": "string",
        "validators": [
            "TagCommonValidators.maxLength"
        ]
    }
},
{
    "TR4": {
        "default": "16",
        "field_min": "1",
        "field_max": "65535",
        "enum": "",
        "datatype": "number",
        "validators": [
            "TagCommonValidators.maxLength",
            "TagCommonValidators.isIntegerValidation",
            "TagCommonValidators.minValue",
            "TagCommonValidators.maxValue"
        ]
    }
},
{
    "A_TS4": {
        "default": "",
        "enum": "",
        "datatype": "string",
        "validators": [
            "TagCommonValidators.maxLength"
        ]
    }
}
```

```

    }
  },
  {
    "TR5": {
      "default": "32",
      "field_min": "1",
      "field_max": "65535",
      "enum": "",
      "datatype": "number",
      "validators": [
        "TagCommonValidators.maxLength",
        "TagCommonValidators.isIntegerValidation",
        "TagCommonValidators.minValue",
        "TagCommonValidators.maxValue"
      ]
    }
  },
  {
    "A_TS5": {
      "default": "",
      "enum": "",
      "datatype": "string",
      "validators": [
        "TagCommonValidators.maxLength"
      ]
    }
  },
  {
    "TR6": {
      "default": "64",
      "field_min": "1",
      "field_max": "65535",
      "enum": "",
      "datatype": "number",
      "validators": [
        "TagCommonValidators.maxLength",
        "TagCommonValidators.isIntegerValidation",

```



```
    ]
  }
},
{
  "TR8": {
    "default": "256",
    "field_min": "1",
    "field_max": "65535",
    "enum": "",
    "datatype": "number",
    "validators": [
      "TagCommonValidators.maxLength",
      "TagCommonValidators.isIntegerValidation",
      "TagCommonValidators.minValue",
      "TagCommonValidators.maxValue"
    ]
  }
},
{
  "A_TS8": {
    "default": "",
    "enum": "",
    "datatype": "string",
    "validators": [
      "TagCommonValidators.maxLength"
    ]
  }
},
{
  "TR9": {
    "default": "512",
    "field_min": "1",
    "field_max": "65535",
    "enum": "",
    "datatype": "number",
    "validators": [
      "TagCommonValidators.maxLength",
```

```

        "TagCommonValidators.isIntegerValidation",
        "TagCommonValidators.minValue",
        "TagCommonValidators.maxValue"
    ]
}
},
{
    "A_TS9": {
        "default": "",
        "enum": "",
        "datatype": "string",
        "validators": [
            "TagCommonValidators.maxLength"
        ]
    }
},
{
    "TR10": {
        "default": "1024",
        "field_min": "1",
        "field_max": "65535",
        "enum": "",
        "datatype": "number",
        "validators": [
            "TagCommonValidators.maxLength",
            "TagCommonValidators.isIntegerValidation",
            "TagCommonValidators.minValue",
            "TagCommonValidators.maxValue"
        ]
    }
},
{
    "A_TS10": {
        "default": "",
        "enum": "",
        "datatype": "string",
        "validators": [

```

```

        "TagCommonValidators.maxLength"
    ]
}
},
{
    "TR11": {
        "default": "2048",
        "field_min": "1",
        "field_max": "65535",
        "enum": "",
        "datatype": "number",
        "validators": [
            "TagCommonValidators.maxLength",
            "TagCommonValidators.isIntegerValidation",
            "TagCommonValidators.minValue",
            "TagCommonValidators.maxValue"
        ]
    }
},
{
    "A_TS11": {
        "default": "",
        "enum": "",
        "datatype": "string",
        "validators": [
            "TagCommonValidators.maxLength"
        ]
    }
},
{
    "TR12": {
        "default": "4096",
        "field_min": "1",
        "field_max": "65535",
        "enum": "",
        "datatype": "number",
        "validators": [

```

```
        "TagCommonValidators.maxLength",
        "TagCommonValidators.isIntegerValidation",
        "TagCommonValidators.minValue",
        "TagCommonValidators.maxValue"
    ]
}
},
{
    "A_TS12": {
        "default": "",
        "enum": "",
        "datatype": "string",
        "validators": [
            "TagCommonValidators.maxLength"
        ]
    }
},
{
    "TR13": {
        "default": "8192",
        "field_min": "1",
        "field_max": "65535",
        "enum": "",
        "datatype": "number",
        "validators": [
            "TagCommonValidators.maxLength",
            "TagCommonValidators.isIntegerValidation",
            "TagCommonValidators.minValue",
            "TagCommonValidators.maxValue"
        ]
    }
},
{
    "A_TS13": {
        "default": "",
        "enum": "",
        "datatype": "string",
```



```

        "validators": [
            "TagCommonValidators.maxLength"
        ]
    },
},
{
    "TR14": {
        "default": "16384",
        "field_min": "1",
        "field_max": "65535",
        "enum": "",
        "datatype": "number",
        "validators": [
            "TagCommonValidators.maxLength",
            "TagCommonValidators.isIntegerValidation",
            "TagCommonValidators.minValue",
            "TagCommonValidators.maxValue"
        ]
    }
},
{
    "A_TS14": {
        "default": "",
        "enum": "",
        "datatype": "string",
        "validators": [
            "TagCommonValidators.maxLength"
        ]
    }
},
{
    "TR15": {
        "default": "32768",
        "field_min": "1",
        "field_max": "65535",
        "enum": "",
        "datatype": "number",

```

```

        "validators": [
            "TagCommonValidators.maxLength",
            "TagCommonValidators.isIntegerValidation",
            "TagCommonValidators.minValue",
            "TagCommonValidators.maxValue"
        ]
    }
},
{
    "A_TS15": {
        "default": "",
        "enum": "",
        "datatype": "string",
        "validators": [
            "TagCommonValidators.maxLength"
        ]
    }
},
{
    "A_TS16": {
        "default": "",
        "enum": "",
        "datatype": "string",
        "validators": [
            "TagCommonValidators.maxLength"
        ]
    }
},
{
    "rank": 4
}
],
"E-Signature": [
    {
        "A_ESIGTYPE": {
            "default": "NONE",
            "enum": [

```

```

        "NONE",
        "PERFONLY",
        "PERFVERI"
    ],
    "datatype": "string"
}
},
{
    "A_ESIGCONT": {
        "default": "YES",
        "enum": [
            "YES",
            "NO"
        ],
        "datatype": "string"
    }
},
{
    "A_ESIGACK": {
        "default": "NO",
        "enum": [
            "YES",
            "NO"
        ],
        "datatype": "string"
    }
},
{
    "A_ESIGREQ_COMMENT": {
        "default": "NO",
        "enum": [
            "YES",
            "NO"
        ],
        "datatype": "string"
    }
},

```

```

    {
      "A_ESIGTRAP": {
        "default": "REJECT",
        "enum": [
          "REJECT",
          "ACCEPT",
          "LOG"
        ],
        "datatype": "string"
      }
    },
    {
      "rank": 5
    }
  ],
  "Advanced_Options": [
    {
      "A_OUT": {
        "default": "NO",
        "enum": [
          "YES",
          "NO"
        ],
        "datatype": "string"
      }
    },
    {
      "A_CASE": {
        "default": "NO",
        "enum": [
          "YES",
          "NO"
        ],
        "datatype": "string"
      }
    }
  ],
  {

```

```
"Security_Areas": {  
  "default": "NONE",  
  "enum": [  
    ""  
  ],  
  "datatype": "string",  
  "applies_to": [  
    "A_SA1",  
    "A_SA2",  
    "A_SA3"  
  ]  
}  
,  
{  
  "A_SA1": {  
    "default": "NONE",  
    "enum": "",  
    "datatype": "string",  
    "validators": [  
      "TagCommonValidators.maxLength"  
    ]  
  }  
},  
{  
  "A_SA2": {  
    "default": "NONE",  
    "enum": "",  
    "datatype": "string",  
    "validators": [  
      "TagCommonValidators.maxLength"  
    ]  
  }  
},  
{  
  "A_SA3": {  
    "default": "NONE",  
    "enum": "",
```

```
        "datatype": "string",
        "validators": [
            "TagCommonValidators.maxLength"
        ]
    },
    {
        "A_ALMEXT1": {
            "default": "",
            "enum": "",
            "datatype": "string",
            "validators": [
                "TagCommonValidators.maxLength"
            ]
        },
        {
            "A_ALMEXT2": {
                "default": "",
                "enum": "",
                "datatype": "string",
                "validators": [
                    "TagCommonValidators.maxLength"
                ]
            },
            {
                "rank": 6
            }
        }
    }
}
```

D16_details.json

```
{
  "tag_type": [
    {
      "type_name": "D16",
      "category": {
        "General": [
          {
            "A_TAG": {
              "default": "",
              "enum": "",
              "datatype": "string",
              "validators": [
                "TagCommonValidators.maxLength",
                "TagCommonValidators.tagName"
              ]
            },
            "A_DESC": {
              "default": "",
              "enum": "",
              "datatype": "string",
              "validators": [
                "TagCommonValidators.maxLength"
              ]
            }
          },
          {
            "rank": 1
          }
        ],
        "IO_addressing": [
          {
            "A_MODE": {
              "default": "A",
              "enum": [
```

```

        "A",
        "D"
    ],
    "datatype": "string"
}
},
{
    "A_IODV": {
        "default": "SIM",
        "enum": [
            ""
        ],
        "datatype": "string"
    }
},
{
    "A_IOAD": {
        "default": "0",
        "enum": "",
        "datatype": "string",
        "validators": [
            "TagCommonValidators.maxLength",
            "TagCommonValidators.ioAddress"
        ]
    }
},
{
    "A_COUNT": {
        "default": "16",
        "enum": "",
        "datatype": "string",
        "field_min": "1",
        "field_max": "16",
        "validators": [
            "TagCommonValidators.maxLength",
            "TagCommonValidators.isIntegerValidation",
            "TagCommonValidators.minValue",

```



```

        "TagCommonValidators.maxValue",
        "TagCommonValidators.isEmpty"
    ]
}
},
{
    "A_IOHT": {
        "default": "None",
        "enum": [
            "None"
        ],
        "datatype": "string"
    }
},
{
    "A_SCANT": {
        "default": "1",
        "enum": "",
        "ProcessByException": "",
        "PhaseAt": "",
        "datatype": "number",
        "validators": [
            "TagCommonValidators.maxLength",
            "TagCommonValidators.scanTime"
        ]
    }
},
{
    "rank": 2
}
],
"Device_States": [
    {
        "A_LABEL[00]": {
            "default": "",
            "enum": "",
            "datatype": "string",

```

```
        "validators": [  
            "TagCommonValidators.maxLength"  
        ]  
    }  
},  
{  
    "A_AE[00]": {  
        "default": "N",  
        "enum": [  
            "Y",  
            "N"  
        ],  
        "datatype": "string"  
    }  
},  
{  
    "A_INVERT[00]": {  
        "default": "N",  
        "enum": [  
            "Y",  
            "N"  
        ],  
        "datatype": "string"  
    }  
},  
{  
    "A_LABEL[01]": {  
        "default": "",  
        "enum": "",  
        "datatype": "string",  
        "validators": [  
            "TagCommonValidators.maxLength"  
        ]  
    }  
},  
{  
    "A_AE[01]": {
```

```
        "default": "N",
        "enum": [
            "Y",
            "N"
        ],
        "datatype": "string"
    }
},
{
    "A_INVERT[01]": {
        "default": "N",
        "enum": [
            "Y",
            "N"
        ],
        "datatype": "string"
    }
},
{
    "A_LABEL[02]": {
        "default": "",
        "enum": "",
        "datatype": "string",
        "validators": [
            "TagCommonValidators.maxLength"
        ]
    }
},
{
    "A_AE[02]": {
        "default": "N",
        "enum": [
            "Y",
            "N"
        ],
        "datatype": "string"
    }
}
```

```
    },
    {
      "A_INVERT[02]": {
        "default": "N",
        "enum": [
          "Y",
          "N"
        ],
        "datatype": "string"
      }
    },
    {
      "A_LABEL[03]": {
        "default": "",
        "enum": "",
        "datatype": "string",
        "validators": [
          "TagCommonValidators.maxLength"
        ]
      }
    },
    {
      "A_AE[03]": {
        "default": "N",
        "enum": [
          "Y",
          "N"
        ],
        "datatype": "string"
      }
    },
    {
      "A_INVERT[03]": {
        "default": "N",
        "enum": [
          "Y",
          "N"
        ]
      }
    }
  ]
}
```

```
    ],
    "datatype": "string"
  }
},
{
  "A_LABEL[04]": {
    "default": "",
    "enum": "",
    "datatype": "string",
    "validators": [
      "TagCommonValidators.maxLength"
    ]
  }
},
{
  "A_AE[04]": {
    "default": "N",
    "enum": [
      "Y",
      "N"
    ],
    "datatype": "string"
  }
},
{
  "A_INVERT[04]": {
    "default": "N",
    "enum": [
      "Y",
      "N"
    ],
    "datatype": "string"
  }
},
{
  "A_LABEL[05]": {
    "default": "",
```

```

        "enum": "",
        "datatype": "string",
        "validators": [
            "TagCommonValidators.maxLength"
        ]
    },
    {
        "A_AE[05]": {
            "default": "N",
            "enum": [
                "Y",
                "N"
            ],
            "datatype": "string"
        }
    },
    {
        "A_INVERT[05]": {
            "default": "N",
            "enum": [
                "Y",
                "N"
            ],
            "datatype": "string"
        }
    },
    {
        "A_LABEL[06]": {
            "default": "",
            "enum": "",
            "datatype": "string",
            "validators": [
                "TagCommonValidators.maxLength"
            ]
        }
    }
},

```

```
{
  "A_AE[06]": {
    "default": "N",
    "enum": [
      "Y",
      "N"
    ],
    "datatype": "string"
  }
},
{
  "A_INVERT[06]": {
    "default": "N",
    "enum": [
      "Y",
      "N"
    ],
    "datatype": "string"
  }
},
{
  "A_LABEL[07]": {
    "default": "",
    "enum": "",
    "datatype": "string",
    "validators": [
      "TagCommonValidators.maxLength"
    ]
  }
},
{
  "A_AE[07]": {
    "default": "N",
    "enum": [
      "Y",
      "N"
    ],
    ],

```

```

        "datatype": "string"
    }
},
{
    "A_INVERT[07]": {
        "default": "N",
        "enum": [
            "Y",
            "N"
        ],
        "datatype": "string"
    }
},
{
    "A_LABEL[08]": {
        "default": "",
        "enum": "",
        "datatype": "string",
        "validators": [
            "TagCommonValidators.maxLength"
        ]
    }
},
{
    "A_AE[08]": {
        "default": "N",
        "enum": [
            "Y",
            "N"
        ],
        "datatype": "string"
    }
},
{
    "A_INVERT[08]": {
        "default": "N",
        "enum": [

```



```

        "Y",
        "N"
    ],
    "datatype": "string"
}
},
{
    "A_LABEL[09]": {
        "default": "",
        "enum": "",
        "datatype": "string",
        "validators": [
            "TagCommonValidators.maxLength"
        ]
    }
},
{
    "A_AE[09]": {
        "default": "N",
        "enum": [
            "Y",
            "N"
        ],
        "datatype": "string"
    }
},
{
    "A_INVERT[09]": {
        "default": "N",
        "enum": [
            "Y",
            "N"
        ],
        "datatype": "string"
    }
},
{

```

```
"A_LABEL[10]": {
    "default": "",
    "enum": "",
    "datatype": "string",
    "validators": [
        "TagCommonValidators.maxLength"
    ]
},
{
    "A_AE[10]": {
        "default": "N",
        "enum": [
            "Y",
            "N"
        ],
        "datatype": "string"
    },
    "A_INVERT[10]": {
        "default": "N",
        "enum": [
            "Y",
            "N"
        ],
        "datatype": "string"
    },
    "A_LABEL[11]": {
        "default": "",
        "enum": "",
        "datatype": "string",
        "validators": [
            "TagCommonValidators.maxLength"
        ]
    }
}
```

```
    }  
  },  
  {  
    "A_AE[11]": {  
      "default": "N",  
      "enum": [  
        "Y",  
        "N"  
      ],  
      "datatype": "string"  
    }  
  },  
  {  
    "A_INVERT[11]": {  
      "default": "N",  
      "enum": [  
        "Y",  
        "N"  
      ],  
      "datatype": "string"  
    }  
  },  
  {  
    "A_LABEL[12]": {  
      "default": "",  
      "enum": "",  
      "datatype": "string",  
      "validators": [  
        "TagCommonValidators.maxLength"  
      ]  
    }  
  },  
  {  
    "A_AE[12]": {  
      "default": "N",  
      "enum": [  
        "Y",
```

```

        "N"
    ],
    "datatype": "string"
}
},
{
    "A_INVERT[12]": {
        "default": "N",
        "enum": [
            "Y",
            "N"
        ],
        "datatype": "string"
    }
},
{
    "A_LABEL[13]": {
        "default": "",
        "enum": "",
        "datatype": "string",
        "validators": [
            "TagCommonValidators.maxLength"
        ]
    }
},
{
    "A_AE[13]": {
        "default": "N",
        "enum": [
            "Y",
            "N"
        ],
        "datatype": "string"
    }
},
{
    "A_INVERT[13]": {

```

```
        "default": "N",
        "enum": [
            "Y",
            "N"
        ],
        "datatype": "string"
    }
},
{
    "A_LABEL[14]": {
        "default": "",
        "enum": "",
        "datatype": "string",
        "validators": [
            "TagCommonValidators.maxLength"
        ]
    }
},
{
    "A_AE[14]": {
        "default": "N",
        "enum": [
            "Y",
            "N"
        ],
        "datatype": "string"
    }
},
{
    "A_INVERT[14]": {
        "default": "N",
        "enum": [
            "Y",
            "N"
        ],
        "datatype": "string"
    }
}
```

```

    },
    {
      "A_LABEL[15]": {
        "default": "",
        "enum": "",
        "datatype": "string",
        "validators": [
          "TagCommonValidators.maxLength"
        ]
      }
    },
    {
      "A_AE[15]": {
        "default": "N",
        "enum": [
          "Y",
          "N"
        ],
        "datatype": "string"
      }
    },
    {
      "A_INVERT[15]": {
        "default": "N",
        "enum": [
          "Y",
          "N"
        ],
        "datatype": "string"
      }
    },
    {
      "rank": 3
    }
  ],
  "Alarms_Options": [
    {

```

```

"Alarm_Areas": {
  "default": "ALL",
  "enum": [
    ""
  ],
  "datatype": "string",
  "applies_to": [
    "A_AREA1",
    "A_AREA2",
    "A_AREA3",
    "A_AREA4",
    "A_AREA5",
    "A_AREA6",
    "A_AREA7",
    "A_AREA8",
    "A_AREA9",
    "A_AREA10",
    "A_AREA11",
    "A_AREA12",
    "A_AREA13",
    "A_AREA14",
    "A_AREA15"
  ]
},
{
  "A_IENAB": {
    "default": "ENABLE",
    "enum": [
      "DISABLE",
      "ENABLE"
    ],
    "datatype": "string"
  }
},
{
  "A_PRI": {

```

```
        "default": "LOW",
        "enum": [
            "INFO",
            "LOW",
            "LOLO",
            "MEDIUM",
            "HIGH",
            "HIHI",
            "CRITICAL"
        ],
        "datatype": "string"
    }
},
{
    "A_AREA1": {
        "default": "ALL",
        "enum": "",
        "datatype": "string",
        "validators": [
            "TagCommonValidators.maxLength"
        ]
    }
},
{
    "A_AREA2": {
        "default": "",
        "enum": "",
        "datatype": "string",
        "validators": [
            "TagCommonValidators.maxLength"
        ]
    }
},
{
    "A_AREA3": {
        "default": "",
        "enum": "",
```



```
        "datatype": "string",
        "validators": [
            "TagCommonValidators.maxLength"
        ]
    }
},
{
    "A_AREA4": {
        "default": "",
        "enum": "",
        "datatype": "string",
        "validators": [
            "TagCommonValidators.maxLength"
        ]
    }
},
{
    "A_AREA5": {
        "default": "",
        "enum": "",
        "datatype": "string",
        "validators": [
            "TagCommonValidators.maxLength"
        ]
    }
},
{
    "A_AREA6": {
        "default": "",
        "enum": "",
        "datatype": "string",
        "validators": [
            "TagCommonValidators.maxLength"
        ]
    }
},
{
```

```
"A_AREA7": {  
    "default": "",  
    "enum": "",  
    "datatype": "string",  
    "validators": [  
        "TagCommonValidators.maxLength"  
    ]  
}  
,  
{  
    "A_AREA8": {  
        "default": "",  
        "enum": "",  
        "datatype": "string",  
        "validators": [  
            "TagCommonValidators.maxLength"  
        ]  
    }  
},  
{  
    "A_AREA9": {  
        "default": "",  
        "enum": "",  
        "datatype": "string",  
        "validators": [  
            "TagCommonValidators.maxLength"  
        ]  
    }  
},  
{  
    "A_AREA10": {  
        "default": "",  
        "enum": "",  
        "datatype": "string",  
        "validators": [  
            "TagCommonValidators.maxLength"  
        ]  
    }  
}
```

```
    }  
  },  
  {  
    "A_AREA11": {  
      "default": "",  
      "enum": "",  
      "datatype": "string",  
      "validators": [  
        "TagCommonValidators.maxLength"  
      ]  
    }  
  },  
  {  
    "A_AREA12": {  
      "default": "",  
      "enum": "",  
      "datatype": "string",  
      "validators": [  
        "TagCommonValidators.maxLength"  
      ]  
    }  
  },  
  {  
    "A_AREA13": {  
      "default": "",  
      "enum": "",  
      "datatype": "string",  
      "validators": [  
        "TagCommonValidators.maxLength"  
      ]  
    }  
  },  
  {  
    "A_AREA14": {  
      "default": "",  
      "enum": "",  
      "datatype": "string",
```

```
        "validators": [
            "TagCommonValidators.maxLength"
        ]
    }
},
{
    "A_AREA15": {
        "default": "",
        "enum": "",
        "datatype": "string",
        "validators": [
            "TagCommonValidators.maxLength"
        ]
    }
},
{
    "A_IALMSHLVENAB": {
        "default": "DISABLE",
        "enum": [
            "ENABLE",
            "DISABLE"
        ],
        "datatype": "string"
    }
},
{
    "A_ALMSHELVEPOLICY": {
        "default": "",
        "enum": [
            ""
        ],
        "datatype": "string"
    }
},
{
    "rank": 4
}
```

```
],  
  
"E-Signature": [  
  {  
    "A_ESIGTYPE": {  
      "default": "NONE",  
      "enum": [  
        "NONE",  
        "PERFONLY",  
        "PERFVERI"  
      ],  
      "datatype": "string"  
    }  
  },  
  {  
    "A_ESIGCONT": {  
      "default": "YES",  
      "enum": [  
        "YES",  
        "NO"  
      ],  
      "datatype": "string"  
    }  
  },  
  {  
    "A_ESIGACK": {  
      "default": "NO",  
      "enum": [  
        "YES",  
        "NO"  
      ],  
      "datatype": "string"  
    }  
  },  
  {  
    "A_ESIGREQ_COMMENT": {  
      "default": "NO",  
      "enum": [  
        "YES",  
        "NO"  
      ],  
      "datatype": "string"  
    }  
  }  
]
```

```

        "YES",
        "NO"
    ],
    "datatype": "string"
}
},
{
    "A_ESIGTRAP": {
        "default": "REJECT",
        "enum": [
            "REJECT",
            "ACCEPT",
            "LOG"
        ],
        "datatype": "string"
    },
    "rank": 5
}
],
"Advanced_Options": [
    {
        "A_ISCAN": {
            "default": "ON",
            "enum": [
                "ON",
                "OFF"
            ],
            "datatype": "string"
        },
        "A_REALM": {
            "default": "YES",
            "enum": [
                "YES",

```

```

        "NO"
    ],
    "datatype": "string"
}
},
{
    "Security_Areas": {
        "default": "NONE",
        "enum": [
            ""
        ],
        "datatype": "string",
        "applies_to": [
            "A_SA1",
            "A_SA2",
            "A_SA3"
        ]
    }
},
{
    "A_SA1": {
        "default": "NONE",
        "enum": "",
        "datatype": "string",
        "validators": [
            "TagCommonValidators.maxLength"
        ]
    }
},
{
    "A_SA2": {
        "default": "NONE",
        "enum": "",
        "datatype": "string",
        "validators": [
            "TagCommonValidators.maxLength"
        ]
    }
}

```

```
    }  
  },  
  {  
    "A_SA3": {  
      "default": "NONE",  
      "enum": "",  
      "datatype": "string",  
      "validators": [  
        "TagCommonValidators.maxLength"  
      ]  
    }  
  },  
  {  
    "A_PREV": {  
      "default": "",  
      "enum": "",  
      "validators": []  
    }  
  },  
  {  
    "A_NEXT": {  
      "default": "",  
      "enum": "",  
      "validators": [  
        "TagCommonValidators.maxLength",  
        "TagCommonValidators.blockName"  
      ]  
    }  
  },  
  {  
    "A_ALMEXT1": {  
      "default": "",  
      "enum": "",  
      "datatype": "string",  
      "validators": [  
        "TagCommonValidators.maxLength"  
      ]  
    }  
  }  
}
```

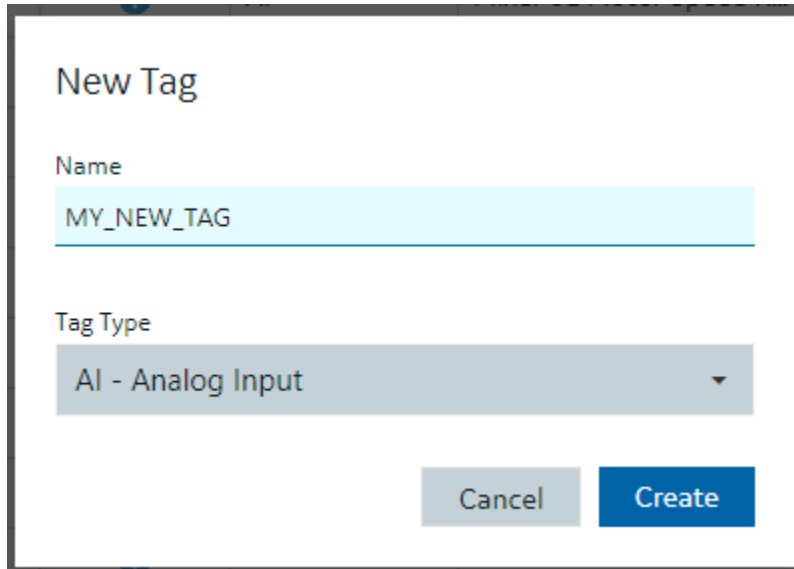


```
    }  
  },  
  {  
    "A_ALMEXT2": {  
      "default": "",  
      "enum": "",  
      "datatype": "string",  
      "validators": [  
        "TagCommonValidators.maxLength"  
      ]  
    }  
  },  
  {  
    "rank": 6  
  }  
]  
}  
]  
}
```

Tag Management

Adding Tags

If you want to add a tag, from the toolbar in Configuration Hub, click the New button. This action will allow you to create a new tag in the iFIX database. When creating a new tag, you are required to choose your Tag Type. The dialog box will show errors if you use characters that are not allowed or if the tag length (256) is too long.



New Tag

Name
MY_NEW_TAG

Tag Type
AI - Analog Input

Cancel Create

Editing Tags

To edit a tag, select it in the Database grid and you will see the Details panel property grid. Find the property you want to change (for example, the I/O address) by either scrolling to the property or searching for it. Making a change to a property will cause the Database panel to go into an unsaved state. When you have made the changes that you want to the tag or to multiple tags, be sure to save your changes, by clicking the Save button. Exiting the panel with unsaved changes will prompt you to save however closing your browser without saving your changes using the Save button will lose your changes.

Deleting or Bulk Deleting Tags

Deleting tags from the Database panel can be accomplished in a few different ways:

- Selecting a row and pressing the delete key.
- Pressing the delete icon in the toolbar.
- Right-clicking a row and selecting Delete will remove the tag from the list and put the panel in an unsaved state.
- Multi-selecting more than one tag using the check boxes in the first column allows you to do bulk deletes.

If you don't want to save your deletions, close the panel, and choose not to save.

Duplicating Tags

The Database panel allows you to select a tag and duplicate it using the toolbar or Right Clicking on a row. Only one tag at a time can be duplicated. You will be prompted to enter a new name for the duplicated tag:

Duplicate Tag

Source Name
MIXER01>MOTOR_OIL

Destination Name
MIXER01>MOTOR_OIL_DUP

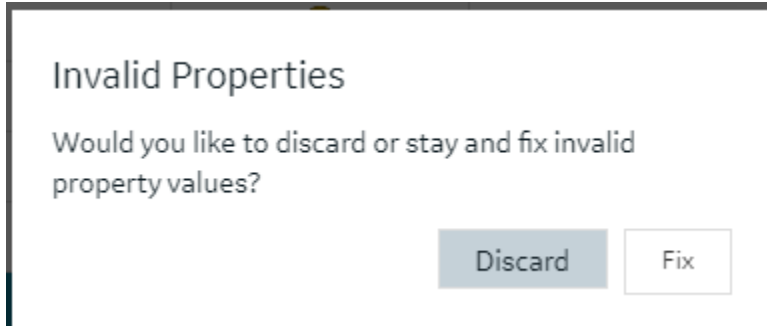
Cancel
Create

Validations

Certain properties of different tag types require input to be of a certain type of format. The Details panel will highlight when you have incorrectly input a value that is not acceptable for a given property. Some properties may become invalid based on other properties. This is indicated by a red shaded and underlined cell color, and a tooltip appears when you hover over the invalid property.

ALARM LIMITS	
Low Low	0
Low	0
High	<u>1,000</u>
High High	<u>1,000</u>
Rate of change	Value entered must be within EGU range
Dead band	50

Generally, you cannot leave a property in an invalid state when leaving the Details panel to select another tag. You will be prompted to revert or stay and fix the invalid property states. An example message is shown in the following graphic.

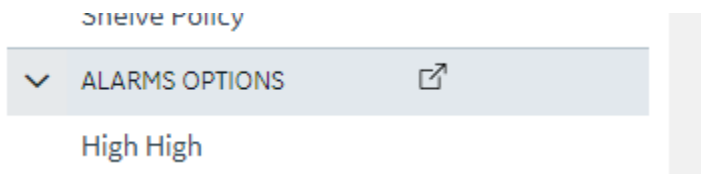


Custom Editors

Some property areas on certain tag types are difficult to understand and edit when flattened into a Field/Value pair properties in the Details panel. In these cases, the Database Details panel will often provide a customized editor, so you have more room to edit the fields. For example:

- The Alarm Options in the AA block.
- The Input Definitions in the PA block.
- The Data Definitions in the SQD block.
- The Programming Statements in the PG block.

Customized editors are indicated in the group/area headers and provide a launch button to open. The following example shows the launch button in the Alarms Options heading.



Here is an example of the dialog box that opens Alarm Options for the AA tag:

Alarms Options

TYPE	VALUE	PRIORITY	CONTACT	OUT MODE	DELAY TIME	RE-ALARM
High High		LOW				
High		LOW				
Low		LOW				
Low Low		LOW				
ROC		LOW				
DEV		LOW				
Other		LOW			00:00:00:00	00:00:00:00

Cancel
Confirm

It is the same content available from the details pane, but just in a larger viewing area. Changes made in the custom dialog boxes are reflected back into the Details panel properties when closed.

Tag Properties

Tag Properties


The following table describes all the tag types (block types) available in the Configuration Hub application.




Note:


iFIX has block types in its database, such as AA (Analog Alarm), AI (Analog Input), and so on. For the purposes of this help document, when we use the term “tag”, we are referring to any block type.


Tag Type	Description
AA Tag (on page 290)	<p>The Analog Alarm (AA) tag sends and receives analog data from the I/O driver, OPC server, or OPC UA server to provide alarm control. Using this tag you can suspend alarms and define limits and priorities for each alarm. The tag can also wait a specified time interval before issuing an alarm,</p>

Tag Type	Description
	close a contact when an alarm occurs, and automatically reissue and acknowledge alarms.
AI Tag (on page 315)	The Analog Input (AI) tag sends and receives analog data from an I/O driver, OPC server, or OPC UA server every time the Scan, Alarm, and Control (SAC) program scans the tag.
AO Tag (on page 348)	The Analog Output (AO) tag sends an analog signal to an I/O driver, OPC server, or OPC UA server every time it receives a value from an upstream tag, an operator, a Program block, a script, or from its Initial Value field.
AR Tag (on page 364)	The Analog Register (AR) tag reads and writes analog values to process hardware. It provides both input and output capacity in a single tag using a minimum amount of memory because iFIX only processes the tag when a picture that references it is open.
BB Tag (on page 386)	The On-Off Control (BB) tag opens and closes up to two digital outputs based upon an incoming analog value or an operator input.
BL Tag (on page 399)	The Boolean (BL) tag calculates a single true/false output from multiple inputs.
CA Tag (on page 417)	<p>The Calculation (CA) tag performs simple mathematical calculations on the value passed by the upstream tag and up to seven other constants or tag values.</p> <div data-bbox="820 1570 1419 1787" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: The precision of calculations is fifteen digits. Round-off errors can occur in the sixteenth digit.</p> </div>
DA Tag (on page 451)	The Digital Alarm (DA) tag sends and receives digital data (1 or 0) from an I/O driver, OPC server, or

Tag Type	Description
	<p>OPC UA server to provide alarm control. Using this tag, you can suspend alarms and define an alarm condition and an alarm priority. The tag can also wait a specified time interval before issuing an alarm, close a contact when an alarm occurs, and automatically reissue and acknowledge alarms.</p>
<p>DC Tag (on page 467)</p>	<p>The Device Control (DC) tag coordinates the opening and closing of digital devices on the plant floor based upon certain user-defined conditions. This tag allows for the timed operation of a device by confirming its status with feedback signals.</p>
<p>DI Tag (on page 481)</p>	<p>The Digital Input (DI) tag sends and receives digital data (1 or 0) from an from the I/O driver, OPC server, or OPC UA server every time the Scan, Alarm, and Control (SAC) program scans the tag.</p>
<p>DO Tag (on page 494)</p>	<p>The Digital Output (DO) tag sends a digital value (1 or 0) to an from the I/O driver, OPC server, or OPC UA server every time it receives a value from an upstream tag, an operator, a Program block, a script, or from its Initial Value field.</p> <p>Because iFIX processes Digital Output tags whenever a new value is sent to the hardware, they generally operate as though they were latched. If you configure a Digital Output tag as a stand alone tag, it outputs a digital value each time the value changes.</p>
<p>DR Tag (on page 504)</p>	<p>The Digital Register (DR) tag reads and writes digital values to process hardware. It provides both input and output capacity in a single tag using a minimum amount of memory because iFIX only processes the tag when a picture that references it is open.</p>

Tag Type	Description
DT Tag <i>(on page 521)</i>	The Dead Time (DT) tag can delay the transfer of an input value to the next tag in the chain.
ETR Tag <i>(on page 530)</i>	<p>The Extended Trend (ETR) tag collects up to 600 values from an upstream tag. By using this tag, you can trend up to 10 minutes worth of data (assuming a one second scan time) with one tag instead of chaining multiple Trend tags together. In addition, you can store several hours, or even days of real-time data, by combining different scan rates in conjunction with the Average Compress field.</p> <p>The upstream primary tag in the chain determines Extended Trend tag's scan time. When the tag receives a value, it stores the data and passes it to the next downstream tag immediately. You can display data collected by the tag using a chart in the iFIX WorkSpace.</p> <div data-bbox="820 1060 1421 1333" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: The process database also provides a Trend tag. This tag trends up to 80 values. If you need to trend more than 80 values, use the Extended Trend tag.</p> </div>
EV Tag <i>(on page 541)</i>	The Event Action (EV) tag tests the value or alarm condition of the previous tag using IF-THEN-ELSE logic. Based upon the outcome of the test expression, the tag can then either open or close a digital point or turn a tag on or off scan.
FN Tag <i>(on page 551)</i>	The Fanout (FN) tag sends the value it receives to the next tag and up to four additional tags. The tag listed as a next tag receives the value immediately. The additional destination tags receive the value the next time iFIX scans those tags. If the destina-

Tag Type	Description
	<p>tion tag is in Manual mode, the update is instantaneous.</p>
<p>HS Tag (on page 570)</p>	<p>The Histogram (HS) tag records how frequently a value occurs during a specified period.</p>
<p>LL Tag (on page 588)</p>	<p>The Lead Lag (LL) tag allows you to simulate process dynamics by combining the advantages of lead and lag compensation strategies.</p> <div data-bbox="821 640 1421 909" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Tip: We suggest you use this tag only if you are thoroughly familiar with lead lag theory. If you simply need a time delay, consider using the Dead Time tag.</p> </div> <p>The Lead Lag formula is:</p> $\text{Output} = C3[C1(\text{Input} - \text{Prior Output}) + (\text{Input} * \text{Scan time}) + C2(\text{Prior Output})]$ <p>where:</p> <ul style="list-style-type: none"> C1 = Lead Time C2 = Lag Time C3 = $\frac{K}{C2 + \text{Scan Time}}$ <p>C1, C2, and the scan time (of the primary tag) are in seconds. K is the constant defined in the tag's Constant field.</p>
<p>MDI Tag (on page 598)</p>	<p>The Multistate Digital Input (MDI) tag provides a means of monitoring the state of one, two, or three related digital inputs. The tag produces a raw input value (0 - 7) based on digital values it receives from an from the I/O driver, OPC server, or OPC UA server every time the Scan, Alarm, and Control (SAC) program scans the tag.</p>

Tag Type	Description
PA Tag (on page 626)	<p>The Pareto (PA) tag can accept up to eight inputs and calculate percentages for them.</p>
PG Tag (on page 641)	<p>The Program (PG) tag provides a powerful means of running short programs to increase the degree of automation in your process or to assist in batch control. For a list of the supported commands that you can use in programming statements see the iFIX Database Reference.</p>
PID Tag (on page 659)	<p>The PID tag maintains balance in a closed loop by changing the controlled variable (an analog output) in response to deviations from a user-defined set point. The difference between the actual value (an analog input) and the set point value is the error, or deviation.</p> <p>In response to errors, the PID tag calculates an appropriate control output signal, which attempts to reduce the error to zero. The adjustment that the PID tag makes is a function of the difference between the set point and the measurement, in addition to the values of the proportional band, the reset, and the rate.</p>
RB Tag (on page 676)	<p>The Ratio Bias (RB) tag lets you change an incoming signal by adding a constant (bias) and/or by multiplying by a constant (ratio). The tag calculates the constant by subtracting an offset from the signal.</p> <p>The following equation illustrates this method:</p> $\text{Output} = \text{Ratio} (\text{Input} - \text{Offset}) + \text{Bias}$ <div data-bbox="820 1690 1421 1816" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: This is a variation of $y = mx + b$.</p> </div>

Tag Type	Description
RM Tag (on page 686)	The Ramp (RM) tag decreases or increases a target output value. The tag provides up to three stages for ramping values. Each ramp stage lets you specify a target value and a ramp rate. The first two stages also provide a hold time. At each scan cycle, the Ramp tag sends its output value to the tag specified in the Next Block field .
SC Tag (on page 701)	The Statistical Control (SC) tag lets you adjust a value from another tag by calculating the average offset and the rate of deviation from the average XBARBAR.
SD Tag (on page 711)	The Statistical Data (SD) tag collects and performs statistical calculations on data.
SQD Tag (on page 727)	The SQL Data (SQD) tag identifies the data to read or write when a SQL Trigger tag executes. The SQL Data tag transfers data between the iFIX process database and your relational database.
SQT Tag (on page 736)	The SQL Trigger (SQT) tag lets iFIX execute SQL commands.
SS Tag (on page 752)	The Signal Select (SS) tag provides a means of sampling up to six inputs, manipulating the inputs according to a user-selected mode, and sending the result to the next tag.
TM Tag (on page 769)	The Timer (TM) tag functions as a time counter by incrementing or decrementing its value.
TR Tag (on page 780)	<p>The Trend (TR) tag can collect up to 80 values over a period of time. You can trend these values by connecting the tag to a chart in the iFIX Workspace.</p> <p>The upstream primary tag in the chain determines Trend tag's scan time. When the tag receives a value, it stores the data and passes it with negligible</p>

Tag Type	Description
	dead time (transportation delay) to the next downstream tag immediately.
TT Tag (on page 790)	The Totalizer (TT) tag maintains a floating-point total for values passed to it from upstream tags.
TX Tag (on page 799)	The Text (TX) tag reads and writes text from your process hardware or an OPC server. When the tag receives text, it sends the data to all enabled alarm destinations assigned to the tag's alarm areas.

AA Tag

This tag contains the following details:




General



Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([),</p>

Field	Description
	<p>close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <p>~ ` + ^ : ? " * = { } . , ; ? @</p> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

I/O Addressing

Field	Description
I/O Driver	<p>Lets you select an I/O driver, OPC server, or OPC UA server for the tag. The selected driver or server enables the tag to communicate with process hardware on the plant floor.</p> <p>Before you can select an I/O driver, OPC server, or OPC UA server you must install it and add it to the available ones in the SCU.</p>


Field	Description
I/O Address	<p>Lets you enter the location in the process hardware where data for this tag is saved and where output is sent.</p> <p>Valid Entries</p> <p>Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations.</p> <div data-bbox="824 667 1419 978" style="border: 1px solid black; border-radius: 10px; background-color: #fff9c4; padding: 10px; margin-bottom: 10px;"> <p> CAUTION:</p> <p>Do not assign the same I/O address to tags when using exception-based and time-based processing. Doing so will cause the exception-based tags to occasionally miss a value.</p> </div> <div data-bbox="824 1010 1419 1451" style="border: 1px solid black; border-radius: 10px; background-color: #fff9c4; padding: 10px;"> <p> CAUTION:</p> <p>Configuration Hub currently does not do I/O address validations before publish. If you enter an invalid IO address into a tag or generate an invalid I/O address via the model and substitutions, the publish may fail to set the IO address into the active database, and your invalid IO address will be removed.</p> </div>
Signal Conditioning	<p>Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p> <div data-bbox="824 1640 1419 1787" style="border: 1px solid black; border-radius: 10px; background-color: #e1f5fe; padding: 10px;"> <p> Note:</p> <p>Signal conditioning and linear scaling cannot be applied simultaneously. If you se-</p> </div>



Field	Description
	<div data-bbox="824 268 1419 373" style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px;">  Select a value for Signal Conditioning verify that Linear Scaling is not selected. </div> <p>Valid Entries</p> <p>Depends on your driver or server. Refer to your driver or server manual for more information.</p>
H/W Options	<p>Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p> <div data-bbox="824 743 1419 1010" style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px;">  Note: Signal conditioning and linear scaling cannot be applied simultaneously. If you select a value for Signal Conditioning verify that Linear Scaling is not selected. </div> <p>Valid Entries</p> <p>Depends on your driver or server. Refer to your driver or server manual for more information.</p>
Process by Exception	Enables exception-based processing for the tag.
Scan Time	<p>Lets you specify how often the Scan, Alarm, and Control (SAC) program processes the tag and any tags (blocks) chained to it.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • 0 (one shot processing) • 0.05 to .95 in .05 increments (subsecond scan times) • 1 to 60 in 1 second increments • 1M to 60M in 1 minute increments • 1H to 24H in 1 hour increments <p>Example</p>




Field	Description
	<p>0.15 specifies a 15-subsecond scan time. 5 specifies a 5-second scan time, 10M specifies a 10-minute scan time, 16H specifies a 16-hour scan time.</p>
Phase At	<p>Lets you specify how long the Scan, Alarm, and Control (SAC) program delays in scanning the tag. When the tag has a second or subsecond scan time, SAC offsets the initial scan by the phase time when iFIX starts or when the database is reloaded. When the tag has a scan time of 1 minute or longer, SAC offsets the initial scan starting at midnight.</p> <p>Valid Entries</p> <p>Depends on the scan time. If the scan time is in hours, the phase must be in hours:minutes. If the scan time is in minutes, the phase must be in minutes:seconds. If the scan time is in seconds, the phase must be in seconds. If the scan time is in subseconds, the phase must be in subseconds.</p>

Limits and Scaling



Field	Description
Low Limit	<p>Lets you enter the tag's minimum value.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38.


Field	Description
	<ul style="list-style-type: none"> Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;">  Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. </div> <p>In a Calculation or Signal Select tag, if the output of the tag is 10 and the Low Limit is 15, the tag clamps the value at 15. You must enter a Low Limit of 10 or less to output a value of 10.</p> <p>If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the Low Limit field.</p> <p>If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
High Limit	<p>Lets you enter the tag's maximum value.</p> <p>Valid Entries</p> <p>You can enter a high limit in one of three formats:</p> <ul style="list-style-type: none"> Standard Integer. Expanded Decimal Notation, ranging from -9999999 to 9999999. Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38.

Field	Description
	<ul style="list-style-type: none"> Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div data-bbox="821 478 1419 743" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;">  Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. </div> <p>In a Calculation or a Signal Select tag, if the output of the tag is 150 and the High Limit is 100, the tag clamps the value at 100. You must enter a High Limit of 150 or more to output a value of 150.</p> <p>If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the High Limit field.</p> <p>If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
Units	<p>Lets you enter text describing the engineering units range.</p> <p>Valid Entries</p> <p>Up to 33 characters.</p> <p>Example</p> <p>Kilograms per square meter, Liters per minute, degrees Celsius,</p> <div data-bbox="821 1745 1419 1892" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;">  Note: This entry does not affect the calculation or function of any variables in iFIX. It is </div>

Field	Description
	<p> used strictly as a display label to identify the engineering units.</p>
<p>Scale Enabled</p>	<p>Lets you enable or disable scaling for this tag.</p> <p>Enabling scaling allows the system to convert the data received from input sensors to designated data ranges.</p> <p> Note: Linear scaling and signal conditioning cannot be applied simultaneously. If you select Linear Scaling, verify that Signal Conditioning is set to NONE.</p> <p>Example</p> <p>Scaling allows conversion of temperature data received in Fahrenheit to an output which uses Celsius values.</p>
<p>Scale Clamping</p>	<p>Lets you enable or disable clamping for this tag.</p> <p>When you enable clamping, any value the tag receives is limited to the raw range. Any value the tag sends is limited to the scaled range.</p> <p> Note: Do not enable clamping unless it is necessary. Because clamping limits the data received and sent, some data may be missed by the tag.</p>
<p>Raw Low</p>	<p>Lets you specify the low limit for the values received by the tag. Usually, this value corresponds to the specifications of the hardware from which the data is received.</p>


Field	Description
	<p>Valid Entries</p> <ul style="list-style-type: none"> • Standard Integer • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary).
Raw High	<p>Lets you specify the high limit for the values sent by the tag. Usually, this value corresponds to the specifications of the hardware from which the data is received.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • Standard Integer • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary).
Use Low/High Limits	<p>Enables the tag to use the range specified in the Engineering Units fields as the output values.</p> <p>Typically, EGU values normally reflect the expected operating ranges, or the Scale Low and Scale High values for the tag. However, the EGU values also dictate behavior in other areas such as alarming. By allowing the Scale Low and Scale High values to be set to values other than the EGU values, you can</p>



Field	Description
	<p>further manage conditions when alarms would be generated.</p> <div data-bbox="821 380 1419 869" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: If you are Using this tag for charts, make sure to select Use EGU. Selecting this option will make it easier for you to see the changes within the expected range in your chart, because the chart axes will correspond to your expected range and not the entire range of the sensors. The smaller range of the chart makes changes in values more obvious.</p> </div>
<p>Scale Low</p>	<p>Lets you specify the low limit for the values sent by the tag. Usually, this value corresponds to the specifications of the hardware from which the data is received. This field is only available if you did not enable Use EGU.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • Standard Integer • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div data-bbox="821 1665 1419 1835" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Changes made to this field are not reflected in the data until after the next tag scan.</p> </div>

Field	Description
Scale High	<p>Lets you specify the high limit for the values sent by the tag. Usually, this value corresponds to the specifications of the hardware from which the data is received. This field is only available if you did not enable Use EGU.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • Standard Integer • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note: Changes made to this field are not reflected in the data until after the next tag scan.</p> </div>

Alarm Settings

Field	Description
Alarm Areas	<p>Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>
Enable Alarm	Lets you enable or disable alarming for this tag.

Field	Description
	<p>When you enable alarming, the tag generates alarms allowing objects in your operator displays to show alarm conditions, and enabling other tags to detect alarms from the tag.</p> <div data-bbox="824 472 1416 781" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: The entire chain can be affected when you disable alarms for a tag. In addition, for both the Digital and Analog Alarm tags, this field is ignored when you enable the Alarm Suspend field.</p> </div>
Remote Ack Tag	<p>Lets you specify a tag and field name pair to use for alarm acknowledgment. When the value of the tag and field name pair changes from zero to a value greater than zero, the block acknowledges the alarm.</p> <p>Valid Entries</p> <p>Any floating point tag and field name (F_CV) pair in the tag.field format.</p> <p>You cannot use an A_CV field as a Remote Acknowledge entry. When the Analog Alarm tag is exception-based, acknowledging an alarm from the iFIX WorkSpace immediately triggers processing of the tag. Acknowledging the alarm with the Remote Acknowledge field does not trigger the Scan, Alarm and Control (SAC) program to process the Analog Alarm tag.</p>
Alarm Suspension Tag	<p>Provides intelligent alarming by defining a tag and field name pair to control alarm processing. When the value of the tag and field name pair is zero, the Analog Alarm block processes alarms. When the value is other than zero, either a positive or nega-</p>

Field	Description
	<p>tive number, the tag suspends alarms and generates a suspend alarm message.</p> <p>Valid Entries</p> <p>Any floating point tag and field name (F_CV) pair in the block.field format.</p> <div data-bbox="821 569 1419 835" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: If you specify the same tag and field name pair for multiple Analog Alarm blocks, you can suspend alarms within one or more alarm areas. This is an optional feature.</p> </div>
Target Value	<p>Lets you specify the optimum value for the tag. A deviation alarm occurs when the current value of the tag varies from the target value by an amount greater than the deviation alarm's value.</p> <p>Valid Entries</p> <p>Any floating point tag and field name (F_CV) pair in the tag.field format or a numeric value within the Low and High Limits (EGU). By default, the field is blank.</p> <div data-bbox="821 1339 1419 1518" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Target Value is an optional field and is used only with deviation alarms.</p> </div>
Shelve Enable	Select this check box to enable Alarm Shelving for the tag.
Shelve Policy	Select an alarm shelving policy from the drop-down list.

Alarm Options


Field	Description
High High	Lets you enter the threshold for the alarm type. If the block's value exceeds this threshold, the block generates an alarm.
HIHI alarm priority	Lets you enter INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL to define the priority of the alarm type.
HIHI cc-tag	Lets you enter the name of a digital tag that closes when an alarm occurs.
HIHI cc-mode	Lets you enter Acknowledge, Return, All Clear, or Never to define when to open the digital contact.
HIHI delay time	Lets you enter the amount of time the tag waits before generating an alarm. Enter a time in days, hours, minutes, and seconds, in the format dd:h-h:mm:ss, within the range of 00:00:00:00 to 03:00:00:00, when the block has time-based scan time. For exception based processing, leave the default entry, 00:00:00:00, which disable the field.
HIHI re-alarm time	Lets you enter the amount of time the tag waits before re-issuing an alarm. Enter a time in days, hours, minutes, and seconds, in the format dd:h-h:mm:ss, within the range of 00:00:00:00 to 03:00:00:00, when the block has time-based scan time. For exception based processing, leave the default entry, 00:00:00:00, which disable the field.
High	Lets you enter the threshold for the alarm type. If the block's value exceeds this threshold, the block generates an alarm.
HI alarm priority	Lets you enter INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL to define the priority of the alarm type.

Field	Description
HI cc-tag	Lets you enter the name of a digital tag that closes when an alarm occurs.
HI cc-mode	Lets you enter Acknowledge, Return, All Clear, or Never to define when to open the digital contact.
HI delay time	Lets you enter the amount of time the tag waits before generating an alarm. Enter a time in days, hours, minutes, and seconds, in the format dd:h-h:mm:ss, within the range of 00:00:00:00 to 03:00:00:00, when the block has time-based scan time. For exception based processing, leave the default entry, 00:00:00:00, which disable the field.
HI re-alarm time	Lets you enter the amount of time the tag waits before re-issuing an alarm. Enter a time in days, hours, minutes, and seconds, in the format dd:h-h:mm:ss, within the range of 00:00:00:00 to 03:00:00:00, when the block has time-based scan time. For exception based processing, leave the default entry, 00:00:00:00, which disable the field.
Low	Lets you enter the threshold for the alarm type. If the block's value exceeds this threshold, the block generates an alarm.
LO alarm priority	Lets you enter INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL to define the priority of the alarm type.
LO cc-tag	Lets you enter the name of a digital tag that closes when an alarm occurs.
LO cc-mode	Lets you enter Acknowledge, Return, All Clear, or Never to define when to open the digital contact.
LO delay time	Lets you enter the amount of time the tag waits before generating an alarm. Enter a time in days, hours, minutes, and seconds, in the format dd:h-h:mm:ss, within the range of 00:00:00:00 to 03:00:00:00, when the block has time-based scan

Field	Description
	time. For exception based processing, leave the default entry, 00:00:00:00, which disable the field.
LO re-alarm time	Lets you enter the amount of time the tag waits before re-issuing an alarm. Enter a time in days, hours, minutes, and seconds, in the format dd:h-h:mm:ss, within the range of 00:00:00:00 to 03:00:00:00, when the block has time-based scan time. For exception based processing, leave the default entry, 00:00:00:00, which disable the field.
Low Low	Lets you enter the threshold for the alarm type. If the block's value exceeds this threshold, the block generates an alarm.
LOLO alarm priority	Lets you enter INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL to define the priority of the alarm type.
LOLO cc-tag	Lets you enter the name of a digital tag that closes when an alarm occurs.
LOLO cc-mode	Lets you enter Acknowledge, Return, All Clear, or Never to define when to open the digital contact.
LOLO delay time	Lets you enter the amount of time the tag waits before generating an alarm. Enter a time in days, hours, minutes, and seconds, in the format dd:h-h:mm:ss, within the range of 00:00:00:00 to 03:00:00:00, when the block has time-based scan time. For exception based processing, leave the default entry, 00:00:00:00, which disable the field.
LOLO re-alarm time	Lets you enter the amount of time the tag waits before re-issuing an alarm. Enter a time in days, hours, minutes, and seconds, in the format dd:h-h:mm:ss, within the range of 00:00:00:00 to 03:00:00:00, when the block has time-based scan time. For exception based processing, leave the default entry, 00:00:00:00, which disable the field.

Field	Description
Rate of Change	Lets you enter the threshold for the alarm type. If the block's value exceeds this threshold, the block generates an alarm.
ROC alarm priority	Lets you enter INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL to define the priority of the alarm type.
ROC cc-tag	Lets you enter the name of a digital tag that closes when an alarm occurs.
ROC cc-mode	Lets you enter Acknowledge, Return, All Clear, or Never to define when to open the digital contact.
ROC delay time	Lets you enter the amount of time the tag waits before generating an alarm. Enter a time in days, hours, minutes, and seconds, in the format dd:h-h:mm:ss, within the range of 00:00:00:00 to 03:00:00:00, when the block has time-based scan time. For exception based processing, leave the default entry, 00:00:00:00, which disable the field.
ROC re-alarm time	Lets you enter the amount of time the tag waits before re-issuing an alarm. Enter a time in days, hours, minutes, and seconds, in the format dd:h-h:mm:ss, within the range of 00:00:00:00 to 03:00:00:00, when the block has time-based scan time. For exception based processing, leave the default entry, 00:00:00:00, which disable the field.
DEV alarm limit	Lets you enter the threshold for the alarm type. If the block's value exceeds this threshold, the block generates an alarm.
DEV alarm priority	Lets you enter INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL to define the priority of the alarm type.
DEV cc-tag	Lets you enter the name of a digital tag that closes when an alarm occurs.

Field	Description
DEV delay time	Lets you enter Acknowledge, Return, All Clear, or Never to define when to open the digital contact.
DEV re-alarm time	Lets you enter the amount of time the tag waits before generating an alarm. Enter a time in days, hours, minutes, and seconds, in the format dd:h-h:mm:ss, within the range of 00:00:00:00 to 03:00:00:00, when the block has time-based scan time. For exception based processing, leave the default entry, 00:00:00:00, which disable the field.
Other Alarm Priority	Lets you enter the threshold for the alarm type. If the block's value exceeds this threshold, the block generates an alarm.
Other cc-tag	Lets you enter INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL to define the priority of the alarm type.
Other cc-mode	Lets you enter the name of a digital tag that closes when an alarm occurs.
Other delay time	Lets you enter Acknowledge, Return, All Clear, or Never to define when to open the digital contact.
Other re-alarm time	Lets you enter the amount of time the tag waits before generating an alarm. Enter a time in days, hours, minutes, and seconds, in the format dd:h-h:mm:ss, within the range of 00:00:00:00 to 03:00:00:00, when the block has time-based scan time. For exception based processing, leave the default entry, 00:00:00:00, which disable the field.
Deadband	Lets you enter the maximum fluctuation the tag accepts without re-issuing an alarm. As long as the fluctuation is within the dead band range, the block issues an alarm once, eliminating nuisance alarms. Once the alarm falls below the dead band and then exceeds the alarm limits, the block generates another alarm.

Field	Description
	<p>Valid Entries</p> <p>Numeric value within the EGU range.</p> <p>Example</p> <p>If the High alarm limit is 80 and the dead band is 5, the tag does not re-issue an alarm after the one while the current value fluctuates between 75 and 85.</p>
<p>Const Contact Output</p>	<p>Selecting this option enables the tags to attempt to write the contact(s) with every scan, even if the value being written is unchanged. Otherwise, the AA tag only attempts to write to the defined contact tag when a value has changed and it needs to be written to the PLC. The write is a one-time attempt, so if it fails, the write will not be retried until the tag needs to write a new value.</p> <div data-bbox="821 1062 1419 1465" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note:</p> <p>There are four modes for the contacts - "Acknowledge", "Return", "All Clear", and "Never" - that control when the contact is cleared. Since the contact mode of "Never" does not reset the contact, the Continuous Output option is not supported for this contact mode.</p> </div>
<p>Suppress COMM Alarm</p>	<p>Select this option to separate the original alarm condition from the COMM alarm, and return the AA tag to the same state as it was prior to a COMM alarm. For example, if prior to the COMM alarm, the AA tag was an active alarm but already acknowledged, that is the state it should return to after communication is restored.</p>

Field	Description
	Otherwise, AA tags handle one alarm at a time. As a result, it is possible that acknowledgement of a COMM alarm could cause the ACK bit in the PLC to be written, and the original alarm condition, if already acknowledged, could re-alarm.
As Event in Suspend	Select this option to enable the Event messaging (Suspend mode), which applies suppression behavior to disable alarm processing. When the tag is in suspend mode, the Alarm state is set to OK, the Alarm is an alarm message only and therefore, does not appear in the alarm summary. Alarm processing continues with each alarm state transition recorded in the alarm loggers but does not display in the alarm summary. The alarm state contact (tag) is not processed.

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.
Collect	<p>Lets you select if the tag is set for collection by the Proficy Historian collector.</p> <p>Select Enabled to allow the tag to be collected by the collector.</p>
Collection Interval	<p>Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector.</p> <p>Valid Entries</p> <p>Must be entered in 100 ms intervals. The default value is 5000ms.</p> <p>Example</p>

Field	Description
	<p>1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.</p>
<p>Collection Offset</p>	<p>Used with the collection interval to schedule collection of data from a tag.</p> <p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p> <p>If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.</p>
<p>Time Resolution</p>	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
<p>Collector Compression</p>	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
<p>Collector Deadband</p>	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values</p>

Field	Description
	<p>that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>
Compression Time-out (ms)	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p> <p>Any numeric value.</p>

E-Signature



Field	Description
Type	The Type of Electronic Signature:


Field	Description
	<ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electron-</p>

Field	Description
	ic Signature settings are available. By default, this check box is disabled.

Advanced Options

Field	Description
Enable Output	Lets you configure the tag to send output to the I/O driver, OPC server, or OPC UA server. The tag sends its output when it is in Automatic mode and converts its data according to the entries in the Low Limit (EGU), High Limit (EGU), and Signal Conditioning fields.
Startup Mode	Lets you select the tag's mode on startup. In Automatic mode, the tag receives data from the I/O driver, OPC server, or OPC UA server. In Manual mode, the tag receives data from the operator, scripts, recipes, or Program blocks.
Initial Scan	<p>Lets you select whether the tag is initially placed on or off scan.</p> <p>Click On Scan to place the tag on scan as soon as the Scan, Alarm, and Control (SAC) program starts or when the database is loaded. Click Off Scan to place the tag on scan by a Program block, an Event Action tag, a script, an operator entry in a Data link, or an Easy Database Access program.</p>
Smoothing	<p>Enables the tag's first order digital filter to reduce noise from the incoming signal. The tag filters the incoming signal by adding part of the previous output and part of the new input from the I/O driver, OPC server, or OPC UA server as the following formula shows:</p> $\text{Output} = (S/16)X1 + ((16-S)/16)X2$ <p>where:</p>

Field	Description
	<ul style="list-style-type: none"> • s is the smoothing value entered in the Value field. • X1 is the initial value or previous output. • X2 is the new input from I/O driver or server.
<p>Security Areas</p>	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
<p>Previous Block</p>	<p>Displays the name of the previous (upstream) tag.</p> <p>Valid Entries</p> <p>None. This is a read-only field.</p>
<p>Next Block</p>	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: In a Statistical Data tag, the Next Block field specifies the tag name of the down-</p> </div>

Field	Description
	 stream Statistical Control tag. No other tag type is valid.
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>

AI Tag



This tag contains the following details:



General

Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p>

Field	Description
	<p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <p>~ ` + ^ : ? " * = { } . , ; ? @</p> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

I/O Addressing


Field	Description
I/O Driver	<p>Lets you select an I/O driver, OPC server, or OPC UA server for the tag. The selected driver or server enables the tag to communicate with process hardware on the plant floor.</p> <p>Before you can select an I/O driver, OPC server, or OPC UA server you must install it and add it to the available ones in the SCU.</p>
I/O Address	<p>Lets you enter the location in the process hardware where data for this tag is saved and where output is sent.</p> <p>Valid Entries</p> <p>Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations.</p> <div data-bbox="821 1094 1419 1409" style="border: 1px solid black; border-radius: 10px; padding: 10px; background-color: #fff9c4;"> <p> CAUTION:</p> <p>Do not assign the same I/O address to tags when using exception-based and time-based processing. Doing so will cause the exception-based tags to occasionally miss a value.</p> </div> <div data-bbox="821 1436 1419 1883" style="border: 1px solid black; border-radius: 10px; padding: 10px; background-color: #fff9c4;"> <p> CAUTION:</p> <p>Configuration Hub currently does not do I/O address validations before publish. If you enter an invalid IO address into a tag or generate an invalid I/O address via the model and substitutions, the publish may fail to set the IO address into the active database, and your invalid IO address will be removed.</p> </div>


Field	Description
Signal Conditioning	<p>Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p> <div data-bbox="821 432 1419 699" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Signal conditioning and linear scaling cannot be applied simultaneously. If you select a value for Signal Conditioning verify that Linear Scaling is not selected.</p> </div> <p>Valid Entries</p> <p>Depends on your driver or server. Refer to your driver or server manual for more information.</p>
H/W Options	<p>Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p> <div data-bbox="821 1066 1419 1333" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Signal conditioning and linear scaling cannot be applied simultaneously. If you select a value for Signal Conditioning verify that Linear Scaling is not selected.</p> </div> <p>Valid Entries</p> <p>Depends on your driver or server. Refer to your driver or server manual for more information.</p>
Process by Exception	<p>Enables exception-based processing for the tag.</p>
Scan Time	<p>Lets you specify how often the Scan, Alarm, and Control (SAC) program processes the tag and any tags (blocks) chained to it.</p> <p>Valid Entries</p>




Field	Description
	<ul style="list-style-type: none"> • 0 (one shot processing) • 0.05 to .95 in .05 increments (subsecond scan times) • 1 to 60 in 1 second increments • 1M to 60M in 1 minute increments • 1H to 24H in 1 hour increments <p>Example</p> <p>0.15 specifies a 15-subsecond scan time. 5 specifies a 5-second scan time, 10M specifies a 10-minute scan time, 16H specifies a 16-hour scan time.</p>
Phase At	<p>Lets you specify how long the Scan, Alarm, and Control (SAC) program delays in scanning the tag. When the tag has a second or subsecond scan time, SAC offsets the initial scan by the phase time when iFIX starts or when the database is reloaded. When the tag has a scan time of 1 minute or longer, SAC offsets the initial scan starting at midnight.</p> <p>Valid Entries</p> <p>Depends on the scan time. If the scan time is in hours, the phase must be in hours:minutes. If the scan time is in minutes, the phase must be in minutes:seconds. If the scan time is in seconds, the phase must be in seconds. If the scan time is in subseconds, the phase must be in subseconds.</p>

Limits and Scaling


Field	Description
Low Limit	<p>Lets you enter the tag's minimum value.</p> <p>Valid Entries</p>



Field	Description
	<ul style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;">  Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. </div> <p>In a Calculation or Signal Select tag, if the output of the tag is 10 and the Low Limit is 15, the tag clamps the value at 15. You must enter a Low Limit of 10 or less to output a value of 10.</p> <p>If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the Low Limit field.</p> <p>If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
High Limit	<p>Lets you enter the tag's maximum value.</p> <p>Valid Entries</p> <p>You can enter a high limit in one of three formats:</p> <ul style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999.

Field	Description
	<ul style="list-style-type: none"> • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;">  Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. </div> <p>In a Calculation or a Signal Select tag, if the output of the tag is 150 and the High Limit is 100, the tag clamps the value at 100. You must enter a High Limit of 150 or more to output a value of 150.</p> <p>If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the High Limit field.</p> <p>If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
Units	<p>Lets you enter text describing the engineering units range.</p> <p>Valid Entries</p> <p>Up to 33 characters.</p> <p>Example</p> <p>Kilograms per square meter, Liters per minute, degrees Celsius,</p>

Field	Description
	<div data-bbox="820 262 1421 535" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;">  Note: This entry does not affect the calculation or function of any variables in iFIX. It is used strictly as a display label to identify the engineering units. </div>
<p>Scale Enabled</p>	<p>Lets you enable or disable scaling for this tag.</p> <p>Enabling scaling allows the system to convert the data received from input sensors to designated data ranges.</p> <div data-bbox="820 787 1421 1050" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;">  Note: Linear scaling and signal conditioning cannot be applied simultaneously. If you select Linear Scaling, verify that Signal Conditioning is set to NONE. </div> <p>Example</p> <p>Scaling allows conversion of temperature data received in Fahrenheit to an output which uses Celsius values.</p>
<p>Scale Clamping</p>	<p>Lets you enable or disable clamping for this tag.</p> <p>When you enable clamping, any value the tag receives is limited to the raw range. Any value the tag sends is limited to the scaled range.</p> <div data-bbox="820 1543 1421 1806" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;">  Note: Do not enable clamping unless it is necessary. Because clamping limits the data received and sent, some data may be missed by the tag. </div>



Field	Description
Raw Low	<p>Lets you specify the low limit for the values received by the tag. Usually, this value corresponds to the specifications of the hardware from which the data is received.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • Standard Integer • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary).
Raw High	<p>Lets you specify the high limit for the values sent by the tag. Usually, this value corresponds to the specifications of the hardware from which the data is received.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • Standard Integer • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary).
Use Low/High Limits	<p>Enables the tag to use the range specified in the Engineering Units fields as the output values.</p> <p>Typically, EGU values normally reflect the expected operating ranges, or the Scale Low and Scale High</p>

Field	Description
	<p>values for the tag. However, the EGU values also dictate behavior in other areas such as alarming. By allowing the Scale Low and Scale High values to be set to values other than the EGU values, you can further manage conditions when alarms would be generated.</p> <div data-bbox="820 556 1421 1050" style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p> Note: If you are Using this tag for charts, make sure to select Use EGU. Selecting this option will make it easier for you to see the changes within the expected range in your chart, because the chart axes will correspond to your expected range and not the entire range of the sensors. The smaller range of the chart makes changes in values more obvious.</p> </div>
Scale Low	<p>Lets you specify the low limit for the values sent by the tag. Usually, this value corresponds to the specifications of the hardware from which the data is received. This field is only available if you did not enable Use EGU.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • Standard Integer • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary).

Field	Description
	<div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: Changes made to this field are not reflected in the data until after the next tag scan. </div>
Scale High	<p>Lets you specify the high limit for the values sent by the tag. Usually, this value corresponds to the specifications of the hardware from which the data is received. This field is only available if you did not enable Use EGU.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • Standard Integer • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF; margin-top: 10px;">  Note: Changes made to this field are not reflected in the data until after the next tag scan. </div>

Alarm Options

Field	Description
Alarm Areas	<p>Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p>

Field	Description
<p>Enable Alarm</p>	<p>ALL or up to 15 alarm area names.</p> <p>Lets you enable or disable alarming for this tag.</p> <p>When you enable alarming, the tag generates alarms allowing objects in your operator displays to show alarm conditions, and enabling other tags to detect alarms from the tag.</p> <div data-bbox="821 604 1419 917" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: The entire chain can be affected when you disable alarms for a tag. In addition, for both the Digital and Analog Alarm tags, this field is ignored when you enable the Alarm Suspend field.</p> </div>
<p>Priority</p>	<p>Lets you specify the alarm priority for a tag. If the priority is equal or greater than the SCADA node's alarm priority, iFIX sends the alarm to all the alarm destinations enabled for this node. However, if the priority is less than the SCADA node's alarm priority, the alarm is automatically acknowledged and filtered out so that it does not appear in your alarm destinations. However, the alarm does appear in Data links configured to display current and latched alarms.</p> <p>Valid Entries</p> <p>INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL</p> <div data-bbox="821 1602 1419 1873" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: To report tag alarms, the appropriate alarm areas must be assigned to each of the alarm services enabled in the System Configuration Utility (SCU).</p> </div>

Field	Description
Shelve Enable	Select this check box to enable Alarm Shelving for the tag.
Shelve Policy	Select an alarm shelving policy from the drop-down list.

Alarm Limits

Field	Description
Low Low	<p>Lets you enter the tag's critically low values. When the tag's value falls below this limit, the tag generates an alarm.</p> <p>Valid Entries</p> <p>A critically low value within the tag's engineering units range.</p> <p>Example</p> <p>If a temperature of 25 degrees indicates that a cooling water flow is frozen, you could enter a value of 30 degrees for your Low Low alarm.</p>
Low	<p>Lets you enter the tag's low process values. When the tag's value falls below this limit, the tag generates an alarm.</p> <p>Valid Entries</p> <p>A low value within the tag's engineering units range. If you want to provide a warning that a value is approaching a critical low limit, enter a slightly higher value than the Low Low alarm.</p> <p>Example</p> <p>If a temperature of 35 degrees indicates that ice crystals are forming in a cooling water flow, you</p>

Field	Description
	could enter a value of 40 degrees for your Low alarm.
High	<p>Lets you enter the tag's high process values. When the tag's value exceeds this limit, the tag generates an alarm.</p> <p>Valid Entries</p> <p>A high value within the tag's engineering units range. If you want to provide a warning that a value is approaching a critically high limit, enter a slightly lower value than the High High alarm.</p> <p>Example</p> <p>If a bearing temperature of 80 degrees indicates machine wear, you could enter a value of 75 degrees for your High alarm.</p>
High High	<p>Lets you enter the tag's critically high values. When the tag's value exceeds this limit, the tag generates an alarm.</p> <p>Valid Entries</p> <p>A critically high value within the tag's engineering units range.</p> <p>Example</p> <p>If a bearing temperature of 90 degrees indicates imminent seizure, you could enter a value of 85 degrees for your High High alarm.</p>
Rate of Change	<p>Lets you enter the maximum, acceptable change in a tag's value. If the tag's current value changes by more than the specified value within one scan period, the tag generates a Rate of Change alarm.</p> <p>Valid Entries</p>

Field	Description
	<p>A value within the tag's engineering units range, to be checked per scan period. Enter 0 to disable this alarm.</p> <p>Example</p> <p>To generate an alarm due to a fluctuation of more than 20 RPMs on a speed drive since the last scan period, you would enter a 20 in this field.</p>
Deadband	<p>Lets you enter the maximum fluctuation the tag accepts without re-issuing an alarm. As long as the fluctuation is within the dead band range, the tag issues an alarm once, eliminating nuisance alarms. Once the alarm falls below the dead band and then exceeds the alarm limits, the tag generates another alarm.</p> <p>Valid Entries</p> <p>Numeric value within the EGU range.</p> <p>Example</p> <p>If the High alarm limit is 80 and the dead band is 5, the tag does not re-issue an alarm after the one while the current value fluctuates between 75 and 85.</p>

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.
Collect	<p>Lets you select if the tag is set for collection by the Proficy Historian collector.</p> <p>Select Enabled to allow the tag to be collected by the collector.</p>

Field	Description
Collection Interval	<p>Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector.</p> <p>Valid Entries</p> <p>Must be entered in 100 ms intervals. The default value is 5000ms.</p> <p>Example</p> <p>1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.</p>
Collection Offset	<p>Used with the collection interval to schedule collection of data from a tag.</p> <p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p> <p>If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.</p>
Time Resolution	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incom-</p>

Field	Description
	<p>ing data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Collector Deadband	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>
Compression Time-out (ms)	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p>

Field	Description
	Any numeric value.


E-Signature


Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>

Field	Description
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>

Advanced Options

Field	Description
Enable Output	<p>Lets you configure the tag to send output to the I/O driver, OPC server, or OPC UA server. The tag sends its output when it is in Automatic mode and converts its data according to the entries in the Low Limit (EGU), High Limit (EGU), and Signal Conditioning fields.</p>
Startup Mode	<p>Lets you select the tag's mode on startup. In Automatic mode, the tag receives data from the I/O driver, OPC server, or OPC UA server. In Manual mode, the tag receives data from the operator, scripts, recipes, or Program blocks.</p>
Initial Scan	<p>Lets you select whether the tag is initially placed on or off scan.</p> <p>Click On Scan to place the tag on scan as soon as the Scan, Alarm, and Control (SAC) program starts or when the database is loaded. Click Off Scan to place the tag on scan by a Program block, an Event Action tag, a script, an operator entry in a Data link, or an Easy Database Access program.</p>

Field	Description
Smoothing	<p>Enables the tag's first order digital filter to reduce noise from the incoming signal. The tag filters the incoming signal by adding part of the previous output and part of the new input from the I/O driver, OPC server, or OPC UA server as the following formula shows:</p> $\text{Output} = (S/16)X1 + ((16-S)/16)X2$ <p>where:</p> <ul style="list-style-type: none"> • s is the smoothing value entered in the Value field. • X1 is the initial value or previous output. • X2 is the new input from I/O driver or server.
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
Previous Block	<p>Displays the name of the previous (upstream) tag.</p> <p>Valid Entries</p>

Field	Description
	None. This is a read-only field.
Next Block	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div data-bbox="820 485 1419 753" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: In a Statistical Data tag, the Next Block field specifies the tag name of the downstream Statistical Control tag. No other tag type is valid.</p> </div>
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>

AIS Tag


This tag contains the following details:





General


Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <pre>~ ` + ^ : ? " * = { } . , ; ? @</pre> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p>

Field	Description
	A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

I/O Addressing

Field	Description
I/O Driver	<p>Lets you select an I/O driver, OPC server, or OPC UA server for the tag. The selected driver or server enables the tag to communicate with process hardware on the plant floor.</p> <p>Before you can select an I/O driver, OPC server, or OPC UA server you must install it and add it to the available ones in the SCU.</p>
I/O Address	<p>Lets you enter the location in the process hardware where data for this tag is saved and where output is sent.</p> <p>Valid Entries</p> <p>Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations.</p> <div data-bbox="820 1596 1412 1785" style="border: 1px solid black; padding: 5px; margin-top: 10px;">  CAUTION: Do not assign the same I/O address to tags when using exception-based and time-based processing. Doing so will </div>


Field	Description
	<p data-bbox="834 275 1386 348"> cause the exception-based tags to occasionally miss a value.</p> <p data-bbox="834 415 1386 821"> CAUTION: Configuration Hub currently does not do I/O address validations before publish. If you enter an invalid IO address into a tag or generate an invalid I/O address via the model and substitutions, the publish may fail to set the IO address into the active database, and your invalid IO address will be removed.</p>
Signal Conditioning	<p data-bbox="818 877 1403 993">Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p> <p data-bbox="834 1045 1403 1272"> Note: Signal conditioning and linear scaling cannot be applied simultaneously. If you select a value for Signal Conditioning verify that Linear Scaling is not selected.</p> <p data-bbox="818 1335 964 1360">Valid Entries</p> <p data-bbox="818 1409 1403 1476">Depends on your driver or server. Refer to your driver or server manual for more information.</p>
H/W Options	<p data-bbox="818 1514 1403 1629">Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p> <p data-bbox="834 1682 1403 1816"> Note: Signal conditioning and linear scaling cannot be applied simultaneously. If you se-</p>

Field	Description
	<div data-bbox="824 268 1417 373" style="border: 1px solid #0070C0; border-radius: 5px; padding: 5px; background-color: #E6F2FF;">  Select a value for Signal Conditioning verify that Linear Scaling is not selected. </div> <p>Valid Entries</p> <p>Depends on your driver or server. Refer to your driver or server manual for more information.</p>
Process by Exception	Enables exception-based processing for the tag.
Scan Time	<p>Lets you specify how often the Scan, Alarm, and Control (SAC) program processes the tag and any tags (blocks) chained to it.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • 0 (one shot processing) • 0.05 to .95 in .05 increments (subsecond scan times) • 1 to 60 in 1 second increments • 1M to 60M in 1 minute increments • 1H to 24H in 1 hour increments <p>Example</p> <p>0.15 specifies a 15-subsecond scan time. 5 specifies a 5-second scan time, 10M specifies a 10-minute scan time, 16H specifies a 16-hour scan time.</p>
Phase At	<p>Lets you specify how long the Scan, Alarm, and Control (SAC) program delays in scanning the tag. When the tag has a second or subsecond scan time, SAC offsets the initial scan by the phase time when iFIX starts or when the database is reloaded. When the tag has a scan time of 1 minute or longer, SAC offsets the initial scan starting at midnight.</p> <p>Valid Entries</p>

Field	Description
	Depends on the scan time. If the scan time is in hours, the phase must be in hours:minutes. If the scan time is in minutes, the phase must be in minutes:seconds. If the scan time is in seconds, the phase must be in seconds. If the scan time is in subseconds, the phase must be in subseconds.


Limits and Scaling


Field	Description
Low Limit	Low EGU limit. The low end of the user readable value.
High Limit	High EGU limit. The high end of the user readable value.
Units	Description of the EGU range (e.g. DEGF, GPH, PSI, etc)
Low Count	The low 'counts' range for the raw input which corresponds to the low EGU range of the user readable value. Note that if LOW and HIGH counts are equal then the input scaling is disabled and the block will function like an ordinary AI block.
High Count_CH	The high 'counts' range for the raw input which corresponds to the high EGU range of the user readable value. Note that if LOW and HIGH counts are equal then the input scaling is disabled and the block will function like an ordinary AI block.
Clamp to Range	If set (and the low/high count is in use) then the input is clamped to the range of the low/hi count. For example if the low count is 819 and the raw input from the driver is 123 then the input will be changed to 819 - the lowest allowable input. If this function is disabled then the raw input will not be clamped.

Field	Description
Alarm on Range	If set (and the low/high count is in use) then if the input is outside the lo/hi count range then an UnderRange or OverRange alarm is generated for the block.
Low Operator Limit	Low operator output limit. Output clamping is enabled if the LOLIM and HILIM values are different. Values sent to the A_CV or F_CV fields of the block will be checked against these limits. Normally, the values will be rejected if they are outside these limits.
High Operator Limit	High operator output limit. Output clamping is enabled if the LOLIM and HILIM values are different. Values sent to the A_CV or F_CV fields of the block will be checked against these limits. Normally the values will be rejected if they are outside these limits.
Clamp Output	<p>If set then an output entered by the operator or some other application is clamped to the operator output limits and then sent to the driver. If clear then any output outside the operator limits is rejected with an error.</p> <div data-bbox="824 1297 1416 1516" style="border: 1px solid black; padding: 5px; background-color: #fff9c4;"> <p> CAUTION: This option should generally be CLEAR (the default state) to prevent unwanted values from being sent to equipment.</p> </div>

Alarm Options

Field	Description
Alarm Areas	Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with

Field	Description
	<p>the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>
<p>Enable Alarm</p>	<p>Lets you enable or disable alarming for this tag.</p> <p>When you enable alarming, the tag generates alarms allowing objects in your operator displays to show alarm conditions, and enabling other tags to detect alarms from the tag.</p> <div data-bbox="821 793 1419 1104" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: The entire chain can be affected when you disable alarms for a tag. In addition, for both the Digital and Analog Alarm tags, this field is ignored when you enable the Alarm Suspend field.</p> </div>
<p>Priority</p>	<p>Lets you specify the alarm priority for a tag. If the priority is equal or greater than the SCADA node's alarm priority, iFIX sends the alarm to all the alarm destinations enabled for this node. However, if the priority is less than the SCADA node's alarm priority, the alarm is automatically acknowledged and filtered out so that it does not appear in your alarm destinations. However, the alarm does appear in Data links configured to display current and latched alarms.</p> <p>Valid Entries</p> <p>INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL</p>

Field	Description
	<div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: To report tag alarms, the appropriate alarm areas must be assigned to each of the alarm services enabled in the System Configuration Utility (SCU). </div>
Shelve Enable	Select this check box to enable Alarm Shelving for the tag.
Shelve Policy	Select an alarm shelving policy from the drop-down list.

Alarm Limits

Field	Description
Low Low	<p>Lets you enter the tag's critically low values. When the tag's value falls below this limit, the tag generates an alarm.</p> <p>Valid Entries</p> <p>A critically low value within the tag's engineering units range.</p> <p>Example</p> <p>If a temperature of 25 degrees indicates that a cooling water flow is frozen, you could enter a value of 30 degrees for your Low Low alarm.</p>
Low	<p>Lets you enter the tag's low process values. When the tag's value falls below this limit, the tag generates an alarm.</p> <p>Valid Entries</p> <p>A low value within the tag's engineering units range. If you want to provide a warning that a value is approaching a critical low limit, enter a slightly higher value than the Low Low alarm.</p> <p>Example</p> <p>If a temperature of 35 degrees indicates that ice crystals are forming in a cooling water flow, you could enter a value of 40 degrees for your Low alarm.</p>

Field	Description
High	<p>Lets you enter the tag's high process values. When the tag's value exceeds this limit, the tag generates an alarm.</p> <p>Valid Entries</p> <p>A high value within the tag's engineering units range. If you want to provide a warning that a value is approaching a critically high limit, enter a slightly lower value than the High High alarm.</p> <p>Example</p> <p>If a bearing temperature of 80 degrees indicates machine wear, you could enter a value of 75 degrees for your High alarm.</p>
High High	<p>Lets you enter the tag's critically high values. When the tag's value exceeds this limit, the tag generates an alarm.</p> <p>Valid Entries</p> <p>A critically high value within the tag's engineering units range.</p> <p>Example</p> <p>If a bearing temperature of 90 degrees indicates imminent seizure, you could enter a value of 85 degrees for your High High alarm.</p>
Rate of Change	<p>Lets you enter the maximum, acceptable change in a tag's value. If the tag's current value changes by more than the specified value within one scan period, the tag generates a Rate of Change alarm.</p> <p>Valid Entries</p> <p>A value within the tag's engineering units range, to be checked per scan period. Enter 0 to disable this alarm.</p> <p>Example</p> <p>To generate an alarm due to a fluctuation of more than 20 RPMs on a speed drive since the last scan period, you would enter a 20 in this field.</p>
Dead-band	<p>Lets you enter the maximum fluctuation the tag accepts without re-issuing an alarm. As long as the fluctuation is within the dead band range, the tag issues an alarm once, eliminating noi-</p>

Field	Description
	<p>sance alarms. Once the alarm falls below the dead band and then exceeds the alarm limits, the tag generates another alarm.</p> <p>Valid Entries</p> <p>Numeric value within the EGU range.</p> <p>Example</p> <p>If the High alarm limit is 80 and the dead band is 5, the tag does not re-issue an alarm after the one while the current value fluctuates between 75 and 85.</p>



E-Signature


Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that</p>

Field	Description
	<p>the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>

Advanced Options

Field	Description
Enable Output	<p>Lets you configure the tag to send output to the I/O driver, OPC server, or OPC UA server. The tag sends its output when it is in Automatic mode and converts its data according to the entries in the Low Limit (EGU), High Limit (EGU), and Signal Conditioning fields.</p>
Startup Mode	<p>Lets you select the tag's mode on startup. In Automatic mode, the tag receives data from the I/O driver, OPC server, or OPC UA server. In Manual mode, the tag receives data from the operator, scripts, recipes, or Program blocks.</p>
Initial Scan	<p>Lets you select whether the tag is initially placed on or off scan.</p>

Field	Description
	<p>Click On Scan to place the tag on scan as soon as the Scan, Alarm, and Control (SAC) program starts or when the database is loaded. Click Off Scan to place the tag on scan by a Program block, an Event Action tag, a script, an operator entry in a Data link, or an Easy Database Access program.</p>
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="820 1039 1421 1344" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
Previous Block	<p>Displays the name of the previous (upstream) tag.</p> <p>Valid Entries</p> <p>None. This is a read-only field.</p>
Next Block	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div data-bbox="820 1732 1421 1879" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: In a Statistical Data tag, the Next Block field specifies the tag name of the down-</p> </div>

Field	Description
	 stream Statistical Control tag. No other tag type is valid.
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>

AO Tag



This tag contains the following details:



General

Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p>

Field	Description
	<p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <p>~ ` + ^ : ? " * = { } . , ; ? @</p> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.


I/O Addressing


Field	Description
I/O Driver	<p>Lets you select an I/O driver, OPC server, or OPC UA server for the tag. The selected driver or server enables the tag to communicate with process hardware on the plant floor.</p> <p>Before you can select an I/O driver, OPC server, or OPC UA server you must install it and add it to the available ones in the SCU.</p>
I/O Address	<p>Lets you enter the location in the process hardware where data for this tag is saved and where output is sent.</p> <p>Valid Entries</p> <p>Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations.</p> <div data-bbox="821 1094 1419 1409" style="border: 1px solid black; border-radius: 10px; padding: 10px; background-color: #fff9c4;"> <p> CAUTION: Do not assign the same I/O address to tags when using exception-based and time-based processing. Doing so will cause the exception-based tags to occasionally miss a value.</p> </div> <div data-bbox="821 1436 1419 1881" style="border: 1px solid black; border-radius: 10px; padding: 10px; background-color: #fff9c4;"> <p> CAUTION: Configuration Hub currently does not do I/O address validations before publish. If you enter an invalid IO address into a tag or generate an invalid I/O address via the model and substitutions, the publish may fail to set the IO address into the active database, and your invalid IO address will be removed.</p> </div>




Field	Description
Signal Conditioning	<p>Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p> <div data-bbox="824 436 1419 699" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Signal conditioning and linear scaling cannot be applied simultaneously. If you select a value for Signal Conditioning verify that Linear Scaling is not selected.</p> </div> <p>Valid Entries</p> <p>Depends on your driver or server. Refer to your driver or server manual for more information.</p>
H/W Options	<p>Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p> <div data-bbox="824 1073 1419 1335" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Signal conditioning and linear scaling cannot be applied simultaneously. If you select a value for Signal Conditioning verify that Linear Scaling is not selected.</p> </div> <p>Valid Entries</p> <p>Depends on your driver or server. Refer to your driver or server manual for more information.</p>

Limits and Scaling


Field	Description
Low Limit	<p>Lets you enter the tag's minimum value.</p> <p>Valid Entries</p>



Field	Description
	<ul style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;">  Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. </div> <p>In a Calculation or Signal Select tag, if the output of the tag is 10 and the Low Limit is 15, the tag clamps the value at 15. You must enter a Low Limit of 10 or less to output a value of 10.</p> <p>If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the Low Limit field.</p> <p>If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
High Limit	<p>Lets you enter the tag's maximum value.</p> <p>Valid Entries</p> <p>You can enter a high limit in one of three formats:</p> <ul style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999.

Field	Description
	<ul style="list-style-type: none"> • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;">  Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. </div> <p>In a Calculation or a Signal Select tag, if the output of the tag is 150 and the High Limit is 100, the tag clamps the value at 100. You must enter a High Limit of 150 or more to output a value of 150.</p> <p>If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the High Limit field.</p> <p>If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
Units	<p>Lets you enter text describing the engineering units range.</p> <p>Valid Entries</p> <p>Up to 33 characters.</p> <p>Example</p> <p>Kilograms per square meter, Liters per minute, degrees Celsius,</p>

Field	Description
	<div data-bbox="820 268 1421 529" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;">  Note: This entry does not affect the calculation or function of any variables in iFIX. It is used strictly as a display label to identify the engineering units. </div>
<p>Scale Enabled</p>	<p>Lets you enable or disable scaling for this tag.</p> <p>Enabling scaling allows the system to convert the data received from input sensors to designated data ranges.</p> <div data-bbox="820 781 1421 1045" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;">  Note: Linear scaling and signal conditioning cannot be applied simultaneously. If you select Linear Scaling, verify that Signal Conditioning is set to NONE. </div> <p>Example</p> <p>Scaling allows conversion of temperature data received in Fahrenheit to an output which uses Celsius values.</p>
<p>Scale Clamping</p>	<p>Lets you enable or disable clamping for this tag.</p> <p>When you enable clamping, any value the tag receives is limited to the raw range. Any value the tag sends is limited to the scaled range.</p> <div data-bbox="820 1537 1421 1801" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;">  Note: Do not enable clamping unless it is necessary. Because clamping limits the data received and sent, some data may be missed by the tag. </div>


Field	Description
Raw Low	<p>Lets you specify the low limit for the values received by the tag. Usually, this value corresponds to the specifications of the hardware from which the data is received.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • Standard Integer • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary).
Raw High	<p>Lets you specify the high limit for the values sent by the tag. Usually, this value corresponds to the specifications of the hardware from which the data is received.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • Standard Integer • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary).
Use Low/High Limits	<p>Enables the tag to use the range specified in the Engineering Units fields as the output values.</p> <p>Typically, EGU values normally reflect the expected operating ranges, or the Scale Low and Scale High</p>

Field	Description
	<p>values for the tag. However, the EGU values also dictate behavior in other areas such as alarming. By allowing the Scale Low and Scale High values to be set to values other than the EGU values, you can further manage conditions when alarms would be generated.</p> <div data-bbox="820 556 1421 1050" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: If you are Using this tag for charts, make sure to select Use EGU. Selecting this option will make it easier for you to see the changes within the expected range in your chart, because the chart axes will correspond to your expected range and not the entire range of the sensors. The smaller range of the chart makes changes in values more obvious.</p> </div>
Scale Low	<p>Lets you specify the low limit for the values sent by the tag. Usually, this value corresponds to the specifications of the hardware from which the data is received. This field is only available if you did not enable Use EGU.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • Standard Integer • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary).

Field	Description
	<div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: Changes made to this field are not reflected in the data until after the next tag scan. </div>
Scale High	<p>Lets you specify the high limit for the values sent by the tag. Usually, this value corresponds to the specifications of the hardware from which the data is received. This field is only available if you did not enable Use EGU.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • Standard Integer • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF; margin-top: 10px;">  Note: Changes made to this field are not reflected in the data until after the next tag scan. </div>

Alarm Options

Field	Description
Alarm Areas	<p>Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p>

Field	Description
	ALL or up to 15 alarm area names.
Enable Event	<p>Lets you enable or disable event messaging for the tag. Event messaging is similar to alarming except that it does not require acknowledgment. Event messages are sent to the same alarm destinations as alarms for a given tag but do not appear in the Alarm Summary object.</p> <p>Analog Output, Analog Register, Digital Output, Digital Register, Digital Input, and Text tags have event messaging capabilities.</p> <div data-bbox="824 785 1414 1182" style="border: 1px solid #00a0c0; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p> Note: Be careful when using event messaging in a chain with a time-based scan time. If the scan time is short, your alarm files (either disk or printed) can grow very large. We recommend enabling event messaging for exception-based chains, one shot chains, and stand-alone output blocks.</p> </div>

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.
Collect	<p>Lets you select if the tag is set for collection by the Proficy Historian collector.</p> <p>Select Enabled to allow the tag to be collected by the collector.</p>
Collection Interval	Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector.

Field	Description
	<p>Valid Entries</p> <p>Must be entered in 100 ms intervals. The default value is 5000ms.</p> <p>Example</p> <p>1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.</p>
Collection Offset	<p>Used with the collection interval to schedule collection of data from a tag.</p> <p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p> <p>If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.</p>
Time Resolution	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p>

Field	Description
	Select Disabled to prevent the tag from being compressed.
Collector Deadband	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>
Compression Time-out (ms)	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p> <p>Any numeric value.</p>


E-Signature


Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during</p>

Field	Description
	<p>run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>

Advanced Options

Field	Description
Output Reverse	<p>Lets you specify the maximum rate of change you want to allow between successive outputs.</p> <p>Valid Entries</p> <p>A value between the Low and High Limit (EGU) fields or a 0 to allow any amount of change.</p>
Initial Value	<p>Lets you specify the value that the Scan, Alarm, and Control (SAC) program sends to the process hardware. SAC sends the data the first time that it reads the block. If an Initial Value is not defined, SAC does not output a value during initialization.</p> <p>Valid Entries</p> <p>A value between the Low and High Limit (EGU) fields.</p>
Low Operator Limit	<p>Lets you specify the lowest value that the tag accepts from another tag or from an operator.</p> <p>Valid Entries</p> <p>A value between the Low and High Limit (EGU) fields. If appropriate, you can use the Low Limit (EGU) for this value.</p>
High Operator Limit	<p>Lets you specify the highest value that the tag can accept from another tag or from an operator.</p>

Field	Description
	<p>Valid Entries</p> <p>A value between the Low and High Limit (EGU) fields. If appropriate, you can use the High Limit (EGU) for this value.</p>
Rate Limit	<p>Lets you specify the maximum rate of change you want to allow between successive outputs.</p> <p>Valid Entries</p> <p>A value between the Low and High Limit (EGU) fields or a 0 to allow any amount of change.</p>
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="821 1268 1419 1579" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
Previous Block	<p>Displays the name of the previous (upstream) tag.</p> <p>Valid Entries</p> <p>None. This is a read-only field.</p>

Field	Description
Next Block	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: In a Statistical Data tag, the Next Block field specifies the tag name of the downstream Statistical Control tag. No other tag type is valid.</p> </div>
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>

AR Tag


This tag contains the following details:





General


Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <pre>~ ` + ^ : ? " * = { } . , ; ? @</pre> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p>

Field	Description
	A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

I/O Addressing


Field	Description
I/O Driver	<p>Lets you select an I/O driver, OPC server, or OPC UA server for the tag. The selected driver or server enables the tag to communicate with process hardware on the plant floor.</p> <p>Before you can select an I/O driver, OPC server, or OPC UA server you must install it and add it to the available ones in the SCU.</p>
I/O Address	<p>Lets you enter the location in the process hardware where data for this tag is saved and where output is sent.</p> <p>Valid Entries</p> <p>Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations.</p> <div data-bbox="820 1596 1412 1785" style="border: 1px solid black; padding: 5px; margin-top: 10px;">  CAUTION: Do not assign the same I/O address to tags when using exception-based and time-based processing. Doing so will </div>



Field	Description
	<div data-bbox="824 268 1416 373" style="border: 1px solid black; border-radius: 5px; padding: 5px; background-color: #fff9c4;">  cause the exception-based tags to occasionally miss a value. </div> <div data-bbox="824 401 1416 848" style="border: 1px solid black; border-radius: 5px; padding: 5px; background-color: #fff9c4; margin-top: 10px;">  CAUTION: Configuration Hub currently does not do I/O address validations before publish. If you enter an invalid IO address into a tag or generate an invalid I/O address via the model and substitutions, the publish may fail to set the IO address into the active database, and your invalid IO address will be removed. </div>
Signal Conditioning	<p>Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p> <div data-bbox="824 1031 1416 1297" style="border: 1px solid black; border-radius: 5px; padding: 5px; background-color: #e1f5fe; margin-top: 10px;">  Note: Signal conditioning and linear scaling cannot be applied simultaneously. If you select a value for Signal Conditioning verify that Linear Scaling is not selected. </div> <p>Valid Entries</p> <p>Depends on your driver or server. Refer to your driver or server manual for more information.</p>
H/W Options	<p>Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p> <div data-bbox="824 1667 1416 1818" style="border: 1px solid black; border-radius: 5px; padding: 5px; background-color: #e1f5fe; margin-top: 10px;">  Note: Signal conditioning and linear scaling cannot be applied simultaneously. If you se- </div>


Field	Description
	<div data-bbox="820 268 1416 373" style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px;">  Select a value for Signal Conditioning verify that Linear Scaling is not selected. </div> <p data-bbox="820 409 971 441">Valid Entries</p> <p data-bbox="820 478 1409 556">Depends on your driver or server. Refer to your driver or server manual for more information.</p>


Limits and Scaling


Field	Description
Low Limit	<p data-bbox="820 751 1286 783">Lets you enter the tag's minimum value.</p> <p data-bbox="820 825 971 856">Valid Entries</p> <ul data-bbox="880 905 1409 1297" style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div data-bbox="820 1339 1416 1606" style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px;"> <p data-bbox="836 1354 885 1396"></p> <p data-bbox="901 1369 1377 1579">Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information.</p> </div> <p data-bbox="820 1642 1422 1799">In a Calculation or Signal Select tag, if the output of the tag is 10 and the Low Limit is 15, the tag clamps the value at 15. You must enter a Low Limit of 10 or less to output a value of 10.</p>


Field	Description
	<p>If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the Low Limit field.</p> <p>If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
<p>High Limit</p>	<p>Lets you enter the tag's maximum value.</p> <p>Valid Entries</p> <p>You can enter a high limit in one of three formats:</p> <ul style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information.</p> </div> <p>In a Calculation or a Signal Select tag, if the output of the tag is 150 and the High Limit is 100, the tag clamps the value at 100. You must enter a High Limit of 150 or more to output a value of 150.</p> <p>If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the High Limit field.</p>

Field	Description
	<p>If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
<p>Units</p>	<p>Lets you enter text describing the engineering units range.</p> <p>Valid Entries</p> <p>Up to 33 characters.</p> <p>Example</p> <p>Kilograms per square meter, Liters per minute, degrees Celsius,</p> <div data-bbox="820 863 1419 1129" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: This entry does not affect the calculation or function of any variables in iFIX. It is used strictly as a display label to identify the engineering units.</p> </div>
<p>Scale Enabled</p>	<p>Lets you enable or disable scaling for this tag.</p> <p>Enabling scaling allows the system to convert the data received from input sensors to designated data ranges.</p> <div data-bbox="820 1381 1419 1648" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Linear scaling and signal conditioning cannot be applied simultaneously. If you select Linear Scaling, verify that Signal Conditioning is set to NONE.</p> </div> <p>Example</p> <p>Scaling allows conversion of temperature data received in Fahrenheit to an output which uses Celsius values.</p>

Field	Description
Scale Clamping	<p>Lets you enable or disable clamping for this tag.</p> <p>When you enable clamping, any value the tag receives is limited to the raw range. Any value the tag sends is limited to the scaled range.</p> <div data-bbox="824 506 1419 772" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Do not enable clamping unless it is necessary. Because clamping limits the data received and sent, some data may be missed by the tag.</p> </div>
Raw Low	<p>Lets you specify the low limit for the values received by the tag. Usually, this value corresponds to the specifications of the hardware from which the data is received.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • Standard Integer • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary).
Raw High	<p>Lets you specify the high limit for the values sent by the tag. Usually, this value corresponds to the specifications of the hardware from which the data is received.</p> <p>Valid Entries</p>

Field	Description
	<ul style="list-style-type: none"> • Standard Integer • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary).
Use Low/High Limits	<p>Enables the tag to use the range specified in the Engineering Units fields as the output values.</p> <p>Typically, EGU values normally reflect the expected operating ranges, or the Scale Low and Scale High values for the tag. However, the EGU values also dictate behavior in other areas such as alarming. By allowing the Scale Low and Scale High values to be set to values other than the EGU values, you can further manage conditions when alarms would be generated.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note: If you are Using this tag for charts, make sure to select Use EGU. Selecting this option will make it easier for you to see the changes within the expected range in your chart, because the chart axes will correspond to your expected range and not the entire range of the sensors. The smaller range of the chart makes changes in values more obvious.</p> </div>
Scale Low	Lets you specify the low limit for the values sent by the tag. Usually, this value corresponds to the specifications of the hardware from which the data

Field	Description
	<p>is received. This field is only available if you did not enable Use EGU.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • Standard Integer • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;">  Note: Changes made to this field are not reflected in the data until after the next tag scan. </div>
Scale High	<p>Lets you specify the high limit for the values sent by the tag. Usually, this value corresponds to the specifications of the hardware from which the data is received. This field is only available if you did not enable Use EGU.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • Standard Integer • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary).

Field	Description
	<div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: Changes made to this field are not reflected in the data until after the next tag scan. </div>

Alarm Options

Field	Description
Alarm Areas	<p>Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.
Collect	<p>Lets you select if the tag is set for collection by the Proficy Historian collector.</p> <p>Select Enabled to allow the tag to be collected by the collector.</p>
Collection Interval	<p>Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector.</p> <p>Valid Entries</p> <p>Must be entered in 100 ms intervals. The default value is 5000ms.</p>

Field	Description
	<p>Example</p> <p>1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.</p>
Collection Offset	<p>Used with the collection interval to schedule collection of data from a tag.</p> <p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p> <p>If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.</p>
Time Resolution	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Collector Deadband	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incom-</p>

Field	Description
	<p>ing data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>
Compression Time-out (ms)	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p> <p>Any numeric value.</p>


E-Signature


Field	Description
Type	The Type of Electronic Signature:

Field	Description
	<ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electron-</p>

Field	Description
	ic Signature settings are available. By default, this check box is disabled.

Advanced Options

Field	Description
Output Enable	<p>Lets you configure the tag to send output to the I/O driver, OPC server, or OPC UA server. The tag sends its output when it is in Automatic mode and converts its data according to the entries in the Low Limit (EGU), High Limit (EGU), and Signal Conditioning fields.</p>
Enable Event	<p>Lets you enable or disable event messaging for the tag. Event messaging is similar to alarming except that it does not require acknowledgment. Event messages are sent to the same alarm destinations as alarms for a given block but do not appear in the Alarm Summary object.</p> <p>Analog Output, Analog Register, Digital Output, Digital Register, Digital Input, and Text blocks have event messaging capabilities.</p> <div data-bbox="820 1283 1421 1688" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note: Be careful when using event messaging in a chain with a time-based scan time. If the scan time is short, your alarm files (either disk or printed) can grow very large. We recommend enabling event messaging for exception-based chains, one shot chains, and stand-alone output blocks.</p> </div>
I/O Address Type	<p>Lets you specify the number format of the block's starting address.</p> <p>Valid Entries</p>

Field	Description
	Hex, Octal, or Decimal
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="820 808 1421 1123" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p>

Field	Description
	Text, up to 80 characters.

AR2 Tag

This tag contains the following details:




General

Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <pre>~ ` + ^ : ? " * = { } . , ; ? @</pre>

Field	Description
	<p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

I/O Addressing

Field	Description
I/O Driver	<p>Lets you select an I/O driver, OPC server, or OPC UA server for the tag. The selected driver or server enables the tag to communicate with process hardware on the plant floor.</p> <p>Before you can select an I/O driver, OPC server, or OPC UA server you must install it and add it to the available ones in the SCU.</p>
I/O Address	<p>Lets you enter the location in the process hardware where data for this tag is saved and where output is sent.</p> <p>Valid Entries</p> <p>Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations.</p>

Field	Description
	<div data-bbox="820 262 1414 577">  CAUTION: Do not assign the same I/O address to tags when using exception-based and time-based processing. Doing so will cause the exception-based tags to occasionally miss a value. </div> <div data-bbox="820 598 1414 1039">  CAUTION: Configuration Hub currently does not do I/O address validations before publish. If you enter an invalid IO address into a tag or generate an invalid I/O address via the model and substitutions, the publish may fail to set the IO address into the active database, and your invalid IO address will be removed. </div>
H/W Options	<p data-bbox="820 1081 1414 1197">Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p> <div data-bbox="820 1228 1414 1501">  Note: Signal conditioning and linear scaling cannot be applied simultaneously. If you select a value for Signal Conditioning verify that Linear Scaling is not selected. </div> <p data-bbox="820 1533 1414 1564">Valid Entries</p> <p data-bbox="820 1606 1414 1680">Depends on your driver or server. Refer to your driver or server manual for more information.</p>

Limits and Scaling

Field	Description
Low Limit	Low EGU limit. The low end of the user readable value.
High Limit	High EGU limit. The high end of the user readable value.
Units	Description of the EGU range (for example: DEGF, GPH, PSI).



E-Signature

Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.
Exempt Alarm Ack	Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.
Comment Required	Select this option to enable Comment enforcement in the Perform Comment section. This means that

Field	Description
	<p>the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>

Advanced Options

Field	Description
Enable Output	<p>Lets you configure the tag to send output to the I/O driver, OPC server, or OPC UA server. The tag sends its output when it is in Automatic mode and converts its data according to the entries in the Low Limit (EGU), High Limit (EGU), and Signal Conditioning fields.</p>
I/O Address Type	<p>Lets you enter the base number system used by the I/O Address field. Valid entries include: Decimal, Hexadecimal, or Octal.</p>
Enable Event	<p>Lets you enable or disable event messaging for the tag. Event messaging is similar to alarming except that it does not require acknowledgment. Event messages are sent to the same alarm destinations</p>

Field	Description
	<p>as alarms for a given block but do not appear in the Alarm Summary object.</p> <p>Analog Output, Analog Register, Digital Output, Digital Register, Digital Input, and Text blocks have event messaging capabilities.</p> <div data-bbox="821 541 1416 940" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Be careful when using event messaging in a chain with a time-based scan time. If the scan time is short, your alarm files (either disk or printed) can grow very large. We recommend enabling event messaging for exception-based chains, one shot chains, and stand-alone output blocks.</p> </div>
<p>Security Areas</p>	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="821 1446 1416 1761" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
<p>Alarm Field 1</p>	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you</p>

Field	Description
	<p>want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>

BB Tag

This tag contains the following details:


General

Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal</p>


Field	Description
	<p>databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), under-scores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <p>~ ` + ^ : ? " * = { } . , ; ? @</p> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

I/O Addressing

Field	Description
Activate High Contact	Enables or disables the High Contact Data fields.


Field	Description
High Contact Driver	<p>Lets you select an I/O driver, OPC server, or OPC UA server for the block. The selected driver or server enables the block to communicate with process hardware on the plant floor.</p> <p>Before you can select an I/O driver, OPC server, or OPC UA server you must install it and add it to the available drivers in the SCU.</p>
High Contact Driver I/O Address	<p>Lets you enter the location in the process hardware where data for this block is saved and where output is sent. In an On-Off Control block, specify the address of the digital point you want opened and closed based on the Turn on Above and Turn off Below values.</p> <p>Valid Entries</p> <p>Depends on your driver. Consult your I/O driver manual for details on the proper input/output addresses and configurations.</p> <div data-bbox="820 1161 1419 1472" style="border: 1px solid black; padding: 10px; background-color: #fff9c4;"> <p> CAUTION:</p> <p>Do not assign the same I/O address to blocks when using exception-based and time-based processing. Doing so will cause the exception-based blocks to occasionally miss a value.</p> </div>
High Contact Hardware Options	<p>Lets you select any specific device control addressing format that the block uses to communicate with process hardware on the plant floor.</p> <p>Valid Entries</p> <p>For most process hardware, this field is usually left blank. Consult your I/O driver manual for the applicable hardware code if necessary.</p>


Field	Description
High Contact - Turn On Above	<p>Lets you specify the highest acceptable analog value for the High Contact Data. When the analog input goes above this value, the High Contact I/O address closes.</p> <p>Valid Entries</p> <p>Enter the number that represents this value according to the Low and High Limits (EGU) of the analog input.</p>
High Contact - Turn On Below	<p>Lets you specify the lowest acceptable analog value for the High Contact Data. When the analog input falls below this value, the High Contact I/O address opens.</p> <p>Valid Entries</p> <p>The number that represents this value according to the Low and High Limits (EGU) of the analog input.</p>
Activate Low Contact	<p>Enables or disables the Low Contact Data fields.</p> <p>Valid Entries</p> <p>Select the check box to use the Low Contact Data fields and provide output to a second digital I/O. Clear the check box to suppress them and use your analog input as the basis of a single digital output.</p>
Low Contact Driver	<p>Lets you select an I/O driver, OPC server, or OPC UA server for the block. The selected driver or server enables the block to communicate with process hardware on the plant floor.</p> <p>Before you can select an I/O driver or OPC server, you must install it and add it to the available drivers in the SCU.</p>
Low Contact I/O Address	<p>Lets you enter the location in the process hardware where data for this block is saved and where out-</p>


Field	Description
	<p>put is sent. In an On-Off Control tag, specify the address of the digital point you want opened and closed based on the Turn on Below and Turn off Above values.</p> <p>Valid Entries</p> <p>Depends on your driver. Consult your I/O driver manual for details on the proper input/output addresses and configurations.</p> <div style="border: 1px solid black; background-color: #fff9c4; padding: 10px; margin-top: 10px;">  CAUTION: Do not assign the same I/O address to blocks when using exception-based and time-based processing. Doing so will cause the exception-based blocks to occasionally miss a value. </div>
<p>Low Contact Hardware Options</p>	<p>Lets you select any specific device control addressing format that the block uses to communicate with process hardware on the plant floor.</p> <p>Valid Entries</p> <p>For most process hardware, this field is usually left blank. Consult your I/O driver manual for the applicable hardware code if necessary.</p>
<p>Low Contact - Turn On Above</p>	<p>Lets you specify the highest acceptable analog value for the Low Contact Data. When the analog input goes above this value, the Low Contact I/O address opens.</p> <p>Valid Entries</p> <p>Enter the number that represents this value according to the Low and High Limits (EGU) of the analog input.</p>

Field	Description
Low Contact - Turn On Below	<p>Lets you specify the lowest acceptable analog value for the Low Contact Data. When the analog input falls below this value, the Low Contact I/O address closes.</p> <p>Valid Entries</p> <p>Enter the number that represents this value according to the Low and High Limits (EGU) of the analog input.</p>

Limits and Scaling


Field	Description
Low Limit	<p>Lets you enter the tag's minimum value.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information.</p> </div> <p>In a Calculation or Signal Select tag, if the output of the tag is 10 and the Low Limit is 15, the tag</p>

Field	Description
	<p>clamps the value at 15. You must enter a Low Limit of 10 or less to output a value of 10.</p> <p>If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the Low Limit field.</p> <p>If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
High Limit	<p>Lets you enter the tag's maximum value.</p> <p>Valid Entries</p> <p>You can enter a high limit in one of three formats:</p> <ul style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information.</p> </div> <p>In a Calculation or a Signal Select tag, if the output of the tag is 150 and the High Limit is 100, the tag clamps the value at 100. You must enter a High Limit of 150 or more to output a value of 150.</p>

Field	Description
	<p>If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the High Limit field.</p> <p>If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
Units	<p>Lets you enter text describing the engineering units range.</p> <p>Valid Entries</p> <p>Up to 33 characters.</p> <p>Example</p> <p>Kilograms per square meter, Liters per minute, degrees Celsius,</p> <div data-bbox="820 1024 1421 1291" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: This entry does not affect the calculation or function of any variables in iFIX. It is used strictly as a display label to identify the engineering units.</p> </div>

Alarm Options

Field	Description
Alarm Areas	<p>Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>

Field	Description
Enable Alarm	<p>Lets you enable or disable alarming for this tag.</p> <p>When you enable alarming, the tag generates alarms allowing objects in your operator displays to show alarm conditions, and enabling other tags to detect alarms from the tag.</p> <div data-bbox="820 548 1421 865" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: The entire chain can be affected when you disable alarms for a tag. In addition, for both the Digital and Analog Alarm tags, this field is ignored when you enable the Alarm Suspend field.</p> </div>

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.
Collect	<p>Lets you select if the tag is set for collection by the Proficy Historian collector.</p> <p>Select Enabled to allow the tag to be collected by the collector.</p>
Collection Interval	<p>Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector.</p> <p>Valid Entries</p> <p>Must be entered in 100 ms intervals. The default value is 5000ms.</p> <p>Example</p>

Field	Description
	1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.
Collection Offset	<p>Used with the collection interval to schedule collection of data from a tag.</p> <p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p> <p>If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.</p>
Time Resolution	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Collector Deadband	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values</p>

Field	Description
	<p>that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>
Compression Time-out (ms)	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p> <p>Any numeric value.</p>


E-Signature


Field	Description
Type	The Type of Electronic Signature:

Field	Description
	<ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electron-</p>

Field	Description
	ic Signature settings are available. By default, this check box is disabled.

Advanced Options

Field	Description
One Shot	<p>Lets you specify how often to activate the four contact data fields. When selected, the On-Off Control tag sends OPEN or CLOSE commands to the High and Low Contacts only when there is a change of state, rather than each time the tag executes. When cleared, the check box sends the commands every scan period.</p>
Invert Output	<p>Inverts the tag's output value. For example, if you want the I/O driver to return a closed contact as a logical 0 and an open contact as a logical 1, click the check box.</p> <p>Alternatively, to return a closed contact as a logical 1 (normal conditions) and an open contact as a logical 0, clear the check box.</p>
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="824 1717 1419 1864" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area.</p> </div>

Field	Description
	 This allows users to retrieve data from a specific security area even if they cannot write to that area.
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>

BL Tag

This tag contains the following details:

General

Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p>

Field	Description
	<p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <p>~ ` + ^ : ? " * = { } . , ; ? @</p> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	<p>The tag type. Display-only field.</p>
Current Value	<p>The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.</p>

Inputs

Field	Description
Input A	<p>Lets you enter a descriptive label for the logical 0 value received by the tag. You can display this label in the iFIX WorkSpace through a Data link to aid operators in interpreting the value for the contact.</p> <p>Valid Entries</p> <p>A label of up to 16 characters.</p> <p>Examples</p> <p>Open, Off</p>
Input B	<p>Lets you enter a descriptive label for the logical 0 value received by the tag. You can display this label in the iFIX WorkSpace through a Data link to aid operators in interpreting the value for the contact.</p> <p>Valid Entries</p> <p>A label of up to 16 characters.</p> <p>Examples</p> <p>Open, Off</p>
Input C	<p>Lets you enter a descriptive label for the logical 0 value received by the tag. You can display this label in the iFIX WorkSpace through a Data link to aid operators in interpreting the value for the contact.</p> <p>Valid Entries</p> <p>A label of up to 16 characters.</p> <p>Examples</p> <p>Open, Off</p>
Input D	<p>Lets you enter a descriptive label for the logical 0 value received by the tag. You can display this label</p>

Field	Description
	<p>in the iFIX WorkSpace through a Data link to aid operators in interpreting the value for the contact.</p> <p>Valid Entries</p> <p>A label of up to 16 characters.</p> <p>Examples</p> <p>Open, Off</p>
Input E	<p>Lets you enter a descriptive label for the logical 0 value received by the tag. You can display this label in the iFIX WorkSpace through a Data link to aid operators in interpreting the value for the contact.</p> <p>Valid Entries</p> <p>A label of up to 16 characters.</p> <p>Examples</p> <p>Open, Off</p>
Input F	<p>Lets you enter a descriptive label for the logical 0 value received by the tag. You can display this label in the iFIX WorkSpace through a Data link to aid operators in interpreting the value for the contact.</p> <p>Valid Entries</p> <p>A label of up to 16 characters.</p> <p>Examples</p> <p>Open, Off</p>
Input G	<p>Lets you enter a descriptive label for the logical 0 value received by the tag. You can display this label in the iFIX WorkSpace through a Data link to aid operators in interpreting the value for the contact.</p> <p>Valid Entries</p>

Field	Description
	<p>A label of up to 16 characters.</p> <p>Examples</p> <p>Open, Off</p>
Input H	<p>Lets you enter a descriptive label for the logical 0 value received by the tag. You can display this label in the iFIX WorkSpace through a Data link to aid operators in interpreting the value for the contact.</p> <p>Valid Entries</p> <p>A label of up to 16 characters.</p> <p>Examples</p> <p>Open, Off</p>
Output Calculation	<p>Lets you specify the Boolean block equation. If the equation is true, a value of 1 is passed to the next block. If the equation is false, a value of 0 is passed to the next tag.</p> <p>Valid Entries</p> <p>Write the equation using the input letters (A - H) that correspond to the defined Input fields. The calculation can use the input values more than once.</p> <p>Example</p> <p>(C+(A+B))</p>

Limits and Scaling

Field	Description
Open Tag	<p>Lets you enter a descriptive label for the logical 1 value received by the tag. You can display this label in the iFIX WorkSpace through a Data link to aid operators in interpreting the value for the contact.</p>

Field	Description
	<p>Valid Entries</p> <p>A label of up to 16 characters.</p> <p>Examples</p> <p>Close, On.</p>
Close Tag	<p>Lets you enter a descriptive label for the logical 0 value received by the tag. You can display this label in the iFIX WorkSpace through a Data link to aid operators in interpreting the value for the contact.</p> <p>Valid Entries</p> <p>A label of up to 16 characters.</p> <p>Examples</p> <p>Open, Off</p>

Alarm Options

Field	Description
Alarm Areas	<p>Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>

Alarm Limits

Field	Description
Low Low	<p>Lets you enter the tag's critically low values. When the tag's value falls below this limit, the tag generates an alarm.</p>

Field	Description
	<p>Valid Entries</p> <p>A critically low value within the tag's engineering units range.</p> <p>Example</p> <p>If a temperature of 25 degrees indicates that a cooling water flow is frozen, you could enter a value of 30 degrees for your Low Low alarm.</p>
Low	<p>Lets you enter the tag's low process values. When the tag's value falls below this limit, the tag generates an alarm.</p> <p>Valid Entries</p> <p>A low value within the tag's engineering units range. If you want to provide a warning that a value is approaching a critical low limit, enter a slightly higher value than the Low Low alarm.</p> <p>Example</p> <p>If a temperature of 35 degrees indicates that ice crystals are forming in a cooling water flow, you could enter a value of 40 degrees for your Low alarm.</p>
High	<p>Lets you enter the tag's high process values. When the tag's value exceeds this limit, the tag generates an alarm.</p> <p>Valid Entries</p> <p>A high value within the tag's engineering units range. If you want to provide a warning that a value is approaching a critically high limit, enter a slightly lower value than the High High alarm.</p> <p>Example</p>

Field	Description
	<p>If a bearing temperature of 80 degrees indicates machine wear, you could enter a value of 75 degrees for your High alarm.</p>
<p>High High</p>	<p>Lets you enter the tag's critically high values. When the tag's value exceeds this limit, the tag generates an alarm.</p> <p>Valid Entries</p> <p>A critically high value within the tag's engineering units range.</p> <p>Example</p> <p>If a bearing temperature of 90 degrees indicates imminent seizure, you could enter a value of 85 degrees for your High High alarm.</p>
<p>Rate of Change</p>	<p>Lets you enter the maximum, acceptable change in a tag's value. If the tag's current value changes by more than the specified value within one scan period, the tag generates a Rate of Change alarm.</p> <p>Valid Entries</p> <p>A value within the tag's engineering units range, to be checked per scan period. Enter 0 to disable this alarm.</p> <p>Example</p> <p>To generate an alarm due to a fluctuation of more than 20 RPMs on a speed drive since the last scan period, you would enter a 20 in this field.</p>
<p>Deadband</p>	<p>Lets you enter the maximum fluctuation the tag accepts without re-issuing an alarm. As long as the fluctuation is within the dead band range, the tag issues an alarm once, eliminating nuisance alarms. Once the alarm falls below the dead band and then</p>

Field	Description
	<p>exceeds the alarm limits, the tag generates another alarm.</p> <p>Valid Entries</p> <p>Numeric value within the EGU range.</p> <p>Example</p> <p>If the High alarm limit is 80 and the dead band is 5, the tag does not re-issue an alarm after the one while the current value fluctuates between 75 and 85.</p>

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.
Collect	<p>Lets you select if the tag is set for collection by the Proficy Historian collector.</p> <p>Select Enabled to allow the tag to be collected by the collector.</p>
Collection Interval	<p>Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector.</p> <p>Valid Entries</p> <p>Must be entered in 100 ms intervals. The default value is 5000ms.</p> <p>Example</p> <p>1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.</p>

Field	Description
Collection Offset	<p>Used with the collection interval to schedule collection of data from a tag.</p> <p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p> <p>If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.</p>
Time Resolution	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Collector Deadband	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p>



Field	Description
	Select Disabled to prevent the tag from being compressed.
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>
Compression Time-out (ms)	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p> <p>Any numeric value.</p>

E-Signature

Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag.

Field	Description
	<ul style="list-style-type: none"> • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>

Advanced Options

Field	Description
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="824 827 1419 1138" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
Previous Block	<p>Displays the name of the previous (upstream) tag.</p> <p>Valid Entries</p> <p>None. This is a read-only field.</p>
Next Block	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div data-bbox="824 1528 1419 1789" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: In a Statistical Data tag, the Next Block field specifies the tag name of the downstream Statistical Control tag. No other tag type is valid.</p> </div>

Field	Description
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Process by Exception	Enables exception-based processing for the block.
Scan Time	<p>Lets you specify how often the Scan, Alarm, and Control (SAC) program processes the tag and any blocks chained to it.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • 0 (one shot processing) • 0.05 to .95 in .05 increments (subsecond scan times) • 1 to 60 in 1 second increments • 1M to 60M in 1 minute increments • 1H to 24H in 1 hour increments <p>Example</p> <p>0.15 specifies a 15-subsecond scan time. 5 specifies a 5-second scan time, 10M specifies a 10-</p>

Field	Description
	minute scan time, 16H specifies a 16-hour scan time.
Phase At	<p>Lets you specify how long the Scan, Alarm, and Control (SAC) program delays in scanning the tag. When the tag has a second or subsecond scan time, SAC offsets the initial scan by the phase time when iFIX starts or when the database is re-loaded. When the tag has a scan time of 1 minute or longer, SAC offsets the initial scan starting at midnight.</p> <p>Valid Entries</p> <p>Depends on the scan time. If the scan time is in hours, the phase must be in hours:minutes. If the scan time is in minutes, the phase must be in minutes:seconds. If the scan time is in seconds, the phase must be in seconds. If the scan time is in subseconds, the phase must be in subseconds.</p>

BPL Tag

This tag contains the following details:

General

Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p>

Field	Description
	<p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <pre>~ ` + ^ : ? " * = { } . , ; ? @</pre> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

Limits and Scaling

Field	Description
Low Limit	Used to clamp PV, SP and internal calculations. Should match the output EGU of the upstream block. Inverted EGU range is not supported by the BPL block. The HI egu must be larger than the LO egu.
High Limit	Used to clamp PV, SP and internal calculations. Should match the output EGU of the upstream block. Inverted EGU range is not supported by the BPL block. The HI egu must be larger than the LO egu.
Units	For display purposes.

Breakpoints


Field	Description
Input 00-10	The input to the block is compared to each of these input breakpoints. The first value which exceeds the actual input determines the Output and Slope to be used. For this reason the inputs should generally be entered in increasing order. The INPUT values can be any float.
Output 00-19	The OUTPUTS correspond to the inputs. Once the breakpoint interval is determined by checking the input table the corresponding OUTPUT is used as the base of the computed output value. The OUTPUT values can be any float.
Slope 00-19	The SLOPE is used to determine how much to add to the OUTPUT. The SLOPE values can be any float.

E-Signature

Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p>

Field	Description
	<p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>

Advanced Options

Field	Description
Previous Block	<p>Displays the name of the previous (upstream) tag.</p> <p>Valid Entries</p> <p>None. This is a read-only field.</p>
Next Block	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note: In a Statistical Data tag, the Next Block field specifies the tag name of the downstream Statistical Control tag. No other tag type is valid.</p> </div>

CA Tag

This tag contains the following details:



General



Field	Description
Tag Name	Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.



Field	Description
	<p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <p>~ ` + ^ : ? " * = { } . , ; ? @</p> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.



Field	Description
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.




Inputs



Field	Description
Input A	<p>Lets you specify the inputs to the Calculation tag.</p> <p>Valid Entries</p> <p>The following are valid entries for defining your equation with Input entries:</p> <ul style="list-style-type: none"> • Constants (a floating point number). • Tag names (representing the tag's current value of the tag), including the Calculation block itself. For example, AI1 to represent AI1.F_CV. <div data-bbox="821 1119 1417 1339" style="border: 1px solid #00a0c0; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note: If you enter a tag name without entering a field name, iFIX automatically enters F_CV as the default field name.</p> </div> <p>Tag and field pairs represent the value of the specified field. For example, PID1.F_TV1 to access the tag's set point.</p> <div data-bbox="821 1530 1417 1707" style="border: 1px solid #00a0c0; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note: Input field A always represents the output of the upstream block (previous block).</p> </div> <p>Example</p>




Field	Description
	<p>To input the value of the Statistical Data block's XBARBAR, you would enter SD1.F_XBB. Note the period between the block and field names.</p>
<p>Input B</p>	<p>Lets you specify the inputs to the Calculation tag.</p> <p>Valid Entries</p> <p>The following are valid entries for defining your equation with Input entries:</p> <ul style="list-style-type: none"> • Constants (a floating point number). • Tag names (representing the tag's current value of the tag), including the Calculation block itself. For example, AI1 to represent AI1.F_CV. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note: If you enter a tag name without entering a field name, iFIX automatically enters F_CV as the default field name.</p> </div> <p>Tag and field pairs represent the value of the specified field. For example, PID1.F_TV1 to access the tag's set point.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note: Input field A always represents the output of the upstream block (previous block).</p> </div> <p>Example</p> <p>To input the value of the Statistical Data block's XBARBAR, you would enter SD1.F_XBB. Note the period between the block and field names.</p>
<p>Input C</p>	<p>Lets you specify the inputs to the Calculation tag.</p>


Field	Description
	<p>Valid Entries</p> <p>The following are valid entries for defining your equation with Input entries:</p> <ul style="list-style-type: none"> • Constants (a floating point number). • Tag names (representing the tag's current value of the tag), including the Calculation block itself. For example, AI1 to represent AI1.F_CV. <div data-bbox="824 720 1419 940" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: If you enter a tag name without entering a field name, iFIX automatically enters F_CV as the default field name.</p> </div> <p>Tag and field pairs represent the value of the specified field. For example, PID1.F_TV1 to access the tag's set point.</p> <div data-bbox="824 1131 1419 1308" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Input field A always represents the output of the upstream block (previous block).</p> </div> <p>Example</p> <p>To input the value of the Statistical Data block's XBARBAR, you would enter SD1.F_XBB. Note the period between the block and field names.</p>
Input D	<p>Lets you specify the inputs to the Calculation tag.</p> <p>Valid Entries</p> <p>The following are valid entries for defining your equation with Input entries:</p>

Field	Description
	<ul style="list-style-type: none"> • Constants (a floating point number). • Tag names (representing the tag's current value of the tag), including the Calculation block itself. For example, AI1 to represent AI1.F_CV. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;">  Note: If you enter a tag name without entering a field name, iFIX automatically enters F_CV as the default field name. </div> <p>Tag and field pairs represent the value of the specified field. For example, PID1.F_TV1 to access the tag's set point.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;">  Note: Input field A always represents the output of the upstream block (previous block). </div> <p>Example</p> <p>To input the value of the Statistical Data block's XBARBAR, you would enter SD1.F_XBB. Note the period between the block and field names.</p>
Input E	<p>Lets you specify the inputs to the Calculation tag.</p> <p>Valid Entries</p> <p>The following are valid entries for defining your equation with Input entries:</p> <ul style="list-style-type: none"> • Constants (a floating point number). • Tag names (representing the tag's current value of the tag), including the Calculation block itself. For example, AI1 to represent AI1.F_CV.

Field	Description
	<div data-bbox="820 268 1417 485" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-bottom: 10px;">  Note: If you enter a tag name without entering a field name, iFIX automatically enters F_CV as the default field name. </div> <p data-bbox="820 520 1417 640">Tag and field pairs represent the value of the specified field. For example, PID1.F_TV1 to access the tag's set point.</p> <div data-bbox="820 676 1417 850" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-bottom: 10px;">  Note: Input field A always represents the output of the upstream block (previous block). </div> <p data-bbox="820 886 1417 1081">Example To input the value of the Statistical Data block's XBARBAR, you would enter SD1.F_XBB. Note the period between the block and field names.</p>
Input F	<p data-bbox="820 1113 1417 1144">Lets you specify the inputs to the Calculation tag.</p> <p data-bbox="820 1186 1417 1218">Valid Entries</p> <p data-bbox="820 1260 1417 1333">The following are valid entries for defining your equation with Input entries:</p> <ul data-bbox="885 1375 1417 1596" style="list-style-type: none"> • Constants (a floating point number). • Tag names (representing the tag's current value of the tag), including the Calculation block itself. For example, AI1 to represent AI1.F_CV. <div data-bbox="820 1638 1417 1848" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;">  Note: If you enter a tag name without entering a field name, iFIX automatically enters F_CV as the default field name. </div>



Field	Description
	<p>Tag and field pairs represent the value of the specified field. For example, PID1.F_TV1 to access the tag's set point.</p> <div data-bbox="824 426 1421 600" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: Input field A always represents the output of the upstream block (previous block). </div> <p>Example</p> <p>To input the value of the Statistical Data block's XBARBAR, you would enter SD1.F_XBB. Note the period between the block and field names.</p>
Input G	<p>Lets you specify the inputs to the Calculation tag.</p> <p>Valid Entries</p> <p>The following are valid entries for defining your equation with Input entries:</p> <ul style="list-style-type: none"> • Constants (a floating point number). • Tag names (representing the tag's current value of the tag), including the Calculation block itself. For example, AI1 to represent AI1.F_CV. <div data-bbox="824 1381 1421 1604" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: If you enter a tag name without entering a field name, iFIX automatically enters F_CV as the default field name. </div> <p>Tag and field pairs represent the value of the specified field. For example, PID1.F_TV1 to access the tag's set point.</p>



Field	Description
	<div data-bbox="820 268 1421 441" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: Input field A always represents the output of the upstream block (previous block). </div> <p data-bbox="820 472 925 504">Example</p> <p data-bbox="820 535 1421 661">To input the value of the Statistical Data block's XBARBAR, you would enter SD1.F_XBB. Note the period between the block and field names.</p>
<p data-bbox="203 693 284 724">Input H</p>	<p data-bbox="820 693 1421 724">Lets you specify the inputs to the Calculation tag.</p> <p data-bbox="820 766 974 798">Valid Entries</p> <p data-bbox="820 829 1421 913">The following are valid entries for defining your equation with Input entries:</p> <ul data-bbox="876 955 1421 1186" style="list-style-type: none"> • Constants (a floating point number). • Tag names (representing the tag's current value of the tag), including the Calculation block itself. For example, AI1 to represent AI1.F_CV. <div data-bbox="820 1218 1421 1438" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: If you enter a tag name without entering a field name, iFIX automatically enters F_CV as the default field name. </div> <p data-bbox="820 1470 1421 1596">Tag and field pairs represent the value of the specified field. For example, PID1.F_TV1 to access the tag's set point.</p> <div data-bbox="820 1627 1421 1816" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: Input field A always represents the output of the upstream block (previous block). </div> <p data-bbox="820 1837 925 1869">Example</p>

Field	Description
	To input the value of the Statistical Data block's XBARBAR, you would enter SD1.F_XBB. Note the period between the block and field names.
Output Calculation	<p>Lets you specify the Calculation block equation.</p> <p>Valid Entries</p> <p>An equation using the input letters (A - H) that correspond to the defined Input fields. The input letters may be used more than once.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note: A mathematical overflow (value >1038), underflow (below 10⁻³⁷), or division by zero causes a Calc error status in the upstream block.</p> </div>


Limits and Scaling

Field	Description
Low Limit	<p>Lets you enter the tag's minimum value.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary).

Field	Description
	<div data-bbox="824 260 1424 529" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. </div> <p data-bbox="816 562 1424 730">In a Calculation or Signal Select tag, if the output of the tag is 10 and the Low Limit is 15, the tag clamps the value at 15. You must enter a Low Limit of 10 or less to output a value of 10.</p> <p data-bbox="816 766 1424 892">If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the Low Limit field.</p> <p data-bbox="816 928 1424 1054">If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
High Limit	<p data-bbox="816 1081 1424 1117">Lets you enter the tag's maximum value.</p> <p data-bbox="816 1150 1424 1186">Valid Entries</p> <p data-bbox="816 1222 1424 1257">You can enter a high limit in one of three formats:</p> <ul data-bbox="880 1306 1424 1705" style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div data-bbox="824 1747 1424 1894" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: The I/O driver can set certain limitations on the engineering units range. Consult </div>

Field	Description
	<div data-bbox="824 268 1414 373" style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px;">  your I/O driver manual for more information. </div> <p data-bbox="818 409 1421 573">In a Calculation or a Signal Select tag, if the output of the tag is 150 and the High Limit is 100, the tag clamps the value at 100. You must enter a High Limit of 150 or more to output a value of 150.</p> <p data-bbox="818 615 1421 737">If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the High Limit field.</p> <p data-bbox="818 779 1421 900">If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
Units	<p data-bbox="818 930 1421 1005">Lets you enter text describing the engineering units range.</p> <p data-bbox="818 1047 971 1077">Valid Entries</p> <p data-bbox="818 1119 1057 1148">Up to 33 characters.</p> <p data-bbox="818 1190 922 1220">Example</p> <p data-bbox="818 1262 1406 1337">Kilograms per square meter, Liters per minute, degrees Celsius,</p> <div data-bbox="824 1371 1414 1635" style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px;">  Note: This entry does not affect the calculation or function of any variables in iFIX. It is used strictly as a display label to identify the engineering units. </div>

Alarm Options

Field	Description
Alarm Areas	<p>Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>
Enable Alarm	<p>Lets you enable or disable alarming for this tag.</p> <p>When you enable alarming, the tag generates alarms allowing objects in your operator displays to show alarm conditions, and enabling other tags to detect alarms from the tag.</p> <div style="border: 1px solid #00a0c0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note:</p> <p>The entire chain can be affected when you disable alarms for a tag. In addition, for both the Digital and Analog Alarm tags, this field is ignored when you enable the Alarm Suspend field.</p> </div>

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.
Collect	<p>Lets you select if the tag is set for collection by the Proficy Historian collector.</p> <p>Select Enabled to allow the tag to be collected by the collector.</p>

Field	Description
Collection Interval	<p>Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector.</p> <p>Valid Entries</p> <p>Must be entered in 100 ms intervals. The default value is 5000ms.</p> <p>Example</p> <p>1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.</p>
Collection Offset	<p>Used with the collection interval to schedule collection of data from a tag.</p> <p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p> <p>If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.</p>
Time Resolution	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incom-</p>

Field	Description
	<p>ing data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Collector Deadband	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>
Compression Time-out (ms)	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p>


Field	Description
	Any numeric value.


E-Signature

Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>

Field	Description
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>

Advanced Options

Field	Description
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="820 1417 1421 1722" style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
Previous Block	<p>Displays the name of the previous (upstream) tag.</p> <p>Valid Entries</p>

Field	Description
	None. This is a read-only field.
Next Block	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div data-bbox="820 485 1421 751" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: In a Statistical Data tag, the Next Block field specifies the tag name of the downstream Statistical Control tag. No other tag type is valid.</p> </div>
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>

CTR Tag

This tag contains the following details:

General


Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <pre>~ ` + ^ : ? " * = { } . , ; ? @</pre> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p>


Field	Description
	A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

Limits and Scaling

Field	Description
Low Limit	Used to clamp PV, SP and internal calculations. Should match the output EGU of the upstream block. Inverted EGU range is not supported by the PI2 block. The HI egu must be larger than the LO egu.
High Limit	Used to clamp PV, SP and internal calculations. Should match the output EGU of the upstream block. Inverted EGU range is not supported by the PI2 block. The HI egu must be larger than the LO egu.
Units	For display purposes.
Limit Value	A value which if reached or exceeded will generate an alarm. This will still function if set to zero. To disable alarming simply clear the Alarm Enable Field.
Gate tag	A TAG:FIELD specifier (normally an F_CV). If non-zero then the counting logic is enabled. If this field is blank then the gate is considered TRUE. Note that a transition to true on the gate will NOT generate a count even if the input is in the active state.

Alarm Options

Field	Description
Alarm Areas	<p>Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>
Enable Alarm	<p>Lets you enable or disable alarming for this tag.</p> <p>When you enable alarming, the tag generates alarms allowing objects in your operator displays to show alarm conditions, and enabling other tags to detect alarms from the tag.</p> <div data-bbox="821 1003 1419 1318" style="border: 1px solid #00a0c0; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p> Note:</p> <p>The entire chain can be affected when you disable alarms for a tag. In addition, for both the Digital and Analog Alarm tags, this field is ignored when you enable the Alarm Suspend field.</p> </div>
Priority	<p>Lets you specify the alarm priority for a tag. If the priority is equal or greater than the SCADA node's alarm priority, iFIX sends the alarm to all the alarm destinations enabled for this node. However, if the priority is less than the SCADA node's alarm priority, the alarm is automatically acknowledged and filtered out so that it does not appear in your alarm destinations. However, the alarm does appear in Data links configured to display current and latched alarms.</p> <p>Valid Entries</p>

Field	Description
	<p>INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL</p> <div data-bbox="824 380 1414 646" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: To report tag alarms, the appropriate alarm areas must be assigned to each of the alarm services enabled in the System Configuration Utility (SCU).</p> </div>
Shelve Enable	Select this check box to enable Alarm Shelving for the tag.
Shelve Policy	Select an alarm shelving policy from the drop-down list.


E-Signature



Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.
Exempt Alarm Ack	Select to allow operators to acknowledge alarms for this tag without entering a signature, even if

Field	Description
	this tag requires electronic signatures for data entry.
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>

Advanced Options

Field	Description
Mode	Count on transition to OPEN, CLOSE or COS (any transition).
Passed Value	<p>INPUT passes raw input (converted to 0/1).</p> <p>ALM passes Current Alarm (converted to 0/1).</p> <p>LIMIT passes 'Limit Reached' (as 0/1 which is checked regardless of Alarm Enable, Auto and Gate states).</p>

Field	Description
	<p>COUNT passes current value of Counter. Note that the counter value is converted to Float. Precision may be lost.</p> <p>Also note that some downstream blocks (such as AO) may clamp this to their EGU or OPERATOR limits.</p>
Startup Mode	Initial Auto/ Manual Status. When in Automatic the output signal is generated. When in Manual the output signal is 'paused'.
Clear on Startup	Should the count be cleared when the chain goes on scan? If not then the count is retained while the block is off scan. Also on system reload, the block will retain the value it had the last time the database was saved to disk (by DBB).
Chain on Transition	<p>If set to YES, the NEXT block will execute only if a transition is counted (requires AUTO and GATE are true).</p> <div data-bbox="821 1136 1419 1356" style="border: 1px solid #00a0c0; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p> Note: A manual change to count via the A_COUNT field will NOT satisfy this condition.</p> </div>
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p>

Field	Description
	<div data-bbox="820 262 1421 577" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;">  Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area. </div>
Previous Block	Displays the name of the previous (upstream) tag. Valid Entries None. This is a read-only field.
Next Block	Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button. <div data-bbox="820 955 1421 1228" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;">  Note: In a Statistical Data tag, the Next Block field specifies the tag name of the downstream Statistical Control tag. No other tag type is valid. </div>
Alarm Field 1	Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information. Valid Entries Text, up to 80 characters.
Alarm Field 2	Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.

Field	Description
	<p>Valid Entries</p> <p>Text, up to 80 characters.</p>

D16 Tag

This tag contains the following details:



General


Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p>

Field	Description
	<p>~ ` + ^ : ? " * = { } . , ; ? @</p> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

I/O Addressing

Field	Description
Mode	<p>The scan time determines how often SAC processes the block and sends the current value to the next block in the chain (ANALOG or DIGITAL). SAC processes all secondary blocks chained to a primary block according to the primary block's scan time.</p> <p>Exception based scanning is supported by this block when used in ANALOG mode. Support for exceptions is a function of the I/O Driver. Most but not all drivers will support exception based processing.</p> <p>Exception based processing is NOT supported in DIGITAL mode.</p>

Field	Description
I/O Driver	<p>Lets you select an I/O driver, OPC server, or OPC UA server for the tag. The selected driver or server enables the tag to communicate with process hardware on the plant floor.</p> <p>Before you can select an I/O driver, OPC server, or OPC UA server you must install it and add it to the available ones in the SCU.</p>
I/O Address	<p>Lets you enter the location in the process hardware where data for this tag is saved and where output is sent.</p> <p>Valid Entries</p> <p>Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations.</p> <div data-bbox="821 1024 1414 1335" style="border: 1px solid black; border-radius: 10px; padding: 10px; background-color: #fff9c4;"> <p> CAUTION: Do not assign the same I/O address to tags when using exception-based and time-based processing. Doing so will cause the exception-based tags to occasionally miss a value.</p> </div> <div data-bbox="821 1367 1414 1808" style="border: 1px solid black; border-radius: 10px; padding: 10px; background-color: #fff9c4;"> <p> CAUTION: Configuration Hub currently does not do I/O address validations before publish. If you enter an invalid IO address into a tag or generate an invalid I/O address via the model and substitutions, the publish may fail to set the IO address into the active database, and your invalid IO address will be removed.</p> </div>

Field	Description
Bitcount	<p>Number of bits to read when in digital mode (default = 16). This is used ONLY when mode is set to DIGITAL and is intended for those rare cases when an error might be generated by reading too many bits (for example you want to read only the last 7 bits in a poll record).</p>
H/W Options	<p>Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p> <div data-bbox="824 720 1417 989" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Signal conditioning and linear scaling cannot be applied simultaneously. If you select a value for Signal Conditioning verify that Linear Scaling is not selected.</p> </div> <p>Valid Entries</p> <p>Depends on your driver or server. Refer to your driver or server manual for more information.</p>
Process by Exception	<p>Enables exception-based processing for the tag.</p>
Scan Time	<p>Lets you specify how often the Scan, Alarm, and Control (SAC) program processes the tag and any tags (blocks) chained to it.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • 0 (one shot processing) • 0.05 to .95 in .05 increments (subsecond scan times) • 1 to 60 in 1 second increments • 1M to 60M in 1 minute increments • 1H to 24H in 1 hour increments <p>Example</p>


Field	Description
	0.15 specifies a 15-subsecond scan time. 5 specifies a 5-second scan time, 10M specifies a 10-minute scan time, 16H specifies a 16-hour scan time.
Phase At	<p>Lets you specify how long the Scan, Alarm, and Control (SAC) program delays in scanning the tag. When the tag has a second or subsecond scan time, SAC offsets the initial scan by the phase time when iFIX starts or when the database is reloaded. When the tag has a scan time of 1 minute or longer, SAC offsets the initial scan starting at midnight.</p> <p>Valid Entries</p> <p>Depends on the scan time. If the scan time is in hours, the phase must be in hours:minutes. If the scan time is in minutes, the phase must be in minutes:seconds. If the scan time is in seconds, the phase must be in seconds. If the scan time is in subseconds, the phase must be in subseconds.</p>


Device States

Field	Description
Status String 0-15	Shows the 16 strings associated with the bits. The strings can be up to 40 bytes (plus NUL). Note that if the string contains the special vertical bar character ' ' then the characters to the left of this will represent the ON state of the input and the characters to the right will represent the OFF state of the input. If it does not contain this character then the entire string represents the ON state and a NULL string represents the OFF state.
Alarm 0-15	Indicate which bits should generate an alarm.

Field	Description
Invert 0-15	Indicates which bits should be inverted before being processed.

Alarm Options

Field	Description
Alarm Areas	<p>Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>
Enable Alarm	<p>Lets you enable or disable alarming for this tag.</p> <p>When you enable alarming, the tag generates alarms allowing objects in your operator displays to show alarm conditions, and enabling other tags to detect alarms from the tag.</p> <div data-bbox="820 1207 1421 1522" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note:</p> <p>The entire chain can be affected when you disable alarms for a tag. In addition, for both the Digital and Analog Alarm tags, this field is ignored when you enable the Alarm Suspend field.</p> </div>
Priority	<p>Lets you specify the alarm priority for a tag. If the priority is equal or greater than the SCADA node's alarm priority, iFIX sends the alarm to all the alarm destinations enabled for this node. However, if the priority is less than the SCADA node's alarm priority, the alarm is automatically acknowledged and filtered out so that it does not appear in your alarm destinations. However, the alarm does ap-</p>

Field	Description
	<p>appear in Data links configured to display current and latched alarms.</p> <p>Valid Entries</p> <p>INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL</p> <div data-bbox="820 569 1414 835" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: To report tag alarms, the appropriate alarm areas must be assigned to each of the alarm services enabled in the System Configuration Utility (SCU).</p> </div>
Shelve Enable	Select this check box to enable Alarm Shelving for the tag.
Shelve Policy	Select an alarm shelving policy from the drop-down list.


E-Signature


Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person perform-

Field	Description
	ing an action and does not affect the person verifying an action.
Exempt Alarm Ack	Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>

Advanced Options

Field	Description
Initial Scan	<p>Lets you select whether the tag is initially placed on or off scan.</p> <p>Click On Scan to place the tag on scan as soon as the Scan, Alarm, and Control (SAC) program starts or when the database is loaded. Click Off Scan to</p>

Field	Description
	place the tag on scan by a Program block, an Event Action tag, a script, an operator entry in a Data link, or an Easy Database Access program.
Realarm Time	If set, then the driver will generate a new alarm message (and new alarm bit) whenever any individual bit goes into alarm. If clear then entire block is either in alarm or not.
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="821 1098 1419 1409" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
Previous Block	<p>Displays the name of the previous (upstream) tag.</p> <p>Valid Entries</p> <p>None. This is a read-only field.</p>
Next Block	Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.

Field	Description
	<div style="border: 1px solid #0070C0; border-radius: 5px; padding: 10px; background-color: #E6F2FF;">  Note: In a Statistical Data tag, the Next Block field specifies the tag name of the downstream Statistical Control tag. No other tag type is valid. </div>
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>

DA Tag

This tag contains the following details:



General




Field	Description
Tag Name	Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.

Field	Description
	<p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <p>~ ` + ^ : ? " * = { } . , ; ? @</p> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.

Field	Description
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

I/O Addressing

Field	Description
I/O Driver	<p>Lets you select an I/O driver, OPC server, or OPC UA server for the tag. The selected driver or server enables the tag to communicate with process hardware on the plant floor.</p> <p>Before you can select an I/O driver, OPC server, or OPC UA server you must install it and add it to the available ones in the SCU.</p>
I/O Address	<p>Lets you enter the location in the process hardware where data for this tag is saved and where output is sent.</p> <p>Valid Entries</p> <p>Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations.</p> <div data-bbox="820 1346 1419 1654" style="border: 1px solid black; border-radius: 10px; background-color: #fff9c4; padding: 10px; margin-bottom: 10px;"> <p> CAUTION: Do not assign the same I/O address to tags when using exception-based and time-based processing. Doing so will cause the exception-based tags to occasionally miss a value.</p> </div> <div data-bbox="820 1686 1419 1881" style="border: 1px solid black; border-radius: 10px; background-color: #fff9c4; padding: 10px;"> <p> CAUTION: Configuration Hub currently does not do I/O address validations before publish. If you enter an invalid IO address into a tag</p> </div>

Field	Description
	<p> or generate an invalid I/O address via the model and substitutions, the publish may fail to set the IO address into the active database, and your invalid IO address will be removed.</p>
Signal Conditioning	<p>Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p> <div data-bbox="821 688 1421 953" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Signal conditioning and linear scaling cannot be applied simultaneously. If you select a value for Signal Conditioning verify that Linear Scaling is not selected.</p> </div> <p>Valid Entries</p> <p>Depends on your driver or server. Refer to your driver or server manual for more information.</p>
H/W Options	<p>Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p> <div data-bbox="821 1325 1421 1589" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Signal conditioning and linear scaling cannot be applied simultaneously. If you select a value for Signal Conditioning verify that Linear Scaling is not selected.</p> </div> <p>Valid Entries</p> <p>Depends on your driver or server. Refer to your driver or server manual for more information.</p>
Process by Exception	<p>Enables exception-based processing for the tag.</p>



Field	Description
Scan Time	<p>Lets you specify how often the Scan, Alarm, and Control (SAC) program processes the tag and any tags (blocks) chained to it.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • 0 (one shot processing) • 0.05 to .95 in .05 increments (subsecond scan times) • 1 to 60 in 1 second increments • 1M to 60M in 1 minute increments • 1H to 24H in 1 hour increments <p>Example</p> <p>0.15 specifies a 15-subsecond scan time. 5 specifies a 5-second scan time, 10M specifies a 10-minute scan time, 16H specifies a 16-hour scan time.</p>
Phase At	<p>Lets you specify how long the Scan, Alarm, and Control (SAC) program delays in scanning the tag. When the tag has a second or subsecond scan time, SAC offsets the initial scan by the phase time when iFIX starts or when the database is reloaded. When the tag has a scan time of 1 minute or longer, SAC offsets the initial scan starting at midnight.</p> <p>Valid Entries</p> <p>Depends on the scan time. If the scan time is in hours, the phase must be in hours:minutes. If the scan time is in minutes, the phase must be in minutes:seconds. If the scan time is in seconds, the phase must be in seconds. If the scan time is in subseconds, the phase must be in subseconds.</p>

Limits and Scaling



Field	Description
Open Tag	<p>Lets you enter a descriptive label for the logical 0 value received by the tag. You can display this label in the iFIX WorkSpace through a Data link to aid operators in interpreting the value for the contact.</p> <p>Valid Entries</p> <p>A label of up to 16 characters.</p> <p>Examples</p> <p>Open, Off</p>
Close Tag	<p>Lets you enter a descriptive label for the logical 1 value received by the tag . You can display this label in the iFIX WorkSpace through a Data link to aid operators in interpreting the value for the contact.</p> <p>Valid Entries</p> <p>A label of up to 16 characters.</p> <p>Examples</p> <p>Close, On.</p>



Alarm Options

Field	Description
Alarm Areas	<p>Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>

Field	Description
<p>Enable Alarm</p>	<p>Lets you enable or disable alarming for this tag.</p> <p>When you enable alarming, the tag generates alarms allowing objects in your operator displays to show alarm conditions, and enabling other tags to detect alarms from the tag.</p> <div data-bbox="820 550 1416 861" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: The entire chain can be affected when you disable alarms for a tag. In addition, for both the Digital and Analog Alarm tags, this field is ignored when you enable the Alarm Suspend field.</p> </div>
<p>Priority</p>	<p>Lets you specify the alarm priority for a tag. If the priority is equal or greater than the SCADA node's alarm priority, iFIX sends the alarm to all the alarm destinations enabled for this node. However, if the priority is less than the SCADA node's alarm priority, the alarm is automatically acknowledged and filtered out so that it does not appear in your alarm destinations. However, the alarm does appear in Data links configured to display current and latched alarms.</p> <p>Valid Entries</p> <p>INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL</p> <div data-bbox="820 1545 1416 1808" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: To report tag alarms, the appropriate alarm areas must be assigned to each of the alarm services enabled in the System Configuration Utility (SCU).</p> </div>

Field	Description
Shelve Enable	Select this check box to enable Alarm Shelving for the tag.
Shelve Policy	Select an alarm shelving policy from the drop-down list.
Alarm Type	<p>Lets you specify the type of condition that generates an alarm from the tag. When an alarm occurs, it is sent to all locations specified in the Alarm Areas field.</p> <p>Valid Entries</p> <p>Open, Close, Change of State, None</p>
Contact Tag	<p>Lets you specify the name of the digital block that the Digital Alarm block closes when the alarm specified in the Alarm Type area occurs.</p> <p>Valid Entries</p> <p>A Digital Output or Digital Input block, in Manual mode.</p>
Contact Mode	<p>Lets you specify when to open the digital tag entered in the Contact Name field.</p> <p>Valid Entries</p> <p>Acknowledge, Return, All Clear, and Never</p>
Cont Contact Output	<p>Selecting this option enables the tags to attempt to write the contact with every scan, even if the value being written is unchanged. Otherwise, the DA tag only attempts to write to the defined contact tag when a value has changed and it needs to be written to the PLC. The write is a one-time attempt, so if it fails, the write will not be retried until the tag needs to write a new value.</p>

Field	Description
	<div data-bbox="834 275 1414 661" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;">  Note: There are four modes for the contacts - "Acknowledge", "Return", "All Clear", and "Never" - that control when the contact is cleared. Since the contact mode of "Never" does not reset the contact, the Continuous Output option is not supported for this contact mode. </div>
Remote Ack Tag	<p>Lets you specify the tag and field name pair to use for alarm acknowledgment from a remote site. When the tag and field's value changes from zero to a value greater than zero, the Digital Alarm tag acknowledges the alarm.</p> <p>Valid Entries</p> <p>Any floating point block and field name pair in the tag.field format.</p> <div data-bbox="834 1125 1414 1528" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;">  Note: When the Digital Alarm tag uses exception-based processing, acknowledging an alarm from an operator display immediately triggers processing of the block. Acknowledging the alarm with the Acknowledge Tag field does not trigger SAC to process the Digital Alarm tag. </div>
Alarm Suspension Tag	<p>Provides intelligent alarming by defining a tag and field name pair to control alarm processing for this tag. When the tag and field's value is zero, the Digital Alarm tag processes alarms. When the value is other than zero, either a positive or negative number, the Digital Alarm tag suspends alarms</p>

Field	Description
	<p>and generates a suspend message to the enabled alarm destinations.</p> <p>Valid Entries</p> <p>Any floating point tag and field name (F_CV) pair in the tag.field format.</p> <div data-bbox="821 569 1419 877" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note:</p> <p>If you specify the same block and field name pair for multiple Digital Alarm blocks, you can suspend alarms within one or more alarm areas. This is an optional feature.</p> </div>
<p>Delay Time</p>	<p>Lets you specify the amount of time the Digital Alarm tag waits before generating an alarm. If an alarm condition persists beyond the specified delay time, the tag generates the alarm.</p> <p>Valid Entries</p> <p>For time-based processing, use a time in days, hours, minutes, and seconds, in the format dd:hh:mm:ss, within the range 00:00:00:00 to 03:00:00:00.</p> <p>For exception-based processing, leave the default entry, 00:00:00:00. This disables any delay.</p> <div data-bbox="821 1503 1419 1682" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note:</p> <p>The value in the Delay Time field does not apply to Change of State (COS) alarms.</p> </div>
<p>Realarm Time</p>	<p>Lets you specify the time interval the Digital Alarm tag waits before re-issuing an alarm. If an alarm condition persists at the time specified, the tag</p>

Field	Description
	<p>re-issues the alarm. Any contact associated with each alarm type is closed.</p> <p>Valid Entries</p> <p>For time-based processing, use a time in days, hours, minutes, and seconds, in the format dd:hh:mm:ss, within the range 00:00:00:00 to 03:00:00:00.</p> <p>For exception-based processing, leave the default entry, 00:00:00:00. This disables any delay.</p>
<p>Suppress COMM Alarm</p>	<p>Select this option to separate the original alarm condition from the COMM alarm, and return the DA tag to the same state as it was prior to a COMM alarm. For example, if prior to the COMM alarm, the DA tag was an active alarm but already acknowledged, that is the state it should return to after communication is restored.</p> <p>Otherwise, DA tags handle one alarm at a time. As a result, it is possible that acknowledgement of a COMM alarm could cause the ACK bit in the PLC to be written, and the original alarm condition, if already acknowledged, could re-alarm.</p>
<p>As Event in Suspend</p>	<p>Select this option to enable the Event messaging (Suspend mode), which applies suppression behavior to disable alarm processing. When the tag is in suspend mode, the Alarm state is set to OK, the Alarm is an alarm message only and therefore, does not appear in the alarm summary. Alarm processing continues with each alarm state transition recorded in the alarm loggers but does not display in the alarm summary. The alarm state contact (tag) is not processed.</p>

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.
Collect	<p>Lets you select if the tag is set for collection by the Proficy Historian collector.</p> <p>Select Enabled to allow the tag to be collected by the collector.</p>
Collection Interval	<p>Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector.</p> <p>Valid Entries</p> <p>Must be entered in 100 ms intervals. The default value is 5000ms.</p> <p>Example</p> <p>1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.</p>
Collection Offset	<p>Used with the collection interval to schedule collection of data from a tag.</p> <p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p>

Field	Description
	If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.
Time Resolution	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Collector Deadband	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>

Field	Description
Compression Time-out (ms)	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p> <p>Any numeric value.</p>


E-Signature


Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if</p>

Field	Description
	this tag requires electronic signatures for data entry.
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>

Advanced Options

Field	Description
Enable Output	Lets you configure the tag to send output to the I/O driver, OPC server, or OPC UA server. The tag sends its output when it is in Automatic mode and converts its data according to the entries in the Low Limit (EGU), High Limit (EGU), and Signal Conditioning fields.
Invert Output	Inverts the output value so that if the value of the tag is 0, it outputs a 1. You can use this option to send a 0 to close a contact and send a 1 to open it.

Field	Description
Startup Mode	<p>Lets you select the tag's mode on startup. In Automatic mode, the tag receives data from the I/O driver, OPC server, or OPC UA server. In Manual mode, the tag receives data from the operator, scripts, recipes, or Program blocks.</p>
Initial Scan	<p>Lets you select whether the tag is initially placed on or off scan.</p> <p>Click On Scan to place the tag on scan as soon as the Scan, Alarm, and Control (SAC) program starts or when the database is loaded. Click Off Scan to place the tag on scan by a Program block, an Event Action tag, a script, an operator entry in a Data link, or an Easy Database Access program.</p>
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="821 1402 1419 1717" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
Previous Block	<p>Displays the name of the previous (upstream) tag.</p> <p>Valid Entries</p>

Field	Description
	None. This is a read-only field.
Next Block	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div data-bbox="820 485 1419 751" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: In a Statistical Data tag, the Next Block field specifies the tag name of the downstream Statistical Control tag. No other tag type is valid.</p> </div>
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>

DC Tag

This tag contains the following details:

General

Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <pre>~ ` + ^ : ? " * = { } . , ; ? @</pre> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p>

Field	Description
	A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

Programming Statements


Field	Description
Step 0 Command	<p>Displays the commands and arguments for each Device Control block. Use the Browse (...) button to select from a list of valid commands.</p> <p>Valid Entries</p> <p>The list box can include up to 12 programming statements each containing up to 34 alphanumeric characters.</p>
Step 1 Command	<p>Displays the commands and arguments for each Device Control block. Use the Browse (...) button to select from a list of valid commands.</p> <p>Valid Entries</p> <p>The list box can include up to 12 programming statements each containing up to 34 alphanumeric characters.</p>
Step 2 Command	<p>Displays the commands and arguments for each Device Control block. Use the Browse (...) button to select from a list of valid commands.</p> <p>Valid Entries</p>


Field	Description
	<p>The list box can include up to 12 programming statements each containing up to 34 alphanumeric characters.</p>
<p>Step 3 Command</p>	<p>Displays the commands and arguments for each Device Control block. Use the Browse (...) button to select from a list of valid commands.</p> <p>Valid Entries</p> <p>The list box can include up to 12 programming statements each containing up to 34 alphanumeric characters.</p>
<p>Step 4 Command</p>	<p>Displays the commands and arguments for each Device Control block. Use the Browse (...) button to select from a list of valid commands.</p> <p>Valid Entries</p> <p>The list box can include up to 12 programming statements each containing up to 34 alphanumeric characters.</p>
<p>Step 5 Command</p>	<p>Displays the commands and arguments for each Device Control block. Use the Browse (...) button to select from a list of valid commands.</p> <p>Valid Entries</p> <p>The list box can include up to 12 programming statements each containing up to 34 alphanumeric characters.</p>
<p>Step 6 Command</p>	<p>Displays the commands and arguments for each Device Control block. Use the Browse (...) button to select from a list of valid commands.</p> <p>Valid Entries</p>

Field	Description
	The list box can include up to 12 programming statements each containing up to 34 alphanumeric characters.
Step 7 Command	<p>Displays the commands and arguments for each Device Control block. Use the Browse (...) button to select from a list of valid commands.</p> <p>Valid Entries</p> <p>The list box can include up to 12 programming statements each containing up to 34 alphanumeric characters.</p>
Step 8 Command	<p>Displays the commands and arguments for each Device Control block. Use the Browse (...) button to select from a list of valid commands.</p> <p>Valid Entries</p> <p>The list box can include up to 12 programming statements each containing up to 34 alphanumeric characters.</p>
Step 9 Command	<p>Displays the commands and arguments for each Device Control block. Use the Browse (...) button to select from a list of valid commands.</p> <p>Valid Entries</p> <p>The list box can include up to 12 programming statements each containing up to 34 alphanumeric characters.</p>
Step 10 Command	<p>Displays the commands and arguments for each Device Control block. Use the Browse (...) button to select from a list of valid commands.</p> <p>Valid Entries</p>

Field	Description
	The list box can include up to 12 programming statements each containing up to 34 alphanumeric characters.


IO Addressing

Field	Description
Input Driver	<p>Lets you select an I/O driver, OPC server, or OPC UA server for the tag. The selected driver or server enables the tag to communicate with process hardware on the plant floor.</p> <p>Before you can select an I/O driver or OPC server, you must install it and add it to the available drivers in the SCU.</p>
Input Address 1 - 16	<p>Lets you specify the addresses of the digital input points that the Device Control block monitors.</p> <p>Valid Entries</p> <p>Up to 16 hardware input bits for input addresses. If necessary, consult your OPC, OPC UA, or I/O driver manual for more information on specifying I/O addresses.</p> <div data-bbox="820 1333 1421 1648" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note:</p> <p>All input addresses must have the same hardware options and all output addresses must have the same hardware options. However, the input and output hardware options do not need to be identical.</p> </div>
Input Hardware Options	<p>Lets you select any specific device control addressing format that the block uses to communicate with process hardware on the plant floor.</p> <p>Valid Entries</p>

Field	Description
	<p>For most process hardware, this field is usually left blank. Consult your I/O driver, OPC, or OPC UA manual for the applicable hardware code if necessary.</p>
<p>Output Driver</p>	<p>Lets you select an I/O driver, OPC UA, or OPC server for the tag. The selected driver or server enables the block to communicate with process hardware on the plant floor.</p> <p>Before you can select an I/O driver, OPCUA server, or OPC server, you must install it and add it to the available drivers in the SCU.</p>
<p>Output Address 1 - 8</p>	<p>Lets you specify the addresses of the digital output points that the Device Control block monitors.</p> <p>Valid Entries</p> <p>Up to 8 hardware output bits for output addresses. If necessary, consult your OPC, OPC UA, or I/O driver manual for more information on specifying I/O addresses.</p> <div data-bbox="820 1213 1419 1528" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: All input addresses must have the same hardware options and all output addresses must have the same hardware options. However, the input and output hardware options do not need to be identical.</p> </div>
<p>Output Hardware Options</p>	<p>Lets you select any specific device control addressing format that the tag uses to communicate with process hardware on the plant floor.</p> <p>Valid Entries</p> <p>For most process hardware, this field is usually left blank. Consult your I/O driver, OPC, or OPC UA</p>

Field	Description
	manual for the applicable hardware code if necessary.

Alarm Options

Field	Description
Alarm Areas	<p>Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>
Priority	<p>Lets you specify the alarm priority for a tag. If the priority is equal or greater than the SCADA node's alarm priority, iFIX sends the alarm to all the alarm destinations enabled for this node. However, if the priority is less than the SCADA node's alarm priority, the alarm is automatically acknowledged and filtered out so that it does not appear in your alarm destinations. However, the alarm does appear in Data links configured to display current and latched alarms.</p> <p>Valid Entries</p> <p>INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL</p> <div data-bbox="824 1587 1419 1850" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note:</p> <p>To report tag alarms, the appropriate alarm areas must be assigned to each of the alarm services enabled in the System Configuration Utility (SCU).</p> </div>

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.
Collect	<p>Lets you select if the tag is set for collection by the Proficy Historian collector.</p> <p>Select Enabled to allow the tag to be collected by the collector.</p>
Collection Interval	<p>Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector.</p> <p>Valid Entries</p> <p>Must be entered in 100 ms intervals. The default value is 5000ms.</p> <p>Example</p> <p>1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.</p>
Collection Offset	<p>Used with the collection interval to schedule collection of data from a tag.</p> <p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p>

Field	Description
	If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.
Time Resolution	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Collector Deadband	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>

Field	Description
Compression Time-out (ms)	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p> <p>Any numeric value.</p>


E-Signature


Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if</p>

Field	Description
	this tag requires electronic signatures for data entry.
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>

Advanced Options

Field	Description
Startup Mode	Lets you select the tag's mode on startup. In Automatic mode, the tag receives data from the I/O driver, OPC server, or OPC UA server. In Manual mode, the tag receives data from the operator, scripts, recipes, or Program blocks.
Initial Scan	<p>Lets you select whether the tag is initially placed on or off scan.</p> <p>Click On Scan to place the tag on scan as soon as the Scan, Alarm, and Control (SAC) program starts</p>

Field	Description
	<p>or when the database is loaded. Click Off Scan to place the tag on scan by a Program block, an Event Action tag, a script, an operator entry in a Data link, or an Easy Database Access program.</p>
Initial Value	<p>Controls the status of digital points on the hardware when the Scan, Alarm, and Control (SAC) program is first started.</p> <p>Valid Entries</p> <p>A valid contact pattern.</p> <p>Example</p> <p>A typical contact pattern entry in the Initial Value Field would look like the following example:</p> <p>OOCCXXXX</p> <p>This entry directs the digital points addressed in the 07 and 06 output Addresses fields to Open, the 05 and 04 fields to Close, and the 03 and 00 fields to remain in their present state.</p>
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="824 1709 1419 1858" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area.</p> </div>

Field	Description
	 This allows users to retrieve data from a specific security area even if they cannot write to that area.
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Process by Exception	Enables exception-based processing for the tag.
Scan Time	<p>Lets you specify how often the Scan, Alarm, and Control (SAC) program processes the block and any tags chained to it.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • 0 (one shot processing) • 0.05 to .95 in .05 increments (subsecond scan times) • 1 to 60 in 1 second increments • 1M to 60M in 1 minute increments • 1H to 24H in 1 hour increments <p>Example</p>

Field	Description
	0.15 specifies a 15-subsecond scan time. 5 specifies a 5-second scan time, 10M specifies a 10-minute scan time, 16H specifies a 16-hour scan time.
Phase At	<p>Lets you specify how long the Scan, Alarm, and Control (SAC) program delays in scanning the tag. When the tag has a second or subsecond scan time, SAC offsets the initial scan by the phase time when iFIX starts or when the database is reloaded. When the tag has a scan time of 1 minute or longer, SAC offsets the initial scan starting at midnight.</p> <p>Valid Entries</p> <p>Depends on the scan time. If the scan time is in hours, the phase must be in hours:minutes. If the scan time is in minutes, the phase must be in minutes:seconds. If the scan time is in seconds, the phase must be in seconds. If the scan time is in subseconds, the phase must be in subseconds.</p>

DI Tag



This tag contains the following details:



General

Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p>

Field	Description
	<p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <p>~ ` + ^ : ? " * = { } . , ; ? @</p> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	<p>The tag type. Display-only field.</p>
Current Value	<p>The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.</p>

I/O Addressing

Field	Description
I/O Driver	<p>Lets you select an I/O driver, OPC server, or OPC UA server for the tag. The selected driver or server enables the tag to communicate with process hardware on the plant floor.</p> <p>Before you can select an I/O driver, OPC server, or OPC UA server you must install it and add it to the available ones in the SCU.</p>
I/O Address	<p>Lets you enter the location in the process hardware where data for this tag is saved and where output is sent.</p> <p>Valid Entries</p> <p>Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations.</p> <div data-bbox="820 1096 1419 1409" style="border: 1px solid black; border-radius: 10px; padding: 10px; background-color: #fff9c4;"> <p> CAUTION: Do not assign the same I/O address to tags when using exception-based and time-based processing. Doing so will cause the exception-based tags to occasionally miss a value.</p> </div> <div data-bbox="820 1438 1419 1885" style="border: 1px solid black; border-radius: 10px; padding: 10px; background-color: #fff9c4;"> <p> CAUTION: Configuration Hub currently does not do I/O address validations before publish. If you enter an invalid IO address into a tag or generate an invalid I/O address via the model and substitutions, the publish may fail to set the IO address into the active database, and your invalid IO address will be removed.</p> </div>

Field	Description
Signal Conditioning	<p>Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p> <div data-bbox="821 432 1419 699" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Signal conditioning and linear scaling cannot be applied simultaneously. If you select a value for Signal Conditioning verify that Linear Scaling is not selected.</p> </div> <p>Valid Entries</p> <p>Depends on your driver or server. Refer to your driver or server manual for more information.</p>
H/W Options	<p>Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p> <div data-bbox="821 1066 1419 1333" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Signal conditioning and linear scaling cannot be applied simultaneously. If you select a value for Signal Conditioning verify that Linear Scaling is not selected.</p> </div> <p>Valid Entries</p> <p>Depends on your driver or server. Refer to your driver or server manual for more information.</p>
Process by Exception	<p>Enables exception-based processing for the tag.</p>
Scan Time	<p>Lets you specify how often the Scan, Alarm, and Control (SAC) program processes the tag and any tags (blocks) chained to it.</p> <p>Valid Entries</p>

Field	Description
	<ul style="list-style-type: none"> • 0 (one shot processing) • 0.05 to .95 in .05 increments (subsecond scan times) • 1 to 60 in 1 second increments • 1M to 60M in 1 minute increments • 1H to 24H in 1 hour increments <p>Example</p> <p>0.15 specifies a 15-subsecond scan time. 5 specifies a 5-second scan time, 10M specifies a 10-minute scan time, 16H specifies a 16-hour scan time.</p>
Phase At	<p>Lets you specify how long the Scan, Alarm, and Control (SAC) program delays in scanning the tag. When the tag has a second or subsecond scan time, SAC offsets the initial scan by the phase time when iFIX starts or when the database is reloaded. When the tag has a scan time of 1 minute or longer, SAC offsets the initial scan starting at midnight.</p> <p>Valid Entries</p> <p>Depends on the scan time. If the scan time is in hours, the phase must be in hours:minutes. If the scan time is in minutes, the phase must be in minutes:seconds. If the scan time is in seconds, the phase must be in seconds. If the scan time is in subseconds, the phase must be in subseconds.</p>



Limits and Scaling


Field	Description
Open Tag	Lets you enter a descriptive label for the logical 0 value received by the tag. You can display this label

Field	Description
	<p>in the iFIX WorkSpace through a Data link to aid operators in interpreting the value for the contact.</p> <p>Valid Entries</p> <p>A label of up to 16 characters.</p> <p>Examples</p> <p>Open, Off</p>
Close Tag	<p>Lets you enter a descriptive label for the logical 1 value received by the tag. You can display this label in the iFIX WorkSpace through a Data link to aid operators in interpreting the value for the contact.</p> <p>Valid Entries</p> <p>A label of up to 16 characters.</p> <p>Examples</p> <p>Close, On.</p>

Alarm Options

Field	Description
Alarm Areas	<p>Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>
Enable Alarm	<p>Lets you enable or disable alarming for this tag.</p> <p>When you enable alarming, the tag generates alarms allowing objects in your operator displays</p>

Field	Description
	<p>to show alarm conditions, and enabling other tags to detect alarms from the tag.</p> <div data-bbox="824 380 1419 688" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: The entire chain can be affected when you disable alarms for a tag. In addition, for both the Digital and Analog Alarm tags, this field is ignored when you enable the Alarm Suspend field.</p> </div>
Enable Event	<p>Lets you enable or disable event messaging for the tag. Event messaging is similar to alarming except that it does not require acknowledgment. Event messages are sent to the same alarm destinations as alarms for a given tag but do not appear in the Alarm Summary object.</p> <p>Analog Output, Analog Register, Digital Output, Digital Register, Digital Input, and Text blocks have event messaging capabilities.</p> <div data-bbox="824 1167 1419 1570" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Be careful when using event messaging in a chain with a time-based scan time. If the scan time is short, your alarm files (either disk or printed) can grow very large. We recommend enabling event messaging for exception-based chains, one shot chains, and stand-alone output blocks.</p> </div>
Priority	<p>Lets you specify the alarm priority for a tag. If the priority is equal or greater than the SCADA node's alarm priority, iFIX sends the alarm to all the alarm destinations enabled for this node. However, if the priority is less than the SCADA node's alarm priority, the alarm is automatically acknowledged</p>

Field	Description
	<p>and filtered out so that it does not appear in your alarm destinations. However, the alarm does appear in Data links configured to display current and latched alarms.</p> <p>Valid Entries</p> <p>INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL</p> <div data-bbox="821 655 1419 926" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: To report tag alarms, the appropriate alarm areas must be assigned to each of the alarm services enabled in the System Configuration Utility (SCU).</p> </div>
Alarm Type	<p>Lets you specify the type of condition that generates an alarm from the tag. When an alarm occurs, it is sent to all locations specified in the Alarm Areas field.</p> <p>Valid Entries</p> <p>Open, Close, Change of State, None</p>
Shelve Enable	<p>Select this check box to enable Alarm Shelving for the tag.</p>
Shelve Policy	<p>Select an alarm shelving policy from the drop-down list.</p>

Historian

Field	Description
Tag Description	<p>Lets you enter the tag description that is used by Historian when the tag is collected.</p>
Collect	<p>Lets you select if the tag is set for collection by the Proficy Historian collector.</p>

Field	Description
	Select Enabled to allow the tag to be collected by the collector.
Collection Interval	<p>Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector.</p> <p>Valid Entries</p> <p>Must be entered in 100 ms intervals. The default value is 5000ms.</p> <p>Example</p> <p>1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.</p>
Collection Offset	<p>Used with the collection interval to schedule collection of data from a tag.</p> <p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p> <p>If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.</p>
Time Resolution	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>

Field	Description
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Collector Deadband	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>
Compression Time-out (ms)	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p>

Field	Description
	<p>Valid Entries</p> <p>Any numeric value.</p>



E-Signature

Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>

Field	Description
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>

Advanced Options

Field	Description
Enable Output	<p>Lets you configure the tag to send output to the I/O driver, OPC server, or OPC UA server. The tag sends its output when it is in Automatic mode and converts its data according to the entries in the Low Limit (EGU), High Limit (EGU), and Signal Conditioning fields.</p>
Invert Output	<p>Inverts the output value so that if the value of the tag is 0, it outputs a 1. You can use this option to send a 0 to close a contact and send a 1 to open it.</p>
Startup Mode	<p>Lets you select the tag's mode on startup. In Automatic mode, the tag receives data from the I/O driver, OPC server, or OPC UA server. In Manual mode, the tag receives data from the operator, scripts, recipes, or Program blocks.</p>
Initial Scan	<p>Lets you select whether the tag is initially placed on or off scan.</p> <p>Click On Scan to place the tag on scan as soon as the Scan, Alarm, and Control (SAC) program starts or when the database is loaded. Click Off Scan to</p>

Field	Description
	place the tag on scan by a Program block, an Event Action tag, a script, an operator entry in a Data link, or an Easy Database Access program.
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="820 898 1421 1213" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
Previous Block	<p>Displays the name of the previous (upstream) tag.</p> <p>Valid Entries</p> <p>None. This is a read-only field.</p>
Next Block	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div data-bbox="820 1600 1421 1871" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: In a Statistical Data tag, the Next Block field specifies the tag name of the downstream Statistical Control tag. No other tag type is valid.</p> </div>

Field	Description
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>

DO Tag



This tag contains the following details:


General

Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain spe-</p>

Field	Description
	<p>cial characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <p>~ ` + ^ : ? " * = { } . , ; ? @</p> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

I/O Addressing

Field	Description
I/O Driver	<p>Lets you select an I/O driver, OPC server, or OPC UA server for the tag. The selected driver or server enables the tag to communicate with process hardware on the plant floor.</p> <p>Before you can select an I/O driver, OPC server, or OPC UA server you must install it and add it to the available ones in the SCU.</p>
I/O Address	<p>Lets you enter the location in the process hardware where data for this tag is saved and where output is sent.</p> <p>Valid Entries</p> <p>Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations.</p> <div data-bbox="821 1098 1419 1409" style="border: 1px solid black; border-radius: 10px; padding: 10px; background-color: #fff9c4;"> <p> CAUTION: Do not assign the same I/O address to tags when using exception-based and time-based processing. Doing so will cause the exception-based tags to occasionally miss a value.</p> </div> <div data-bbox="821 1440 1419 1879" style="border: 1px solid black; border-radius: 10px; padding: 10px; background-color: #fff9c4;"> <p> CAUTION: Configuration Hub currently does not do I/O address validations before publish. If you enter an invalid IO address into a tag or generate an invalid I/O address via the model and substitutions, the publish may fail to set the IO address into the active database, and your invalid IO address will be removed.</p> </div>


Field	Description
H/W Options	<p>Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p> <div data-bbox="821 432 1417 699" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Signal conditioning and linear scaling cannot be applied simultaneously. If you select a value for Signal Conditioning verify that Linear Scaling is not selected.</p> </div> <p>Valid Entries</p> <p>Depends on your driver or server. Refer to your driver or server manual for more information.</p>

Limits and Scaling

Field	Description
Open Tag	<p>Lets you enter a descriptive label for the logical 0 value received by the tag. You can display this label in the iFIX WorkSpace through a Data link to aid operators in interpreting the value for the contact.</p> <p>Valid Entries</p> <p>A label of up to 16 characters.</p> <p>Examples</p> <p>Open, Off</p>
Close Tag	<p>Lets you enter a descriptive label for the logical 1 value received by the tag. You can display this label in the iFIX WorkSpace through a Data link to aid operators in interpreting the value for the contact.</p> <p>Valid Entries</p> <p>A label of up to 16 characters.</p>

Field	Description
	<p>Examples</p> <p>Close, On.</p>

Alarm Options

Field	Description
Alarm Areas	<p>Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>
Enable Event	<p>Lets you enable or disable event messaging for the tag. Event messaging is similar to alarming except that it does not require acknowledgment. Event messages are sent to the same alarm destinations as alarms for a given tag but do not appear in the Alarm Summary object.</p> <p>Analog Output, Analog Register, Digital Output, Digital Register, Digital Input, and Text tags have event messaging capabilities.</p> <div data-bbox="820 1409 1419 1812" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note:</p> <p>Be careful when using event messaging in a chain with a time-based scan time. If the scan time is short, your alarm files (either disk or printed) can grow very large. We recommend enabling event messaging for exception-based chains, one shot chains, and stand-alone output blocks.</p> </div>

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.
Collect	<p>Lets you select if the tag is set for collection by the Proficy Historian collector.</p> <p>Select Enabled to allow the tag to be collected by the collector.</p>
Collection Interval	<p>Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector.</p> <p>Valid Entries</p> <p>Must be entered in 100 ms intervals. The default value is 5000ms.</p> <p>Example</p> <p>1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.</p>
Collection Offset	<p>Used with the collection interval to schedule collection of data from a tag.</p> <p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p>

Field	Description
	If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.
Time Resolution	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Collector Deadband	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>

Field	Description
Compression Time-out (ms)	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p> <p>Any numeric value.</p>



E-Signature


Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if</p>

Field	Description
	this tag requires electronic signatures for data entry.
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>

Advanced Options

Field	Description
Invert Output	Inverts the output value so that if the value of the tag is 0, it outputs a 1. You can use this option to send a 0 to close a contact and send a 1 to open it.
Write if Different	Writes a value only if it is different than the current value.
Initial Value	Lets you specify the value that is sent to the process hardware the first time the Scan, Alarm, and Control (SAC) program processes the tag. If an

Field	Description
	<p>Initial Value is not defined, SAC does not output a value during initialization.</p> <p>Valid Entries</p> <p>A value between the Low and High Limit (EGU) fields.</p>
<p>Security Areas</p>	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="821 1045 1419 1356" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
<p>Previous Block</p>	<p>Displays the name of the previous (upstream) tag.</p> <p>Valid Entries</p> <p>None. This is a read-only field.</p>
<p>Next Block</p>	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div data-bbox="821 1745 1419 1894" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: In a Statistical Data tag, the Next Block field specifies the tag name of the down-</p> </div>

Field	Description
	 stream Statistical Control tag. No other tag type is valid.
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>

DR Tag



This tag contains the following details:


General

Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p>

Field	Description
	<p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <pre>~ ` + ^ : ? " * = { } . , ; ? @</pre> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

I/O Addressing

Field	Description
I/O Driver	<p>Lets you select an I/O driver, OPC server, or OPC UA server for the tag. The selected driver or server enables the tag to communicate with process hardware on the plant floor.</p> <p>Before you can select an I/O driver, OPC server, or OPC UA server you must install it and add it to the available ones in the SCU.</p>
I/O Address	<p>Lets you enter the location in the process hardware where data for this tag is saved and where output is sent.</p> <p>Valid Entries</p> <p>Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations.</p> <div data-bbox="820 1094 1419 1404" style="border: 1px solid black; border-radius: 10px; padding: 10px; background-color: #fff9c4;"> <p> CAUTION: Do not assign the same I/O address to tags when using exception-based and time-based processing. Doing so will cause the exception-based tags to occasionally miss a value.</p> </div> <div data-bbox="820 1436 1419 1879" style="border: 1px solid black; border-radius: 10px; padding: 10px; background-color: #fff9c4;"> <p> CAUTION: Configuration Hub currently does not do I/O address validations before publish. If you enter an invalid IO address into a tag or generate an invalid I/O address via the model and substitutions, the publish may fail to set the IO address into the active database, and your invalid IO address will be removed.</p> </div>

Field	Description
H/W Options	<p>Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p> <div data-bbox="824 436 1419 699" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Signal conditioning and linear scaling cannot be applied simultaneously. If you select a value for Signal Conditioning verify that Linear Scaling is not selected.</p> </div> <p>Valid Entries</p> <p>Depends on your driver or server. Refer to your driver or server manual for more information.</p>

Limits and Scaling

Field	Description
Open Tag	<p>Lets you enter a descriptive label for the logical 0 value received by the tag. You can display this label in the iFIX WorkSpace through a Data link to aid operators in interpreting the value for the contact.</p> <p>Valid Entries</p> <p>A label of up to 16 characters.</p> <p>Examples</p> <p>Open, Off</p>
Close Tag	<p>Lets you enter a descriptive label for the logical 1 value received by the tag. You can display this label in the iFIX WorkSpace through a Data link to aid operators in interpreting the value for the contact.</p> <p>Valid Entries</p> <p>A label of up to 16 characters.</p>

Field	Description
	<p>Examples</p> <p>Close, On.</p>

Alarm Options

Field	Description
Alarm Areas	<p>Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>

Historian

Field	Description
Tag Description	<p>Lets you enter the tag description that is used by Historian when the tag is collected.</p>
Collect	<p>Lets you select if the tag is set for collection by the Proficy Historian collector.</p> <p>Select Enabled to allow the tag to be collected by the collector.</p>
Collection Interval	<p>Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector.</p> <p>Valid Entries</p> <p>Must be entered in 100 ms intervals. The default value is 5000ms.</p> <p>Example</p>

Field	Description
	1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.
Collection Offset	<p>Used with the collection interval to schedule collection of data from a tag.</p> <p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p> <p>If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.</p>
Time Resolution	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Collector Deadband	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values</p>

Field	Description
	<p>that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>
Compression Time-out (ms)	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p> <p>Any numeric value.</p>


E-Signature



Field	Description
Type	The Type of Electronic Signature:


Field	Description
	<ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electron-</p>

Field	Description
	ic Signature settings are available. By default, this check box is disabled.

Advanced Options

Field	Description
Enable Output	<p>Lets you configure the tag to send output to the I/O driver, OPC server, or OPC UA server. The tag sends its output when it is in Automatic mode and converts its data according to the entries in the Low Limit (EGU), High Limit (EGU), and Signal Conditioning fields.</p>
Invert Output	<p>Inverts the output value so that if the value of the tag is 0, it outputs a 1. You can use this option to send a 0 to close a contact and send a 1 to open it.</p>
Enable Event	<p>Lets you enable or disable event messaging for the tag. Event messaging is similar to alarming except that it does not require acknowledgment. Event messages are sent to the same alarm destinations as alarms for a given tag but do not appear in the Alarm Summary object.</p> <p>Analog Output, Analog Register, Digital Output, Digital Register, Digital Input, and Text blocks have event messaging capabilities.</p> <div data-bbox="820 1438 1421 1833" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Be careful when using event messaging in a chain with a time-based scan time. If the scan time is short, your alarm files (either disk or printed) can grow very large. We recommend enabling event messaging for exception-based chains, one shot chains, and stand-alone output tags.</p> </div>

Field	Description
IO Address Type	<p>Lets you enter the base number system used by the I/O Address field.</p> <p>Valid Entries</p> <p>Decimal, Hexadecimal, or Octal.</p>
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="821 1005 1419 1318" style="border: 1px solid #00a0c0; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
Previous Block	<p>Displays the name of the previous (upstream) tag.</p> <p>Valid Entries</p> <p>None. This is a read-only field.</p>
Next Block	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div data-bbox="821 1705 1419 1856" style="border: 1px solid #00a0c0; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p> Note: In a Statistical Data tag, the Next Block field specifies the tag name of the down-</p> </div>

Field	Description
	 stream Statistical Control tag. No other tag type is valid.
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>

DR2 Tag



This tag contains the following details:


General

Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p>

Field	Description
	<p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <p>~ ` + ^ : ? " * = { } . , ; ? @</p> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

I/O Addressing

Field	Description
I/O Driver	<p>Lets you select an I/O driver, OPC server, or OPC UA server for the tag. The selected driver or server enables the tag to communicate with process hardware on the plant floor.</p> <p>Before you can select an I/O driver, OPC server, or OPC UA server you must install it and add it to the available ones in the SCU.</p>
I/O Address	<p>Lets you enter the location in the process hardware where data for this tag is saved and where output is sent.</p> <p>Valid Entries</p> <p>Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations.</p> <div data-bbox="820 1096 1419 1409" style="border: 1px solid black; border-radius: 10px; padding: 10px; background-color: #fff9c4;"> <p> CAUTION: Do not assign the same I/O address to tags when using exception-based and time-based processing. Doing so will cause the exception-based tags to occasionally miss a value.</p> </div> <div data-bbox="820 1438 1419 1879" style="border: 1px solid black; border-radius: 10px; padding: 10px; background-color: #fff9c4;"> <p> CAUTION: Configuration Hub currently does not do I/O address validations before publish. If you enter an invalid IO address into a tag or generate an invalid I/O address via the model and substitutions, the publish may fail to set the IO address into the active database, and your invalid IO address will be removed.</p> </div>

Field	Description
H/W Options	<p>Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p> <div data-bbox="824 432 1414 699" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Signal conditioning and linear scaling cannot be applied simultaneously. If you select a value for Signal Conditioning verify that Linear Scaling is not selected.</p> </div> <p>Valid Entries</p> <p>Depends on your driver or server. Refer to your driver or server manual for more information.</p>

Limits and Scaling

Field	Description
Open Tag	<p>Lets you enter a descriptive label for the logical 0 value received by the tag. You can display this label in the iFIX WorkSpace through a Data link to aid operators in interpreting the value for the contact.</p> <p>Valid Entries</p> <p>A label of up to 16 characters.</p> <p>Examples</p> <p>Open, Off</p>
Close Tag	<p>Lets you enter a descriptive label for the logical 1 value received by the tag. You can display this label in the iFIX WorkSpace through a Data link to aid operators in interpreting the value for the contact.</p> <p>Valid Entries</p> <p>A label of up to 16 characters.</p>

Field	Description
	<p>Examples</p> <p>Close, On.</p>



E-Signature

Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electron-</p>

Field	Description
	ic Signature settings are available. By default, this check box is disabled.
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>

Advanced Options

Field	Description
Enable Output	Lets you configure the tag to send output to the I/O driver, OPC server, or OPC UA server. The tag sends its output when it is in Automatic mode and converts its data according to the entries in the Low Limit (EGU), High Limit (EGU), and Signal Conditioning fields.
Invert Output	Inverts the output value so that if the value of the tag is 0, it outputs a 1. You can use this option to send a 0 to close a contact and send a 1 to open it.
Enable Event	<p>Lets you enable or disable event messaging for the tag. Event messaging is similar to alarming except that it does not require acknowledgment. Event messages are sent to the same alarm destinations as alarms for a given block but do not appear in the Alarm Summary object.</p> <p>Analog Output, Analog Register, Digital Output, Digital Register, Digital Input, and Text blocks have event messaging capabilities.</p>

Field	Description
	<div data-bbox="820 268 1421 665" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;">  Note: Be careful when using event messaging in a chain with a time-based scan time. If the scan time is short, your alarm files (either disk or printed) can grow very large. We recommend enabling event messaging for exception-based chains, one shot chains, and stand-alone output blocks. </div>
I/O Address Type	Lets you enter the base number system used by the I/O Address field. Valid entries include: Decimal, Hexadecimal, or Octal.
Security Areas	Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area. <p>Valid Entries</p> One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. <div data-bbox="820 1325 1421 1633" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;">  Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area. </div>
Alarm Field 1	Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.

Field	Description
	<p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>

DT Tag

This tag contains the following details:


General



Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points</p>


Field	Description
	<p>(!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <pre>~ ` + ^ : ? " * = { } . , ; ? @</pre> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	<p>The tag type. Display-only field.</p>
Current Value	<p>The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.</p>

Limits and Scaling

Field	Description
Low Limit	<p>Lets you enter the tag's minimum value.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999.

Field	Description
	<ul style="list-style-type: none"> • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;">  Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. </div> <p>In a Calculation or Signal Select tag, if the output of the tag is 10 and the Low Limit is 15, the tag clamps the value at 15. You must enter a Low Limit of 10 or less to output a value of 10.</p> <p>If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the Low Limit field.</p> <p>If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
High Limit	<p>Lets you enter the tag's maximum value.</p> <p>Valid Entries</p> <p>You can enter a high limit in one of three formats:</p> <ul style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38.

Field	Description
	<ul style="list-style-type: none"> Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div data-bbox="821 478 1419 743" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;">  Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. </div> <p>In a Calculation or a Signal Select tag, if the output of the tag is 150 and the High Limit is 100, the tag clamps the value at 100. You must enter a High Limit of 150 or more to output a value of 150.</p> <p>If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the High Limit field.</p> <p>If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
Units	<p>Lets you enter text describing the engineering units range.</p> <p>Valid Entries</p> <p>Up to 33 characters.</p> <p>Example</p> <p>Kilograms per square meter, Liters per minute, degrees Celsius,</p> <div data-bbox="821 1745 1419 1892" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;">  Note: This entry does not affect the calculation or function of any variables in iFIX. It is </div>

Field	Description
	 used strictly as a display label to identify the engineering units.

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.
Collect	<p>Lets you select if the tag is set for collection by the Proficy Historian collector.</p> <p>Select Enabled to allow the tag to be collected by the collector.</p>
Collection Interval	<p>Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector.</p> <p>Valid Entries</p> <p>Must be entered in 100 ms intervals. The default value is 5000ms.</p> <p>Example</p> <p>1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.</p>
Collection Offset	<p>Used with the collection interval to schedule collection of data from a tag.</p> <p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p>

Field	Description
	<p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p> <p>If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.</p>
Time Resolution	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Collector Deadband	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p>

Field	Description
	Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.
Compression Time-out (ms)	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p> <p>Any numeric value.</p>


E-Signature


Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person perform-</p>

Field	Description
	ing an action and does not affect the person verifying an action.
Exempt Alarm Ack	Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>

Advanced Options

Field	Description
Dead Time	<p>Lets you specify the length of the delay in seconds before transferring the value of upstream tag to the next tag in the chain.</p> <p>Valid Entries</p>

Field	Description
	<p>A value from 1 to 59 * scan_time, up to a maximum of 255 seconds, where scan_time is the scan time of the upstream block.</p> <p>Examples</p> <p>Assume you have an Analog Input tag chained to a Dead Time tag. If the Analog Input's scan time is 2 seconds, you can enter a dead time from 1 to 118 seconds.</p> <p>You can lengthen the dead time by either changing the scan time of the upstream block or by chaining multiple Dead Time blocks together. For example, using the previous example, if you change the scan time of the Analog Input block to 10 seconds, you can enter a dead time from 1 to 255 seconds.</p>
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="820 1480 1421 1785" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
Previous Block	Displays the name of the previous (upstream) tag.

Field	Description
	<p>Valid Entries</p> <p>None. This is a read-only field.</p>
Next Block	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div data-bbox="821 558 1419 827" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: In a Statistical Data tag, the Next Block field specifies the tag name of the downstream Statistical Control tag. No other tag type is valid.</p> </div>
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>

ETR Tag


This tag contains the following details:


General


Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <pre>~ ` + ^ : ? " * = { } . , ; ? @</pre> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p>

Field	Description
	A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

Limits and Scaling

Field	Description
Low Limit	<p>Lets you enter the tag's minimum value.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information.</p> </div> <p>In a Calculation or Signal Select tag, if the output of the tag is 10 and the Low Limit is 15, the tag</p>

Field	Description
	<p>clamps the value at 15. You must enter a Low Limit of 10 or less to output a value of 10.</p> <p>If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the Low Limit field.</p> <p>If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
<p>High Limit</p>	<p>Lets you enter the tag's maximum value.</p> <p>Valid Entries</p> <p>You can enter a high limit in one of three formats:</p> <ul style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information.</p> </div> <p>In a Calculation or a Signal Select tag, if the output of the tag is 150 and the High Limit is 100, the tag clamps the value at 100. You must enter a High Limit of 150 or more to output a value of 150.</p>

Field	Description
	<p>If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the High Limit field.</p> <p>If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
Units	<p>Lets you enter text describing the engineering units range.</p> <p>Valid Entries</p> <p>Up to 33 characters.</p> <p>Example</p> <p>Kilograms per square meter, Liters per minute, degrees Celsius,</p> <div data-bbox="820 1024 1421 1289" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: This entry does not affect the calculation or function of any variables in iFIX. It is used strictly as a display label to identify the engineering units.</p> </div>

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.
Collect	<p>Lets you select if the tag is set for collection by the Proficy Historian collector.</p> <p>Select Enabled to allow the tag to be collected by the collector.</p>

Field	Description
Collection Interval	<p>Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector.</p> <p>Valid Entries</p> <p>Must be entered in 100 ms intervals. The default value is 5000ms.</p> <p>Example</p> <p>1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.</p>
Collection Offset	<p>Used with the collection interval to schedule collection of data from a tag.</p> <p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p> <p>If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.</p>
Time Resolution	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incom-</p>

Field	Description
	<p>ing data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Collector Deadband	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>
Compression Time-out (ms)	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p>


Field	Description
	Any numeric value.


E-Signature



Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electron-</p>

Field	Description
	ic Signature settings are available. By default, this check box is disabled.
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>

Advanced Options

Field	Description
Buffer Clear Status	<p>Lets you clear the block's data buffers every time the block is put on scan.</p> <p>Valid Entries</p> <p>Select the check box to clear data buffers. Clear it to suppress this feature.</p>
Input Tag	<p>Lets you specify the name of the tag and field that the Extended Trend tag stores. If this field is left blank, the Extended Trend block stores the value passed by the upstream block.</p> <p>Valid Entries</p> <p>A block and field name pair in the tag.field (F_CV) format.</p> <div data-bbox="824 1612 1416 1831" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: To chain Extended Trend blocks, enter the Extended Trend tag's name and the field F_INP.</p> </div>

Field	Description
Compression Factor	<p>Lets you specify the amount of data stored in the trend history by collecting the number of samples entered in the field, averaging them, and storing up to 600 averages in the trend history.</p> <p>Valid Entries</p> <p>A value from 1 - 255 that represents the number of samples to collect.</p> <p>Example</p> <p>If you have a scan time of 10 seconds and enter 5 as the Average Compress, the Extended Trend tag creates a trend history of 600 averages of 5 samples. In essence, the tag now represents a trend history of 3000 scan periods (5 x 600), or 500 minutes (30,000 seconds).</p> <div data-bbox="820 1033 1416 1255" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Using this field does not affect or delay the value passed by the Next tag field to the downstream tag.</p> </div>
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p>

Field	Description
	<div data-bbox="820 268 1421 575" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;">  Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area. </div>
Previous Block	Displays the name of the previous (upstream) tag. Valid Entries None. This is a read-only field.
Next Block	Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button. <div data-bbox="820 961 1421 1228" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;">  Note: In a Statistical Data tag, the Next Block field specifies the tag name of the downstream Statistical Control tag. No other tag type is valid. </div>
Alarm Field 1	Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information. Valid Entries Text, up to 80 characters.
Alarm Field 2	Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.

Field	Description
	<p>Valid Entries</p> <p>Text, up to 80 characters.</p>

EV Tag


This tag contains the following details:



General



Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p>



Field	Description
	<p>~ ` + ^ : ? " * = { } . , ; ? @</p> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.


Event Definitions

Field	Description
If Condition 1	<p>Lets you control the execution of the THEN or ELSE operation based upon a test expression on the previous tag. If the previous tag satisfies the conditions for a logical TRUE, the THEN operation is executed; otherwise, the ELSE operation is executed.</p> <div data-bbox="824 1486 1421 1755" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note:</p> <p>The command is latched. This means that the tag remembers the last operation and only performs a new operation if the condition has changed.</p> </div> <p>Valid Entries</p> <p>An expression in the following format:</p>

Field	Description
	<p>Value or Alarm operator condition</p> <p>Example</p> <p>Value = 83.2</p> <div data-bbox="824 478 1414 789" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note:</p> <p>You can use either one VALUE or one ALARM in each IF field. When entering your IF statement, leave a space between the VALUE/ALARM, the operator, and the condition entries.</p> </div>
Then	<p>Lets you specify the operation that occurs when the test expression in the IF field is TRUE. This operation executes only if the condition has changed.</p> <p>Valid Entries</p> <p>An expression in the following format:</p> <p>command tag</p> <p>Example</p> <p>RUN PROG1</p> <div data-bbox="824 1329 1414 1686" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note:</p> <p>You must enter the name of an existing tag. iFIX does not notify you that the specified tag does not exist until the Event Action block goes on scan. If you specify a nonexistent tag, an alarm is sent to all of the node's active alarm destinations.</p> </div>
Else	<p>Lets you specify the operation that occurs when the test expression in the IF field is FALSE. This operation executes only if the condition has changed.</p>

Field	Description
	<p>Valid Entries</p> <p>An expression in the following format:</p> <p>command tag</p> <p>Example</p> <p>CLOSE D03</p> <div data-bbox="821 621 1419 978" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note:</p> <p>You must enter the name of an existing tag. iFIX does not notify you that the specified tag does not exist until the Event Action block goes on scan. If you specify a nonexistent tag, an alarm is sent to all of the node's active alarm destinations.</p> </div>
<p>If Condition 2</p>	<p>Lets you control the execution of the THEN or ELSE operation based upon a test expression on the previous tag. If the previous block satisfies the conditions for a logical TRUE, the THEN operation is executed; otherwise, the ELSE operation is executed.</p> <div data-bbox="821 1251 1419 1516" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note:</p> <p>The command is latched. This means that the tag remembers the last operation and only performs a new operation if the condition has changed.</p> </div> <p>Valid Entries</p> <p>An expression in the following format:</p> <p>Value or Alarm operator condition</p> <p>Example</p> <p>Value = 83.2</p>

Field	Description
	<div data-bbox="834 275 1421 571" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;">  Note: You can use either one VALUE or one ALARM in each IF field. When entering your IF statement, leave a space between the VALUE/ALARM, the operator, and the condition entries. </div>
Then	<p>Lets you specify the operation that occurs when the test expression in the IF field is TRUE. This operation executes only if the condition has changed.</p> <p>Valid Entries</p> <p>An expression in the following format:</p> <p>command tag</p> <p>Example</p> <p>RUN PROG1</p> <div data-bbox="834 1115 1421 1465" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;">  Note: You must enter the name of an existing tag. iFIX does not notify you that the specified block does not exist until the Event Action block goes on scan. If you specify a nonexistent block, an alarm is sent to all of the node's active alarm destinations. </div>
Else	<p>Lets you specify the operation that occurs when the test expression in the IF field is FALSE. This operation executes only if the condition has changed.</p> <p>Valid Entries</p> <p>An expression in the following format:</p> <p>command tag</p>

Field	Description
	<p>Example</p> <p>CLOSE D03</p> <div data-bbox="821 405 1419 760" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note:</p> <p>You must enter the name of an existing tag. iFIX does not notify you that the specified tag does not exist until the Event Action block goes on scan. If you specify a nonexistent tag, an alarm is sent to all of the node's active alarm destinations.</p> </div>

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.
Collect	<p>Lets you select if the tag is set for collection by the Proficy Historian collector.</p> <p>Select Enabled to allow the tag to be collected by the collector.</p>
Collection Interval	<p>Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector.</p> <p>Valid Entries</p> <p>Must be entered in 100 ms intervals. The default value is 5000ms.</p> <p>Example</p> <p>1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.</p>

Field	Description
Collection Offset	<p>Used with the collection interval to schedule collection of data from a tag.</p> <p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p> <p>If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.</p>
Time Resolution	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Collector Deadband	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p>



Field	Description
	Select Disabled to prevent the tag from being compressed.
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>
Compression Time-out (ms)	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p> <p>Any numeric value.</p>

E-Signature

Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag.

Field	Description
	<ul style="list-style-type: none"> • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>

Advanced Options

Field	Description
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="824 827 1419 1142" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
Previous Block	<p>Displays the name of the previous (upstream) tag.</p> <p>Valid Entries</p> <p>None. This is a read-only field.</p>
Next Block	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div data-bbox="824 1528 1419 1793" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: In a Statistical Data tag, the Next Block field specifies the tag name of the downstream Statistical Control tag. No other tag type is valid.</p> </div>

Field	Description
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>

FN Tag

This tag contains the following details:

General

Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain spe-</p>

Field	Description
	<p>cial characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <p>~ ` + ^ : ? " * = { } . , ; ? @</p> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

Alarm Options

Field	Description
Alarm Areas	<p>Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.
Collect	<p>Lets you select if the tag is set for collection by the Proficy Historian collector.</p> <p>Select Enabled to allow the tag to be collected by the collector.</p>
Collection Interval	<p>Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector.</p> <p>Valid Entries</p> <p>Must be entered in 100 ms intervals. The default value is 5000ms.</p> <p>Example</p> <p>1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.</p>
Collection Offset	Used with the collection interval to schedule collection of data from a tag.

Field	Description
	<p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p> <p>If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.</p>
Time Resolution	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Collector Deadband	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>



Field	Description
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>
Compression Time-out (ms)	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p> <p>Any numeric value.</p>



E-Signature

Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag.

Field	Description
	<ul style="list-style-type: none"> • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>

Advanced Options

Field	Description
Output Areas A, B, C, D	<p>Lets you specify the destinations of the Fanout tag.</p> <p>Valid Entries</p> <p>A tag name (F_CV is appended automatically) or specific tag and field name pair in the tag.field format.</p> <p>Example</p> <p>To send the Fanout tag's value to a PID tag's set point Value field and to a Ramp tag's Target field, you would type PID1.F_TV1 and RM1.F_TV1 into the Destination fields.</p> <div data-bbox="821 926 1419 1192" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Tip: A value sent to a secondary tag does not place that tag on scan. Make sure that the target tag's upstream primary tag is on scan.</p> </div>
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="821 1696 1419 1896" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a</p> </div>

Field	Description
	<div data-bbox="820 260 1417 371" style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px;">  specific security area even if they cannot write to that area. </div>
Previous Block	<p>Displays the name of the previous (upstream) tag.</p> <p>Valid Entries</p> <p>None. This is a read-only field.</p>
Next Block	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div data-bbox="820 758 1417 1024" style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px;"> <p> Note:</p> <p>In a Statistical Data tag, the Next Block field specifies the tag name of the downstream Statistical Control tag. No other tag type is valid.</p> </div>
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>

GAB Tag

This tag contains the following details:

General

Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <pre>~ ` + ^ : ? " * = { } . , ; ? @</pre> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>

Field	Description
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

Alarm Tags

Field	Description
Tag 0-15	The tag of another block to monitor for alarms.

Alarm Options

Field	Description
Alarm Areas	<p>Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>


E-Signature

Field	Description
Type	The Type of Electronic Signature:

Field	Description
	<ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p>

Field	Description
	When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.

Advanced Options

Field	Description
Initial Scan	<p>Lets you select whether the tag is initially placed on or off scan.</p> <p>Click On Scan to place the tag on scan as soon as the Scan, Alarm, and Control (SAC) program starts or when the database is loaded. Click Off Scan to place the tag on scan by a Program block, an Event Action tag, a script, an operator entry in a Data link, or an Easy Database Access program.</p>
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="820 1472 1421 1785" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
Alarm Field 1	Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you

Field	Description
	<p>want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Process by Exception	<p>Enables exception-based processing for the tag.</p>
Scan Time	<p>Lets you specify how often the Scan, Alarm, and Control (SAC) program processes the tag and any tags (blocks) chained to it.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • 0 (one shot processing) • 0.05 to .95 in .05 increments (subsecond scan times) • 1 to 60 in 1 second increments • 1M to 60M in 1 minute increments • 1H to 24H in 1 hour increments <p>Example</p> <p>0.15 specifies a 15-subsecond scan time. 5 specifies a 5-second scan time, 10M specifies a 10-minute scan time, 16H specifies a 16-hour scan time.</p>

Field	Description
Phase At	<p>Lets you specify how long the Scan, Alarm, and Control (SAC) program delays in scanning the tag. When the tag has a second or subsecond scan time, SAC offsets the initial scan by the phase time when iFIX starts or when the database is re-loaded. When the tag has a scan time of 1 minute or longer, SAC offsets the initial scan starting at midnight.</p> <p>Valid Entries</p> <p>Depends on the scan time. If the scan time is in hours, the phase must be in hours:minutes. If the scan time is in minutes, the phase must be in minutes:seconds. If the scan time is in seconds, the phase must be in seconds. If the scan time is in subseconds, the phase must be in subseconds.</p>

GEN Tag

This tag contains the following details:

General

Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at</p>

Field	Description
	<p>least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <pre>~ ` + ^ : ? " * = { } . , ; ? @</pre> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

Limits and Scaling

Field	Description
Low Limit	Used to clamp input and to scale output.


Field	Description
High Limit	Used to clamp input and to scale output.
Units	For display purposes.



E-Signature



Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electron-</p>

Field	Description
	ic Signature settings are available. By default, this check box is disabled.
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>

Advanced Options

Field	Description
Wave	Select the desired waveform (SQUARE, SAW, SINE, TRIANGLE).
Period	The length of the full wave form is scan cycles. This also determines the resolution of the wave form. (1 to 1000)
Scale	Percent of the EGU scale used by basic wave form. (0.0 - 100.0) If you set the scale to 50 then the waveform value will range from the 0 to 50% of the EGU span (hi - lo).
Noise	<p>Percent of randomness in output value. (0.0 to 100.0). A random value is generated over the EGU span (hi - lo) and a percentage is added to the output.</p> <div data-bbox="820 1585 1421 1785" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: If the SCALE and NOISE fields total more than 100% then the output will be clamped to the EGU range. If they total less than</p> </div>

Field	Description
	 100% then the range of the output will be less than the EGU Span.
Center Output	If set then the output is centered on the EGU range otherwise it is 0 based. This is only meaningful if the SCALE and NOISE fields do not total 100%.
Startup Mode	Lets you select the tag's mode on startup. In Automatic mode, the tag receives data from the I/O driver, OPC server, or OPC UA server. In Manual mode, the tag receives data from the operator, scripts, recipes, or Program blocks.
Initial Scan	<p>Lets you select whether the tag is initially placed on or off scan.</p> <p>Click On Scan to place the tag on scan as soon as the Scan, Alarm, and Control (SAC) program starts or when the database is loaded. Click Off Scan to place the tag on scan by a Program block, an Event Action tag, a script, an operator entry in a Data link, or an Easy Database Access program.</p>
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="824 1682 1419 1875" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;">  Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a </div>

Field	Description
	 specific security area even if they cannot write to that area.
Previous Block	Displays the name of the previous (upstream) tag. Valid Entries None. This is a read-only field.
Next Block	Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.  Note: In a Statistical Data tag, the Next Block field specifies the tag name of the downstream Statistical Control tag. No other tag type is valid.
Alarm Field 1	Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information. Valid Entries Text, up to 80 characters.
Alarm Field 2	Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information. Valid Entries Text, up to 80 characters.
Process by Exception	Enables exception-based processing for the tag.

Field	Description
Scan Time	<p>Lets you specify how often the Scan, Alarm, and Control (SAC) program processes the tag and any tags (blocks) chained to it.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • 0 (one shot processing) • 0.05 to .95 in .05 increments (subsecond scan times) • 1 to 60 in 1 second increments • 1M to 60M in 1 minute increments • 1H to 24H in 1 hour increments <p>Example</p> <p>0.15 specifies a 15-subsecond scan time. 5 specifies a 5-second scan time, 10M specifies a 10-minute scan time, 16H specifies a 16-hour scan time.</p>

HS Tag


This tag contains the following details:


General


Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p>

Field	Description
	<p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <pre>~ ` + ^ : ? " * = { } . , ; ? @</pre> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

Limits and Scaling

Field	Description
<p>Low Limit</p>	<p>Lets you enter the tag's minimum value.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information.</p> </div> <p>In a Calculation or Signal Select tag, if the output of the tag is 10 and the Low Limit is 15, the tag clamps the value at 15. You must enter a Low Limit of 10 or less to output a value of 10.</p> <p>If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the Low Limit field.</p> <p>If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
<p>High Limit</p>	<p>Lets you enter the tag's maximum value.</p> <p>Valid Entries</p>

Field	Description
	<p>You can enter a high limit in one of three formats:</p> <ul style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;">  Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. </div> <p>In a Calculation or a Signal Select tag, if the output of the tag is 150 and the High Limit is 100, the tag clamps the value at 100. You must enter a High Limit of 150 or more to output a value of 150.</p> <p>If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the High Limit field.</p> <p>If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
Units	<p>Lets you enter text describing the engineering units range.</p> <p>Valid Entries</p> <p>Up to 33 characters.</p>

Field	Description
	<p>Example</p> <p>Kilograms per square meter, Liters per minute, degrees Celsius,</p> <div data-bbox="820 451 1421 716" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note:</p> <p>This entry does not affect the calculation or function of any variables in iFIX. It is used strictly as a display label to identify the engineering units.</p> </div>

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.
Collect	<p>Lets you select if the tag is set for collection by the Proficy Historian collector.</p> <p>Select Enabled to allow the tag to be collected by the collector.</p>
Collection Interval	<p>Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector.</p> <p>Valid Entries</p> <p>Must be entered in 100 ms intervals. The default value is 5000ms.</p> <p>Example</p> <p>1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.</p>
Collection Offset	Used with the collection interval to schedule collection of data from a tag.

Field	Description
	<p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p> <p>If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.</p>
Time Resolution	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Collector Deadband	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>


Field	Description
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>
Compression Time-out (ms)	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p> <p>Any numeric value.</p>



E-Signature



Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag.

Field	Description
	<ul style="list-style-type: none"> • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>

Advanced Options

Field	Description
Auto Clear Status	<p>Lets you specify when the Histogram tag clears the histogram chart.</p> <p>Valid Entries</p> <p>When you enable the check box, the tag clears the display each time the upstream tag goes on scan. If the chain goes off and then back on scan, the histogram chart does not appear until the block generates new values according to the Group field value.</p> <p>When you disable the check box retains old values even if the upstream tag goes off scan. If the chain goes off and then back on scan, old values are displayed. However, this occurs only if the group value was reached.</p>
Interval	<p>Lets you specify the range of values represented by each column in the bar graph.</p> <p>Valid Entries</p> <p>A number within the EGU range.</p> <div data-bbox="824 1329 1419 1640" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Tip: Enter the Low and High Limits (EGU) before entering the Interval value. If you enter the Interval value first, the tag automatically readjusts the Interval value when you enter the Low and High Limits.</p> </div>
Group Size	<p>Lets you specify:</p> <ul style="list-style-type: none"> • How often the Histogram updates the associated chart. The tag calculates the update period by multiplying the Group value by the

Field	Description
	<p>scan time of the chain. For example, if you enter a Group value of 10 and you scan an Analog Input tag every 5 seconds, the histogram updates every 50 seconds.</p> <ul style="list-style-type: none"> • The number of occurrences displayed on the histogram and the maximum height of the display bars. <div data-bbox="824 615 1417 1060" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Some input readings may fall outside of the Histogram tag's engineering units range. When this happens, the histogram registers the readings but does not display them. The histogram only displays those incoming values that fall within the specified engineering units range during the specified group limit.</p> </div> <p>Valid Entries</p> <p>A time in seconds from 1 to 1000.</p>
<p>Security Areas</p>	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="824 1707 1417 1854" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area.</p> </div>

Field	Description
	 This allows users to retrieve data from a specific security area even if they cannot write to that area.
Previous Block	Displays the name of the previous (upstream) tag. Valid Entries None. This is a read-only field.
Next Block	Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.  Note: In a Statistical Data tag, the Next Block field specifies the tag name of the downstream Statistical Control tag. No other tag type is valid.
Alarm Field 1	Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information. Valid Entries Text, up to 80 characters.
Alarm Field 2	Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information. Valid Entries Text, up to 80 characters.

ITM Tag

This tag contains the following details:


General

Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <p>~ ` + ^ : ? " * = { } . , ; ? @</p> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>


Field	Description
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.


Timer and Total Options

Field	Description
Pass	<p>INP passes raw input (converted to 0.0 or 1.0), ALM passes Current Alarm (converted to 0.0 or 1.0), INT passes the most recent interval in seconds (as a FLOAT with milliseconds as a fraction), TOT passes current total timer in seconds (as a FLOAT with fraction of 0). Note that the passed values are converted to Float. Also note that some downstream blocks (such as AO) may clamp the passed value to their EGU or OPERATOR limits.</p>
Gate	A TAG:FIELD specifier (normally an F_CV). This gate input is 'anded' with the upstream value and the AUTO status. If blank then the GATE is assumed to be TRUE.
Reset	A TAG:FIELD specifier (normally an F_CV). A transition from 0 to non-zero (e.g. from OPEN to CLOSE) on this optional input will clear the total interval (like writing 0 to the A_TOTAL field). It can optionally clear the current interval and the history based

Field	Description
	on the two check boxes. If the block was previously in alarm as a result of the TOTAL value, the current alarm will return to OK and the latched alarm will remain in place until it is acknowledged. If current interval reset is selected and a current interval is active then it will be reset from its current value back to 0 and will continue to count up from 0.
Reset History	Select this to enable reset history.
Reset Current	Select this to enable reset current.
Range *	<p>A range value which if exceeded for an interval or total will generate a HI alarm. The format is DD:HH:MM:SS.TTT. This will still function if set to zero. To disable, clear the Enable check box for the Alarm Limits (Interval or Total). The alarm occurs as soon as the limit is exceeded. At the start of the next interval the current alarm state will return to normal (although the latched alarm will remain set until it is acknowledged).</p> <div data-bbox="820 1155 1421 1512" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Alarming is only done on the current interval, not on any of the saved intervals. For example if the limit is changed from 50 to 25 and a previous interval had been 35 then no alarm is generated for that stored interval.</p> </div>
Interval Limit	Select to set the INTERVAL LIMIT alarm. Enter the alarm value in the adjoining field.
Total Limit	Select to set the TOTAL LIMIT alarm. Enter the alarm value in the adjoining field.

Alarm Options

Field	Description
Alarm Areas	<p>Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>
Enable Alarm	<p>Lets you enable or disable alarming for this tag.</p> <p>When you enable alarming, the tag generates alarms allowing objects in your operator displays to show alarm conditions, and enabling other tags to detect alarms from the tag.</p> <div data-bbox="821 1003 1417 1318" style="border: 1px solid #00a0c0; border-radius: 10px; padding: 10px; background-color: #e6f2f8;"> <p> Note:</p> <p>The entire chain can be affected when you disable alarms for a tag. In addition, for both the Digital and Analog Alarm tags, this field is ignored when you enable the Alarm Suspend field.</p> </div>
Priority	<p>Lets you specify the alarm priority for a tag. If the priority is equal or greater than the SCADA node's alarm priority, iFIX sends the alarm to all the alarm destinations enabled for this node. However, if the priority is less than the SCADA node's alarm priority, the alarm is automatically acknowledged and filtered out so that it does not appear in your alarm destinations. However, the alarm does appear in Data links configured to display current and latched alarms.</p> <p>Valid Entries</p>

Field	Description
	<p>INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL</p> <div data-bbox="824 380 1414 646" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: To report tag alarms, the appropriate alarm areas must be assigned to each of the alarm services enabled in the System Configuration Utility (SCU).</p> </div>



E-Signature

Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that</p>

Field	Description
	<p>the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>

Advanced Options

Field	Description
Startup Mode	<p>Lets you select the tag's mode on startup. In Automatic mode, the tag receives data from the I/O driver, OPC server, or OPC UA server. In Manual mode, the tag receives data from the operator, scripts, recipes, or Program blocks.</p>
Clear	<p>If Set then the saved intervals and total will be cleared when the chain goes on scan. If not they will retain values when off scan. Also if this is clear then on system startup or database reload the block will retain the values it had the last time the process database was saved to disk by DBB.</p>
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Man-</p>

Field	Description
	<p>ager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="821 611 1419 926" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
Previous Block	<p>Displays the name of the previous (upstream) tag.</p> <p>Valid Entries</p> <p>None. This is a read-only field.</p>
Next Block	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div data-bbox="821 1310 1419 1577" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: In a Statistical Data tag, the Next Block field specifies the tag name of the downstream Statistical Control tag. No other tag type is valid.</p> </div>
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p>

Field	Description
	Text, up to 80 characters.
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>

LL Tag

This tag contains the following details:


General



Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([),</p>


Field	Description
	<p>close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <p>~ ` + ^ : ? " * = { } . , ; ? @</p> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	<p>The tag type. Display-only field.</p>
Current Value	<p>The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.</p>

Limits and Scaling

Field	Description
Low Limit	<p>Lets you enter the tag's minimum value.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999.

Field	Description
	<ul style="list-style-type: none"> • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;">  Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. </div> <p>In a Calculation or Signal Select tag, if the output of the tag is 10 and the Low Limit is 15, the tag clamps the value at 15. You must enter a Low Limit of 10 or less to output a value of 10.</p> <p>If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the Low Limit field.</p> <p>If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
High Limit	<p>Lets you enter the tag's maximum value.</p> <p>Valid Entries</p> <p>You can enter a high limit in one of three formats:</p> <ul style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38.

Field	Description
	<ul style="list-style-type: none"> Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div data-bbox="821 478 1419 743" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;">  Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. </div> <p>In a Calculation or a Signal Select tag, if the output of the tag is 150 and the High Limit is 100, the tag clamps the value at 100. You must enter a High Limit of 150 or more to output a value of 150.</p> <p>If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the High Limit field.</p> <p>If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
Units	<p>Lets you enter text describing the engineering units range.</p> <p>Valid Entries</p> <p>Up to 33 characters.</p> <p>Example</p> <p>Kilograms per square meter, Liters per minute, degrees Celsius,</p> <div data-bbox="821 1743 1419 1894" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;">  Note: This entry does not affect the calculation or function of any variables in iFIX. It is </div>

Field	Description
	 used strictly as a display label to identify the engineering units.

Alarm Options

Field	Description
Alarm Areas	<p>Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.
Collect	<p>Lets you select if the tag is set for collection by the Proficy Historian collector.</p> <p>Select Enabled to allow the tag to be collected by the collector.</p>
Collection Interval	<p>Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector.</p> <p>Valid Entries</p> <p>Must be entered in 100 ms intervals. The default value is 5000ms.</p> <p>Example</p>

Field	Description
	1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.
Collection Offset	<p>Used with the collection interval to schedule collection of data from a tag.</p> <p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p> <p>If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.</p>
Time Resolution	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Collector Deadband	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values</p>

Field	Description
	<p>that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>
Compression Time-out (ms)	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p> <p>Any numeric value.</p>

E-Signature




Field	Description
Type	The Type of Electronic Signature:


Field	Description
	<ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electron-</p>

Field	Description
	ic Signature settings are available. By default, this check box is disabled.

Advanced Options

Field	Description
Scaling Factor	<p>Lets you specify a scaling factor that modifies the lead lag curve. The constant may be applied to the input prior to performing the calculation.</p> <p>Valid Entries</p> <p>A value from -100.00 to +100.00. Enter 1 to disable this function.</p>
Lead Time Constant	<p>Lets you specify the lead time constant.</p> <p>Valid Entries</p> <p>A value from 0.00 to +100.00 minutes. Enter 0 to disable this function.</p> <p>iFIX accounts for the chain's scan time in the calculation. This scan time controls the size of the offset introduced by a change in the input. The offset is delayed according to the lag constant.</p>
Lag Time Constant	<p>Lets you specify the lag time constant that controls the rate at which the output of the tag approaches the input. A large lag time changes the output very slowly, aside from the lead time, and a small lag time tracks input more closely.</p> <p>Valid Entries</p> <p>A value from 0.00 to +100.00 minutes. Enter 0 if you do not want to use any lag time.</p>

Field	Description
	<div data-bbox="820 262 1425 493" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;">  Note: If the Lag time and Lead time are equal, they cancel each other out because the Lead calculation is the inverse of the Lag. </div>
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="820 987 1425 1312" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;">  Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area. </div>
Previous Block	<p>Displays the name of the previous (upstream) tag.</p> <p>Valid Entries</p> <p>None. This is a read-only field.</p>
Next Block	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div data-bbox="820 1690 1425 1839" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;">  Note: In a Statistical Data tag, the Next Block field specifies the tag name of the down- </div>

Field	Description
	 stream Statistical Control tag. No other tag type is valid.
Alarm Field 1	Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information. Valid Entries Text, up to 80 characters.
Alarm Field 2	Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information. Valid Entries Text, up to 80 characters.

MDI Tag



This tag contains the following details:



General


Field	Description
Tag Name	Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs. Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it. Valid Entries

Field	Description
	<p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <p>~ ` + ^ : ? " * = { } . , ; ? @</p> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

I/O Addressing

Field	Description
Driver	<p>Lets you select an I/O driver, OPC server, or OPC UA server for the tag. The selected driver or server enables the tag to communicate with process hardware on the plant floor.</p> <p>Before you can select an I/O driver, OPC server, or OPC UA server you must install it and add it to the available ones in the SCU.</p>
I/O Address	<p>Lets you enter the location in the process hardware where data for this tag is saved and where output is sent.</p> <p>Valid Entries</p> <p>Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations.</p> <div data-bbox="820 1096 1416 1402" style="border: 1px solid black; border-radius: 10px; padding: 10px; background-color: #fff9c4;"> <p> CAUTION: Do not assign the same I/O address to tags when using exception-based and time-based processing. Doing so will cause the exception-based tags to occasionally miss a value.</p> </div> <div data-bbox="820 1438 1416 1873" style="border: 1px solid black; border-radius: 10px; padding: 10px; background-color: #fff9c4;"> <p> CAUTION: Configuration Hub currently does not do I/O address validations before publish. If you enter an invalid IO address into a tag or generate an invalid I/O address via the model and substitutions, the publish may fail to set the IO address into the active database, and your invalid IO address will be removed.</p> </div>


Field	Description
H/W Options	<p>Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p> <div data-bbox="824 436 1419 699" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Signal conditioning and linear scaling cannot be applied simultaneously. If you select a value for Signal Conditioning verify that Linear Scaling is not selected.</p> </div> <p>Valid Entries</p> <p>Depends on your driver or server. Refer to your driver or server manual for more information.</p>
Enable Driver 1-2	<p>Allows you to enable or disable the second or third digital input value.</p> <div data-bbox="824 1024 1419 1287" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: If you select the check box(es), enter the driver name, I/O address, and any options for that particular driver in the appropriate fields.</p> </div>
Driver 1-2	<p>Lets you select an I/O driver, OPC UA server, or OPC server for the tag. The selected driver or server enables the tag to communicate with process hardware on the plant floor.</p> <p>Before you can select an I/O driver, OPC UA server, or OPC server, you must install it and add it to the available drivers in the SCU.</p>
I/O Address 1-2	<p>Lets you enter the location in the process hardware where data for this tag is saved and where output is sent. In an On-Off Control tag, specify the address of the digital point you want opened and</p>

Field	Description
	<p>closed based on the Turn on Above and Turn off Below values.</p> <p>Valid Entries</p> <p>Depends on your driver. Consult your I/O driver manual for details on the proper input/output addresses and configurations.</p> <div style="border: 1px solid black; background-color: #fff9c4; padding: 10px; margin-top: 10px;"> <p> CAUTION:</p> <p>Do not assign the same I/O address to tags when using exception-based and time-based processing. Doing so will cause the exception-based blocks to occasionally miss a value.</p> </div>
H/W Options 1-2	<p>Lets you select any specific device control addressing format that the tag uses to communicate with process hardware on the plant floor.</p> <p>Valid Entries</p> <p>For most process hardware, this field is usually left blank. Consult your I/O driver manual for the applicable hardware code if necessary.</p>
Process by Exception	<p>Enables exception-based processing for the tag.</p>
Scan Time	<p>Lets you specify how often the Scan, Alarm, and Control (SAC) program processes the tag and any tags (blocks) chained to it.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • 0 (one shot processing) • 0.05 to .95 in .05 increments (subsecond scan times) • 1 to 60 in 1 second increments

Field	Description
	<ul style="list-style-type: none"> • 1M to 60M in 1 minute increments • 1H to 24H in 1 hour increments <p>Example</p> <p>0.15 specifies a 15-subsecond scan time. 5 specifies a 5-second scan time, 10M specifies a 10-minute scan time, 16H specifies a 16-hour scan time.</p>
Phase At	<p>Lets you specify how long the Scan, Alarm, and Control (SAC) program delays in scanning the tag. When the tag has a second or subsecond scan time, SAC offsets the initial scan by the phase time when iFIX starts or when the database is reloaded. When the tag has a scan time of 1 minute or longer, SAC offsets the initial scan starting at midnight.</p> <p>Valid Entries</p> <p>Depends on the scan time. If the scan time is in hours, the phase must be in hours:minutes. If the scan time is in minutes, the phase must be in minutes:seconds. If the scan time is in seconds, the phase must be in seconds. If the scan time is in subseconds, the phase must be in subseconds.</p>


Device States


Field	Description
Alarm 0-7 Enable	<p>Enables or disables alarming for each of the 8 possible raw values. If the tag enters any of the states for which the alarm column is checked, the tag generates a CFN (change from normal) alarm.</p>

Field	Description
	<div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: The Multistate Digital Input tag generates alarms only on a transition between alarm status and no alarm status. Transitions between different alarm states do not generate new alarms. </div>
Value 0 (000) Value 1 (001) Value 2 (010) Value 3 (011) Value 4 (100) Value 5 (101) Value 6 (110) Value 7 (111)	Lets you enter a descriptive label for each of the 8 possible raw values. Valid Entries Up to 9 alphanumeric characters.

Alarm Options

Field	Description
Alarm Areas	Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field. Valid Entries ALL or up to 15 alarm area names.
Enable Alarm	Lets you enable or disable alarming for this tag. When you enable alarming, the tag generates alarms allowing objects in your operator displays

Field	Description
	<p>to show alarm conditions, and enabling other tags to detect alarms from the tag.</p> <div data-bbox="824 380 1421 688" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: The entire chain can be affected when you disable alarms for a tag. In addition, for both the Digital and Analog Alarm tags, this field is ignored when you enable the Alarm Suspend field.</p> </div>
Realarm	<p>Enables or disables the re-alarm status of the tag.</p> <p>Valid Entries</p> <p>Select the re-alarm check box to generate new alarm messages each time there is a transition between alarm states. Clear this check box if you do not want to generate new alarm messages whenever the alarm state changes.</p>
Priority	<p>Lets you specify the alarm priority for a tag. If the priority is equal or greater than the SCADA node's alarm priority, iFIX sends the alarm to all the alarm destinations enabled for this node. However, if the priority is less than the SCADA node's alarm priority, the alarm is automatically acknowledged and filtered out so that it does not appear in your alarm destinations. However, the alarm does appear in Data links configured to display current and latched alarms.</p> <p>Valid Entries</p> <p>INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL</p>

Field	Description
	<div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: To report tag alarms, the appropriate alarm areas must be assigned to each of the alarm services enabled in the System Configuration Utility (SCU). </div>
Shelve Enable	Select this check box to enable Alarm Shelving for the tag.
Shelve Policy	Select an alarm shelving policy from the drop-down list.

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.
Collect	Lets you select if the tag is set for collection by the Proficy Historian collector. Select Enabled to allow the tag to be collected by the collector.
Collection Interval	Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector. Valid Entries Must be entered in 100 ms intervals. The default value is 5000ms. Example 1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.

Field	Description
Collection Offset	<p>Used with the collection interval to schedule collection of data from a tag.</p> <p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p> <p>If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.</p>
Time Resolution	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Collector Deadband	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p>


Field	Description
	Select Disabled to prevent the tag from being compressed.
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>
Compression Time-out (ms)	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p> <p>Any numeric value.</p>


E-Signature

Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag.

Field	Description
	<ul style="list-style-type: none"> • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>

Advanced Options

Field	Description
Initial Scan	<p>Lets you select whether the tag is initially placed on or off scan.</p> <p>Click On Scan to place the tag on scan as soon as the Scan, Alarm, and Control (SAC) program starts or when the database is loaded. Click Off Scan to place the tag on scan by a Program block, an Event Action tag, a script, an operator entry in a Data link, or an Easy Database Access program.</p>
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="821 1230 1419 1543" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
Previous Block	<p>Displays the name of the previous (upstream) tag.</p> <p>Valid Entries</p> <p>None. This is a read-only field.</p>

Field	Description
Next Block	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div data-bbox="824 432 1417 699" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: In a Statistical Data tag, the Next Block field specifies the tag name of the downstream Statistical Control tag. No other tag type is valid.</p> </div>
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>

MDO Tag


This tag contains the following details:




General

Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <pre>~ ` + ^ : ? " * = { } . , ; ? @</pre> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p>

Field	Description
	A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

I/O Addressing

Field	Description
I/O Driver	<p>Lets you select an I/O driver, OPC server, or OPC UA server for the tag. The selected driver or server enables the tag to communicate with process hardware on the plant floor.</p> <p>Before you can select an I/O driver, OPC server, or OPC UA server you must install it and add it to the available ones in the SCU.</p>
I/O Address	<p>Lets you enter the location in the process hardware where data for this tag is saved and where output is sent.</p> <p>Valid Entries</p> <p>Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p> CAUTION: Do not assign the same I/O address to tags when using exception-based and time-based processing. Doing so will</p> </div>

Field	Description
	<p> cause the exception-based tags to occasionally miss a value.</p> <p> CAUTION: Configuration Hub currently does not do I/O address validations before publish. If you enter an invalid IO address into a tag or generate an invalid I/O address via the model and substitutions, the publish may fail to set the IO address into the active database, and your invalid IO address will be removed.</p>
H/W Options	<p>Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p> <p> Note: Signal conditioning and linear scaling cannot be applied simultaneously. If you select a value for Signal Conditioning verify that Linear Scaling is not selected.</p> <p>Valid Entries</p> <p>Depends on your driver or server. Refer to your driver or server manual for more information.</p>
Normally Closed	<p>Most contacts are normally OPEN. In this case the normal state is 0 and the normal pattern of a pulse is 0, 1, 0. Setting this flag tells the block to assume this is a normally CLOSED contact. In this case the normal state is 1 and the normal pulse pattern is 1, 0, 1.</p>
Retry Output	<p>If SET then the initial 'CLOSE' output is sent every scan cycle until a confirming CLOSE is read back</p>

Field	Description
	<p>from the device. If clear then the initial CLOSE output is sent only once (this should be sufficient in most applications). In general the system will operate more efficiently if this flag is clear. However if it is possible for the output device to lose synchronization with the PC (e.g. thru a power loss) then you may wish to resend the output every cycle to insure that the system will recover from this situation.</p>
Process by Exception	Enables exception-based processing for the tag.
Scan Time	<p>Lets you specify how often the Scan, Alarm, and Control (SAC) program processes the tag and any tags (blocks) chained to it.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • 0 (one shot processing) • 0.05 to .95 in .05 increments (subsecond scan times) • 1 to 60 in 1 second increments • 1M to 60M in 1 minute increments • 1H to 24H in 1 hour increments <p>Example</p> <p>0.15 specifies a 15-subsecond scan time. 5 specifies a 5-second scan time, 10M specifies a 10-minute scan time, 16H specifies a 16-hour scan time.</p>
Phase At	<p>Lets you specify how long the Scan, Alarm, and Control (SAC) program delays in scanning the tag. When the tag has a second or subsecond scan time, SAC offsets the initial scan by the phase time when iFIX starts or when the database is reloaded. When the tag has a scan time of 1 minute</p>

Field	Description
	<p>or longer, SAC offsets the initial scan starting at midnight.</p> <p>Valid Entries</p> <p>Depends on the scan time. If the scan time is in hours, the phase must be in hours:minutes. If the scan time is in minutes, the phase must be in minutes:seconds. If the scan time is in seconds, the phase must be in seconds. If the scan time is in subseconds, the phase must be in subseconds.</p>

Limits and Scaling

Field	Description
Open Tag	<p>Lets you enter a descriptive label for the logical 0 value received by the tag. You can display this label in the iFIX WorkSpace through a Data link to aid operators in interpreting the value for the contact.</p> <p>Valid Entries</p> <p>A label of up to 16 characters.</p> <p>Examples</p> <p>Open, Off</p>
Close Tag	<p>Lets you enter a descriptive label for the logical 1 value received by the tag. You can display this label in the iFIX WorkSpace through a Data link to aid operators in interpreting the value for the contact.</p> <p>Valid Entries</p> <p>A label of up to 16 characters.</p> <p>Examples</p> <p>Close, On.</p>


E-Signature

Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p>

Field	Description
	<p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>

Advanced Options

Field	Description
Startup Mode	<p>Lets you select the tag's mode on startup. In Automatic mode, the tag receives data from the I/O driver, OPC server, or OPC UA server. In Manual mode, the tag receives data from the operator, scripts, recipes, or Program blocks.</p>
Initial Scan	<p>Lets you select whether the tag is initially placed on or off scan.</p> <p>Click On Scan to place the tag on scan as soon as the Scan, Alarm, and Control (SAC) program starts or when the database is loaded. Click Off Scan to place the tag on scan by a Program block, an Event Action tag, a script, an operator entry in a Data link, or an Easy Database Access program.</p>
Duty Cycle	<p>Length of duty cycle in multiples of the SCAN TIME from 0 to 100. This is the minimum time the output will remain closed. For '0' the output will be OPENED as soon as it is detected to be CLOSED. Otherwise the block will delay for 'n' scan cycles before opening the output.</p>
Timeout	<p>This is the maximum number of scan cycles that we will wait for the leading and trailing edge confirms. If the confirm is not received before the timeout expires the request is aborted. The block stays on scan and another request can be attempt-</p>

Field	Description
	<p>ed. Note that if OUTPUT RETRY is set then we will also resend the leading or trailing edge request at each scan cycle if we do not get the confirm.</p>
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="821 905 1419 1213" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p>

Field	Description
	<p>Valid Entries</p> <p>Text, up to 80 characters.</p>

ODO Tag

This tag contains the following details:




General

Field	Description
<p>Tag Name</p>	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p>

Field	Description
	<p>~ ` + ^ : ? " * = { } . , ; ? @</p> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

I/O Addressing

Field	Description
I/O Driver	<p>Lets you select an I/O driver, OPC server, or OPC UA server for the tag. The selected driver or server enables the tag to communicate with process hardware on the plant floor.</p> <p>Before you can select an I/O driver, OPC server, or OPC UA server you must install it and add it to the available ones in the SCU.</p>
I/O Address	<p>Lets you enter the location in the process hardware where data for this tag is saved and where output is sent.</p> <p>Valid Entries</p>

Field	Description
	<p>Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations.</p> <div data-bbox="821 426 1414 737" style="border: 1px solid #ccc; padding: 10px; background-color: #fff9c4;"> <p> CAUTION: Do not assign the same I/O address to tags when using exception-based and time-based processing. Doing so will cause the exception-based tags to occasionally miss a value.</p> </div> <div data-bbox="821 768 1414 1209" style="border: 1px solid #ccc; padding: 10px; background-color: #fff9c4;"> <p> CAUTION: Configuration Hub currently does not do I/O address validations before publish. If you enter an invalid IO address into a tag or generate an invalid I/O address via the model and substitutions, the publish may fail to set the IO address into the active database, and your invalid IO address will be removed.</p> </div>
H/W Options	<p>Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p> <div data-bbox="821 1394 1414 1661" style="border: 1px solid #0070c0; padding: 10px; background-color: #e1f5fe;"> <p> Note: Signal conditioning and linear scaling cannot be applied simultaneously. If you select a value for Signal Conditioning verify that Linear Scaling is not selected.</p> </div> <p>Valid Entries</p> <p>Depends on your driver or server. Refer to your driver or server manual for more information.</p>


Field	Description
Invert Output	Inverts the output value so that if the value is 0, it outputs a 1. You can use this option to send a 0 to close a contact and send a 1 to open it.
Time	The duration of the momentary pulse.


Limits and Scaling

Field	Description
Open Tag	<p>Lets you enter a descriptive label for the logical 0 value received by the tag. You can display this label in the iFIX WorkSpace through a Data link to aid operators in interpreting the value for the contact.</p> <p>Valid Entries</p> <p>A label of up to 16 characters.</p> <p>Examples</p> <p>Open, Off</p>
Close Tag	<p>Lets you enter a descriptive label for the logical 1 value received by the tag. You can display this label in the iFIX WorkSpace through a Data link to aid operators in interpreting the value for the contact.</p> <p>Valid Entries</p> <p>A label of up to 16 characters.</p> <p>Examples</p> <p>Close, On.</p>



Alarm Options


Field	Description
Alarm Areas	Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an

Field	Description
	<p>item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>
<p>Enable Alarm</p>	<p>Lets you enable or disable alarming for this tag.</p> <p>When you enable alarming, the tag generates alarms allowing objects in your operator displays to show alarm conditions, and enabling other tags to detect alarms from the tag.</p> <div data-bbox="820 835 1419 1148" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: The entire chain can be affected when you disable alarms for a tag. In addition, for both the Digital and Analog Alarm tags, this field is ignored when you enable the Alarm Suspend field.</p> </div>
<p>Priority</p>	<p>Lets you specify the alarm priority for a tag. If the priority is equal or greater than the SCADA node's alarm priority, iFIX sends the alarm to all the alarm destinations enabled for this node. However, if the priority is less than the SCADA node's alarm priority, the alarm is automatically acknowledged and filtered out so that it does not appear in your alarm destinations. However, the alarm does appear in Data links configured to display current and latched alarms.</p> <p>Valid Entries</p> <p>INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL</p>

Field	Description
	<div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;">  Note: To report tag alarms, the appropriate alarm areas must be assigned to each of the alarm services enabled in the System Configuration Utility (SCU). </div>

Advanced Options

Field	Description
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;">  Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area. </div>
Next Block	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;">  Note: In a Statistical Data tag, the Next Block field specifies the tag name of the down- </div>

Field	Description
	 stream Statistical Control tag. No other tag type is valid.

PA Tag

This tag contains the following details:

General

Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p>

Field	Description
	<p>~ ` + ^ : ? " * = { } . , ; ? @</p> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

Input Definitions

Field	Description
Input 1-8 Identifier	Any two-character alphanumeric ID that identifies the corresponding input. Default IDs for input values 1 through 8 are A through H.
Input 1-8 Tag	<p>An input can be any primary or secondary tag that accepts analog values (for example, an Analog Input or Totalizer tag) or an operator entry into this field.</p> <p>To configure the Pareto tag to accept values from another tag, enter the tag and field name pair in the input column (for example, AI1.F_CV). If the input goes off scan, the Pareto block treats the input's value as zero.</p>

Field	Description
	You can also configure the Pareto block to use a numeric constant that is greater than or equal to zero. The Pareto block treats negative numbers as zero.
Input 1-8 Descriptor	Up to 30 alphanumeric characters for each Pareto block input.

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.
Collect	Lets you select if the tag is set for collection by the Proficy Historian collector. Select Enabled to allow the tag to be collected by the collector.
Collection Interval	Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector. Valid Entries Must be entered in 100 ms intervals. The default value is 5000ms. Example 1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.
Collection Offset	Used with the collection interval to schedule collection of data from a tag. Valid Entries

Field	Description
	<p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p> <p>If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.</p>
Time Resolution	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Collector Deadband	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p>

Field	Description
	<p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>
<p>Compression Time-out (ms)</p>	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p> <p>Any numeric value.</p>


E-Signature



Field	Description
<p>Type</p>	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.

Field	Description
Remember User	Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.
Exempt Alarm Ack	Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>

Advanced Options

Field	Description
Display Format	Lets you specify the number of decimal digits that appear to the right of the decimal point in operator displays.

Field	Description
	<p>Valid Entries</p> <p>Any number from 0 to 6 digits of precision.</p> <div data-bbox="824 407 1414 669" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: In the iFIX WorkSpace, the Display field can contain a total of 15 characters, consisting of numbers to the left and right of the decimal point</p> </div> <p>.</p>
Sort Order	<p>Lets you specify the order in which the input values appear in operator displays. An operator can change the sort order through a Data link that displays the A_SORT field.</p> <p>Valid Entries</p> <p>Descending, Ascending, or No Sorting. By default, the sort order is Descending. Database Manager sorts the data as follows:</p> <ul style="list-style-type: none"> • 1 Special characters (such as punctuation marks) by ASCII value. • 2 Numbers by numeric value. • 3 Letters in alphabetic order.
Initial Scan	<p>Lets you select whether the tag is initially placed on or off scan.</p> <p>Click On Scan to place the tag on scan as soon as the Scan, Alarm, and Control (SAC) program starts or when the database is loaded. Click Off Scan to place the tag on scan by a Program block, an Event Action tag, a script, an operator entry in a Data link, or an Easy Database Access program.</p>

Field	Description
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="824 751 1419 1066" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
Previous Block	<p>Displays the name of the previous (upstream) tag.</p> <p>Valid Entries</p> <p>None. This is a read-only field.</p>
Next Block	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div data-bbox="824 1453 1419 1724" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: In a Statistical Data tag, the Next Block field specifies the tag name of the downstream Statistical Control tag. No other tag type is valid.</p> </div>
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Imple-</p>

Field	Description
	<p>menting Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Process by Exception	<p>Enables exception-based processing for the tag.</p>
Scan Time	<p>Lets you specify how often the Scan, Alarm, and Control (SAC) program processes the tag and any tags (blocks) chained to it.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • 0 (one shot processing) • 0.05 to .95 in .05 increments (subsecond scan times) • 1 to 60 in 1 second increments • 1M to 60M in 1 minute increments • 1H to 24H in 1 hour increments <p>Example</p> <p>0.15 specifies a 15-subsecond scan time. 5 specifies a 5-second scan time, 10M specifies a 10-minute scan time, 16H specifies a 16-hour scan time.</p>
Phase At	<p>Lets you specify how long the Scan, Alarm, and Control (SAC) program delays in scanning the tag.</p>

Field	Description
	<p>When the tag has a second or subsecond scan time, SAC offsets the initial scan by the phase time when iFIX starts or when the database is reloaded. When the tag has a scan time of 1 minute or longer, SAC offsets the initial scan starting at midnight.</p> <p>Valid Entries</p> <p>Depends on the scan time. If the scan time is in hours, the phase must be in hours:minutes. If the scan time is in minutes, the phase must be in minutes:seconds. If the scan time is in seconds, the phase must be in seconds. If the scan time is in subseconds, the phase must be in subseconds.</p>

PAR Tag

This tag contains the following details:



General



Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal</p>

Field	Description
	<p>databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), under-scores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <p>~ ` + ^ : ? " * = { } . , ; ? @</p> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

Limits and Scaling


Field	Description
Low Limit	Lets you enter the block's minimum value.

Field	Description
	<p>Valid Entries</p> <p>You can enter a low limit in one of three formats:</p> <ul style="list-style-type: none"> • Standard Integer. Standard integers range from -32768 to 32767 (signed integers); 0 to 65535 (unsigned integers); 0 to 999 (3BCD); or 0 to 4095 (12 Binary). • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. <div data-bbox="820 810 1419 1077" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p> </div>
High Limit	<p>Lets you enter the block's maximum value.</p> <p>Valid Entries</p> <p>You can enter a low limit in one of three formats:</p> <ul style="list-style-type: none"> • Standard Integer. Standard integers range from -32768 to 32767 (signed integers); 0 to 65535 (unsigned integers); 0 to 999 (3BCD); or 0 to 4095 (12 Binary). • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. <div data-bbox="820 1715 1419 1866" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: If you are using scientific notation, up to six decimal places may be configured with</p> </div>

Field	Description
	<div style="border: 1px solid #0070C0; border-radius: 5px; padding: 5px;">  precision, and the range may be positive or negative. </div>
Units	<p>Lets you enter text describing the engineering units range.</p> <p>Valid Entries</p> <p>Up to 33 characters.</p> <p>Example</p> <p>Kilograms per square meter; liters per minute; degrees Celsius.</p> <div style="border: 1px solid #0070C0; border-radius: 5px; padding: 5px; margin-top: 10px;">  Note: This entry does not affect the calculation or function of any variables in iFIX. It is used strictly as a display label to identify the engineering units. </div>

Array Values

Field	Description
Value 01-60	<p>Lets you read values from or write values to each of the 60 fields.</p> <p>Valid Entries</p> <p>You can enter a value in one of three formats:</p> <p>Stan</p> <ul style="list-style-type: none"> • dard Integer. Standard integers range from -32768 to 32767 (signed integers); 0 to 65535 (unsigned integers); 0 to 999 (3BCD); or 0 to 4095 (12 Binary).


Field	Description
	<ul style="list-style-type: none"> Expanded Decimal Notation, ranging from -9999999 to 9999999. Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. <div data-bbox="821 478 1421 743" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note: If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p> </div>
Text 01-60	<p>Lets you read descriptions from or write descriptions to each of the 60 fields.</p> <p>Valid Entries</p> <p>Up to 40 characters.</p>

Alarm Options

Field	Description
Alarm Areas	<p>Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>

Advanced Options

Field	Description
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Man-</p>

Field	Description
	<p>ager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="821 611 1419 921" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
Previous Block	<p>Displays the name of the previous (upstream) tag.</p> <p>Valid Entries</p> <p>None. This is a read-only field.</p>
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p>

Field	Description
	Text, up to 80 characters.

PG Tag

This tag contains the following details:

General

Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <pre>~ ` + ^ : ? " * = { } . , ; ? @</pre>


Field	Description
	<p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.


Programming Statements

Field	Description
PGM Statement 0 -19	<p>Lets you enter the commands and arguments for the Program tag. Use the Browse (...) button to select from a list of valid commands.</p> <p>Valid Entries</p> <p>The list box can include up to 20 programming statements, each containing up to 44 alphanumeric characters in length.</p>

Alarm Options

Field	Description
Alarm Areas	Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with

Field	Description
	<p>the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>
Enable Alarm	<p>Lets you enable or disable alarming for this tag.</p> <p>When you enable alarming, the tag generates alarms allowing objects in your operator displays to show alarm conditions, and enabling other tags to detect alarms from the tag.</p> <div data-bbox="821 793 1419 1104" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: The entire chain can be affected when you disable alarms for a tag. In addition, for both the Digital and Analog Alarm tags, this field is ignored when you enable the Alarm Suspend field.</p> </div>
Priority	<p>Lets you specify the alarm priority for a tag. If the priority is equal or greater than the SCADA node's alarm priority, iFIX sends the alarm to all the alarm destinations enabled for this node. However, if the priority is less than the SCADA node's alarm priority, the alarm is automatically acknowledged and filtered out so that it does not appear in your alarm destinations. However, the alarm does appear in Data links configured to display current and latched alarms.</p> <p>Valid Entries</p> <p>INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL</p>

Field	Description
	<div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: To report tag alarms, the appropriate alarm areas must be assigned to each of the alarm services enabled in the System Configuration Utility (SCU). </div>
Shelve Enable	Select this check box to enable Alarm Shelving for the tag.
Shelve Policy	Select an alarm shelving policy from the drop-down list.

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.
Collect	Lets you select if the tag is set for collection by the Proficy Historian collector. Select Enabled to allow the tag to be collected by the collector.
Collection Interval	Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector. Valid Entries Must be entered in 100 ms intervals. The default value is 5000ms. Example 1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.

Field	Description
Collection Offset	<p>Used with the collection interval to schedule collection of data from a tag.</p> <p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p> <p>If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.</p>
Time Resolution	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Collector Deadband	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p>


Field	Description
	Select Disabled to prevent the tag from being compressed.
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>
Compression Time-out (ms)	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p> <p>Any numeric value.</p>


E-Signature

Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag.

Field	Description
	<ul style="list-style-type: none"> • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>

Advanced Options

Field	Description
Startup Mode	<p>Lets you select the tag's mode on startup. In Automatic mode, the tag receives data from the I/O driver, OPC server, or OPC UA server. In Manual mode, the tag receives data from the operator, scripts, recipes, or Program blocks.</p>
Initial Scan	<p>Lets you select whether the tag is initially placed on or off scan.</p> <p>Click On Scan to place the tag on scan as soon as the Scan, Alarm, and Control (SAC) program starts or when the database is loaded. Click Off Scan to place the tag on scan by a Program block, an Event Action tag, a script, an operator entry in a Data link, or an Easy Database Access program.</p>
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="821 1476 1419 1787" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
Previous Block	Displays the name of the previous (upstream) tag.

Field	Description
	<p>Valid Entries</p> <p>None. This is a read-only field.</p>
Next Block	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div data-bbox="824 562 1421 829" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: In a Statistical Data tag, the Next Block field specifies the tag name of the downstream Statistical Control tag. No other tag type is valid.</p> </div>
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Process by Exception	<p>Enables exception-based processing for the tag.</p>
Scan Time	<p>Lets you specify how often the Scan, Alarm, and Control (SAC) program processes the tag and any tags chained to it.</p> <p>Valid Entries</p>

Field	Description
	<ul style="list-style-type: none"> • 0 (one shot processing) • 0.05 to .95 in .05 increments (subsecond scan times) • 1 to 60 in 1 second increments • 1M to 60M in 1 minute increments • 1H to 24H in 1 hour increments <p>Example</p> <p>0.15 specifies a 15-subsecond scan time. 5 specifies a 5-second scan time, 10M specifies a 10-minute scan time, 16H specifies a 16-hour scan time.</p>
Phase At	<p>Lets you specify how long the Scan, Alarm, and Control (SAC) program delays in scanning the tag. When the tag has a second or subsecond scan time, SAC offsets the initial scan by the phase time when iFIX starts or when the database is reloaded. When the tag has a scan time of 1 minute or longer, SAC offsets the initial scan starting at midnight.</p> <p>Valid Entries</p> <p>Depends on the scan time. If the scan time is in hours, the phase must be in hours:minutes. If the scan time is in minutes, the phase must be in minutes:seconds. If the scan time is in seconds, the phase must be in seconds. If the scan time is in subseconds, the phase must be in subseconds.</p>

PI2 Tag

This tag contains the following details:

General

Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <p>~ ` + ^ : ? " * = { } . , ; ? @</p> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p>

Field	Description
	A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

Limits and Scaling

Field	Description
Low Limit	Used to clamp PV, SP and internal calculations (unless NO CLAMP is set). Should match the output EGU of the upstream block. NOTE: inverted EGU range is not supported by the PI2 block. The HI egu must be larger than the LO egu.
High Limit	Used to clamp PV, SP and internal calculations (unless NO CLAMP is set). Should match the output EGU of the upstream block. NOTE: inverted EGU range is not supported by the PI2 block. The HI egu must be larger than the LO egu.
Units	For display purposes.
Low Output Limit	Used to rescale and clamp the computed value for output. Inverted EGU range is not allowed; HI must be larger than LO.
High Output Limit	Used to rescale and clamp the computed value for output. Inverted EGU range is not allowed; HI must be larger than LO.
Output EGU Tag	For display purposes.

Tuning Constants and Algorithm


Field	Description
Proportional Band	The proportional band tuning constant from 0 to 10,000.
Integral Time	Minutes per repeat - the Integral tuning constant from 0 to 99. Entering 0 disables reset (integral).
Rate Limit	In minutes - the Derivative tuning constant from 0 to 20. Entering 0 disables rate (derivative).
Gap Action	Suppresses control action if the error is less than this limit. That is, the output remains constant if the error drops below the GAP limit. This is can be used to suppress valve chatter. The default is 0.0.
Derivative Filter	If enabled, a first order filter is applied to the derivative term to limit response to high frequency noise. The derivative filter is suppressed if the RATE is less than $10 * \text{the block scan time}$.


Setpoint Limits and Options

Field	Description
Low Setpoint Clamp	Values outside the limits entered by the operator or sent by other blocks, other applications or CDA programs will be rejected and an error will be returned. Remote setpoints outside this range will be accepted but will be clamped to these limits. Note there is no visible indication that clamping of a remote SP has occurred.
High Setpoint Clamp	Values outside the limits entered by the operator or sent by other blocks, other applications or CDA programs will be rejected and an error will be returned. Remote setpoints outside this range will be accepted but will be clamped to these limits. Note there is no visible indication that clamping of a remote SP has occurred.

Field	Description
Setpoint Tag	The value of the remote block.
Balance	If enabled, then SP is set to PV on any MANL to AUTO transition. This has no effect on remote set-points.
Direct Action	If enabled then the Proportional band is multiplied by -1.
Force Remote	If enabled then a MANL to AUTO transition will also force the Setpoint from Local to Remote (if a remote SP is used).

Alarm Options

Field	Description
Alarm Areas	<p>Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>
Enable Alarm	<p>Lets you enable or disable alarming for this tag.</p> <p>When you enable alarming, the tag generates alarms allowing objects in your operator displays to show alarm conditions, and enabling other tags to detect alarms from the tag.</p> <div data-bbox="824 1577 1421 1892" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note:</p> <p>The entire chain can be affected when you disable alarms for a tag. In addition, for both the Digital and Analog Alarm tags, this field is ignored when you enable the Alarm Suspend field.</p> </div>

Field	Description
Priority	<p>Lets you specify the alarm priority for a tag. If the priority is equal or greater than the SCADA node's alarm priority, iFIX sends the alarm to all the alarm destinations enabled for this node. However, if the priority is less than the SCADA node's alarm priority, the alarm is automatically acknowledged and filtered out so that it does not appear in your alarm destinations. However, the alarm does appear in Data links configured to display current and latched alarms.</p> <p>Valid Entries</p> <p>INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL</p> <div data-bbox="820 934 1421 1207" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note: To report tag alarms, the appropriate alarm areas must be assigned to each of the alarm services enabled in the System Configuration Utility (SCU).</p> </div>
Shelve Enable	Select this check box to enable Alarm Shelving for the tag.
Shelve Policy	Select an alarm shelving policy from the drop-down list.
Alarm in Manual	If enabled, then the deviation alarm is checked when the block is in MANL as well as when it is in AUTO.
Dead Band	Once a deviation alarm is generated the difference must drop to the DEVIATION LIMIT - DEADBAND for the alarm to clear.
Deviation Value	If the difference between SP and PV exceeds this limit a DEV alarm is generated. Entering 0.0 disables alarming.



E-Signature


Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p>

Field	Description
	<p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>

Advanced Options

Field	Description
Startup Mode	<p>Lets you select the tag's mode on startup. In Automatic mode, the tag receives data from the I/O driver, OPC server, or OPC UA server. In Manual mode, the tag receives data from the operator, scripts, recipes, or Program blocks.</p>
Feedback Tag	<p>Can be the tag of another block (typically an Analog Input) which directly reads back the value of the actuator. If present, the feedback value will override the internally saved previous output. The next output will be the sum of the P, I and D terms added to the feedback rather than added to the previous output.</p>
Reverse Output	<p>If enabled the output is inverted just before being passed downstream. A computed output of 100% is passed downstream as 0 and an output of 0% is passed downstream as 100. Note that the selection of this field does not affect the display or entry of the output. Example: enable output reverse. Enter a manual output of 25. Any read of the output by any application will return 25. However a downstream block such as AO or TR will see a value of 75.</p>
No Initial Clamp	<p>Indicates if the blocks internal calculations should be clamped at the hi/lo egu range. If clamp is disabled then the 'previous' output is allowed to fall</p>

Field	Description
	below the lo limit. This can be useful in proportional only control.
Clear Output	Indicates if the OUTPUT should be cleared when the chain is placed ON SCAN.
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="820 961 1419 1276" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
Previous Block	<p>Displays the name of the previous (upstream) tag.</p> <p>Valid Entries</p> <p>None. This is a read-only field.</p>
Next Block	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div data-bbox="820 1661 1419 1812" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: In a Statistical Data tag, the Next Block field specifies the tag name of the down-</p> </div>

Field	Description
	 stream Statistical Control tag. No other tag type is valid.
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>

PID Tag


This tag contains the following details:


General


Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p>

Field	Description
	<p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <p>~ ` + ^ : ? " * = { } . , ; ? @</p> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

Limits and Scaling

Field	Description
<p>Low Limit</p>	<p>Lets you enter the tag's minimum value.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information.</p> </div> <p>In a Calculation or Signal Select tag, if the output of the tag is 10 and the Low Limit is 15, the tag clamps the value at 15. You must enter a Low Limit of 10 or less to output a value of 10.</p> <p>If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the Low Limit field.</p> <p>If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
<p>High Limit</p>	<p>Lets you enter the tag's maximum value.</p> <p>Valid Entries</p>



Field	Description
	<p>You can enter a high limit in one of three formats:</p> <ul style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information.</p> </div> <p>In a Calculation or a Signal Select tag, if the output of the tag is 150 and the High Limit is 100, the tag clamps the value at 100. You must enter a High Limit of 150 or more to output a value of 150.</p> <p>If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the High Limit field.</p> <p>If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
EGU Tag	<p>Lets you enter text describing the engineering units range.</p> <p>Valid Entries</p> <p>Up to 33 characters.</p>

Field	Description
	<p>Example</p> <p>Kilograms per square meter, Liters per minute, degrees Celsius.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: This entry does not affect the calculation or function of any variables in iFIX. It is used strictly as a display label to identify the engineering units.</p> </div>
<p>Low Output Limit</p>	<p>Displays the low limit for the output of the PID block.</p> <p>Valid Entries</p> <p>The lowest value the controlled variable (the Analog Output or another PID block) can have should be specified in the Low Limit field.</p> <p>This entry can be different from the PID block's Low Limit. In addition, your I/O driver, OPC UA server, or OPC server can impose certain limitations on the engineering units range. If necessary, consult your I/O driver, OPC UA server, or OPC server manual for more information.</p>
<p>High Output Limit</p>	<p>Displays the high limit for the output of the PID block.</p> <p>Valid Entries</p> <p>The highest value the controlled variable (the Analog Output or another PID block) can have should be specified in the High Limit field.</p> <p>This entry can be different from the PID block's High Limit. In addition, your I/O driver, OPC UA server, or OPC server can impose certain limita-</p>

Field	Description
	tions on the engineering units range. If necessary, consult your I/O driver, OPC UA server, or OPC server manual for more information.
Output EGU Tag	Enter a label for the limits in the Units field, such as PCT or DEG.

Tuning Constants and Algorithms

Field	Description
Proportional band	<p>Lets you enter a tuning constant, equal to the inverse of the proportional gain multiplied by 100%.</p> <p>Valid Entries</p> <p>A value from 1.00 to 10,000.00 percent. This value is the range of input deviation that drives the controller's output through its full range. The change in controller output is inversely proportional to the proportional band.</p>
Integral Time	<p>Lets you enter an integral time constant.</p> <p>Valid Entries</p> <p>A value from 0.000 to 99.000 minutes per repeat.</p> <p>For large capacity control systems, the reset tuning parameter provides a temporary change in the PID output, even if the deviation is small and the rate of deviation is fast. When the rate of change measurement becomes steady, the Reset is adjusted internally to zero (0) in the PID algorithm. Decreasing the reset time tends to minimize overshoot of the set point, but it will then take longer to reach the set point.</p>

Field	Description
	<div data-bbox="820 262 1416 531" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;">  Note: If you apply a reset tuning parameter to a small-capacity process loop, oscillations in the PID output could develop, causing damage to process control equipment. </div>
Derivative Time	<p>Lets you enter a derivative time constant measured in minutes per repeat.</p> <p>Valid Entries</p> <p>A value from 0 to 20 minutes. Enter values smaller than a minute in decimals.</p> <p>Example</p> <p>Enter a value of .25 (of a minute) to represent a rate of 15 seconds. The tag automatically adjusts internally to account for the scan cycle of the loop.</p> <div data-bbox="820 1087 1416 1444" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;">  Tip: The rate value provides a backwards push to rapidly changing controller output. Usually this value is between 0 and 1. This can help minimize overshoot and stabilize the loop. Higher values can result in loop instability. </div>
Alpha-rate Factor	<p>Lets you specify a derivative mode filter for algorithm tuning. This value specifies the amount of derivative filtering that is applied to the algorithm. The Alpha value performs a filtering of the derivative portion of the output signal and is a first order lag term.</p> <p>Valid Entries</p>

Field	Description
	A value in the range of 0.0 to 0.125. The default value of 0.0 disables this function.
Beta-rate Factor	<p>Lets you specify a proportional action constant for algorithm tuning. This value serves as a multiplier for the proportional term.</p> <p>Valid Entries</p> <p>A value in the range of 0.0 to 1.0. The default value of 1.0 provides normal proportional action. A value of 0.0 disables the function.</p>
Gamma-reset Factor	<p>Lets you specify a derivative action constant for algorithm tuning. This value specifies the action of the derivative component of the algorithm. Therefore, a value in this field can limit the amount of derivative action performed in the algorithm.</p> <p>Valid Entries</p> <p>A value in the range of 0.0 to 1.0. The default value of 1.0 provides normal derivative action. A value of 0.0 disables the function.</p>


Setpoint Limits and Options

Field	Description
Dead band value	<p>Lets you enter the maximum fluctuation the tag accepts without re-issuing an alarm. As long as the fluctuation is within the dead band range, the tag issues an alarm once, eliminating nuisance alarms. Once the alarm falls below the dead band and then exceeds the alarm limits, the tag generates another alarm.</p> <p>Valid Entries</p> <p>Numeric value within the EGU range.</p>

Field	Description
	<p>Example</p> <p>If the High alarm limit is 80 and the dead band is 5, the tag does not re-issue an alarm after the one while the current value fluctuates between 75 and 85.</p>
Deviation value	<p>Generates an alarm if the difference between the set point value and the measured value (Analog Input tag) is greater than the entry in this field. The deviation is the difference between the set point value and the process variable:</p> <p>DEVIATION = SET POINT VALUE - PROCESS VARIABLE</p> <p>Valid Entries</p> <p>The appropriate value, in engineering units. Use 0 to disable the deviation alarm.</p>
Gap Action	<p>Compensates for controller error by providing a dead band in updates to the PID algorithm. The Gap Action value prevents the PID tag from sending out adjustments to the process if the deviation from the set point value is within this dead band.</p> <p>Valid Entries</p> <p>Enter a value that represents the dead band range. If the change is within this range, the deviation is set to 0 (zero).</p>
Low Setpoint Clamp	<p>Lets you specify the lowest acceptable value for the PID set point. Any changes to the set point must fall within the Low and High Clamp values. This limit applies to set points derived from cascades, ramps, and other control loop strategies in addition to the set point values entered by an operator.</p>

Field	Description
	<p>Valid Entries</p> <p>The minimum value for the set point.</p>
High Setpoint Clamp	<p>Lets you specify the highest acceptable value for the PID set point. Any changes to the set point must fall within the High and Low Clamp values. This limit applies to set points derived from cascades, ramps, and other control loop strategies in addition to the set point values entered by an operator.</p> <p>Valid Entries</p> <p>The maximum value for the set point.</p>
Setpoint Tag	<p>Lets you specify the desired value of a controlled variable.</p> <p>Valid Entries</p> <p>Blank (to let operators type a fixed value from a Data link, this set point is a local set point.) or an Analog Input tag, in the tag.field format. (F_CV). By controlling the set point from an Analog Input tag, the PID block retrieves the current value through the Scan, Alarm, and Control (SAC) program. This set point is called a remote set point.</p> <p>When the set point is displayed through a Data link (using the TV1 field), it appears with either an L or an R to the right of the set point value to indicate a local or remote set point.</p> <p>In addition, the entry in the set point value field is in effect any time the database is saved and reloaded, even if an operator has manually changed the value.</p>

Alarm Options

Field	Description
Alarm Areas	<p>Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>
Enable Alarm	<p>Lets you enable or disable alarming for this tag.</p> <p>When you enable alarming, the tag generates alarms allowing objects in your operator displays to show alarm conditions, and enabling other tags to detect alarms from the tag.</p> <div style="border: 1px solid #00a0c0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note:</p> <p>The entire chain can be affected when you disable alarms for a tag. In addition, for both the Digital and Analog Alarm tags, this field is ignored when you enable the Alarm Suspend field.</p> </div>
Shelve Enable	Select this check box to enable Alarm Shelving for the tag.
Shelve Policy	Select an alarm shelving policy from the drop-down list.

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.

Field	Description
Collect	<p>Lets you select if the tag is set for collection by the Proficy Historian collector.</p> <p>Select Enabled to allow the tag to be collected by the collector.</p>
Collection Interval	<p>Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector.</p> <p>Valid Entries</p> <p>Must be entered in 100 ms intervals. The default value is 5000ms.</p> <p>Example</p> <p>1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.</p>
Collection Offset	<p>Used with the collection interval to schedule collection of data from a tag.</p> <p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p> <p>If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.</p>

Field	Description
Time Resolution	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Collector Deadband	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>
Compression Time-out (ms)	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p>

Field	Description
	<p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p> <p>Any numeric value.</p>

E-Signature



Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>

Field	Description
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>

Advanced Options

Field	Description
Reverse Output	Inverts the output of the tag.
Startup Mode	<p>Lets you select the tag's mode on startup. In Automatic mode, the tag receives data from the I/O driver, OPC server, or OPC UA server. In Manual mode, the tag receives data from the operator, scripts, recipes, or Program blocks.</p>
Transfer Status	<p>Lets you control how the PID tag reacts during a transition between automatic and manual modes.</p> <p>Valid Entries</p>

Field	Description
	<ul style="list-style-type: none"> • Track – Tracks the position of the output when the tag is in Manual mode. When there is a transition back to Automatic mode, the PID tag calculates the output using the current and previous error terms. • Balance – Enables the Scan, Alarm, and Control (SAC) program to provide a bumpless transfer when the PID tag changes from Manual to Automatic mode. Error is removed from the process by balancing the set point to make it equal to the process measurement. • None – Disables the transfer options and is the default selection.
Feedback Tag	<p>Lets you control how the PID tag reacts during a transition between automatic and manual modes.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • Track – Tracks the position of the output when the tag is in Manual mode. When there is a transition back to Automatic mode, the PID tag calculates the output using the current and previous error terms. • Balance – Enables the Scan, Alarm, and Control (SAC) program to provide a bumpless transfer when the PID tag changes from Manual to Automatic mode. Error is removed from the process by balancing the set point to make it equal to the process measurement. • None – Disables the transfer options and is the default selection.
Derivative Time	

Field	Description
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="824 751 1419 1066" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
Previous Block	<p>Displays the name of the previous (upstream) tag.</p> <p>Valid Entries</p> <p>None. This is a read-only field.</p>
Next Block	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div data-bbox="824 1453 1419 1724" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: In a Statistical Data tag, the Next Block field specifies the tag name of the downstream Statistical Control tag. No other tag type is valid.</p> </div>
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Imple-</p>

Field	Description
	<p>menting Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>

RB Tag

This tag contains the following details:


General


Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p>



Field	Description
	<p>Tag names can also include dashes (-), under-scores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <pre>~ ` + ^ : ? " * = { } . , ; ? @</pre> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

Limits and Scaling

Field	Description
Low Limit	<p>Lets you enter the tag's minimum value.</p> <p>Valid Entries</p>


Field	Description
	<ul style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;">  Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. </div> <p>In a Calculation or Signal Select tag, if the output of the tag is 10 and the Low Limit is 15, the tag clamps the value at 15. You must enter a Low Limit of 10 or less to output a value of 10.</p> <p>If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the Low Limit field.</p> <p>If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
High Limit	<p>Lets you enter the tag's maximum value.</p> <p>Valid Entries</p> <p>You can enter a high limit in one of three formats:</p> <ul style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999.

Field	Description
	<ul style="list-style-type: none"> • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;">  Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. </div> <p>In a Calculation or a Signal Select tag, if the output of the tag is 150 and the High Limit is 100, the tag clamps the value at 100. You must enter a High Limit of 150 or more to output a value of 150.</p> <p>If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the High Limit field.</p> <p>If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
Units	<p>Lets you enter text describing the engineering units range.</p> <p>Valid Entries</p> <p>Up to 33 characters.</p> <p>Example</p> <p>Kilograms per square meter, Liters per minute, degrees Celsius,</p>

Field	Description
	<div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: This entry does not affect the calculation or function of any variables in iFIX. It is used strictly as a display label to identify the engineering units. </div>
Ratio Value	<p>Multiplies the value from the upstream block by a constant.</p> <p>Valid Entries</p> <p>The constant by which you want to multiply the incoming signal. The default value is 1.</p>
Bias Value	<p>Lets you specify the bias constant for the ratio bias equation. The bias allows the value to be adjusted by up to +/- half the engineering units span.</p> <p>Valid Entries</p> <p>A numeric constant or a tag and field name pair in the format tag.field that represents the value you want to add to the incoming signal.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: The range of the bias constant is a function of the engineering units range. Therefore, if you want the bias to use the same EGU range as the incoming signal, enter the EGU range of the upstream block into the Ratios Bias's EGU fields. </div>
Offset Value	<p>Lets you specify the value you want to subtract from the upstream tag's incoming signal.</p> <p>Valid Entries</p>

Field	Description
	A numeric constant or a tag and field name pair in the format tag.field.

Alarm Options

Field	Description
Alarm Areas	<p>Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>
Enable Alarm	<p>Lets you enable or disable alarming for this tag.</p> <p>When you enable alarming, the tag generates alarms allowing objects in your operator displays to show alarm conditions, and enabling other tags to detect alarms from the tag.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note:</p> <p>The entire chain can be affected when you disable alarms for a tag. In addition, for both the Digital and Analog Alarm tags, this field is ignored when you enable the Alarm Suspend field.</p> </div>

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.
Collect	Lets you select if the tag is set for collection by the Proficy Historian collector.

Field	Description
	<p>Select Enabled to allow the tag to be collected by the collector.</p>
<p>Collection Interval</p>	<p>Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector.</p> <p>Valid Entries</p> <p>Must be entered in 100 ms intervals. The default value is 5000ms.</p> <p>Example</p> <p>1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.</p>
<p>Collection Offset</p>	<p>Used with the collection interval to schedule collection of data from a tag.</p> <p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p> <p>If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.</p>
<p>Time Resolution</p>	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>

Field	Description
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Collector Deadband	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>
Compression Time-out (ms)	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p>


Field	Description
	<p>Valid Entries</p> <p>Any numeric value.</p>


E-Signature

Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>

Field	Description
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>

Advanced Options

Field	Description
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="820 1417 1421 1732" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
Previous Block	<p>Displays the name of the previous (upstream) tag.</p> <p>Valid Entries</p>

Field	Description
	None. This is a read-only field.
Next Block	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div data-bbox="820 487 1419 751" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: In a Statistical Data tag, the Next Block field specifies the tag name of the downstream Statistical Control tag. No other tag type is valid.</p> </div>
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>

RM Tag


This tag contains the following details:


General


Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <pre>~ ` + ^ : ? " * = { } . , ; ? @</pre> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p>

Field	Description
	A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

Limits and Scaling

Field	Description
Low Limit	<p>Lets you enter the tag's minimum value.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information.</p> </div> <p>In a Calculation or Signal Select tag, if the output of the tag is 10 and the Low Limit is 15, the tag</p>


Field	Description
	<p>clamps the value at 15. You must enter a Low Limit of 10 or less to output a value of 10.</p> <p>If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the Low Limit field.</p> <p>If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
<p>High Limit</p>	<p>Lets you enter the tag's maximum value.</p> <p>Valid Entries</p> <p>You can enter a high limit in one of three formats:</p> <ul style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information.</p> </div> <p>In a Calculation or a Signal Select tag, if the output of the tag is 150 and the High Limit is 100, the tag clamps the value at 100. You must enter a High Limit of 150 or more to output a value of 150.</p>



Field	Description
	<p>If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the High Limit field.</p> <p>If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
Units	<p>Lets you enter text describing the engineering units range.</p> <p>Valid Entries</p> <p>Up to 33 characters.</p> <p>Example</p> <p>Kilograms per square meter, Liters per minute, degrees Celsius,</p> <div data-bbox="820 1024 1419 1291" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: This entry does not affect the calculation or function of any variables in iFIX. It is used strictly as a display label to identify the engineering units.</p> </div>
Low Operator Limit	<p>Lets you specify the lowest operational target value accepted from a SETTARG command in a Program tag or from an operator entry into a Data link.</p> <p>Valid Entries</p> <p>A value between the Low and High EGU fields. If appropriate, you can use the Low EGU for this value.</p>
High Operator Limit	<p>Lets you specify the highest operational target value accepted from a SETTARG command in a Program tag or from an operator entry into a Data link.</p>



Field	Description
	<p>Valid Entries</p> <p>A value between the Low and High EGU fields. If appropriate, you can use the High EGU for this value.</p>
<p>Scan Time</p>	<p>Lets you specify how often the Scan, Alarm, and Control (SAC) program processes the tag and any tags chained to it.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • 0 (one shot processing) • 0.05 to .95 in .05 increments (subsecond scan times) • 1 to 60 in 1 second increments • 1M to 60M in 1 minute increments • 1H to 24H in 1 hour increments <p>Example</p> <p>0.15 specifies a 15-subsecond scan time. 5 specifies a 5-second scan time, 10M specifies a 10-minute scan time, 16H specifies a 16-hour scan time.</p>
<p>Phase At</p>	<p>Lets you specify how long the Scan, Alarm, and Control (SAC) program delays in scanning the tag. When the tag has a second or subsecond scan time, SAC offsets the initial scan by the phase time when iFIX starts or when the database is reloaded. When the tag has a scan time of 1 minute or longer, SAC offsets the initial scan starting at midnight.</p> <p>Valid Entries</p> <p>Depends on the scan time. If the scan time is in hours, the phase must be in hours:minutes. If the scan time is in minutes, the phase must be in min-</p>



Field	Description
	utes:seconds. If the scan time is in seconds, the phase must be in seconds. If the scan time is in subseconds, the phase must be in subseconds.

Ramp Definitions

Field	Description
Target Value 1	<p>Lets you specify the value you want the tag to reach.</p> <p>Valid Entries</p> <p>A value or a tag and field name (uses the current value of another block).</p> <div data-bbox="821 884 1414 1373" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note:</p> <p>You can use a Program tag to set the target values of a Ramp tag. SETTARG sets the value of the first target value, SETTARG2 sets the value of the second target value, and SETTARG3 sets the value of the third target value. If a target value that is outside the Ramp tag's EGU range, iFIX clamps the value to the block's Low and High Operator Limits.</p> </div>
Ramp Rate 1	<p>Lets you specify the increments at which the current value is modified until reaching the target value for each stage.</p> <p>Valid Entries</p> <p>A value based on hours. Use 0.00 to prevent the execution of the ramp stage.</p> <p>Example</p>

Field	Description
	<p>To use a rate of 1 degree per second, enter 3600, for 3600 degrees per hour. The precision, or number of decimal points, of the ramp rate is the same as the Low and High EGU range.</p>
<p>Hold Time 1</p>	<p>Lets you specify how long the Ramp tag waits after reaching the target value and before continuing on to the next stage.</p> <p>Valid Entries</p> <p>A value based on hours. The default hold time is 0.000. The maximum hold time is 1000 hours.</p> <p>Example</p> <p>To hold for one hour, enter 1.000.</p> <div data-bbox="824 953 1419 1268" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: You can use a Program tag to set the hold time of a Ramp block. SETTIME sets the ramp time for the first stage and SET-TIME2 sets the ramp time for the second stage.</p> </div>
<p>Target Value 2</p>	<p>Lets you specify the value you want the tag to reach.</p> <p>Valid Entries</p> <p>A value or a tag and field name (uses the current value of another block).</p> <div data-bbox="824 1591 1419 1877" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: You can use a Program tag to set the target values of a Ramp tag. SETTARG sets the value of the first target value, SET-TARG2 sets the value of the second target value, and SETTARG3 sets the value of</p> </div>

Field	Description
	 the third target value. If a target value that is outside the Ramp tag's EGU range, iFIX clamps the value to the block's Low and High Operator Limits.
Ramp Rate 2	<p>Lets you specify the increments at which the current value is modified until reaching the target value for each stage.</p> <p>Valid Entries</p> <p>A value based on hours. Use 0.00 to prevent the execution of the ramp stage.</p> <p>Example</p> <p>To use a rate of 1 degree per second, enter 3600, for 3600 degrees per hour. The precision, or number of decimal points, of the ramp rate is the same as the Low and High EGU range.</p>
Hold Time 2	<p>Lets you specify how long the Ramp tag waits after reaching the target value and before continuing on to the next stage.</p> <p>Valid Entries</p> <p>A value based on hours. The default hold time is 0.000. The maximum hold time is 1000 hours.</p> <p>Example</p> <p>To hold for one hour, enter 1.000.</p> <div data-bbox="820 1591 1421 1791" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;">  Note: You can use a Program tag to set the hold time of a Ramp block. SETTIME sets the ramp time for the first stage and SET- </div>

Field	Description
	<div style="border: 1px solid #0070C0; border-radius: 5px; padding: 5px;">  TIME2 sets the ramp time for the second stage. </div>
<p>Target Value 3</p>	<p>Lets you specify the value you want the tag to reach.</p> <p>Valid Entries</p> <p>A value or a block and field name (uses the current value of another tag).</p> <div style="border: 1px solid #0070C0; border-radius: 5px; padding: 5px; margin-top: 10px;">  Note: You can use a Program tag to set the target values of a Ramp tag. SETTARG sets the value of the first target value, SETTARG2 sets the value of the second target value, and SETTARG3 sets the value of the third target value. If a target value that is outside the Ramp tag's EGU range, iFIX clamps the value to the block's Low and High Operator Limits. </div>
<p>Ramp Rate 3</p>	<p>Lets you specify the increments at which the current value is modified until reaching the target value for each stage.</p> <p>Valid Entries</p> <p>A value based on hours. Use 0.00 to prevent the execution of the ramp stage.</p> <p>Example</p> <p>To use a rate of 1 degree per second, enter 3600, for 3600 degrees per hour. The precision, or number of decimal points, of the ramp rate is the same as the Low and High EGU range.</p>

Alarm Options

Field	Description
Alarm Areas	<p>Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.
Collect	<p>Lets you select if the tag is set for collection by the Proficy Historian collector.</p> <p>Select Enabled to allow the tag to be collected by the collector.</p>
Collection Interval	<p>Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector.</p> <p>Valid Entries</p> <p>Must be entered in 100 ms intervals. The default value is 5000ms.</p> <p>Example</p> <p>1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.</p>
Collection Offset	Used with the collection interval to schedule collection of data from a tag.

Field	Description
	<p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p> <p>If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.</p>
Time Resolution	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Collector Deadband	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>


Field	Description
<p>Compression Type</p>	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>
<p>Compression Time-out (ms)</p>	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p> <p>Any numeric value.</p>


E-Signature

Field	Description
<p>Type</p>	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag.

Field	Description
	<ul style="list-style-type: none"> • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>

Advanced Options

Field	Description
Startup Mode	<p>Lets you select the tag's mode on startup. In Automatic mode, the tag receives data from the I/O driver, OPC server, or OPC UA server. In Manual mode, the tag receives data from the operator, scripts, recipes, or Program blocks.</p>
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="821 1066 1419 1381" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
Previous Block	<p>Displays the name of the previous (upstream) tag.</p> <p>Valid Entries</p> <p>None. This is a read-only field.</p>
Next Block	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p>

Field	Description
	<div style="border: 1px solid #0070C0; border-radius: 5px; padding: 10px; background-color: #E6F2FF;">  Note: In a Statistical Data tag, the Next Block field specifies the tag name of the downstream Statistical Control tag. No other tag type is valid. </div>
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>

SC Tag

This tag contains the following details:

General


Field	Description
Tag Name	Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.


Field	Description
	<p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <p>~ ` + ^ : ? " * = { } . , ; ? @</p> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.

Field	Description
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

SC Specifics and Constants


Field	Description
Add to Block	<p>Lets you pass the adjustment value of the Statistical Control block to the specified tag. The tag can add this adjustment to:</p> <ul style="list-style-type: none"> • The current value of the Analog Output block. • The target value of the PID block. • The target value of the Ramp block. <p>Valid Entries</p> <p>The tag and field name pair in tag.field format.</p>
Recalculate Status	<p>Re-computes the upstream Statistical Data tag's upper and lower control limits after adjusting a value and the delay time expires.</p> <p>Valid Entries</p> <p>Select the check box to recalculate the limits. Clear the check box to maintain previously set control limits.</p>
Alarm Suppression	<p>Suppresses the generation of alarms until the Statistical Data tag processes a new set of groups.</p> <p>Valid Entries</p> <p>Select the check box to suppress alarms. Clear the check box to generate alarms.</p>

Field	Description
Track Messages	<p>Sends a message to the Statistical Control block's active alarm destinations each time the tag adjusts a value.</p> <p>Valid Entries</p> <p>Select the check box to send messages. Clear the check box to suppress messages.</p>
Show Calc Adjustment	<p>Lets you display the latest calculated adjustment in the iFIX WorkSpace.</p> <p>Valid Entries</p> <p>Select the check box to display the adjustment through a Data link, using block.A_CV as the entry. Clear the check box to prevent this display.</p> <div data-bbox="821 961 1419 1360" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Enabling the Show Calculation option allows you to display the calculated adjustments in a picture. You can use these values to adjust your tuning constants more precisely. If you want to see only the values the block sends to its downstream block, use A_SENT in the Data link.</p> </div>
Slope Constant	<p>Multiplies the slope of the plotted XBAR values found in the upstream Statistical Data tag by the specified value. The slope constant is a floating-point scaling factor.</p> <p>Valid Entries</p> <p>A value between -99,999.0 and 900,000.0</p>
Deviation Constant	<p>Multiplies the average deviation of XBAR values from XBARBAR by the specified value. The deviation constant is a floating-point scaling factor.</p>

Field	Description
	<p>Valid Entries</p> <p>The appropriate floating point value.</p>
<p>Delay Time</p>	<p>Lets you specify the length of time the Statistical Control tag remains dormant. This period lets the process settle after receiving the adjusted value. During this time, the Scan, Alarm, and Control (SAC) program suppresses alarms in the upstream Statistical Data tag and the Statistical Control tag makes no further adjustments.</p> <p>Valid Entries</p> <p>A time in seconds between 1 and 32767.</p> <div data-bbox="824 884 1419 1056" style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Tip: Allow time for the upstream block to read at least one full set of data groups.</p> </div>

Alarm Options

Field	Description
<p>Alarm Areas</p>	<p>Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>
<p>Enable Alarm</p>	<p>Lets you enable or disable alarming for this tag.</p> <p>When you enable alarming, the tag generates alarms allowing objects in your operator displays to show alarm conditions, and enabling other tags to detect alarms from the tag.</p>

Field	Description
	<div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: The entire chain can be affected when you disable alarms for a tag. In addition, for both the Digital and Analog Alarm tags, this field is ignored when you enable the Alarm Suspend field. </div>

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.
Collect	Lets you select if the tag is set for collection by the Proficy Historian collector. Select Enabled to allow the tag to be collected by the collector.
Collection Interval	Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector. Valid Entries Must be entered in 100 ms intervals. The default value is 5000ms. Example 1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.
Collection Offset	Used with the collection interval to schedule collection of data from a tag. Valid Entries

Field	Description
	<p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p> <p>If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.</p>
Time Resolution	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Collector Deadband	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p>

Field	Description
	<p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>
<p>Compression Time-out (ms)</p>	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p> <p>Any numeric value.</p>


E-Signature

Field	Description
<p>Type</p>	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.

Field	Description
Remember User	Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.
Exempt Alarm Ack	Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>

Advanced Options

Field	Description
Startup Mode	Lets you select the tag's mode on startup. In Automatic mode, the tag receives data from the I/O driver, OPC server, or OPC UA server. In Manual

Field	Description
	<p>mode, the tag receives data from the operator, scripts, recipes, or Program blocks.</p>
<p>Security Areas</p>	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="821 856 1419 1167" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
<p>Alarm Field 1</p>	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
<p>Alarm Field 2</p>	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p>

Field	Description
	Text, up to 80 characters.

SD Tag

This tag contains the following details:



General



Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <pre>~ ` + ^ : ? " * = { } . , ; ? @</pre>


Field	Description
	<p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.



Limits and Scaling



Field	Description
Low Limit	<p>Lets you enter the tag's minimum value.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary).

Field	Description
	<div data-bbox="824 260 1424 529" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. </div> <p data-bbox="816 562 1424 730">In a Calculation or Signal Select tag, if the output of the tag is 10 and the Low Limit is 15, the tag clamps the value at 15. You must enter a Low Limit of 10 or less to output a value of 10.</p> <p data-bbox="816 766 1424 892">If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the Low Limit field.</p> <p data-bbox="816 928 1424 1054">If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
High Limit	<p data-bbox="816 1081 1424 1117">Lets you enter the tag's maximum value.</p> <p data-bbox="816 1150 1424 1186">Valid Entries</p> <p data-bbox="816 1222 1424 1257">You can enter a high limit in one of three formats:</p> <ul data-bbox="880 1306 1424 1705" style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div data-bbox="824 1747 1424 1894" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: The I/O driver can set certain limitations on the engineering units range. Consult </div>

Field	Description
	<div data-bbox="820 260 1417 373" style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px;">  your I/O driver manual for more information. </div> <p data-bbox="820 411 1417 575">In a Calculation or a Signal Select tag, if the output of the tag is 150 and the High Limit is 100, the tag clamps the value at 100. You must enter a High Limit of 150 or more to output a value of 150.</p> <p data-bbox="820 617 1417 737">If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the High Limit field.</p> <p data-bbox="820 779 1417 898">If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
Units	<p data-bbox="820 930 1417 1003">Lets you enter text describing the engineering units range.</p> <p data-bbox="820 1045 971 1077">Valid Entries</p> <p data-bbox="820 1119 1057 1150">Up to 33 characters.</p> <p data-bbox="820 1192 922 1224">Example</p> <p data-bbox="820 1266 1406 1339">Kilograms per square meter, Liters per minute, degrees Celsius,</p> <div data-bbox="820 1371 1417 1633" style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px;"> <p data-bbox="836 1392 1385 1612">  Note: This entry does not affect the calculation or function of any variables in iFIX. It is used strictly as a display label to identify the engineering units. </p> </div>
Scan Qualifier	<p data-bbox="820 1665 1417 1875">Lets you specify a digital tag that controls when the Statistical Data block samples the block specified in the Input Tag field. When the digital tag transitions from open to closed, the Statistical Data tag samples the input tag.</p>


Field	Description
	<p>Valid Entries</p> <p>The name of a block with an F_CV field that returns a 1 or 0.</p>
Input Score	<p>Lets you specify the input source of the Statistical Data tag.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • The name of an Analog Alarm, Analog Input, Analog Output, or Calculation tag. • Blank, to indicate input from an operator or from an Easy Database Access program.
Groups	<p>Lets you specify the input source of the Statistical Data tag.</p> <p>Valid Entries</p> <p>The name of an Analog Alarm, Analog Input, Analog Output, or Calculation tag.</p> <p>Blank, to indicate input from an operator or from an Easy Database Access program.</p>
Observations/group	<p>Lets you specify the number of observations that the Statistical Data tag makes per group.</p> <p>Valid Entries</p> <p>A value from 1 to 25.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note: You can change the Observations/Group field with a Data link in the iFIX WorkSpace. After making your changes, turn the Statistical Data tag off scan and then back on scan to restart it with the new values.</p> </div>


Field	Description
Wait time	<p>Lets you specify the time, in seconds, that the Statistical Data tag pauses between the last observation of one group and the first observation of the next group.</p> <p>Valid Entries</p> <p>A value from 0 to 32767 seconds.</p> <div data-bbox="821 621 1419 793" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: The wait time is valid only when the tag is in Automatic mode.</p> </div>
CTL limit calc mode	<p>Lets you specify the calculation mode of control, warning, and specification limits for XBAR, S, and R charts.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • Startup – Instructs the tag not to recalculate limits for XBAR, R, and S charts after start-up. This option is the default selection. Operators can change these limits through Data links in the WorkSpace at any time. • Always – Lets the tag update values for the limits on a moving average basis. The block overwrites operator entries as soon as the group is updated. • Never – Lets the tag calculate limits for XBAR, R, and S charts based upon defaults. Operators can enter values at any time before or after startup. The block does not overwrite these values. <div data-bbox="821 1726 1419 1875" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: If you choose to manually input limit values, verify that the values are very close to</p> </div>

Field	Description
	<div style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px;">  the ones the block would calculate. Otherwise, the validity of statistical alarms and control charts is questionable. </div>
XBB calc mode	<p>Specifies the calculation mode of XBARBAR, SBAR, and RBAR values.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • Startup – Instructs the tag not to recalculate alarm limits, XBARBAR, RBAR, and SBAR values after startup. This option is the default selection. Operators can change these limits with Data links in the WorkSpace at any time. • Always – Lets the tag update values for alarm limits on a moving average basis. The tag overwrites operator entries as soon as the group is updated. • Never – Lets the tag calculate alarm limits, XBAR, R and S values based upon defaults. Operators can enter values at any time before or after startup. The tag does not overwrite these values. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: If you choose to manually input limit values, verify that the values are very close to the ones the block would calculate. Otherwise, the validity of statistical alarms and control charts is questionable. </div>
Process by Exception	Enables exception-based processing for the tag.
Scan Time	Lets you specify how often the Scan, Alarm, and Control (SAC) program processes the tag and any tags (blocks) chained to it.

Field	Description
	<p>Valid Entries</p> <ul style="list-style-type: none"> • 0 (one shot processing) • 0.05 to .95 in .05 increments (subsecond scan times) • 1 to 60 in 1 second increments • 1M to 60M in 1 minute increments • 1H to 24H in 1 hour increments <p>Example</p> <p>0.15 specifies a 15-subsecond scan time. 5 specifies a 5-second scan time, 10M specifies a 10-minute scan time, 16H specifies a 16-hour scan time.</p>
Phase At	<p>Lets you specify how long the Scan, Alarm, and Control (SAC) program delays in scanning the tag. When the tag has a second or subsecond scan time, SAC offsets the initial scan by the phase time when iFIX starts or when the database is reloaded. When the tag has a scan time of 1 minute or longer, SAC offsets the initial scan starting at midnight.</p> <p>Valid Entries</p> <p>Depends on the scan time. If the scan time is in hours, the phase must be in hours:minutes. If the scan time is in minutes, the phase must be in minutes:seconds. If the scan time is in seconds, the phase must be in seconds. If the scan time is in subseconds, the phase must be in subseconds.</p>

Alarm Options

Field	Description
Alarm Areas	<p>Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>
Enable Alarm	<p>Lets you enable or disable alarming for this tag.</p> <p>When you enable alarming, the tag generates alarms allowing objects in your operator displays to show alarm conditions, and enabling other tags to detect alarms from the tag.</p> <div data-bbox="821 1005 1419 1318" style="border: 1px solid #00a0c0; border-radius: 10px; padding: 10px; background-color: #e6f2f8;"> <p> Note:</p> <p>The entire chain can be affected when you disable alarms for a tag. In addition, for both the Digital and Analog Alarm tags, this field is ignored when you enable the Alarm Suspend field.</p> </div>
Priority	<p>Lets you specify the alarm priority for a tag. If the priority is equal or greater than the SCADA node's alarm priority, iFIX sends the alarm to all the alarm destinations enabled for this node. However, if the priority is less than the SCADA node's alarm priority, the alarm is automatically acknowledged and filtered out so that it does not appear in your alarm destinations. However, the alarm does appear in Data links configured to display current and latched alarms.</p> <p>Valid Entries</p>

Field	Description
	<p>INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL</p> <div data-bbox="824 380 1419 646" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: To report tag alarms, the appropriate alarm areas must be assigned to each of the alarm services enabled in the System Configuration Utility (SCU).</p> </div>
Shelve Enable	Select this check box to enable Alarm Shelving for the tag.
Shelve Policy	Select an alarm shelving policy from the drop-down list.
N point control limit alarm on XBAR	Generates an alarm when the XBAR value of the specified number of groups is outside the control limits (+ 3 sigma).
Number of groups for control limit alarm	Enter the appropriate number of groups in the On Groups column so the tag can send alarms to its alarm areas.
N point warning limit alarm on XBAR	Generates an alarm when the XBAR values of the specified number of consecutive groups are outside the control warning limits (control warning limit is 2/3 of the upper or lower control limit values, which is + 2 sigma.)
Number of groups for warning limit alarm	Enter the appropriate number of groups in the On Groups column so the tag can send alarms to its alarm areas.
N point specification limit on XBAR	Generates an alarm if the specified number of groups are outside the range of the control limits. Generates an alarm if the specified number of groups are outside the range of the control limits.

Field	Description
Number of groups for the specification limit alarm	Enter the appropriate number of groups in the On Groups column so the tag can send alarms to its alarm areas.
N point Alarm on RBAR	Generates an alarm when the range of the specified number of groups is outside the standard deviation control limits.
Number of groups for the RBAR alarm	Enter the appropriate number of groups in the On Groups column so the tag can send alarms to its alarm areas.
N point Alarm on SBAR	Generates an alarm when the specified number of groups is outside the standard deviation control limits.
Number of groups for the SBAR alarm	Enter the appropriate number of groups in the On Groups column so the tag can send alarms to its alarm areas.
Trend of runs alarm	Generates an alarm when the specified number of groups is outside the standard deviation control limits.
Number of groups for the Trend alarm	Enter the appropriate number of groups in the On Groups column so the tag can send alarms to its alarm areas.
Lenth of runs alarm	Generates an alarm if the specified number of consecutive groups are above or below XBARBAR.
Number of groups for the Length Alarm	Enter the appropriate number of groups in the On Groups column so the tag can send alarms to its alarm areas.
N Point Critical Runs on XBAR	Generates an alarm if the Statistical Data Block observes less than the specified number of crossings of the mean by serial observations.
Number of groups for critical runs alarm	Enter the appropriate number of groups in the On Groups column so the tag can send alarms to its alarm areas.

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.
Collect	<p>Lets you select if the tag is set for collection by the Proficy Historian collector.</p> <p>Select Enabled to allow the tag to be collected by the collector.</p>
Collection Interval	<p>Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector.</p> <p>Valid Entries</p> <p>Must be entered in 100 ms intervals. The default value is 5000ms.</p> <p>Example</p> <p>1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.</p>
Collection Offset	<p>Used with the collection interval to schedule collection of data from a tag.</p> <p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p>

Field	Description
	If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.
Time Resolution	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Collector Deadband	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>

Field	Description
Compression Time-out (ms)	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p> <p>Any numeric value.</p>



E-Signature


Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if</p>

Field	Description
	this tag requires electronic signatures for data entry.
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>

Advanced Options

Field	Description
Startup Mode	Lets you select the tag's mode on startup. In Automatic mode, the tag receives data from the I/O driver, OPC server, or OPC UA server. In Manual mode, the tag receives data from the operator, scripts, recipes, or Program blocks.
Initial Scan	<p>Lets you select whether the tag is initially placed on or off scan.</p> <p>Click On Scan to place the tag on scan as soon as the Scan, Alarm, and Control (SAC) program starts</p>

Field	Description
	<p>or when the database is loaded. Click Off Scan to place the tag on scan by a Program block, an Event Action tag, a script, an operator entry in a Data link, or an Easy Database Access program.</p>
<p>Security Areas</p>	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="821 947 1419 1260" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
<p>Previous Block</p>	<p>Displays the name of the previous (upstream) tag.</p> <p>Valid Entries</p> <p>None. This is a read-only field.</p>
<p>Next Block</p>	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div data-bbox="821 1646 1419 1795" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: In a Statistical Data tag, the Next Block field specifies the tag name of the down-</p> </div>

Field	Description
	 stream Statistical Control tag. No other tag type is valid.
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>

SQD Tag


This tag contains the following details:


General

Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p>

Field	Description
	<p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <p>~ ` + ^ : ? " * = { } . , ; ? @</p> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

Data Definitions

Field	Description
Tag 1 - 20	<p>Enter up to 20 tag and field name pairs that store data from your relational database or from the iFIX process database. Depending on the Tag.Field direction (In or Out), the SQL system task either reads the value of the tag and field and writes it to a relational database, or reads a selected value from the relational database and writes to it to the specified tag and field.</p> <p>The field entry can be any ASCII (A_) or floating point (F_) field available to the tag. In addition, you can also use SQL keywords.</p>
Direction 1 - 20	<p>Determines the data transfer direction between the process database and the relational database for up to 20 tag and field name pairs. Valid entries are:</p> <ul style="list-style-type: none"> • A SQL keyword, In (to receive data from the relational database), or Out (to send data to the relational database) • A single SQL command can use both directions. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note: Most SQL commands delete, select, update, or insert values in a relational database. When selecting values from a relational database, the tag sets the value of each data point's Direction field to In. When inserting or updating rows, or in a SELECT command with a "where" clause, the tag sends process data values to the relational database. In these cases, the tag</p> </div>

Field	Description
	 sets the value of each data point's Direction field to Out.
Reset Status Tag 1 - 20	<p>Allows you to clear numeric or text data in the process database each time the SQL Trigger and Data tag chain executes. This field provides better control over monitoring the actual data retrieved by the SQL Data tag each time the SQL Trigger tag executes. Valid entries are:</p> <ul style="list-style-type: none"> • None – Prevents the tag from resetting the field. • Blank – Removes any text data in the field. This setting is commonly used when you are retrieving text from tag Description fields. • Zero – Writes a numeric zero to the specified tag and field.

Alarm Options

Field	Description
Alarm Areas	<p>Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.

Field	Description
Collect	<p>Lets you select if the tag is set for collection by the Proficy Historian collector.</p> <p>Select Enabled to allow the tag to be collected by the collector.</p>
Collection Interval	<p>Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector.</p> <p>Valid Entries</p> <p>Must be entered in 100 ms intervals. The default value is 5000ms.</p> <p>Example</p> <p>1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.</p>
Collection Offset	<p>Used with the collection interval to schedule collection of data from a tag.</p> <p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p> <p>If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.</p>

Field	Description
Time Resolution	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Collector Deadband	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>
Compression Time-out (ms)	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p>

Field	Description
	<p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p> <p>Any numeric value.</p>



E-Signature

Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>

Field	Description
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>

Advanced Options

Field	Description
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p>

Field	Description
	<div data-bbox="834 275 1421 571" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;">  Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area. </div>
Previous Block	Displays the name of the previous (upstream) tag. Valid Entries None. This is a read-only field.
Next Block	Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button. <div data-bbox="834 961 1421 1234" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;">  Note: In a Statistical Data tag, the Next Block field specifies the tag name of the downstream Statistical Control tag. No other tag type is valid. </div>
Alarm Field 1	Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information. Valid Entries Text, up to 80 characters.
Alarm Field 2	Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.

Field	Description
	<p>Valid Entries</p> <p>Text, up to 80 characters.</p>

SQT Tag

This tag contains the following details:


General

Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p>

Field	Description
	<p>~ ` + ^ : ? " * = { } . , ; ? @</p> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

SQL Definitions and Date Filters

Field	Description
SQL Command Name	<p>Lets you specify the SQL command alias that SQL System Task uses when the SQL Trigger tag runs. SQL commands are stored in an SQL Library Table. Each row in the table consists of a SQL command and an alias. If the Database ID field is specified, that database ID will be used to seek the SQL LIB and SQL name for the SQL command, and the Database ID configured inside this block will only be used for the DATA portion of the SQL database and not for the SQL LIB portion.</p> <p>Valid Entries</p> <p>An alias up to eight characters. Lowercase letters are automatically capitalized.</p>

Field	Description
Database ID	<p>Lets you specify the relational database (data source) to use for the current block. If you specify a Database ID here, it will be used to seek the SQL LIB and SQL name for the SQL command, and override the block configuration related to the location of the SQL LIB.</p>
Event Start Date	<p>Lets you specify when the SQL Trigger tag executes.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • 1-31 – Specifies a day of the month to trigger the tag. • Sun, Mon, Tue, Wed, Thu, Fri, Sat – Specifies a day of the week to trigger the tag. • All – Runs the block based upon the Event Time or Event Tag fields. • None – Disables all time and tag based events. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note: If the start date is later than the end date, the block runs through the end of the week or month and into the next week or month. When you specify All or None for the Start Date, the End Date should always be None.</p> </div>
Event End Date	<p>Lets you specify when the SQL Trigger tag stops. Use the following guidelines when defining the End Date:</p>


Field	Description
	<ul style="list-style-type: none"> • If the start date is later than the end date, the tag runs through the end of the week or month and into the next week or month. • If you do not define an end time or period, the tag executes once on the start time. • If you do not define the end time, but you define a period, the tag uses an implied end time of 24:00:00 (midnight). <p>Valid Entries</p> <ul style="list-style-type: none"> • 1-31 – Specifies a day of the month the tag stops. • Sun, Mon, Tue, Wed, Thu, Fri, Sat – Specifies a day of the week the tag stops. • None – Specifies the tag stops on the same day or date it started on.
Process By Exception	Enables exception-based processing for the tag.
Scan Time	<p>Lets you specify how often the Scan, Alarm, and Control (SAC) program processes the tag and any tags chained to it.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • 0 (one shot processing) • 0.05 to .95 in .05 increments (subsecond scan times) • 1 to 60 in 1 second increments • 1M to 60M in 1 minute increments • 1H to 24H in 1 hour increments
Phase At	<p>Lets you specify how long the Scan, Alarm, and Control (SAC) program delays in scanning the tag. When the tag has a second or subsecond scan time, SAC offsets the initial scan by the phase time when iFIX starts or when the database is re-loaded. When the tag has a scan time of 1 minute</p>

Field	Description
	<p>or longer, SAC offsets the initial scan starting at midnight.</p> <p>Valid Entries</p> <p>Depends on the scan time. If the scan time is in hours, the phase must be in hours:minutes. If the scan time is in minutes, the phase must be in minutes:seconds. If the scan time is in seconds, the phase must be in seconds. If the scan time is in subseconds, the phase must be in subseconds.</p>

Time and Block Events

Field	Description
Event Start Time	<p>Lets you specify a time between 00:00:00 to 23:59:59 to indicate the time that the SQL Trigger tag executes. Use the following guidelines when defining the Start Time field:</p> <ul style="list-style-type: none"> • If you leave the Start Time field blank, the SQL Trigger block does not run based on time. • If you specify a start time without an end time, the block triggers once at the specified time on every day within the date range specified in the Start Date and End Date fields. • If you define a start and end time and do not define an Event Period, the block triggers based on its scan time.
Event End Time	<p>Lets you specify a time between 00:00:00 and 23:59:59 to indicate the time that the SQL Trigger tag stops. Use the following guidelines when defining the Start Time field:</p>


Field	Description
	<ul style="list-style-type: none"> • If you do not enter an end time, the tag automatically stops at midnight. • If you define the Start Time and Event Period but not the End Time, then the tag executes once every day within the date range of Start Date and End Date fields. The tag assumes the End Time is the end of the day.
Event Period	<p>Lets you specify a time between 00:00:00 and 23:59:59 to indicate how often the SQL Trigger tag triggers after reaching the start time. Use the following guidelines when defining the period:</p> <ul style="list-style-type: none"> • If you enter a time less than the tag's scan time, the tag triggers every time it is scanned; otherwise, the tag triggers according to the period time. • If you enter start and end times, the tag triggers at the start time and every event period after that until reaching the end time. Then, the tag stops until reaching the start time again, provided the day or date is still within the range specified in the Start Date and End Date fields. • Once a period starts, it always finishes even if it spills over into a day that is not within the range specified in the Start Date and End Date fields.
Event Tag	<p>Lets you specify the tag and field name pair that activates the SQL Trigger tag. You can configure the tag to trigger when the value of the specified event tag changes from zero to a non-zero value, from a non-zero value to zero, or simply changes value.</p> <p>Valid Entries</p>


Field	Description
	<ul style="list-style-type: none"> • If you specify an ASCII field (A_), you can only trigger the tag by a Change Of Value event type. • If you specify a floating point field (F_), you can trigger the tag by either a Change Of Value, High to Low, or Low To High event type. Low is defined as 0 and a High is defined as non-zero, so you can use an analog tag. • To trigger a tag by an event tag and type, the current day or date must be within the date range specified by the Start and End Date fields.
Confirmation Tag	<p>Lets you enter an analog or digital tag (where low is 0 and high is non-zero) to allow your process hardware to confirm the execution of the SQL Trigger tag. The process hardware does this by examining the value of the tag and field entered into this field. When the value is non-zero, the process hardware assumes the execution is complete. In addition, you can use this field in conjunction with the Event Tag and Event Type fields to establish synchronization between the device and the SQL Trigger tag.</p> <div style="border: 1px solid #FFD700; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Important: This field requires a floating point (F_) field. Furthermore, the tag only uses the specified tag when the Low to High or High to Low Event Type is selected.</p> </div> <p>Example</p> <p>Assume your process hardware sets a value, holds all values for the process database, and then waits for the Confirm Tag's value to change. By setting</p>

Field	Description
	<p>a value, the process hardware triggers the SQL Trigger tag. This causes the SQL System task to process the downstream SQL Data blocks and write a non-zero value in the Confirm Tag. In response, the process hardware clears the value it set and resumes processing.</p> <p>If you do not have your hardware configured to reset the Confirmation tag, it will reset to 0 anyway when the EVENT tag triggers the SQT to set it back to the default position.</p>
Event Type	<p>Lets you specify the type of event that starts the SQL Trigger tag in conjunction with the Event Tag field. Select one of the following options:</p> <ul style="list-style-type: none"> • Change of Value – Starts the tag when the value of the Event Tag field changes. To use this event type, enter any ASCII (A_) or floating point (F_) field as the Event Tag. For example, A_CUALM. • Low to High – Starts the tag any time value of the Event Tag field changes from zero to non-zero. To use this event type, enter a floating point field (F_) as the Event Tag. For example: F_CV. • High to Low – Starts the tag any time the value of the Event Tag field changes from non-zero to zero. To use this event type, enter a floating point field (F_) as the Event Tag. For example, F_CV.

Alarm Options

Field	Description
Alarm Areas	Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an

Field	Description
	<p>item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>
<p>Enable Alarm</p>	<p>Lets you enable or disable alarming for this tag.</p> <p>When you enable alarming, the tag generates alarms allowing objects in your operator displays to show alarm conditions, and enabling other tags to detect alarms from the tag.</p> <div data-bbox="820 835 1419 1150" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: The entire chain can be affected when you disable alarms for a tag. In addition, for both the Digital and Analog Alarm tags, this field is ignored when you enable the Alarm Suspend field.</p> </div>
<p>Priority</p>	<p>Lets you specify the alarm priority for a tag. If the priority is equal or greater than the SCADA node's alarm priority, iFIX sends the alarm to all the alarm destinations enabled for this node. However, if the priority is less than the SCADA node's alarm priority, the alarm is automatically acknowledged and filtered out so that it does not appear in your alarm destinations. However, the alarm does appear in Data links configured to display current and latched alarms.</p> <p>Valid Entries</p> <p>INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL</p>

Field	Description
	 Note: To report tag alarms, the appropriate alarm areas must be assigned to each of the alarm services enabled in the System Configuration Utility (SCU).
Shelve Enable	Select this check box to enable Alarm Shelving for the tag.
Shelve Policy	Select an alarm shelving policy from the drop-down list.

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.
Collect	Lets you select if the tag is set for collection by the Proficy Historian collector. Select Enabled to allow the tag to be collected by the collector.
Collection Interval	Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector. Valid Entries Must be entered in 100 ms intervals. The default value is 5000ms. Example 1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.

Field	Description
Collection Offset	<p>Used with the collection interval to schedule collection of data from a tag.</p> <p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p> <p>If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.</p>
Time Resolution	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Collector Deadband	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p>


Field	Description
	Select Disabled to prevent the tag from being compressed.
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>
Compression Time-out (ms)	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p> <p>Any numeric value.</p>


E-Signature


Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag.


Field	Description
	<ul style="list-style-type: none"> • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>

Advanced Options

Field	Description
Startup Mode	<p>Lets you select the tag's mode on startup. In Automatic mode, the tag receives data from the I/O driver, OPC server, or OPC UA server. In Manual mode, the tag receives data from the operator, scripts, recipes, or Program blocks.</p>
Initial Scan	<p>Lets you select whether the tag is initially placed on or off scan.</p> <p>Click On Scan to place the tag on scan as soon as the Scan, Alarm, and Control (SAC) program starts or when the database is loaded. Click Off Scan to place the tag on scan by a Program block, an Event Action tag, a script, an operator entry in a Data link, or an Easy Database Access program.</p>
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="821 1476 1419 1787" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
Previous Block	Displays the name of the previous (upstream) tag.

Field	Description
	<p>Valid Entries</p> <p>None. This is a read-only field.</p>
<p>Next Block</p>	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div data-bbox="821 558 1419 827" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: In a Statistical Data tag, the Next Block field specifies the tag name of the downstream Statistical Control tag. No other tag type is valid.</p> </div>
<p>Alarm Field 1</p>	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
<p>Alarm Field 2</p>	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
<p>Table Mode</p>	<p>Lets you specify the SELECT mode of the SQL Data tag. Select one of the following options:</p>

Field	Description
	<ul style="list-style-type: none"> • Single Row – The SQL Data block accepts one row from a SELECT command. • Multiple Rows – The SQL Data block accepts more than one row from a SELECT command and write values to individual blocks. • Array Mode – The SQL Data block accepts more than one row from a SELECT command and write values to register blocks. Be sure you specify a register block for each column returned from the SELECT command.
Command Type	<p>Choose one of the following:</p> <ul style="list-style-type: none"> • SQL Command – Lets you select a SQL command as the command type. Once selected, enter the name of the SQL command in the SQL Name field on the Basic tab. • Procedure – Lets you select a SQL command as the command type. Once selected, enter the name of the SQL command in the SQL Name field on the Basic tab.
Backup Data	<p>Lets you enable the SQL Trigger tag to back up process data if it detects a problem with the relational database.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: The SQL software option does not back up a SELECT command's request because there is no means of accurately determining when the connection to the server can be re-established. Since the SELECT command inserts values into the process database, the process of inserting must be performed on a controlled and predictable ba-</p> </div>

Field	Description
	 sis, not whenever the connection is re-established.
Rows	Lets you specify the starting row, depending on the Select Parameters mode: <ul style="list-style-type: none"> • Single Row – Enter the starting row of the resulting data if multiple rows are returned. • Multiple Rows – Enter the starting row of the resulting data. • Array Mode – Enter the number of rows returned.
Cols	Lets you specify the number of columns configured in the SELECT command.

SS Tag

This tag contains the following details:



General



Field	Description
Tag Name	Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs. <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal</p>

Field	Description
	<p>databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), under-scores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <p>~ ` + ^ : ? " * = { } . , ; ? @</p> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	<p>The tag type. Display-only field.</p>
Current Value	<p>The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.</p>

I/O Addressing

Field	Description
I/O Driver	<p>Lets you select an I/O driver, OPC server, or OPC UA server for the tag. The selected driver or serv-</p>


Field	Description
	<p>er enables the tag to communicate with process hardware on the plant floor.</p> <p>Before you can select an I/O driver, OPC server, or OPC UA server you must install it and add it to the available ones in the SCU.</p>
I/O Address	<p>Lets you enter the location in the process hardware where data for this tag is saved and where output is sent.</p> <p>Valid Entries</p> <p>Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations.</p> <div data-bbox="821 926 1419 1236" style="border: 1px solid black; border-radius: 10px; padding: 10px; background-color: #fff9c4;"> <p> CAUTION: Do not assign the same I/O address to tags when using exception-based and time-based processing. Doing so will cause the exception-based tags to occasionally miss a value.</p> </div> <div data-bbox="821 1268 1419 1713" style="border: 1px solid black; border-radius: 10px; padding: 10px; background-color: #fff9c4;"> <p> CAUTION: Configuration Hub currently does not do I/O address validations before publish. If you enter an invalid IO address into a tag or generate an invalid I/O address via the model and substitutions, the publish may fail to set the IO address into the active database, and your invalid IO address will be removed.</p> </div>
Signal Conditioning	<p>Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p>



Field	Description
	<div data-bbox="820 262 1414 531" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: Signal conditioning and linear scaling cannot be applied simultaneously. If you select a value for Signal Conditioning verify that Linear Scaling is not selected. </div> <p data-bbox="820 562 971 594">Valid Entries</p> <p data-bbox="820 636 1409 709">Depends on your driver or server. Refer to your driver or server manual for more information.</p>
H/W Options	<p data-bbox="820 741 1404 867">Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p> <div data-bbox="820 898 1414 1167" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: Signal conditioning and linear scaling cannot be applied simultaneously. If you select a value for Signal Conditioning verify that Linear Scaling is not selected. </div> <p data-bbox="820 1199 971 1230">Valid Entries</p> <p data-bbox="820 1272 1409 1346">Depends on your driver or server. Refer to your driver or server manual for more information.</p>
Process by Exception	<p data-bbox="820 1377 1386 1409">Enables exception-based processing for the tag.</p>
Scan Time	<p data-bbox="820 1440 1404 1566">Lets you specify how often the Scan, Alarm, and Control (SAC) program processes the tag and any tags (blocks) chained to it.</p> <p data-bbox="820 1598 971 1629">Valid Entries</p> <ul data-bbox="881 1682 1382 1848" style="list-style-type: none"> • 0 (one shot processing) • 0.05 to .95 in .05 increments (subsecond scan times) • 1 to 60 in 1 second increments



Field	Description
	<ul style="list-style-type: none"> • 1M to 60M in 1 minute increments • 1H to 24H in 1 hour increments <p>Example</p> <p>0.15 specifies a 15-subsecond scan time. 5 specifies a 5-second scan time, 10M specifies a 10-minute scan time, 16H specifies a 16-hour scan time.</p>
Phase At	<p>Lets you specify how long the Scan, Alarm, and Control (SAC) program delays in scanning the tag. When the tag has a second or subsecond scan time, SAC offsets the initial scan by the phase time when iFIX starts or when the database is reloaded. When the tag has a scan time of 1 minute or longer, SAC offsets the initial scan starting at midnight.</p> <p>Valid Entries</p> <p>Depends on the scan time. If the scan time is in hours, the phase must be in hours:minutes. If the scan time is in minutes, the phase must be in minutes:seconds. If the scan time is in seconds, the phase must be in seconds. If the scan time is in subseconds, the phase must be in subseconds.</p>


Limits and Inputs

Field	Description
Low Limit	<p>Lets you enter the tag's minimum value.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999.

Field	Description
	<ul style="list-style-type: none"> • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;">  Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. </div> <p>In a Calculation or Signal Select tag, if the output of the tag is 10 and the Low Limit is 15, the tag clamps the value at 15. You must enter a Low Limit of 10 or less to output a value of 10.</p> <p>If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the Low Limit field.</p> <p>If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
High Limit	<p>Lets you enter the tag's maximum value.</p> <p>Valid Entries</p> <p>You can enter a high limit in one of three formats:</p> <ul style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38.

Field	Description
	<ul style="list-style-type: none"> Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div data-bbox="821 478 1419 743" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information.</p> </div> <p>In a Calculation or a Signal Select tag, if the output of the tag is 150 and the High Limit is 100, the tag clamps the value at 100. You must enter a High Limit of 150 or more to output a value of 150.</p> <p>If you want to display a value of 1.236 from the Calculation tag, you must enter three or more decimal places in the High Limit field.</p> <p>If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
Units	<p>Lets you enter text describing the engineering units range.</p> <p>Valid Entries</p> <p>Up to 33 characters.</p> <p>Example</p> <p>Kilograms per square meter, Liters per minute, degrees Celsius,</p> <div data-bbox="821 1745 1419 1892" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note: This entry does not affect the calculation or function of any variables in iFIX. It is</p> </div>

Field	Description
	<p> used strictly as a display label to identify the engineering units.</p>
<p>Scale Enabled</p>	<p>Lets you enable or disable scaling for this tag.</p> <p>Enabling scaling allows the system to convert the data received from input sensors to designated data ranges.</p> <p> Note: Linear scaling and signal conditioning cannot be applied simultaneously. If you select Linear Scaling, verify that Signal Conditioning is set to NONE.</p> <p>Example</p> <p>Scaling allows conversion of temperature data received in Fahrenheit to an output which uses Celsius values.</p>
<p>Input 1-6</p>	<p>Lets you specify where the Signal Select tag receives input data. You can specify any EGU range for the Signal Select tag's inputs. However, if the value of an input is outside the specified EGU range, the tag clamps it to the highest or lowest acceptable value.</p> <p>Valid Entries</p> <p>A tag and field name pair in the format tag.field or a numeric constant. Named blocks must exist in the same database as your Signal Select tag. An input entry may also include zero (0). If you select Low in the Selected Mode field, the Signal Select tag processes a zero entry if that entry is the lowest value entered in all Input fields.</p>

Field	Description
	<div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: Input 1 is always the upstream tag, tied to the Signal Select tag through the upstream block's Next Block field. </div>
<p>Selection Mode</p>	<p>Lets you specify how the Signal Select tag uses its input values to calculate its output value. You can change the selected mode field with a modifiable Data link in the iFIX WorkSpace, a SETSEL command from a Program block, or an Easy Database Access program. Select one of the following options:</p> <ul style="list-style-type: none"> • Inputs 1-6 – Outputs the corresponding input number. • Average – Outputs the average of all the assigned inputs. • Good – Outputs the first good input. A good value is one that is within the tag's EGU range. • High – Outputs the highest input. • Low – Outputs the lowest input. • Sum – Outputs the sum of all the inputs. <p>Notes</p> <ul style="list-style-type: none"> • An Input number, for example, Input 5, is usually specified when you are loading recipes and want the value from a particular input passed to the next tag when a recipe loads. • If one or more of the inputs are bad or off scan and the selected mode is Average or

Field	Description
	Sum, the Signal Select tag ignores these inputs and continues with the calculation based on the remaining ones.

Alarm Options

Field	Description
Alarm Areas	<p>Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.
Collect	<p>Lets you select if the tag is set for collection by the Proficy Historian collector.</p> <p>Select Enabled to allow the tag to be collected by the collector.</p>
Collection Interval	<p>Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector.</p> <p>Valid Entries</p> <p>Must be entered in 100 ms intervals. The default value is 5000ms.</p> <p>Example</p>

Field	Description
	<p>1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.</p>
<p>Collection Offset</p>	<p>Used with the collection interval to schedule collection of data from a tag.</p> <p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p> <p>If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.</p>
<p>Time Resolution</p>	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
<p>Collector Compression</p>	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
<p>Collector Deadband</p>	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values</p>

Field	Description
	<p>that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>
Compression Time-out (ms)	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p> <p>Any numeric value.</p>



E-Signature


Field	Description
Type	The Type of Electronic Signature:

Field	Description
	<ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electron-</p>

Field	Description
	ic Signature settings are available. By default, this check box is disabled.

Advanced Options

Field	Description
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="820 1020 1419 1331" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
Previous Block	<p>Displays the name of the previous (upstream) tag.</p> <p>Valid Entries</p> <p>None. This is a read-only field.</p>
Next Block	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div data-bbox="820 1719 1419 1869" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: In a Statistical Data tag, the Next Block field specifies the tag name of the down-</p> </div>

Field	Description
	 stream Statistical Control tag. No other tag type is valid.
Alarm Field 1	Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information. Valid Entries Text, up to 80 characters.
Alarm Field 2	Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information. Valid Entries Text, up to 80 characters.

TDS Tag



This tag contains the following details:

General

Field	Description
Tag Name	Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs. Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it. Valid Entries

Field	Description
	<p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <p>~ ` + ^ : ? " * = { } . , ; ? @</p> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

Advanced Options

Field	Description
Previous Block	<p>Displays the name of the previous (upstream) tag.</p> <p>Valid Entries</p> <p>None. This is a read-only field.</p>
Next Block	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div data-bbox="821 709 1419 976" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: In a Statistical Data tag, the Next Block field specifies the tag name of the downstream Statistical Control tag. No other tag type is valid.</p> </div>
Mode	<p>Trigger on OPEN, CLOSE or COS.</p> <div data-bbox="821 1066 1419 1472" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: The 0 is treated as OPEN and any non-zero value is treated as CLOSE. For example a change from 0 to any other value will trigger on CLOSE. A change from any non-zero value to 0 will trigger on OPEN and a change between 0 and any non-zero value will trigger on COS.</p> </div> <p>A change between two non-zero values will not trigger COS. As mentioned elsewhere this block is generally used with Digital Inputs.</p>
Format	<p>Allows a variety of date formats to allow for different country and/or relational database needs.</p>
Separator	<p>Allows a variety of date separators to allow for different country and/or relational database needs.</p>

TM Tag


This tag contains the following details:


General


Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <pre>~ ` + ^ : ? " * = { } . , ; ? @</pre> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>

Field	Description
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

Timer and Setup Options


Field	Description
Timing Direction	Lets you increment or decrement the Timer tag value. Up is the default direction.
Target Value	<p>Lets you specify the value that triggers the following events when alarms are enabled:</p> <ul style="list-style-type: none"> • Generates an alarm. • Closes the specified digital block, if the Alarm Tag field contains an entry. • Continues counting. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note: If alarms are disabled, the block continues counting when it reaches this value.</p> </div> <p>Valid Entries</p> <p>The tag and field pair in tag.field format or a numeric value in the format ddd:hh:mm:ss, up</p>


Field	Description
	<p>to 365:23:59:59. The default target value is 365:00:00:00.</p> <p>When you enter a numeric value in the format ddd:hh:mm:ss, the tag converts the time into seconds for internal use while displaying the value you entered. Likewise, the Timer tag converts the value a tag and field pair into seconds for internal use. This feature allows the Timer tag to use the value from the another tag regardless of how it stores its value.</p>
Preset Value	<p>Lets you specify an initial value for the tag. This field also controls the value of the tag when it resets.</p> <p>Valid Entries</p> <p>The tag and field pair in tag.field format or a numeric value in the format ddd:hh:mm:ss, up to 365:23:59:59. The default target value is 000:00:00:00.</p> <div data-bbox="820 1197 1421 1417" style="border: 1px solid #00a0c0; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p> Note: If you use a tag name (tag.field) in the Preset Value field, you must check the Clear on Startup check box.</p> </div>
Clear on Startup	<p>Lets you specify whether the Timer tag retains the last value saved when you save the database, or resets its value to zero when loading the database (on system startup or using the Database Reload command).</p>


Field	Description
	<ul style="list-style-type: none"> • If you want to retain the last value saved, clear the Clear on Startup check box. • If you want to reset the counter to a specific value, select the Clear on Startup check box and specify a value in the Preset Value field. • If you want to reset the counter to zero, select the Clear on Startup check box and leave the Preset Value field blank. • If you want to use a tag in the Preset Value field, specify the tag name in the Preset Value field and select the Clear on Startup check box.
Reset Tag	<p>Lets you specify a tag that controls when to reset the Timer block. When the specified block's value changes from zero to one, the Timer tag resets to the value in the Preset Value field and clears any alarms.</p> <p>Valid Entries</p> <p>Any of the following tag types:</p> <ul style="list-style-type: none"> • Digital Alarm • Digital Input • Digital Output • Boolean <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note: Placing the upstream block off scan stops the Timer tag. When the upstream block is placed on scan again, the Timer tag restarts as defined by the Clear on Startup field.</p> </div>
Hold Tag	<p>Lets you specify an optional digital tag that temporarily suspends Timer tag counting when the</p>

Field	Description
	<p>hold tag's value changes from zero to one. When the value changes from one to zero, the tag resumes counting.</p> <p>Valid Entries</p> <p>A tag name with the F_CV field.</p>

Alarm Options

Field	Description
Alarm Areas	<p>Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>
Enable Alarm	<p>Lets you enable or disable alarming for this tag.</p> <p>When you enable alarming, the tag generates alarms allowing objects in your operator displays to show alarm conditions, and enabling other tags to detect alarms from the tag.</p> <div data-bbox="824 1388 1419 1698" style="border: 1px solid #00a0c0; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p> Note:</p> <p>The entire chain can be affected when you disable alarms for a tag. In addition, for both the Digital and Analog Alarm tags, this field is ignored when you enable the Alarm Suspend field.</p> </div>
Priority	<p>Lets you specify the alarm priority for a tag. If the priority is equal or greater than the SCADA node's alarm priority, iFIX sends the alarm to all the alarm destinations enabled for this node. However, if</p>

Field	Description
	<p>the priority is less than the SCADA node's alarm priority, the alarm is automatically acknowledged and filtered out so that it does not appear in your alarm destinations. However, the alarm does appear in Data links configured to display current and latched alarms.</p> <p>Valid Entries</p> <p>INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL</p> <div data-bbox="820 745 1421 1018" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: To report tag alarms, the appropriate alarm areas must be assigned to each of the alarm services enabled in the System Configuration Utility (SCU).</p> </div>
Shelve Enable	Select this check box to enable Alarm Shelving for the tag.
Shelve Policy	Select an alarm shelving policy from the drop-down list.
Alarm Contact Mode	<p>Lets you specify when to open the digital tag specified in the Alarm Contact field. Select one of the following options:</p> <ul style="list-style-type: none"> • Acknowledge – Opens the digital tag when the operator acknowledges the alarm. This mode is the default. • Return – Opens the digital tag when the alarm is cleared. • All Clear – Opens the digital tag when the alarm is acknowledged and cleared. • Never – Does not open the digital tag.
Alarm Contact Tag	Lets you specify a digital tag that closes when the Timer tag reaches the value specified in the Tar-

Field	Description
	<p>get Value field. If the digital tag controls an alarm, an external horn sounds when the tag closes. If the digital tag controls a digital contact, the contact closes.</p> <p>Valid Entries</p> <p>The name of a:</p> <ul style="list-style-type: none"> • Digital Output tag • Digital Input tag • Digital Alarm tag (in manual mode) <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note: Disabling alarms prevents this field from generating alarms.</p> </div>

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.
Collect	<p>Lets you select if the tag is set for collection by the Proficy Historian collector.</p> <p>Select Enabled to allow the tag to be collected by the collector.</p>
Collection Interval	<p>Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector.</p> <p>Valid Entries</p> <p>Must be entered in 100 ms intervals. The default value is 5000ms.</p> <p>Example</p>

Field	Description
	<p>1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.</p>
<p>Collection Offset</p>	<p>Used with the collection interval to schedule collection of data from a tag.</p> <p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p> <p>If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.</p>
<p>Time Resolution</p>	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
<p>Collector Compression</p>	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
<p>Collector Deadband</p>	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values</p>

Field	Description
	<p>that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>
Compression Time-out (ms)	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p> <p>Any numeric value.</p>



E-Signature


Field	Description
Type	The Type of Electronic Signature:

Field	Description
	<ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electron-</p>

Field	Description
	ic Signature settings are available. By default, this check box is disabled.

Advanced Options

Field	Description
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
Previous Block	<p>Displays the name of the previous (upstream) tag.</p> <p>Valid Entries</p> <p>None. This is a read-only field.</p>
Next Block	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: In a Statistical Data tag, the Next Block field specifies the tag name of the down-</p> </div>

Field	Description
	 stream Statistical Control tag. No other tag type is valid.
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Next Blk Processing	<p>Lets you specify when the Scan, Alarm, and Control (SAC) program processes the next tag in the chain. Select one of the following options:</p> <ul style="list-style-type: none"> • Always – Directs the Scan, Alarm, and Control (SAC) program to process the tag without waiting for the Timer block to reach its target value. Always is the default condition. • Time – Directs SAC to process the tag when the Timer tag reaches its target value.

TR Tag


This tag contains the following details:


General


Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <p>~ ` + ^ : ? " * = { } . , ; ? @</p> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p>



Field	Description
	A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

Limits and Options

Field	Description
Low Limit	<p>Lets you enter the tag's minimum value.</p> <p>Valid Entries</p> <ul style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information.</p> </div> <p>In a Calculation or Signal Select tag, if the output of the tag is 10 and the Low Limit is 15, the block</p>

Field	Description
	<p>clamps the value at 15. You must enter a Low Limit of 10 or less to output a value of 10.</p> <p>If you want to display a value of 1.236 from the Calculation block, you must enter three or more decimal places in the Low Limit field.</p> <p>If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
<p>High Limit</p>	<p>Lets you enter the tag's maximum value.</p> <p>Valid Entries</p> <p>You can enter a high limit in one of three formats:</p> <ul style="list-style-type: none"> • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information.</p> </div> <p>In a Calculation or a Signal Select tag, if the output of the block is 150 and the High Limit is 100, the block clamps the value at 100. You must enter a High Limit of 150 or more to output a value of 150.</p>

Field	Description
	<p>If you want to display a value of 1.236 from the Calculation block, you must enter three or more decimal places in the High Limit field.</p> <p>If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.</p>
Units	<p>Lets you enter text describing the engineering units range.</p> <p>Valid Entries</p> <p>Up to 33 characters.</p> <p>Example</p> <p>Kilograms per square meter, Liters per minute, degrees Celsius,</p> <div data-bbox="820 1024 1419 1293" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: This entry does not affect the calculation or function of any variables in iFIX. It is used strictly as a display label to identify the engineering units.</p> </div>
Buffer Clear Status	<p>Lets you clear the block's data buffers every time the block is put on scan.</p>
Input	<p>Lets you specify the name of the tag and field that the Trend block stores. If this field is blank, the Trend block stores the value passed by the upstream block.</p> <p>Valid Entries</p> <p>A tag and field name pair in the tag.field (F_CV) format.</p>

Field	Description
	<div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: To chain Trend tag, enter a Trend block's name followed by the F_INP field. </div>
Compression Factor	<p>Lets you increase the amount of data stored in the trend history by collecting the number of samples entered in the field, averaging them, and storing up to 80 averages in the trend history.</p> <p>Valid Entries</p> <p>A value from 1 - 255.</p> <p>Example</p> <p>If you have a scan time of 10 seconds and enter 5 in the Average Compress field, the Trend tag creates a trend history of 80 averages of 5 samples. In essence the block now represents a trend history of 400 scan periods(5 x 80), or 66.66 minutes (4000 seconds).</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: Using this field does not affect or delay the value passed by the Next Block field to the downstream block. </div>

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.
Collect	Lets you select if the tag is set for collection by the Proficy Historian collector.

Field	Description
	<p>Select Enabled to allow the tag to be collected by the collector.</p>
<p>Collection Interval</p>	<p>Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector.</p> <p>Valid Entries</p> <p>Must be entered in 100 ms intervals. The default value is 5000ms.</p> <p>Example</p> <p>1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.</p>
<p>Collection Offset</p>	<p>Used with the collection interval to schedule collection of data from a tag.</p> <p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p> <p>If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.</p>
<p>Time Resolution</p>	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>

Field	Description
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Collector Deadband	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>
Compression Time-out (ms)	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p>


Field	Description
	<p>Valid Entries</p> <p>Any numeric value.</p>


E-Signature

Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>

Field	Description
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>

Advanced Options

Field	Description
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="820 1417 1421 1722" style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
Previous Block	<p>Displays the name of the previous (upstream) tag.</p> <p>Valid Entries</p>

Field	Description
	None. This is a read-only field.
Next Block	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div data-bbox="820 485 1419 751" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: In a Statistical Data tag, the Next Block field specifies the tag name of the downstream Statistical Control tag. No other tag type is valid.</p> </div>
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>

TT Tag

This tag contains the following details:

General

Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <pre>~ ` + ^ : ? " * = { } . , ; ? @</pre> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p>

Field	Description
	A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

Alarm Options

Field	Description
Alarm Areas	<p>Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.
Collect	<p>Lets you select if the tag is set for collection by the Proficy Historian collector.</p> <p>Select Enabled to allow the tag to be collected by the collector.</p>
Collection Interval	Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector.

Field	Description
	<p>Valid Entries</p> <p>Must be entered in 100 ms intervals. The default value is 5000ms.</p> <p>Example</p> <p>1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.</p>
Collection Offset	<p>Used with the collection interval to schedule collection of data from a tag.</p> <p>Valid Entries</p> <p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p> <p>If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.</p>
Time Resolution	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p>


Field	Description
	<p>Select Disabled to prevent the tag from being compressed.</p>
<p>Collector Deadband</p>	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
<p>Compression Type</p>	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p> <p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>
<p>Compression Time-out (ms)</p>	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p> <p>Any numeric value.</p>


E-Signature



Field	Description
Type	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during</p>


Field	Description
	<p>run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>

Advanced Options

Field	Description
<p>Display Format</p>	<p>Lets you specify the number of decimal digits that appear to the right of the decimal point in an operator display.</p> <p>Valid Entries</p> <p>A value from 0 to 15, to indicate the digits of precision.</p> <div data-bbox="820 1094 1417 1358" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: From a picture, the Display field can contain 15 characters total, consisting of numbers to the left and right of a decimal point.</p> </div>
<p>Units</p>	<p>Lets you enter text describing the engineering units range.</p> <p>Valid Entries</p> <p>Up to 33 characters.</p> <p>Example</p> <p>Kilograms per square meter, Liters per minute, degrees Celsius,</p>

Field	Description
	<div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: This entry does not affect the calculation or function of any variables in iFIX. It is used strictly as a display label to identify the engineering units. </div>
Period	<p>Lets the tag calculate the correction factor to account for the difference in timing between the chain's scan time and the quantity being measured. When you enter a time in this field, the Totalizer block calculates the number of inputs and then divides the raw total by this number.</p> <p>Valid Entries</p> <p>A time in the format HH:MM:SS.</p> <p>Example</p> <p>Assume you are using the Totalizer tag to calculate the total number of gallons in a tank, and you have an Analog block measuring the flow (in gallons per minute) into the tank.</p> <p>If the Analog tag has a scan time of five seconds and is reading a flow of 50 gallons per minute, in a minute's time it will send 12 values of 50 gallons per minute to the Totalizer block. If the Totalizer block simply added these 12 values together, the result would be an erroneous raw total of 600 gallons for that one minute's time. The Per field lets the Totalizer block calculate the number of inputs and then divide the raw total by this number (that is, divide by 12):</p> <ul style="list-style-type: none"> • $\#inputs/period = period/scan\ time$ • $corrected\ total/period = raw\ total/\# inputs$

Field	Description
	<p>Therefore, if you enter 00:01:00 (one minute) in the Per field, the Totalizer block automatically divides the raw total (600 gallons) by the number of inputs (12) per period. This gives you a correct value of 50 gallons entering the tank within the minute.</p>
<p>Security Areas</p>	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="821 989 1419 1304" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
<p>Previous Block</p>	<p>Displays the name of the previous (upstream) tag.</p> <p>Valid Entries</p> <p>None. This is a read-only field.</p>
<p>Next Block</p>	<p>Displays the name of the next tag in the database chain. You can select a tag for this field by clicking the browse button.</p> <div data-bbox="821 1692 1419 1841" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: In a Statistical Data tag, the Next Block field specifies the tag name of the down-</p> </div>

Field	Description
	 stream Statistical Control tag. No other tag type is valid.
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>

TX Tag



This tag contains the following details:



General

Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p>

Field	Description
	<p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <p>~ ` + ^ : ? " * = { } . , ; ? @</p> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

I/O Addressing



Field	Description
I/O Driver	<p>Lets you select an I/O driver, OPC server, or OPC UA server for the tag. The selected driver or server enables the tag to communicate with process hardware on the plant floor.</p> <p>Before you can select an I/O driver, OPC server, or OPC UA server you must install it and add it to the available ones in the SCU.</p>
I/O Address	<p>Lets you enter the location in the process hardware where data for this tag is saved and where output is sent.</p> <p>Valid Entries</p> <p>Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations.</p> <div data-bbox="821 1096 1419 1407" style="border: 1px solid black; border-radius: 10px; padding: 10px; background-color: #fff9c4;"> <p> CAUTION: Do not assign the same I/O address to tags when using exception-based and time-based processing. Doing so will cause the exception-based tags to occasionally miss a value.</p> </div> <div data-bbox="821 1440 1419 1885" style="border: 1px solid black; border-radius: 10px; padding: 10px; background-color: #fff9c4;"> <p> CAUTION: Configuration Hub currently does not do I/O address validations before publish. If you enter an invalid IO address into a tag or generate an invalid I/O address via the model and substitutions, the publish may fail to set the IO address into the active database, and your invalid IO address will be removed.</p> </div>


Field	Description
Signal Conditioning	<p>Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p> <div data-bbox="824 432 1414 699" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Signal conditioning and linear scaling cannot be applied simultaneously. If you select a value for Signal Conditioning verify that Linear Scaling is not selected.</p> </div> <p>Valid Entries</p> <p>Depends on your driver or server. Refer to your driver or server manual for more information.</p>
H/W Options	<p>Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p> <div data-bbox="824 1068 1414 1335" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Signal conditioning and linear scaling cannot be applied simultaneously. If you select a value for Signal Conditioning verify that Linear Scaling is not selected.</p> </div> <p>Valid Entries</p> <p>Depends on your driver or server. Refer to your driver or server manual for more information.</p>
Process by Exception	<p>Enables exception-based processing for the tag.</p>
Scan Time	<p>Lets you specify how often the Scan, Alarm, and Control (SAC) program processes the tag and any tags (blocks) chained to it.</p> <p>Valid Entries</p>

Field	Description
	<ul style="list-style-type: none"> • 0 (one shot processing) • 0.05 to .95 in .05 increments (subsecond scan times) • 1 to 60 in 1 second increments • 1M to 60M in 1 minute increments • 1H to 24H in 1 hour increments <p>Example</p> <p>0.15 specifies a 15-subsecond scan time. 5 specifies a 5-second scan time, 10M specifies a 10-minute scan time, 16H specifies a 16-hour scan time.</p>
Phase At	<p>Lets you specify how long the Scan, Alarm, and Control (SAC) program delays in scanning the tag. When the tag has a second or subsecond scan time, SAC offsets the initial scan by the phase time when iFIX starts or when the database is reloaded. When the tag has a scan time of 1 minute or longer, SAC offsets the initial scan starting at midnight.</p> <p>Valid Entries</p> <p>Depends on the scan time. If the scan time is in hours, the phase must be in hours:minutes. If the scan time is in minutes, the phase must be in minutes:seconds. If the scan time is in seconds, the phase must be in seconds. If the scan time is in subseconds, the phase must be in subseconds.</p>

Alarm Options

Field	Description
Alarm Areas	Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an item in the list box and select an alarm area with

Field	Description
	<p>the Browse button, or enter the alarm area name in the field.</p> <p>Valid Entries</p> <p>ALL or up to 15 alarm area names.</p>
<p>Enable Alarm</p>	<p>Lets you enable or disable alarming for this tag.</p> <p>When you enable alarming, the tag generates alarms allowing objects in your operator displays to show alarm conditions, and enabling other tags to detect alarms from the tag.</p> <div data-bbox="824 793 1414 1102" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: The entire chain can be affected when you disable alarms for a tag. In addition, for both the Digital and Analog Alarm tags, this field is ignored when you enable the Alarm Suspend field.</p> </div>
<p>Enable Event</p>	<p>Lets you enable or disable event messaging for the tag. Event messaging is similar to alarming except that it does not require acknowledgment. Event messages are sent to the same alarm destinations as alarms for a given block but do not appear in the Alarm Summary object.</p> <p>Analog Output, Analog Register, Digital Output, Digital Register, Digital Input, and Text tags have event messaging capabilities.</p> <div data-bbox="824 1581 1414 1869" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Be careful when using event messaging in a chain with a time-based scan time. If the scan time is short, your alarm files (either disk or printed) can grow very large. We recommend enabling event messaging for</p> </div>

Field	Description
	 exception-based chains, one shot chains, and stand-alone output blocks.
Shelve Enable	Select this check box to enable Alarm Shelving for the tag.
Shelve Policy	Select an alarm shelving policy from the drop-down list.

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.
Collect	<p>Lets you select if the tag is set for collection by the Proficy Historian collector.</p> <p>Select Enabled to allow the tag to be collected by the collector.</p>
Collection Interval	<p>Lets you set the collection interval, or the amount of time between readings of data of this tag by the Proficy Historian collector.</p> <p>Valid Entries</p> <p>Must be entered in 100 ms intervals. The default value is 5000ms.</p> <p>Example</p> <p>1500 is a valid entry, because it is in 100ms intervals. However, 1545 is not a valid entry, because it is not in 100ms intervals.</p>
Collection Offset	<p>Used with the collection interval to schedule collection of data from a tag.</p> <p>Valid Entries</p>

Field	Description
	<p>Any numeric value that does not exceed the collection interval. The value is in seconds.</p> <p>Examples</p> <p>If you want to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), you would enter a collection interval of 1 hour and an offset of 30 minutes.</p> <p>If you want to collect a value each day at 8 am, you would enter a collection interval of 1 day and an offset of 8 hours.</p>
Time Resolution	<p>Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.</p> <p>Select either Milliseconds or Seconds.</p>
Collector Compression	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Collector Deadband	<p>Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values that fall within a deadband centered around the last reported value.</p> <p>Select Disabled to prevent the tag from being compressed.</p>
Compression Type	<p>Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.</p>

Field	Description
	<p>Select Absolute to set the Collector Deadband value to an absolute value.</p> <p>Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.</p>
<p>Compression Time-out (ms)</p>	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.</p> <p>After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.</p> <p>The Collector Compression Timeout value should be in increments of your collection interval, and not less.</p> <p>Valid Entries</p> <p>Any numeric value.</p>


E-Signature

Field	Description
<p>Type</p>	<p>The Type of Electronic Signature:</p> <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.

Field	Description
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>

Advanced Options

Field	Description
Startup Mode	<p>Lets you select the tag's mode on startup. In Automatic mode, the tag receives data from the I/O driver, OPC server, or OPC UA server. In Manual</p>

Field	Description
	mode, the tag receives data from the operator, scripts, recipes, or Program blocks.
Initial Scan	<p>Lets you select whether the tag is initially placed on or off scan.</p> <p>Click On Scan to place the tag on scan as soon as the Scan, Alarm, and Control (SAC) program starts or when the database is loaded. Click Off Scan to place the tag on scan by a Program block, an Event Action tag, a script, an operator entry in a Data link, or an Easy Database Access program.</p>
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="821 1262 1419 1570" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>
Message Length	<p>Lets you specify the length of text that the tag reads and writes.</p> <p>Valid Entries</p> <p>1 to 80 characters.</p>

Field	Description
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>

TXR Tag



This tag contains the following details:




General


Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p> <p>Tag names must begin with a letter or number and can be up to 256 characters, including certain spe-</p>

Field	Description
	<p>cial characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <p>~ ` + ^ : ? " * = { } . , ; ? @</p> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

I/O Addressing

Field	Description
I/O Driver	<p>Lets you select an I/O driver, OPC server, or OPC UA server for the tag. The selected driver or server enables the tag to communicate with process hardware on the plant floor.</p> <p>Before you can select an I/O driver, OPC server, or OPC UA server you must install it and add it to the available ones in the SCU.</p>
I/O Address	<p>Lets you enter the location in the process hardware where data for this tag is saved and where output is sent.</p> <p>Valid Entries</p> <p>Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations.</p> <div data-bbox="821 1094 1419 1404" style="border: 1px solid black; border-radius: 10px; padding: 10px; background-color: #fff9c4;"> <p> CAUTION: Do not assign the same I/O address to tags when using exception-based and time-based processing. Doing so will cause the exception-based tags to occasionally miss a value.</p> </div> <div data-bbox="821 1436 1419 1881" style="border: 1px solid black; border-radius: 10px; padding: 10px; background-color: #fff9c4;"> <p> CAUTION: Configuration Hub currently does not do I/O address validations before publish. If you enter an invalid IO address into a tag or generate an invalid I/O address via the model and substitutions, the publish may fail to set the IO address into the active database, and your invalid IO address will be removed.</p> </div>

Field	Description
H/W Options	<p>Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p> <div data-bbox="824 436 1419 699" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Signal conditioning and linear scaling cannot be applied simultaneously. If you select a value for Signal Conditioning verify that Linear Scaling is not selected.</p> </div> <p>Valid Entries</p> <p>Depends on your driver or server. Refer to your driver or server manual for more information.</p>
Signal Conditioning	<p>Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p> <div data-bbox="824 1066 1419 1329" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Signal conditioning and linear scaling cannot be applied simultaneously. If you select a value for Signal Conditioning verify that Linear Scaling is not selected.</p> </div> <p>Valid Entries</p> <p>Depends on your driver or server. Refer to your driver or server manual for more information.</p>
Message Length	<p>Indicates the number of bytes to read from the poll table. Maximum value is 80.</p> <div data-bbox="824 1665 1419 1810" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Most GE drivers will only read or write an EVEN number of bytes and will round</p> </div>


Field	Description
	 'down'. For that reason, it is strongly recommended that this value be EVEN.


E-Signature

Field	Description
Type	The Type of Electronic Signature: <ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.
Exempt Alarm Ack	Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.
Comment Required	Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional. <p>The Perform by Comments Required check box appears in every tag configuration where Electron-</p>

Field	Description
	ic Signature settings are available. By default, this check box is disabled.
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p> <p>When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.</p>

Advanced Options

Field	Description
Enable Output	<p>Lets you configure the tag to send output to the I/O driver, OPC server, or OPC UA server. The tag sends its output when it is in Automatic mode and converts its data according to the entries in the Low Limit (EGU), High Limit (EGU), and Signal Conditioning fields.</p>
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="820 1696 1421 1890" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a</p> </div>

Field	Description
	 specific security area even if they cannot write to that area.
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>

TXT Tag



This tag contains the following details:



General

Field	Description
Tag Name	<p>Lets you enter the tag's name. The tag name is referenced by other tags, display links, and other programs.</p> <p>Each tag's name must be unique in the database. If you need to change a tag's name, copy the tag and rename it.</p> <p>Valid Entries</p>

Field	Description
	<p>Tag names must begin with a letter or number and can be up to 256 characters, including certain special characters. Tag names must also contain at least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names.</p> <p>Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs (\$).</p> <p>Invalid Entries</p> <p>You cannot use the following special characters in a tag name:</p> <pre>~ ` + ^ : ? " * = { } . , ; ? @</pre> <p>Examples</p> <p>AI1, CA_10, DI#, 4PID, 'TEST'</p>
Description	<p>Lets you enter optional descriptive text about the tag.</p> <p>Valid Entries</p> <p>A text string of up to 256 characters can describe the block and its function. This string is appended to each alarm message and can also be shown on operator displays.</p>
Type	The tag type. Display-only field.
Current Value	The current value of the tag in the database. Display-only field. Click the update button to update the displayed value, if one exists.

I/O Addressing

Field	Description
I/O Driver	<p>Lets you select an I/O driver, OPC server, or OPC UA server for the tag. The selected driver or server enables the tag to communicate with process hardware on the plant floor.</p> <p>Before you can select an I/O driver, OPC server, or OPC UA server you must install it and add it to the available ones in the SCU.</p>
I/O Address	<p>Lets you enter the location in the process hardware where data for this tag is saved and where output is sent.</p> <p>Valid Entries</p> <p>Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations.</p> <div data-bbox="821 1094 1419 1409" style="border: 1px solid black; border-radius: 10px; padding: 10px; background-color: #fff9c4;"> <p> CAUTION: Do not assign the same I/O address to tags when using exception-based and time-based processing. Doing so will cause the exception-based tags to occasionally miss a value.</p> </div> <div data-bbox="821 1436 1419 1879" style="border: 1px solid black; border-radius: 10px; padding: 10px; background-color: #fff9c4;"> <p> CAUTION: Configuration Hub currently does not do I/O address validations before publish. If you enter an invalid IO address into a tag or generate an invalid I/O address via the model and substitutions, the publish may fail to set the IO address into the active database, and your invalid IO address will be removed.</p> </div>

Field	Description
Signal Conditioning	<p>Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p> <div data-bbox="824 436 1414 699" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Signal conditioning and linear scaling cannot be applied simultaneously. If you select a value for Signal Conditioning verify that Linear Scaling is not selected.</p> </div> <p>Valid Entries</p> <p>Depends on your driver or server. Refer to your driver or server manual for more information.</p>
H/W Options	<p>Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.</p> <div data-bbox="824 1066 1414 1329" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Signal conditioning and linear scaling cannot be applied simultaneously. If you select a value for Signal Conditioning verify that Linear Scaling is not selected.</p> </div> <p>Valid Entries</p> <p>Depends on your driver or server. Refer to your driver or server manual for more information.</p>

Limits and Scaling

Field	Description
Low Limit	<p>Used to clamp input and to scale output. In most cases you should enter the low and hi EGU ranges for the TXT block as 0 to 65535, as this is the range of a 16 bit integer value. The text lookup ta-</p>

Field	Description
	ble on the 2nd page of the TXT dialog requires that you enter exact integer values which will also generally be in this range.
High Limit	Used to clamp input and to scale output. In most cases you should enter the low and hi EGU ranges for the TXT block as 0 to 65535, as this is the range of a 16 bit integer value. The text lookup table on the 2nd page of the TXT dialog requires that you enter exact integer values which will also generally be in this range.
Units	For display purposes.

Text Strings

Field	Description
Target Value 0-16	The list of 16 target values for which the block will check for an exact match. These will default to powers of 2. NOTE: The system will NOT check for duplicates; it will use the first exact match found. The values must be within the EGU range of the block. Although these values are entered as floating point numbers it is STRONGLY recommended that you restrict your use to integers since they must exactly match the value returned from the I/O driver.
Target State 0-16	The list of 16 corresponding ASCII strings. The strings are up to 40 bytes each.


E-Signature

Field	Description
Type	The Type of Electronic Signature:

Field	Description
	<ul style="list-style-type: none"> • Select None to require no Electronic Signature for this tag. • Select Perform Only to require a Perform By signature for any data entry changes or alarm acknowledgements for this tag. • Select Perform and Verify to require both a Perform By and a Verify By signature for any data entry changes or alarm acknowledgements for this tag.
Remember User	<p>Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action.</p>
Exempt Alarm Ack	<p>Select to allow operators to acknowledge alarms for this tag without entering a signature, even if this tag requires electronic signatures for data entry.</p>
Comment Required	<p>Select this option to enable Comment enforcement in the Perform Comment section. This means that the operator must enter comments in the Comment box in the Electronic Signature section during run mode. Comments in the Verify Comment section are optional.</p> <p>The Perform by Comments Required check box appears in every tag configuration where Electronic Signature settings are available. By default, this check box is disabled.</p>
Unsigned Writes	<p>Select to allow this tag to accept or reject unsigned writes.</p> <p>Unsigned writes can originate from scripts, recipe downloads, and other data sources.</p>

Field	Description
	When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.

Advanced Options

Field	Description
Enable Output	Lets you configure the tag to send output to the I/O driver, OPC server, or OPC UA server. The tag sends its output when it is in Automatic mode and converts its data according to the entries in the Low Limit (EGU), High Limit (EGU), and Signal Conditioning fields.
Case Sensitive	Enter Y if operator entry must exactly match the string defined in the block. If N (no) then 'ONE', 'One' and 'one' are all equivalent. If YES then they are not.
Security Areas	<p>Lets you specify up to three security areas to restrict operator access to the tag. To change the value of a write-protected tag in the Database Manager or the iFIX WorkSpace, the operator must have access to that tag's security area.</p> <p>Valid Entries</p> <p>One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.</p> <div data-bbox="824 1556 1419 1864" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a specific security area even if they cannot write to that area.</p> </div>

Field	Description
Alarm Field 1	<p>Lets you enter text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>
Alarm Field 2	<p>Lets you enter more text about the tag. Typically, one of these alarm fields contains a path to a picture you want to associate with the tag. Refer to the Implementing Alarms and Messages electronic book for more information.</p> <p>Valid Entries</p> <p>Text, up to 80 characters.</p>

Project Security

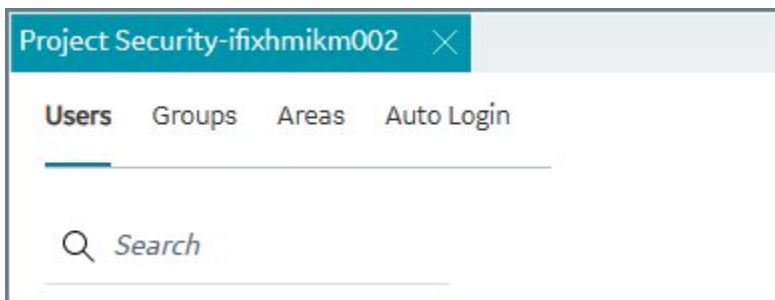
Overview of Project Security

Configuration Hub allows you to manage your iFIX users, groups, and security areas from the Project Security panel. It also allows you to access iFIX Auto Login settings.

Overview of Project Security

To access Project Security settings:

- From the Navigation panel, select your node, the iFIX project, and then **Project Security**. The Project Security menu appears as shown in the following figure.



From the Project Security panel, you can do the following:

- [Add or Modify Users \(on page 824\)](#)
- [Add or Modify Groups for Proficy Authentication \(on page 827\)](#)
- [Add or Modify Security Areas \(on page 828\)](#)
- [Auto Login Configuration \(on page 830\)](#)

Limitations for Project Security Settings in Configuration Hub

When configuring security settings from the Project Security panel, be aware that assignment of direct Application Features and Security Areas is not supported from the Users page of the Project Security panel. To do this, use the security [Groups page \(on page 827\)](#)

For iFIX users which already have Application Features and/or Security Areas assigned outside of Configuration Hub, be aware that:

- Those details will not be shown in Configuration Hub. However, you can view other user details and still can edit these users through Configuration Hub.
- After editing and publishing these iFIX users, their existing Application Features and Security Areas assignments will remain intact and other edits will get applied to that user.
- When deploying these iFIX users, existing Application Features and Security Areas assignments will be lost as only user information that is visible in Configuration Hub is sent to target node when the Deploy is performed.

Add or Modify Users

Configuration Hub allows you to manage your iFIX Users from the Project Security panel. User accounts define the security areas, application features, and group accounts available to individuals.

Manage Users

To manage users:

1. From the Navigation panel, select your node, the iFIX project, and then **Project Security**.
2. Click **Users**. The user security settings appear as shown in the following figure.

The screenshot shows a web interface for managing users. At the top, there are navigation tabs: 'Users' (selected), 'Groups', 'Areas', and 'Auto Login'. A search bar with a magnifying glass icon and the text 'Search' is on the left. On the right, there are icons for a plus sign and a refresh symbol. Below the search bar is a table with the following data:

<input type="checkbox"/>	NAME ↑	ACCOUNT TYPE	STATUS
	GUEST	Native	✓
	SYSTEM ADMINISTRATOR	Native	✓

User Details

The following table describes the details you can manage for each user.

Field	Description
User Full Name	Displays the full name of the operator whose account you are defining as an iFIX user. You can change the text by typing a new name, up to 30 alphanumeric characters in length. The name you enter must be unique.
Login Name	Contains the login name of the user. You can change the text by entering a new name. The user enters this name when logging in to iFIX. If you enable Windows security for this account, the login name must match the login name of the operator's Windows user account. The login name you enter must be unique.

Field	Description
Password	<p>Displays the account password. Entering a password is optional. Each password can be up to 20 alphanumeric characters.</p> <p>The password is not displayed in this field for security reasons. When you create or modify a password, the field displays an asterisk (*) for every character you specify. iFIX user passwords are case insensitive when not using Windows security</p>
Account Type	<p>Specifies whether the user is a Native or Windows user. This is view-only field.</p>
Domain	<p>Displays the account domain name when Windows security is enabled. The domain name can be up to 20 alphanumeric characters.</p> <p>Be aware that when configuring your Windows users in iFIX Security, the Domain Name entry needs to be your domain's NetBIOS name.</p>
Login Timeout	<p>Controls the length of time operators can remain logged in Windows. You can enter any time interval from 00:00:01 to 23:59:59. A value of 00:00:00 disables this field. When an operator attempts to access a restricted application feature or security area after the time interval expires, iFIX logs out the operator, requiring him or her to log in again. This feature prevents operators from remaining logged in indefinitely.</p> <p>This feature does not eliminate the need for operators to manually log out, particularly if you have strict security requirements. If you decide to use this feature, consider it a safety mechanism.</p>
Groups	<p>Lists the groups this user has access to.</p>

Add or Modify Groups for Proficy Authentication

Configuration Hub allows you to manage your iFIX security groups from the Project Security panel. Group accounts define the security areas and application features available to group members.

Manage Groups

To manage groups:

1. From the Navigation panel, select your node, the iFIX project, and then **Project Security**.
2. Click **Groups**. The group security settings appear as shown in the following figure.

NAME ↑	MEMBERS	STATUS
APPLICATION_DESIGNER	0	✓
IFIX_PROFICY_AUTH_ADMIN	0	✓
OPERATORS	0	✓
SUPERVISORS	0	✓

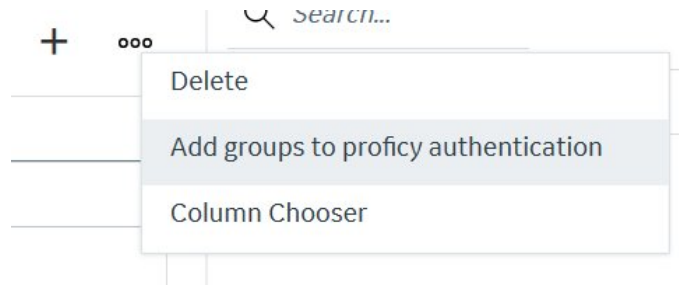
To add a group, click the plus (+) sign at the top of the grid. the Add Group dialog box appears.

Create New Group

GROUP NAME

Cancel Add

To add a group to Proficy Authentication, right-click the group in the list, and then select **Add Groups to Proficy Authentication**.



Group Details

The following table describes the details you can manage for each group.

Field	Description
Name	Displays the name of the group account you are defining. You add or modify the text by typing a name, up to 30 alphanumeric characters in length.
Security Areas	Displays the security areas (on page 828) accessible to this group.
Application Features	Displays the iFIX application features accessible to this account.

Add or Modify Security Areas

Configuration Hub allows you to manage your iFIX security areas from the Project Security panel.

After you define your users and groups, the next step is to define your security areas and specify a name for each area. You can define up to 254 security areas, and each name can be up to 20 characters. iFIX names the first 16 security areas A through P, by default. However, you can rename these areas or create a new area. After you define a security area, you can assign it to a group or user account.

To manage security areas:

1. From the Navigation panel, select your node, the iFIX project, and then **Project Security**.
2. Click **Areas**. The security areas appear as shown in the following figure.

<input type="checkbox"/>	NAME ↑	STATUS ↓
	A	✓
	B	✓
	C	✓
	D	✓
	E	✓
	F	✓
	G	✓
	H	✓
	I	✓
	J	✓
	K	✓
	L	✓
	M	✓
	N	✓
	O	✓
	P	✓

Click in the Area Name field to change the name of a security area.

To add a security area, click the plus (+) at the top of the security area list. The Create New Security Area dialog box appears. Enter a name and click Add.

Create New Security Area

AREA NAME

Cancel Add

Auto Login Configuration

You can set up iFIX to log in an operator automatically when the user starts iFIX. Configuration Hub allows you to manage iFIX auto login information from the Project Security panel.

You can create this auto login configuration by specifying the name of the:

- Node you want to automatically log in.
- User you want logged in.

To manage auto login settings:

1. From the Navigation panel, select your node, iFIX project, and then **Project Security**.
2. Click **Auto Login**. The Auto Login settings appear as shown in the following figure.



To add auto login settings, click the plus (+) icon at the top of the grid. The New Auto Login dialog box appears as shown in the following figure.

New AutoLogin

NODE

APPLICATION USER

USER
 Select... ▼

PASSWORD

SYSTEM USER

USER
 Select... ▼

PASSWORD

Cancel Create

Enter the following information, and click **Create** to add auto login information.

Field	Description
Node	The name of the node that you want to provide automatic login for the specified user.
Application User	Select an iFIX application user from the drop-down list.
Application User Password	The password for the application user.
System User	Select a system user from the drop-down list.
System User Password	The password for the system user.

Alarms

Defining Alarm Areas

Configuration Hub allows you to manage your iFIX alarm areas from the Alarms panel.

Overview of Alarm Areas

One of your first tasks when configuring alarms is to create alarm areas by naming them. iFIX provides 16 default alarm areas, named A through P; however, you can rename the default areas or add new ones. Each alarm area name you enter must be unique and can be up to 29 alphanumeric characters.

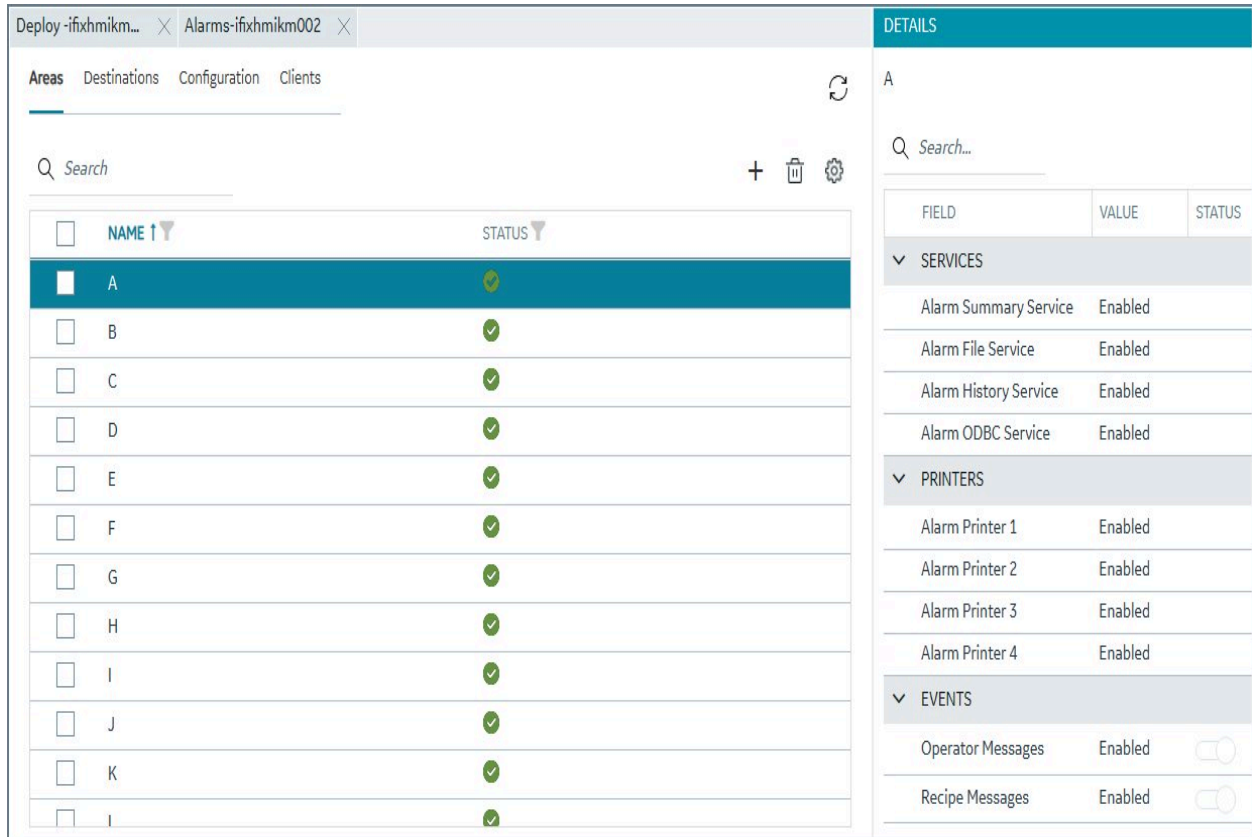
In order to enter or edit an alarm area name, iFIX must be running. In addition, you can only edit the alarm area database from a SCADA server.

Alarm area names cannot contain the characters "*", "?", or "\".

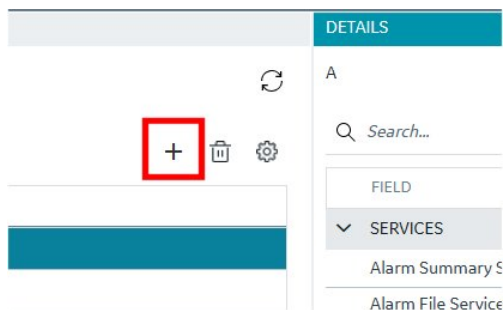
Access Alarm Areas

To access Alarm Areas:

1. From the Navigation panel, select your node, iFIX project, and then **Alarms**.
2. Click **Areas**. The Alarm Areas settings appear as shown in the following figure.



To add an Alarm Area, click the plus (+) icon to access the [Common Alarm Areas Configuration \(on page 846\)](#) dialog box.



Alarm Area Details

For each of the alarm areas you can configure what is enabled for:

- [Alarm Services \(on page 834\)](#)
- [Alarm Printers \(on page 839\)](#)
- [Alarm Events \(on page 841\)](#)

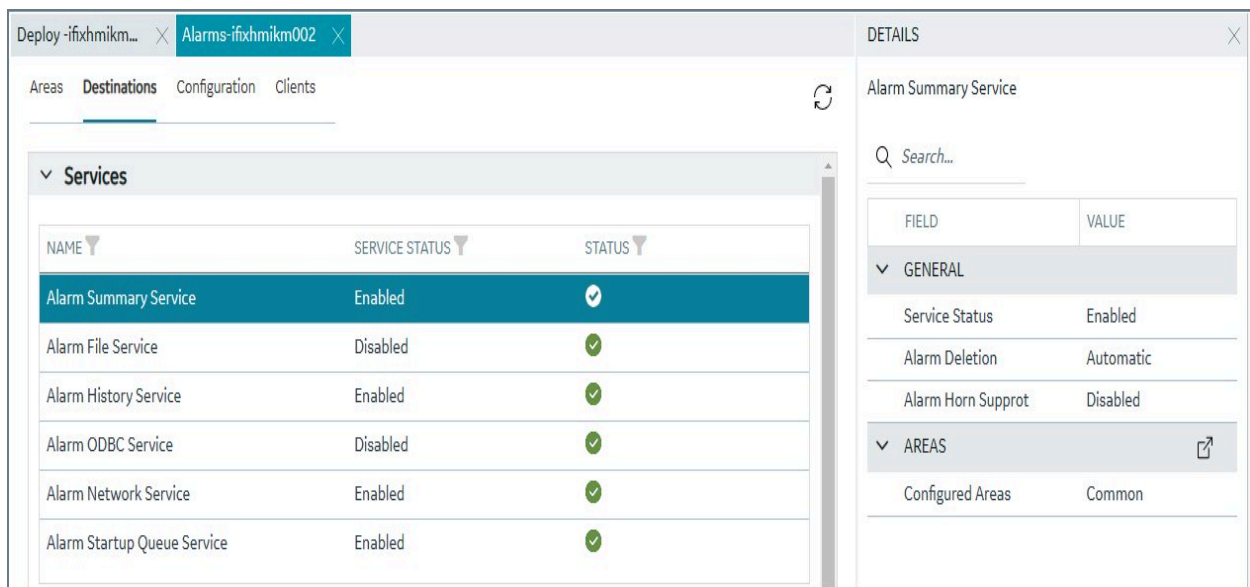
Alarm Services

Configuration Hub allows you to manage your iFIX alarm services from the Alarms panel.

Access Alarm Services

To access Alarm Services:

1. From the Navigation panel, select your node, iFIX project, and then **Alarms**.
2. Click **Destinations**. The Alarm Services settings appear as shown in the following figure.



Details for Alarm Services

The following tables describe the details you can manage for alarm services.

Table 7. Alarm Summary Service

Field	Description	Default
Service Status	<p>Species whether the service is enabled or disabled.</p> <p>By default, the Alarm Summary Service automatically deletes an acknowledged alarm when the block's current value returns to normal. If you do not want to</p>	Enabled

Table 7. Alarm Summary Service (continued)


Field	Description	Default
	delete acknowledged alarms automatically, you can disable this feature and delete the alarms manually by re-acknowledging them after the block's value returns to normal.	
Alarm Deletion	Specifies whether alarms can be deleted automatically or manually.	Automatic
Alarm Horn Support	Allows you to enable the alarm horn so that an alarm sounds when a new alarm appears. The horn repeats at three speeds to distinguish between low, medium, and high priority alarms. A one-second increment between beeps signifies high priority alarm, a two-second increment signifies a medium priority, and a three-second increment signifies a low priority.	Disabled
Configured Areas	Specifies whether to use Common alarm areas, or specific alarm areas for the specified alarm service. Select the  button to pick your options.	Common

Table 8. Alarm File Service

Field	Description	Default
Service Status	Species whether the service is enabled or disabled.	Disabled

Table 8. Alarm File Service (continued)



Field	Description	Default
	When enabled, the Alarm File service receives alarms and messages, and saves them to a text file, yymmdd.ALM. This file resides in the Alarm path.	
Configured Areas	Specifies whether to use Common alarm areas, or specific alarm areas for the specified alarm service. Select the  button to pick your options.	Common
Use Common Message Format	Leave the default of yes, or click the  button to display the Alarm File Service Message Format Configuration dialog box, and select the service's message format.	Yes

Table 9. Alarm History Service

Field	Description	Default
Service Status	<p>Species whether the service is enabled or disabled.</p> <p>Be sure that the Alarm History Service is always enabled. If the Alarm History Service is disabled, you may receive an error message stating that no destination is currently available to dispatch the alarm.</p>	Enabled
Configured Areas	Specifies whether to use Common alarm areas, or specific alarm areas for the specified	Common

Table 9. Alarm History Service (continued)



Field	Description	Default
	alarm service. Select the  button to pick your options.	
Use Common Message Format	Leave the default of yes, or click the  button to display the Alarm File Service Message Format Configuration dialog box, and select the service's message format.	Yes

Table 10. Alarm ODBC Service



Field	Description	Default
Service Status	Species whether the service is enabled or disabled. When enabled, this service sends alarms and messages to an ODBC-compliant relational database, allowing you to retrieve any information you want by querying the database. You can use the iFIX ODBC Alarm Service Configuration dialog box to configure the Alarm ODBC Service.	Disabled
Configured Areas	Specifies whether to use Common alarm areas, or specific alarm areas for the specified alarm service. Select the  button to pick your options.	Common
ODBC Configure	Describes whether this feature is configured. Select the  to	No

Table 10. Alarm ODBC Service (continued)

Field	Description	Default
	configure your Alarm ODBC Service.	

Table 11. Alarm Network Service

Field	Description	Default
Service Status	<p>Specifies whether the service is enabled or disabled.</p> <p>If your system is networked, be sure that the Alarm Network Service is always enabled. If the Alarm Network Service is disabled, you may receive an error message stating that no destination is currently available to dispatch the alarm.</p>	Enabled
Send Startup Queue to Original Typers	Select the Send Startup Queue Alarms to Original Typers check box to distribute alarms from the SCADA server to all the enabled alarm destinations on the View client. Clear the check box if you want to send the alarms to the Alarm Summary and Alarm Startup Queue Services, or if the Alarm Queue Service is disabled.	Check box cleared

Table 12. Alarm Startup Queue Service

Field	Description	Default
Service Status	<p>Specifies whether the service is enabled or disabled.</p> <p>When enabled, the Alarm Startup Queue Service provides a View</p>	Disabled

Table 12. Alarm Startup Queue Service (continued)

Field	Description	Default
	<p>client with a list of the alarms that occurred on a SCADA server prior to starting iFIX on the View client. In addition, iFIX can send messages to the Alarm Start-up Queue Service along with the alarms.</p> <p>If you are using the Startup Queue, be sure to enable the Alarm Summary Service.</p>	
Summary Alarms Only	Select the Summary Alarms Only check box to receive alarms and messages. To receive only alarms from the Alarm Summary Service, leave the check box selected.	Check box selected
Enable Time Filter	If you want to filter alarms by time, select the Enable Time Filter check box and then enter the maximum age of the alarms and messages you want to receive in the Hours and Minutes fields.	Check box cleared
Filter Alarms Older Than	The maximum age of the alarms and message you want to receive.	23:59:59

Alarm Printers

Configuration Hub allows you to manage your iFIX alarm printers from the Alarms panel.

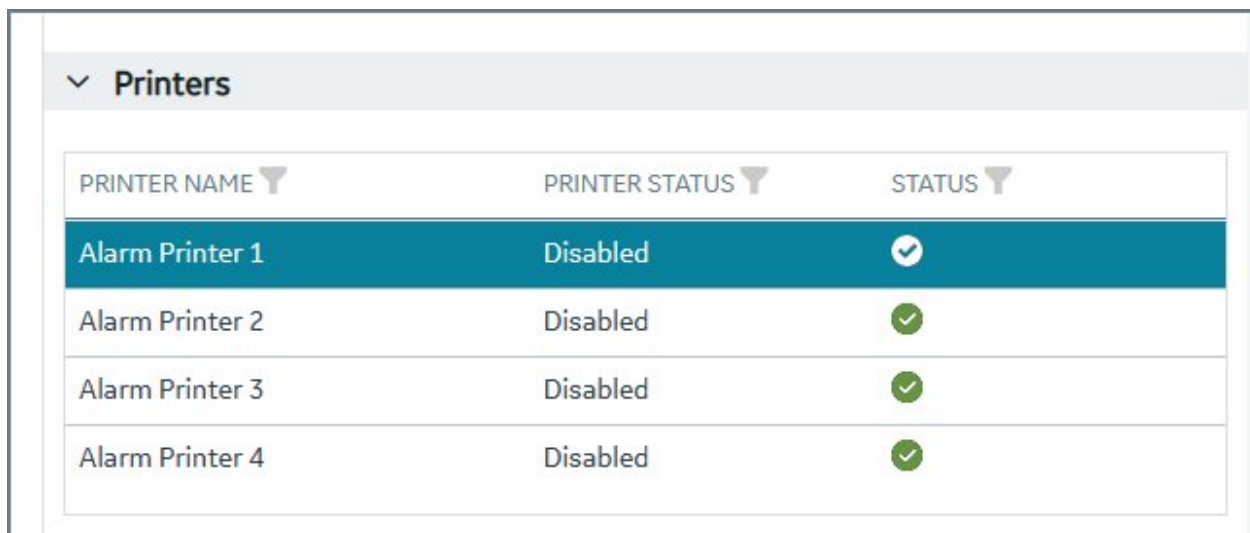
Alarm Printers Overview

You can configure up to four Alarm Printer Services for your nodes. For each alarm printer service, you select a printer port and enter a name in the Alarm Printer Configuration. For each printer service, you can connect the printer to serial ports (COM) 1 or 2, to parallel ports (LPT) 1 or 2, or to a USB port. Keep in mind that each printer service must be attached to a unique port, and that the printer name can be up to 32 alphanumeric characters. If you have multiple USB ports and need to specify the USB port, use the Printer.ini as described in [Specifying a USB Port with the Printer.ini File](#) in the iFIX e-books.

When configuring the Alarm Printer Service, you can also select the alarm areas and message format you want for the Alarm Printer Service.

To access Alarm Printers:

1. From the Navigation panel, select your node, iFIX project, and then **Alarms**.
2. Click **Destinations**, and scroll to the Printers areas. The Alarm Printers settings appear as shown in the following figure.





PRINTER NAME	PRINTER STATUS	STATUS
Alarm Printer 1	Disabled	<input checked="" type="checkbox"/>
Alarm Printer 2	Disabled	<input checked="" type="checkbox"/>
Alarm Printer 3	Disabled	<input checked="" type="checkbox"/>
Alarm Printer 4	Disabled	<input checked="" type="checkbox"/>

Details for Alarm Printers

Table 13. Alarm Printer Fields

Field	Description	Default
Service Status	The status of the alarm printer service: Enabled or Disabled.	Disabled

Table 13. Alarm Printer Fields (continued)

Field	Description	Default
Port Definition	The port to use for the Alarm Printer service.	COM#
Printer Name	The name of the Alarm Printer.	Alarm Printer #
Configured Alarm Areas	Specifies whether to use Common alarm areas, or specific alarm areas for the specified alarm service. Select the  button to pick your options.	Common
Message Format > Use Common Format	Leave the default of yes, or click the  button to display the Alarm File Service Message Format Configuration dialog box, and select the service's message format.	Yes

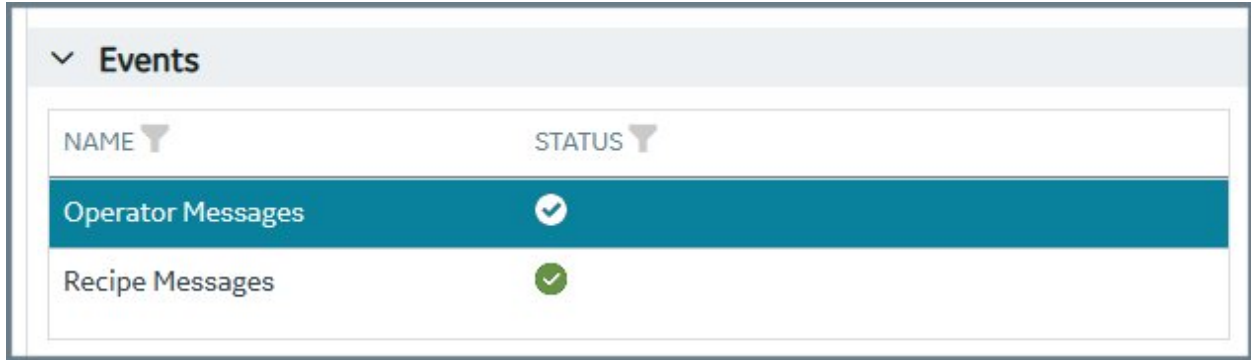
Alarm Events

Configuration Hub allows you to manage your iFIX alarm events from the Alarms panel.

Alarm Events Overview

To access Alarm Events:

1. From the Navigation panel, select your node, iFIX project, and then **Alarms**.
2. Click **Destinations**, and scroll to the Events areas. The Alarm Events settings appear as shown in the following figure.

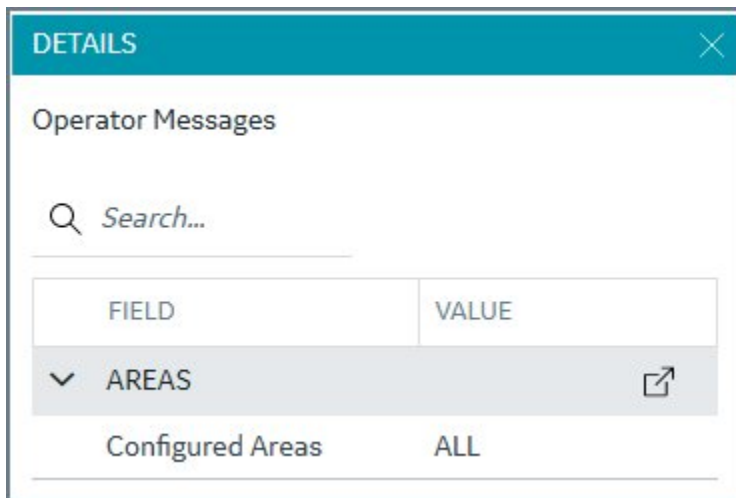


The screenshot shows a table with the following data:

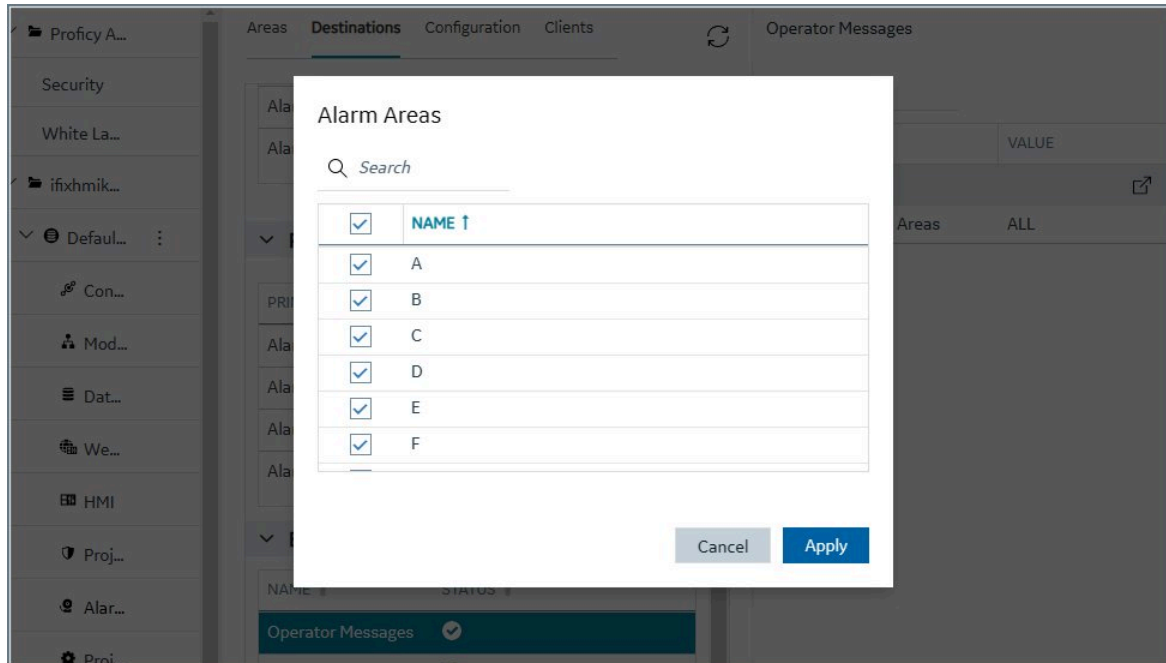
NAME	STATUS
Operator Messages	✓
Recipe Messages	✓

Details for Alarm Events

For alarm events, you can also configure the alarm areas from the Details panel, as shown in the following figure.



Select the  button to pick open the Alarm Areas dialog box and pick your options.



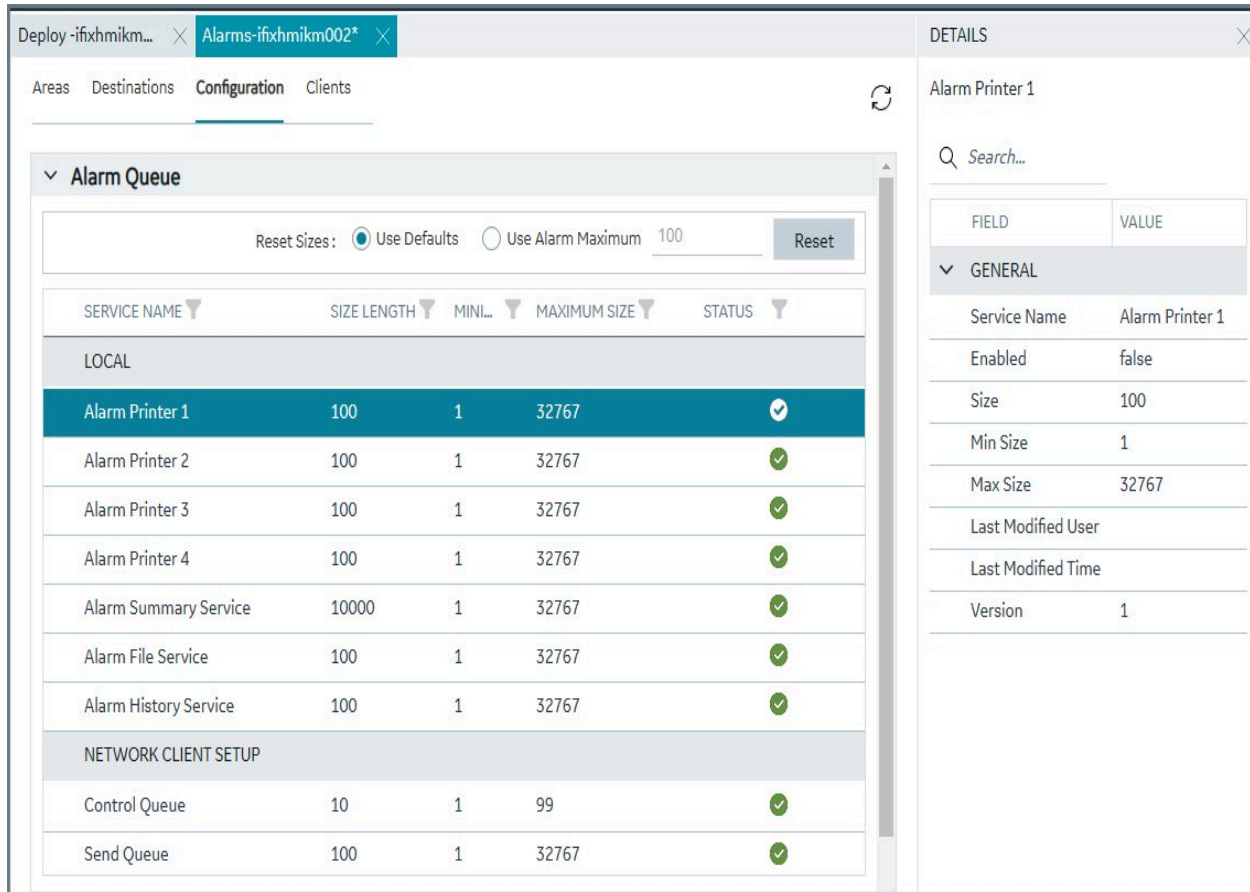
Alarm Queue Configuration

Configuration Hub allows you to manage your iFIX alarm queue configuration from the Alarms panel.

Alarm Queue Overview

To access Alarm Queue Configuration:

1. From the Navigation panel, select your node, iFIX project, and then **Alarms**.
2. Click **Configuration**. The Alarm Queue settings appear as shown in the following figure.



Details of Alarm Queue Configuration

The following table displays the read-only fields of the Alarm Queue Configuration.

Field	Description
Service Name	The name of the Alarm service.
Enabled	Whether the Alarm service is enabled or disabled.
Size	The actual size of the service. The queue size is the number of records stored in the alarm queue.
Min Size	The minimize size of the queue. This value can be any number from 1 to 32,767.
Max Size	The maximum size of the queue. This value can be any number from 1 to 32,767.

Field	Description
	The maximum queue size is the maximum number of records stored in the alarm queue.
Last Modified User	The name of the user who last modified the service.
Last Modified Time	The current time of the last modification.
Version	The version of the queue.

Common Message Format Configuration

Configuration Hub allows you to manage your iFIX alarm message format from the Alarms panel.

Overview of Alarm Message Format Configuration

To access Alarm Message Format Configuration:

1. From the Navigation panel, select your node, iFIX project, and then **Alarms**.
2. Click **Configuration** and scroll to the Common Message Format section. The Common Message Format settings appear as shown in the following figure.

▼ **Common Message Format**
Reset to Defaults

	SELECT	ATTRIBUTE	LENGTH
⋮	<input checked="" type="checkbox"/>	Date	10
⋮	<input checked="" type="checkbox"/>	Time	10
⋮	<input checked="" type="checkbox"/>	Node	10
⋮	<input checked="" type="checkbox"/>	Tagname	30
⋮	<input checked="" type="checkbox"/>	Alarm Type	7
⋮	<input checked="" type="checkbox"/>	Value	13
⋮	<input checked="" type="checkbox"/>	Unit	4

MESSAGE LENGTH Range: 1-579

CURRENT LENGTH

Details of Alarm Message Format Configuration

The following table describes the settings for the common message format fields.

Field	Description
Reset to Defaults button	Select this button to reset the settings back to the defaults.
Date	The default is 10.
Time	The default is 10.
Node	The default is 10.
Tagname	The default is 30.
Alarm Type	The default is 7.
Value	The default is 13.
Unit	The default is 4.
Message Length	The Message Length field allows you to specify the maximum number of characters that the printer can support. Valid entries are from 1-132. The default is 132.
Current Length	The Current Length field displays the number of characters that the printer currently supports.

Common Alarm Areas Configuration

Configuration Hub allows you to manage your iFIX alarm area configuration from the Alarms panel.

Overview of Alarm Areas Configuration

To access Alarm Areas Configuration:

1. From the Navigation panel, select your node, iFIX project, and then **Alarms**.
2. Click **Configuration** and scroll to the end, and expand the section if needed. The Common Areas settings appear as shown in the following figure.

Common Areas	
<input checked="" type="checkbox"/> NAME ↑ ▾	STATUS ▾
<input checked="" type="checkbox"/> A	✓
<input checked="" type="checkbox"/> B	✓
<input checked="" type="checkbox"/> C	✓
<input checked="" type="checkbox"/> D	✓
<input checked="" type="checkbox"/> E	✓
<input checked="" type="checkbox"/> F	✓
<input checked="" type="checkbox"/> G	✓
<input checked="" type="checkbox"/> H	✓
<input checked="" type="checkbox"/> I	✓
<input checked="" type="checkbox"/> J	✓
<input checked="" type="checkbox"/> K	✓

Overview of Alarm Areas Configuration

Select a check box to enable or disable an alarm area from the common configuration.

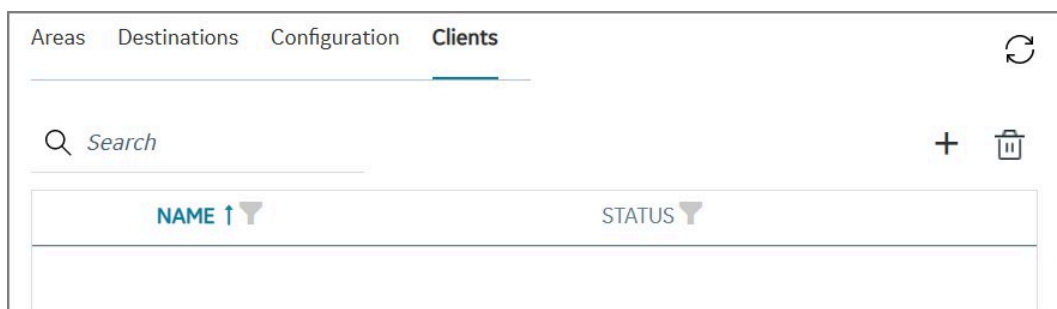
Alarm Clients

Configuration Hub allows you to manage your iFIX alarm clients from the Alarms panel.

Access Alarm Clients

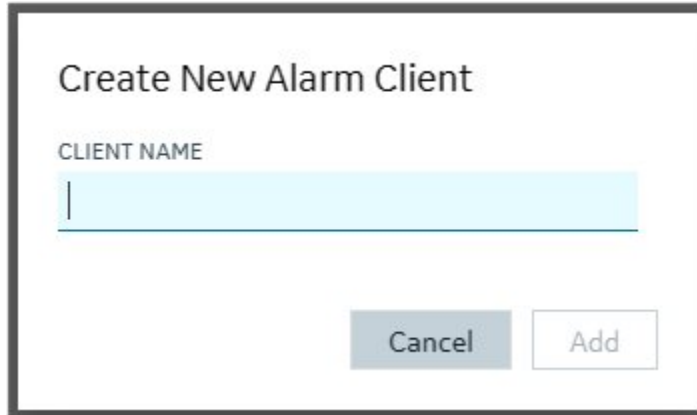
To access Alarm Services:

1. From the Navigation panel, select your node, iFIX project, and then **Alarms**.
2. Click **Clients**. The Alarm Clients settings appear as shown in the following figure.



Add an Alarm Client

To add an alarm client, click the plus (+) icon. The Create New Alarm Client dialog box appears. Enter a Client Name and click **Add**.



The image shows a dialog box titled "Create New Alarm Client". Inside the dialog, there is a text input field with the label "CLIENT NAME" above it. The input field is currently empty. Below the input field, there are two buttons: "Cancel" and "Add". The "Add" button is highlighted with a light blue background.

Project Settings

Overview of Project Settings

In Configuration Hub, you can manage iFIX project settings on the **Project Settings** panel. You can configure your project **Preferences**, **Failover**, and **Task Configuration** settings from this screen. You can manage multiple iFIX Projects through this panel.

Overview

After installing iFIX and Configuration Hub, the originally installed iFIX project displays the name **DefaultProject** in the Navigation panel. Any other iFIX projects created manually and started in iFIX, will also display in the Project List, but as a named project. You can choose to [add a new projects \(on page 853\)](#) through Configuration Hub by selecting the node name in the Navigation panel, clicking the plus (+) icon, and selecting **Create new iFIX Project**.

To manage project settings for a project, select your node name, the iFIX project, and then **Project Settings**. Most of the **Project Settings** that you can manage in Configuration Hub can also be found in the iFIX [SCU app](#).

After you make your changes to Project Settings in Configuration Hub, you will need to apply them to the SCADA Server using the [Save and Publish \(on page 874\)](#) options. Restart iFIX after you publish, to see these new changes applied.

**Important:**

Any project settings that you edit, save, and publish in Configuration Hub, require a restart of iFIX to apply them to the SCADA node.

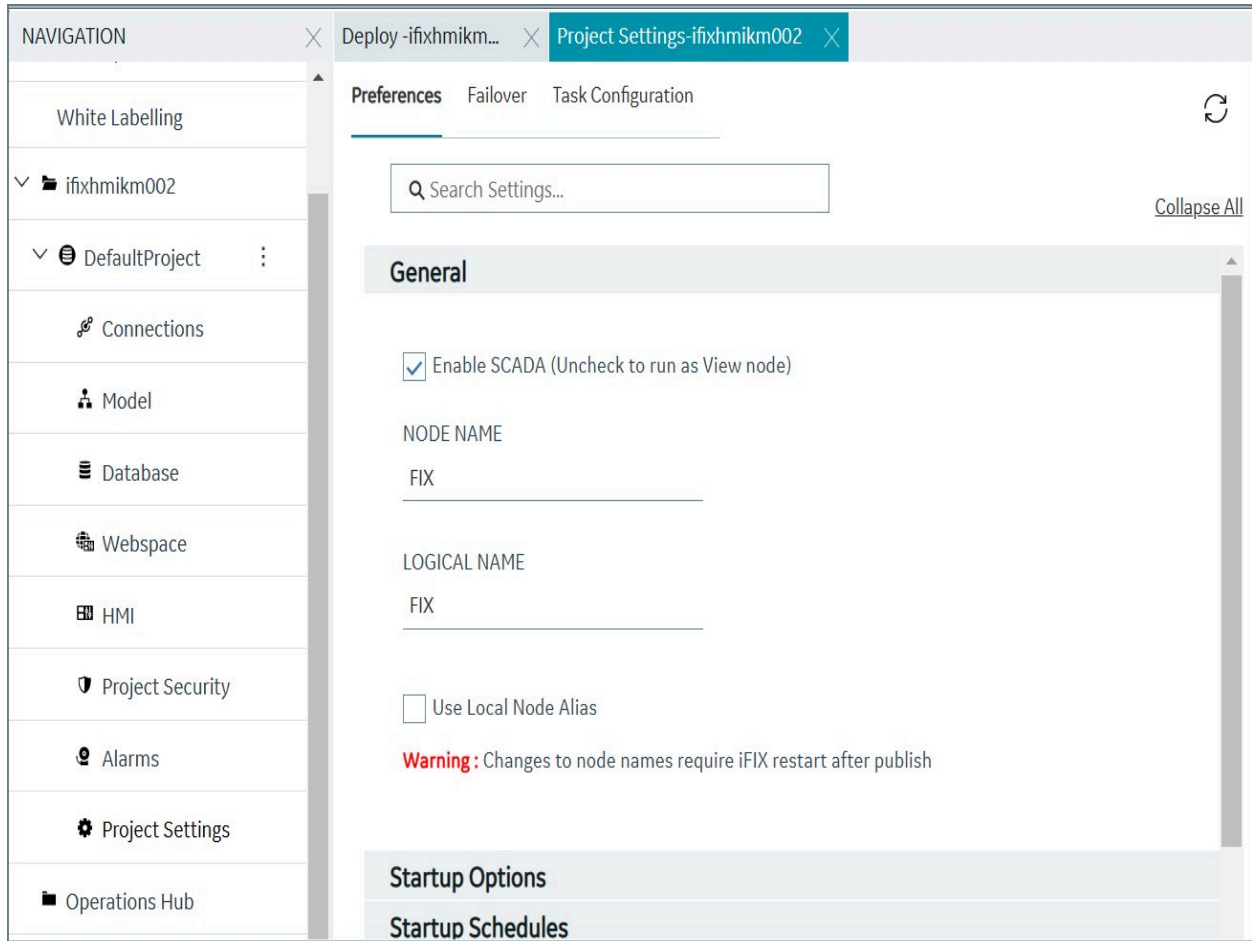
Troubleshooting

If you cannot start a project in Configuration Hub and you modified the iFIX node name in Configuration Hub, after you saved and published your changes, restart iFIX (as a service) through Configuration Hub. If the node was modified in iFIX, restart iFIX manually. For instance, restart from the iFIX Startup app. (One of these steps should help get the node name updated in project list and Project Settings in Configuration Hub.)

Accessing Project Settings

To access iFIX project settings in Configuration Hub:

- From the Navigation panel, select your node name, the iFIX project, and then **Project Settings**. The Project Settings appear as shown in the following figure.



Project Settings Summary Screen

To view the Project Summary settings, select your node name, and then the project name. For instance: Default Project. Click the Overview link (it displays by default) to view the project summary settings.

The screenshot displays the Configuration Hub interface for a project named 'Deploy - ifixhmikm002'. The left sidebar shows a navigation menu with various project management options. The main content area is divided into two tabs: 'Overview' (selected) and 'Deployment'. The 'Overview' tab contains the following sections:

- Configuration Summary**: A refresh icon is present on the right.
- Node Options**: A table with two columns: 'OPTION' and 'VALUE'.

OPTION	VALUE
Database Name	DATABASE
Node Type	SCADA
Local Node Name	FIX
Local Logical Name	FIX
- Number of Configured Drivers - 4**: A table listing the configured drivers.

DRIVER
SM2 - Sim Driver 2 v6.42a
OUA - OPC UA Client Driver v1.0
IGS - Industrial Gateway Server 7.62
- Database Block Configuration**: A table with three columns: 'BLOCK TYPE', 'ALLOCATED', and 'UTILIZED'.

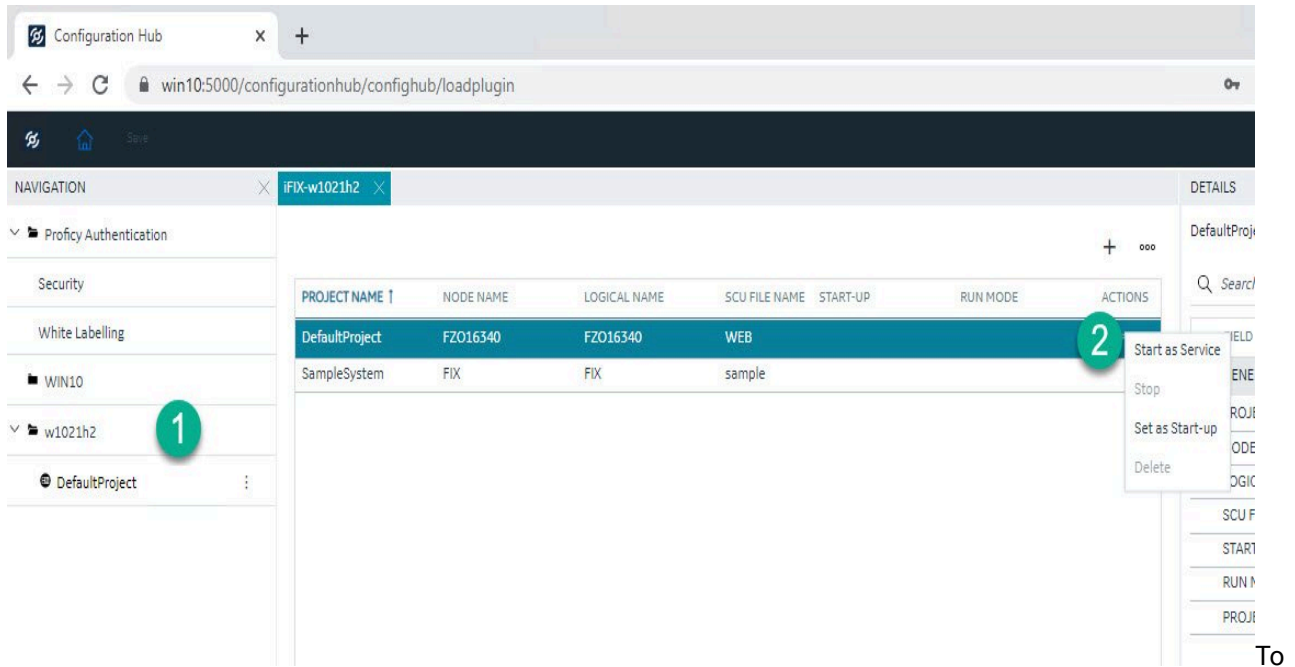
BLOCK TYPE	ALLOCATED	UTILIZED
AI	1000	1
DI	1000	1

Starting and Stopping iFIX Projects

From the Project Panel in Configuration Hub, you can start and stop projects using the ellipsis (...) button in Project name list.

You cannot update or start iFIX with a specific Node Name from Configuration Hub. For instance, if iFIX Webservice sessions or iFIX Remote Desktop (terminal server) sessions are started, then the node name for the iFIX DefaultProject gets updated with the last run iFIX Project Node Name/SCU file. In this case, to start iFIX with a specific Node Name, you should manually start iFIX the traditional way, such as from the iFIX Startup app, instead of through Configuration Hub.

Start a Project as a Service



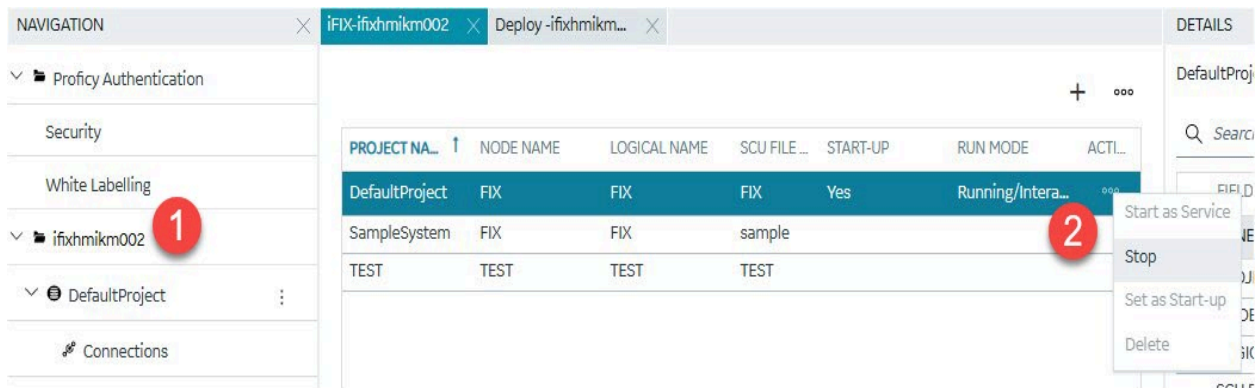
start a project:

1. From the Navigation panel, select your node name to display the grid of project names.
2. Select the project name you want to start, and then select the ellipsis (...) button and then **Start as Service**.

A message box appears asking if you want to continue.

3. Click Yes to proceed. You will then be prompted to save any open files before the process stops.

Stop a Project



To stop a project:

1. From the Navigation panel, select your node name to display the grid of project names.
2. Select the project name you want to stop, and then select the ellipsis (...) button and then **Stop**.

A message box appears asking if you want to continue.

3. Click Yes to proceed.

Troubleshooting

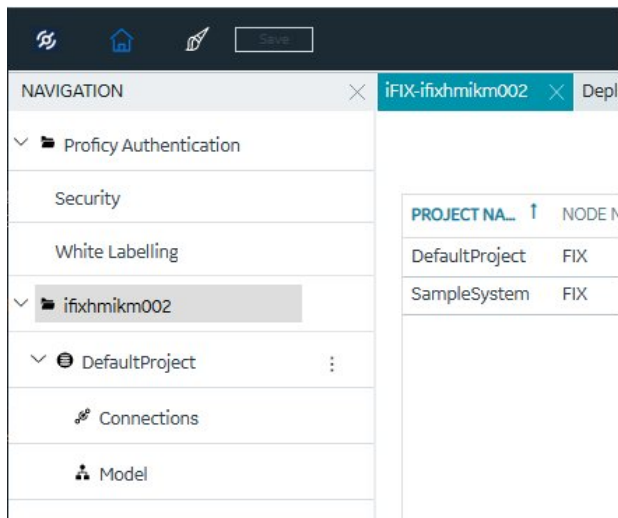
If you need to start iFIX with a specific node name other than the default, use the iFIX Startup app instead of Configuration Hub to start that instance.

Add a New Project

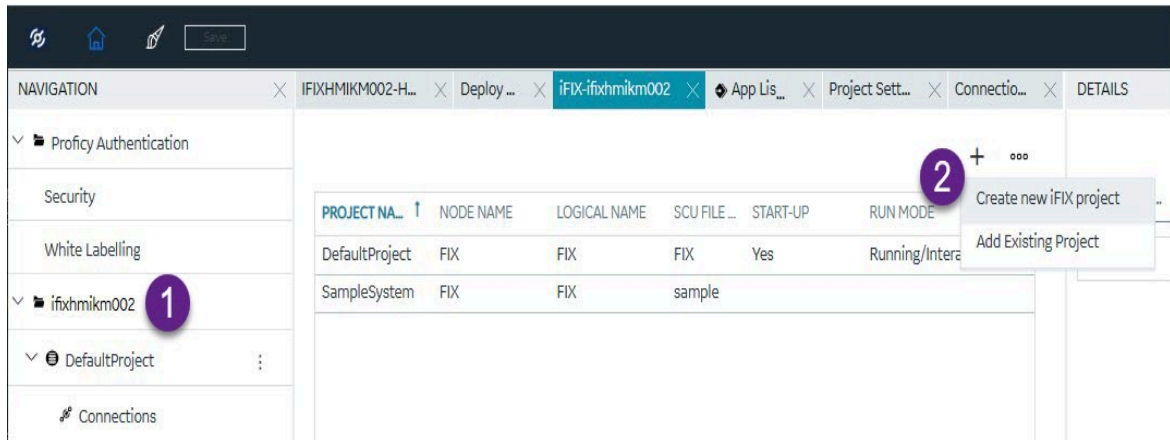
Use the following steps if you want to add a new project to your node.

Steps to Add a New Project

1. Configuration Hub, on the Navigation panel, click the node name. This action will open the Project Name panel.



2. Click the + icon at the top of the grid, and select **Create new iFIX project**.



The New Project dialog box appears.

3. Enter a Project Name, Node Name, and Logical Name, as shown in the following figure.

NEW PROJECT

PROJECT NAME

NODE NAME

LOGICAL NAME

4. Click **Create**.

You should now be able to view the new project from within Configuration Hub or the standard iFIX SCU application.

5. Manually copy any additional driver files to the new project's PDB folder on the installed iFIX instance. For example, for IGS, copy the Fix.igs or nodename.igs file from PDB folder in the iFIX install path to the new project's PDB folder. This copy only needs to be done once when you create the new project.



Important:

If you do not copy the driver files, like the one for the IGS I/O Driver, you will not be able to later save and publish your driver updates from Configuration Hub.

If you get error or fail to create a new iFIX project from the Configuration Hub, and iFIX access control is enabled with iFIX is running a service, shut down iFIX and then create the new project.

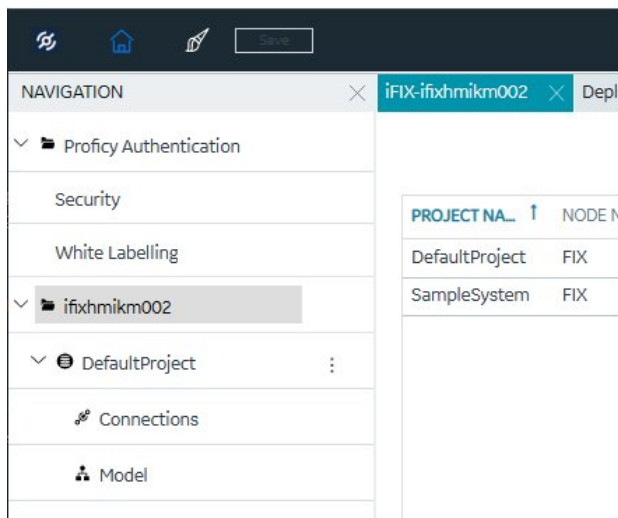
Troubleshooting

1. If you have issues publishing your driver changes to your new project, copy the driver files from PDB folder in the iFIX install path to the new project's PDB folder. For example, for IGS, copy the Fix.igs or nodename.igs file from PDB folder in the iFIX install path to the new project's PDB folder.
2. If you have issues creating a new project when iFIX is running with access control and enabled as a service, shut down iFIX and then create the new project. After you do that, you can start the project again and create, save, and publish any updated settings.

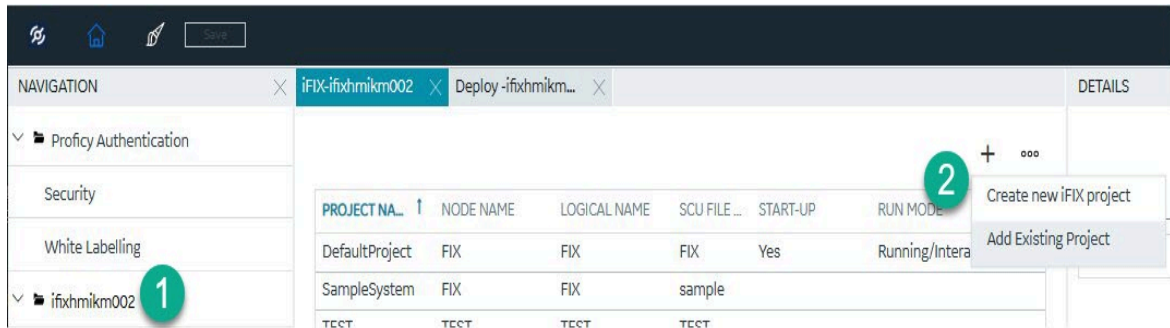
Add an Existing Project

Use the following steps if you want to add an existing project from another folder to Configuration Hub. Configuration Hub will recognize the new project after this is done.

1. Configuration Hub, on the Navigation panel, click the node name. This action will open the Project Name panel.



2. Click the + icon at the top of the grid and select **Add Existing project**.



The New Project dialog box appears.

3. Enter the Project Path, select the SCU file name, and then enter a Node Name and Logical Name, as shown in the following figure.

Add Existing Project

PROJECT PATH

PROJECT SCU FILE NAME

Select...

NODE NAME

LOGICAL NAME

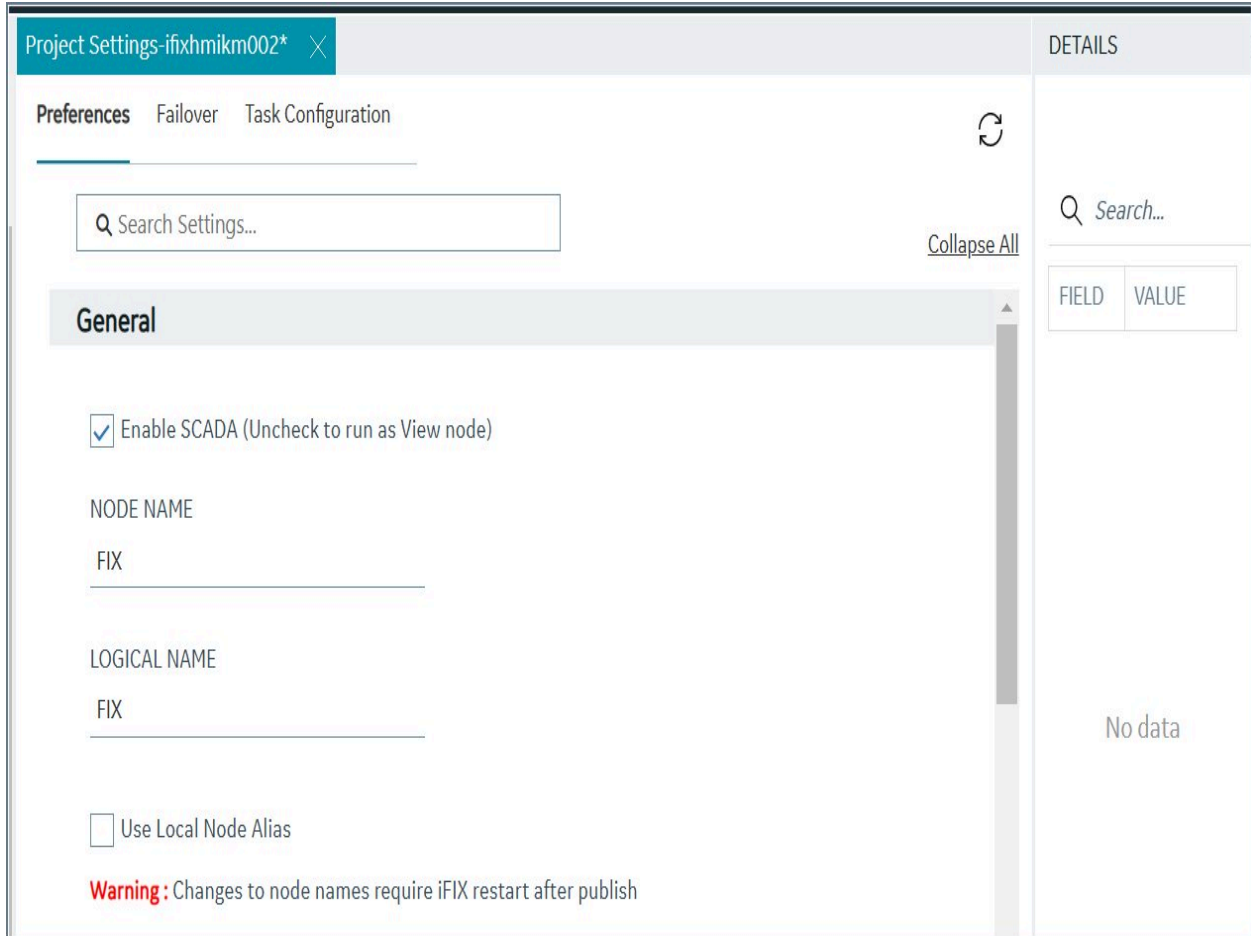
4. Click **Add**.

You should now be able to view the existing project from within Configuration Hub.

General Settings

The General settings allow you to define configuration options that apply to the node you want to configure. You can specify the SCADA or View node preference, the node name, the logical name, and the local node alias.

From the Navigation pane, select your node, iFIX project, and then Project Settings. Next, click Preferences. The General project settings appear at the top of the list as shown in the following figure.



The following table describes the General settings you can configure.

Field	Description
Enable SCADA (uncheck to run as View node)	Select this check box to use this node as a SCA-DA node. Clear the check box to use this node as a View node (iClient).
Node Name	Allows you to specify a unique local node name. Node names can be up to eight characters long. They can include alphanumeric characters, but must begin with a letter. Special characters cannot be used.

Field	Description
	<div style="border: 1px solid #ccc; padding: 10px; background-color: #fff9c4;"> <p>! Important: If modifying the iFIX node name here in Configuration Hub, after you save and publish your changes, you must restart iFIX (as a service) through Configuration Hub to view your applied changes. If the node name was modified in iFIX, and not displaying properly in this field, you must restart iFIX manually from iFIX Startup.</p> </div>
Logical Name	<p>Allows you to specify a unique local node name to specify the name in your operating system's Registry.</p> <p>Node names can be up to eight characters long. They can include alphanumeric characters, but must begin with a letter. Special characters cannot be used.</p>
Use Local Node Alias	<p>Allows you to specify a unique local node name to specify the name in your operating system's Registry.</p> <p>Node names can be up to eight characters long. They can include alphanumeric characters, but must begin with a letter. Special characters cannot be used.</p> <p>You must be logged in as a user in the Administrators group to change the Local Node Alias.</p>

Startup Options

The Startup Options let you define the initial settings you want to use when iFIX starts in run mode.

To access the Startup Options, from the Navigation panel, click your node, project, and then select Project Settings. Next, click Preferences and scroll to the Startup Options settings that appears second in the list.

The Startup Options appear as shown in the following figure.

Startup Options

Project

Run iFIX as service

Service Startup

Manual ▾

Other Options

Disable <Ctrl><Alt>

Disable Task Switching

Disable VBE Access

WorkSpace Options

Start Workspace in Run mode

Zoom To Fit in Run mode

Full Screen in Run mode

Fire DataChange Event on Startup


Extend workspace to support multiple monitors

Enable High Performance HMI Graphics

USER ACCOUNT DISABLED MESSAGE:

The following table describes the Startup Options that you can configure.

Field	Description
Run as iFIX Service	<p>Allows you to configure iFIX to run as a service under Microsoft Windows when you start iFIX. iFIX continues to run as a service for the next user who logs on. To stop the service, stop iFIX.</p> <p>You must be logged in as a user in the Administrators group to configure this settings. Additionally, this check box is unavailable when iFIX is running.</p>
Service Startup	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Manual: Requires that you manually start and stop iFIX via the UI, on demand. • Automatic: Allows you to automatically start iFIX when Windows starts. <p>This option is available only if you select the Run iFIX as a Service check box.</p>

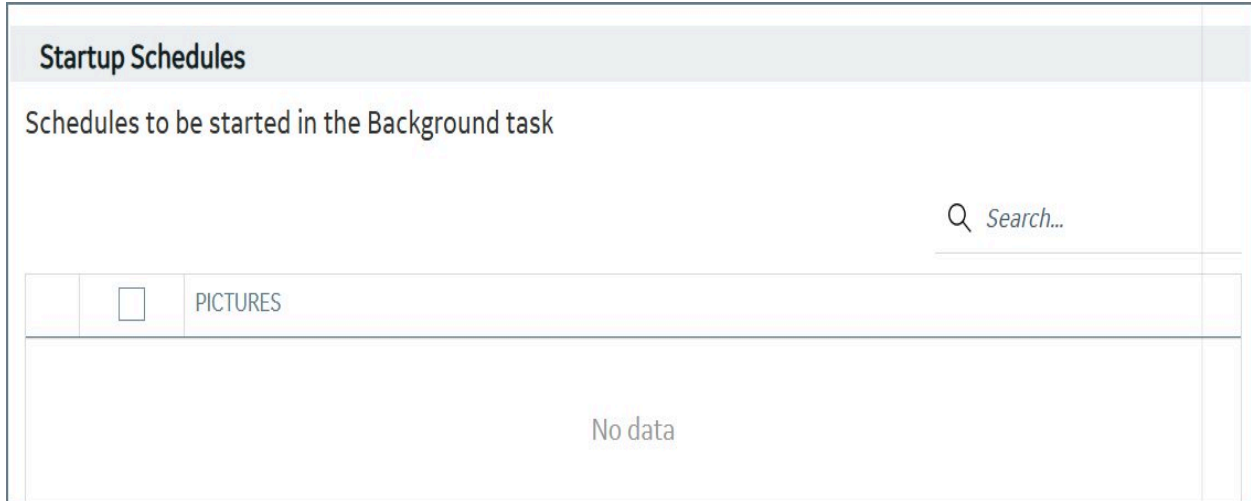
Field	Description
Disable <Ctrl><Alt><Delete>	Select this check box to disable the <Ctrl><Alt><Delete> key sequence at run-time, thereby restricting operators from accessing the Task Manager, changing their password, logging off, or shutting down the computer.
Disable Task Switching	<p>Select this check box to disable run-time task switching through <Alt><Tab> and the Start button.</p> <div data-bbox="820 630 1421 808" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: The Shift + F10 key macro does not work if you select this option. </div>
Disable VBE	Select this check box to allow you to restrict access to the Visual Basic Editor at run-time in the iFIX WorkSpace. If access is not restricted, the editor appears when a compilation or run-time error occurs, allowing you to correct the error. When you restrict access, the iFIX WorkSpace suppresses the Visual Basic Editor even if an error occurs.
Start Workspace in Run Mode	Select this check box to indicate that the iFIX WorkSpace starts in the run-time environment. Clear this check box to indicate that the iFIX WorkSpace starts in the configuration environment.
Zoom to Fit in Run Mode	Select this check box to suppress the scroll bars and to show the entire picture in the current picture window in run mode. Only pictures using Enhanced Coordinates that are opened in Run mode will honor this setting. If you do not want to apply this setting to a specific picture, then a script change under the picture initialization code is required. For more information, refer to the ZoomToFit Method section in iFIX Automation Reference e-book.
Full Screen in Run Mode	Select this check box to display pictures in the run-time environment with the maximum screen space

Field	Description
	possible. When the iFIX WorkSpace displays full-screen in the run-time environment, the menu bar is hidden. The system tree and all toolbars are always hidden in this environment.
Fire DataChange Event on Startup	<p>Select this check box to configure the Data Change event of an event object to fire only when there is new data after the initialization.</p> <p>Actions such as switching from the Configuration environment to the Run-time environment while an iFIX schedule is open will cause the DataChange event to trigger accordingly.</p> <p>If you select this option, iFIX fires the event when initializing the event object at the time you open a picture and switch to run mode. Clear this check box if you want events to fire only if the data source truly changes.</p>
Extend Workspace to Support Multiple Monitors	Select this check box if you plan to use multiple monitors with your iFIX displays.
Enable High Performance HMI Graphics	Select this check box to create high performance graphics in iFIX pictures that use the High Performance color set and the high performance settings for shapes and picture creation. For more information, refer to the Creating High Performance Pictures e-book.
User Account Disabled Message	Specifies the message that appears from the Electronic Signature dialog box when a user account is no longer valid.

Startup Schedules

Startup Schedules can also be viewed from Configuration Hub. Startup Schedules display the schedules configured to automatically load in the background when the background task is started.

To access Startup Schedules, from the Navigation panel, click your node, project, and then select Project Settings. Next, click Preferences and then scroll to the Startup Schedules settings that appear third in the list. The Startup Schedules appear as shown in the following figure.



Startup Pictures

The Startup Pictures settings displays the pictures that you want to open automatically when the iFIX WorkSpace starts in the run-time environment.

To access Startup Pictures, from the Navigation pane, select your node, iFIX project, and then Project Settings. Next, click Preferences and then scroll down to the Startup Pictures settings. The Startup Pictures appear as shown in the following figure. Select a check box to add that picture to the startup list.

Startup Pictures

Pictures to open when Workspace starts in Run mode

	<input type="checkbox"/>	PICTURES
::	<input type="checkbox"/>	ChartGroupDemo.grf
::	<input type="checkbox"/>	DynamoPopupHist.grf
::	<input type="checkbox"/>	HistorianDataEntryWizard.grf
::	<input type="checkbox"/>	HistorianDataExportWizard.grf
::	<input type="checkbox"/>	LineChartPopupHist.grf
::	<input type="checkbox"/>	LineChartPopupReal.grf
::	<input type="checkbox"/>	PT_HeaderMenuDemo.grf

Historian

From the Historian settings, you can choose to set whether you enable **Automatically configure tags for collection in Historian**, by clearing or selecting the check box.

From the Navigation panel, select your node, iFIX project, and then Project Settings. Next, click Preferences and then scroll to the Historian settings at the bottom of the list. The Historian settings appear as shown in the following figure.

Historian

Configuration of tags for collection in Historian

ENABLING THIS OPTION CAUSES ALL TAGS FROM YOUR CURRENTLY LOADED PDB FILE TO BE ADDED TO THE HISTORIAN FOR COLLECTION.

WARNING! ENABLING THIS GLOBAL OPTION WILL ALSO OVERWRITE CURRENT HISTORIAN CONFIGURATION FILES ON THE LOCAL SYSTEM.

Automatically configure tags for collection in historian

Select this check box to enable collection of all database tags by Proficy Historian.

Enabling this option will add all tags from the currently loaded database to Historian for collection on the next reload.

SCADA Failover

SCADA Enhanced Failover settings can be configured and viewed from Configuration Hub. SCADA Enhanced Failover is the ability to define two SCADA nodes to function as one logical node. The logical node provides data and alarms to its clients even if one of the SCADA nodes becomes inoperable. When you start iFIX on both nodes, one SCADA will be your active node, and the other will be your standby node.

When managing Failover settings, be sure that you review [Special Considerations for SCADA Enhanced Failover \(on page 198\)](#) before you make any changes.



Note:

Be aware that iFIX SCADA Enhanced Failover is not the same as [High Availability for Configuration Hub \(on page 50\)](#)

For complete details on setting up SCADA Enhanced Failover, see the [Enhanced Failover](#) e-book.

To access Failover settings, from the Navigation panel, select your node, iFIX project, and then Project Settings. Next, click Failover. The Failover settings appear as shown in the following figure.

Project Settings- ifxhmikm002 ✕
DETAILS

Preferences
Failover
Task Configuration

Enable Failover

Failover Setup

This Project node is Primary Secondary

Node Name

Logical Name

Partner SCADA Name

Security Area

Data Sync Protocol

FIE...	VALUE
No data	

The following tables describes the Failover settings you can manage or view.

Table 14. Failover Setup

Field	Description
Enable Failover	Use the slider to enable Enhanced Failover on this SCADA node.
Project Node Designation	<p>Select whether the node is the Primary or Secondary node in the Enhanced Failover configuration.</p> <p>For more details on setting up SCADA Enhanced Failover, see the Enhanced Failover e-book.</p>

Table 14. Failover Setup (continued)

Field	Description
Node Name	<p>Allows you to specify a unique local node name to specify the name in your operating system's Registry.</p> <p>Node names can be up to eight characters long. They can include alphanumeric characters, but must begin with a letter. Special characters cannot be used.</p>
Logical Name	<p>Allows you to specify a logical node name used for configuring redundancy.</p> <p>Node names can be up to eight characters long. They can include alphanumeric characters, but must begin with a letter. Special characters cannot be used.</p>
Partner SCADA Name	Enter the name of the partner SCADA node.
Security Area	<p>If using security areas in iFIX, enter the letter associated with the security area assigned to administrators of your Enhanced Failover configurations.</p> <p>Only one security area is supported for Enhanced Failover.</p>

Table 15. Data Sync Protocol

Field	Description
Protocol	Select the type of protocol you want to use: TCP or UDP. TCP is the default.
Transport Enable	Select to enable Data Sync Transport, where you configure you network preferences for data transport.
MAC Address	This field is for viewing purposes only. The Media Access Control (MAC) address represents a

Table 15. Data Sync Protocol (continued)

Field	Description
	unique identifier for the selected network adapter on the local computer.
IP Address	This field is for viewing purposes only. The Address is the IP address for the selected network adapter on the local computer.
Partner's IP Address	<p>Enter the IP address of the partner SCADA node.</p> <p>If you are configuring the primary SCADA, this IP address is the IP address of the corresponding network adapter on the secondary SCADA node.</p> <p>If you are configuring the secondary SCADA, this IP address is the IP address of the corresponding network adapter on the primary SCADA.</p> <p>The IP address that you enter should be a static or fixed IP address. Do not use DNS-assigned IP addresses for Enhanced Failover.</p>
Message Reply Count	The default setting is 3.
Bandwidth Limit (MBs)	The default setting is 0.
Watchdog Time	The default setting is 1.
Watchdog Timeout	Enter a value, in seconds, indicating how long you want ScadaSync.exe to wait before determining that this transport is not connected. The default setting is 4 seconds.
Message Timeout	Enter a value, in seconds, indicating how long ScadaSync.exe waits for an acknowledgement from the partner SCADA (indicating that a data packet is received successfully). If an acknowledgement is not received by this time-out period, the retry logic initiates according to the value of the Message Retry field.

Table 15. Data Sync Protocol (continued)

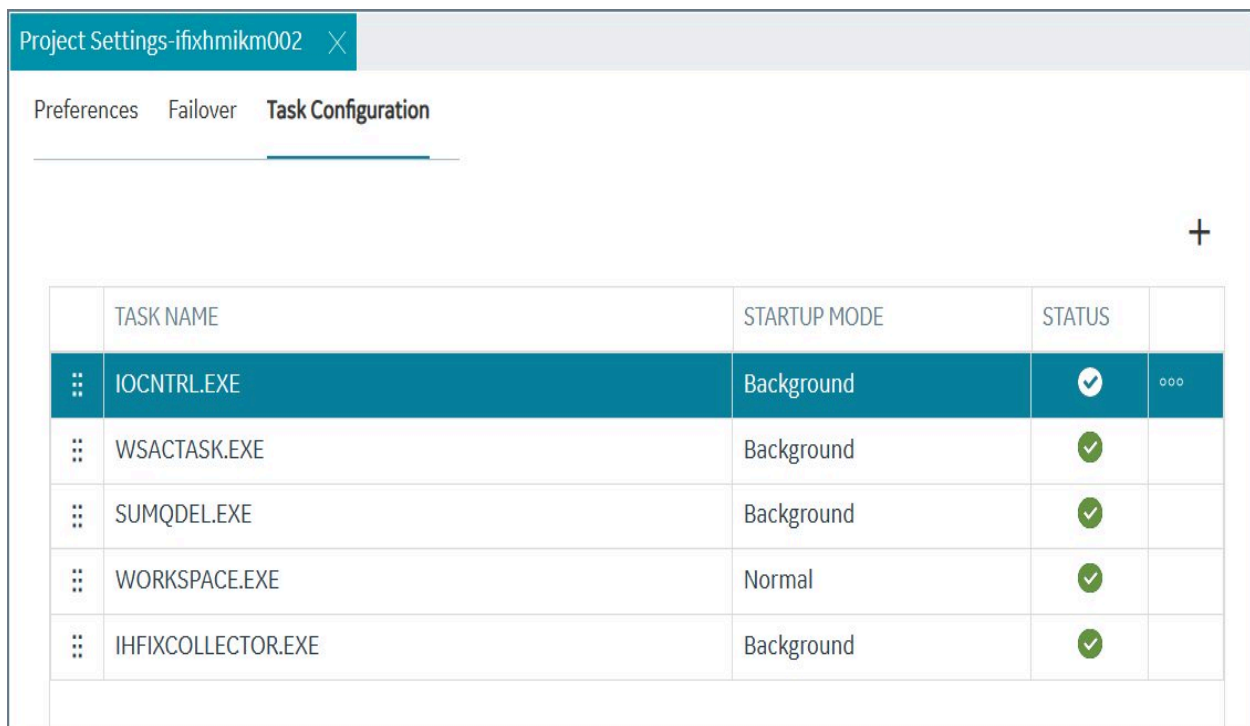
Field	Description
	<p>When a message times out, the SCADA Sync Monitor (a diagnostic program in iFIX) displays a message on the debug output screen. On this screen, the timer will show up as milliseconds. For more information on this screen in the SCADA Sync Monitor, refer to the Debug Log for Troubleshooting section.</p> <p>The default setting is 2 seconds.</p>

Task Configuration

From the Task Configuration, you can manage the tasks for automatic start-up, and whether they start as normal tasks or in the background.

The tasks listed in this dialog box start when you start iFIX. For example, if you always want to use I/O Control when you start iFIX, add a task for IOCNTRL.EXE to the top of the configured task list.

In the Navigation panel, select the node, project, and then **Project Settings**, and then click **Task Configuration**. The following figure shows an example of the Task Configuration screen.



Command line parameters can also be added for each task. iFIX executes the tasks in the same order as they appear in the configured task name list from the Details panel. Drag-and-drop tasks to move items up and down in the list.

If you run iFIX as a service, the tasks listed in the task list also start as a service.

**Note:**

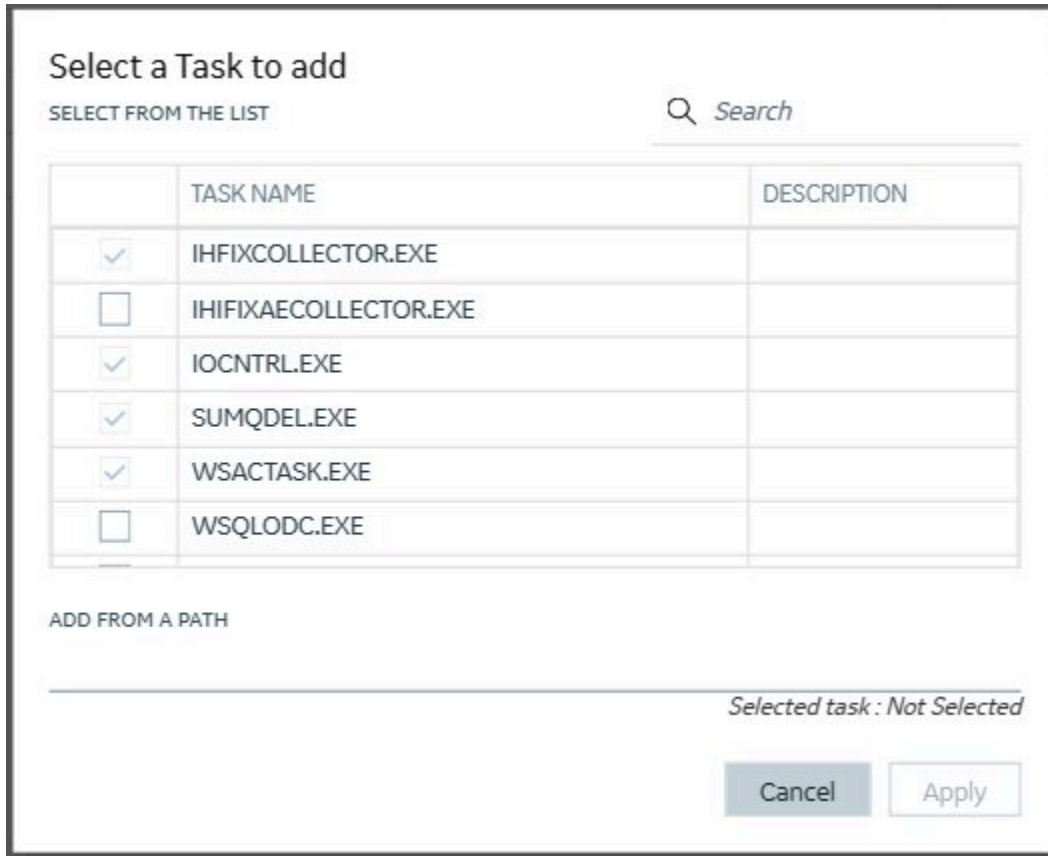
It is not recommended that you run Workspace.exe in the SCU task list when iFIX is running as a service.

Add a Startup Task Settings

To add a new task, click the plus (+) icon at the top of the task list.

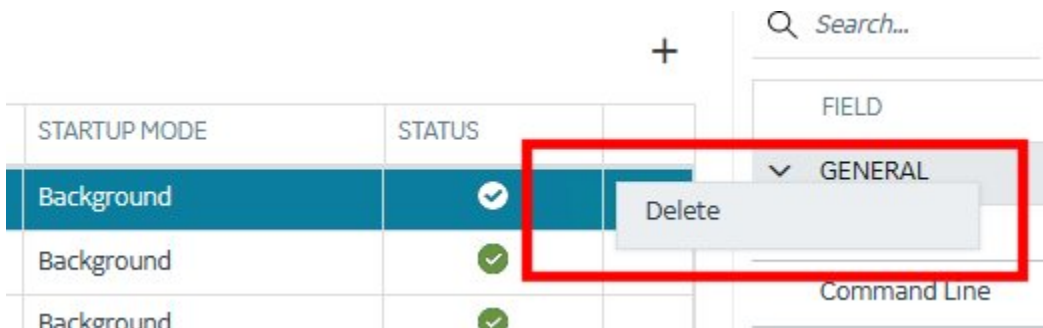
STARTUP MODE	STATUS
Background	✓
Background	✓

The Select a Task to Add dialog box appears. Select the executable from the list that you want to add on iFIX startup. The files that appear in this list are from the iFIX/LOCAL folder.



Delete a Startup Task


To remove a task from the list, select the task from the configured task name list, click the ellipsis (...) at the end of the row, and then click Delete.



Task Configuration Settings

The following table describes the Task Configuration settings you can configure on the Details panel.

Field	Description
Startup Mode	Select the mode for startup:

Field	Description
	<ul style="list-style-type: none"> • Normal: Allows you to start the task with its window open. • Minimize: Allows you to start the task with its window minimized. • Background: Allows you to start the task as a background task.
Command Line	<p>Allows you to add any command line parameters associated with the specified executable file. For example, you can define command line parameters for SAC (WSACTASK.EXE), I/O Control (IOCNTRL.EXE), and selected iFIX applications.</p> <p>For some tasks, you can enter the text for the command directly into the Value field. For other pre-defined ones, you need to select a task option to populate the Command-line field. For example, when adding an iFIX collector to the task list of an iFIX project from within Configuration Hub, you need to select the options such as Run as a Service. Otherwise, the command line is created with a dangling = sign, and does not start.</p> <div style="border: 1px solid #f0e68c; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Important:</p> <p>If you need to pass in a value associated with the command line, be sure that you either enter it in the Value field, or select a check box(es) from the Task Options to populate the Command line field.</p> </div> <p>To add command line parameters to third-party executables, check the application's reference documentation for valid entries.</p>
Task Options	These are options are specific to the file selected.

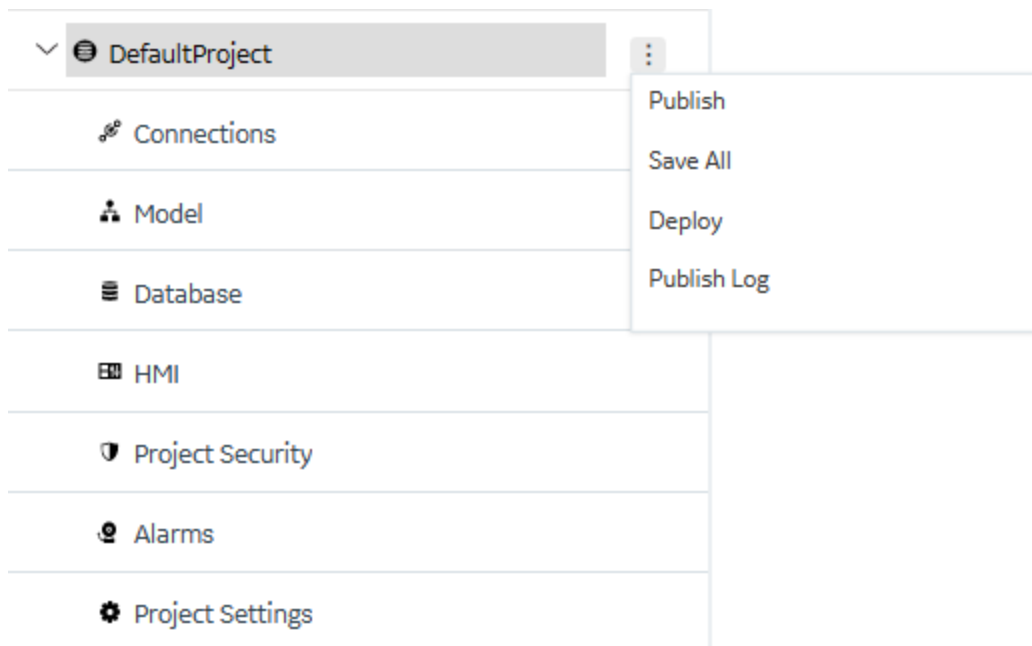
Deployment

Project Deployment

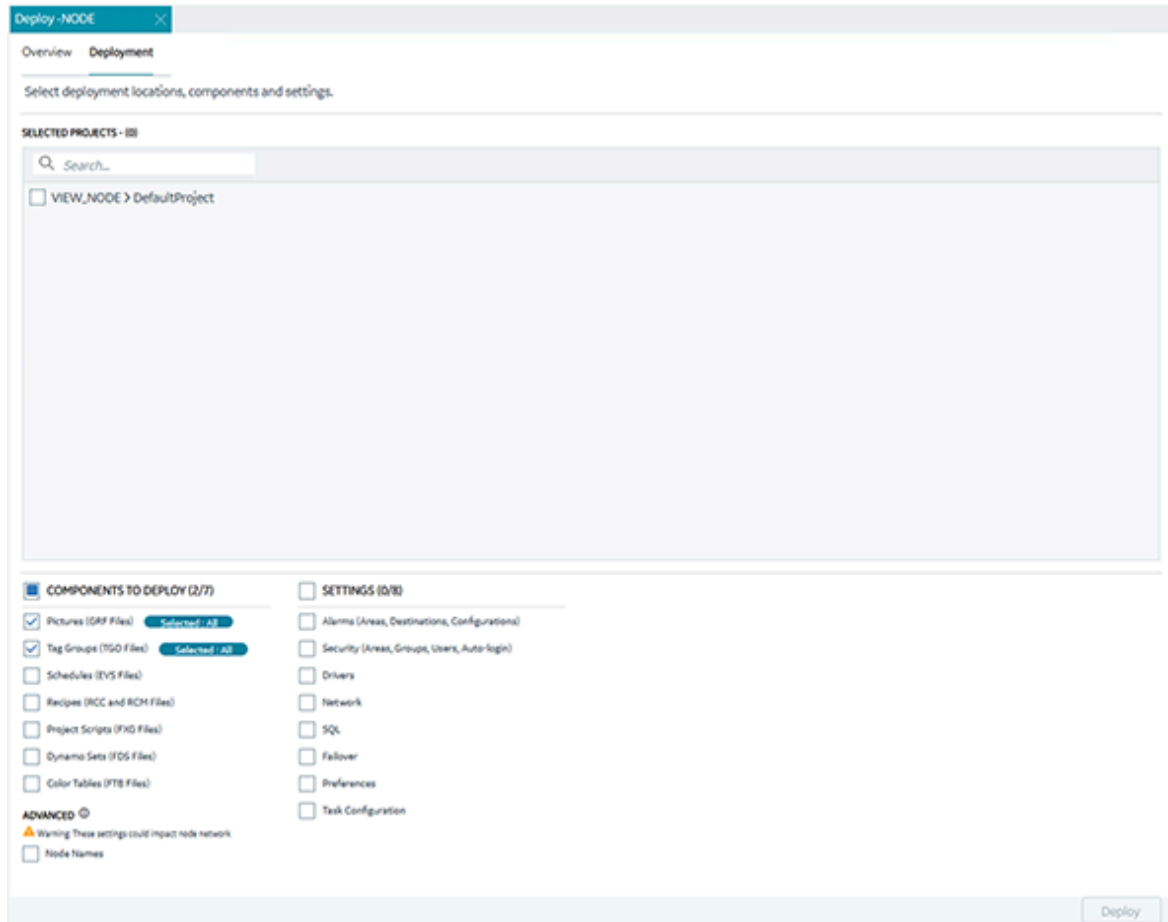
Project Deployment provides the ability to deploy (copy) key HMI components and/or settings between iFIX SCADA or View nodes. This feature allows a user to develop components/settings (for example: picture files, alarm areas, security groups, and so on) on one node and then easily transfer them to multiple nodes, eliminating the need to connect to each one to make local updates, or to employ shared folders as a means of distribution. To use this feature:

- The nodes must be running iFIX 2023 or later and be registered to a Configuration Hub server.
- The user must be a member of the Project Administration group (scada.project.admin) in Configuration Hub.

1. Log into Configuration Hub.
2. From the **NAVIGATION** pane, click the chevron for the iFIX node from which you want to copy (the “source” node) the components and/or settings.
3. Click the vertical ellipsis. From the menu that appears, click **Deploy**. This will open the **Deploy** panel.



4. The **Selected Projects** section will list all nodes to which components and/or settings can be deployed (the “target” node). Enable the checkboxes to select the “target” node(s). Any nodes not listed here may not be running the required version of iFIX or be registered to a Configuration Hub server.



5. Use the checkboxes for **Components To Deploy**, **Settings** and **Advanced** to enable the selection of specific items to be deployed to the target node. **Note:** The **Advanced** section contains only one item, **Node Names**. Exercise caution when selecting this item, as nodes on the same network must have unique names.
6. Within **Components To Deploy**, the items **Pictures** and **Tag Groups** are selected by default as they are the most common items deployed between nodes. For these two components, when selected, a **Selected:** button will indicate how many specific items are currently selected. Click the button to refine the list of specific items to deploy. A selection window will appear (for example, **Select Pictures to deploy**).



Important:

The deployment of pictures from subfolders is not supported. Only pictures in the **PIC** folder can be deployed.

7. Use the check boxes to select the specific items to be deployed. Click **Add**.

**Note:**

When you choose **Preferences**, be aware that only iFIX User Preferences are included. It does not include Node and SCU local startup settings.

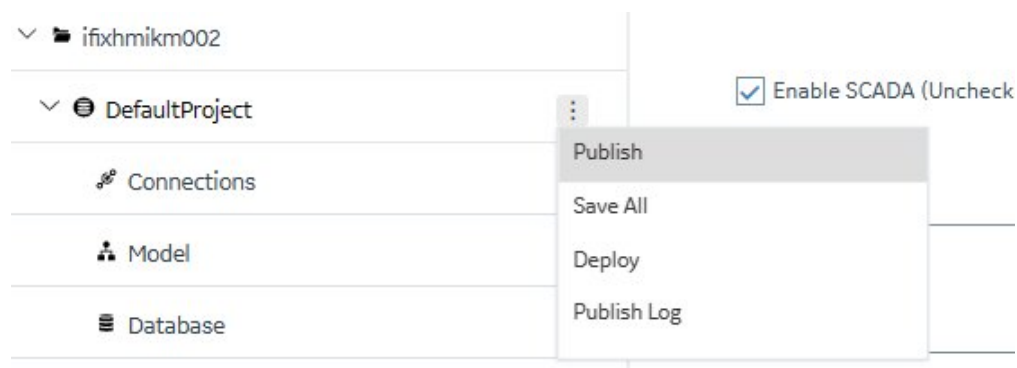
**Important:**

The following **Settings** cannot be deployed to View nodes (only to SCADA nodes): **Drivers** and **Failover**.

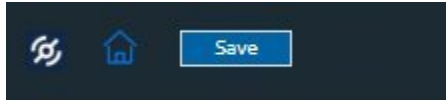
8. Once all items have been chosen, click **Deploy**.
9. Once the deployment has completed, click **Close**.
10. To see the items copied on the target node, select the target node from the **NAVIGATION** pane. Expand the node by clicking the chevron. Click the name of the panel into which you deployed the component/setting (for example, if you deployed a picture, select **HMI**). Click the tab for the panel in the main viewing area of the interface. Click the refresh icon (icon image to be inserted here) to update the list. Note that the new components/settings have been deployed to the target node, but are in an unpublished state.
11. For the new components/settings to take effect, they must be published on the target node.

Save and Publish

When configuring an iFIX node in Configuration Hub, access the **Publish** and **Save All** settings from the iFIX project name. The following figure shows an example of this menu.

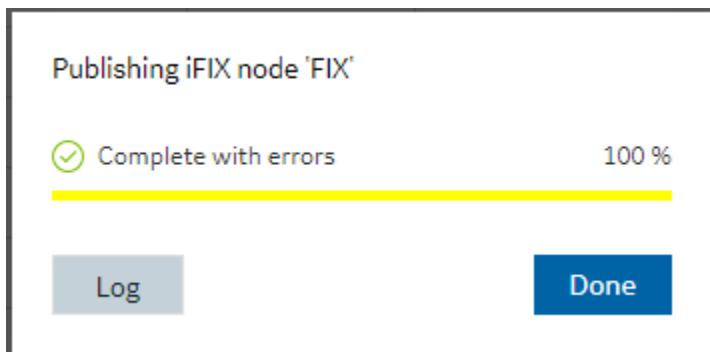


There is also a Save button available to save changes locally (but not publish them), from wherever you are in the Configuration Hub application.



For example, any changes in the Database panel must be saved before they are applied. If you do not want to save changes you have made, close the panel and choose not to save. An asterisk (*) appears in the panel tab when there are unsaved changes. Save is also used when editing a type, but the majority of operations in the Model tab are applied with no saving required.

Changes made in Configuration Hub for iFIX nodes do not update the running system until the changes are published. Until then, any changes are kept in a separate directory on the node being configured. When you are ready to apply the changes to the running system, click the Publish button to push the changes over to the server.

**Note:**

When Publishing, the Progress Bar does not update quickly and may take a while to complete. The Publish operation may take a while depending on the number of tags being published to the active iFIX node. Please wait for the Done indication.

You can discover unpublished changes in each panel via the status column in the panel's respective grids. Configured items are either in Published, Unpublished, or Modified state.

When publishing, you will be prompted to proceed and will see the progress of the publish. While publishing from one browser session, no other browser sessions are allowed to publish. Once publish has completed you will be able to download and view the results of the publish in a log file.

**Note:**

It is recommended that you only perform one publish operations at a time.

The log file reports the results and contains sections for Unpublished updates, modified updates and deleted update results.

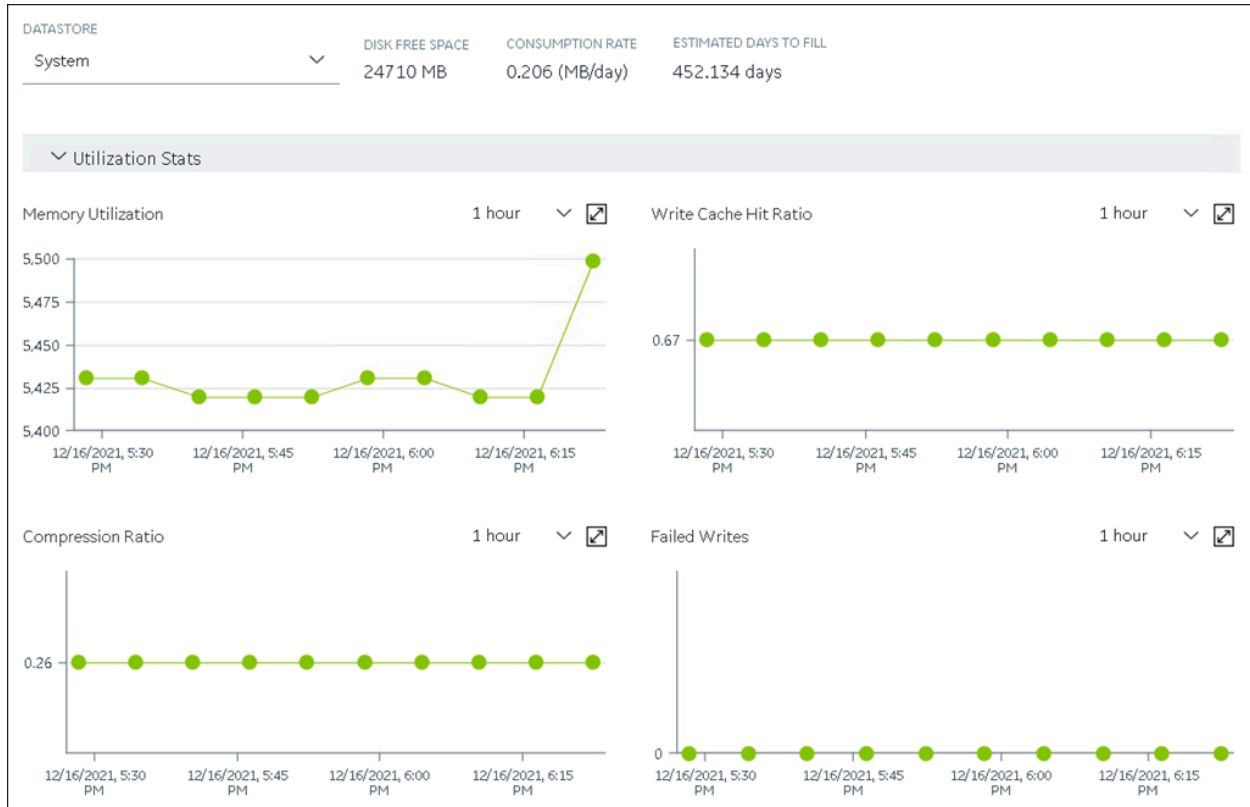
During a publish, depending on your system and other factors, your publish may Fail completely (for example if the connection is lost to a the SCADA), Succeed, or be Complete with Errors. When partially successful, the log file will be the best source to determine what did not publish fully.

Chapter 4. Historian

Overview of Historian with Configuration Hub

About Historian in Configuration Hub

The Configuration Hub application allows you to manage the Historian models, Historian systems, and their components.



Advantages of Using Configuration Hub:

- **Creating a Historian model:** You can create and manage object models, which is a hierarchical classification of objects. A model contains object types, variables, and instances.
- **A single application that enables you to manage multiple Historian systems:** A Historian system is a network of Historian servers that collect, store, and retrieve data related to tags, alarms, and events. You can create and manage Historian systems using Configuration Hub. In addition, you can manage collectors, data stores, and tags.

- **Horizontal scalability:** You can increase the storage capacity of a Historian system by connecting multiple software entities so that they work as a single logical unit. This will improve the performance of the Historian system. The storage capacity depends on the number of Historian licenses that you have purchased.
- **High availability:** You can create mirror locations in a Historian system to achieve high availability of the server. If one of the servers is not available, you can retrieve data from the remaining servers in the mirror location.
- **Ease of setting up:** You can install all the collectors used in a Historian system easily by providing the required details with the help of the user-friendly interface.

Types of Historian Systems

- **Stand-Alone:** In a stand-alone Historian system, there is only one Historian server. This type of system is suitable for a small-scale Historian setup. For information on setting up a stand-alone Historian system, refer to [About Setting up a Stand-Alone Historian System \(on page 907\)](#).
- **Horizontally scalable:** In a horizontally scalable Historian system, there are multiple Historian servers, all of which are connected to one another. This type of system is used to scale out the system horizontally. For example, if you have 5,00,000 tags in your Historian system, you can distribute them among the various servers to improve performance. For information on setting up a horizontally scalable system, refer to [About Setting up a Horizontally Scalable System \(on page 911\)](#).

Limitations

- If only one machine remains in a mirror location, you cannot remove it.
- You cannot add comments, enable the debug mode, pause data collection, resume data collection, or modify an instance of offline collectors. In addition, you cannot compress network messages.
- If you install Configuration Hub and the Web Admin console on the same machine, and use self-signed certificates for both of them, the login page for Configuration Hub does not appear. To prevent this issue, disable the domain security policies:
 1. Access the following URL: `chrome://net-internals/#hsts`
 2. In the **Domain Security Policy** section, in the **Delete domain security policies** field, enter the domain name for Configuration Hub, and then select **Delete**.
- If the primary server is down, you cannot add tags using a distributed node because the Configuration Manager service is down.

Configuration Hub Workflow for Historian

This topic provides the high-level steps in using Configuration Hub with Historian.

1. [Set up Configuration Hub](#). This involves installing the Historian server, the collectors, and Web-based Clients.
2. [Apply the license](#).
3. Depending on your requirements, set up [a stand-alone system \(on page 907\)](#) or [a horizontally scalable system \(on page 911\)](#). This involves adding the required components.

**Note:**

When you set up Configuration Hub, by default, a system and a data store are created. You can add more systems and data stores as needed.

4. For a horizontally scalable system, you can choose to [set up high availability \(on page 917\)](#).
5. As needed, [create an object model \(on page 921\)](#).
6. [Specify the tags for data collection \(on page 909\)](#).

After you perform these initial steps, data is collected and stored in the Historian server. You can then retrieve and analyze the data.

Setting up Configuration Hub for Historian

About Setting up Configuration Hub with Historian

To set up Configuration Hub, you must perform the following steps:

1. [Install the Historian server \(on page 880\)](#).
 - For a stand-alone Historian server, install single-server Historian.
 - For a horizontally scalable Historian server, install the mirror primary server and distributed/mirror servers.
2. [Install Web-based Clients \(on page 885\)](#).
3. [Install collectors \(on page 898\)](#).
4. [Perform the post-installation tasks \(on page 901\)](#).

If you want to upgrade Configuration Hub, refer to [Upgrade Configuration Hub \(on page 902\)](#).

After you install or upgrade the required components, you can [access Configuration Hub \(on page 902\)](#).

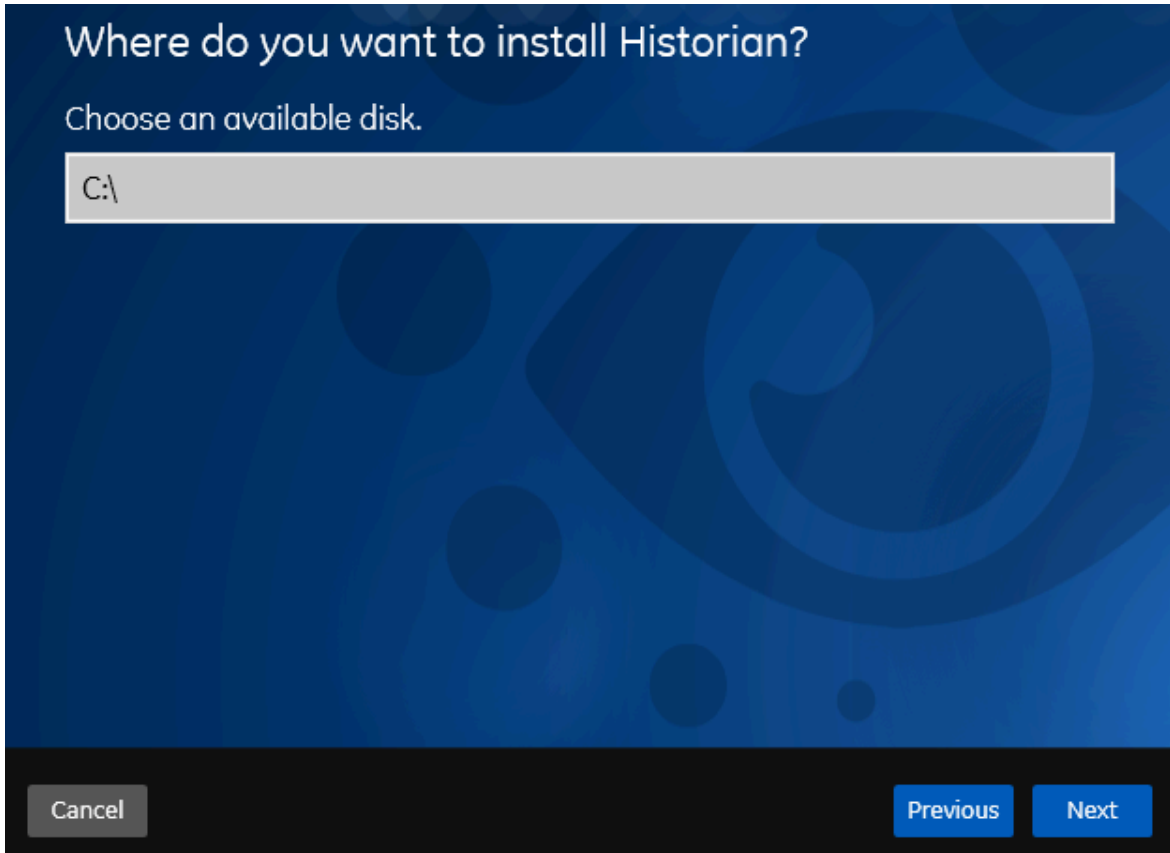
Install the Historian Server Using the Installer

- [Set up the Historian environment.](#)
- If you are changing the role of a Historian server that was previously a distributed/mirror server to any other configuration (single-server or mirror primary server), you must first [Uninstall Historian](#).
- If you are installing a distributed/mirror server, use the same configuration, license key, installation drive, Proficy Authentication instance, and domain as the primary server.

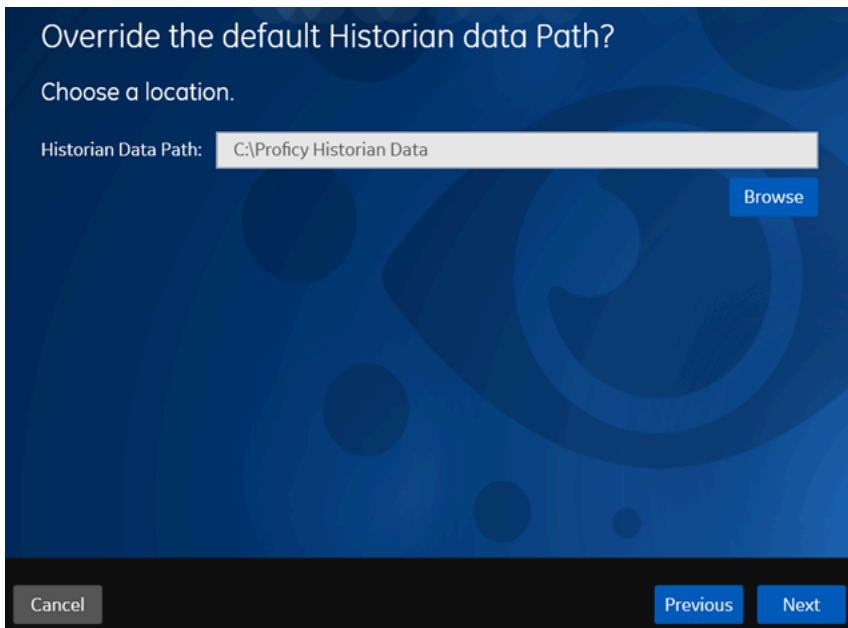
This topic describes how to install the Historian server using the installer.

You can also [install it at a command prompt](#).

1. Log in as an administrator to the machine on which you want to install the Historian server.
2. Run the `InstallLauncher.exe` file.
3. Select **Install Historian**.
The welcome page appears.
4. Select **Next**.
The license agreement appears.
5. Select the **Accept** check box, and then select **Next**.
The **Where do you want to install Historian?** page appears.



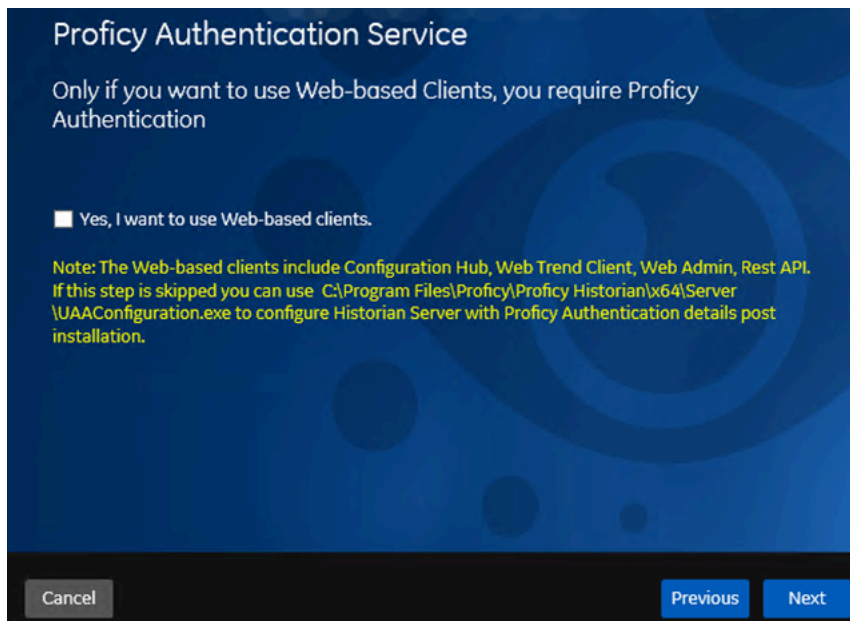
6. If needed, change the default installation drive of the Historian server, and then select **Next**.
The **Override the default Historian data Path?** page appears.



- If needed, change the default folder of the log files, and then select **Next**. If you want to include the Historian server in a cluster, enter the path to the shared folder of the cluster.

The **Proficy Authentication Service** page appears.

Only if you want to use Web-based Clients (such as Configuration Hub, Trend Client, the Web Admin console, and REST APIs), you need Proficy Authentication. Otherwise, you can skip this step. If you use Web-based Clients, Proficy Authentication is required for user authentication. It provides identity-based security for applications and APIs. It supports open standards for authentication and authorization, including Oauth2.



- If you want to use Web-based Clients, select the **Yes, I want to use Web-based Clients** check box, and provide values as described in the following table.

Field	Description
Proficy Authentication server name	Enter the name of the machine on which the Proficy Authentication server is installed. If the machine uses a fully qualified domain name (FQDN), provide the FQDN. By default, the local hostname is considered.
Public https port	Enter the port number used by the Proficy Authentication service. The default value is 443. Ensure that this port number matches the one

Field	Description
	on the TCP Port Assignments page during Web-based Clients installation.

**Note:**

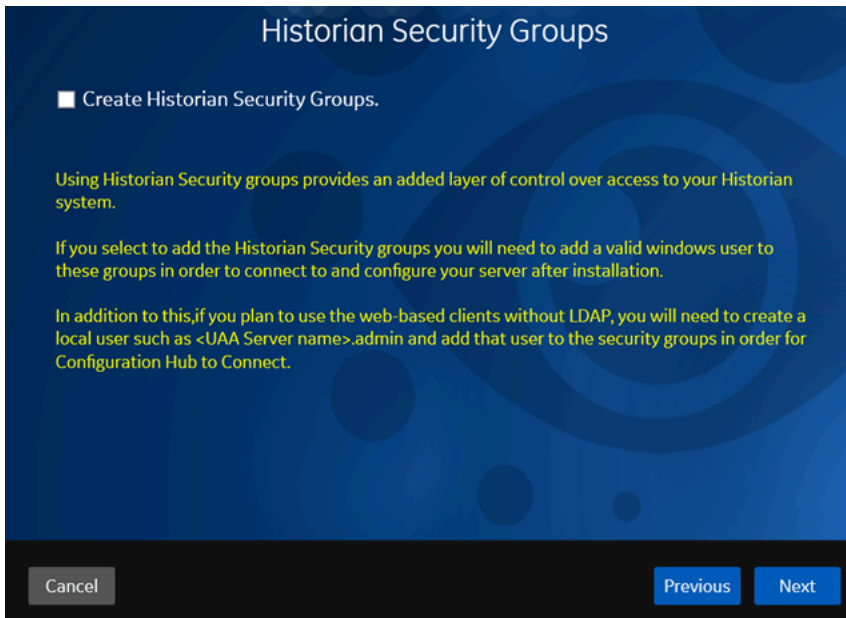
- You can install a Proficy Authentication service using Operations Hub or Historian Web-based Clients. You can provide the URL of an existing Proficy Authentication instance. Or, if a Proficy Authentication service is not available, you can install it during Web-based Clients installation.
- If you change the Proficy Authentication server for Web-based Clients later, you must [change the Proficy Authentication server for the Historian server](#) as well. You can do so using the Proficy Authentication Configuration tool without the need to install the Historian server again.

9. Select **Next**.

The **Historian Security Groups** page appears.

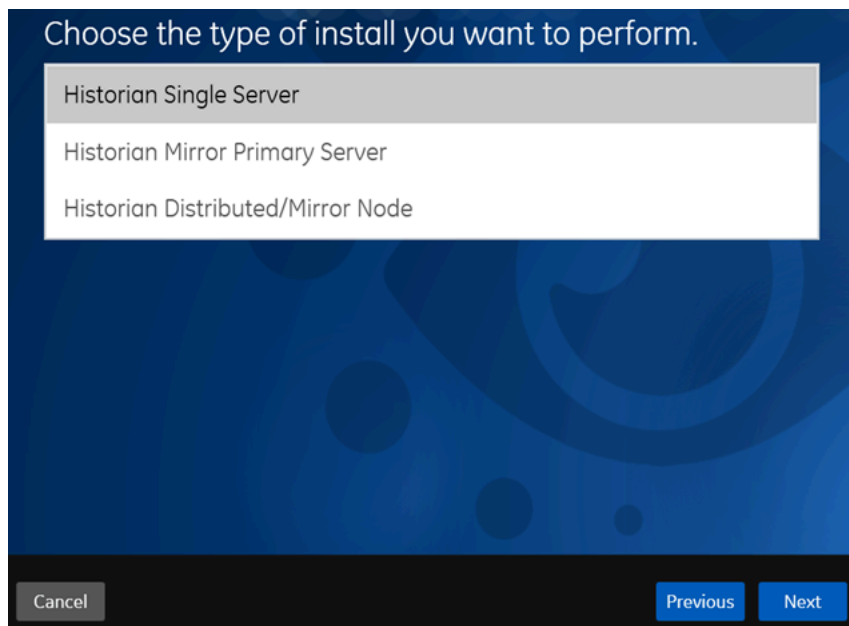
Using Historian security groups provides an added layer of control over access to your Historian system.

By default, the option to create Historian security groups is not selected.



10. If you want the installer to create [Historian security groups](#), select the corresponding check box, and then select **Next**.

The **Choose the type of install you want to perform** page appears.



11. Select the type of the Historian server that you want to install, and then select **Next**.
 - **Historian Single Server:** This is for a stand-alone Historian system, which contains only one Historian server. This type of system is suitable for a small-scale Historian setup.
 - **Historian Mirror Primary Server:** This is for a horizontally scalable Historian system, which contains multiple Historian servers, all of which are connected to one another. Installing this server will allow you to add machines and distributed/mirror servers to this system.
 - **Historian Distributed/Mirror Node:** This is for a horizontally scalable Historian system. Installing this server will allow you to add this node to a primary server.

The **Ready to Install** page appears.

12. Select **Install**.

The installation begins.

13. When you are asked to reboot your system, select **Yes**.

The Historian server is installed on your machine in the following folder: `<installation drive>:\Program Files\Proficy\Proficy Historian\x64\Server`, and the following registry path is created: `HKEY_LOCAL_MACHINE\SOFTWARE\Intellution, Inc.\iHistorian\Services`.

In addition, the following components are installed:

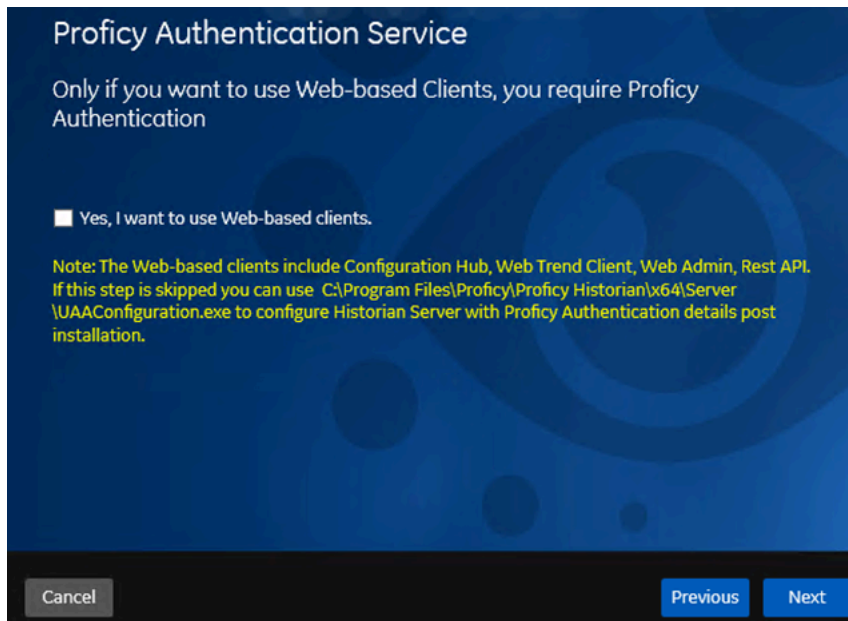
- **The RemoteCollectorConfigurator utility:** A command-line tool, which allows you to manage collectors remotely. By default, it is located in the `C:\Program Files\GE Digital\NonWebCollectorInstantiationTool` folder. For instructions on using this

utility, refer to [Overview of Remote Collector Management](#) About Installing and Managing Collectors Remotely.

- **The Proficy Authentication Configuration tool:** A utility that allows you to specify the Proficy Authentication server details to match with the Proficy Authentication server used by Web-based Clients. By default, it is located in the `C:\Program Files\Proficy\Proficy Historian\x64\Server` folder. For instructions on using this tool, refer to [Change the Proficy Authentication Server](#).

Install Web-Based Clients Using the Installer

1. [Install the Historian server \(on page 880\)](#). During the installation, in the **Proficy Authentication** page, select the **Yes, I want to use Web-based Clients** check box, and provide the Proficy Authentication server name and port number.



2. If you want to use Web-based Clients in a cluster environment, ensure that your network is enabled for multicast traffic, and [set up high availability](#) on each node in the cluster.

This topic describes how to install Web-based Clients using a GUI-based installer. During the installation, you can choose to use Web-based Clients in a cluster environment, thus ensuring high availability of connection to the Historian server using the client applications.

1. Run the `InstallLauncher.exe` file.
2. Select **Install Web-based Clients**.
The welcome page appears.

3. Select **Next**.

The license agreement appears.

4. Select the **Accept** check box, and then select **Next**.

The **TCP port assignments** page appears.

TCP port assignments	
Public https port:	443
Proficy Authentication http port:	9480
Proficy Authentication database port:	9432
Historian http port:	8070
Historian database port:	8432
Proficy Authentication ldp config service port:	7010
Proficy Authentication security app port:	7011

Note: Public HTTPS port cannot be changed as the Proficy Authentication server already exists on the local machine. It may have been installed with previous versions of Historian Web-based Clients or with other products such as Operations Hub or common components.

Buttons: Cancel, Previous, Next

5. As needed, change the values for TCP port assignments as described in the following table, and then select **Next**.

Field	Description
Public https port	Port for https protocol communication used by Web-based Clients (through a firewall). The default value is 443. Ensure that this port number matches the one you specify while installing the Historian server. In addition: <ul style="list-style-type: none"> ◦ If you will install Operations Hub later on the same machine, the value that you provide in this field is populated while installing Operations Hub. ◦ If you have already installed Operations Hub on the same machine, this field is disabled and populated with the value you have provided while installing Operations Hub.
Proficy Authentication http port	Port for http protocol communication used by the Proficy Authentication service. The default value is 9480.

Field	Description
Proficy Authentication database port	Port for the Proficy Authentication database. The default value is 9432.
Historian http port	Port for the http protocol communication used by Web-based Clients. The default value is 8070.
Historian database port	Port for the PostgreSQL Historian database. The default value is 8432.
Proficy Authentication Idp config service port	Port for the Configuration Hub identity provider service. The default value is 7010.
Proficy Authentication security app port	Port for the Proficy Authentication Configuration tool. The default value is 7011.

The **Fully Qualified Domain Name(s)** page appears.

- If you will install Operations Hub later on the same machine, the value that you provide in the **FQDNs** field is populated while installing Operations Hub.
- If you have already installed Operations Hub on the same machine, the **FQDNs** field is disabled and populated with the value you have provided while installing Operations Hub.

Fully Qualified Domain Name(s).

To allow users to access Historian web applications remotely using fully qualified domain names (FQDN), please list one or more here, separated by semicolons. Otherwise, you may leave this blank.

FQDNs:

Cancel
Previous
Next

6. In the **FDQNs** field, enter the fully qualified domain names, and then select **Next**.

This enables you to access Historian web applications remotely. You can use it to access the Web Admin console using alias names. Enter the values separated by commas.

To access the Web Admin console using any of the following URLs, enter

`Test.abc.ge.com,localhost,127.0.0.1,aliasName`

- [https:// Test.abc.ge.com /historian-visualization/hwa](https://Test.abc.ge.com/historian-visualization/hwa)
- [https:// 127.0.0.1 /historian-visualization/hwa](https://127.0.0.1/historian-visualization/hwa)
- [https:// aliasName /historian-visualization/hwa](https://aliasName/historian-visualization/hwa)
- [https:// localhost /historian-visualization/hwa](https://localhost/historian-visualization/hwa)



Important:

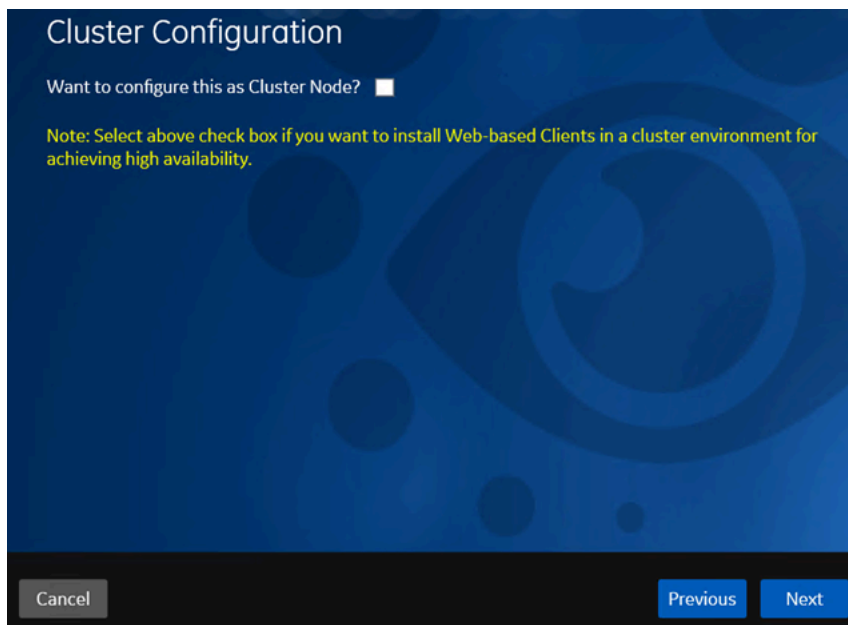
- Do not enter a space between the values.
- You must add the IP address and alias name in the `hosts` file located at `C:\Windows\System32\drivers\etc`. The IP address that you add must be a static or fixed IP address.

Format: `<IP address> <alias name>`

Example: `1.2.3.4 myservername`

- FQDN is not supported for Configuration Hub.

The **Cluster Configuration** page appears.



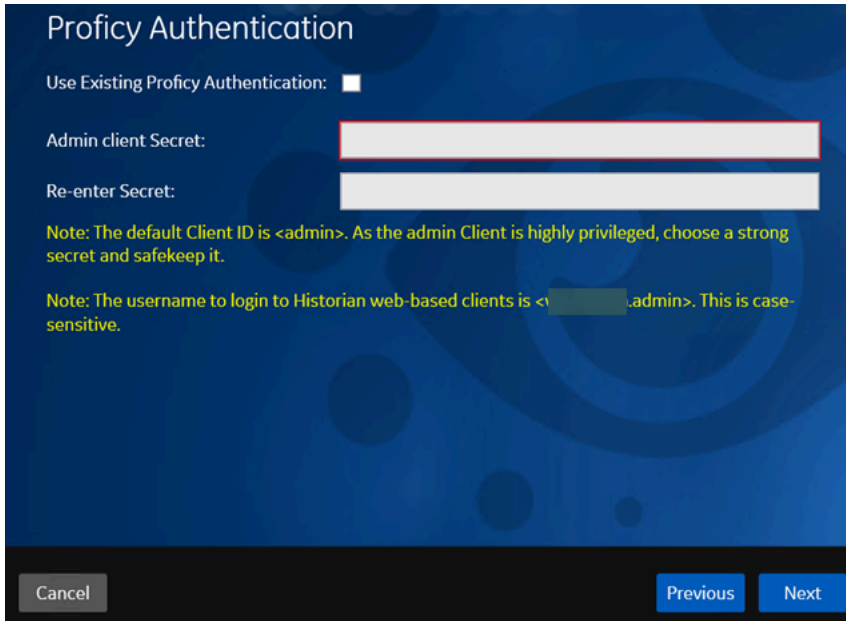
If, however, you are upgrading Web-based Clients, this page does not appear. In that case, skip the next step.

7. If you want high availability of Web-based Clients, select the **Cluster Node** check box, and enter values as described in the following table.

Field	Description
Historian Database Folder	Provide the database folder in the shared drive that you have created. The default value is C:\ProgramData\GE\OperationsHub. You <i>must</i> change this value.
Cluster FQDN	Enter the client access point of the role for which you have added the resources while setting up high availability .
Multicast Address	If needed, modify the common IP address that all the nodes in the cluster can use. Enter a value between 224.0.0.0 and 239.255.255.255 (or a hostname whose IP address falls in this range). The default value is 228.0.0.4.
Historian Cluster Membership Port	If needed, modify the common port number that all the nodes in the cluster can use. The default value is 45564. This port number, in conjunction with the multicast address, is used to create the cluster.
Historian Cluster Receiver Port	If needed, modify the multicast port number that you want to use for incoming Historian data. The default value is 4000.

8. Select **Next**.

The **Proficy Authentication** page appears, allowing you to choose whether you want to install Proficy Authentication along with Web-based Clients installation or use an existing Proficy Authentication.



- If you want to install Proficy Authentication, clear the **Use External Proficy Authentication** check box. If you want to include Proficy Authentication in the cluster, you must install Proficy Authentication locally on each cluster node.
 - If you want to use an existing Proficy Authentication server, select the **Use External Proficy Authentication** check box. Proficy Authentication is detected if you installed it using a unified installer or Operations Hub, or if Historian uses Proficy Authentication installed remotely from an earlier version.
9. If you want to install Proficy Authentication, enter the **Admin client secret**, re-enter the secret, and then select **Next**.

The admin client secret must satisfy the following conditions:

- Must not contain only numbers.
- Must not begin or end with a special character.
- Must not contain curly braces.



Note:

The format of username for Historian Web-based Clients is <host name>.admin, where <host name> is the machine on which Web-based Clients are installed. And, the default client ID is admin. Both the host name and client ID are case-sensitive.

If, however, the Proficy Authentication server hostname is long, resulting in a username longer than 20 characters, Windows does not allow you to create the user. In that case, you




can create a Proficy Authentication user, and then [create the corresponding Windows user](#), using the uaa_config_tool utility.

10. Alternatively, if you want to use an external Proficy Authentication service (that is, a Proficy Authentication instance already installed by an external application such as Operations Hub):

a. Select the **Use External Proficy Authentication** check box.

The fields for the external Proficy Authentication service appear.

b. Enter values as described in the following table.

Field	Description
Proficy Authentication Base URL	<p>Enter the URL of the external Proficy Authentication server in the following format: <code>https://<Proficy Authentication server name>:<port number></code>, where <code><Proficy Authentication server name></code> is the FQDN or hostname of the machine on which Proficy Authentication is installed. By default, the port number is 443.</p> <div style="border: 1px solid #0070c0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note: Do not enter a trailing slash character.</p> </div>
Admin Client ID	<p>Enter the client name that you provided while installing the external Proficy Authentication. The default value is admin.</p>

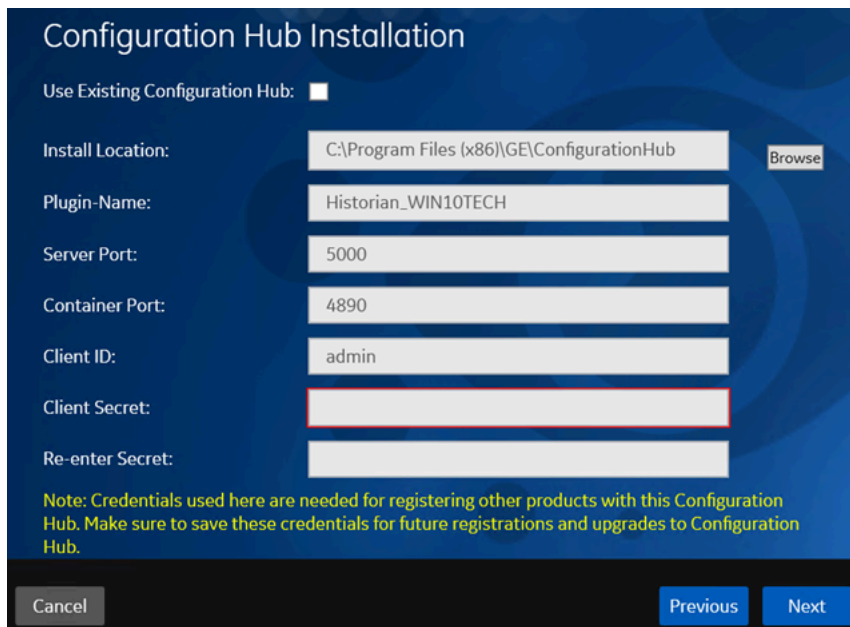
Field	Description
Admin Client Secret	Enter the client secret that you provided while installing the external Proficy Authentication.

c. Select **Test Connection**.

The results of the connection test appear. You cannot proceed until the connection is successful.

11. Select **Next**.

The **Configuration Hub Installation** page appears, allowing you to choose whether you want to install Configuration Hub along with Web-based Clients or use an existing Configuration Hub.



Configuration Hub allows you to add and manage a collector instance remotely. For more information, refer to [About Historian in Configuration Hub \(on page 877\)](#) [About Configuration Hub](#).

If, however, an earlier version of Configuration Hub is available on the same machine, you will be prompted to enter the details of the existing Configuration Hub, and it will be upgraded to the latest version. If that happens, skip the next step.

**Important:**

By default, Configuration Hub points to the same Proficy Authentication server as the one you provided during the Historian server installation. If you want to install Web-based Clients in a cluster environment, ensure that:

- Configuration Hub does not use the same Proficy Authentication server as that used by the cluster.
- The Proficy Authentication and Configuration Hub details must be the same for all cluster nodes.

12. If you want to install Configuration Hub, ensure that the **Use Existing Configuration Hub** check box is cleared, and then provide values as described in the following table.

Field	Description
Install Location	If needed, modify the installation folder for Configuration Hub.
Plugin Name	If needed, modify the name of the Configuration Hub plugin for Historian. The default value is in the following format: Historian_<host name>. If, however, you are installing Web-based Clients in a cluster environment, the default value is Historian_<cluster name>. You can modify this value, but provide the same value for all the nodes in the cluster.
Server Port	If needed, modify the port number that you want to use for the web server (NGINX). The default value is 5000. If you want to install Web-based Clients in a cluster environment, provide the same value for all the nodes in the cluster.
Container Port	If needed, modify the port number for the Configuration Hub container. The default value is 4890.
Client ID	Enter the username to connect to Configuration Hub. The default value is admin. The value that you enter can contain:

Field	Description
	<ul style="list-style-type: none"> ◦ All English alphanumeric characters (ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz_0123456789) ◦ The following special characters: ><:~!@#%&*?
Client Secret	<p>Enter the password to connect to Configuration Hub. The value that you enter can contain:</p> <ul style="list-style-type: none"> ◦ Must contain at least eight characters. ◦ All English alphanumeric characters (ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz_0123456789) ◦ The following special characters: ><:~!@#%&*?
Re-enter Secret	<p>Re-enter the password to connect to Configuration Hub.</p>

13. Alternatively, if you want to use an existing Configuration Hub:

- a. Select the **Use External Configuration Hub** check box. This check box is disabled if an existing Configuration Hub is detected.
The fields for external Configuration Hub appear.

Configuration Hub Installation

Use Existing Configuration Hub:

Plugin-Name:

Server Name:

Server Port:

Client ID:

Client Secret:

Test Connection Status: Test connection with Existing Configuration Hub Server is pending; click Test Connection

Enter the Client ID and Secret that you provided while installing Configuration Hug plugin for Historian to register with existing Configuration Hub.

b. Provide values as described in the following table.

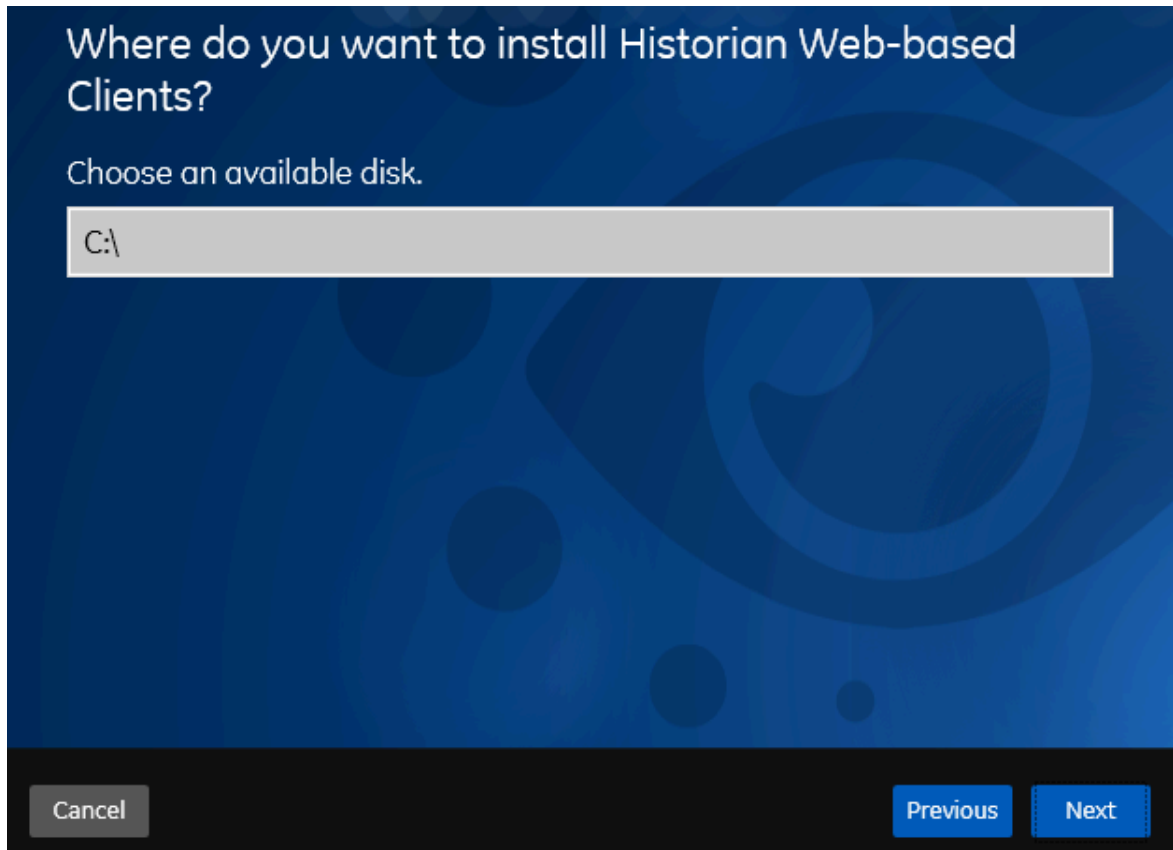
Field	Description
Plugin Name	If needed, modify the name of the Configuration Hub plugin for Historian. The default value is in the following format: Historian_- <host name>
Server Name	Enter the server name or the FQDN of the existing Configuration Hub server, as displayed in the address bar of the browser when you access Configuration Hub from the machine where Configuration Hub is installed.
Server Port	If needed, modify the port number that you want to use for the web server (NGINX). The default value is 5000.
Client ID	If needed, modify the username to connect to Configuration Hub. The default value is admin.
Client Secret	Enter the password to connect to Configuration Hub.

c. Select **Test Connection**.

The results of the connection test appear. You cannot proceed until the connection is successful.

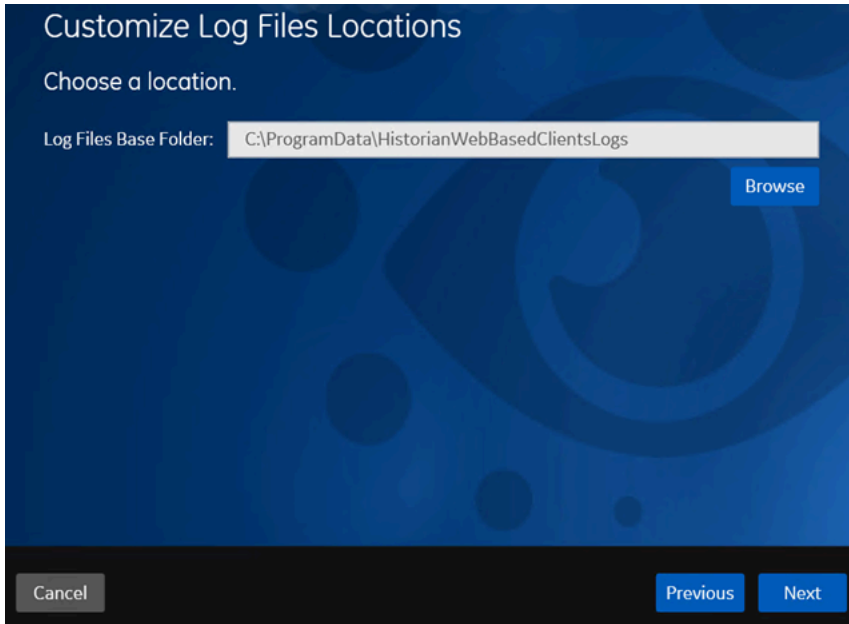
14. Select **Next**.

The default installation drive appears.



15. If needed, change the installation drive for Web-based Clients, and then select **Next**.

The log files location page appears.



Customize Log Files Locations

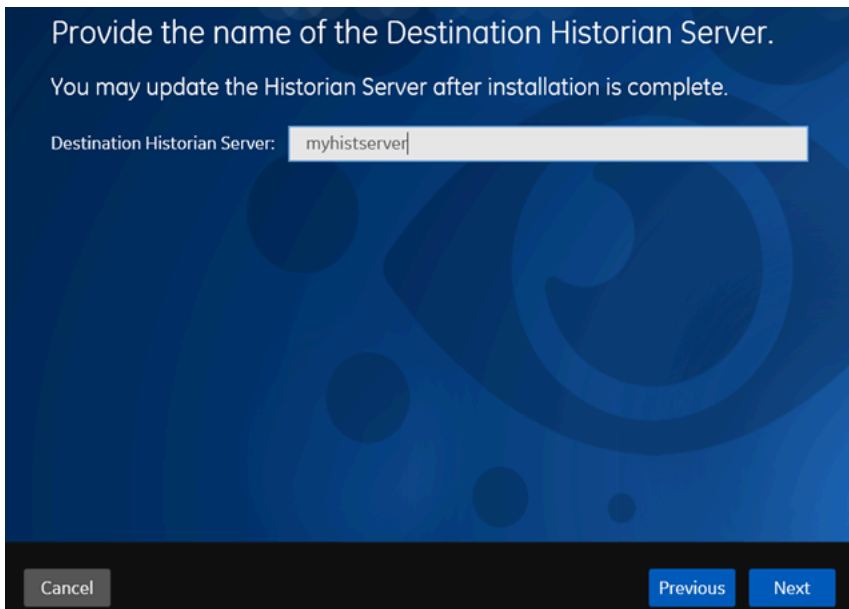
Choose a location.

Log Files Base Folder:

[Browse](#)

[Cancel](#) [Previous](#) [Next](#)

16. If needed, change the location for log files, and then select **Next**.
The destination Historian server page appears.



Provide the name of the Destination Historian Server.

You may update the Historian Server after installation is complete.

Destination Historian Server:

[Cancel](#) [Previous](#) [Next](#)

17. Provide the name of the destination Historian server to which Web-based Clients are connected by default. When you login to Configuration Hub, the default system will point to this server.

**Note:**

- Provide the name of either Historian single-server or mirror primary server because the systems in Configuration Hub will be either a stand-alone system or a horizontally scalable system.
- If you want to connect to a remote Historian server, you must disable the **Enforce Strict Client Authentication** and **Enforce Strict Collector Authentication** options using Historian Administrator in the remote server.

18. Select **Next**.

A message appears, stating that you are ready to install Web-based Clients.

19. Select **Install**.

The Web-based Clients installation begins.

20. When you are prompted to reboot your machine, select **Yes**.

Historian Web-based Clients are installed in the following folder: *<installation drive>*:\Program Files\GE, and the following registry paths are created:

- HKEY_LOCAL_MACHINE\SOFTWARE\GE Digital
- HKEY_LOCAL_MACHINE\SOFTWARE\GE

If you want to use Configuration Hub installed using other products such as iFIX, Plant Applications, and so on, [set up authentication](#) to point to the Proficy Authentication instance.

Install Collectors Using the Installer

After you install collectors, the following artefacts will be available:

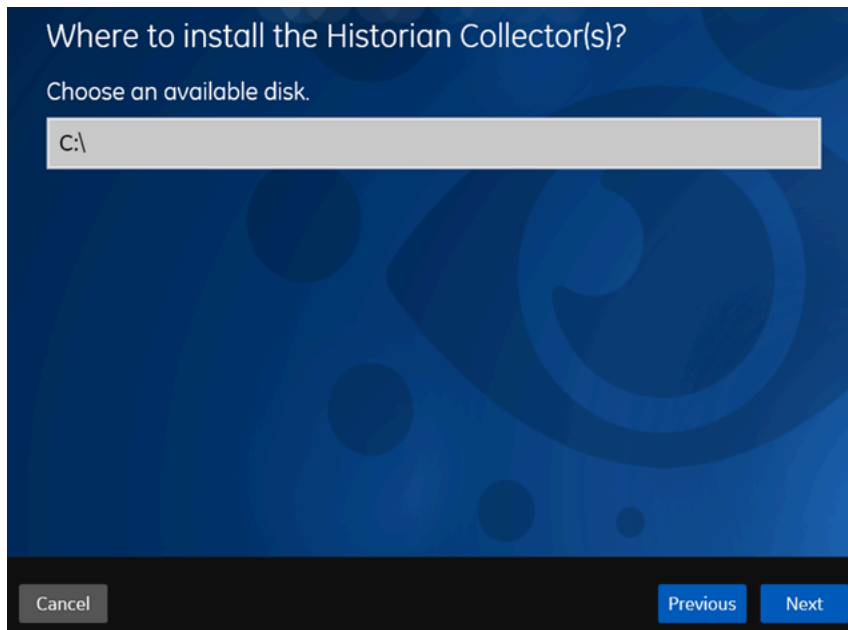
- **Executable files:** These files are required to add a collector instance.
- **Instances of the following collectors:**
 - The iFIX collector
 - The iFIX Alarms & Events collector
 - The OPC Classic Data Access collector for CIMPLICITY
 - The OPC Classic Alarms and Events collector for CIMPLICITY

These instances will be created only if iFIX and/or CIMPLICITY are installed on the same machine as the collectors.

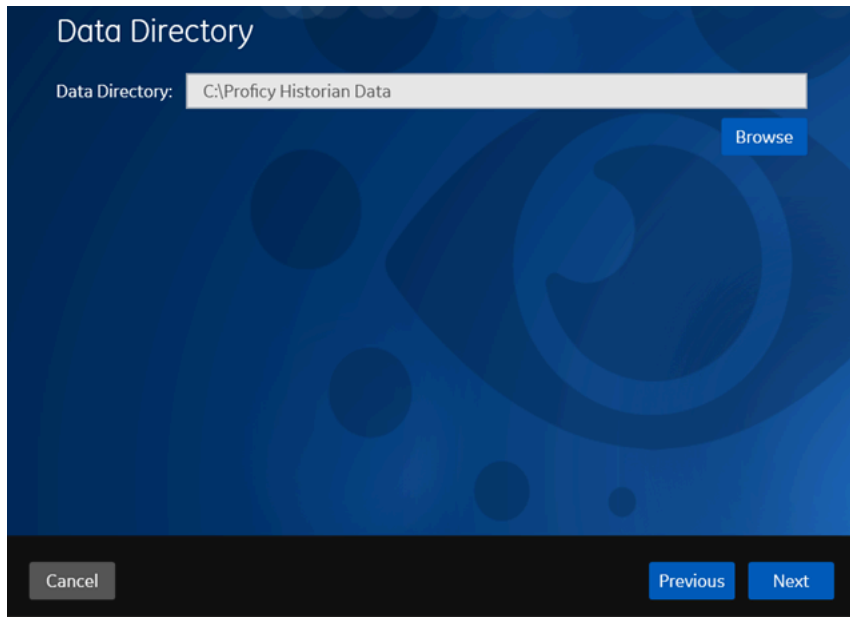
- **The Remote Collector Management agent:** Provides the ability to [manage collectors remotely](#)manage collectors remotely.

You can also [install them at a command prompt](#).

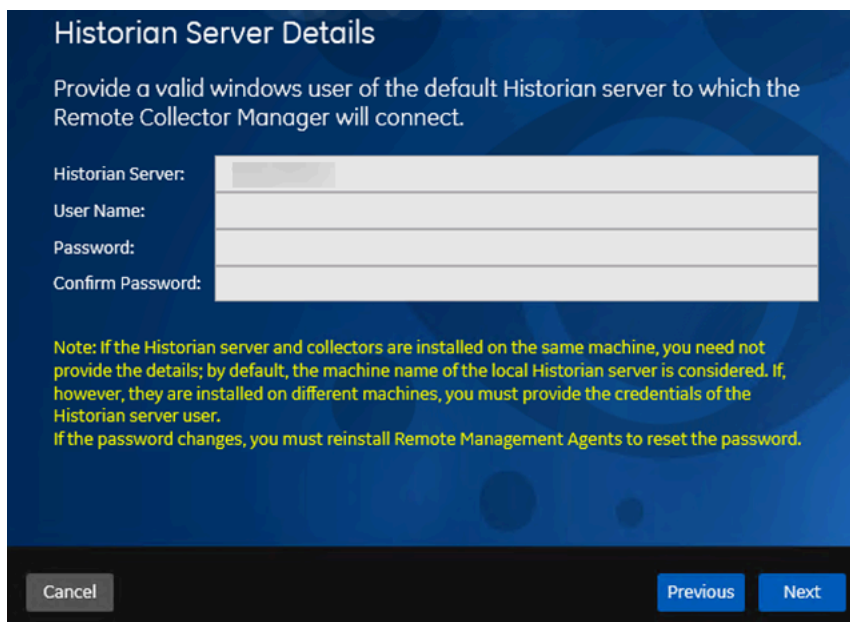
1. Run the `InstallLauncher.exe` file.
2. Select **Install Collectors**.
The welcome page appears.
3. Select **Next**.
The license agreement appears.
4. Select the **Accept** check box, and then select **Next**.
The default installation drive appears.



5. If needed, modify the installation drive, and then select **Next**.
The data directory page appears.



6. If needed, change the folder for storing the collector log files, and then select **Next**.
The destination Historian server page appears.



7. Provide the credentials of the Windows user account of the destination Historian server to which you want Remote Management Agent to connect.

These details are required for Remote Collector Manager to connect to Historian to manage the collectors remotely. If are installing collectors on same machine as the Historian server, and if strict collector authentication is disabled, you need not provide these details; by default, the machine name of the local Historian server is considered. If, however, they are installed on different

machines, or if strict collector authentication is enabled, you must provide the credentials of the Historian server user.

8. Select **Next**.

A message appears, stating that you are ready to install collectors.

9. Select **Install**.

The installation begins.

10. When you are prompted to reboot your system, select **Yes**.

The collector executable files are installed in the following folder: *<installation drive>*: \Program Files (x86)\GE Digital*<collector name>*. The iFIX collectors are installed in the following folder: C:\Program Files\GE\iFIX. The following registry paths are created:

- HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ GE Digital\iHistorian\Services*<collector type>*
- HKEY_LOCAL_MACHINE\SOFTWARE\GE Digital\iHistorian\Services*<collector type>*

In addition, if iFIX and/or CIMPLICITY are installed on the same machine as the collectors, instances of the following collectors are created:

- The iFIX collector
- The iFIX Alarms & Events collector
- The OPC Classic Data Access collector for CIMPLICITY
- The OPC Classic Alarms and Events collector for CIMPLICITY

Perform Post-Installation Tasks

1. If you do not want strict authentication, disable the **Enforce Strict Client Authentication** and **Enforce Strict Collector Authentication** options under Historian Administrator > **Data Stores > Security**.
2. While installing the Historian server, if you have allowed the installer to create Historian security groups, create a local Windows user with the format *<Web-based Clients server name>.admin*, and [add the user to the ihSecurityAdmins group](#). This user will log in to Web-based Clients. Alternatively, you can create Proficy Authentication users in an external Proficy Authentication and map their security groups. For information, refer to [About Proficy Authentication Groups](#).

Depending on whether the Historian server will use local or domain security groups, select the appropriate option in Historian Administrator.

3. Ensure that the Windows user that you have specified while installing collectors is added to the iH Security Admins and iH Collector Admins groups.
4. [Enable trust for a client certificate for Configuration Hub.](#)
5. [Enable trust for a self-signed certificate on Chrome](#)Enable trust for a self-signed certificate on Chrome.
6. [Import an issuer certificate.](#)

You are now ready to use Configuration Hub.

[Access Configuration Hub \(on page 902\).](#)


Upgrade Configuration Hub

If you install Web-based Clients before uninstalling the previous version, you cannot modify the Configuration Hub credentials. If an earlier version of Configuration Hub is available on the same machine, you will be allowed to use the same; you cannot install Configuration Hub again.

1. Uninstall Configuration Hub.
2. [Set up Configuration Hub \(on page 879\).](#)

Access Configuration Hub

Perform the tasks outlined in [About Setting up Configuration Hub with Historian \(on page 879\).](#)

1. Double-click the Configuration Hub icon on your desktop ().
The Configuration Hub login page appears.
2. Depending on whether you want to use Proficy Authentication or custom authentication, select the appropriate tab. If custom authentication is not applicable, skip this step.



Note:

For instructions on setting up authentication, refer to https://www.ge.com/digital/documentation/confighub/version2023/t_authentication_setup.html

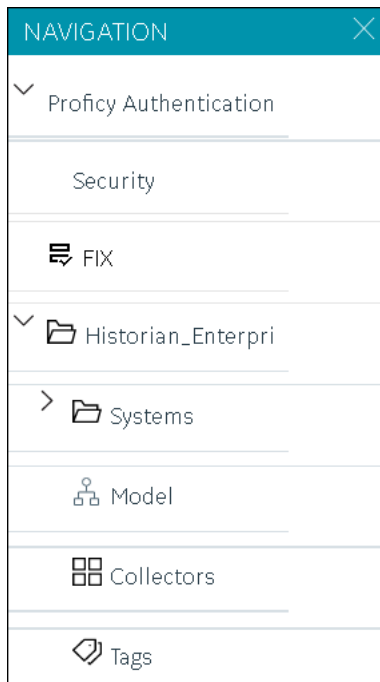
3. Select the Configuration Hub node that you want to access, and then select **Continue to Login**.
The Proficy Authentication login page appears.
If you cannot access the login page, start the GE Operations Hub Httpd Reverse Proxy and the Data Archiver services.
4. Log in with your credentials.

**Note:**

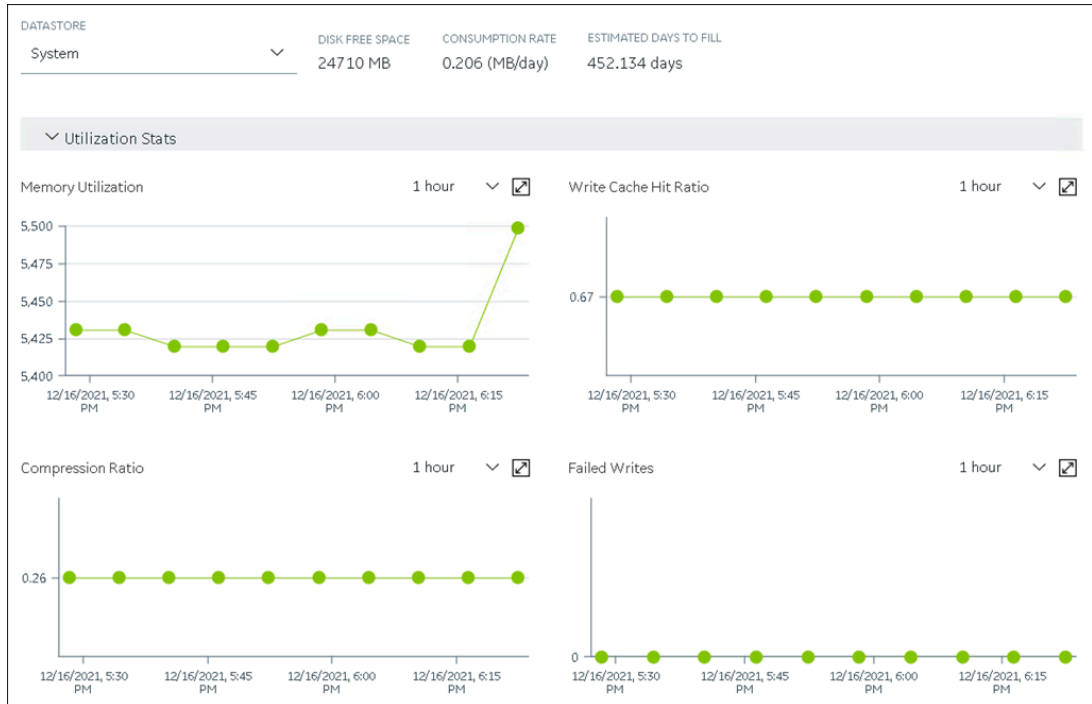
By default, the username is *<host name>.admin*, and the password is the value that you have entered in the **Admin client secret** field on the **Proficy Authentication Service** page during Web-based Clients installation.

The Configuration Hub application appears, displaying the following sections:

- **The Navigation section:** Contains a list of systems that you have added. In addition, it helps you navigate to the Model, Collectors, and Tags sections. You can also [access Proficy Authentication to create users and groups](#).









- **The main section:** Displays content based on your selection in the **NAVIGATION** section. For example, if you select a Historian system, you can access a list of servers in the system. You can also navigate to the system statistics as shown in the following image.




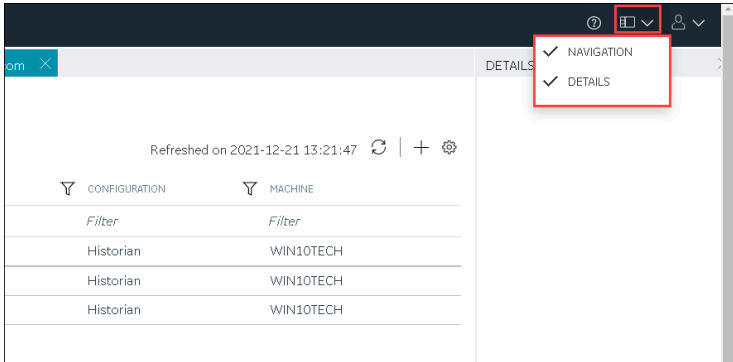


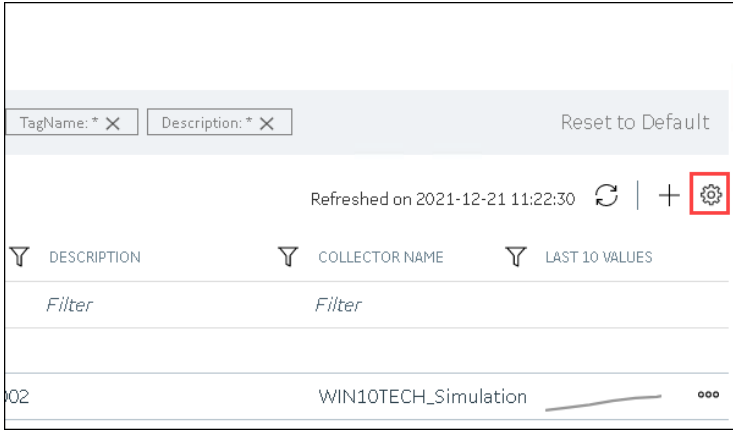
Similarly, if you select **Model** in the **NAVIGATION** section, you can access the Historian model.



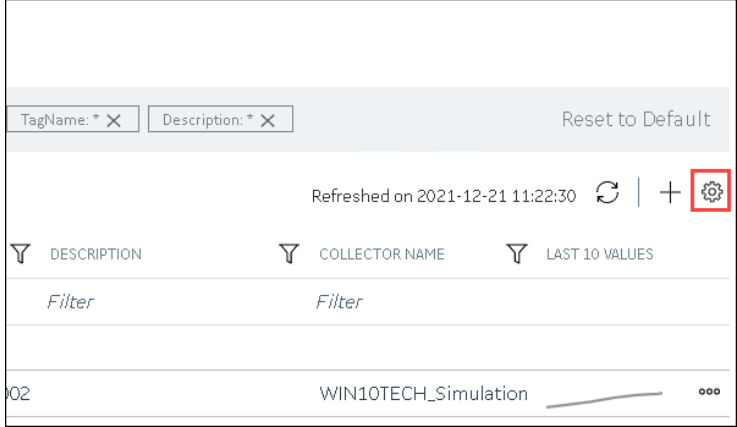

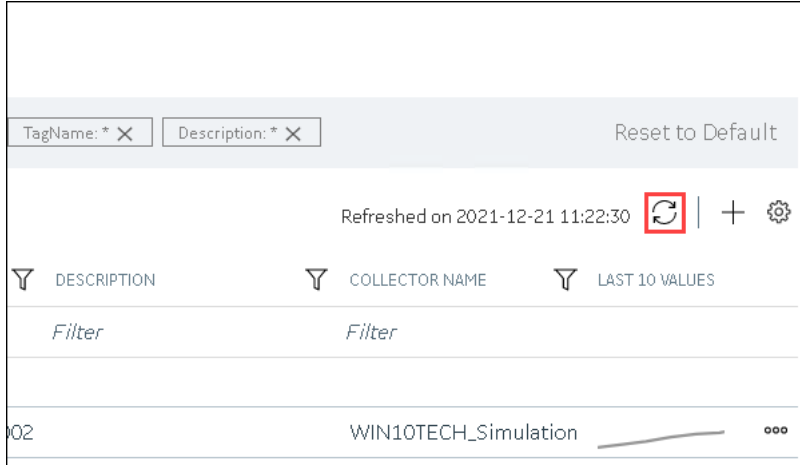
- **The Details section:** Contains the details of the item selected in the main section. For example, If you select a system, you can view the description of the system, and add data stores and mirror locations using the **Details** section.

DETAILS	
<input type="text" value="Search"/>	
General Properties	
Name	ctorcollector...
System Type	Horizontally S...
Primary Server	oriz-collectors...
Description	oriz-collectors...
Default System	Yes
Collectors	10 
Tags	1 
Data Stores	3 
Clients	3 
System Defaults	
Default Locati...	oriz-collec... 
Default Data S...	User 
Alarms and Events	
Alarm Rate	0 (Alarms/min)
License	
Historian Tags	1 (214748364...
Scada Tags	0 (2500 Licens...
Users	1 (1000 Licens...
Data Stores	3 (200 License...
Calculations	Enabled

Depending on your requirements, set up [a stand-alone system \(on page 907\)](#) a stand-alone system or [a horizontally scalable system \(on page 911\)](#) a horizontally scalable system.

Common Tasks in Configuration Hub

Task	Procedure
<p>Show or hide the Navigation or the Details section.</p>	<ol style="list-style-type: none"> In the upper-right corner of the page, select . Select the check boxes for the sections that you want to show. 
<p>Show or hide columns in a table.</p> <div data-bbox="203 1171 594 1440" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note: You cannot hide some of the columns (for example, the COLLECTOR NAME column).</p> </div>	<ol style="list-style-type: none"> In the upper-right corner of the table, select .  <p>The Table Settings window appears.</p> <ol style="list-style-type: none"> Select the check boxes in the SHOW COLUMN column, and then select Apply.

Task	Procedure
<p>Reorder columns in a table.</p> <div data-bbox="203 342 594 520" style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note: You cannot reorder some of the columns.</p> </div>	<p>1. In the upper-right corner of the table, select .</p> <div data-bbox="690 342 1421 766" style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  </div> <p>The Table Settings window appears.</p> <p>2. Use the arrow buttons in the RE-ORDER column, and then select Apply.</p>
<p>Refresh a page/table.</p>	<p>In the upper-right corner of the main section or a table, select .</p> <div data-bbox="609 1092 1404 1554" style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  </div>

Setting up a Stand-Alone System

About Setting up a Stand-Alone Historian System

In a stand-alone Historian system, there is only one Historian server. This type of system is suitable for a small-scale Historian setup.

To set up a stand-alone Historian system, you must first [set up Configuration Hub \(on page 879\)](#).

Components of a Historian System: In a Historian system, the following components are used. This list is not comprehensive. For a complete list, refer to [System Components](#).

- **The Historian server:** You must install a single-server Historian, and [apply the license](#).
- **A Historian system:** A Historian system is a network of Historian servers that collect, store, and retrieve data related to tags, alarms, and events.

By default, a system is created when you set up Configuration Hub.

- **A data store:** A data store is a logical collection of tags used to store, organize, and manage tags according to your requirements. The primary use of data stores is segregating tags by data collection intervals. For example, you can put name plate or static tags (where the value rarely changes) in one data store, and put process tags in another data store. This can improve the query performance.

By default, a user data store is created when you set up Configuration Hub. You can add more as needed.

- **A collector instance:** Collectors are the applications that collect data from a data source, and send it to an on-premises Historian server or a cloud destination such as Predix Time Series and Azure IoT hub.

You must [add a collector instance \(on page 909\)](#) to begin collecting data. You can choose the type of the collector depending on your need. You can use any existing instances (created during collector installation or ported during an upgrade).

- **Tags:** Tags are the parameters for which you want to store data (for example, temperature, pressure, torque).

You must [specify the tags \(on page 909\)](#) for which you want to collect data.

- **Data archiver:** This is a service that indexes all the data by tag name and timestamp, and stores the result in an .iha file.

By default, this is installed when you install the Historian server.

- **Clients:** These are applications that retrieve data from the archive files using the Historian API.

By default, these are installed when you set up Configuration Hub.

Add a Collector Instance

Before you begin using a collector, you must add an instance of the collector. You can add multiple instances of the same collector or instances of multiple collectors. To add multiple instances of a collector, perform the steps once again.

You can add and configure the following types of collector instances:

- [The Calculation collector \(on page 1024\)](#)
- [The CygNet collector \(on page 1027\)](#)
- [The File collector \(on page 1031\)](#)
- [The HAB collector \(on page 1035\)](#)
- [The iFIX collector \(on page 1051\)](#)
- [The MQTT collector \(on page 1056\)](#)
- [The ODBC collector \(on page 1062\)](#)
- [The OPC Classic Alarms and Events collector \(on page 1067\)](#)
- [The OPC Classic DA collector \(on page 1070\)](#)
- [The OPC Classic HDA collector \(on page 1076\)](#)
- [The OPC UA DA collector \(on page 1080\)](#)
- [The OSI PI collector \(on page 1084\)](#)
- [The OSI PI distributor \(on page 1088\)](#)
- [The Server-to-Server collector \(on page 1093\)](#)
- [The Server-to-Server distributor \(on page 1098\)](#)
- [The Simulation collector \(on page 1102\)](#)
- [The Windows Performance collector \(on page 1106\)](#)
- [The Wonderware collector \(on page 1110\)](#)

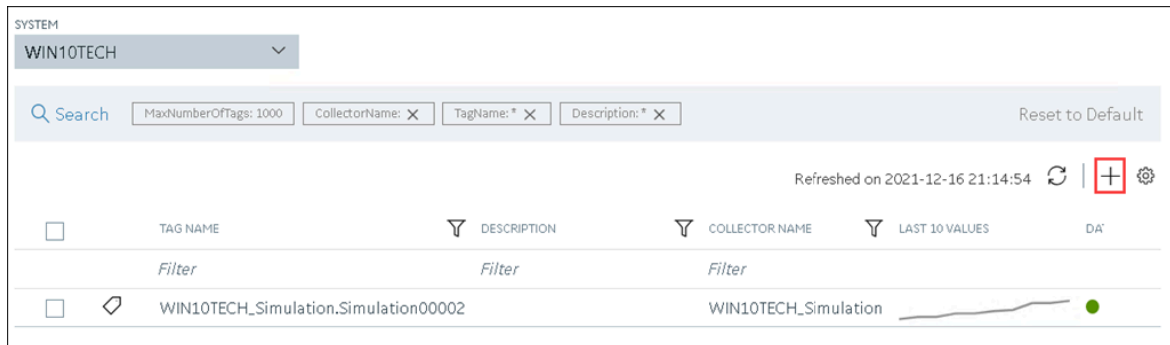
Add Tags for the Data Store Using Configuration Hub

- [Add the collector instance \(on page 909\)](#) using which you want to collect data. Ensure that the collector is running.
- By default, the tag data is stored in the user data store, which is created automatically when you set up Configuration Hub. If, however, you want to store the data in a different data store, [create it \(on page 920\)](#).

This topic describes how to specify the tags for which you want to collect data by browsing through the tags in the data source. For example, for an iFIX collector, if there are 1,00,000 tags in the iFIX server, you must specify the ones for which you want to collect data. Only then data is collected for those tags.

In addition to adding tags from the data source, you can [create tags manually \(on page 1018\)](#).

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Tags**.
3. Select **+**.



The **Add Tag-<system name>** page appears. The **Add Tags from Collector** option is selected by default.

4. Enter values as described in the following table.

Field	Description
COLLECTOR NAME	Select the collector instance that you want to use to collect data. A value is required.
COLLECTED TYPE	Specify whether you want to browse through all the tags in the data source or only from the tags that you have not added yet. A value is required.
SOURCE TAG NAME	Enter the name of the tag (either completely or partially) to narrow down the search results.
SOURCE TAG DESCRIPTION	Enter the description of the tag (either completely or partially) to narrow down the search results.

5. Select **Search Tags**.
A list of tags that match *all* the criteria that you have specified appears. If a tag is already added, it is disabled.
6. Select the check box corresponding to each tag for which you want to collect data.

Add Tags from Collector
 Add Manually

COLLECTOR NAME*
 COLLECTED TYPE*
 SOURCE TAG NAME
 SOURCE TAG DESCRIPTION

SEARCH RESULTS FOR SOURCE TAGS NAMES

<input type="checkbox"/>	TAG NAME	DESCRIPTION
	<i>Filter</i>	<i>Filter</i>
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00001	WIN10TECH_Simulation.Simulation00001
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00002	WIN10TECH_Simulation.Simulation00002
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00003	WIN10TECH_Simulation.Simulation00003
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00004	WIN10TECH_Simulation.Simulation00004
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00005	WIN10TECH_Simulation.Simulation00005
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00006	WIN10TECH_Simulation.Simulation00006
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00007	WIN10TECH_Simulation.Simulation00007
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00008	WIN10TECH_Simulation.Simulation00008
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00009	WIN10TECH_Simulation.Simulation00009
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00010	WIN10TECH_Simulation.Simulation00010
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00011	WIN10TECH_Simulation.Simulation00011
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00012	WIN10TECH_Simulation.Simulation00012

DATASTORE*

7. In the **DATA STORE** field, if you want to store the data in a different data store than the user data store, select the same.
8. Select **Add Tag**.
Data collection begins for the selected tags.

As needed, configure each tag by providing values for the tag properties. For information on the delta query modes, refer to [Counter Delta Queries](#).

Setting up a Horizontally Scalable System

About Setting up a Horizontally Scalable System

In a horizontally scalable Historian system, there are multiple Historian servers, all of which are connected to one another. This type of system is used to scale out the system horizontally. For example, if you have

5,00,000 tags in your Historian system, you can distribute them among the various servers to improve performance.

To set up a horizontally scalable system, you must first [set up Configuration Hub \(on page 879\)](#).

Components of a Historian System: In a Historian system, the following components are used. This list is not comprehensive. For a complete list, refer to [System Components](#).

- **The Historian servers:** You must install the following types of Historian servers:

- **Primary:** A primary server is the only server in a system where the Configuration Manager service runs. For the entire system, Configuration Manager manages the system configuration licensed by the user (that is, the number of tags, options, and so on). Each system can have only one primary server.

You must [apply the Enterprise license](#) to the primary server.

- **Distributed/Mirror:** These servers collect and store data. If added to a mirror group/location, you can [achieve high availability \(on page 917\)](#).

You must [apply the Distributed license](#) to the distributed/mirror servers.

- **A Historian system:** A Historian system is a network of Historian servers that collect, store, and retrieve data related to tags, alarms, and events.

By default, a system is created when you set up Configuration Hub.

- **Data stores:** A data store is a logical collection of tags used to store, organize, and manage tags according to your requirements. The primary use of data stores is segregating tags by data collection intervals. For example, you can put name plate or static tags (where the value rarely changes) in one data store, and put process tags in another data store. This can improve the query performance.

By default, a user data store is created when you set up Configuration Hub. You can add more as needed.

- **Locations:** These are virtual entities in which data stores are created. They are used for storage.

The following types of locations are used in a horizontally scalable system:

- **Distributed location:** This location is created automatically when you install a Historian mirror primary server, or when you install a Historian distributed/mirror node and add it to the primary server. You cannot modify or delete this location, and you cannot create another one.

- **Mirror location:** This location is used to replicate data collected in a data store. For more information, refer to [About Data Mirroring \(on page 917\)](#).

- **A collector instance:** Collectors are the applications that collect data from a data source, and send it to an on-premises Historian server or a cloud destination such as Predix Time Series and Azure IoT hub.

You must [add a collector instance \(on page 909\)](#) to begin collecting data. You can choose the type of the collector depending on your need. You can use any existing instances (created during collector installation or ported during an upgrade).

- **Tags:** Tags are the parameters for which you want to store data (for example, temperature, pressure, torque).

You must [specify the tags \(on page 909\)](#) for which you want to collect data.

- **Data archiver:** This is a service that indexes all the data by tag name and timestamp, and stores the result in an .iha file.

By default, this is installed when you install the Historian server.


- **Clients:** These are applications that retrieve data from the archive files using the Historian API.

By default, these are installed when you set up Configuration Hub.

Add a Distributed/Mirror Server

1. [Install Historian server \(on page 880\)](#) on the machine that you want to add as a distributed server.
2. [Add a system \(on page 978\)](#). The server that you specify while adding the system serves as the primary server for the system.

If you want to create a horizontally scalable Historian system, you must first add a primary server, and then add one or more distributed/mirror machines to scale out the primary server horizontally and thus, improve performance.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Systems**.
A list of systems appears in the main section.
3. Expand the system in which you want to add a distributed/mirror server.
A list of servers in the system appears.
4. Select .

System	Historian Server																														
Filter	Filter																														
<div style="border: 1px solid #0070c0; padding: 5px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> SERVERS + </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Machine Name</th> <th>STATUS</th> <th>Archive Compre...</th> <th>Write Cache Hit ...</th> <th>CONSUMPTION R...</th> <th>Read Thread Usa...</th> <th>Write Thread Us...</th> <th>Out Of</th> </tr> </thead> <tbody> <tr> <td>██████████</td> <td style="color: green;">✔ Connected</td> <td>43.3</td> <td>0.5</td> <td>0.45</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>██████████</td> <td style="color: red;">✘ Not Connected</td> <td>NA</td> <td>NA</td> <td>NA</td> <td>NA</td> <td>NA</td> <td>NA</td> </tr> </tbody> </table> </div>								Machine Name	STATUS	Archive Compre...	Write Cache Hit ...	CONSUMPTION R...	Read Thread Usa...	Write Thread Us...	Out Of	██████████	✔ Connected	43.3	0.5	0.45	0	0	0	██████████	✘ Not Connected	NA	NA	NA	NA	NA	NA
Machine Name	STATUS	Archive Compre...	Write Cache Hit ...	CONSUMPTION R...	Read Thread Usa...	Write Thread Us...	Out Of																								
██████████	✔ Connected	43.3	0.5	0.45	0	0	0																								
██████████	✘ Not Connected	NA	NA	NA	NA	NA	NA																								

The **Add Server Machine: <system name>** window appears.

- Enter the host name or IP address of the machine that you want to add, and then select **Add**. The distributed server is added to the system. A distributed location is added in the server. You cannot modify or delete this location.

If you want high availability of one or more data stores in the server, [create a mirror location \(on page 918\)](#), and then [add the data stores \(on page 920\)](#). If not, [add the data store \(on page 920\)](#) to the distributed location.

Add a Collector Instance

Before you begin using a collector, you must add an instance of the collector. You can add multiple instances of the same collector or instances of multiple collectors. To add multiple instances of a collector, perform the steps once again.

You can add and configure the following types of collector instances:

- [The Calculation collector \(on page 1024\)](#)
- [The CygNet collector \(on page 1027\)](#)
- [The File collector \(on page 1031\)](#)
- [The HAB collector \(on page 1035\)](#)
- [The iFIX collector \(on page 1051\)](#)
- [The MQTT collector \(on page 1056\)](#)
- [The ODBC collector \(on page 1062\)](#)
- [The OPC Classic Alarms and Events collector \(on page 1067\)](#)
- [The OPC Classic DA collector \(on page 1070\)](#)
- [The OPC Classic HDA collector \(on page 1076\)](#)
- [The OPC UA DA collector \(on page 1080\)](#)
- [The OSI PI collector \(on page 1084\)](#)

- The OSI PI distributor ([on page 1088](#))
- The Server-to-Server collector ([on page 1093](#))
- The Server-to-Server distributor ([on page 1098](#))
- The Simulation collector ([on page 1102](#))
- The Windows Performance collector ([on page 1106](#))
- The Wonderware collector ([on page 1110](#))

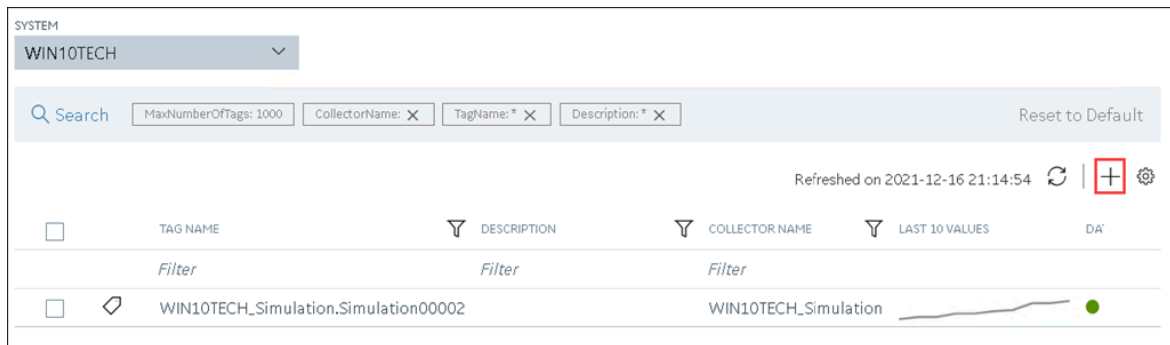
Add Tags for the Data Store Using Configuration Hub

- [Add the collector instance \(on page 909\)](#) using which you want to collect data. Ensure that the collector is running.
- By default, the tag data is stored in the user data store, which is created automatically when you set up Configuration Hub. If, however, you want to store the data in a different data store, [create it \(on page 920\)](#).

This topic describes how to specify the tags for which you want to collect data by browsing through the tags in the data source. For example, for an iFIX collector, if there are 1,00,000 tags in the iFIX server, you must specify the ones for which you want to collect data. Only then data is collected for those tags.

In addition to adding tags from the data source, you can [create tags manually \(on page 1018\)](#).

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Tags**.
3. Select **+**.



The **Add Tag-<system name>** page appears. The **Add Tags from Collector** option is selected by default.

4. Enter values as described in the following table.

Field	Description
COLLECTOR NAME	Select the collector instance that you want to use to collect data. A value is required.
COLLECTED TYPE	Specify whether you want to browse through all the tags in the data source or only from the tags that you have not added yet. A value is required.
SOURCE TAG NAME	Enter the name of the tag (either completely or partially) to narrow down the search results.
SOURCE TAG DESCRIPTION	Enter the description of the tag (either completely or partially) to narrow down the search results.

5. Select **Search Tags**.

A list of tags that match *all* the criteria that you have specified appears. If a tag is already added, it is disabled.

6. Select the check box corresponding to each tag for which you want to collect data.

Add Tags from Collector
 Add Manually

COLLECTOR NAME* WIN10TECH_Simulation
 COLLECTED TYPE* All Source Tags
 SOURCE TAG NAME *
 SOURCE TAG DESCRIPTION *

SEARCH RESULTS FOR SOURCE TAGS NAMES

<input type="checkbox"/>	TAG NAME	DESCRIPTION
	<i>Filter</i>	<i>Filter</i>
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00001	WIN10TECH_Simulation.Simulation00001
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00002	WIN10TECH_Simulation.Simulation00002
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00003	WIN10TECH_Simulation.Simulation00003
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00004	WIN10TECH_Simulation.Simulation00004
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00005	WIN10TECH_Simulation.Simulation00005
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00006	WIN10TECH_Simulation.Simulation00006
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00007	WIN10TECH_Simulation.Simulation00007
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00008	WIN10TECH_Simulation.Simulation00008
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00009	WIN10TECH_Simulation.Simulation00009
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00010	WIN10TECH_Simulation.Simulation00010
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00011	WIN10TECH_Simulation.Simulation00011
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00012	WIN10TECH_Simulation.Simulation00012

DATASTORE* User

7. In the **DATA STORE** field, if you want to store the data in a different data store than the user data store, select the same.
8. Select **Add Tag**.
Data collection begins for the selected tags.

As needed, configure each tag by providing values for the tag properties. For information on the delta query modes, refer to [Counter Delta Queries](#).

Setting up High Availability

About Data Mirroring

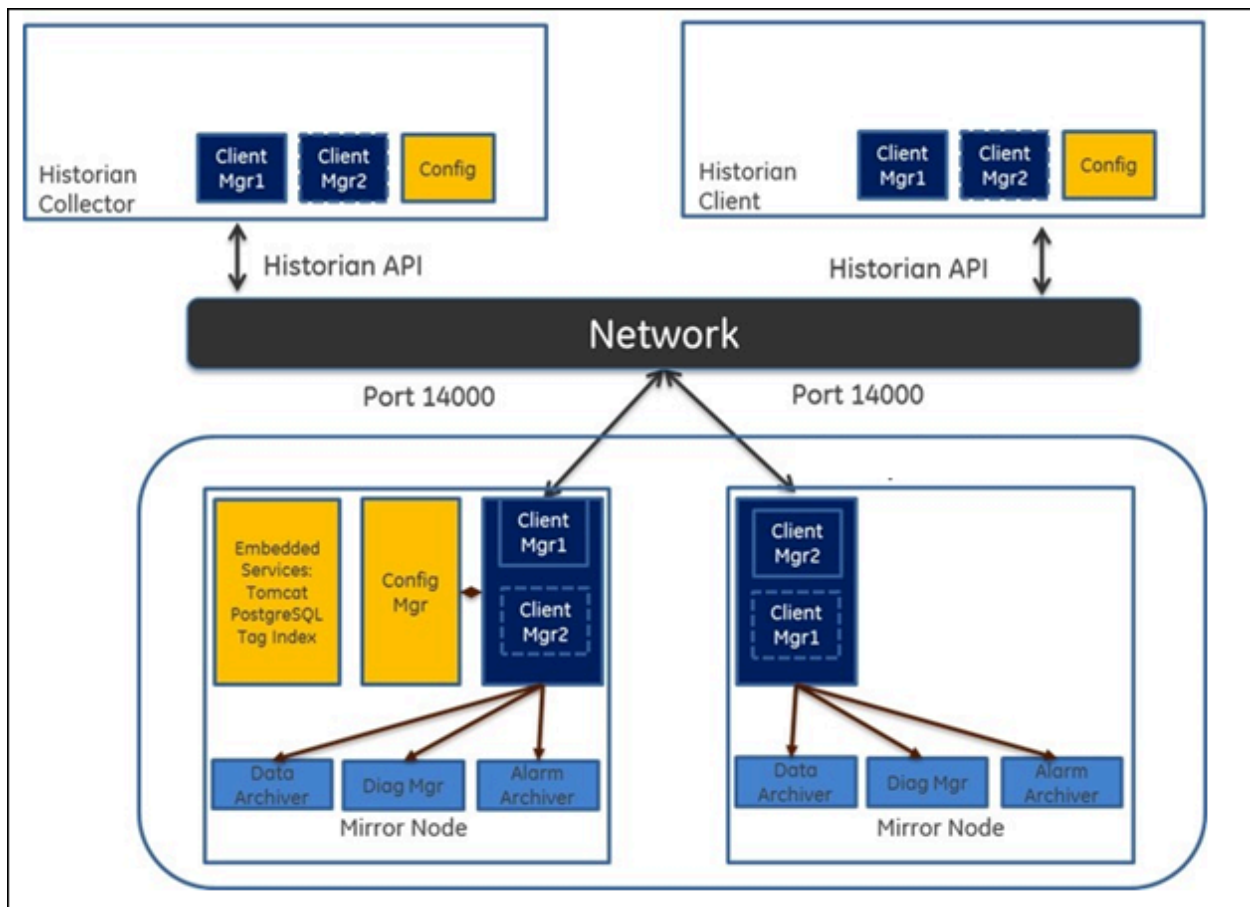
Historian provides mirroring of stored data on multiple nodes to provide high levels of data reliability. Data Mirroring also involves the simultaneous action of every insert, update and delete operations that occurs on any node. Data mirroring provides continuous data read and write functionality.

In a typical data mirroring scenario, one server acts as a primary server to which the clients connect. All communication goes through the Client Manager, and each Client Manager knows about the others. Mirrors must be set up in a single domain.

When you create a mirror location, you add one or more servers to the group, and then create the data stores whose data you want to replicate. For example, suppose you want to create a data store for collecting the data for 100 tags, for which you want high availability. In that case, you must create a mirror location, add two or more servers to the mirror location, and then create the data store. When you do so, the data retrieved in the data store is stored in all the servers in the mirror location. If one of the servers is down, you can retrieve the data from the other servers in the group.

Mirror Node Setup

The following diagram helps you to understand a typical single mirror node setup.



Create a Mirror Location

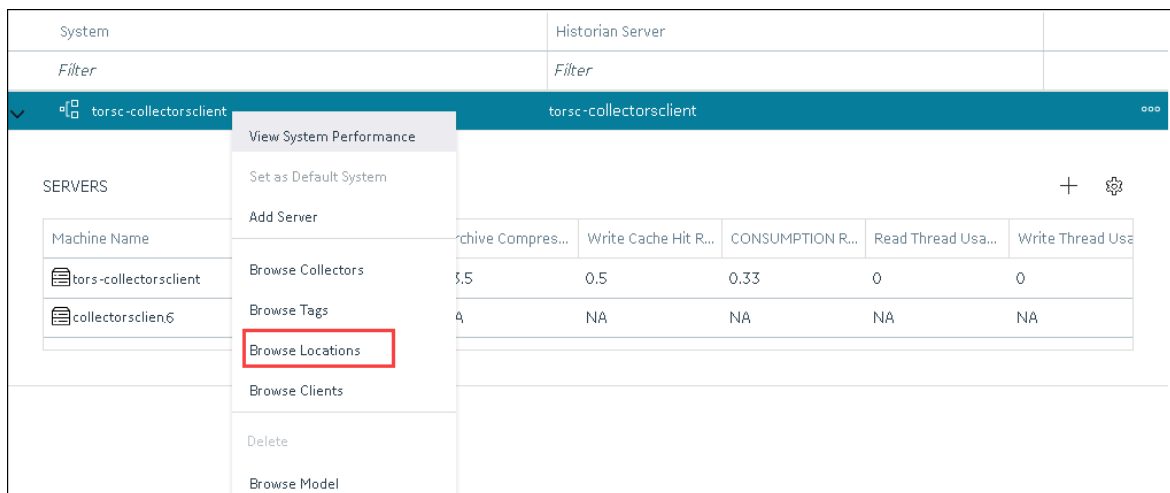
Add one or more distributed servers ([on page 913](#)) to the system in which you want to create a mirror group.

If you want high availability of one or more data stores, you must create a mirror group (also called a mirror location), and then add servers to it. When you do so, the data in the data stores of the mirror locations is replicated. Therefore, even if one of the servers is down, you can retrieve data from the other servers in the mirror location, thus achieving high availability.

The following conditions apply when you create a mirror location:

- You must add minimum two servers to a mirror location. The maximum number of servers that you can add depends on your Historian license.
- You can add a mirror location only in a horizontally scalable Historian system.
- You can rename a mirror location, remove a machine from a mirror location, or add an additional one even after you create the mirror location. However, if only one machine remains in the group, you cannot remove it.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Systems**. The **Systems** section appears, displaying a list of systems.
3. Right-click the system in which you want to create a mirror location (or select **☰**), and then select **Browse Locations**.



A list of distributed locations in the system appears.

4. Select **Mirror Locations**.

A list of mirror locations in the system appears.

5. In the upper-right corner of the main section, select **+**.

The **Add Mirror Location** window appears.

6. Provide values as described in the following table.

Field	Description
MIRROR LOCATION NAME	Enter a name for the mirror location. A value is required and must be unique for the system.
SERVER MACHINES	Select the servers that you want to add to the mirror group. This box contains a list of all the servers in the system. You must add minimum two servers to a mirror location.

7. Select **Add**.

The mirror location is created.

[Add a data store to the mirror location \(on page 920\).](#)

Create a Data Store

The number of data stores that you can create depends on your license.

1. [Access Configuration Hub \(on page 902\).](#)
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Datstores**.
Alternatively, you can select **Systems**, right-click the system in which you want to create a data store (or select **☰**), and then select **Browse Data Stores**.
The **Data Stores** section appears.
3. Select **+**.
If Historian Standard version, then the **Add Data Store** window appears.

If Historian Enterprise version, then the **Add Data Store: <location name>** window appears.
4. Enter values as described in the following table.

Field	Description
DATA STORE NAME	Enter a unique name for the data store. A value is required. You can use all alphanumeric characters and special characters except / \ * ? < >
DESCRIPTION	Enter a description for the data store.

Field	Description
LOCATION	Enter the host name or IP address of the distributed location on which you want to create the data store. This field is available only for a horizontally scalable system.
Is Default	Switch the toggle on if you want to set this data store as the default one. A default data store is the one that is considered if you do not specify a data store while adding a tag. You can set only one data store as default.

5. Select .

The data store is created.

When you add tags to the data store, it will have its own set of .IHA (iHistorian Archive) files.

Ensure that you back up the new data store archives periodically.

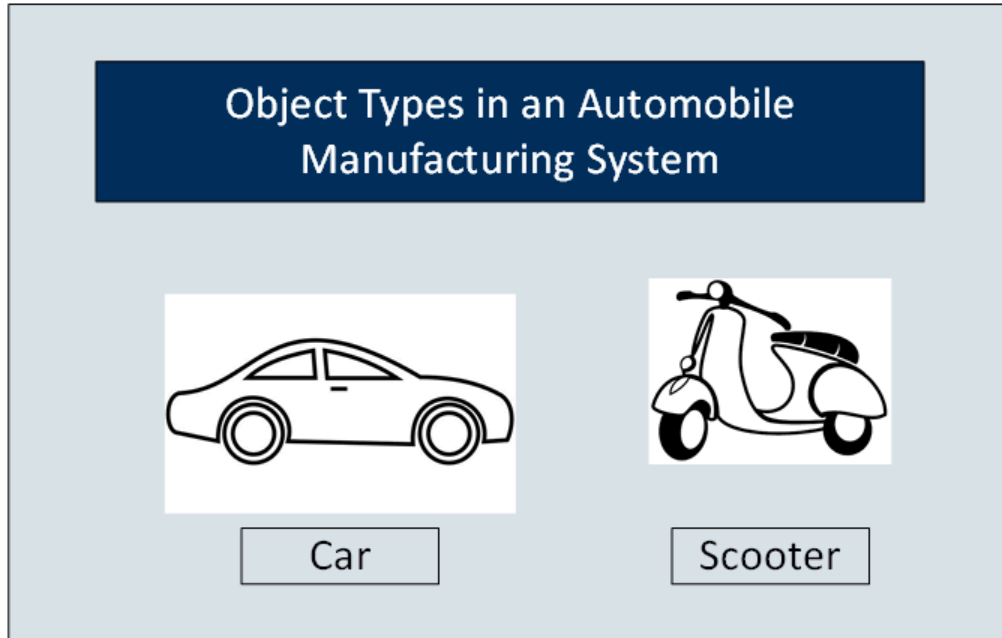
Creating a Model

About a Historian Model

A Historian model is a hierarchical classification of various objects in a system. A model contains the following components:

- Object Types
- Contained Types
- Object Instances
- Variables

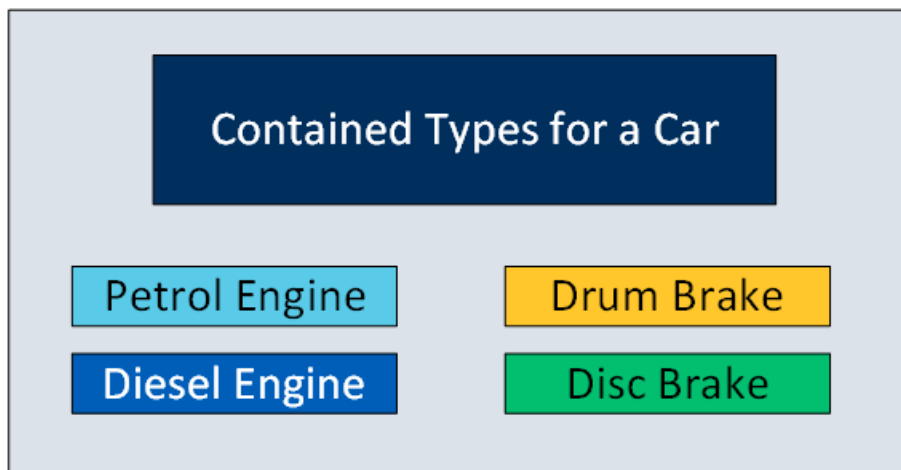
Object Type: An object type is a blueprint, which you want to replicate that will have a common structure (common properties/attributes and contained types). These object types can be the products you manufacture, your assets, byproducts, or anything else for which you want to classify information hierarchically and inherit properties/attributes. For example, in an automobile manufacturing unit, the vehicles you manufacture are object types (for example, a car or a scooter).



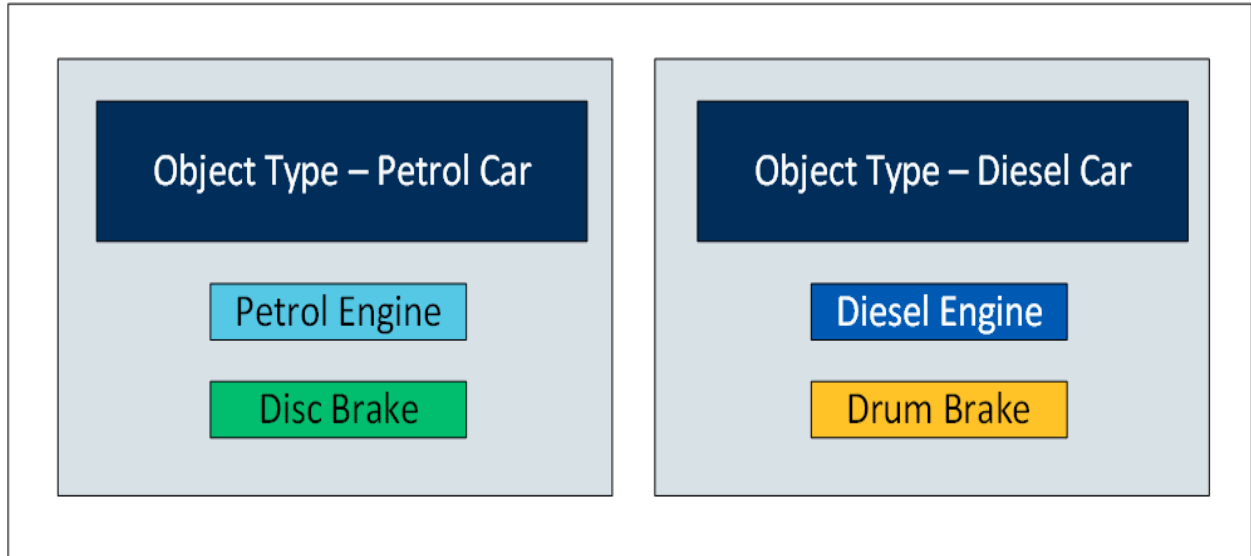
Contained Types: A contained type is an object type that you can include in another object type. For example, suppose you manufacture cars with the following types of engines:

- Petrol
- Diesel

You can then create one contained type for a petrol engine and one for a diesel engine. Similarly, you can create contained types for various types of brake systems, testing parameters, and so on.

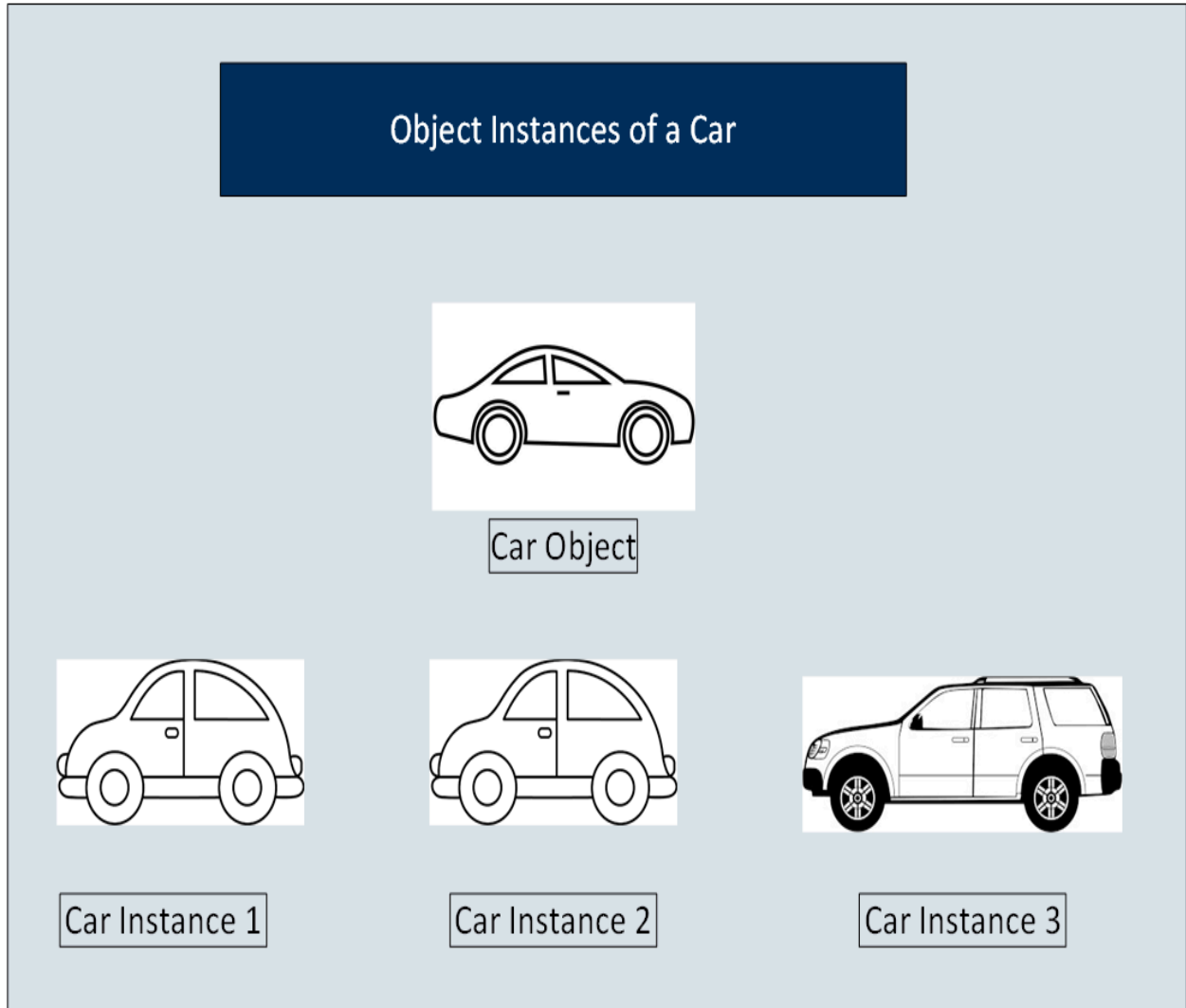


When you create an object type for a car, you can include any of these contained types.



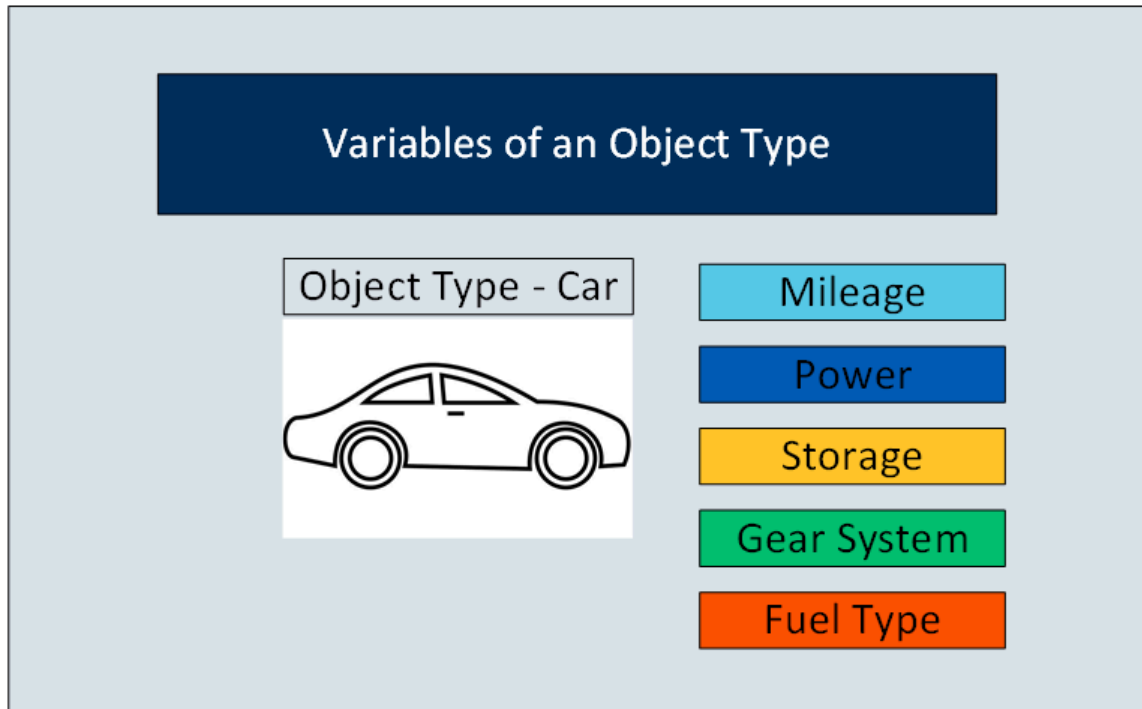
You can include multiple contained types in a single object instance. In addition, you can include a single contained type in multiple object instances.

Object Instances: Each item of an object type that you manufacture is called an object instance. For example, if you manufacture three cars, each one is an instance.



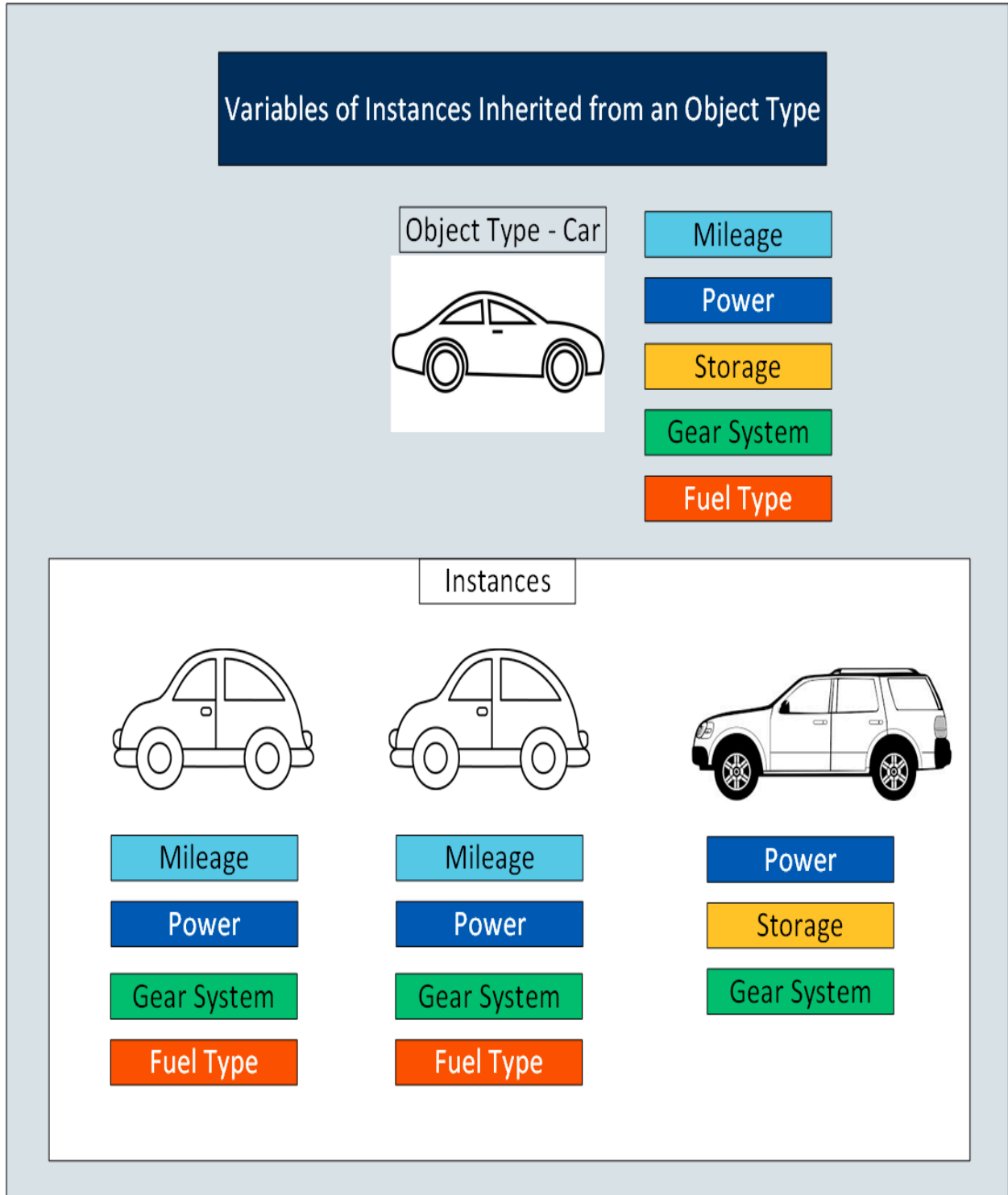
An object instance is specific to a Historian system. An object type, however, is not associated with a system.

Variables: Each attribute or property of an object is called a variable. These variables are common across all objects of a certain type. They represent tags whose values are collected by data collectors. For example, a car can have the following variables.



When you create instances of an object type, by default, the variables in the object type are inherited to all the instance as well. You can choose to include or exclude one or more of these variables for each instance.

In the following image, all the variables of the car object type are inherited to each of the instances. However, the first two instances do not include Storage. And the third instance does not include Mileage and Fuel Type.



If an object type contains contained types, the variables in the contained types are inherited as well.

After you create an object instance, you must store the values of each variable of the instance. To do so, you must map each variable with a Historian tag or create one, depending on the type of the variable.

Types of Variables:

- **Direct:** Tags for these variables are created in Historian when you select a collector instance. For instructions on collecting data for these types of tags, refer to [Collect Data for a Direct Variable \(on page 944\)](#).
- **Indirect:** These variables are mapped with existing Historian tags. For instructions on collecting data for these types of tags, refer to [Collect Data for an Indirect Variable \(on page 947\)](#).
- **Static:** These variables have a static value, which you provide when you create an object instance. For instructions on providing data for these types of tags, refer to [Provide Data for a Static Variable \(on page 941\)](#).

Limitations:

- An OPC UA model is not supported.
- If the name of a tag associated with a variable in a model contains a period (.), you cannot import the tag while importing the model into a Historian system.

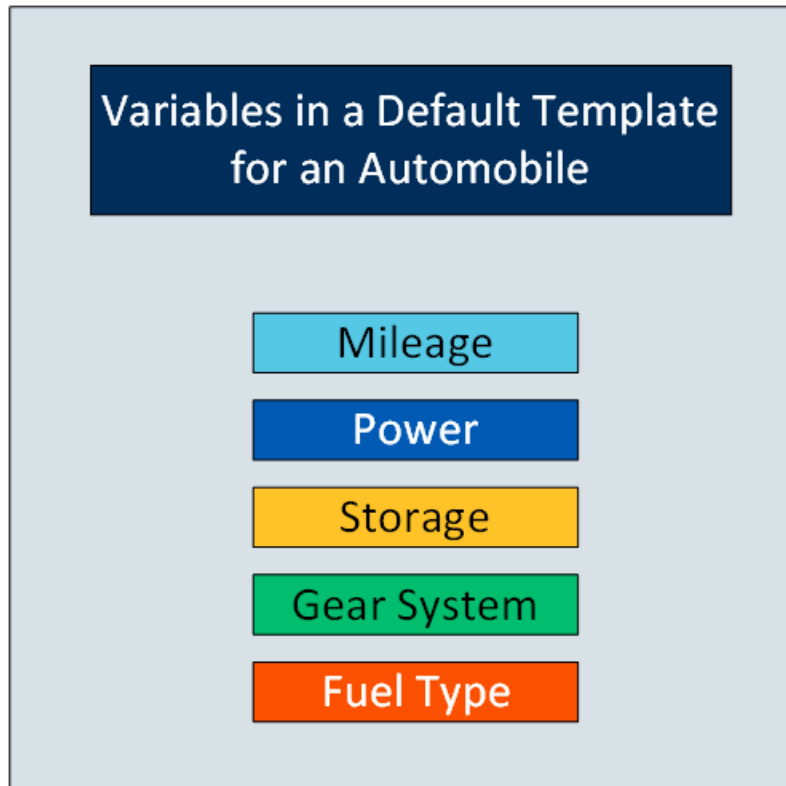
About Object Templates

When you create an object type, you create a template. A template contains attributes/properties of an object type, called variables. When you apply a template to an object instance, the variables included in the template are added to the object instance.

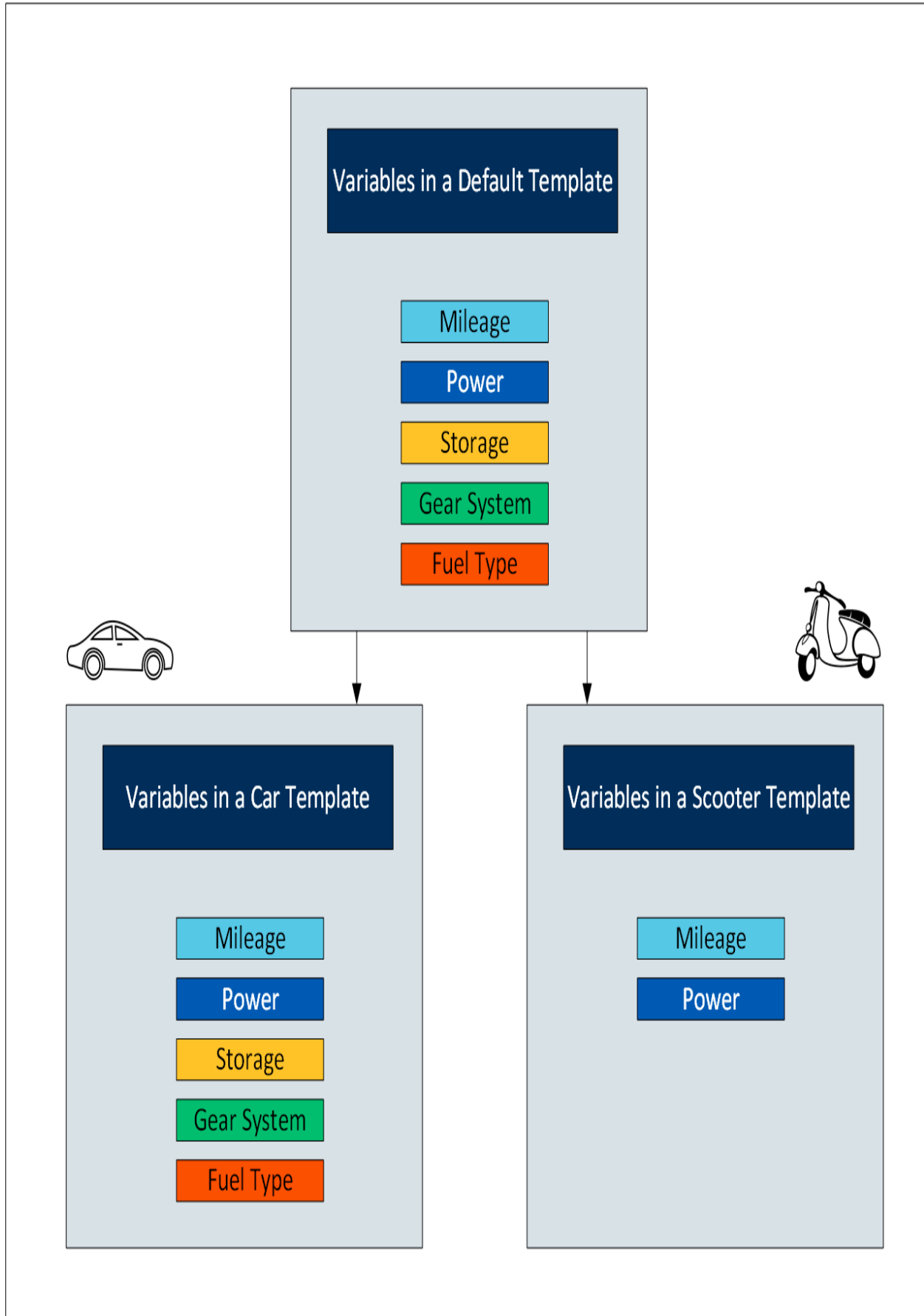
Types of Templates:

- **Default Template:** The default template contains generic/common variables of an object type. Each object type contains one and only one default template; you cannot delete it.
- **Custom Template:** In addition to the default template, if needed, you can create one or more custom templates for an object type. When you do so, you can choose to include variables from the default template or other custom templates in the same object type.

For example, suppose you have an automobile manufacturing unit. You can create a default template that contains generic details about an automobile. Each of these details is a variable.



In addition to the default template, you can create custom templates for the object type, and add variables to it. For example, in the automobile object type, you can create a template for a car and another one for a scooter. Some of the variables in the default template (such as storage and gear system) may not be applicable to a scooter. Therefore, you can exclude them.



When you later create instances of the object type, you can choose any of the three templates. When you do so, all the variables in the template are included in the object instance. You will then capture values of these variables in Historian.

Workflow for Creating a Historian Model

To create a model and store tag values of object instances, you must perform the following steps.

Step Number	Description	Notes
1	Set up Configuration Hub (on page 879).	This step is required. It involves installing the required components to get started with Configuration Hub.
2	Create a collector instance (on page 909).	This step is required. It involves creating a collector instance using which you want to collect data from the object instance and store it in an on-premises Historian server or a cloud destination.
3	Specify the tags for data collection (on page 909).	This step is required. It involves specifying the tags for which you want to collect data by browsing through the tags in the data source. For example, for an iFIX collector, if there are 1,00,000 tags in the iFIX server, you must specify the ones for which you want to collect data. Only then data is collected for those tags. You will later map these tags with the variables in each object instance, thus collecting data for the variables (explained later in this workflow).
4	Create an object type (on page 931).	This step is required. It involves creating an object type, a default template, one or more custom templates as needed, and adding variables to each object type.
5	Create an object instance (on page 939).	This step is required. It involves creating an object instance and applying the required

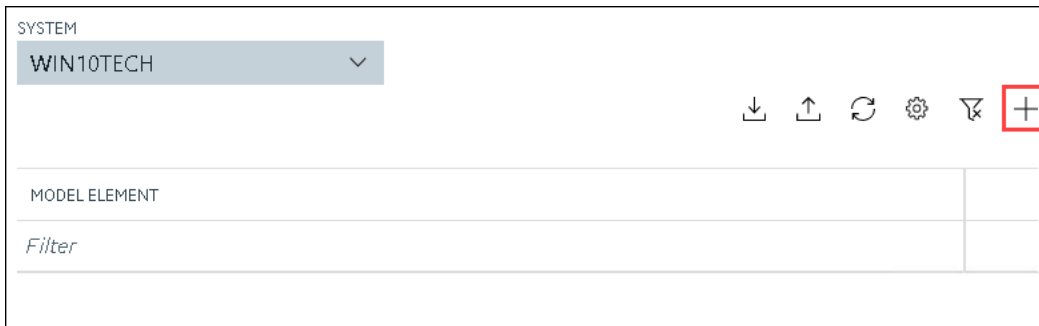
Step Number	Description	Notes
6	Provide/collect data for static (on page 941) , direct (on page 944) , and indirect (on page 947) variables.	<p>template from the object type. The object instance then inherits the variables from the object type.</p> <p>This step is required. You can provide data for the following types of variables:</p> <ul style="list-style-type: none"> • Static: For a static variable, the value does not change; therefore, you just provide the value of the variable. • Direct: For a direct variable, you associate the variable with a collector instance and a tag. When you do so, the tag is created in Historian, and values for the variable are collected by the collector instance and stored in Historian. • Indirect: For an indirect variable, you associate the variable with a collector instance and an <i>existing</i> Historian tag. The values for the variable are then collected by the collector instance and stored in Historian. <p>For more information on the types of variables, refer to About a Historian Model (on page 921).</p>

Create an Object Type

When you create an object type, you also create the default template, custom templates, and variables for each template. For information on each of these template types and variables, refer to [About Object Templates \(on page 927\)](#) and [About a Historian Model \(on page 921\)](#).

This topic describes how to create an object type. You can also [copy one \(on page 954\)](#).

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Model**.
Alternatively, you can select **Systems**, and then in the row containing the system in which you want to create a model, select **☰**, and then select **Browse Model**.
The **Model** section appears.
3. In the upper-right corner of the section, select **+**.

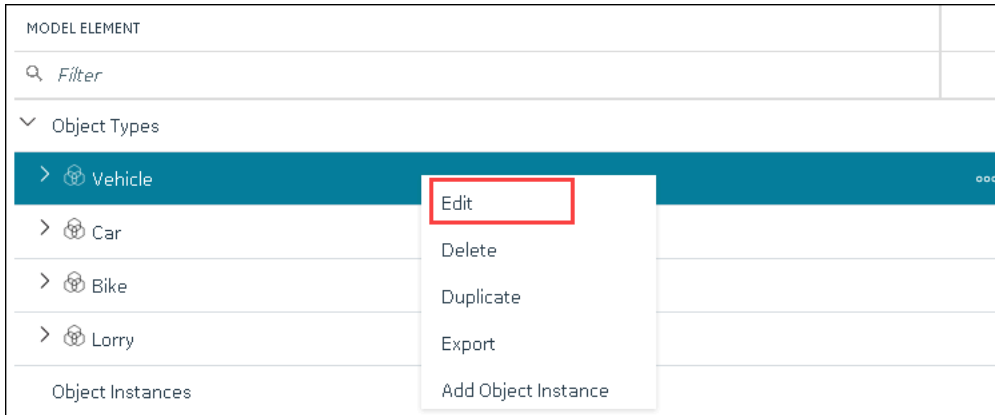


The **New Object Type** window appears.

4. Enter values as described in the following table.

Field	Description
NAME	<p>Enter a name for the object type. A value is required and must be unique.</p> <p>The value that you enter:</p> <ul style="list-style-type: none"> ◦ Must begin with a letter or a number. ◦ Can contain up to 256 characters. ◦ Can include any of the following special characters: /!#{}%\$-_ ◦ Must not include a space or any of the following characters: ~`+^;,:?"*={}@
DESCRIPTION	Enter a description for the object type.

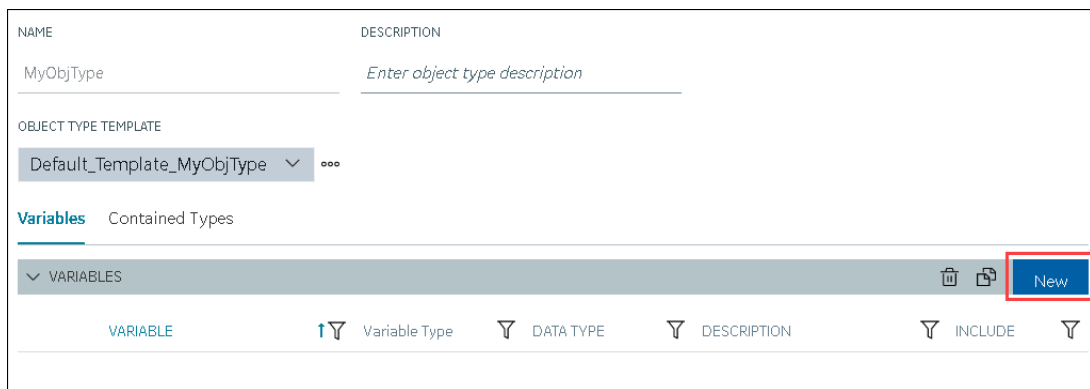
5. Select **Create**.
The object type is created.
6. In the main section, under **Object Types**, right-click the object type that you have created (or select **☰**), and then select **Edit**.



The **<object type name>** section appears. The **OBJECT TYPE TEMPLATE** field contains the default template.

7. To add variables to the default template:

a. In the **Variables** table, select **New**.




A blank row appears in the table.

b. Enter values as described in the following table.



Column	Description
VARIABLES	<p>Enter the name of the variable. A value is required and must be unique for the object type.</p> <p>The value that you enter:</p> <ul style="list-style-type: none"> ▪ Must begin with a letter or a number. ▪ Can contain up to 256 characters.

Column	Description
VARIABLE TYPE	<ul style="list-style-type: none"> ▪ Can include any of the following special characters: /!#{}%\$-_ ▪ Must not include a space or any of the following characters: ~`+^:;,?"*={}@ <p>Choose one of the following types of variables:</p> <ul style="list-style-type: none"> ▪ Direct: Tags for these variables are created in Historian for a selected collector instance. ▪ Indirect: These variables are mapped with existing Historian tags. ▪ Static: These variables have a static value, which you provide when you create an object instance.
DATATYPE	Select the data type of the variable.
DESCRIPTION	Enter a description for the variable.
INCLUDE	Switch the toggle to indicate whether you want to include the variable in the template.

 **Note:**
 After you apply a template to an object instance, you cannot modify or delete a variable in the object type; you can only add more variables. You can, however, [copy the object type \(on page 954\)](#), and modify or delete variables in the copied one.

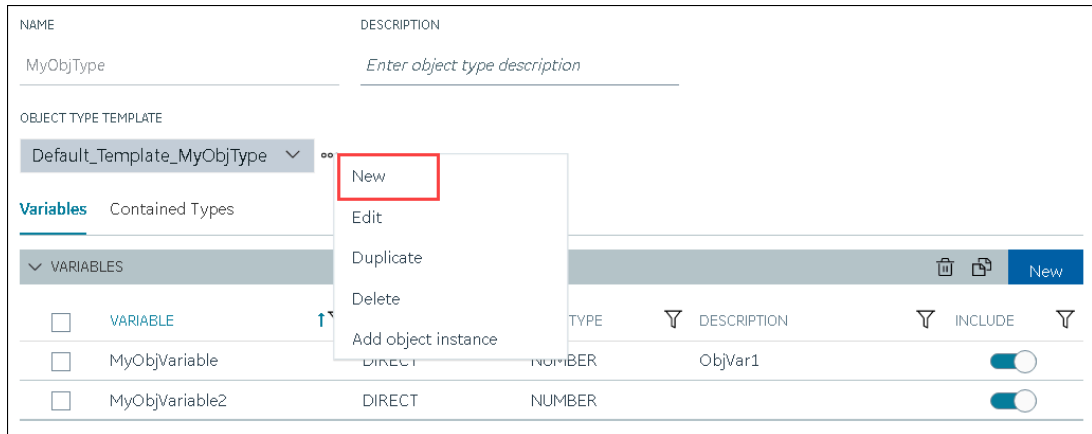
c. Press ENTER.

The default template is created, along with the variable that you have added. You can add more variables or include/exclude variables later too.

 **Note:**
 If you want to create a variable by copying an existing one, select the check box next to the variable that you want to copy, and then select . You can copy only one variable at a time.

8. To create a custom template:

a. Next to the **TEMPLATE** field, select **☰**, and then select **New**.



The **New Object Template** window appears.

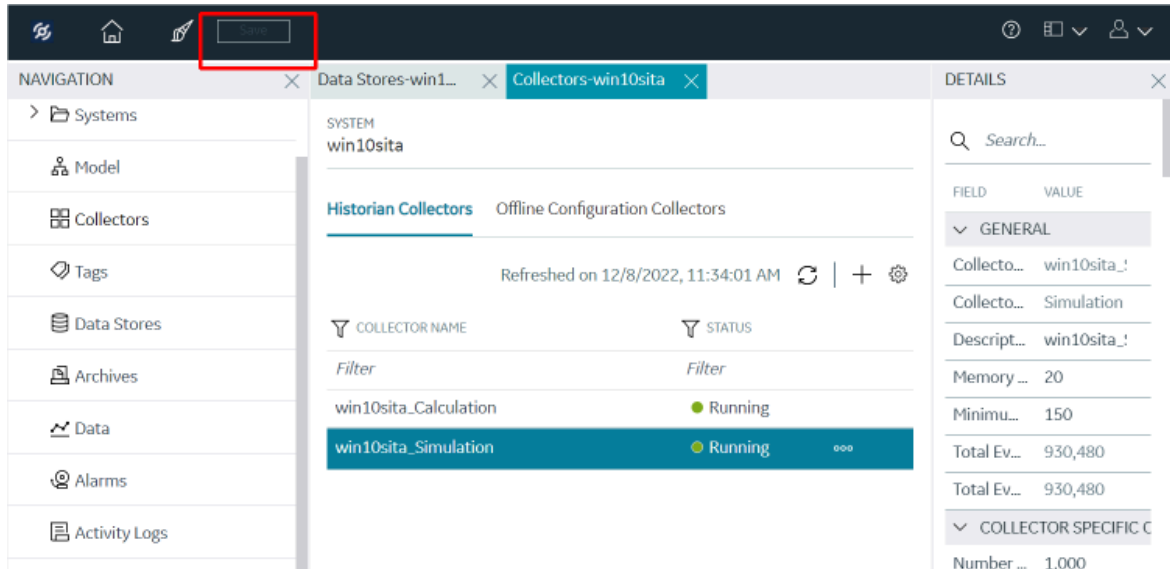
b. Enter values as described in the following table.

Field	Description
NAME	<p>Enter a name for the template. A value is required and must be unique.</p> <p>The value that you enter:</p> <ul style="list-style-type: none"> ▪ Must begin with a letter or a number. ▪ Can contain up to 256 characters. ▪ Can include any of the following special characters: /!#{}%\$-_ +^:;,?"*=}{@ ▪ Must not include a space or any of the following characters: ~`
DESCRIPTION	Enter a description for the template.

c. Repeat step 7 to add variables to the custom template.

The custom template is created, along with the variables. You can add more variables, and include/exclude existing variables later too.

9. In the upper-left corner of the page, select **Save**.



The object type, along with the default template, custom templates, and variables, is created.

[Create an object instance \(on page 939\).](#)

Include a Contained Type in an Object Type

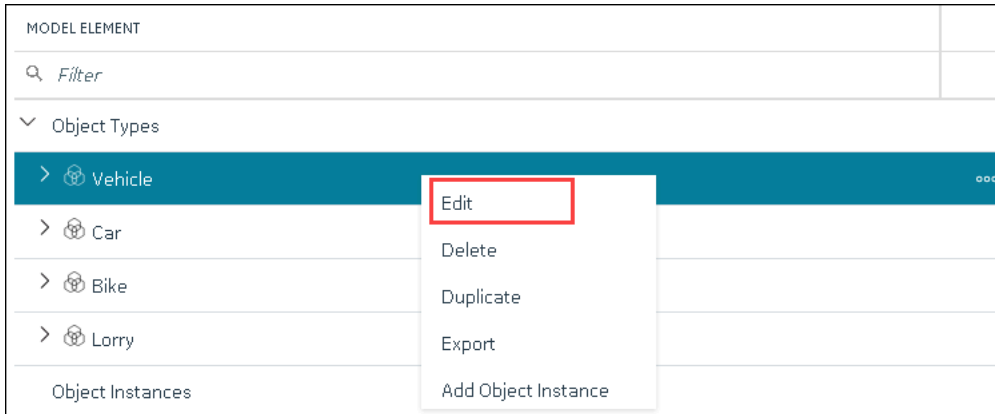
[Create an object type \(on page 931\)](#) that you want to use as a contained type.

A contained type is an object type that you can include in another object type. When you do so, you can reuse the variables in the contained type without creating them again manually. These variables are inherited by object instances of the object type in which you include the contained type.

You can include a single contained type in multiple object types and multiple contained types in a single object type.

For more information, refer to [About a Historian Model \(on page 921\)](#).

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Model**.
Alternatively, you can select **Systems**, and then in the row containing the system in which you want to create a contained type, select **...**, and then select **Browse Model**.
The **Model** section appears.
3. Under **Object Types**, right-click the object type in which you want to include the contained type (or select **...**), and then select **Edit**.



The **<object type name>** section appears, displaying a list of variables in the object type.

4. Select **Contained Types**.

NAME	DESCRIPTION																								
Vehicle	vehicle description																								
OBJECT TYPE TEMPLATE																									
Default_Template_Vehicle	...																								
Variables	Contained Types																								
<div style="display: flex; justify-content: space-between; align-items: center;"> ▼ VARIABLES 🗑️ 📄 New </div> <table border="1"> <thead> <tr> <th><input type="checkbox"/></th> <th>VARIABLE</th> <th>↑▼ VARIABLE TYPE</th> <th>▼ DATA TYPE</th> <th>▼ DESCRIPTION</th> <th>▼ INCLUDE</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>Color</td> <td>STATIC</td> <td>NUMBER</td> <td></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input type="checkbox"/></td> <td>Mileage</td> <td>INDIRECT</td> <td>NUMBER</td> <td></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input type="checkbox"/></td> <td>Speed</td> <td>DIRECT</td> <td>NUMBER</td> <td></td> <td><input checked="" type="checkbox"/></td> </tr> </tbody> </table>		<input type="checkbox"/>	VARIABLE	↑▼ VARIABLE TYPE	▼ DATA TYPE	▼ DESCRIPTION	▼ INCLUDE	<input type="checkbox"/>	Color	STATIC	NUMBER		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Mileage	INDIRECT	NUMBER		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Speed	DIRECT	NUMBER		<input checked="" type="checkbox"/>
<input type="checkbox"/>	VARIABLE	↑▼ VARIABLE TYPE	▼ DATA TYPE	▼ DESCRIPTION	▼ INCLUDE																				
<input type="checkbox"/>	Color	STATIC	NUMBER		<input checked="" type="checkbox"/>																				
<input type="checkbox"/>	Mileage	INDIRECT	NUMBER		<input checked="" type="checkbox"/>																				
<input type="checkbox"/>	Speed	DIRECT	NUMBER		<input checked="" type="checkbox"/>																				

A list of contained types in the object type appears.

5. In the **CONTAINED TYPES** table, select **New**.

NAME	DESCRIPTION
Vehicle	vehicle description

OBJECT TYPE TEMPLATE

Default_Template_Vehicle ▼ ⋮

Variables [Contained Types](#)

▼ CONTAINED TYPES 🗑️ 📄 New

<input type="checkbox"/>	ALIAS	TYPE	TEMPLATE
<input type="checkbox"/>	MyObjType	MyObjectType	Default_Template_MyObjectType
<input type="checkbox"/>	manufacturecontain	Manufacture	Default_Template_Manufacture
<input type="checkbox"/>			

A blank row appears in the table.

6. Enter values as described in the following table, and press ENTER.

Field	Description
ALIAS	<p>Enter a name for the contained type. A value is required. It need not match the original name of the contained type that you want to include.</p> <p>The value that you enter:</p> <ul style="list-style-type: none"> ◦ Must begin with a letter or a number. ◦ Can contain up to 256 characters. ◦ Can include any of the following special characters: /!#{}%\$-_ ◦ Must not include a space or any of the following characters: ~`+^;,:?"*={}@
TYPE	<p>Select the object type that you want to include as a contained type. This field contains a list of all the object types in the Historian system.</p>
TEMPLATE	<p>Select the template from the object type that you want to include. This field contains a list of templates in the object type. Only the variables in the selected template will be inherited by instances of the object type in which you want to include the contained type.</p>

The contained type is included in the object instance.

7. In the upper-left corner of the page, select **Save**.

The screenshot shows the Configuration Hub interface for the 'win10sita' system. The top navigation bar includes a 'Save' button, which is highlighted with a red box. The main content area displays the 'Historian Collectors' configuration, showing a table of collectors with columns for 'COLLECTOR NAME' and 'STATUS'. The table lists two collectors: 'win10sita_Calculation' and 'win10sita_Simulation', both with a 'Running' status. The 'win10sita_Simulation' row is highlighted in blue. The right-hand side of the interface shows a 'DETAILS' pane with a search bar and a table of fields and values, including 'Collecto...', 'Descript...', 'Memory ...', 'Minimu...', 'Total Ev...', and 'Number ...'.

The changes to the object type are saved.

[Create an object instance \(on page 939\)](#). The object instance will include the variables directly added in the object type, along with the ones in the selected template in the contained type.

Create an Object Instance

[Create an object type \(on page 931\)](#).

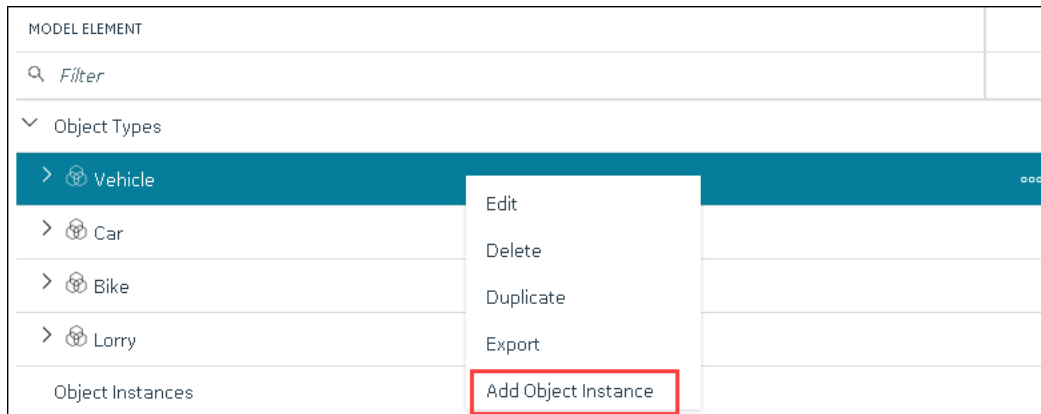
For each item of an object type, you must create an object instance so that you can capture values of the variables in the instance. These values are then stored in Historian.



Note:

After you create an object instance, you cannot rename, import, export, or delete a variable, contained types, or templates in the associated object type; you can only create new ones.


1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Model**.
Alternatively, you can select **Systems**, and then in the row containing the system in which you want to create a model, select **⋮**, and then select **Browse Model**.
The **Model** section appears.
3. In the **SYSTEM** list, select the system in which you want to create an object instance.
4. Under **Object Types**, right-click the object type whose instance you want to create (or select **⋮**), and then select **Add Object Instance**.



The **New Object Instance** window appears.

5. Enter values as described in the following table.

Field	Description
NAME	<p>Enter a name for the object instance. A value is required and must be unique for the object type.</p> <p>The value that you enter:</p> <ul style="list-style-type: none"> ◦ Must begin with a letter or a number. ◦ Can contain up to 256 characters.

Field	Description
DESCRIPTION	<ul style="list-style-type: none"> ◦ Can include any of the following special characters: /!#{}%\$-_ ◦ Must not include a space or any of the following characters: ~`+^:;,?"*={}@
OBJECT TYPE	Enter a description for the object instance.
OBJECT TYPE TEMPLATE	This field is disabled and populated with the object type that you have selected.
	Select the template that you want to apply to the object instance.
	<div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;"> <p> Note: After you apply a template to an object instance, you cannot modify or delete a variable in the object type; you can only add more variables.</p> </div>

6. Select **Create**.

The object instance is created.

7. In the **Model** section, under **Instances**, expand the instance that you have created, and then expand **Variables**.


A list of variables inherited from the template in the object type appear.

8. Select a variable.

The details of the variable appear in the **DETAILS** section.




Tip:

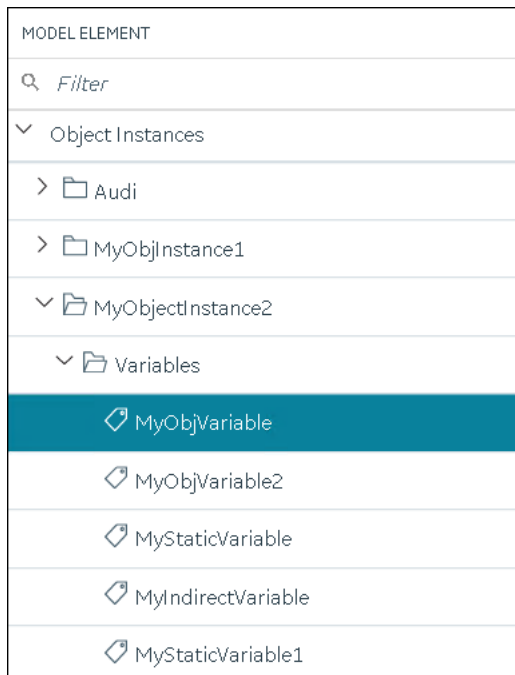
If the **DETAILS** section does not appear, in the upper-right corner of the page, select , and then select **DETAILS**.

- [Provide data for static variables \(on page 941\)](#).
- Collect data for [direct \(on page 944\)](#) and [indirect \(on page 947\)](#) variables.

Provide Data for a Static Variable

A static variable contains a fixed value. Therefore, when you create an object instance, you can access the variable, and provide its value.


1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Model**.
Alternatively, you can select **Systems**, and then in the row containing the system in which you want to create a model, select , and then select **Browse Model**.
The **Model** section appears.
3. Under **Object Instances**, expand the object instance, expand **Variables**, and then select the variable whose data you want to provide.



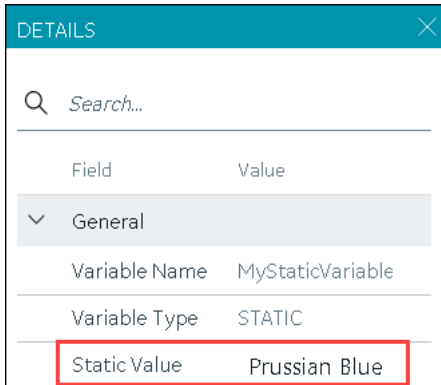
The details of the variable appear in the **DETAILS** section.



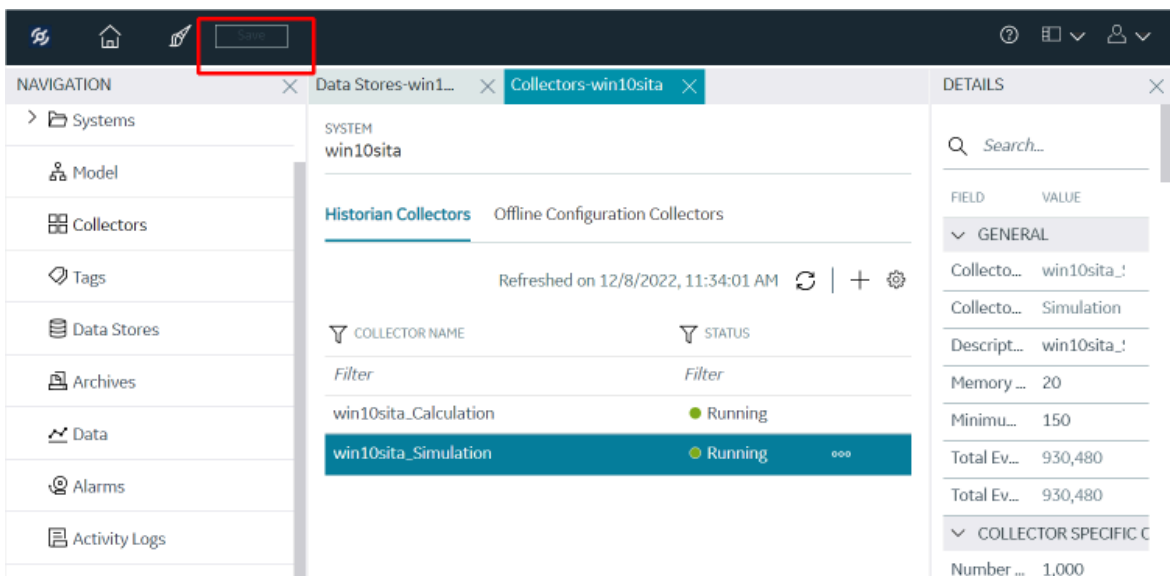
Note:

If the **DETAILS** section does not appear, in the upper-right corner of the page, select , and then select **DETAILS**.

4. In the **DETAILS** section, in the **Static Value** field, enter the value that you want to provide for the variable, and then press ENTER.



5. In the upper-left corner of the page, select **Save**.



The value for the variable is saved.

Collect Data for a Direct Variable

1. [Create a collector instance \(on page 909\)](#) using which you want to collect data for the variable.
2. [Add the tag \(on page 909\)](#) using which you want to collect data.

To collect data of a direct variable, you must associate the variable with a collector instance and a tag. When you do so, the tag is created in Historian, and values for the variable are collected by the collector instance and stored in Historian.



Important:

If the name of a tag associated with a variable in a model contains a period (.), you cannot import the tag while importing the model into a Historian system.


1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Model**.
Alternatively, you can select **Systems**, and then in the row containing the system in which you want to create a model, select **☰**, and then select **Browse Model**.
The **Model** section appears.
3. Under **Object Instances**, expand the object instance, expand **Variables**, and then select the variable whose data you want to collect.

MODEL ELEMENT
🔍 Filter
▼ Object Instances
> 📁 Audi
> 📁 MyObjInstance1
▼ 📁 MyObjectInstance2
▼ 📁 Variables
🔗 MyObjVariable
🔗 MyObjVariable2
🔗 MyStaticVariable
🔗 MyIndirectVariable
🔗 MyStaticVariable1

The details of the variable appear in the **DETAILS** section.



Note:

If the **DETAILS** section does not appear, in the upper-right corner of the page, select , and then select **DETAILS**.

4. In the **Source Address** field, select .

The **Browse Source Tag** window appears.

5. Enter values as described in the following table.

Field	Description
COLLECTOR NAME	Enter the name of the collector using which you want to collect data of the variable. A value is required.
COLLECTED TYPE	Specify whether you want to browse through all the tags in the data source or only from the

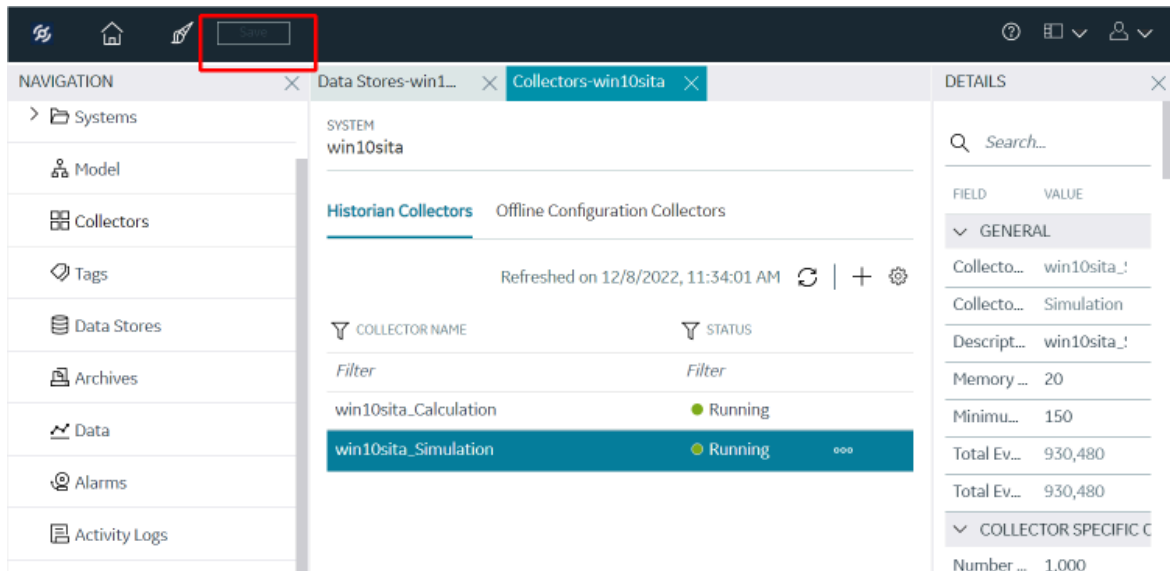
Field	Description
	tags that you have not added yet. A value is required.
SOURCE TAG NAME	Enter the name of the tag (either completely or partially) to narrow down the search results.
SOURCE TAG DESCRIPTION	Enter the description of the tag (either completely or partially) to narrow down the search results.

6. Select **Search Tags**.

A list of tags that match *all* the search criteria appears.

7. Select the collector tag that you want to map with the variable, and then select **Apply**.

8. In the upper-left corner of the page, select **Save**.



The tag is mapped with the variable. A corresponding tag is created in Historian. The details of the tag and the collector instance are disabled and populated in the **DETAILS** section. All the data that is collected for the tag is now stored in Historian (or in a cloud destination as configured in the collector instance).

Collect Data for an Indirect Variable

1. [Add or ensure there is a collector instance \(on page 909\)](#) which you want to collect data for the variable.
2. [Add the tag \(on page 909\)](#) that you want to map with the variable.

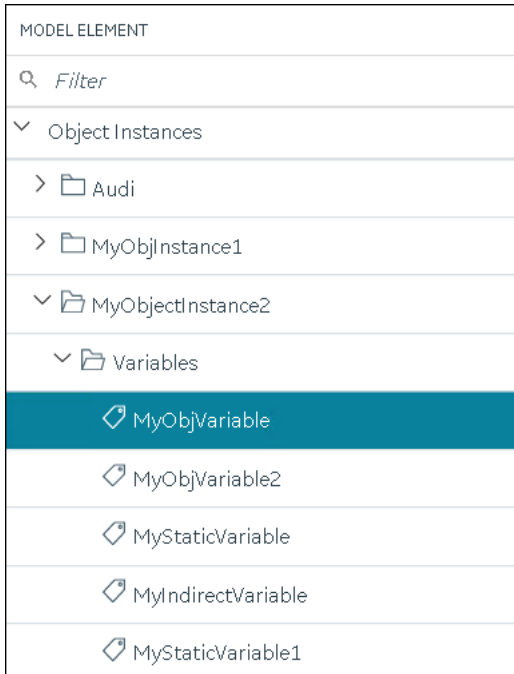
To collect data of an indirect variable, you must associate the variable with a collector instance and an existing Historian tag. The values for the variable are then collected by the collector instance and stored in Historian.




Important:


- If the name of a tag associated with a variable in a model contains a period (.), you cannot import the tag while importing the model into a Historian system.
- If you want to later delete the tag, first remove the mapping between the tag and the variable.


1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Model**.
Alternatively, you can select **Systems**, and then in the row containing the system in which you want to create a model, select **☰**, and then select **Browse Model**.
The **Model** section appears.
3. Under **Object Instances**, expand the object instance, expand **Variables**, and then select the variable whose data you want to collect.

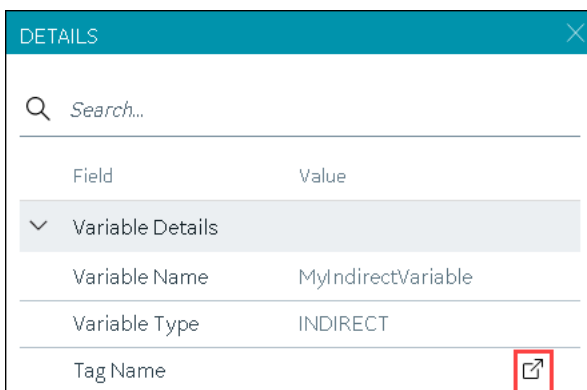


The details of the variable appear in the **DETAILS** section.

 **Note:**

If the **DETAILS** section does not appear, in the upper-right corner of the page, select , and then select **DETAILS**.

4. In the **DETAILS** section, in the **Tag Name** field, select .



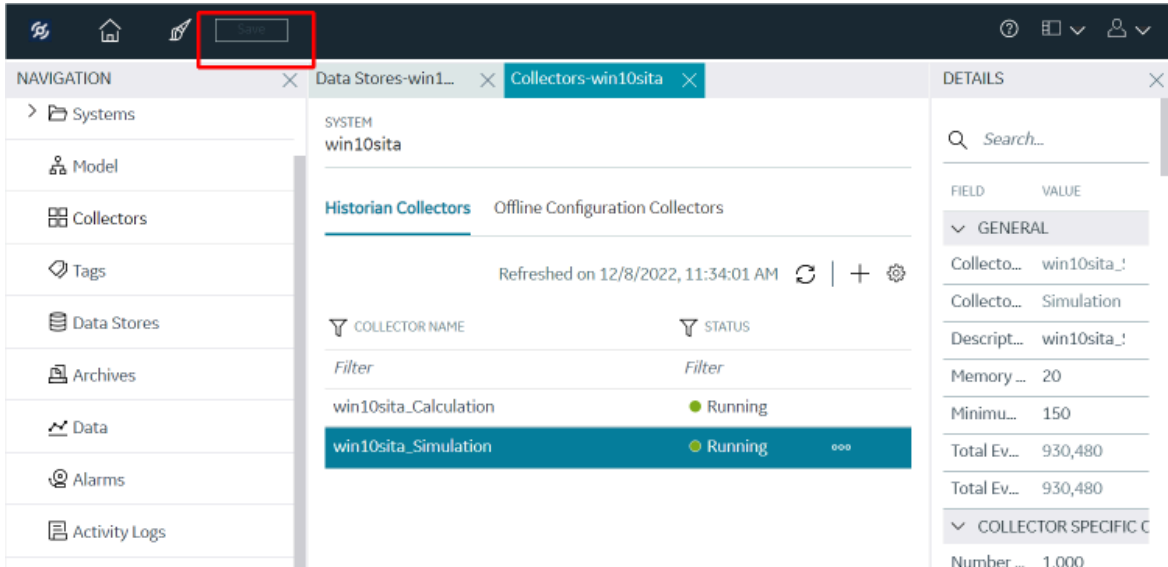
The **Tag Selection: <variable name>** window appears.

5. Select **Search** to search for tags.

6. Enter the search criteria, and then select **Search**. You can enter a name or a value partially or use the wildcard character asterisk (*). You can add more search criteria by selecting **Add Attribute**.

The list of tags are filtered based on the search criteria.

7. Select the collector tag that you want to map with the variable, and then select **Apply**.
8. In the upper-left corner of the page, select **Save**.



The screenshot shows the Configuration Hub interface for the 'win10sita' system. The 'Collectors' page is active, displaying a table of 'Historian Collectors'. The 'win10sita_Simulation' collector is selected and highlighted in blue. The interface includes a navigation pane on the left, a main content area with a table of collectors, and a details pane on the right.

COLLECTOR NAME	STATUS
win10sita_Calculation	Running
win10sita_Simulation	Running

The details pane on the right shows the following information:

FIELD	VALUE
Collecto...	win10sita_!
Collecto...	Simulation
Descript...	win10sita_!
Memory ...	20
Minimu...	150
Total Ev...	930,480
Total Ev...	930,480
Number ...	1,000

You can choose any of the following options provided while mapping the indirect variable with an existing Historian tag to save in Historian with or without the model hierarchy.

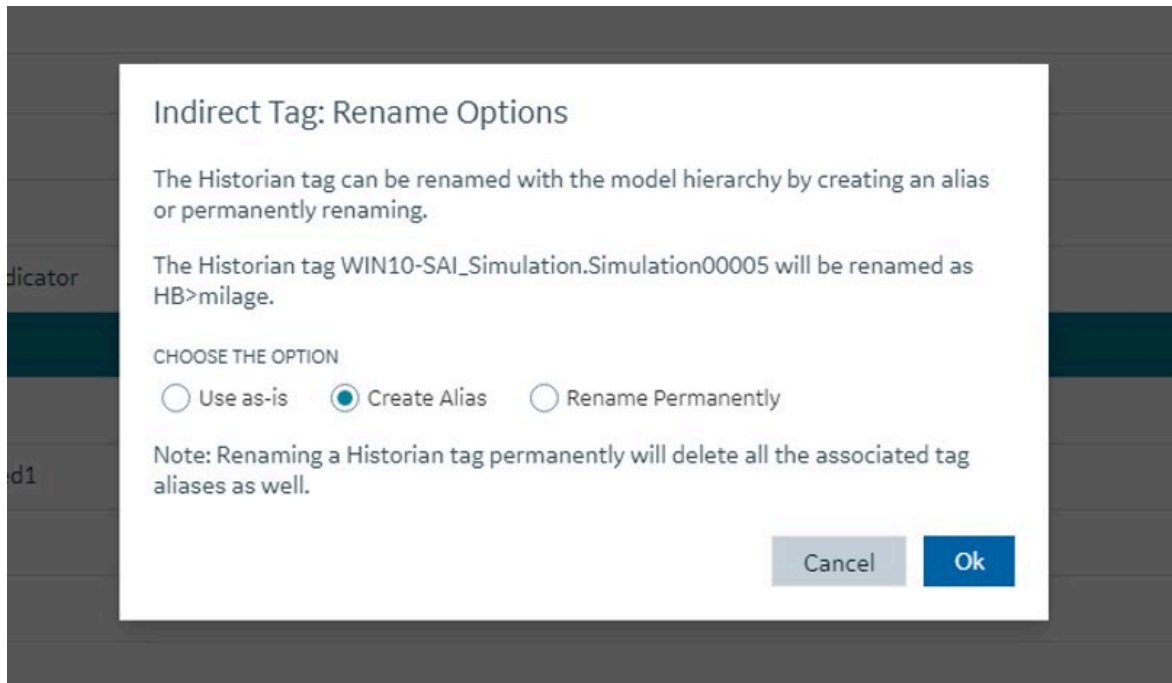


Table 16.

Field	Description
Use as is	Choosing this option will not update the Historian tag name. Mapping Information will be saved only in model database. Mapping information won't be available with Historian (when you export and try to trend with trending tools like Operations Hub, you will not be able to trend as they are connected to Historian Database).
Create Alias	Choosing this option creates an alias of Historian tag mapped with indirect variable. This option will save the model tag both in the model database and Historian database as an alias. When you export the model, you will be able to trend and see the data. (This is the default option.)
Rename Permanently	Choosing this option will permanently rename the Historian tag mapped with the model indi-


Field	Description
	rect variable and removes the existing tag. So, there will be chance that existing trends using this Historian tag might have impact.

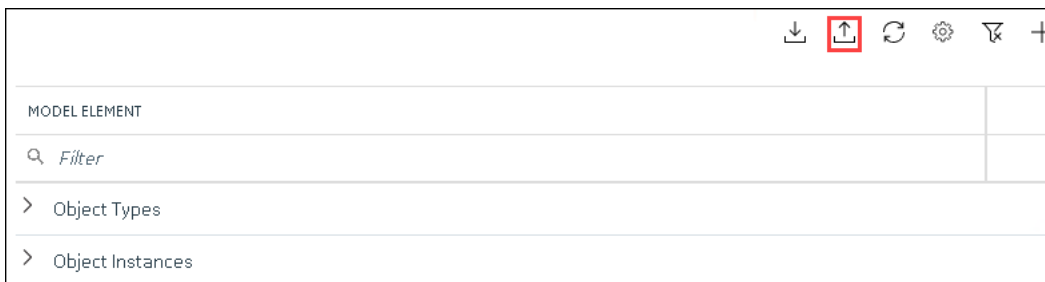
Export an Object Type/Instance

When you create an object type or an object instance, you can use it only in the Historian system in which you have created it. If, however, you want to use the object type/instance in a different Historian system or Operations Hub, you can export it and then import it into the other Historian system or Operations Hub.

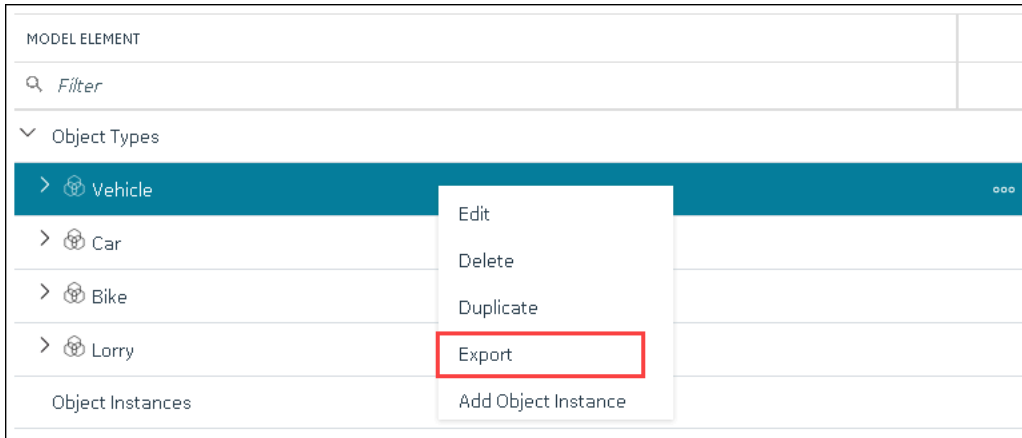
The following conditions apply when you export an object type/instance:

- You can export each object type/instance separately or all the object types and object instances in a Historian system at once.
- You can choose to export the variables or object instances of an object type (or both).
- You can choose to export the variables and templates of an object instance (or both). You cannot, however, export templates to Operations Hub.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Model**. Alternatively, you can select **Systems**, and then in the row containing the system in which you want to create a model, select **☰**, and then select **Browse Model**. The **Model** section appears.
3. If you want to export all the object types/instances in the Historian system, in the upper-right corner of the main section, select .

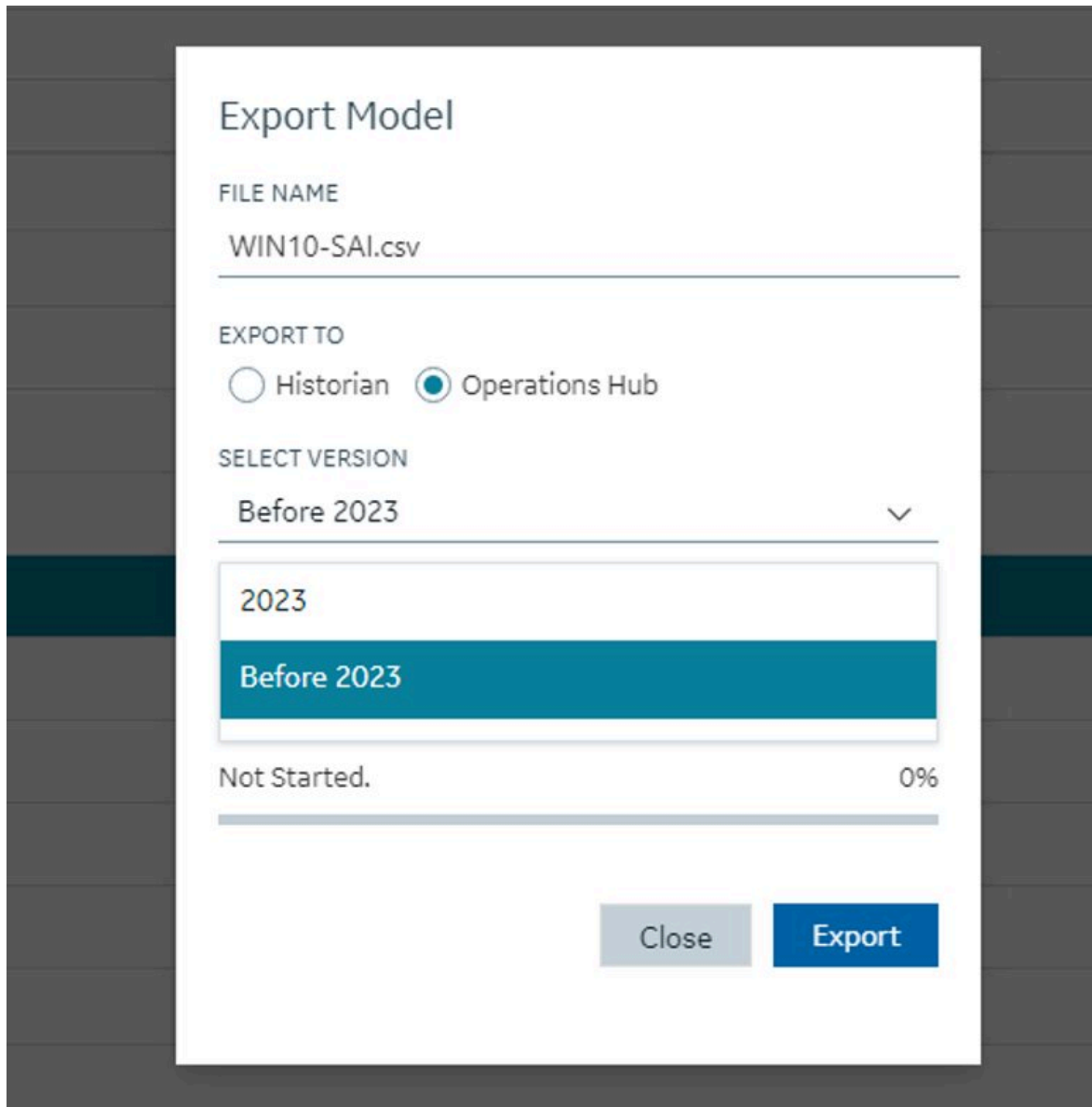


If you want to export a single object type/instance, under **Object Types** or **Object Instances**, right-click the object type/instance that you want to export (or select **☰**), and then select **Export**.



The **Export Model** window appears. Depending on whether you are exporting all the object types/ instances in the system or just a single one, the **File name** field contains a value in the following format: *<host name>.csv* or *<object type>.csv* or *<object instance.csv>*.

4. If needed, modify the value in the **File name** field.
5. Depending on whether you want to export to another Historian system or Operations Hub, select the appropriate option.
6. Operations Hub 2023 supports multi model with multiple roots, you can choose the version while exporting the model either to 2023 or versions prior to 2023.



7. Depending on whether you want to export the templates, the object instances, or both, ensure that the corresponding check boxes are selected. However, you can export templates only to a Historian system, not to Operations Hub.

8. Select **Export**.

The object types/instances, along with the underlying object variables, are exported in to a .csv file.

Import an Object Type/Instance

When you create an object type or an object instance, you can use it only in the Historian system in which you have created it. If, however, you want to use the object type/instance in a different Historian system or Operations Hub, you can export it and then import it into the other Historian system or Operations Hub.


You can import each object type/instance separately or all the object types/instances in a Historian system at once.

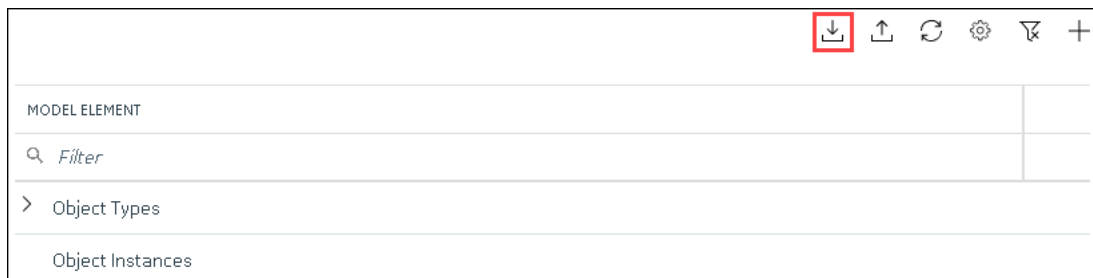


Important:

If the name of a tag associated with a variable in a model contains a period (.), you cannot import the tag while importing the model into a Historian system.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Model**.
Alternatively, you can select **Systems**, and then in the row containing the system in which you want to create a model, select **☰**, and then select **Browse Model**.
The **Model** section appears.

3. In the upper-right corner of the main section, select .



The **Import Model** window appears.

4. Select **Choose File**, and then select the .csv file that contains the object types/instances that you want to import.
5. Depending on whether you want to import the templates, the object instances, or both, ensure that the corresponding check boxes are selected.
6. Select **Import**.

The object types/instances are imported.

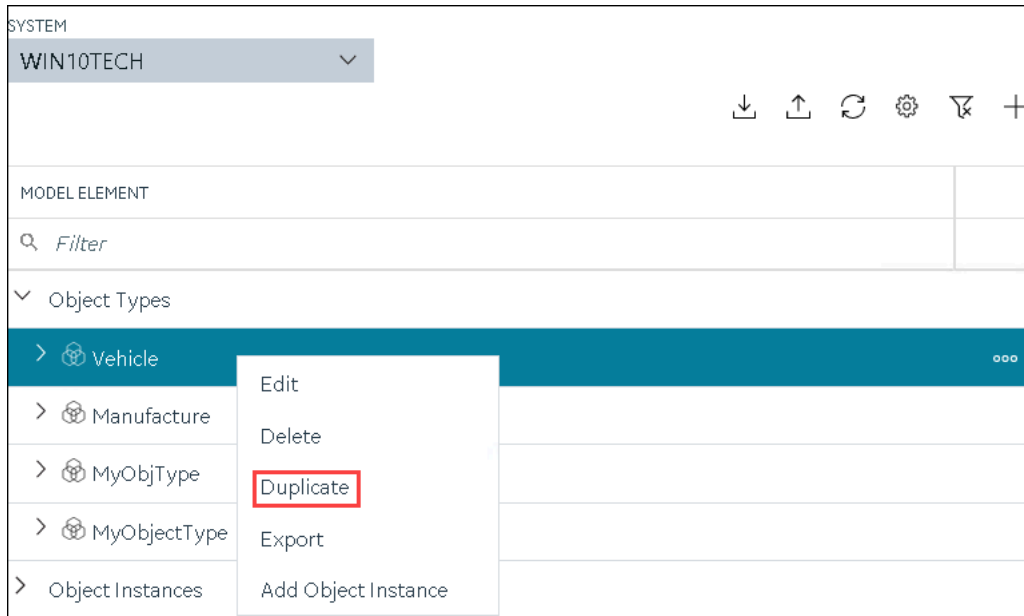
Copy an Object Type

When you create an object type, you also create the default template, custom templates, and variables for each template. For information on each of these template types and variables, refer to [About a Historian Model \(on page 921\)](#) and [About Object Templates \(on page 927\)](#).

When you copy an object type, all the templates and variables are copied too.

This topic describes how to copy an object type. You can also [create one \(on page 931\)](#).

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Model**.
Alternatively, you can select **Systems**, and then in the row containing the system in which you want to create a model, select **...**, and then select **Browse Model**.
The **Model** section appears.
3. Under **Object Types**, select the object type that you want to copy, and then select **Duplicate**.



The **Duplicate Object Type** window appears.

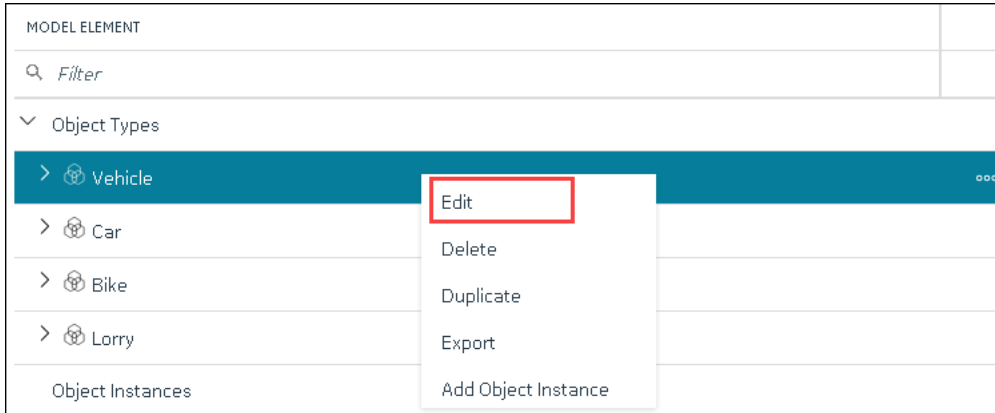
4. Enter values as described in the following table.

Field	Description
NAME	<p>Enter a name for the object type. A value is required and must be unique.</p> <p>The value that you enter:</p> <ul style="list-style-type: none"> ◦ Must begin with a letter or a number. ◦ Can contain up to 256 characters. ◦ Can include any of the following special characters: /!#{}%\$-_ ◦ Must not include a space or any of the following characters: ~`+^:;,?"*={}@
DESCRIPTION	Enter a description for the object type.

5. Select **Create**.

The object type is copied, along with the variables and templates in the original object type.

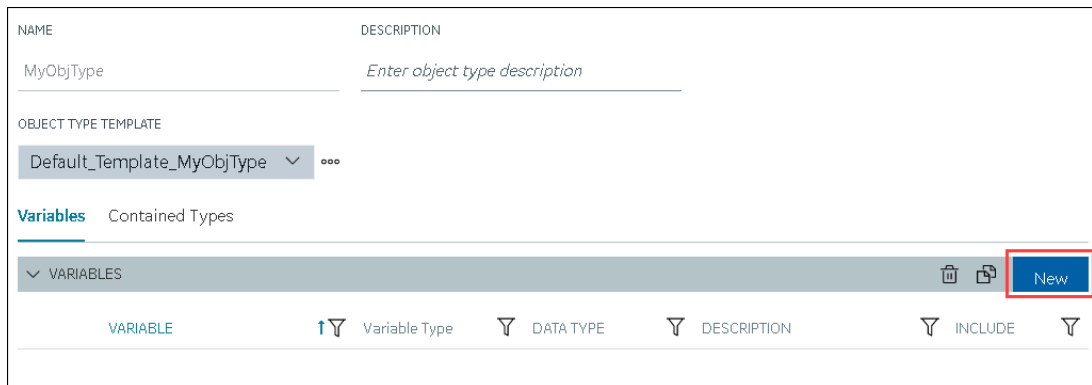
6. Right-click the object type that you have copied (or select **☰**), and then select **Edit**.



The **<object type name>** section appears. The **OBJECT TYPE TEMPLATE** field contains all the templates in the original object type. In addition, each template contains all the variables as defined in the original object type.

7. To add more variables to a template:

- a. In the **OBJECT TYPE TEMPLATE** field, select the template to which you want to add more variables.
- b. In the **Variables** table, select **New**.



A blank row appears in the table.

- c. Enter values as described in the following table.

Column	Description
VARIABLES	Enter the name of the variable. It must be unique for the object type.
VARIABLE TYPE	Choose one of the following types of variables: <ul style="list-style-type: none"> ▪ Direct: Tags for these variables are created in Historian when you select a collector instance. ▪ Indirect: These variables are mapped with existing Historian tags. ▪ Static: These variables have a static value, which you provide when you create an object instance.
DATATYPE	Select the data type of the variable.
DESCRIPTION	Enter a description for the variable.
INCLUDE	Switch the toggle to indicate whether you want to include the variable in the template.

**Tip:**

If you want to modify a variable, change the values in the aforementioned fields.

If you want to delete a variable, select the check box next to the variable, and then

select .

**Note:**


After you apply a template to an object instance, you cannot modify or delete a variable in the object type; you can only add more variables.

d. Press ENTER.

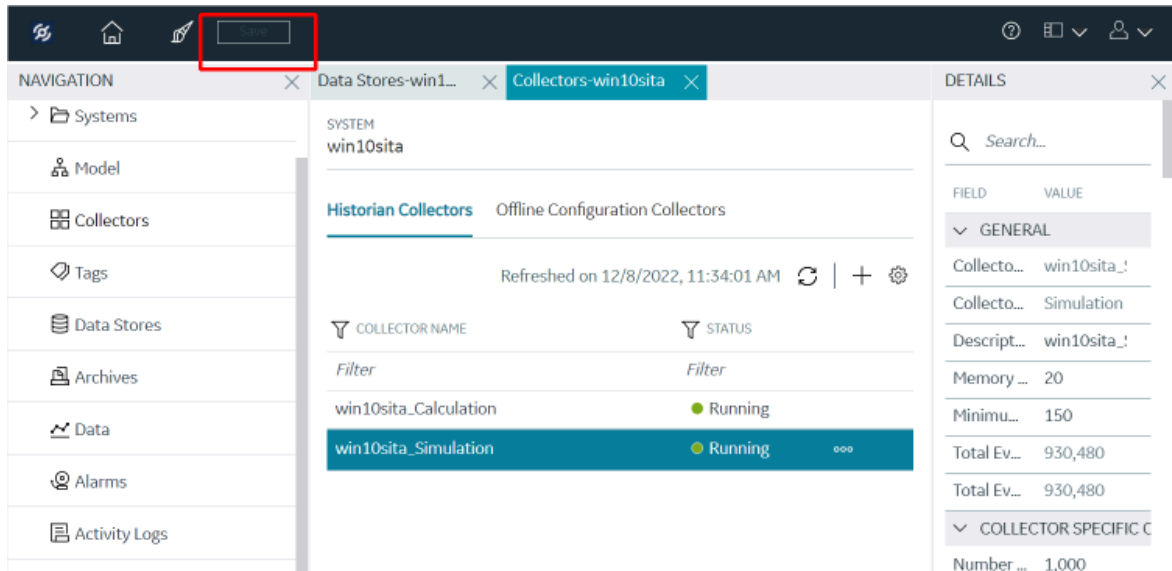
The default template is modified, and the new variables have been added. You can add more variables or include/exclude variables later too.



Note:

If you want to create a variable by copying an existing one, select the check box next to the variable that you want to copy, and then select . You can copy only one variable at a time.

8. In the upper-left corner of the page, select **Save**.



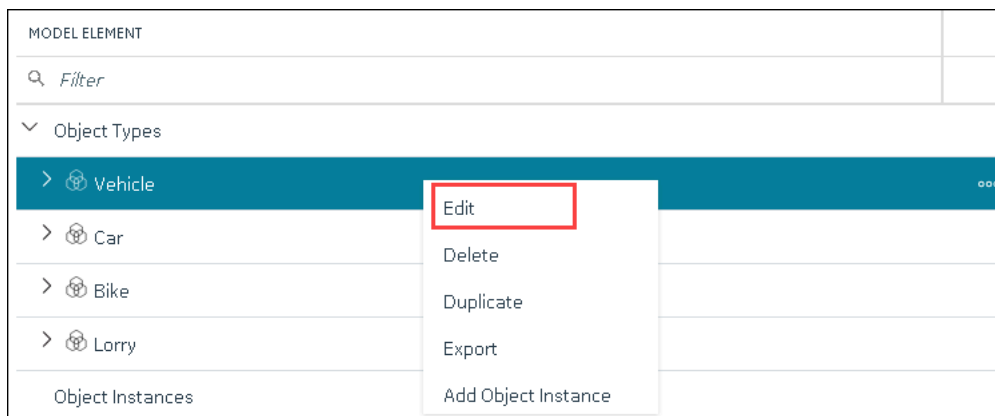
The object type, along with the default template, custom templates, and variables, is created.

[Create an object instance \(on page 939\).](#)

Delete a Template

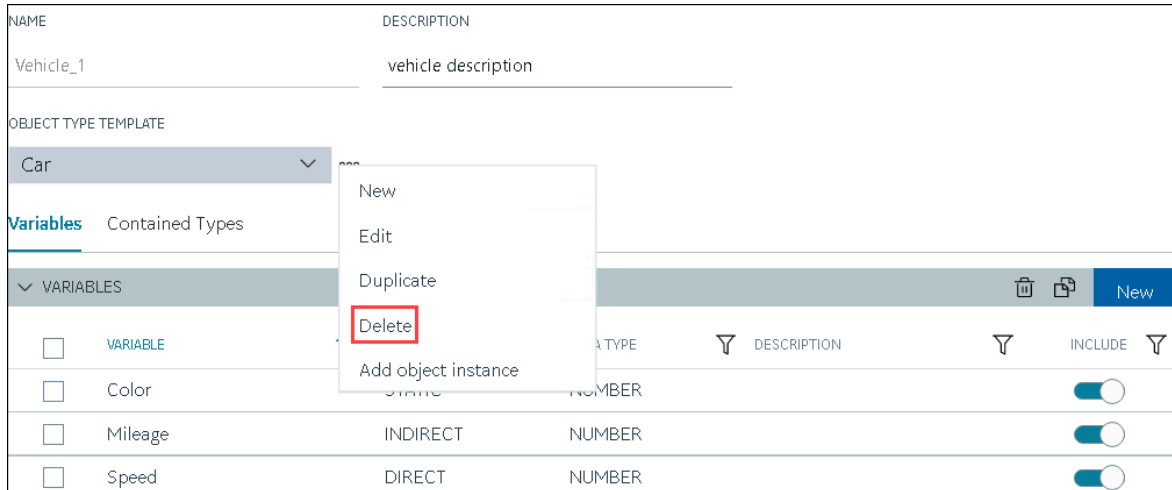
This topic describes how to delete a custom template. You cannot delete a template that is in use (that is, an object instance has been created for the object type). And, you cannot delete the default template in an object type.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Model**.
Alternatively, you can select **Systems**, and then in the row containing the system in which you want to create a model, select **...**, and then select **Browse Model**.
The **Model** section appears.
3. In the main section, under **Object Types**, right-click the object type from which you want to delete a template (or select **...**), and then select **Edit**.



The **<object type name>** section appears. The **OBJECT TYPE TEMPLATE** field contains the default template.

4. In the **OBJECT TYPE TEMAPLTE** field, select the template that you want to delete.
5. Next to the **OBJECT TYPE TEMPLATE** field, select **...**, and then select **Delete**.

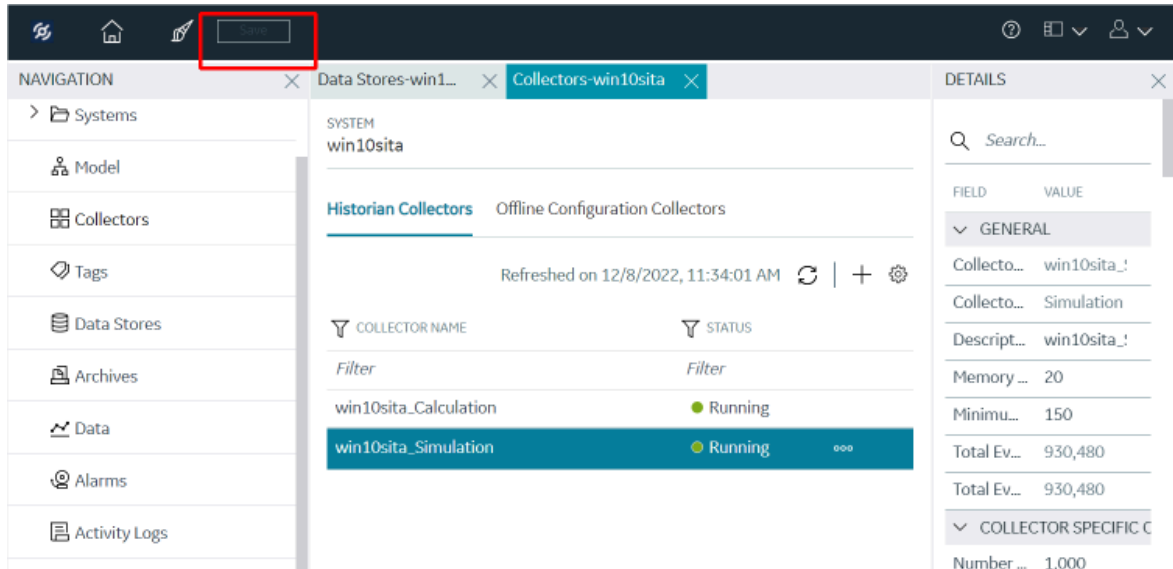


A message appears, asking you to confirm that you want to delete the template.

6. Select **Yes**.

The template is deleted.

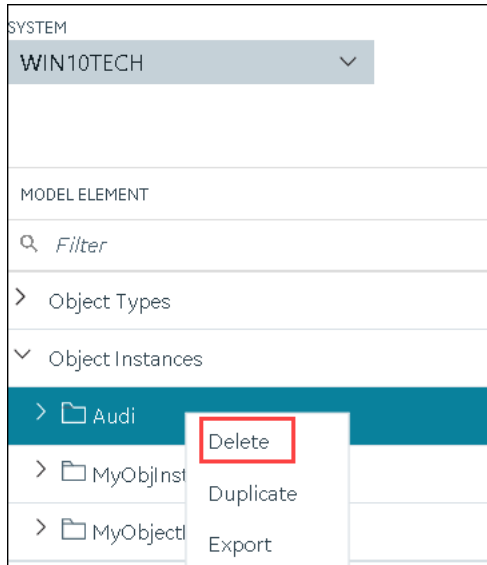
7. In the upper-left corner of the page, select **Save**.



The changes to the object type are saved.

Delete an Object Instance

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Model**.
Alternatively, you can select **Systems**, and then in the row containing the system in which you want to create a model, select **...**, and then select **Browse Model**.
The **Model** section appears.
3. Under **Object Instances**, right-click the object instance that you want to delete (or select **...**), and then select **Delete**.



A message appears, asking you to confirm that you want to delete the object instance. If there are direct variables in the object type, you can also choose to delete the tags associated with these variables (along with their data).

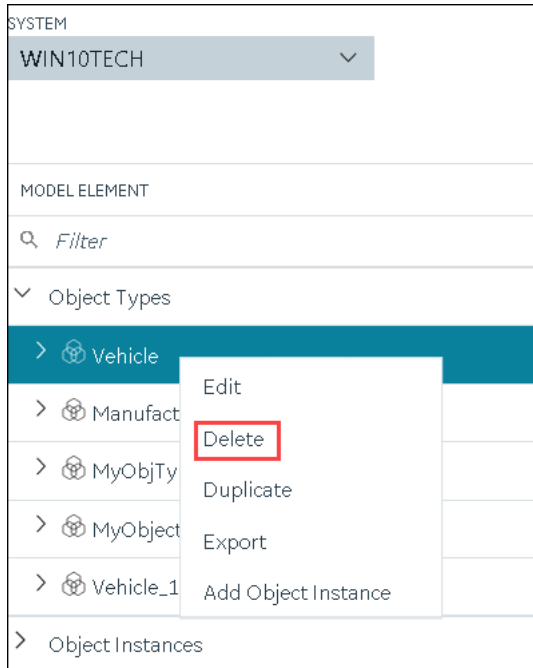
4. Select **Yes**.

The object instance is deleted, along with the underlying variables and templates.

Delete an Object Type

You cannot delete an object type if it is used in an object instance; you must first [delete the object instance \(on page 961\)](#).

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Model**.
Alternatively, you can select **Systems**, and then in the row containing the system in which you want to create a model, select **☰**, and then select **Browse Model**.
The **Model** section appears.
3. Under **Object Types**, right-click the object type that you want to delete (or select **☰**), and then select **Delete**.



A message appears, asking you to confirm that you want to delete the object type.

4. Select **Yes**.

The object type is deleted, along with the underlying variables and templates in the object type.

If, however, the object type is used in an object instance, a message appears, asking you to first delete the object instance.

Managing Historian Systems

Access a System

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, expand **Systems**, and then select the system that you want to access.

The system appears in the main section. The following details of the system appear in the **DETAILS** section.

Table 17. The General Section

Field	Description
Name	The name of the system.
System Type	The type of the system (whether stand-alone or distributed).
Primary Server	The primary server of the system.

Field	Description
Description	The description of the system.
Default System	<p>Indicates whether the system is a default one. If yes, when you log in to Configuration Hub, this system appears by default. The following conditions apply for a default system:</p> <ul style="list-style-type: none"> ◦ You can have only one default system in Configuration Hub. ◦ You cannot delete a default system. <p>For instructions of setting a default system, refer to Set a Default System (on page 996).</p>
Collectors	The number of collectors in the system.
Tags	The number of tags in the system.
Data Stores	The number of data stores in the system.
Clients	The number of clients in the system.
Server Time	The current time of the server.
Server Version	The version of the server.
Demo Mode	Indicates whether the server is currently in demo-license mode.
Clustered	Indicates whether the server is currently in clustered environment.

Table 18. The System Defaults Section



Field	Description
Default Data Store	The default data store in the system. A default data store is the one that is considered if you do not specify a data store while adding a tag. For instructions on setting a data store as default, refer to Set a Default Data Store (on page 1013) .
Default Location	<p>The default location in the system. A default location is a server in a system which is considered when you do not specify a location while creating a Data Store. By default, the distributed location on the primary server is the default location. You can, however, set a different default location. To set the default location</p> <p>select  .</p>

Table 19. The Alarms and Events Section

Field	Description
Alarms Rate	The rate at which alarm data (on page 1259) is collected in the system.

Table 20. The License Section

Field	Description
Historian Tags	<p>The number of tags in the system (out of the total number of licensed tags).</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: If this field displays 100 tags and the Users field displays 1 client, you are likely running in demonstration mode and may have incorrectly installed your hardware key.</p> </div>
Scada Tags	The number of SCADA tags in the system (out of the total number of licensed SCADA tags).
Users	<p>The number of users in the system (out of the total number of users authorized to access Historian using the software key and license).</p> <p>The number of users that are authorized to access Historian is strictly based on the software key and license. However, if you have utilized your available Client Access Licenses (CAL) and need an additional one to use the system in an emergency, you have an option to reserve a CAL. This reserved CAL allows you to access the server. To do so, provide the reserved CAL to the system administrators and add them to the ih Security Admins group. A system administrator can then connect to Historian in an emergency.</p> <p>This facility is optional and does not provide a guaranteed connection. It only eliminates the emergency situations when a CAL is preventing you from accessing the system and may not work</p>

Field	Description
	if there are other conditions. For example, if the Historian server is busy, you will not be able to connect using this feature.
Data Stores	The number of data stores in the system (out of the total number of licensed data stores).
Calculations	Indicates whether the Calculation collector is licensed on the software key.
Server to Server	Indicates whether the Server-to-Server collector is licensed on the software key.
OPC HDA Server	Indicates whether the OPC Classic HDA server is licensed on the software key.
OPC UA HDA Server	Indicates whether the OPC UA HDA server is licensed on the software key.
Model	Indicates whether the object model is licensed on the software key.
Electronic Signature	Indicates whether electronic signature is licensed on the software key.

Table 21. The Global Security Section

Field	Description
Security Group	Indicates whether you want to use local or domain security groups.
Enforce Strict Client Authentication	If you enable this option, only known user accounts configured on the Data Archiver server computer will be able to access the Historian server.
Enforce Strict Collector Authentication	If you enable this option, only known collector connections configured on the Data Archiver server computer will be able to send data to the Historian server.

For more information on global security, refer to [Strict Authentication](#).

Table 22. The Electronic Signatures/Records Section

Field	Description
Require Point Verification	<p>Indicates whether you must enter identifying information whenever you attempt a restricted action. Whenever you attempt to change the system configuration (for the tag, archive, or collector), a tag value, or another record, you must electronically sign the action with a username and password. If the user is authorized to make this change, the identity of the person, the action performed, and the time it was performed, are all recorded in the audit trail.</p> <p>Note:</p> <ul style="list-style-type: none"> ◦ The audit features are not dependent on this feature being enabled. Historian audits all user actions regardless of whether this option is enabled. ◦ If you plan to create multiple archives at the same time, select the Disabled option. <p>Enabling electronic signatures and electronic records also requires you to reverify your identity when you use the Historian Excel add-in, modify or create a tag, or import data or messages.</p> <p>Note: This feature is available only if you have purchased the Electronic Signatures and Electronic Records option.</p>
Verification Message	<p>When point verification is enabled, you are prompted to enter the username and password whenever you attempt to perform an action specified as requiring point verification.</p>

3. Expand the system in the main section.

A list of servers in the system appears, displaying the following information.

Field	Description
MACHINE NAME	<p>In a stand-alone Historian system, this column displays the host name of the Historian server. In a horizontally scalable Historian system, this column displays the host name of the primary server.</p>


Field	Description
STATUS	The current status of the Historian system.
ARCHIVE COMPRESSION	<p>The current effect of archive data compression. At the system level, this value is calculated as the average of the corresponding values of individual servers in the system.</p> <p>If the value is zero, it indicates that archive compression is either ineffective or turned off. To increase the effect of data compression, increase the value of archive compression deadbands on individual tags in the Tags section to activate compression.</p> <p>In calculating the effect of archive compression, Historian counts internal system tags as well as data source tags. Therefore, when working with a very small number of tags and with compression disabled on data source tags, this field may indicate a value other than zero. If you use a realistic number of tags, however, system tags will constitute a very small percentage of total tags and will therefore not cause a significant error in calculating the effect of archive compression on the total system.</p>
WRITE CACHE HIT RATIO	<p>The hit ratio of the write cache in percentage of total writes. At the system level, this value is calculated as the average of the corresponding values of individual servers in the system.</p> <p>It is a measure of how efficiently the system is collecting data. Typically, this value should range from 95 to 99.99%. If the data is changing rapidly over a wide range, however, the hit percentage drops significantly because current values differ from recently cached values. More regular sampling may increase the hit percentage. Out-of-order data also reduces the hit ratio.</p>
CONSUMPTION RATE	<p>The rate at which the archive disk space is consumed. At the system level, this value is calculated as the sum of the corresponding values of individual servers in the system.</p> <p>If the value is too high, you can reduce it by slowing the poll rate on selected tags or data points or by increasing the filtering on</p>

Field	Description
	the data (widening the compression deadband to increase compression).
READ THREAD USAGE	The percentage of the read threads currently in use by the system. At the system level, this value is calculated as the average of the corresponding values of individual servers in the system.
WRITE THREAD USAGE	The percentage of the write threads currently in use by the system. At the system level, this value is calculated as the average of the corresponding values of individual servers in the system.
OUT OF ORDER WRITE RATE	The number of out-of-order events per minute. At the system level, this value is calculated as the sum of the corresponding values of individual servers in the system.
MIN DISK SPACE LEFT	The minimum free disk space in MB that must be available on the computer. If the minimum space required is not available when the collector starts, the collector will shut down.
FAILED WRITE RATE (EVENTS/MIN)	<p>The number of samples that failed to be written per minute. At the system level, this value is calculated as the sum of the corresponding values of individual servers in the system.</p> <p>Since failed samples are a measure of system malfunctions or an indication of offline archive problems, this value should be zero. If you observe a non-zero value, investigate the cause of the problem and take corrective action.</p> <p>Historian also generates a message if a writing a sample fails. Note that the message only appears once per tag, for a succession of failed writes associated with that tag. For example, if the number displayed in this field is 20, but they all pertain to one Historian tag, you will only receive one message until that Historian tag is functional again.</p>
MEMORY USAGE	Indicates how much server memory is being consumed.
READ QUEUE RATE (40 MSG/MIN)	The number of read requests processed per minute, that came into the archiver from all clients.

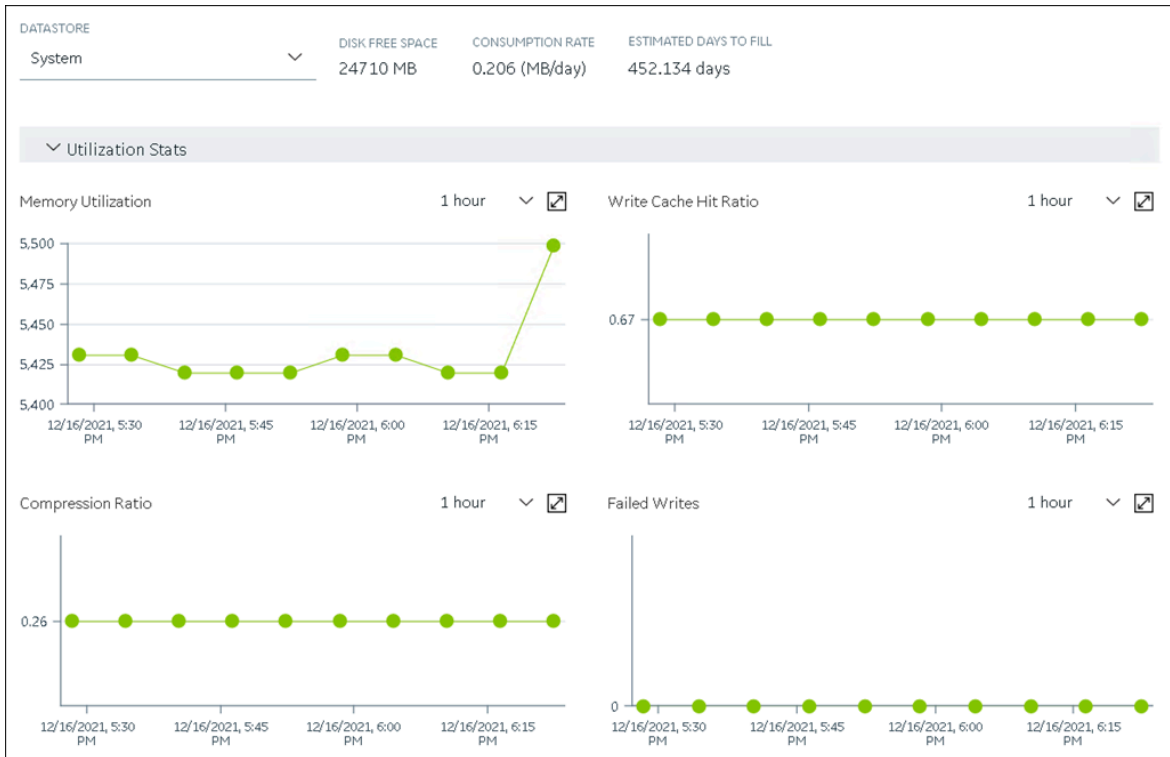
Field	Description
WRITE QUEUE RATE (MSG/MIN)	The number of write requests processed per minute, that came into the archiver from all clients.
MESSAGE QUEUE RATE (MSG/MIN)	The number of messages processed per minute.
READ QUEUE SIZE (EVENTS)	The total number of messages present in the Read queue.
WRITE QUEUE SIZE (EVENTS)	The total number of messages present in the Write queue.
MESSAGE QUEUE SIZE (MSG)	The total number of messages present in the Message queue.

**Tip:**

You can show/hide/reorder columns in the table. For instructions, refer to [Common Tasks in Configuration Hub \(on page 906\)](#).

4. To access the system performance, right-click the system (or select ) , and then select **View Server Performance**.

The **<system name> - Performance** section appears, displaying graphs for some of the metrics described in the previous table.



Access the Collectors in a System

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, expand **Systems**, and then select the system whose collectors you want to access.
The system appears in the main section.
3. Right-click the system whose collectors you want to access (or select **☰**), and then select **Browse Collectors**.

This displays the list of Historian collectors and Offline configuration collectors. By default, the Historian collector instances added to the system appear, displaying the following information.

Column	Description
COLLECTOR NAME	The name of the collector instance. If you select the link in this column, the details of the collector instance appears.

Column	Description
STATUS	The status of the collector. Contains one of the following values: <ul style="list-style-type: none"> ◦ Started ◦ Stopped ◦ Running ◦ Paused ◦ Unknown
CONFIGURATION	The source of the tag configuration for the collector. Contains one of the following values: <ul style="list-style-type: none"> ◦ HISTORIAN: Indicates that tags are configured using Historian Administrator. ◦ OFFLINE: Indicates that tags are configured using an offline configuration file.
MACHINE	The name of the machine on which the collector is installed.
VERSION	The version number of the collector.
REDUNDANCY	Indicates whether collector redundancy is enabled, which decreases the likelihood of lost data due to software or hardware failures. For more information, refer to About Collector Redundancy .
REPORT RATE	The average rate at which the collector is sending data. This is a general indicator of load on the collector.
OVERRUNS	The total number of data events not collected. In normal operation and under normal conditions, this value should always be zero. If the value is not zero, which indicates that data is being lost, you must take steps to reduce peak load on the system by increasing the collection interval.
COMPRESSION	The effectiveness of collector compression. If the value is low, you can increase the compression deadbands to pass fewer values and thus increase the effect of compression.
OUT OF ORDER	The total number of out-of-order samples for the collector.
TAG COUNT	The number of tags for which the collector collects data.
COMMENTS	The comments that you have entered for the collector.

i Tip:

- To access the details of a collector, select the row containing the collector instance. The details appear in the **DETAILS** section.
- You can show/hide/reorder columns in the table. For instructions, refer to [Common Tasks in Configuration Hub \(on page 906\)](#).

Access Offline Configuration Collectors

Offline Configuration Collectors are the instances of collectors whose destination is the cloud and display the configuration details as Offline Configuration.

Add Collector Instance: santhoshwin10

<ul style="list-style-type: none"> Collector Selection Simulation Collector Source Configuration santhoshwin10 Destination Configuration Predix Timeseries Collector Initiation 	CLIENT ID*	CLIENT SECRET*
	<i>Enter client ID</i>	<i>Enter secret</i>
	ZONE ID*	PROXY
	<i>Enter zone ID</i>	<i>Enter proxy</i>
	PROXY USERNAME	PROXY PASSWORD
	<i>Enter username</i>	<i>Enter password</i>
DATAPoint ATTRIBUTES (OPTIONAL) ⓘ		
ATTRIBUTE + Add Attributes		
CONFIGURATION DETAILS		
CHOOSE CONFIGURATION*		
<input type="radio"/> Historian Configuration <input checked="" type="radio"/> Offline Configuration		


1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, expand **Systems**, and then select the system whose collectors you want to access.
The system appears in the main section.
3. Right-click the system whose collectors you want to access (or select **☰**), and then select **Browse Collectors**.
This displays the list of Historian collectors and Offline configuration collectors. By default, the Historian collector instances added to the system appear, displaying the following information.



Tip:

- To access the details of a collector, select the row containing the collector instance. The details appear in the **DETAILS** section.
- You can show/hide/reorder columns in the table. For instructions, refer to [Common Tasks in Configuration Hub \(on page 906\)](#).

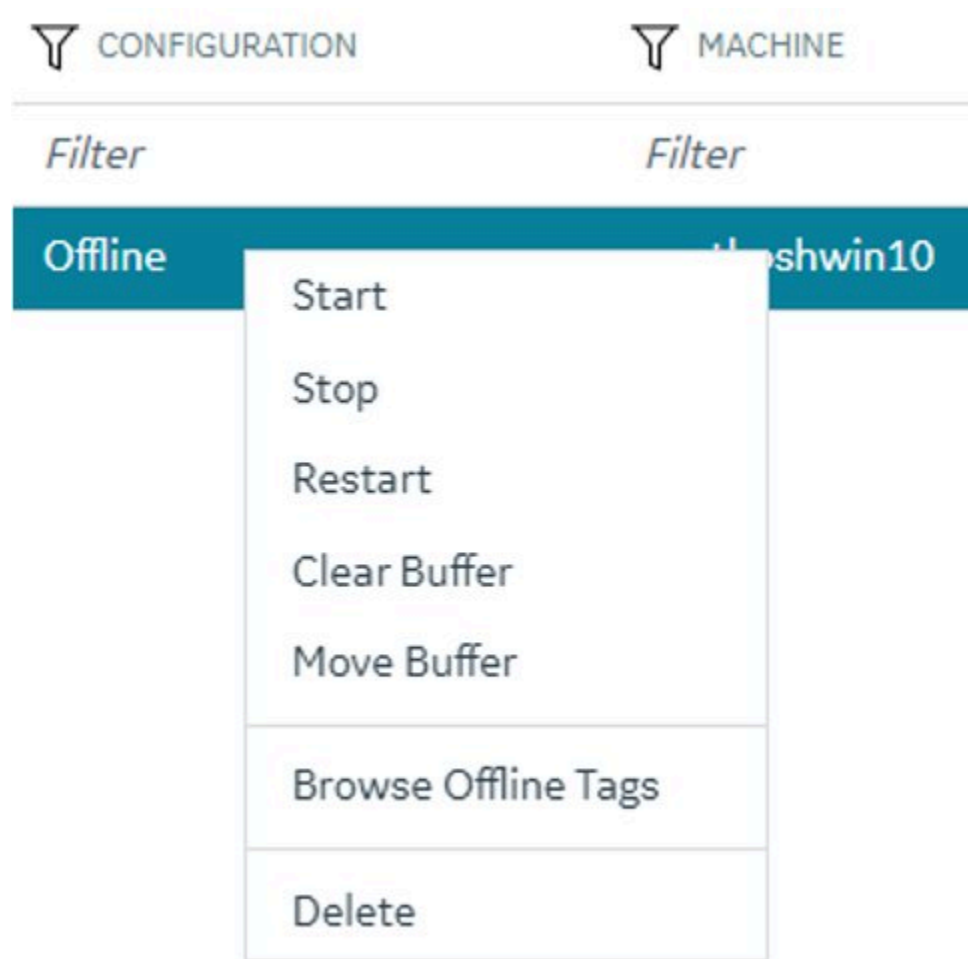
The Details panel for the Offline Configuration Collector Interface contains information regarding the instance configuration provided for the destination while installing software

 like Predix, MQTT, or Azure. For example, here is an example of the Details panel for the Offline Configuration Collector:

DETAILS ✕	
<input type="text" value="Search..."/>	
FIELD	VALUE
▾ INSTANCE CONFIGURATION	
Historian Server	SANTHOSHWIN10
Destination	Predix Timeseries
Cloud Destination Address	wss://gateway-predix-data-
Identity Issuer	https://9d4d55e0-14e1-4a4
Client ID	HistQA
Client Secret	
Zone ID	d459998a-656c-46c2-b525-
Proxy	http://PITC-Zscaler-America
Proxy Username	
Proxy Password	
Configuration	Offline
Configuration Historian S...	none

Manage Offline Configuration Collectors

Like other Historian collectors, Offline Configuration collectors can also be managed by selecting different options:




Refer to the following sections on how to use these options:

- [Start a Collector \(on page 1170\)](#)
- [Stop a Collector \(on page 1172\)](#)
- [Restart a Collector \(on page 1173\)](#)
- [Delete the Buffer Files of a Collector \(on page 1177\)](#)
- [Move the Buffer Files of the Collector \(on page 1179\)](#)
- [Delete a Collector Instance \(on page 1184\)](#)

Access the Tags in a System

This topic describes how to access all the tags in a system, regardless of whether they are added to a collector instance. You can also [access all the tags added to a collector instance \(on page 1164\)](#).

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, expand **Systems**, and then select the system whose tags you want to access.
3. Right-click the system whose tags you want to access (or select ) , and then select **Browse Tags**.

The tags added to the system appears, displaying the following information.

Column	Description
TAG NAME	The name of the tag.
DESCRIPTION	The description of the tag.
COLLECTOR NAME	The name of the collector instance to which you have added the tag.
LAST 10 VALUES	The last 10 values collected for the tag, plotted as a trend chart. If you pause over the chart, the minimum, maximum, first, and last values among the 10 values appear.
DATA COLLECTION	Indicates the status of the data collection.
TAG ALIAS	Indicates whether the tag contains aliases, which are created when you rename the tag using an alias (on page 1224) .



Tip:

You can show/hide/reorder columns in the table. For instructions, refer to [Common Tasks in Configuration Hub \(on page 906\)](#).

4. To narrow down your search results:

You can enter a name or a value partially or use the wildcard character asterisk (*).

 - a. Select **Search**.
 - b. Enter the search criteria, and then select **Apply**. You can add more search criteria by selecting **Add Attribute**.

The list of tags are filtered based on the search criteria. The search criteria that you have provided appear at the top of the page. You can remove any of the criteria as needed.

**Tip:**

To access the details of a tag, select the row containing the tag. The details appear in the **DETAILS** section.

Add a System

Install Historian on the machine that you want to add. If you want to create a stand-alone system, [install single-server Historian \(on page 880\)](#). If you want to create a horizontally scalable system, [install Historian primary server \(on page 880\)](#).

If you want to manage a Historian system using Configuration Hub, you must add it to Configuration Hub.

When you access Configuration Hub for the first time, a default Historian system is available. In a distributed environment, the primary server of this system is the machine whose Configuration Hub details you enter while installing Web-based Clients. This topic describes how to add another system.

**Note:**

Adding a Historian system is specific to the logged-in user.

1. [Access Configuration Hub \(on page 902\)](#)
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Systems**.
A list of systems appears in the main section.
3. Select **+**.
The **Add System** window appears.
4. Provide values as specified in the following table.

Field	Description
SYSTEM NAME	Enter a name for the Historian system. This name must be unique for a user.
HISTORIAN SERVER	Enter the host name or the IP address of the system that you want to add. This name must be unique for a user.
DESCRIPTION	Enter a description for the system.

Field	Description
Set as Default System	Select this check box if you want to set this system as the default one. If you do so, when you access Configuration Hub, this system appears by default. The default system varies with the user.

5. Select **Add**.

The Historian system is added, and it appears in the **Navigation** section.

- As needed, [add another data store \(on page 920\)](#).
- If you want to create a horizontally scalable system, the machine that you have added serves as the primary server. On the machines that you want to use as distributed servers, you must [install Historian distributed nodes \(on page 880\)](#) and then [add them to the system \(on page 913\)](#).

Add a Distributed/Mirror Server

1. [Install Historian server \(on page 880\)](#) on the machine that you want to add as a distributed server.
2. [Add a system \(on page 978\)](#). The server that you specify while adding the system serves as the primary server for the system.

If you want to create a horizontally scalable Historian system, you must first add a primary server, and then add one or more distributed/mirror machines to scale out the primary server horizontally and thus, improve performance.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Systems**.
A list of systems appears in the main section.
3. Expand the system in which you want to add a distributed/mirror server.
A list of servers in the system appears.
4. Select **+**.

System	Historian Server																														
Filter	Filter																														
<div style="border: 1px solid #0070c0; padding: 5px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> SERVERS + ⚙️ </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Machine Name</th> <th>STATUS</th> <th>Archive Compre...</th> <th>Write Cache Hit ...</th> <th>CONSUMPTION R...</th> <th>Read Thread Usa...</th> <th>Write Thread Us...</th> <th>Out Of</th> </tr> </thead> <tbody> <tr> <td>██████████</td> <td style="color: green;">✔ Connected</td> <td>43.3</td> <td>0.5</td> <td>0.45</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>██████████</td> <td style="color: red;">❌ Not Connected</td> <td>NA</td> <td>NA</td> <td>NA</td> <td>NA</td> <td>NA</td> <td>NA</td> </tr> </tbody> </table> </div>								Machine Name	STATUS	Archive Compre...	Write Cache Hit ...	CONSUMPTION R...	Read Thread Usa...	Write Thread Us...	Out Of	██████████	✔ Connected	43.3	0.5	0.45	0	0	0	██████████	❌ Not Connected	NA	NA	NA	NA	NA	NA
Machine Name	STATUS	Archive Compre...	Write Cache Hit ...	CONSUMPTION R...	Read Thread Usa...	Write Thread Us...	Out Of																								
██████████	✔ Connected	43.3	0.5	0.45	0	0	0																								
██████████	❌ Not Connected	NA	NA	NA	NA	NA	NA																								

The **Add Server Machine: <system name>** window appears.

5. Enter the host name or IP address of the machine that you want to add, and then select **Add**. The distributed server is added to the system. A distributed location is added in the server. You cannot modify or delete this location.

If you want high availability of one or more data stores in the server, [create a mirror location \(on page 918\)](#), and then [add the data stores \(on page 920\)](#). If not, [add the data store \(on page 920\)](#) to the distributed location.

Set Up a Mirror of Mirror

1. [Install Historian server \(on page 880\)](#) on each machine that you want to use in the mirror of mirror setup.
2. [Set up Configuration Hub \(on page 879\)](#) on each machine that you want to use in the mirror of mirror setup.
3. [Add a system \(on page 978\)](#). The server that you specify while adding the system serves as the primary server for the system.
4. [Create data stores \(on page 920\)](#) in the primary server in the public/IT network with the same name as the data stores in the primary server in your organization network.

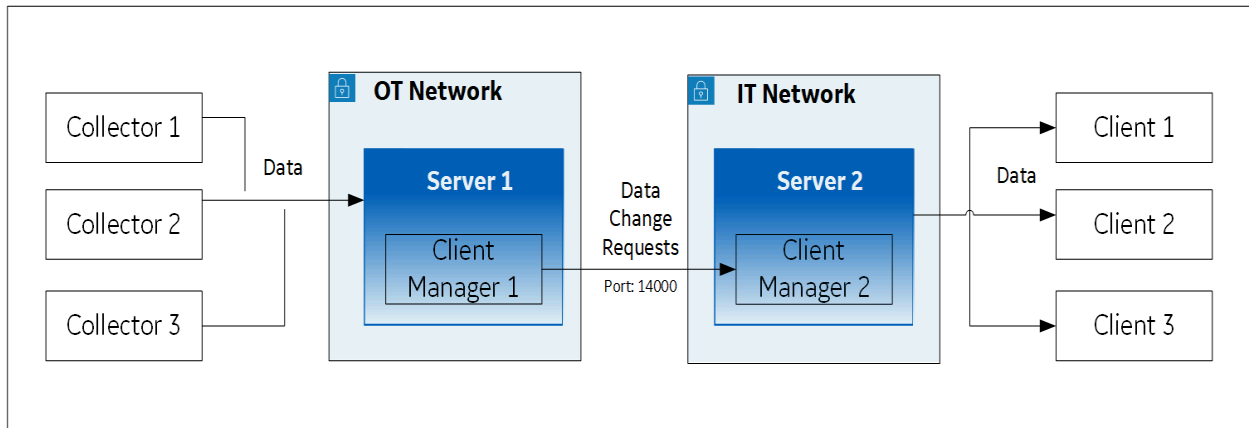
You can set up a mirror of the Historian server in a network different from that of your organization. When you do so, any tag/data update requests to the Historian server can be routed to the public and IT network instead of your organization's network.



Note:

For the Historian Enterprise Mirror Architecture, only "Time based" archives are supported.

Single-Node Setup: The following image shows two networks - OT and IT - with a Historian server installed in each network. These networks communicate using port 14000.



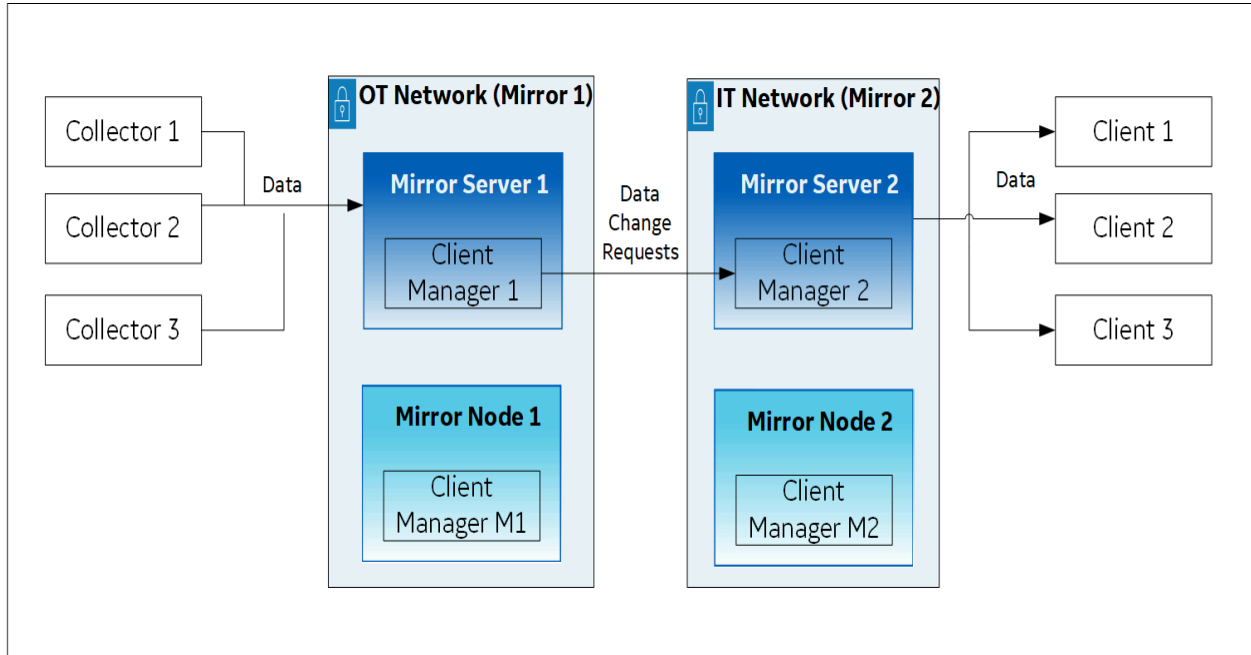
In this setup:

1. Server 1 is the primary server in the OT network; it stores data from collectors.
2. Server 2 is the primary server in the IT network; it is connected to clients.
3. When a tag/data is created, updated, or deleted, Client Manager 1 communicates the same with Client Manager 2 (installed with Server 2 in the IT network).
4. The change in the tag/data is replicated in Server 2 (that is, data is created, updated, or deleted accordingly).
5. The latest data is retrieved from Server 2 using the clients.

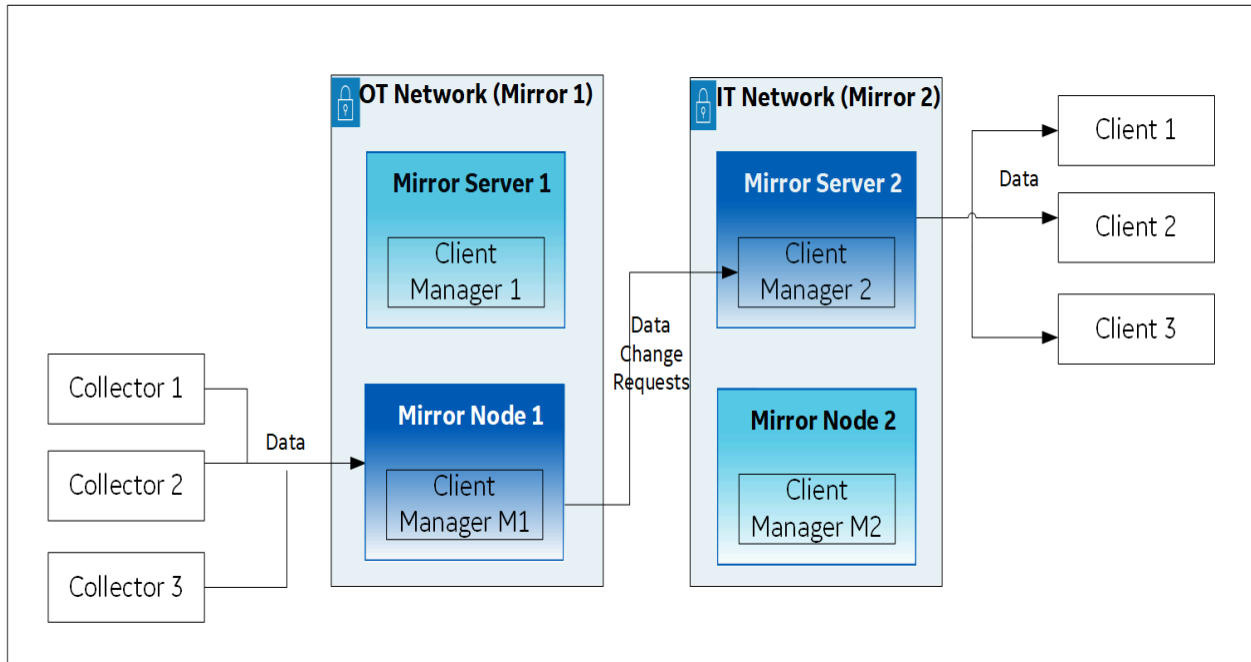
Mirror Setup: The following image shows two mirrors:

- Mirror 1 includes Mirror Server 1 and Mirror Node 1, which is a backup/standby node for Mirror Server 1; both these machines are in the OT network.
- Mirror 2 includes Mirror Server 2 and Mirror Node 2, which is a backup/standby node for Mirror Server 2; both these machines are in the IT network.

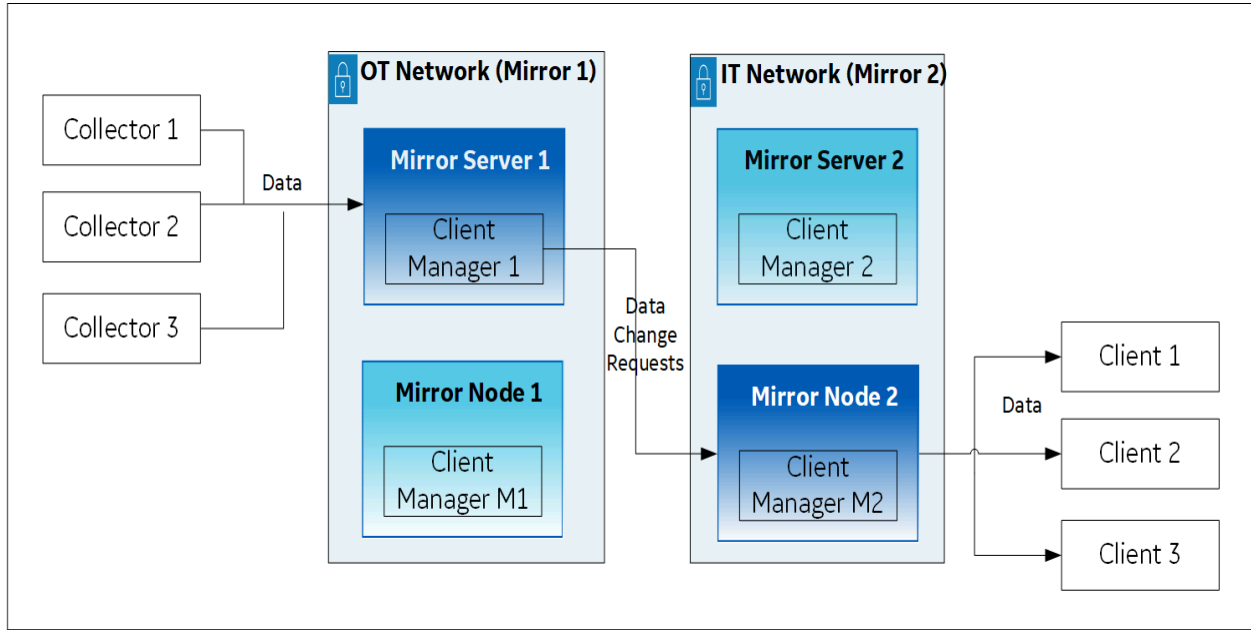
Client Manager 1 in Mirror Server 1 communicates with Client Manager 2 in Mirror Server 2.



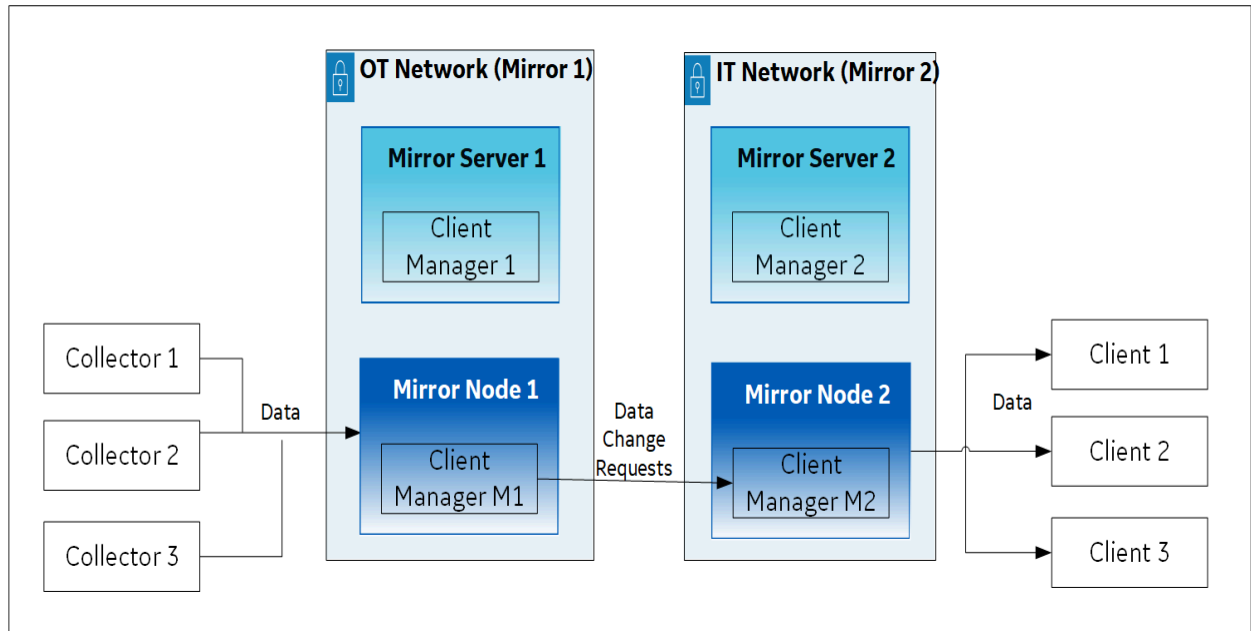
If Mirror Server 1 goes down, Client Manager M1 in Mirror Node 1 communicates with Client Manager 2 in Mirror Server 2.



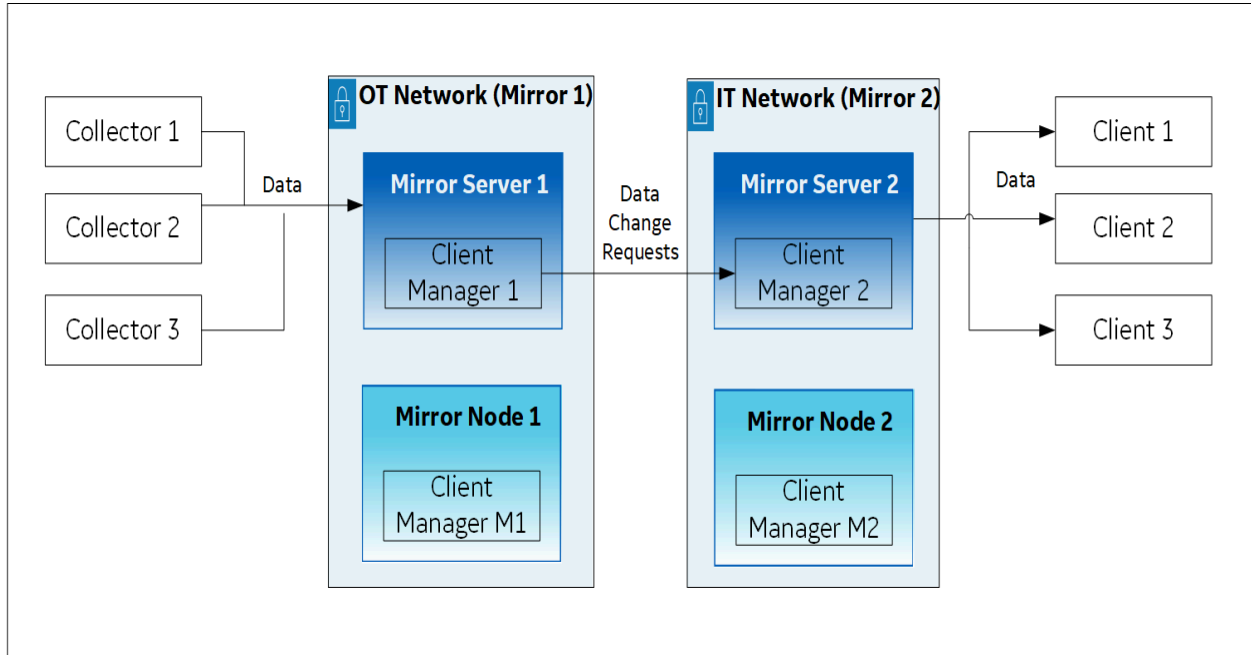
Similarly, if Mirror Server 2 goes down, Client Manager 1 in Mirror Server 1 communicates with Client Manager M2 in Mirror Node 2.



If both Mirror Server 1 and Mirror Server 2 are down, Client Managers M1 and M2 communicate with each other.



If Mirror Server 1 and/or Mirror Server 2 are available, the connection is re-established using these primary servers.



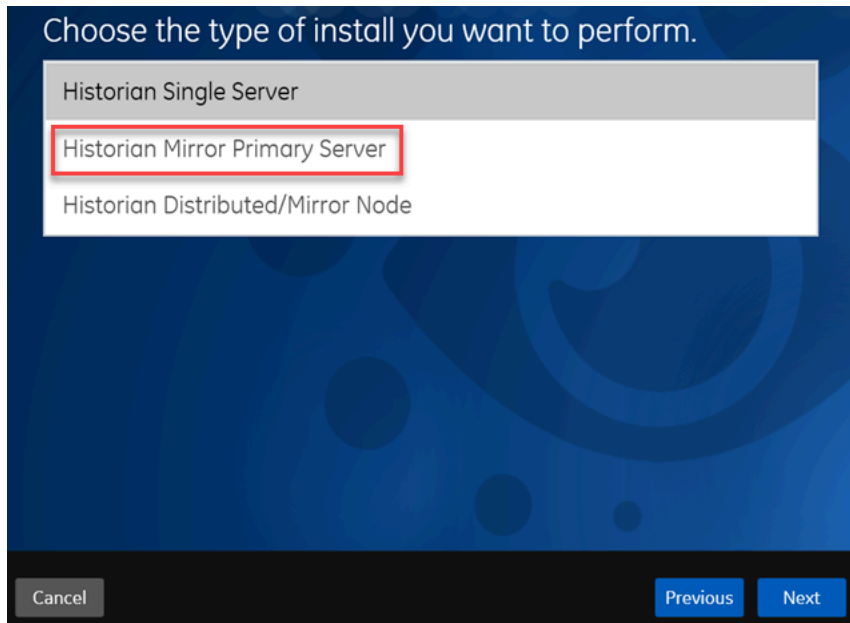
Thus, you can choose to always retrieve data from either Mirror Server 2 or Mirror Node 2. In addition, the store-and-forward functionality is available (in case Client Managers are not yet connected).

This topic describes how to set up a mirror of mirror for the configuration described in the preceding example. It includes the following high-level steps:

1. Installing the Historian server on all the machines
2. Setting up mirror 1
3. Setting up mirror 2
4. Setting up a mirror of mirror

Installing the Historian server

1. On the machines designated as the mirror primary servers (Mirror Server 1 and Mirror Server 2 in the example), [install the Historian server \(on page 880\)](#). During the installation, select **Historian Mirror Primary Server** on the **Choose the type of install you want to perform** page.



2. On the machines designated as mirror nodes (Mirror Node 1 and Mirror Node 2 in the example), [install the Historian server \(on page 880\)](#). During the installation, select **Historian Distributed/Mirror Node** on the **Choose the type of install you want to perform** page.

Set up Mirror 1:

3. On the mirror primary server in your organization's network (Mirror Server 1 in the example), [access Configuration Hub \(on page 902\)](#).
4. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Systems**.
A list of systems appears in the main section.
5. Expand Mirror Server 1.
A list of servers in the system appears.
6. Select **+**.

Machine Name	STATUS	Archive Compre...	Write Cache Hit ...	CONSUMPTION R...	Read Thread Usa...	Write Thread Us...	Out Of
[blurred]	Connected	43.3	0.5	0.45	0	0	0
[blurred]	Not Connected	NA	NA	NA	NA	NA	NA

The **Add Server Machine: <system name>** window appears.

- Enter the host name or IP address of the mirror node in your organization's network (Mirror Node 1 in the example), and then select **Add**.

The distributed server is added to the system. A distributed location is added in the server.

- Right-click Mirror Node 1, and then select **Browse Locations**.

Machine Name	Archive Compre...	Write Cache Hit R...	CONSUMPTION R...	Read Thread Usa...	Write Thread Usa...
torsc-collectorsclient	5,5	0.5	0.33	0	0
collectorsclien.6	4	NA	NA	NA	NA

A list of distributed locations in the system appears.

- Select **Mirror Locations**.

A list of mirror locations in the system appears.

- In the upper-right corner of the main section, select **+**.

The **Add Mirror Location** window appears.

- Provide values as described in the following table.

Field	Description
MIRROR LOCATION NAME	Enter a name for the mirror location. A value is required and must be unique for the system.
SERVER MACHINES	Select the servers that you want to add to the mirror group (Mirror Server 1 and Mirror Node 1 in this example). This box contains a list of all the servers in the system. You must add minimum two servers to a mirror location.

12. Select **Add**.

Mirror Node 1 is created.

13. Right-click the system name, and then select **Add Data Store**.

The **Add Data Store: Mirror Node 1** window appears.

14. Enter values as described in the following table.

Field	Description
DATA STORE NAME	Enter a unique name for the data store. A value is required. You can use all alphanumeric characters and special characters except / \ * ? < > You must provide the same name for the mirror setup in the IT network (mirror 2 in the example).
DESCRIPTION	Enter a description for the data store.
Set as default data store for the system	Select this check box if you want to set this data store as the default one. A default data store is the one that is considered if you do not specify a data store while adding a tag. You can set only one data store as default.

15. Select **Add**.

Mirror 1 is configured.

Set up Mirror 2:

16. On the mirror primary server in the IT network (Mirror Server 2 in the example), [access Configuration Hub \(on page 902\)](#).
17. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Systems**.
A list of systems appears in the main section.

18. Expand Mirror Server 2.

A list of servers in the system appears.

19. Select **+**.

Machine Name	STATUS	Archive Compre...	Write Cache Hit ...	CONSUMPTION R...	Read Thread Usa...	Write Thread Us...	Out Of
[blurred]	Connected	43.3	0.5	0.45	0	0	0
[blurred]	Not Connected	NA	NA	NA	NA	NA	NA

The **Add Server Machine: <system name>** window appears.

20. Enter the host name or IP address of the mirror node in your organization's network (Mirror Node 2 in the example), and then select **Add**.

The distributed server is added to the system. A distributed location is added in the server.

21. Right-click the system name, and then select **Browse Locations**.

Machine Name	STATUS	Archive Compre...	Write Cache Hit R...	CONSUMPTION R...	Read Thread Usa...	Write Thread Usa...
torsk-collectorsclient	Connected	5.5	0.5	0.33	0	0
collectorsclient6	Not Connected	NA	NA	NA	NA	NA

A list of distributed locations in the system appears.

22. Select **Mirror Locations**.

A list of mirror locations in the system appears.

23. In the upper-right corner of the main section, select **+**.

The **Add Mirror Location** window appears.

24. Provide values as described in the following table.

Field	Description
MIRROR LOCATION NAME	Enter a name for the mirror location. A value is required and must be unique for the system.
SERVER MACHINES	Select the servers that you want to add to the mirror group (Mirror Server 2 and Mirror Node 2 in this example). This box contains a list of all the servers in the system. You must add minimum two servers to a mirror location.

25. Select **Add**.

Mirror Node 2 is created.

26. Right-click Mirror Node 2, and then select **Add Data Store**.

The **Add Data Store: Mirror Node 2** window appears.

27. Enter values as described in the following table.

Field	Description
DATA STORE NAME	Provide the same name that you provided while setting up mirror 1.
DESCRIPTION	Enter a description for the data store.
Set as default data store for the system	Select this check box if you want to set this data store as the default one. A default data store is the one that is considered if you do not specify a data store while adding a tag. You can set only one data store as default.

28. Select **Add**.

Mirror 2 is configured.

Set up Mirror of Mirror:

29. Access Configuration Hub in the primary server in the OT network (Mirror Server 2).

30. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Systems**.

A list of systems appears in the main section.

31. Expand Mirror Server 1.

A list of servers in the system appears.

32. Select **+**.

The **Add Server Machine: <system name>** window appears.

33. Enter the host name or IP address of the mirror server in the IT network (Mirror Server 2 in the example), select the **Set as Mirror of Mirror** check box, and then select **Add**.

The distributed server is added to the system. A distributed location is added in the server.

34. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Systems**.

A list of systems appears in the main section.

35. Expand Mirror Server 1.

A list of servers in the system appears. In the example, Mirror Server 1, Mirror Node 1, and Mirror Server 2 appear.

A mirror of mirror is configured with one primary node and one mirror node each in the OT and IT networks. As needed, you can add more mirror nodes in each network.

Remove a Distributed/Mirror Server

- [Delete the data stores](#) in the machine (using the Web Admin console).
- If the machine is added to a mirror location, [remove it from the location](#).


You cannot delete the default server in a system.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Systems**.

A list of systems appear in the main section.

3. Expand the system from which you want to remove a distributed/mirror server.

A list of servers in the system appears.

4. In the row containing the server that you want to remove, select  , and then select **Delete Server**.

A message appears, asking you to confirm that you want to remove the distributed machine from the system.


5. Select **Delete**.

The machine is removed from the system.

Set a Default Location

A default location is a server in a system which is considered when you do not specify a location while [adding a data store \(on page 920\)](#). By default, the distributed location in the primary server is the default location. You can, however, set a different default location. The following conditions apply when you set a default location:

- You can have only one default location in a system.
- You cannot delete a default location.
- You can set any of the distributed/mirror locations as default.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Systems**.
A list of systems appears in the main section.
3. Select the system in which you want to set a default location.
The details of the system appear in the **DETAILS** section.
4. Expand **System Defaults**, and then next to **Default Location**, select .
The **Default Location: <system name>** window appears. The **Location** box contains a list of all the servers in the system.
5. Select the location that you want to set as default, and then select **Set as Default**.
The location is set as default.

Modify a Historian System


You can change the following details of a system:

- Name
- Description
- Default data store
- Default location (in case of a horizontally scalable system)

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, expand **Systems**, and then select the system that you want to modify.
The details of the system appear in the **DETAILS** section.
3. Modify values as specified in the following table.


Field	Description
Name	Enter a name for the Historian system. This value must be unique for a user.
Description	Enter a description for the system.

4. If you want to change the default data store:

- a. Under **System Defaults**, next to **Default Data Store**, select  .
The **Default Data Store: <system name>** window appears.
- b. Select the data store that you want to set as default, and then select **Set as Default**.

The default data store is changed.

5. If you want to change the default location:

- a. Under **System Defaults**, next to **Default Location**, select  .
The **Default Location: <system name>** window appears. The **Location** box contains a list of all the servers in the system.
- b. Select the location that you want to set as default, and then select **Set as Default**.

The changes to the system are saved automatically.

Configure Advanced Settings of a System

You can now configure a few advanced settings for the Archiver, Collector, and Data Store to achieve some specific functionality in Historian. You must be careful while modifying the configuration as this might impact the stability and security of the Historian System.

Ensure that you are a member of the iH Security Admins group.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Systems**.
A list of systems appears in the main section.
3. Right-click the system whose advanced settings you want to configure, and then select **Advanced Configuration**.
The advanced settings of the system appear, displaying the **Server** section by default.
4. Enter values as described in the following table.



Note:

If you have changed the values of any * marked fields, restart the Historian Data Archiver service. Only then will your changes be reflected.

Field	Description
ALARM TIMESTAMP CHECK	<p>Specify whether you want to speed up, slow down, or disable alarm timestamp checking:</p> <ul style="list-style-type: none"> ◦ 0 - Disabled: Select this option if you want to disable alarm timestamp checking. Only the data is sent to the alarm archiver. ◦ 1 - Fast: Select this option if you want to check the timestamp of the alarm data for the last 10 minutes. ◦ 2 - Slow: Select this option if you want to check the timestamp of the alarm data beyond the last 10 minutes.
ALLOW DATA OVERWRITES	Switch the toggle to enable or disable overwriting data.
ARCHIVER MEMORY SIZE	Enter the memory usage in MB that you want to allocate to an archive. If you enter 0, Data Archiver will dynamically allocate the memory usage. If Data Archiver is running on a 32-bit operating system, you can allocate upto 1800 MB. If Data Archiver is running on a 64-bit operating system, we recommend that you use the default value.
BUFER MEMORY MAX	Enter the maximum memory buffer size in MB that an archiver queue can use before switching to disk buffer.
COLLECTOR IDLE TIME (SECONDS)	Enter the number of seconds of no data collection after which a collector is considered idle.
DEBUG MODE	Specify whether you want to enable or disable the debug mode. If you enable this option, the debug information is included in the Historian log files, which helps you troubleshoot issues. However, this can result in large size of the log files.
DISABLE CA HOSTING	Enable CA Hosting to continue using the Client Access API based clients when you have converted a Mirror Primary to a standalone server while installing the Historian server.
DO NOT ZIP ARCHIVES	Switch the toggle to store the archive files as .zip files. This will help optimize the storage space of the archive files. However, if you are collecting alarm data as well, the alarm data may not be backed up. Also, you cannot export alarm data to another Data

Field	Description
	Archiver. Therefore, exercise caution while enabling this option if you are collecting alarm data as well.
FIREWALL PERMISSION	Use this parameter to disable port 14000 in the firewall. By default, Historian installation enables port 14000 in the firewall.
MAINTAIN AUTO RECOVERY FILE	Switch the toggle if you want to back up the archive and configuration files (.iha and .ihc files) every hour. This will prevent data loss. However, these files are used by Historian internally. Also, exercise caution in enabling this option because it can impact Historian performance.
MAX QUERY TIME (SECONDS)	Enter the maximum time in seconds that a query can take to process. After this time limit exceeds, the query is terminated.
MAXIMUM QUERY INTERVALS	Enter the maximum number of samples per tag that Historian can return from a query on non-raw data. You can use this setting to limit the number of query results on non-raw data.
NUMBER OF READ THREADS	Enter the number of read threads to use parallel reading of data. The minimum number you can enter is 8.
NUMBER OF WRITE THREADS	Enter the number of write threads to use parallel writing of data.
USE ADSI CALLS	Switch the toggle to allow Data Archiver to use Active Directory Service Interfaces (ADSI) calls.

5. Select **Save**.
6. Expand **Collector**, and then select the collector whose settings you want to configure.
The fields specific to the selected collector appear.
7. Enter values as described in the following table.

Field	Description
BUFFER FLUSH MULTIPLIER	<p>Select the multiplier to the buffer flow speed while using the store-and-forward feature:</p> <ul style="list-style-type: none"> ◦ 0: Select this option if you want to disable throttling. ◦ 1: Select this option if you want normal speed. ◦ 2: Select this option if you want the collector to never send data faster than twice the normal speed.

Field	Description
NUM INTERVALS FLUSH	Specify how quickly you want the collector to send data to Data Archiver. The value you enter in this field is multiplied by 100 milliseconds. For example, if you enter 5, the collector sends data to Data Archiver every 500 milliseconds. We recommend that you enter 5.

8. Select **Save**.

A message appears, asking you whether you want to save and restart the collector as well.

9. If you want to save your changes and restart the collector as well, select **Save and Restart**. If you want to just save your changes, select **Save**. In that case, you must restart the collector later for the changes to reflect.

Your changes are saved. If you have selected **Save and Restart**, the collector is restarted.

10. Expand **Datastore**, and then, select the data store whose settings you want to configure.

The fields specific to the selected data store appear,

11. Enter values as described in the following table.

Field	Description
ALLOW FUTURE DATA	Switch the toggle to enable storing future data .
CREATE OFFLINE ARCHIVES	Switch the toggle to create offline archives. This is to avoid receiving an outside-active-hours error. It happens if you attempt to store data when the current archive file is set to read-only.

12. Select **Save**.

The advanced settings are configured for the data store.

Configure Labels of Spare Fields

For each tag, a set of five spare fields are available, which are named Spare 1 to Spare 5. You can use these fields to enter values for any tag details apart from those captured in the tag fields (for example, the name, location, and phone number of the manufacturer of a device).

This topic describes how to change the label of these spare fields at the system level. The changes are then cascaded to all the tags in the system.

You can configure any or all of these fields. The new labels of the fields then appear under **SPARE FIELDS** in the **DETAILS** section when you access a tag.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, expand **Systems**, and then select the system that you want to modify.
The details of the system appear in the **DETAILS** section.
3. Right-click the system whose spare fields you want to configure (or select **☰**), and then select **Configure Spare Fields Labels**.
The **Configure Spare Fields Labels: <system name>** window appears.
4. Enter values in the available fields, and then select **Save**.
For example, if you want to capture the name, location, and phone number of the manufacturer of a device, enter Name, Location, and Phone Number in the **SPARE FIELD 1 LABEL**, **SPARE FIELD 2 LABEL**, and **SPARE FIELD 3 LABEL** fields.
The labels of the spare fields are configured. When you access a tag, the new labels appear under **SPARE FIELDS** in the **DETAILS** section.



Note:

The labels that you have configured only appear in Configuration Hub. For other applications, such as Historian Administrator, Trend Client, and so on, Spare 1 to Spare 5 are displayed. The values of spare fields can be configured for tags.

Set a Default System

If you set a system as default, when you log in to Configuration Hub, this system appears by default. The following conditions apply when you set a system as default:

- You can have only one default system in Configuration Hub.
- You cannot delete a default system.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Systems**.
A list of systems appears in the main section.
3. Right-click the system that you want to set as default (or select **☰**), and then select **Set as Default System**.
The system is set as default.

Delete a Historian System

You can delete a Historian system if you no longer want to manage it using Configuration Hub. You cannot, however, delete a system if it is set as default.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Systems**.
A list of systems appears in the main section.
3. Right-click the system that you want to delete (or select **☰**), and then select **Delete**.
A message appears, asking if you want to delete the system.
4. Select **Delete**.
The system is deleted.

Managing Mirror Locations

Create a Mirror Location

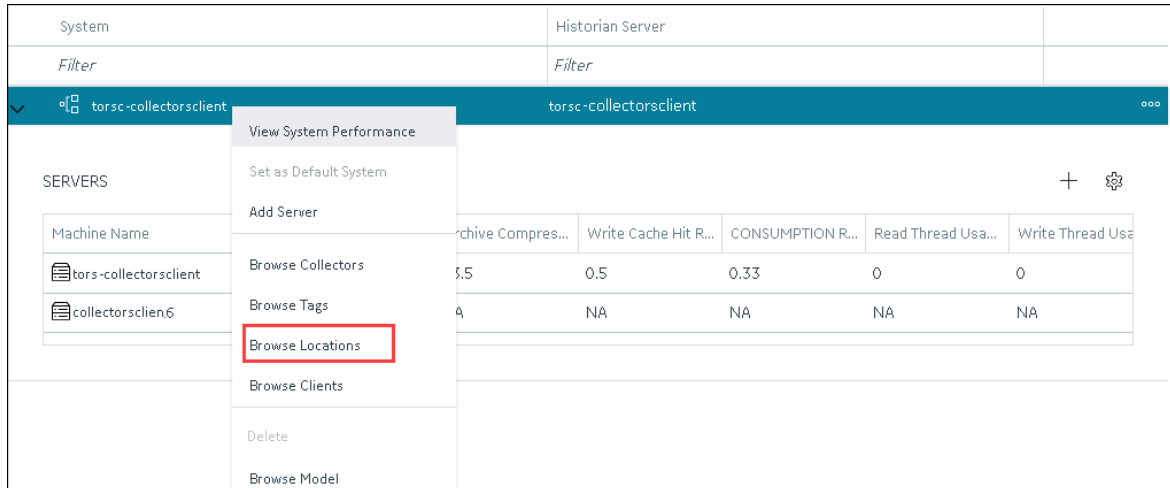
[Add one or more distributed servers \(on page 913\)](#) to the system in which you want to create a mirror group.

If you want high availability of one or more data stores, you must create a mirror group (also called a mirror location), and then add servers to it. When you do so, the data in the data stores of the mirror locations is replicated. Therefore, even if one of the servers is down, you can retrieve data from the other servers in the mirror location, thus achieving high availability.

The following conditions apply when you create a mirror location:

- You must add minimum two servers to a mirror location. The maximum number of servers that you can add depends on your Historian license.
- You can add a mirror location only in a horizontally scalable Historian system.
- You can rename a mirror location, remove a machine from a mirror location, or add an additional one even after you create the mirror location. However, if only one machine remains in the group, you cannot remove it.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Systems**.
The **Systems** section appears, displaying a list of systems.
3. Right-click the system in which you want to create a mirror location (or select **☰**), and then select **Browse Locations**.



A list of distributed locations in the system appears.

4. Select **Mirror Locations**.

A list of mirror locations in the system appears.

5. In the upper-right corner of the main section, select **+**.

The **Add Mirror Location** window appears.

6. Provide values as described in the following table.

Field	Description
MIRROR LOCATION NAME	Enter a name for the mirror location. A value is required and must be unique for the system.
SERVER MACHINES	Select the servers that you want to add to the mirror group. This box contains a list of all the servers in the system. You must add minimum two servers to a mirror location.

7. Select **Add**.

The mirror location is created.

[Add a data store to the mirror location \(on page 920\).](#)

Rename a Mirror Location

1. [Access Configuration Hub \(on page 902\).](#)

2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Systems**.

The **Systems** section appears, displaying a list of systems.

- Right-click the system in which you want to rename a mirror location (or select **☰**), and then select **Browse Locations**.

The screenshot displays the Configuration Hub interface. At the top, there are fields for 'System' (Historian Server) and 'Filter'. Below this is a header for 'torsk-collectorsclient' with a menu icon (☰) on the right. A left sidebar titled 'SERVERS' contains a table with columns for 'Machine Name' and two server entries: 'torsk-collectorsclient' and 'collectorsclient.6'. A context menu is open over the 'torsk-collectorsclient' system, listing options: 'View System Performance', 'Set as Default System', 'Add Server', 'Browse Collectors', 'Browse Tags', 'Browse Locations' (highlighted with a red box), 'Browse Clients', 'Delete', and 'Browse Model'. The background shows a performance table with columns: 'Archive Compres...', 'Write Cache Hit R...', 'CONSUMPTION R...', 'Read Thread Usa...', and 'Write Thread Usa...'. The table contains two rows of data.

Machine Name	Archive Compres...	Write Cache Hit R...	CONSUMPTION R...	Read Thread Usa...	Write Thread Usa...
torsk-collectorsclient	5.5	0.5	0.33	0	0
collectorsclient.6	4	NA	NA	NA	NA

A list of distributed locations in the system appears.

- Select **Mirror Locations**.

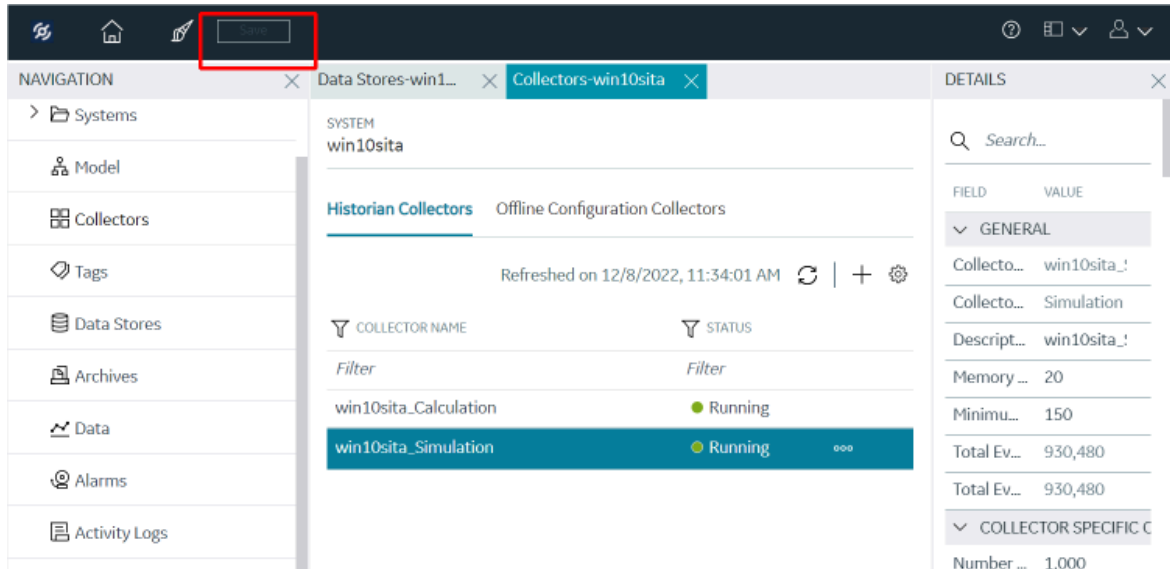
A list of mirror locations in the system appears.

- Select the location that you want to rename.

The details of the mirror location appear in the **Details** section.

- In the **Name** field, enter the new name of the mirror location.

- In the upper-left corner of the page, select **Save**.



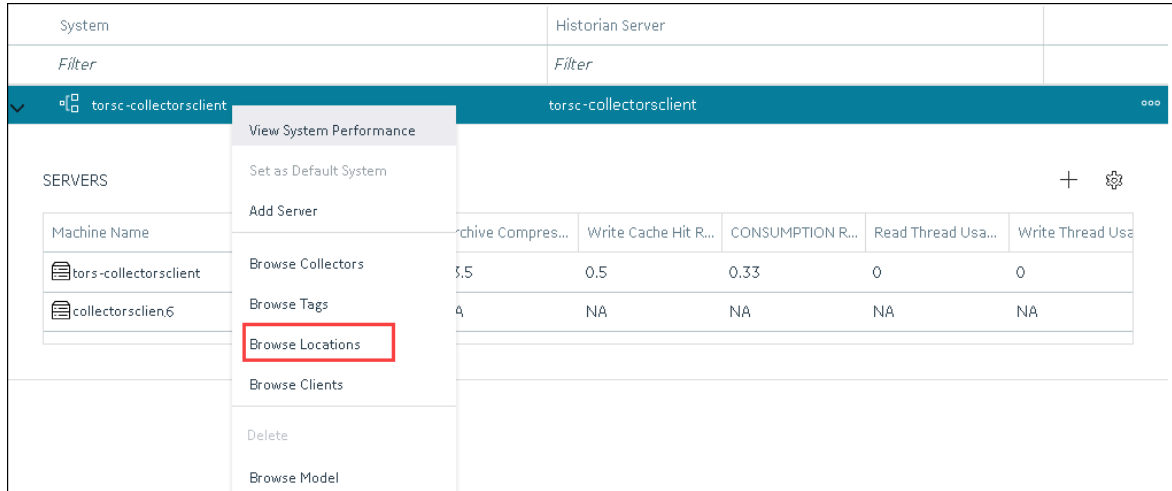
The mirror location is renamed.

Add a Machine to a Mirror Location

If you want to add machine to a mirror location that already contains machines, and if you want to copy the archive and configuration information from the existing machines to the new machine, perform the following steps:

1. Copy the archive files and configuration files from an existing machine in the mirror location to the one that you have added.
 2. Rename the configuration file <machine name>_Config.ihc.
1. [Access Configuration Hub \(on page 902\)](#).
 2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Systems**. The **Systems** section appears, displaying a list of systems.

- Right-click the system to which you want to add a machine (or select **☰**), and then select **Browse Locations**.



A list of distributed locations in the system appears.

- Select **Mirror Locations**.

A list of mirror locations in the system appears.

- Right-click the mirror location in which you want to add a machine (or select **☰**), and then select **Add Server Machine**.

The **Add Machine: <mirror location>** window appears. The **SERVER MACHINES** field contains a list of machines in the system that are not yet added to the mirror location.

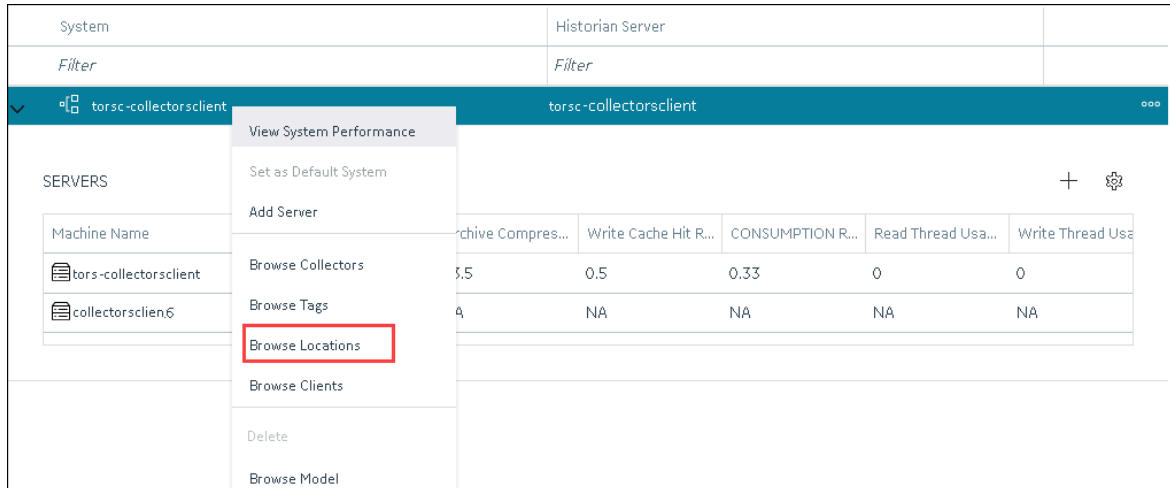
- In the **SERVER MACHINES** field, select the machine that you want to add to the mirror location, and then select **Add**.

The machine is added to the mirror location.

Remove a Machine from a Mirror Location

If a mirror location contains only one machine, you cannot remove it.

- [Access Configuration Hub \(on page 902\)](#).
- In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Systems**.
The **Systems** section appears, displaying a list of systems.
- Right-click the system from which you want to remove a machine (or select **☰**), and then select **Browse Locations**.



A list of distributed locations in the system appears.

4. Select **Mirror Locations**.

A list of mirror locations in the system appears.

5. Right-click the mirror location from which you want to remove a machine (or select **...**), and then select **Remove Server Machine**.

The **Remove Server Machine: <mirror location>** window appears, displaying a list of machines in the mirror location.

6. Select the machine that you want to remove, and then select **Remove**.

A message appears, asking you to confirm that you want to remove the machine from the mirror location.

7. Select **Remove**.

The machine is removed from the mirror location.

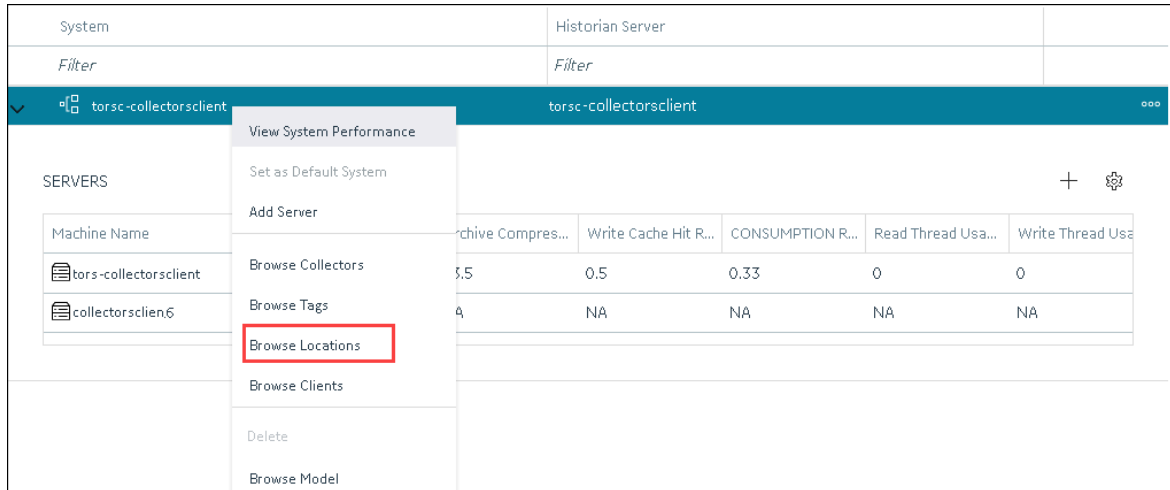
Delete a Mirror Location

Delete all the data stores in the mirror location; you cannot delete a mirror location if it contains a data store.

1. [Access Configuration Hub \(on page 902\)](#).

2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Systems**.
The **Systems** section appears, displaying a list of systems.

3. Right-click the system in which you want to delete a mirror location (or select **...**), and then select **Browse Locations**.



A list of distributed locations in the system appears.

4. Select **Mirror Locations**.

A list of mirror locations in the system appears.

5. Right-click the mirror location that you want to delete (or select **☰**), and then select **Delete Mirror Location**.

A message appears, asking you to confirm that you want to delete the mirror location.

6. Select **Delete**.

The mirror location is deleted.

Managing Data Stores

About Data Stores

A data store is a logical collection of tags. It is used to store, organize, and manage tags according to the data source and storage requirements. A data store can have multiple archive files (*.IHA), and includes both logical and physical storage definitions.

Tags can be segregated into separate archives through the use of data stores. The primary use of data stores is to segregate tags by data collection intervals. For example, you can put a name plate or static tags where the value rarely changes into one data store, and your process tags into another data store. This can improve query performance.

Historian data stores are stored as archive files that contain data gathered from all data sources during a specific period of time. You can write and read data from the archive files.

You can define two types of data stores:

- **Historical Data Store:** Tags stored under historical data store will store data as long as the disk space is available. Depending on your license, you may be able to create multiple historical data stores. The maximum number of historical data stores supported depends on the license.
- **SCADA Buffer Data Store:** Tags stored under the SCADA buffer data store will store data for a specific duration of time based on license.

When you install the Historian server, two historical data stores are installed by default.

- **System:** Stores Historian messages and performance tags. This is only for internal usage within Historian, and you cannot add tags to this data store. You cannot rename or delete the system data store.
- **User:** Stores tag data. This is a default data store. You can rename and delete a user data store as long as there is another default data store set for tag addition.

Based on your license, a SCADA Buffer data store may also be installed. It stores short-term tags and data.

Create a Data Store

The number of data stores that you can create depends on your license.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Datstores**. Alternatively, you can select **Systems**, right-click the system in which you want to create a data store (or select **☰**), and then select **Browse Data Stores**.
The **Data Stores** section appears.
3. Select **+**.
If Historian Standard version, then the **Add Data Store** window appears.

If Historian Enterprise version, then the **Add Data Store: <location name>** window appears.
4. Enter values as described in the following table.

Field	Description
DATA STORE NAME	Enter a unique name for the data store. A value is required. You can use all alphanumeric characters and special characters except / \ * ? < >
DESCRIPTION	Enter a description for the data store.

Field	Description
LOCATION	Enter the host name or IP address of the distributed location on which you want to create the data store. This field is available only for a horizontally scalable system.
Is Default	Switch the toggle on if you want to set this data store as the default one. A default data store is the one that is considered if you do not specify a data store while adding a tag. You can set only one data store as default.

5. Select .

The data store is created.

When you add tags to the data store, it will have its own set of .IHA (iHistorian Archive) files. Ensure that you back up the new data store archives periodically.

Access a Data Store


1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Datstores**. Alternatively, you can select **Systems**, right-click the system in which the data store is available (or select ), and then select **Browse Data Stores**. The **Data Stores** section appears.
3. Select the data store that you want to access. The **DETAILS** section displays the following details of the data store.

Table 23. General

Field	Description
Data Store Name	The name of the data store. A value is required and must be unique for the system.
Description	The description of the data store.
State	The current state of the data store: <ul style="list-style-type: none"> ◦ Running: Indicates that the data store is actively storing data. ◦ (whether it is running). This field is disabled.

Field	Description
Location	The host name or IP address of the distributed location on which the data store has been created. This field is available only for a horizontally scalable system. It is disabled.
Storage Type	<p>The storage type of the data store, which can be one of the following values:</p> <ul style="list-style-type: none"> ◦ Historical: Tags stored in a historical data store will store data as long as disk space is available. The maximum number of Historical data stores supported depends on the license. ◦ SCADA Buffer: Tags stored under SCADA buffer data store will store data for a specific duration of time based on license. <p>This field is disabled.</p>
System Default Storage	Indicates whether the data store is a default one. If yes, while creating a tag, this data store will be used by default.
Number of Tags	The number of tags in the data store. For instructions on how to add a tag, refer to Add Tags for the Data Store Using Configuration Hub (on page 909) and Add a Tag Manually (on page 1018) .

Table 24. Archive Creation

Field	Description
Automatically Create Archives	Indicates whether you want to create an archive automatically (on page 1245) after the current one is full. An archive file is considered full based on the size or duration you specify in the Create Archive By and the Archive Duration or Default Size fields.
Overwrite Old Archives	<p>Indicates whether you want to overwrite an old archive file when a new one is created.</p> <p>If you enable this option, the oldest archived data is replaced with the latest one when the latest archive default size is reached. Since this action deletes historical data, exercise caution in using this feature. Be sure that you have a backup of the</p>

Field	Description
	archive so that you can restore it later. Best practice is to create an additional archive to prevent premature loss of data due to overwriting. For example, if you want to save 12 months of data into 12 archives, create 13 archives.
Create Archive By	<p>Indicates whether you want to create a new archive automatically after the current one reaches a specific size or after a specific duration. This field is enabled only if you switch the Automatically Create Archives toggle on.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> ◦ Size: Select this option if you want to create a new archive when the current one reaches a specific size. Specify the size in the Default Size (MB) field (which appears only if you select Size). ◦ Days or Hours: Select one of these options if you want to create a new archive after a specific duration. Specify the duration in the Archive Duration field (which appears only if you select Days or Hours).
Default Size (MB)	The default size of an archive after which a new one will be automatically created if you switch the Automatically Create Archives toggle on. The Default Size (MB) field appears only if you select Size in the Create Archive By field.
Archive Duration	The duration after which a new archive will be automatically created if you switch the Automatically Create Archives toggle on. The Archive Duration field appears only if you select Days or Hours in the Create Archive By field.

Table 25. Maintenance

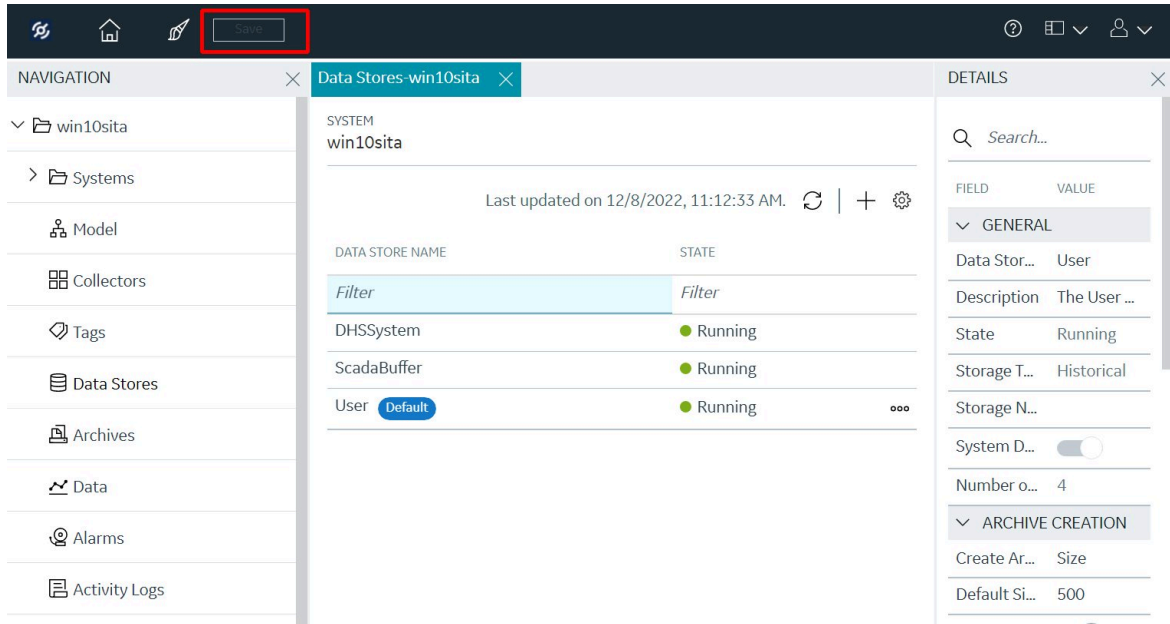
Field	Description
Default Archive Path	The default folder in which you want to create archives.
Default Backup Path	The default folder in which you want to place the backup archives.
Base Archive Name	A prefix that you want to add to all the archive files.

Field	Description
Free Space Required (MB)	<p>Indicates the remaining disk space required after a new archive is created. If the available space is less than the requirement, a new archive is not created. The default value is 5000 MB.</p> <p>This field is not applicable to alarms and events archives. The alarms and events archiver will continue writing to the alarms and events archive until the drive is full. If this occurs, the alarms and events archiver will buffer incoming alarms and events data until the drive has free space. An error message is logged in the Historian message log.</p>
Store OPC Quality	Indicates whether OPC data quality is stored.
Use Caching	Indicates whether caching is enabled. When reading data from the archiver, some data is saved in the system memory and retrieved using caching. This results in faster retrieval as the data is already stored in the buffer.

Table 26. Security

Field	Description
Data is Read-Only After (Hours)	The number of hours for data to be stored in a read/write archive. After the time lapses, that portion of the archive file is automatically made read-only. Incoming data values with time-stamps prior to this time are rejected. A single archive file, therefore, may have a portion made read-only, another portion that is read/write containing recently written data, and another that is unused free space.
Generate Message on Data Update	Indicates whether an audit log entry will be made any time the value of a previously archived data point is overwritten. This log entry will contain both the original and new values.

4. As needed, modify values in the available fields.
5. In the upper-left corner of the page, select **Save**.



The data store is modified.

Rename a Data Store

You cannot rename the system data store. You can rename a user data store as long as there is another default data store set for tag addition.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Datastores**. Alternatively, you can select **Systems**, right-click the system in which the data store is available (or select **...**), and then select **Browse Data Stores**. The **Data Stores** section appears.
3. Select the data store that you want to access. The details section displays the following details of the data store.

Table 27. General

Field	Description
Data Store Name	The name of the data store. A value is required and must be unique for the system.
Description	The description of the data store.
State	The current state of the data store (whether it is running). This field is disabled.

Field	Description
Location	The host name or IP address of the distributed location on which the data store has been created. This field is available only for a horizontally scalable system. It is disabled.
Storage Type	<p>The storage type of the data store, which can be one of the following values:</p> <ul style="list-style-type: none"> ◦ Historical: Tags stored in a historical data store will store data as long as disk space is available. The maximum number of Historical data stores supported depends on the license. ◦ SCADA Buffer: Tags stored under SCADA buffer data store will store data for a specific duration of time based on license. <p>This field is disabled.</p>
System Default Storage	Indicates whether the data store is a default one. If yes, while creating a tag, this data store will be used by default.
Number of Tags	The number of tags in the data store. For instructions on how to add a tag, refer to Add Tags for the Data Store Using Configuration Hub (on page 909) and Add a Tag Manually (on page 1018) .

Table 28. Archive Creation

Field	Description
Automatically Create Archives	Indicates whether you want to create a new archive (on page 1241) automatically after the current one is full. An archive file is considered full based on the size or duration you specify in the Create Archive By and the Archive Duration or Default Size fields.
Overwrite Old Archives	<p>Indicates whether you want to overwrite an old archive file when a new one is created.</p> <p>If you enable this option, the oldest archived data is replaced with the latest one when the latest archive default size is reached. Since this action deletes historical data, exercise caution in using this feature. Be sure that you have a backup of the</p>

Field	Description
	archive so that you can restore it later. Best practice is to create an additional archive to prevent premature loss of data due to overwriting. For example, if you want to save 12 months of data into 12 archives, create 13 archives.
Create Archive By	<p>Indicates whether you want to create a new archive automatically after the current one reaches a specific size or after a specific duration. This field is enabled only if you switch the Automatically Create Archives toggle on.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> ◦ Size: Select this option if you want to create a new archive when the current one reaches a specific size. Specify the size in the Default Size (MB) field (which appears only if you select Size). ◦ Days or Hours: Select one of these options if you want to create a new archive after a specific duration. Specify the duration in the Archive Duration field (which appears only if you select Days or Hours).
Default Size (MB)	The default size of an archive after which a new one will be automatically created if you switch the Automatically Create Archives toggle on. The Default Size (MB) field appears only if you select Size in the Create Archive By field.
Archive Duration	The duration after which a new archive will be automatically created if you switch the Automatically Create Archives toggle on. The Archive Duration field appears only if you select Days or Hours in the Create Archive By field.

Table 29. Maintenance

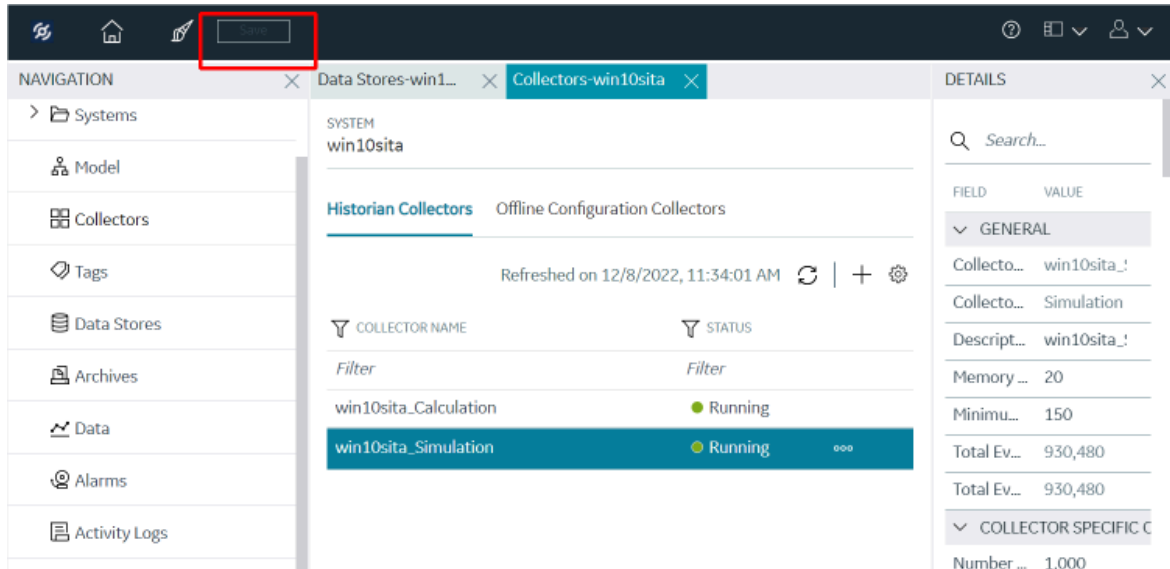
Field	Description
Default Archive Path	The default folder in which you want to create archives.
Default Backup Path	The default folder in which you want to place the backup archives.
Base Archive Name	A prefix that you want to add to all the archive files.

Field	Description
Free Space Required (MB)	<p>Indicates the remaining disk space required after a new archive is created. If the available space is less than the requirement, a new archive is not created. The default value is 5000 MB.</p> <p>This field is not applicable to alarms and events archives. The alarms and events archiver will continue writing to the alarms and events archive until the drive is full. If this occurs, the alarms and events archiver will buffer incoming alarms and events data until the drive has free space. An error message is logged in the Historian message log.</p>
Store OPC Quality	Indicates whether OPC data quality is stored.
Use Caching	Indicates whether caching is enabled. When reading data from the archiver, some data is saved in the system memory and retrieved using caching. This results in faster retrieval as the data is already stored in the buffer.

Table 30. Security

Field	Description
Data is Read-Only After (Hours)	The number of hours for data to be stored in a read/write archive. After the time lapses, that portion of the archive file is automatically made read-only. Incoming data values with time-stamps prior to this time are rejected. A single archive file, therefore, may have a portion made read-only, another portion that is read/write containing recently written data, and another that is unused free space.
Generate Message on Data Update	Indicates whether an audit log entry will be made any time the value of a previously archived data point is overwritten. This log entry will contain both the original and new values.


4. As needed, modify values in the available fields.
5. In the upper-left corner of the page, select **Save**.



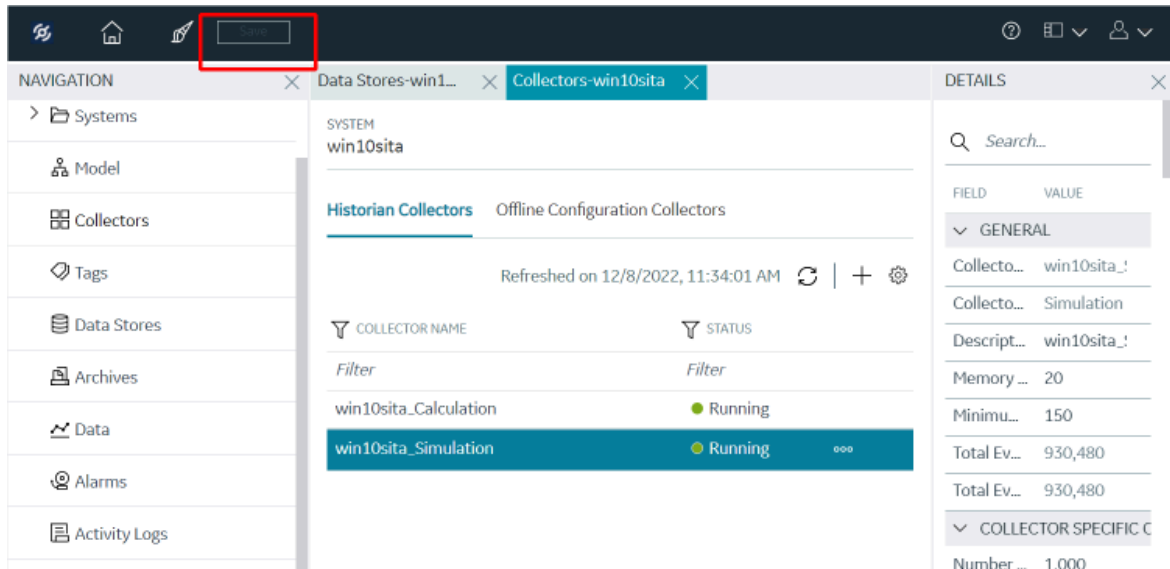
The data store is modified.

Set a Default Data Store

A default data store is the one that is considered if you do not specify a data store while adding a tag.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Datstores**.
Alternatively, you can select **Systems**, right-click the system in which the data store is available (or select **☰**), and then select **Browse Data Stores**.
3. Select the system whose default data store you want to change.
The details of the system appear in the **DETAILS** section.
4. Under **System Defaults**, next to **Default Data Store**, select  .
The **Default Data Store: <data store name>** window appears, displaying a list of data stores in the system.

5. Select the data store that you want to set as default, and then select **Set as Default**.
6. In the upper-left corner of the page, select **Save**.



The data store is set as default.

Access the Archives in a Data Store

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Datstores**.
Alternatively, you can select **Systems**, right-click the system in which the data store is available (or select **☰**), and then select **Browse Data Stores**.
The **Data Stores** section appears.
3. Right-click the data store whose archives you want to access (or select **☰**), and then select **Browse Archives**.
The archives in the data store appear, indicating the current one and the old ones.

Access the Activity Logs of a Data Store

Activity logs are generated when activities are performed on tags and collectors in a data store.

Examples:

- When a tag is created, modified, or deleted
- When a collector instance is created, modified, or deleted
- When data collection for a tag or a collector begins or ends
- When an archive is created or will be closed soon

You can access these logs for each tag/collector or for all the tags and collectors in a system. You can filter these logs based on the start and end dates, priority, topics, and the content in the logs. You can also export all the logs or selected ones.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Datastores**.
Alternatively, you can select **Systems**, right-click the system in which the data store is available (or select **☰**), and then select **Browse Data Stores**.
The **Data Stores** section appears.
3. Right-click the data store whose archives you want to access (or select **☰**), and then select **Browse Activity Logs**.
The activity logs of the data store appear. You can filter on the Start Time and End Time along with other fields to search for activity log.

Access the Tags in a Data Store

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Datastores**.
Alternatively, you can select **Systems**, right-click the system in which the data store is available (or select **☰**), and then select **Browse Data Stores**.
The **Data Stores** section appears.
3. Right-click the data store whose tags you want to access (or select **☰**), and then select **Browse Tags**.
The tags in the data store appear, indicating the current status of the data collection for each tag.

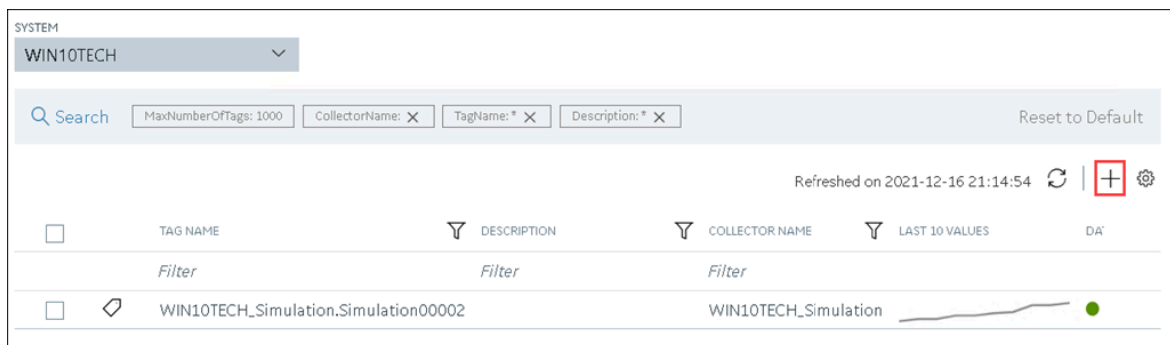
Add Tags for the Data Store Using Configuration Hub

- Add the collector instance (on page 909) using which you want to collect data. Ensure that the collector is running.
- By default, the tag data is stored in the user data store, which is created automatically when you set up Configuration Hub. If, however, you want to store the data in a different data store, create it (on page 920).

This topic describes how to specify the tags for which you want to collect data by browsing through the tags in the data source. For example, for an iFIX collector, if there are 1,00,000 tags in the iFIX server, you must specify the ones for which you want to collect data. Only then data is collected for those tags.

In addition to adding tags from the data source, you can create tags manually (on page 1018).

1. Access Configuration Hub (on page 902).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Tags**.
3. Select **+**.



The **Add Tag-<system name>** page appears. The **Add Tags from Collector** option is selected by default.

4. Enter values as described in the following table.

Field	Description
COLLECTOR NAME	Select the collector instance that you want to use to collect data. A value is required.
COLLECTED TYPE	Specify whether you want to browse through all the tags in the data source or only from the tags that you have not added yet. A value is required.

Field	Description
SOURCE TAG NAME	Enter the name of the tag (either completely or partially) to narrow down the search results.
SOURCE TAG DESCRIPTION	Enter the description of the tag (either completely or partially) to narrow down the search results.

5. Select **Search Tags**.

A list of tags that match *all* the criteria that you have specified appears. If a tag is already added, it is disabled.

6. Select the check box corresponding to each tag for which you want to collect data.

Add Tags from Collector
 Add Manually

COLLECTOR NAME*
WIN10TECH_Simulation

COLLECTED TYPE*
All Source Tags

SOURCE TAG NAME
*

SOURCE TAG DESCRIPTION
*

SEARCH RESULTS FOR SOURCE TAGS NAMES

	TAG NAME	DESCRIPTION
	<i>Filter</i>	<i>Filter</i>
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00001	WIN10TECH_Simulation.Simulation00001
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00002	WIN10TECH_Simulation.Simulation00002
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00003	WIN10TECH_Simulation.Simulation00003
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00004	WIN10TECH_Simulation.Simulation00004
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00005	WIN10TECH_Simulation.Simulation00005
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00006	WIN10TECH_Simulation.Simulation00006
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00007	WIN10TECH_Simulation.Simulation00007
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00008	WIN10TECH_Simulation.Simulation00008
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00009	WIN10TECH_Simulation.Simulation00009
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00010	WIN10TECH_Simulation.Simulation00010
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00011	WIN10TECH_Simulation.Simulation00011
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00012	WIN10TECH_Simulation.Simulation00012

DATASTORE*
User

7. In the **DATA STORE** field, if you want to store the data in a different data store than the user data store, select the same.

8. Select **Add Tag**.

Data collection begins for the selected tags.

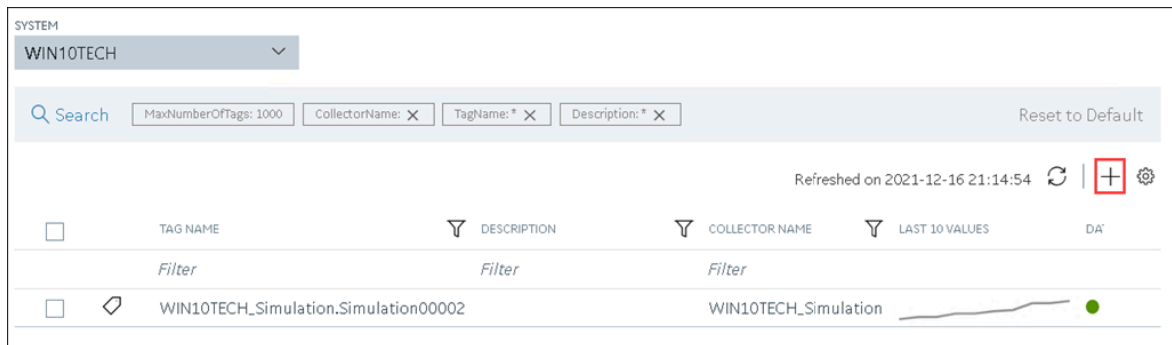
As needed, configure each tag by providing values for the tag properties. For information on the delta query modes, refer to [Counter Delta Queries](#).

Add a Tag Manually

- [Add the collector instance \(on page 909\)](#) using which you want to collect data.
- By default, the tag data is stored in the user data store, which is created automatically when you set up Configuration Hub. If, however, you want to store the data in a different data store, [create it \(on page 920\)](#).

After you create a collector instance, you [specify which tags from the source must be used for data collection \(on page 909\)](#). In addition, if you want to use the same tag twice (say, with a different collection interval or collector compression settings), you can add the tag manually. You can also create a calculation tag or a tag to store the values imported using the Excel Add-in.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Tags**.
3. Select **+**.



The **Add Tag-<system name>** page appears. The **Add Tags from Collector** option is selected by default.


4. Select **Add Manually**.

Add Tags from Collector
 Add Manually

COLLECTOR NAME* COLLECTED TYPE* SOURCE TAG NAME SOURCE TAG DESCRIPTION
Select.. ▼ All Source Tags ▼ * *

Search Tags

SEARCH RESULTS FOR SOURCE TAGS NAMES




Click on 'Search Tags' to view results

DATASTORE*

5. Enter values as described in the following table.

Field	Description
COLLECTOR NAME	Select the collector instance that you want to use to collect data. If, however, this tag is not associated with a collector, you can leave the field blank (for example, you want to ingest this data manually instead of using a collector).
SOURCE ADDRESS	Specify the source tag to which you want to map the one you are creating. This field is enabled only if you select a value in the COLLECTOR NAME field. When you select □□□ , the Browse Source Tag: <collector name> window appears. Provide the search criteria to find the tag that you want to map.
TAG NAME	<p>Enter a name for the tag. A value is required and must be unique for the Historian server.</p> <p>The value that you enter:</p> <ul style="list-style-type: none"> ◦ Must begin with a letter or a number. ◦ Can contain up to 256 characters.

Field	Description
	<ul style="list-style-type: none"> ◦ Can include any of the following special characters: /!#{}%\$-_ ◦ Must not include a space or any of the following characters: ~`+^;,:?*"={}@
DATA TYPE	<p>Select the data type of the tag data. To find out the data types supported by a collector, refer to the documentation on the collector that you have created.</p> <div style="border: 1px solid #ffc107; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Important: If you select an unsupported data type, you may receive incorrect data or even lose data.</p> </div> <p>If you select Multi-Field, the USER-DEFINED TYPE NAME field appears, and the ENUMERATED SET and ARRAY TAG fields are disabled.</p> <p>If you select Fixed String, the STRING LENGTH field appears.</p>
STRING LENGTH	<p>Enter the maximum character length allowed for the tag data. This field appears only if the value in the DATA TYPE field is Fixed String. A value is required.</p> <p>You can enter a value between 1 and 255. The default value is 8.</p>
USER-DEFINED TYPE NAME	<p>Select the user-defined data type (UDT) (<i>on page 1238</i>) that you want to assign to the tag. This field appears only if the value in the DATA TYPE field is Multi-Field. A value is required.</p>
ENUMERATED SET	<p>Select the enumerated set (<i>on page 1234</i>) that you want to assign to the tag. This field is not applicable for string and multi-field data types (enumerated sets) and for array tags.</p>
ARRAY TAG	<p>Switch the toggle to indicate whether the tag stores an array of data. This field is disabled if you select a value in the ENUMERATED SET field or if the value in the DATA TYPE field is Multi-Field.</p> <p>For information on array tags, refer to About Array Tags (<i>on page 1190</i>).</p>

Field	Description
TIME RESOLUTION	Select the time resolution for the tag. A value is required. For example, if you select Seconds , when you plot the data on a trend chart, the timestamp of the data points will be one second apart.
DATA STORE	If you want to store the data in a different data store than the user data store, select the same.

6. Select **Add Tag**.

Data collection begins for the selected tags.

As needed, configure each tag by providing values for the tag properties.

View the Performance of a Data Store

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Datstores**.
Alternatively, you can select **Systems**, right-click the system in which the data store is available (or select **☰**), and then select **Browse Data Stores**.
The **Data Stores** section appears.
3. Right-click the data store whose performance you want to access (or select **☰**), and then select **View Data Store Performance**.
The performance of the data store appears, displaying the following information.

Field	Description
ARCHIVE COMPRESSION	The current effect of archive data compression. If the value is zero, it indicates that archive compression is either ineffective or disabled. To increase the effect of data compression, increase the value of archive compression deadbands on individual tags. In calculating the effect of archive compression, Historian counts internal system tags as well as data source tags. Therefore, when working with a very small number of tags and with compression disabled on data source tags, this field may indicate a value other than zero. If you use a realistic number of tags, however, system tags will constitute a very small percent-

Field	Description
	age of total tags and will therefore not cause a significant error in calculating the effect of archive compression on the total system.
WRITE CACHE HIT	The hit ratio of the write cache in percentage of total writes. It is a measure of how efficiently the system is collecting data. Typically, this value should range from 95 to 99.99%. If the data is changing rapidly over a wide range, however, the hit percentage drops significantly because current values differ from recently cached values. More regular sampling may increase the hit percentage. Out-of-order data also reduces the hit ratio.
RECEIVE RATE	Indicates how busy the server is at a given instance and the rate at which the server is receiving data from collectors.
FREE SPACE	Indicates how much disk space (in MB) is left in the current archive.
CONSUMPTION RATE	Indicates how fast the archive disk space is consumed. If the value is too high, you can reduce it by slowing the poll rate on selected tags or data points or by increasing the filtering on the data (widening the compression deadband to increase compression).
EST. DAYS TO FULL	<p>Indicates how much time is left before the archive is full, based on the current consumption rate. This value is dynamically calculated by the server and becomes more accurate as an archive file gets closer to completion. This value is only an estimate and will vary based on a number of factors, including the current compression effectiveness. The system sends messages notifying you at 5, 3, and 1 days until full. After the archive is full, a new archive must be created (can be automatic or manual).</p> <p>To increase this value, you must reduce the consumption rate. To ensure that collection is not interrupted, make sure that the Automatically Create Archives option is enabled.</p> <p>You may also want to enable the Overwrite Old Archives option if you have limited disk capacity. Enabling this option, however, means that some old data will be lost when new data overwrites</p>

Field	Description
	the data in the oldest online archive. Use this feature only when necessary.
FAILED WRITES	<p>Indicates the number of samples that failed to be written. Since failed writes are a measure of system malfunctions or an indication of offline archive problems, this value should be zero. If you observe a non-zero value, investigate the cause of the problem and take corrective action.</p> <p>Historian also generates a message if a write fails. Note that the message only appears once per tag, for a succession of failed writes associated with that tag. For example, if the number displayed in this field is 20, but they all pertain to one Historian tag, you will only receive one message until that Historian tag is functional again.</p>
ALERTS SINCE STARTUP	Indicates a count of system warnings or alerts generated since the last startup. A high value here may indicate a problem of some kind. You should review the alerts and determine the probable cause. The count resets to zero on restart. The message database, however, may contain more alerts than this value.
MESSAGE SINCE STARTUP	Displays a count of system messages generated since the last startup. The system resets the value to zero on restart. The message database, however, may contain more messages than this value.

Delete a Data Store

The following conditions apply when deleting a data store:

- You cannot delete the system data store.
- You cannot delete a data store if it contains tags. If you remove the tags from the system or permanently delete them, you can delete the data store. However, the archives are not deleted.
- You cannot delete the default data store. You can delete a user data store as long as there is another default data store set for tag addition.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Datstores**.

The **Data Stores** section appears.

3. Right-click the data store that you want to delete (or select **⋮**), and then select **Delete**.

A message appears, asking you to confirm that you want to delete the data store.

4. Select **Delete**.

The data store is deleted. However, the archives in the data store are not deleted.

Adding a Collector Instance

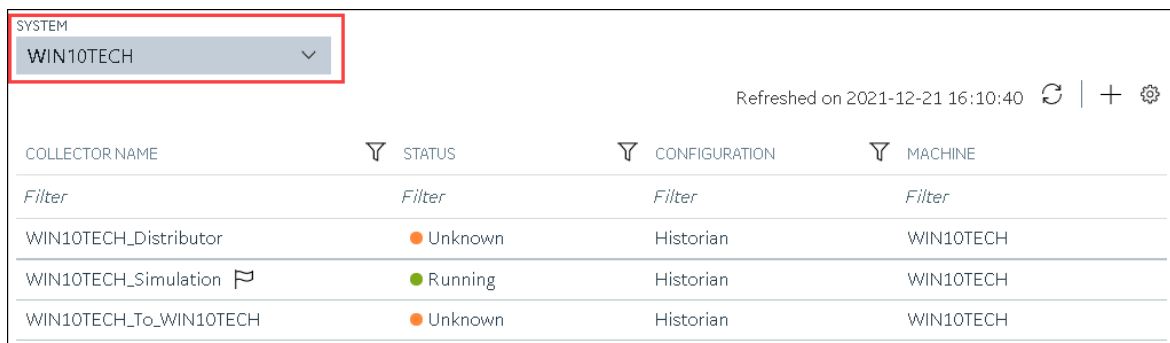
Add and Configure a Calculation Collector

Using the Calculation collector, you can perform data calculations on values already in the archiver. It retrieves data from tags in the Historian archive, performs the calculation, and then stores the resulting values into new archive tags.

You can create a Calculation collector only for an on-premises Historian server, not for a cloud destination.

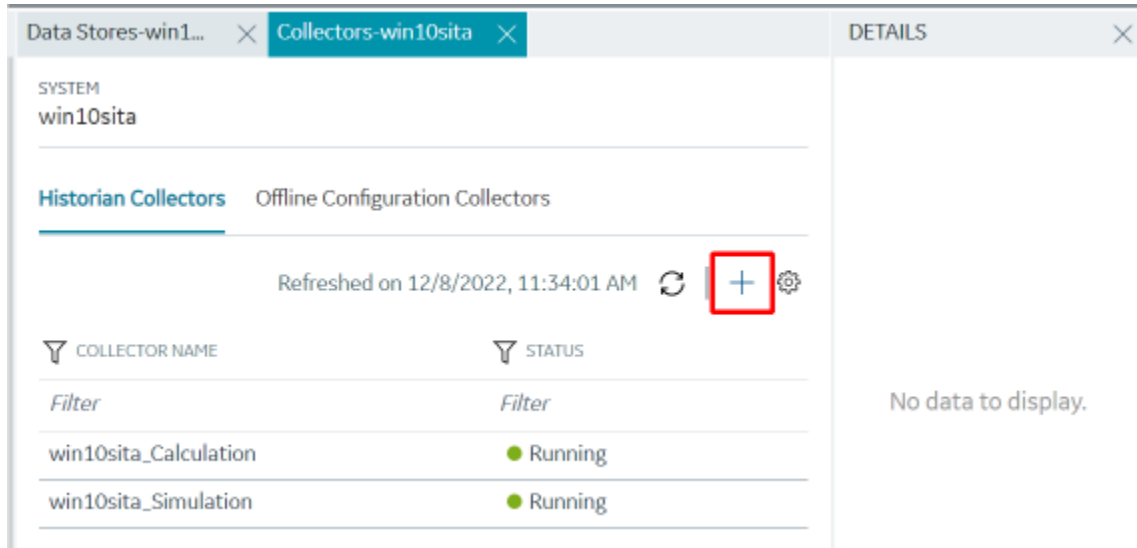
This topic describes how to add a collector instance using Configuration Hub. You can also [add a collector instance using the RemoteCollectorConfigurator utility](#), which does not require you to install Web-based Clients.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.
A list of collectors in the default system appears.
3. If needed, select the system in which you want to add a collector instance.



COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

4. In the upper-right corner of the main section, select **+**.



The **Add Collector Instance: <system name>** window appears, displaying the **Collector Selection** section. The **MACHINE NAME** field contains a list of machines on which you have installed collectors.

5. In the **MACHINE NAME** field, select the machine in which you want to add a collector instance.
6. In the **COLLECTOR TYPE** field, select **Calculation Collector**, and then select **Get Details**.

The **INSTALLATION DRIVE** and **DATA DIRECTORY** fields are disabled and populated.

7. Select **Next**.

The **Source Configuration** section appears. The **HISTORIAN SERVER** field is disabled and populated.

8. Select **Next**.

The **Destination Configuration** section appears. Under **CHOOSE DESTINATION**, the **Historian Server** option is selected by default; the other options are disabled. In addition, the **DESTINATION HISTORIAN SERVER** field is disabled and populated with the value you selected in the **MACHINE NAME** field in the **Collector Selection** section.

9. In the **USERNAME** and **PASSWORD** fields, enter the credentials to access the destination Historian server. Values are required only for a remote Historian server.

10. Select **Next**.

The **Collector Initiation** section appears.

11. If needed, modify the value in the **COLLECTOR NAME** field.

The value that you enter:

- Must be unique.
 - Must not exceed 15 characters.
 - Must not contain a space.
 - Must not contain special characters except a hyphen, period, and an underscore.
12. In the **RUNNING MODE** field, select one of the following options.
- **Service - Local System Account:** Select this option if you want to run the collector as a Windows service using the credentials of the local user (that is, the currently logged-in user). If you select this option, the **USERNAME** and **PASSWORD** fields are disabled.
 - **Service Under Specific User Account:** Select this option if you want to run the collector as a Windows service using a specific user account. If you select this option, you must enter values in the **USERNAME** and **PASSWORD** fields. If you have enabled the **Enforce Strict Collector Authentication** option in Historian Administrator, you must provide the credentials of a user who is added to at least one of the following security groups:
 - iH Security Admins
 - iH Collector Admins
 - iH Tag Admins

You can also configure the collector to start automatically when you start the computer.

13. Select **Add**.

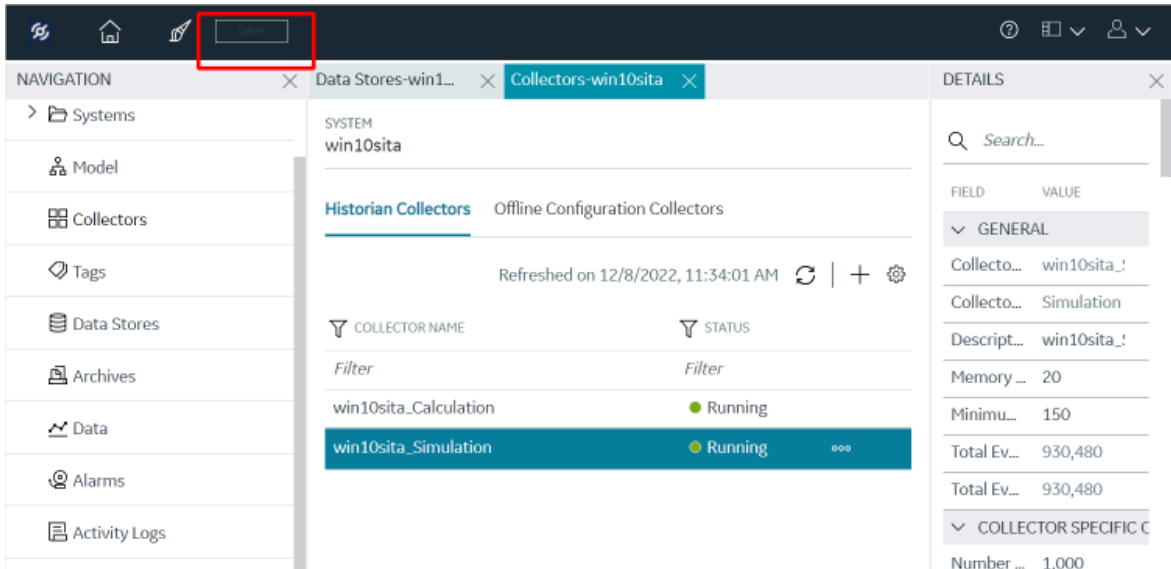
The collector instance is added. The fields specific to the collector section appear in the **DETAILS** section.

14. Under **Collector-Specific Configuration**, enter values as described in the following table.

Field	Description
Calculation Timeout (sec)	The maximum time a calculation must be performed before being terminated. The default value is 10 seconds. If the calculation takes longer, it is cancelled, and a bad data quality sample is stored in the destination tag with a subquality, calculation error.
Max Recovery Time (hr)	The maximum time, in hours till now, that the collector will attempt to restore data. This is applicable only to event-based tags. The default value is 4 hours. If you want to disable automatic calculation of the tag, set the value of this field to 0.

15. If needed, enter values in [the other sections \(on page 1114\)](#).

16. In the upper-left corner of the page, select **Save**.



The changes to the collector instance are saved.

17. If needed, restart the collector.

Specify the tags ([on page 909](#)) whose data you want to collect using the collector.

Add and Configure a CygNet Collector

A CygNet collector collects data from a CygNet server and stores it in the Historian server. For more information, refer to the [Overview of the CygNet Collector](#).



Note:

You cannot send data to a cloud destination using a CygNet collector.

This topic describes how to add a collector instance using Configuration Hub. You can also [add a collector instance using the RemoteCollectorConfigurator utility](#), which does not require you to install Web-based Clients.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.
A list of collectors in the default system appears.
3. If needed, select the system in which you want to add a collector instance.

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

4. In the upper-right corner of the main section, select **+**.

COLLECTOR NAME	STATUS
<i>Filter</i>	<i>Filter</i>
win10sita_Calculation	Running
win10sita_Simulation	Running

The **Add Collector Instance: <system name>** window appears, displaying the **Collector Selection** section. The **MACHINE NAME** field contains a list of machines on which you have installed collectors.

5. In the **MACHINE NAME** field, select the machine in which you want to add a collector instance.
6. In the **COLLECTOR TYPE** field, select **Cygnnet Collector**, and then select **Get Details**.

The **INSTALLATION DRIVE** and **DATA DIRECTORY** fields are disabled and populated.

7. Select **Next**.

The **Source Configuration** section appears.

8. In the **SERVER SITE** field, enter the host name or IP address of the CygNET server from which you want to collect data.

9. Select **Next**.

The **Destination Configuration** section appears. Under **CHOOSE DESTINATION**, the **Historian Server** option is selected by default; the other options are disabled.

10. In the **USERNAME** and **PASSWORD** fields, enter the credentials to access the destination Historian server. Values are required only for a remote Historian server.

11. Select **Next**.

The **Collector Initiation** section appears. The **COLLECTOR NAME** field is populated with a value in the following format: `<Historian server name>_Cygnet`

12. If needed, modify the value in the **COLLECTOR NAME** field.

The value that you enter:

- Must be unique.
- Must contain the string `Cygnet`.
- Must not exceed 15 characters.
- Must not contain a space.
- Must not contain special characters except a hyphen, period, and an underscore.

13. In the **RUNNING MODE** field, select one of the following options.

- **Service - Local System Account:** Select this option if you want to run the collector as a Windows service using the credentials of the local user (that is, the currently logged-in user). By default, this option is selected, and the **USERNAME** and **PASSWORD** fields are disabled.
- **Service Under Specific User Account:** Select this option if you want to run the collector as a Windows service using a specific user account. If you select this option, you must enter values in the **USERNAME** and **PASSWORD** fields.

If you have enabled the **Enforce Strict Collector Authentication** option in Historian Administrator, you must provide the credentials of a user who is added to at least one of the following security groups:


- iH Security Admins
- iH Collector Admins
- iH Tag Admins

You can also configure the collector to start automatically when you start the computer.

14. Select **Add**.

The collector instance is added. The fields specific to the collector section appear in the **DETAILS** section.

15. Under **Collector-Specific Configuration**, enter values as described in the following table.

Field	Description
Recovery Time	<p>The maximum time, in hours, for which the collector will attempt to recover data after the collector is started or when connection between the collector and the CygNet server is re-established. This time is calculated as the duration between the current time and the last known write time.</p> <p>Continuous data collection is resumed only after the previous data has been recovered.</p> <p>By default, this value is set to 0, which means data recovery is not attempted. The maximum value you can provide is 168 hours (that is, 7 days).</p>
Thread Count	<p>The maximum number of threads that you want collector to use to query data from the CygNet server.</p>
CygNet Debug Mode	<p>The debug mode for the collector. You can enter a value between 0 and 255, where 0 turns off debugging and 255 enables detailed debugging (with query transactions).</p> <div data-bbox="386 1041 1414 1262" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Do not turn on debugging for a long period. If you do so, very large log files are created, which can consume a great deal of disk space. We recommend a maximum of 10 minutes.</p> </div>
General Optimized	<p>Indicates whether you want to apply optimization on the tag data reads.</p>
Service-Site	<p>Identifies the CygNet site or data source from which the CygNet collector collects data. A value is required.</p>

16. If needed, enter values in [the other sections \(on page 1114\)](#).

17. In the upper-left corner of the page, select **Save**.

The changes to the collector instance are saved.

18. If needed, restart the collector.

Specify the tags ([on page 909](#)) whose data you want to collect using the collector.

Add and Configure a File Collector

A File collector is used to send data from one Historian server to another one.



Note:

- You cannot send data to a cloud destination using the File collector.
- You can create only one instance of the File collector.

For more information, refer to [Overview of the File Collector](#).

This topic describes how to add a collector instance using Configuration Hub. You can also [add a collector instance using the RemoteCollectorConfigurator utility](#), which does not require you to install Web-based Clients.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.
A list of collectors in the default system appears.
3. If needed, select the system in which you want to add a collector instance.

SYSTEM			
WIN10TECH			
Refreshed on 2021-12-21 16:10:40			
COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

4. In the upper-right corner of the main section, select **+**.

SYSTEM	
win10sita	
Historian Collectors Offline Configuration Collectors	
Refreshed on 12/8/2022, 11:34:01 AM	
COLLECTOR NAME	STATUS
<i>Filter</i>	<i>Filter</i>
win10sita_Calculation	Running
win10sita_Simulation	Running

No data to display.

The **Add Collector Instance: <system name>** window appears, displaying the **Collector Selection** section. The **MACHINE NAME** field contains a list of machines on which you have installed collectors.

5. In the **MACHINE NAME** field, select the machine in which you want to add a collector instance. The collector will send data to this machine.
6. In the **COLLECTOR TYPE** field, select **File Collector**, and then select **Get Details**.
The **INSTALLATION DRIVE** and **DATA DIRECTORY** fields are disabled and populated.
7. Select **Next**.

The **Destination Configuration** section appears. Under **CHOOSE DESTINATION**, the **Historian Server** option is selected by default; the other options are disabled.

8. In the **USERNAME** and **PASSWORD** fields, enter the credentials to access the destination Historian server. Values are required only for a remote Historian server.
9. Select **Next**.

The **Collector Initiation** section appears. The **COLLECTOR NAME** field is populated with a value in the following format: *<Historian server name>_File*

10. If needed, modify the value in the **COLLECTOR NAME** field.

The value that you enter:

- Must be unique.
 - Must not exceed 15 characters.
 - Must not contain a space.
 - Must not contain special characters except a hyphen, period, and an underscore.
11. In the **RUNNING MODE** field, select one of the following options.
 - **Service - Local System Account:** Select this option if you want to run the collector as a Windows service using the credentials of the local user (that is, the currently logged-in user). By default, this option is selected, and the **USERNAME** and **PASSWORD** fields are disabled.
 - **Service Under Specific User Account:** Select this option if you want to run the collector as a Windows service using a specific user account. If you select this option, you must enter values in the **USERNAME** and **PASSWORD** fields. If you have enabled the **Enforce Strict Collector Authentication** option in Historian Administrator, you must provide the credentials of a user who is added to at least one of the following security groups:
 - iH Security Admins
 - iH Collector Admins
 - iH Tag Admins

You can also configure the collector to start automatically when you start the computer.

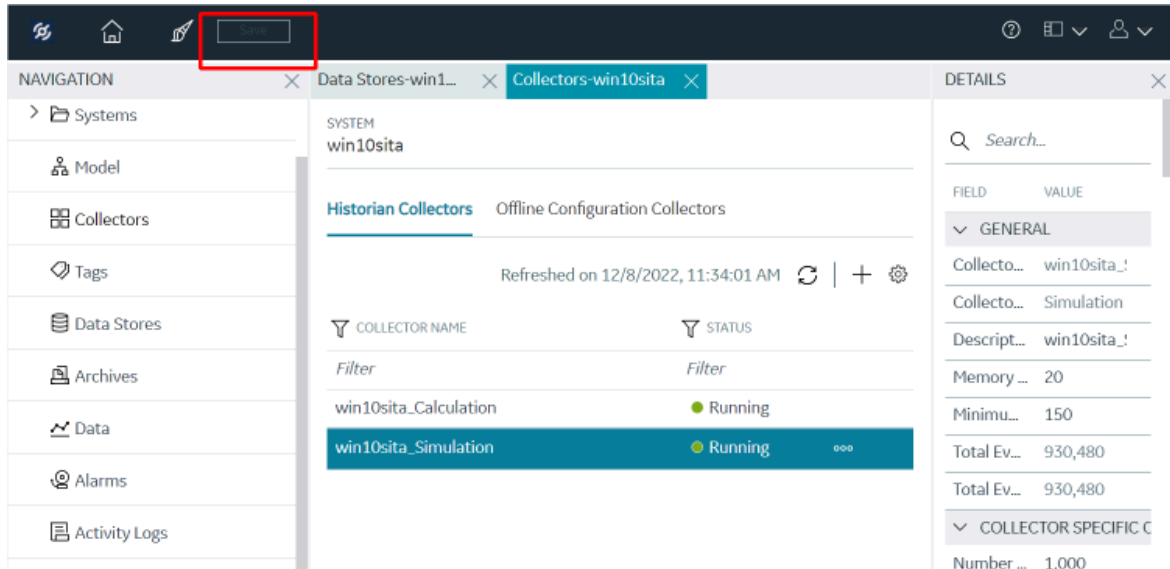
12. Select **Add**.

The collector instance is added. The fields specific to the collector section appear in the **DETAILS** section.

13. Under **Collector-Specific Configuration**, enter values as described in the following table.

Field	Description
Scan Interval	The interval, in seconds, after which the collector initiates an import operation. The maximum value that you can enter is 65.
CSV File Spec	The file extension for a CSV file to be imported. You can specify more than one extension type, such as csv, txt, dat.
XML File Spec	The file extension for an XML file to be imported.
Purge Processed (days)	The number of days after which you want the contents of the <code>Processed Files</code> folder to be automatically purged.
Purge Error (days)	The number of days after which you want the contents of the <code>Error Files</code> folder to be automatically purged.

14. If needed, enter values in [the other sections \(on page 1114\)](#).
15. In the upper-left corner of the page, select **Save**.



The changes to the collector instance are saved.

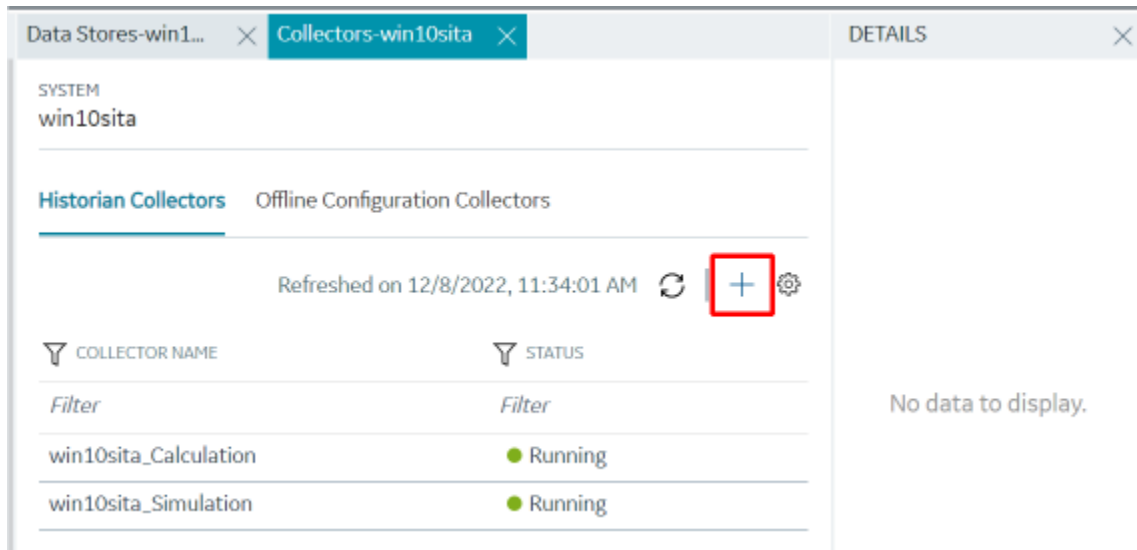
16. If needed, restart the collector.

[Import files using the collector.](#)

Add and Configure a HAB Collector

The HAB collector collects data from Habitat, which is a SCADA application that contains real-time data. The collector interacts with the Habitat Sampler application to fetch data from the Habitat database records and stores the data in a Historian server. For more information, refer to the [Overview of the HAB Collector](#).

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.
A list of collectors in the default system appears.
3. On the right, next to Settings in the main section, select **+**.



The **Add Collector Instance: <system name>** window appears, displaying the **Collector Selection** section. The **MACHINE NAME** field contains a list of machines on which you have installed collectors.

4. In the **MACHINE NAME** field, select the machine in which you want to add a collector instance.
5. In the **COLLECTOR TYPE** field, select **Hab Collector**, and then select **Get Details**.

The **INSTALLATION DRIVE** and **DATA DIRECTORY** fields are disabled and populated.

6. Select **Next**.

The **Source Configuration** section appears.

7. Enter values as described in the following table.

Field	Description
SERVER SITE	Enter name that you want to assign to the site. A value is required and must be unique. It is used by Habitat to identify the collector instance. By default, this field is populated with a value in the following format: <code><Historian server name>Hab</code>
SERVER 1 (under NODE 1)	Enter the host name or IP address of the Habitat server in the primary site from which you want to collect data. This server acts as the primary/active server from which the collector receives data. A value is required.

Field	Description
SERVER 1 (under NODE 2)	Enter the host name or IP address of the Habitat server in the second/backup site from which you want to collect data. This server acts as a standby server in case server 1 under node 1 fails. A value is required. If you do not have a secondary/backup site, enter the same value as SERVER 1 under node 1.
SERVER 2 (under NODE 1)	Enter the host name or IP address of the Habitat server that you want to use as a standby server in the same site as server 1. This server acts as a standby server in case server 1 under node 2 fails.
SERVER 2 (under NODE 2)	<p>Enter the host name or IP address of the Habitat server in the secondary/backup site from which you want to collect data. This server acts as a standby server in case server 2 under node 1 fails.</p> <p>For example, suppose Machine A and Machine B are in node AB, and Machine X and Machine Y are in node XY. Suppose you want to use Machine A as the primary server and the remaining machines as standby servers. In that case, enter values as follows:</p> <ul style="list-style-type: none"> ◦ SERVER 1 (under Node 1): Machine A ◦ SERVER 2 (under Node 1): Machine B ◦ SERVER 1 (under Node 2): Machine X ◦ SERVER 2 (under Node 2): Machine Y <p>If Machine A fails, the Machine B becomes active. If Machine B fails, Machine X becomes active. If Machine X fails, Machine Y becomes active.</p>
SOCKET	The socket number (port number) used by the Habitat Sampler application to connect. Each collector instance can connect to only one socket. The default value is 8040.
RETRY	The duration, in seconds, after which the collector tries to communicate with the site. The default value is 5 seconds.

8. Select **Next**.

The **Destination Configuration** section appears. Under **CHOOSE DESTINATION**, the **Historian Server** option is selected by default. The other options are disabled because you cannot send data to a cloud destination using the HAB collector.

9. If you want to connect to a remote Historian server, enter values in the **USERNAME** and **PASSWORD** fields.

10. Select **Next**.

The **Collector Initiation** section appears. By default, the **COLLECTOR NAME** field is populated with a value in the following format: `<Historian server name>_Hab`

11. If needed, modify the value in the **COLLECTOR NAME** field.

The value that you enter:

- Must be unique.
- Must not exceed 15 characters.
- Must not contain a space.
- Must not contain special characters except a hyphen, period, and an underscore.

12. In the **SamplerID** field, enter the user ID to connect to Habitat Sampler.

By default, this field contains the Collector Name. You can first provide the Collector Name and update the Sample ID field as this field will automatically take the Collector Name.

13. In the **RUNNING MODE** field, select one of the following options.


- **Service - Local System Account:** Select this option if you want to run the collector as a Windows service using the credentials of the local user (that is, the currently logged-in user). If you select this option, the **USERNAME** and **PASSWORD** fields are disabled. By default, this option is selected.
- **Service Under Specific User Account:** Select this option if you want to run the collector as a Windows service using a specific user account. If you select this option, you must enter values in the **USERNAME** and **PASSWORD** fields.



If you have enabled the **Enforce Strict Collector Authentication** option in Historian Administrator, you must provide the credentials of a user who is added to at least one of the following security groups:

- iH Security Admins
- iH Collector Admins
- iH Tag Admins

14. Select **Add**.

The collector instance is added. The fields specific to the collector appear in the **DETAILS** section.

15. Depending on whether you want to configure tags or alarms, select  next to the corresponding field under **Collection Definitions**.

DETAILS	
FIELD	VALUE
<div style="background-color: #f2f2f2; padding: 2px;"> ▼ General </div>	
Collector Name	WIN10TECH_Hab
Collector Type	Hab Collector
Description	WIN10TECH_Hab
Memory Buffer Size(MB)	20
Minimum Free Space(MB)	150
Total Events Collected	0
Total Events Reported	0
<div style="background-color: #f2f2f2; padding: 2px;"> ▼ Collection Definitions </div>	
Data Collection Definitions	0 
Alaram Collection Definitons	0 

The **Data Collections** or **Alarm Collections** section appears.

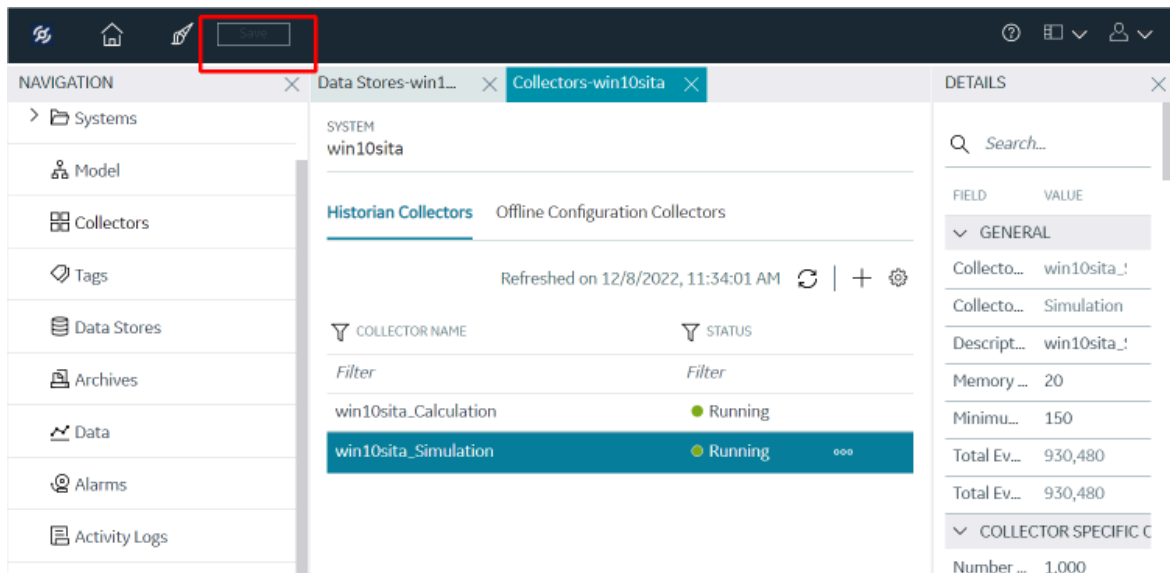
16. Select **+**, and then enter values in the available fields for [data collection and/or alarm collection \(on page 1041\)](#). You can also copy a collection definition by right-clicking it and selecting **Duplicate**.
17. Under **Collector Specific Configuration**, enter values as described in the following table.

Field	Description
Auto Tag Sync	<p>If you enable this option, the collector creates tags automatically in Historian based on the key value. In addition, any tag changes in Habitat (such as adding, renaming, and deleting tags) will reflect automatically in Historian. No manual steps are required.</p> <p>If you disable this option, any tag changes in Habitat will be captured in the <code><collector name>_Tag_Unconfirmed.xml</code> file. Only after you approve these changes, they are reflected in Historian.</p>
Tag Deletion Type	Specify whether deleted tags in Habitat that you have approved must be deleted or disabled for data collection in Historian. Enter one of the following values:

Field	Description
	<ul style="list-style-type: none"> ◦ DISABLE_TAG (this is the default value) ◦ DELETE_TAG

18. As needed, provide values in the [remaining fields \(on page 1114\)](#).

19. In the upper-left corner of the page, select **Save**.



The changes to the collector instance are saved.

20. [Start the collector \(on page 1170\)](#).

If you have disabled the automatic tag sync option in the configuration file, tag changes in Habitat (such as adding, renaming, and deleting tags) are captured in the `<collector_name>_tag.xml` file. You must approve the changes so that they are reflected in Historian. To do so:

1. Right-click the HAB collector instance that you have created, and then select **Confirm Queued Tags**.

A list of tags that have been changed appears.

2. Select the check boxes corresponding to the tags whose changes you want to approve, and then select **Confirm**. You can filter the list using the **TAG TYPE** field.

The tag changes are approved. The status of the tags is updated in the

`<collector_name>_tag.xml` file (that is, the Confirmed parameter is set to true).

Collection Definitions of a HAB Collector

Table 31. Tag Data Collection Definition Parameters


Parameter	Description
DEFINITION NAME	<p>The name of the collection definition. A value is required and must be unique.</p> <div style="border: 1px solid #ffc107; border-radius: 10px; padding: 10px; background-color: #fff3cd;"> <p> Important: You must not change the name after the collector starts collecting data. If, however, you want to change the name after the collector has started collecting data, refer to FAQs on the HAB Collector.</p> </div>
STATUS	Indicates whether the collection definition is enabled. If an error occurs while processing the collection definition, the collector automatically disables the collection definition.
FAMILY	The name of the Habitat family from which you want to collect data (for example, EMS, DTS). A value is required and must be unique.
APPLICATION	The name of the Habitat application from which you want to collect data (for example, SCADA). A value is required.
DATABASE	The name of the Habitat database from which you want to collect data (for example, SCADAMOM). A value is required.
RECORD TYPE	The name of the HDB record from which you want to collect data (for example, ANALOG, POINT, COUNT). A value is required. Enter any record type that contains the composite key and MRID fields (because the collector uses these two fields to create tags).

Table 31. Tag Data Collection Definition Parameters (continued)

Parameter	Description
COLLECTION TYPE	<p>Indicates whether you want to perform polled or unsolicited data collection.</p> <ul style="list-style-type: none"> • Polled: Indicates a periodic data collection, where data is collected at a regular time interval (indicated as PERIODIC in Habitat). • Unsolicited: Indicates that data is collected only when values have changed since the last time data was collected (indicated as EXCEPTION in Habitat).
KEY	<p>The value that will be used to filter tags for data collection. A value is required. You can use the wildcard character * to get a range of values. For example, if you want to collect data from all tags that begin with SUBSTN.LAKEVIEW, enter: SUBSTN.LAKEVIEW*.*.*.*</p>
PREFIX FIELD	<p>The prefix that you want to use for tags. You can provide a different value for each collection definition, which helps you identify tags based on the collection definition.</p>
TAG NAME FIELD	<p>Determines how the tags created in Historian must be named. A value is required.</p> <p>For example, if you want the tags to be named after the value in the LOC_CIRCLG field, enter LOC_CIRCLG. When you do so, if the value in the LOC_CIRCLG field in Habitat is DOUGLAS, the tag created in Historian will be named <TagPrefix value>.<AlarmPrefix value>.DOUGLAS.</p> <p>You can enter multiple values separated by commas.</p> <p>For example, if you want the tags to be named after the values in the LOC_CIRCLG and PRIOR_CIRCLG fields, enter LOC_CIRCLG,PRIOR_CIRCLG. When you do so, if the values in the LOC_CIRCLG and PRIOR_CIRCLG fields are Douglas and 1 respectively, the tag created in Historian will be named <TagPrefix value>.<AlarmPrefix value>.DOUGLAS.1.</p>

Table 31. Tag Data Collection Definition Parameters (continued)

Parameter	Description
MRID FIELD	The MRID of the record. A value is required. If, however, MRID is not available, enter the composite key or any other unique identifier of the record.
DESCRIPTION FIELD	The description of the tag. A value is required.
VALUE FIELD	<p>The name of the property that stores the tag value in Habitat. A value is required.</p> <p>You can enter multiple values, separated by commas. One Historian tag will be created for each value you enter in this field.</p>
TIMESTAMP FIELD	<p>The name of the property that stores the timestamp of a tag in Habitat. You can use a HDB timestamp or custom/alias timestamps.</p> <p>Examples:</p> <p>For analog, you can use:</p> <ul style="list-style-type: none"> • FIELDTIME: A combination of FLDTIME_ANALOG and FLD-MSEC_ANALOG, in the hour: min:sec: millisec format. • SCADATIME: Used to capture SCTIME_ANALOG in the hour: min:sec: millisec format. • SAMPLETIME: The time at which the data sample was collected in Habitat in the hour: min:sec format. <p>For point, you can use:</p> <ul style="list-style-type: none"> • FIELDTIME: A combination of FLDTIME_POINT and FLD-MSEC_POINT, in the hour: min:sec: millisec format. • SCADATIME: Used to capture SCTIME_POINT in the hour: min:sec: millisec format. • SAMPLETIME: The time at which the data sample was collected in Habitat in the hour: min:sec format. <p>For count, you can use:</p>

Table 31. Tag Data Collection Definition Parameters (continued)

Parameter	Description
	<ul style="list-style-type: none"> • FIELDTIME: A combination of FLDTIME_COUNT and FLD-MSEC_COUNT, in the hour: min:sec: millisec format. • SAMPLETIME: The time at which the data sample was collected in Habitat in the hour: min:sec format. <p>You can edit the names of these custom/alias timestamps using the registry entries FieldTimeCustomFieldName, ScadaTimeCustom-FieldName, and SampleTimeCustomFieldName respectively.</p>
QUALITY FIELD	The name of the property that stores the tag quality in Habitat.
SAMPLE RATE	<p>The rate at which you want to collect or poll data. A value is required.</p> <p>For example, if the sample rate is 10 seconds:</p> <ul style="list-style-type: none"> • For a polled collection type, data is written to Data Archiver every 10 seconds. • For an unsolicited collection type, the collector checks for any data changes every 10 seconds. Only if there are changes, the data is written to Data Archiver.
SAMPLE UNIT	<p>The unit of measurement for the sample rate. A value is required.</p> <p>Valid values:</p> <ul style="list-style-type: none"> • sec • min • hour • day • week • month
PERMANENT	Indicates whether you want to store the data in buffer files in Habitat in the event of a connection loss. We strongly recommend that you set this parameter to true to prevent loss of data.

Table 32. Alarm Data Collection Definition Parameters


Parameter	Description
DEFINITION NAME	<p>The name of the collection definition. A value is required and must be unique.</p> <div data-bbox="617 445 1421 709" style="border: 1px solid orange; border-radius: 10px; padding: 10px;"> <p> Important: You must not change the name after the collector starts collecting data. If, however, you want to change the name after the collector has started collecting data, refer to FAQs on the HAB Collector.</p> </div>
STATUS	Indicates whether the collection definition is enabled. If an error occurs while processing the collection definition, the collector automatically disables the collection definition.
FAMILY	The name of the Habitat family from which you want to collect data (for example, EMS, DTS). A value is required and must be unique.
APPLICATION	The name of the Habitat application from which you want to collect data (for example, SCADA). A value is required.
DATABASE	The name of the Habitat database from which you want to collect data (for example, ALARMLIST). A value is required.
RECORD TYPE	The name of the HDB record from which you want to collect data (for example, CIRCLG, ALMQ). A value is required. Enter any record type that contains the composite key and MRID fields (because the collector uses these two fields to create tags).
KEY	This field is not applicable to alarms. Enter *.
TAG NAME FIELD	<p>Determines how the tags created in Historian must be named. A value is required.</p> <p>For example, if you want the tags to be named after the value in the LOC_CIRCLG field, enter <code>LOC_CIRCLG</code>. When you do so, if the value in the LOC_CIRCLG field in Habitat is DOUGLAS, the tag created in Historian will be named <code><TagPrefix value>.<AlarmPrefix value>.DOUGLAS</code>.</p> <p>You can enter multiple values separated by commas.</p>

Table 32. Alarm Data Collection Definition Parameters (continued)

Parameter	Description
	For example, if you want the tags to be named after the values in the LOC_CIRCLG and PRIOR_CIRCLG fields, enter LOC_CIRCLG,PRIOR_CIRCLG. When you do so, if the values in the LOC_CIRCLG and PRIOR_CIRCLG fields are Douglas and 1 respectively, the tag created in Historian will be named <TagPrefix value>.<AlarmPrefix value>.DOUGLAS.1.
PREFIX	The prefix that you want to use for tags. A value is required. You can provide a different value for each collection definition, which helps you identify tags based on the collection definition.
VALUE	<p>The name of the property that stores the tag value in Habitat. A value is required.</p> <p>You can enter multiple values, separated by commas (for example, TEXT_CIRCLG, PRIOR_CIRCLG, TIME_CIRCLG). The values will then be concatenated in the corresponding Historian tag.</p>
TIMESTAMP	This field is not applicable to alarms. Leave the field blank. You can use the VALUE FIELD field to provide the timestamp (for example, TIME_CIRCLG).
QUALITY	This field is not applicable to alarms. Leave the field blank.
DISABLED	Switch the toggle to enable alarm filtering. You can then collect data only for the filtered alarms.
ALARM LOCATION	The alarm location based on which you want to filter alarm data. A value is required if alarm filtering is enabled. You can enter multiple values separated by commas (for example, LA,NY). The default value is *, which indicates that data for that parameter is not filtered.
ALARM AREA	The alarm area based on which you want to filter alarm data. A value is required if alarm filtering is enabled. You can enter multiple values separated by commas (for example, LAKEVIEW,RICHVIEW). The default value is *, which indicates that data for that parameter is not filtered.
ALARM CATEGORY	The alarm category based on which you want to filter alarm data. A value is required if alarm filtering is enabled. You can enter multiple

Table 32. Alarm Data Collection Definition Parameters (continued)

Parameter	Description
	values separated by commas (for example, PressureSensor,Motion-Sensor). The default value is *, which indicates that data for that parameter is not filtered.
ALARM PRIORITY	The alarm priority based on which you want to filter alarm data. A value is required if alarm filtering is enabled. You can enter multiple values separated by commas (for example, 1,2). The default value is *, which indicates that data for that parameter is not filtered.
ALARM EXCEPTION	The alarm exception based on which you want to filter alarm data. A value is required if alarm filtering is enabled. You can enter multiple values separated by commas. The default value is *, which indicates that data for that parameter is not filtered.
SAMPLE RATE	The rate at which you want to collect data. A value is required.
SAMPLE UNIT	<p>The unit of measurement for the sample rate. A value is required.</p> <p>Valid values:</p> <ul style="list-style-type: none"> • sec • min • hour • day • week • month
PERMANENT	Indicates whether you want to store the data in buffer files in Habitat in the event of a connection loss. We strongly recommend that you set this parameter to true to prevent loss of data.

About Adding an iFIX Collector Instance

This topic provides guidelines on how to configure the iFIX collector using Configuration Hub based on the running mode of iFIX. It also describes the collector behaviour and recommended configuration in each case.

iFIX Running Mode	Recommended Configuration for the iFIX Collector	Collector Behaviour After You Add the Collector Instance
<p>iFIX is running in service mode and is secured.</p> <p>The iFIX Alarms and Events and the OPC Alarms and Events Servers are running as service.</p>	<p>Configure the iFIX collector services under a user account under which iFIX is running as a service. While adding an instance of the iFIX collector or the iFIX Alarms and Events collector using Configuration Hub, select Service Under Specific User Account.</p>	<ul style="list-style-type: none"> • The iFIX collector starts running as a service. It appears in the collectors list in Configuration Hub. • You can run the collector at a command prompt using the Collector Start action. A shortcut is created in the Windows Start menu so that you can run the collector in the command-line mode. • By default, when not started as an SCU task, the iFIX collector points to the iFIX nodename. You must configure the iFIX node in the Collector Configuration section in Historian Administrator.
<p>iFIX is running as a service and is not secured.</p> <p>The iFIX Alarms and Events and the OPC Alarms and Events servers are running as service.</p>	<p>You can configure the iFIX collector service using a local system account or a specific user account.</p>	<ul style="list-style-type: none"> • The iFIX collector starts running as a service. • You can run the collector at a command prompt using the Collector Start action. A shortcut is created in the Windows Start menu so that you can run the collector in the command-line mode. • By default, when not started as an SCU task, the iFIX collector points to the iFIX nodename. You must con-

iFIX Running Mode	Recommended Configuration for the iFIX Collector	Collector Behaviour After You Add the Collector Instance
		figure the iFIX node in the Collector Configuration section in Historian Administrator.
iFIX is not running as a service mode and is secured.	Configure the iFIX collector services under a user account that is added in the IFIXUSERS group. Do not configure as a local system service. While adding an instance of the iFIX collector or the iFIX Alarms and Events collector using Configuration Hub, select Service Under Specific User Account .	<ul style="list-style-type: none"> • Since Remote Collector Manager tries to start the collector as a service, and iFIX is not running as a service, an error message appears while adding a collector instance. However, the instance is configured successfully although it does not appear in the collectors list in Configuration Hub. • A shortcut is created in the Windows Start menu so that you can run the collector in the command-line mode, and the related registry folder is created. • You must start the collector manually for the first time using the shortcut. It will then connect to the Historian server, and it will then appear in the collectors list in Configuration Hub. • Once connected to server, you can start/stop it at a command prompt.

iFIX Running Mode	Recommended Configuration for the iFIX Collector	Collector Behaviour After You Add the Collector Instance
<p>iFIX is not running as a service mode, and is not secured.</p>	<p>You can configure the iFIX collector service using a local system account or a specific user account.</p>	<ul style="list-style-type: none"> • Since Remote Collector Manager tries to start the collector as a service, and iFIX is not running as a service, an error message appears while adding a collector instance. However, the instance is configured successfully. • A shortcut is created in the Windows Start menu so that you can run the collector in the command-line mode, and the related registry folder is created. • You must start the collector manually for the first time using the shortcut. It will then connect to the Historian server. • Once connected to server, you can start/stop it at a command prompt.
<p>iFIX is not running.</p>	<p>You can configure the iFIX collector service using a local system account or a specific user account, as per the security configuration of iFIX.</p>	<ul style="list-style-type: none"> • Since Remote Collector Manager tries to start the collector as a service, and iFIX is not running as a service, an error message appears while adding a collector instance. However, the instance is configured successfully although it does not appear

iFIX Running Mode	Recommended Configuration for the iFIX Collector	Collector Behaviour After You Add the Collector Instance
		<p>in the collectors list in Configuration Hub.</p> <ul style="list-style-type: none"> • A shortcut is created in the Windows Start menu so that you can run the collector in the command-line mode, and the related registry folder is created. • After you start iFIX, you must start the collector manually for the first time using the shortcut. It will then connect to the Historian server. • Once connected to server, you can start/stop it at a command prompt.

Add and Configure an iFIX Collector

Ensure that iFIX is running in a Windows-service mode. For more information, refer to https://www.ge.com/digital/documentation/historian/version2023/c_best_practices.html.

The iFIX collectors collect data from iFIX and store it in the Historian server. They include:

- The iFIX collector
- The iFIX Alarms and Events collector

When you install collectors, if iFIX is installed on the same machine as the collectors, instances of the iFIX collectors are created automatically. This topic describes how to create additional instances if needed.

This topic describes how to add a collector instance using Configuration Hub. You can also [add a collector instance using the RemoteCollectorConfigurator utility](#), which does not require you to install Web-based Clients.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.
A list of collectors in the default system appears.
3. If needed, select the system in which you want to add a collector instance.

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

4. In the upper-right corner of the main section, select **+**.

COLLECTOR NAME	STATUS
<i>Filter</i>	<i>Filter</i>
win10sita_Calculation	Running
win10sita_Simulation	Running

The **Add Collector Instance: <system name>** window appears, displaying the **Collector Selection** section. The **MACHINE NAME** field contains a list of machines on which you have installed collectors.

5. In the **MACHINE NAME** field, select the machine in which you want to add a collector instance.

6. In the **COLLECTOR TYPE** field, select **iFIX Alarms Events Collector** or **iFIX Collector**, and then select **Get Details**.

The **INSTALLATION DRIVE** and **DATA DIRECTORY** fields are disabled and populated.

7. Select **Next**.

The **Source Configuration** section appears. The **iFIX SERVER** field is disabled and populated.

8. Select **Next**.

The **Destination Configuration** section appears. The **Historian Server** option is selected by default.

You cannot select any other option for an iFIX Alarms and Events collector.

9. Select the destination to which you want to send data, and then enter values in the available fields.

You can send data to an on-premises Historian server or to a cloud destination such as [Alibaba Cloud](#), [AWS Cloud](#), [Azure Cloud](#), [Google Cloud](#), or [Predix Cloud](#). For an iFIX Alarms and Events collector, however, you can only send data to an on-premises Historian server.

10. In the **RUNNING MODE** field, select one of the following options.

- **Service - Local System Account:** Select this option if you want to run the collector as a Windows service using the credentials of the local user (that is, the currently logged-in user). If you select this option, the **USERNAME** and **PASSWORD** fields are disabled. By default, this option is selected.
- **Service Under Specific User Account:** Select this option if you want to run the collector as a Windows service using a specific user account. If you select this option, you must enter values in the **USERNAME** and **PASSWORD** fields.

If you have enabled the **Enforce Strict Collector Authentication** option in Historian Administrator, you must provide the credentials of a user who is added to at least one of the following security groups:

- iH Security Admins
- iH Collector Admins
- iH Tag Admins

11. Select **Next**.

The **Collector Initiation** section appears.

12. If needed, modify the value in the **COLLECTOR NAME** field.

The value that you enter:

- Must be unique.
- Must not exceed 15 characters.
- Must not contain a space.
- Must not contain special characters except a hyphen, period, and an underscore.

13. In the **RUNNING MODE** field, select one of the following options.

- **Service - Local System Account:** Select this option if you want to run the collector as a Windows service using the credentials of the local user (that is, the currently logged-in user). If you select this option, the **USERNAME** and **PASSWORD** fields are disabled.
- **Service Under Specific User Account:** Select this option if iFIX is running in a secured mode, or if you want to run the collector as a Windows service using a specific user account. If you select this option, you must enter the credentials of the iFIX user in the **USERNAME** and **PASSWORD** fields.

If you have enabled the **Enforce Strict Collector Authentication** option in Historian Administrator, you must provide the credentials of a user who is added to at least one of the following security groups:

- iH Security Admins
- iH Collector Admins
- iH Tag Admins

You can also configure the collector to start automatically when you start iFIX.

14. Select **Add**.

The collector instance is added, and appears in the Collectors list. A shortcut is created so that you can open it at a command prompt.

If iFIX is not running in a service mode, an error message may appear. However, the collector instance is created; therefore, you can ignore the error message. Although the collector instance does not appear in the list of collectors in Configuration Hub, a shortcut is created. You can run the collector manually at a command prompt or as a SCU task. For more information, refer to [About Adding an iFIX Collector Instance](#).

15. Under **Collector Specific Configuration**, in the **Nodes to Browse** field, enter the mask that you want to use to select tags when browsing for tags in the collector. The default value is FIX.

If you want to browse for tags on other iFIX nodes via FIX networking, you can enter the other node name(s) here, separated by commas with no spaces. You must have the iFIX system configured for networking. For more information, refer to the iFIX product documentation on iFIX networking.



Note:

If you have modified iFIX node name, then you must also update the value in the **Nodes to Browse** field before browsing for tags in the iFIX collector.

When you browse multiple nodes for tags to add to an iFIX collector, do not use space characters between node names or between the required comma and next node name. All characters after the space are ignored.

16. Under **Tag Browse Criteria**, specify the tags for data collection (on page 909).



Note:

If you want to add block or field types to the list, edit the `FixTag.dat` file for Historian Administrator you are using. Refer to [Editing the FixTag.dat file](#) for more information.

17. If needed, enter values in the other sections (on page 1114).

18. In the upper-left corner of the page, select **Save**.

The screenshot displays the Configuration Hub interface for the 'Collectors-win10sita' configuration page. The top navigation bar includes a 'Save' button, which is highlighted with a red box. The main content area shows a table of 'Historian Collectors' with columns for 'COLLECTOR NAME' and 'STATUS'. Two collectors are listed: 'win10sita_Calculation' (Running) and 'win10sita_Simulation' (Running). The 'win10sita_Simulation' row is highlighted in blue. The right sidebar shows a 'DETAILS' panel with a search bar and a table of fields and values.

FIELD	VALUE
Collecto...	win10sita_!
Collecto...	Simulation
Descript...	win10sita_!
Memory ...	20
Minimu...	150
Total Ev...	930,480
Total Ev...	930,480
Number ...	1,000

The changes to the collector instance are saved.

19. If needed, restart the collector.

Specify the tags whose data you want to collect using the collector. In the **CHOOSE CONFIGURATION** field,

- If you have selected **Historian Configuration**, [specify the tags using Configuration Hub \(on page 909\)](#).
- If you have selected **Offline Configuration**, modify the offline configuration file of the collector. By default, the file is available in the following location: `<installation folder of Historian>\GE Digital\<collector name>`. For information, refer to [offline configuration](#). This option is applicable only if you have selected a cloud destination. This option is not applicable to an iFIX Alarms and Events collector.

Add and Configure an MQTT Collector

1. Ensure that you have an MQTT broker.

**Note:**

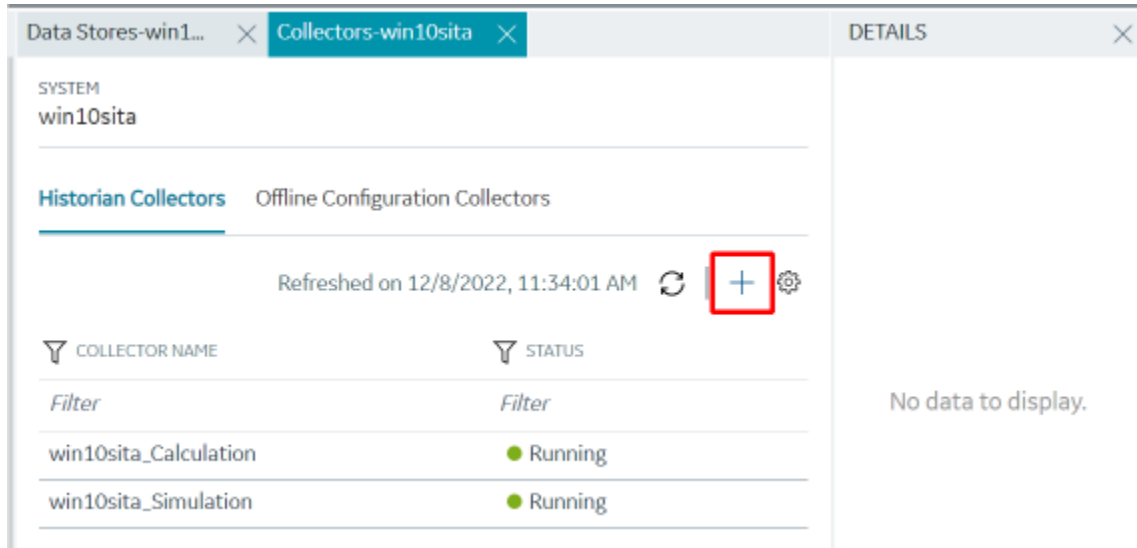
We have tested with the MQTT brokers Mosquitto 2.0.15 and HiveMQ-4.2.1. You can, however, use other MQTT brokers as well.

2. If you want to use username/password-based authentication or certificate-based authentication to connect the MQTT broker and the MQTT collector, configure the authentication in the MQTT broker.
3. If you want to use certificate-based authentication, ensure that the following files are available on your collector machine:
 - CA server root file
 - Private key file
 - Client certificate file

The MQTT collector collects data published to a topic using an MQTT broker. For more information, refer to the [Overview of the MQTT Collector](#).

This topic describes how to add a collector instance using Configuration Hub. You can also [add a collector instance using the RemoteCollectorConfigurator utility](#), which does not require you to install Web-based Clients.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**. A list of collectors in the default system appears.
3. In the upper-right corner of the main section, select **+**.



The **Add Collector Instance: <system name>** window appears, displaying the **Collector Selection** section. The **MACHINE NAME** field contains a list of machines on which you have installed collectors.

4. In the **MACHINE NAME** field, select the machine in which you want to add a collector instance.
5. In the **COLLECTOR TYPE** field, select **MQTT Collector**, and then select **Get Details**.

The **INSTALLATION DRIVE** and **DATA DIRECTORY** fields are disabled and populated.

6. Select **Next**.

The **Source Configuration** section appears.

7. Enter values as described in the following table.

Field	Description
MQTT BROKER ADDRESS	Enter the host name of the MQTT broker using which you want to collect data. A value is required.
MQTT BROKER PORT	Enter the port number of the MQTT broker. A value is required.
TOPIC	Enter the MQTT topic from which you want to collect data. A value is required. You can enter multiple topics separated by commas.

Field	Description
	<p>If you want to use the SparkplugB format, enter a value in the following format: <code>namespace/group_id/message_type/edge_node_id/device_id</code></p> <p>where:</p> <ul style="list-style-type: none"> ◦ <code>namespace</code> is the Sparkplug version. Enter <code>spBv1.0</code>. ◦ <code>group_id</code> is the ID of the group of nodes from which you want to collect data. ◦ <code>message_type</code> is the message type from which you want to collect data. The collector processes data only from NDATA and DDATA message types. ◦ <code>edge_node_id</code> is used to identify the MQTT EoN node within the infrastructure. ◦ <code>device_id</code> a device attached to the MQTT EoN node either physically or logically. <p>You can use the wildcard character <code>#</code> for any of these parameters (except for namespace).</p>
USERNAME	Enter the username to connect to the MQTT broker. A value is required if you have configured username/password-based authentication in the MQTT broker.
PASSWORD	Enter the password to connect to the MQTT broker. A value is required if you have configured username/password-based authentication in the MQTT broker.
CA SERVER ROOT FILE	Enter the path to the CA server root file to connect to the MQTT broker. A value is required if you have configured certificate-based authentication in the MQTT broker.
PRIVATE KEY FILE	Enter the path to the private key file to connect to the MQTT broker. A value is required if you have configured certificate-based authentication in the MQTT broker.
CLIENT CERTIFICATE FILE	Enter the path to the client certificate file to connect to the MQTT broker. A value is required if you have configured certificate-based authentication in the MQTT broker.

Field	Description
REQUESTED QUALITY OF SERVICE (QOS) LEVEL	<p>Select the quality of service that you want to use while collecting data from an MQTT broker.</p> <ul style="list-style-type: none"> ◦ QoS 0: Indicates that the message is delivered at most once or it is not delivered at all. ◦ QoS 1: Indicates that the message is always delivered at least once. ◦ QoS 2: Indicates that the message is delivered once. <p>For more information, refer to https://www.hivemq.com/blog/mqtt-essentials-part-6-mqtt-quality-of-service-levels/.</p>
MQTT VERSION	Select the version of the MQTT that you want to use.
CLEAN SESSION	<p>Select one of the following options:</p> <ul style="list-style-type: none"> ◦ True: Select this option if you do not want to create a new session when the MQTT broker and the collector are disconnected from each other. ◦ False: Select this option if you want to retain the session when the MQTT broker and the collector are disconnected from each other. This ensures that there is no loss of data. If you want to choose this option, ensure that you have selected QoS 1 or QoS 2 in the REQUESTED QUALITY OF SERVICE (QOS) LEVEL field.
SESSION EXPIRY INTERVAL	<p>Enter the duration, in seconds, after which the data will be discarded when connection between the MQTT broker and collector is re-established.</p> <p>For example, if you enter 100 in this field, and if the MQTT broker and collector are disconnected for 90 seconds, the data is collected. If, however, the MQTT broker and the collector are disconnected for more than 100 seconds, the data will be discarded.</p> <p>This field is applicable only for MQTT V5 and only if you set the CLEAN SESSION field to False.</p>
CONTENT TYPE	Select the format that you want to use for the payload:

Field	Description
	<ul style="list-style-type: none"> ◦ JSON: Select this option if you want to use the KairosDB format. ◦ SparkPlug B v1.0: Select this option if you want to use the Sparkplug format.

8. Select **Next**.

The **Destination Configuration** section appears. Under **CHOOSE DESTINATION**, the **Historian Server** option is selected by default. In addition, the **DESTINATION HISTORIAN SERVER** field is disabled and populated with the value you selected in the **MACHINE NAME** field in the **Collector Selection** section.

9. Select the destination to which you want to send data, and then enter values in the available fields.

You can send data to an on-premises Historian server or to a cloud destination such as [Alibaba Cloud \(on page 1122\)](#), [AWS Cloud \(on page 1127\)](#), [Azure Cloud \(on page 1134\)](#), [Google Cloud \(on page 1148\)](#), or [Predix Cloud \(on page 1154\)](#).

10. Select **Next**.

The **Collector Initiation** section appears.

11. If needed, modify the value in the **COLLECTOR NAME** field. The value must be unique, must contain the string `MQTT`, and must not contain a space.

The value that you enter:

- Must be unique.
- Must contain the string `MQTT`.
- Must not exceed 15 characters.
- Must not contain a space.
- Must not contain special characters except a hyphen, period, and an underscore.

12. In the **RUNNING MODE** field, select one of the following options.

- **Service - Local System Account**: Select this option if you want to run the collector as a Windows service using the credentials of the local user (that is, the currently logged-in user). If you select this option, the **USERNAME** and **PASSWORD** fields are disabled.
- **Service Under Specific User Account**: Select this option if you want to run the collector as a Windows service using a specific user account. If you select this option, you must enter values in the **USERNAME** and **PASSWORD** fields.

If you have enabled the **Enforce Strict Collector Authentication** option in Historian Administrator, you must provide the credentials of a user who is added to at least one of the following security groups:

- iH Security Admins
- iH Collector Admins
- iH Tag Admins

You can also configure the collector to start automatically when you start the computer.

13. Select **Add**.

The collector instance is added. The fields specific to the collector section appear in the **DETAILS** section.

14. If needed, enter values in [available fields \(on page 1114\)](#).

15. In the upper-left corner of the page, select **Save**.

The screenshot displays the Configuration Hub interface for managing collectors. The top navigation bar includes a 'Save' button, which is highlighted with a red box. The main content area is divided into three sections: NAVIGATION, SYSTEM, and DETAILS. The NAVIGATION section on the left lists various system components. The SYSTEM section shows the configuration for the 'win10sita' system, including a table of collector instances. The DETAILS section on the right provides configuration options for the selected collector.

COLLECTOR NAME	STATUS
win10sita_Calculation	Running
win10sita_Simulation	Running

The changes to the collector instance are saved.

16. If needed, restart the collector.

Specify the tags whose data you want to collect using the collector. In the **CHOOSE CONFIGURATION** field,

- If you have selected **Historian Configuration**, [specify the tags using Configuration Hub \(on page 909\)](#).
- If you have selected **Offline Configuration**, modify the offline configuration file of the collector. By default, the file is available in the following location: *<installation folder of Historian>\GE Digital\<collector name>*. For information, refer to [Offline Configuration for Collectors](#). This option is applicable only if you have selected a cloud destination.

Add and Configure an ODBC Collector Using Configuration Hub

The ODBC collector collects data from an application based on an ODBC driver. For more information, refer to [Overview of the ODBC Collector](#).

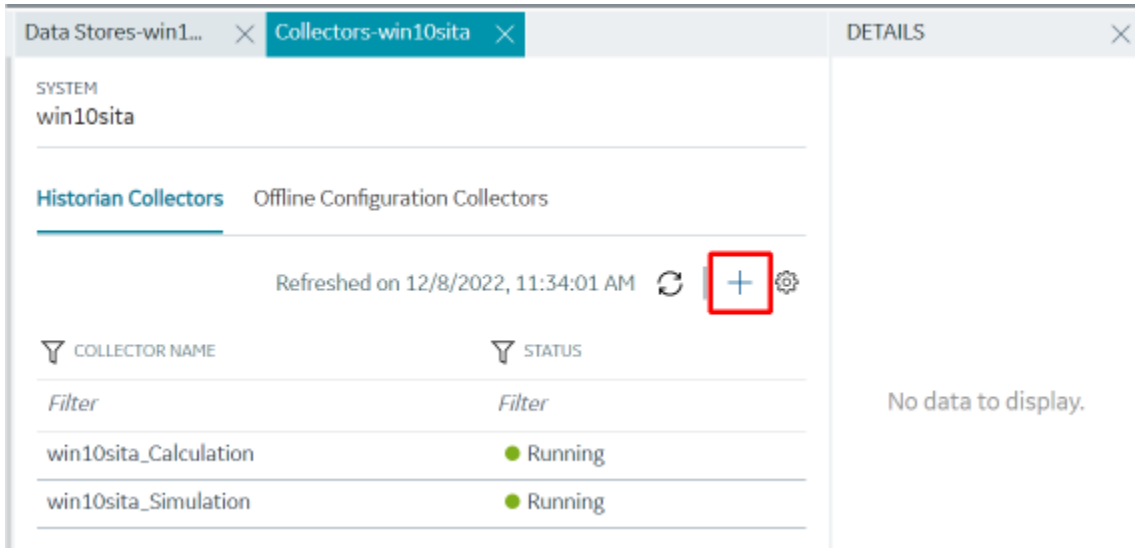
This topic describes how to add a collector instance using Configuration Hub. You can also [add a collector instance using the RemoteCollectorConfigurator utility](#), which does not require you to install Web-based Clients.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**. A list of collectors in the default system appears.
3. If needed, select the system in which you want to add a collector instance.

The screenshot shows a web interface for managing collectors. At the top left, there is a dropdown menu labeled 'SYSTEM' with 'WIN10TECH' selected. To the right, it says 'Refreshed on 2021-12-21 16:10:40' with refresh, add, and settings icons. Below is a table with columns: COLLECTOR NAME, STATUS, CONFIGURATION, and MACHINE. Each column has a filter icon and the word 'Filter' below it. The table contains three rows of collector data.

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

4. In the upper-right corner of the main section, select **+**.



The **Add Collector Instance: <system name>** window appears, displaying the **Collector Selection** section. The **MACHINE NAME** field contains a list of machines on which you have installed collectors.

5. In the **MACHINE NAME** field, select the machine in which you want to add a collector instance.
6. In the **COLLECTOR TYPE** field, select **ODBC Collector**, and then select **Get Details**.

The **INSTALLATION DRIVE** and **DATA DIRECTORY** fields are disabled and populated.

7. Select **Next**.

The **Source Configuration** section appears.

8. Enter values as described in the following table.

Field	Description
ODBC SERVER	Enter the host name or IP address of the ODBC server from which you want to collect data. A value is required.
USERNAME	Enter the username to connect to the ODBC server. A value is required.
PASSWORD	Enter the password to connect to the ODBC server. A value is required.

9. Select **Next**.

The **Destination Configuration** section appears. Under **CHOOSE DESTINATION**, the **Historian Server** option is selected by default. In addition, the **DESTINATION HISTORIAN SERVER** field is disabled and populated.

10. Select the destination to which you want to send data, and then enter values in the available fields. You can send data to an on-premises Historian server or to a cloud destination such as [Alibaba Cloud \(on page 1122\)](#), [AWS Cloud \(on page 1127\)](#), [Azure Cloud \(on page 1134\)](#), [Google Cloud \(on page 1148\)](#), or [Predix Cloud \(on page 1154\)](#).

11. Select **Next**.

The **Collector Initiation** section appears.

12. If needed, modify the value in the **COLLECTOR NAME** field.

The value that you enter:

- Must be unique.
 - Must contain the string `ODBC`.
 - Must not exceed 15 characters.
 - Must not contain a space.
 - Must not contain special characters except a hyphen, period, and an underscore.
13. In the **RUNNING MODE** field, select one of the following options.
 - **Service - Local System Account:** Select this option if you want to run the collector as a Windows service using the credentials of the local user (that is, the currently logged-in user). If you select this option, the **USERNAME** and **PASSWORD** fields are disabled.
 - **Service Under Specific User Account:** Select this option if you want to run the collector as a Windows service using a specific user account. If you select this option, you must enter values in the **USERNAME** and **PASSWORD** fields.

If you have enabled the **Enforce Strict Collector Authentication** option in Historian Administrator, you must provide the credentials of a user who is added to at least one of the following security groups:


- iH Security Admins
- iH Collector Admins
- iH Tag Admins

You can also configure the collector to start automatically when you start the computer.

14. Select **Add**.

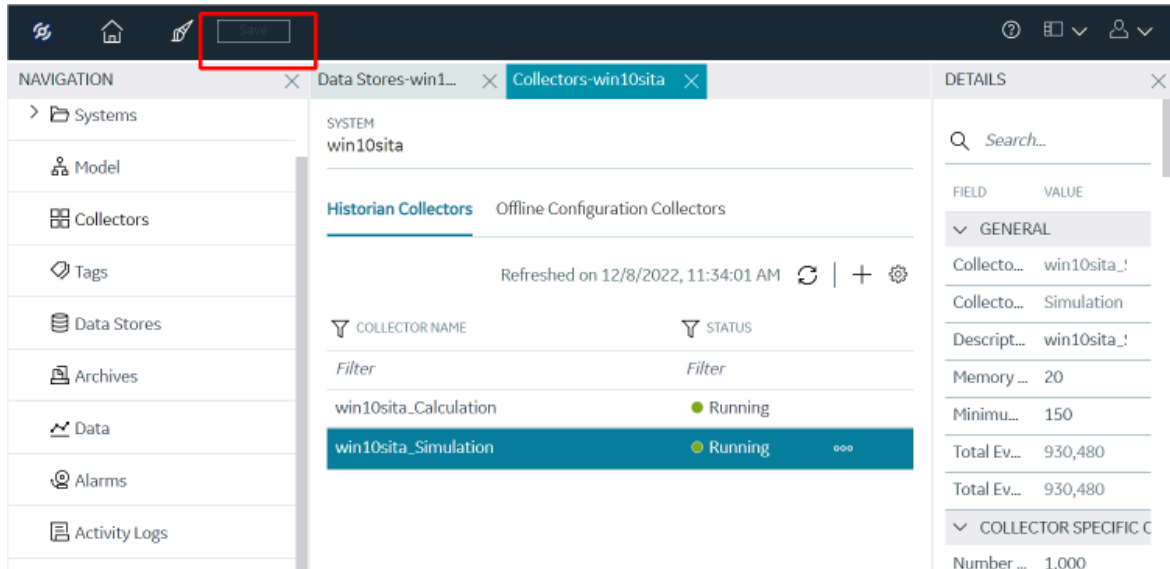
The collector instance is added. The fields specific to the collector appear in the **DETAILS** section.

15. Under **Collector-Specific Configuration**, enter values as described in the following table.

Field	Description
Recovery Time (hours)	<p>Enter the maximum time, in hours, for which the collector will attempt to recover data after the collector is started or when connection between the collector and the ODBC server is re-established. This time is calculated as the duration between the current time and the last known write time.</p> <p>Continuous data collection is resumed only after the previous data has been recovered.</p> <p>By default, this value is set to 0, which means data recovery is not attempted. The maximum value you can provide is 168 hours (that is, 7 days).</p>
Throttle (Milliseconds)	<p>Enter the frequency, in milliseconds, at which you want the ODBC collector to query the ODBC server for tag data. This will minimize the load on the ODBC server. You can enter a value up to 16 hours.</p> <div data-bbox="862 1178 1421 1354" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: If this field is blank, enter the required minimum value of 100 milliseconds.</p> </div>

16. If needed, enter values in [the other sections \(on page 1114\)](#).

17. In the upper-left corner of the page, select **Save**.



The changes to the collector instance are saved.

18. If needed, restart the collector.

Specify the tags whose data you want to collect using the collector. In the **CHOOSE CONFIGURATION** field,

- If you have selected **Historian Configuration**, specify the tags using Configuration Hub (on page 909).
- If you have selected **Offline Configuration**, modify the offline configuration file of the collector. By default, the file is available in the following location: *<installation folder of Historian>\GE Digital\<collector name>*. For information, refer to [creating an offline collection file](#). This option is applicable only if you have selected a cloud destination.

Add and Configure an OPC Classic Alarms and Events Collector

The OPC Classic Alarms and Events collector collects alarms and events data from any OPC 1.0 or OPC 2.0 compliant OPC server.

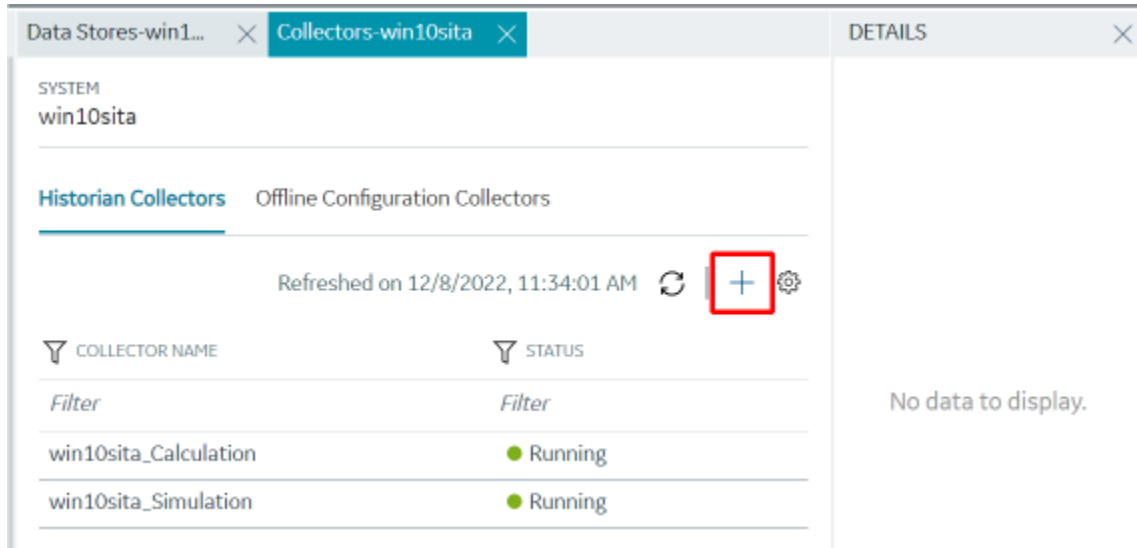
You can create an OPC Alarms and Events collector only for an on-premises Historian server, not for a cloud destination.

This topic describes how to add a collector instance using Configuration Hub. You can also [add a collector instance using the RemoteCollectorConfigurator utility](#), which does not require you to install Web-based Clients.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.
A list of collectors in the default system appears.
3. If needed, select the system in which you want to add a collector instance.

SYSTEM			
WIN10TECH			
Refreshed on 2021-12-21 16:10:40			
COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

4. In the upper-right corner of the main section, select **+**.



The **Add Collector Instance: <system name>** window appears, displaying the **Collector Selection** section. The **MACHINE NAME** field contains a list of machines on which you have installed collectors.

5. In the **MACHINE NAME** field, select the machine in which you want to add a collector instance.
6. In the **COLLECTOR TYPE** field, select **OPC Alarms and Events Collector**, and then select **Get Details**.

The **INSTALLATION DRIVE** and **DATA DIRECTORY** fields are disabled and populated.

7. Select **Next**.

The **Source Configuration** section appears.

8. In the **OPC A&E SERVER** field, enter the host name or IP address of the OPC server from which you want to collect alarms and events data.
9. Select **Next**.

The **Destination Configuration** section appears. Under **CHOOSE DESTINATION**, the **Historian Server** option is selected by default; the other options are disabled. In addition, the **DESTINATION HISTORIAN SERVER** field is disabled and populated.

10. In the **USERNAME** and **PASSWORD** fields, enter the credentials to access the destination Historian server. Values are required only for a remote Historian server.
11. Select **Next**.

The **Collector Initiation** section appears.

12. If needed, modify the value in the **COLLECTOR NAME** field.

The value that you enter:

- Must be unique.
- Must not exceed 15 characters.
- Must not contain a space.
- Must not contain special characters except a hyphen, period, and an underscore.

13. In the **RUNNING MODE** field, select one of the following options.

- **Service - Local System Account:** Select this option if you want to run the collector as a Windows service using the credentials of the local user (that is, the currently logged-in user). If you select this option, the **USERNAME** and **PASSWORD** fields are disabled.
- **Service Under Specific User Account:** Select this option if you want to run the collector as a Windows service using a specific user account. If you select this option, you must enter values in the **USERNAME** and **PASSWORD** fields.

If you have enabled the **Enforce Strict Collector Authentication** option in Historian Administrator, you must provide the credentials of a user who is added to at least one of the following security groups:

- iH Security Admins
- iH Collector Admins
- iH Tag Admins

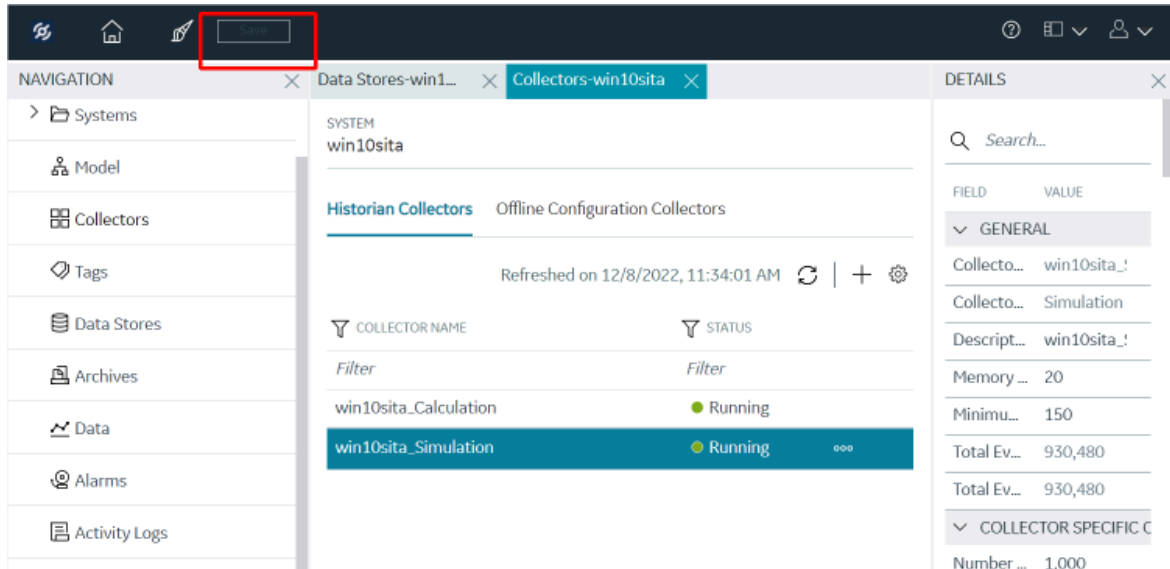
You can also configure the collector to start automatically when you start the computer.

14. Select **Add**.

The collector instance is added. The fields specific to the collector section appear in the **DETAILS** section.

15. If needed, enter values in [the available sections \(on page 1114\)](#).

16. In the upper-left corner of the page, select **Save**.



The changes to the collector instance are saved.

17. If needed, restart the collector.

[Specify the tags \(on page 909\)](#) whose data you want to collect using the collector.

Add and Configure an OPC Classic Data Access Collector

The OPC Classic Data Access (DA) collector collects data from any OPC 1.0 or OPC 2.0 compliant OPC Classic server. For more information, refer to [Overview of the OPC Classic DA Collector](#).


This topic describes how to add a collector instance using Configuration Hub. You can also [add a collector instance using the RemoteCollectorConfigurator utility](#), which does not require you to install Web-based Clients.







1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.

A list of collectors in the default system appears.

3. If needed, select the system in which you want to add a collector instance.

SYSTEM			
WIN10TECH			
Refreshed on 2021-12-21 16:10:40			
COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

4. In the upper-right corner of the main section, select .

Data Stores-win1... 		Collectors-win10sita 	DETAILS 
SYSTEM		win10sita	
Historian Collectors		Offline Configuration Collectors	
		Refreshed on 12/8/2022, 11:34:01 AM	
		  	
COLLECTOR NAME	STATUS	No data to display.	
<i>Filter</i>	<i>Filter</i>		
win10sita_Calculation	Running		
win10sita_Simulation	Running		

The **Add Collector Instance: <system name>** window appears, displaying the **Collector Selection** section. The **MACHINE NAME** field contains a list of machines on which you have installed collectors.

5. In the **MACHINE NAME** field, select the machine in which you want to add a collector instance.
6. In the **COLLECTOR TYPE** field, select **OPC Collector**, and then select **Get Details**.

The **INSTALLATION DRIVE** and **DATA DIRECTORY** fields are disabled and populated.

7. Select **Next**.

The **Source Configuration** section appears.

8. Enter values as described in the following table.

Field	Description
OPC SERVER	Select the machine on which you have installed the OPC Classic DA server from which you want to collect data.
MACHINE NAME	Enter the host name or IP address of the OPC server. This field appears only if you have selected a remote OPC server. A value is required.
OPC DA SERVER PROG ID	Enter the prog ID of the OPC server. This field appears only if you have selected a remote OPC server. A value is required.

9. Select **Next**.

The **Destination Configuration** section appears. Under **CHOOSE DESTINATION**, the **Historian Server** option is selected by default.

10. Select the destination to which you want to send data, and then enter values in the available fields.

You can send data to an on-premises Historian server or to a cloud destination such as [Alibaba Cloud \(on page 1122\)](#), [AWS Cloud \(on page 1127\)](#), [Azure Cloud \(on page 1134\)](#), [Google Cloud \(on page 1148\)](#), or [Predix Cloud \(on page 1154\)](#).

11. Select **Next**.

The **Collector Initiation** section appears. The **COLLECTOR NAME** field is populated with a value in the following format: `<system name>_OPC_<OPC server name>`

12. If needed, modify the value in the **COLLECTOR NAME** field.

The value that you enter:

- Must be unique.
- Must not exceed 15 characters.
- Must not contain a space.
- Must not contain special characters except a hyphen, period, and an underscore.

13. In the **RUNNING MODE** field, select one of the following options.

- **Service - Local System Account:** Select this option if you want to run the collector as a Windows service using the credentials of the local user (that is, the currently logged-in user). By default this option is selected, and the **USERNAME** and **PASSWORD** fields are disabled.
- **Service Under Specific User Account:** Select this option if you want to run the collector as a Windows service using a specific user account. If you select this option, you must enter values in the **USERNAME** and **PASSWORD** fields.

If you have enabled the **Enforce Strict Collector Authentication** option in Historian Administrator, you must provide the credentials of a user who is added to at least one of the following security groups:

- iH Security Admins
- iH Collector Admins
- iH Tag Admins


You can also configure the collector to start automatically when you start the computer.

14. Select **Add**.

The collector instance is added. The fields specific to the collector section appear in the **DETAILS** section.

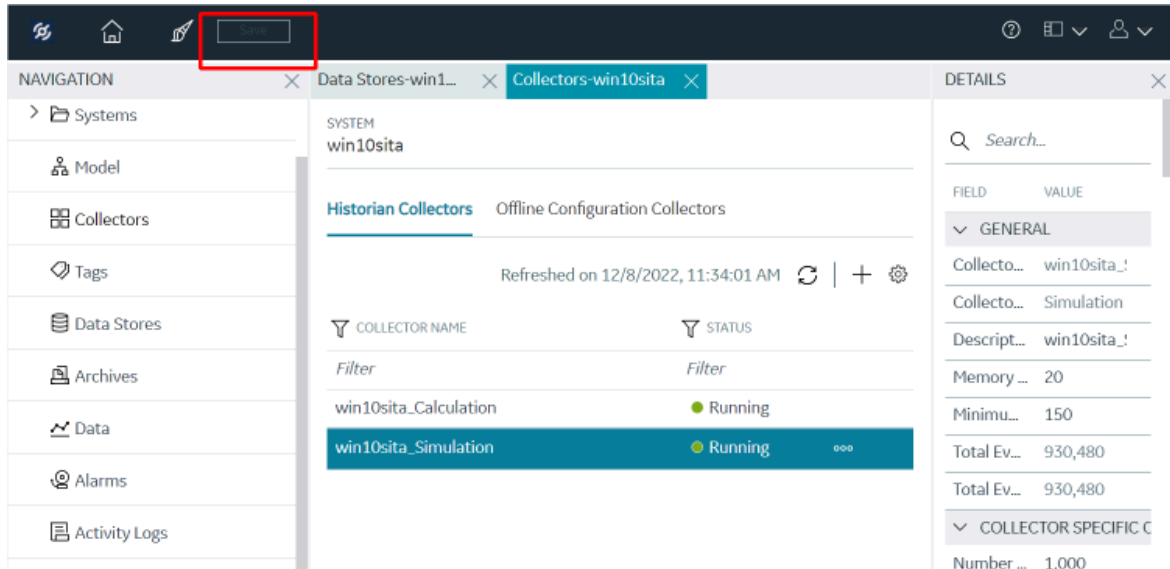
15. Under **Collector-Specific Configuration**, enter values as described in the following table.

Field	Description
OPC Server Prog ID	The program ID of the OPC server from which you want to collect data.
Read Mode	The read mode that you want the collector to use. For information, refer to the documentation of the OPC server that you are using or the OPC specification on the OPC Foundation website.
First Browse Criteria	<p>A comma-separated first-level search criterion for browsing tags from the data source. The top-level and second-level criteria are used together by the AND operation to browse tags.</p> <p>For example, if you enter <code>USGB014</code> in the First Browse Criteria field and <code>F_CV, B_CUALM</code> in the Second Browse Criteria field, it returns all the tags that contain:</p> <ul style="list-style-type: none"> ◦ USGB014 -and- ◦ F_CV or B_CUALM
Second Browse Criteria	A comma-separated second-level search criterion for browsing tags from the data source. The top-level and second-level criteria are used together by the AND operation to browse tags.

Field	Description
Threading Model	<p>The type of the threading model selected for the collector. The model selected must match the threading model of the OPC server.</p> <ul style="list-style-type: none"> ◦ Multithreaded: Select this option for better performance. We recommend that you configure your collector to use the default multi-threading model. ◦ Apparent: Select this option for best compatibility. Some OPC servers do not work well with multi-threading. If you experience problems running your collector with multi-threading, use the apartment model. <p>The default setting is multi-threaded. For information, refer to the documentation of the OPC server you are using.</p>
Configuration Changes	<p>Indicates whether the collector configuration changes are processed in real time or after restarting the collector.</p> <ul style="list-style-type: none"> ◦ Made On-Line: Select this option to process any configuration changes immediately (after 30 seconds) after you select the Update button. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note:</p> <ul style="list-style-type: none"> ▪ Some OPC servers cannot handle processing configuration changes online. If you experience any instability with changes made online, use the next option. </div> <ul style="list-style-type: none"> ◦ Made After Collector Restart: Select this option to hold all configuration changes until you manually restart the collector.

16. If needed, enter values in [the other sections \(on page 1114\)](#).

17. In the upper-left corner of the page, select **Save**.



The changes to the collector instance are saved.

18. If needed, restart the collector.

Specify the tags whose data you want to collect using the collector. In the **CHOOSE CONFIGURATION** field,

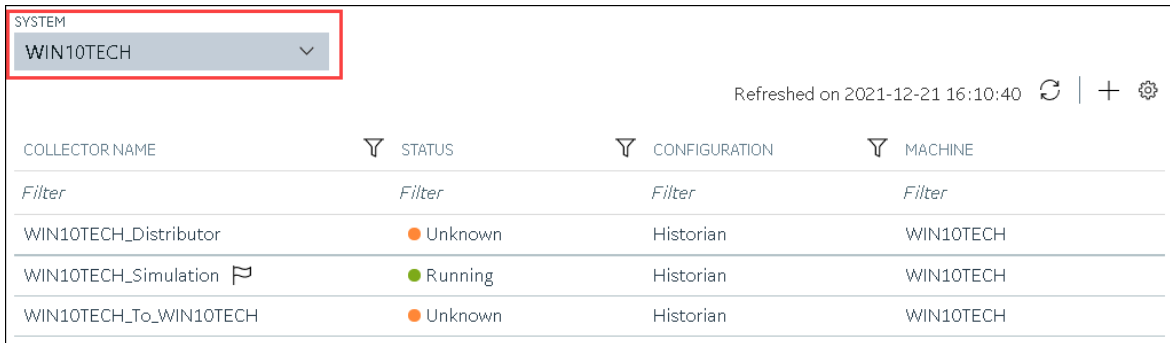
- If you have selected **Historian Configuration**, [specify the tags for data collection \(on page 909\)](#).
- If you have selected **Offline Configuration**, modify the offline configuration file of the collector. By default, the file is available in the following location: `<installation folder of Historian>\GE Digital\<collector name>`. For information, refer to [Offline Configuration for Collectors](#). This option is applicable only if you have selected a cloud destination.

Add and Configure an OPC Classic HDA Collector

The OPC Classic Historical Data Access (HDA) collector collects data from any OPC HDA 1.2 - compliant OPC Classic HDA server. For more information, refer to [Configure the OPC Classic HDA Collector Using Historian Administrator](#)..

This topic describes how to add a collector instance using Configuration Hub. You can also [add a collector instance using the RemoteCollectorConfigurator utility](#), which does not require you to install Web-based Clients.

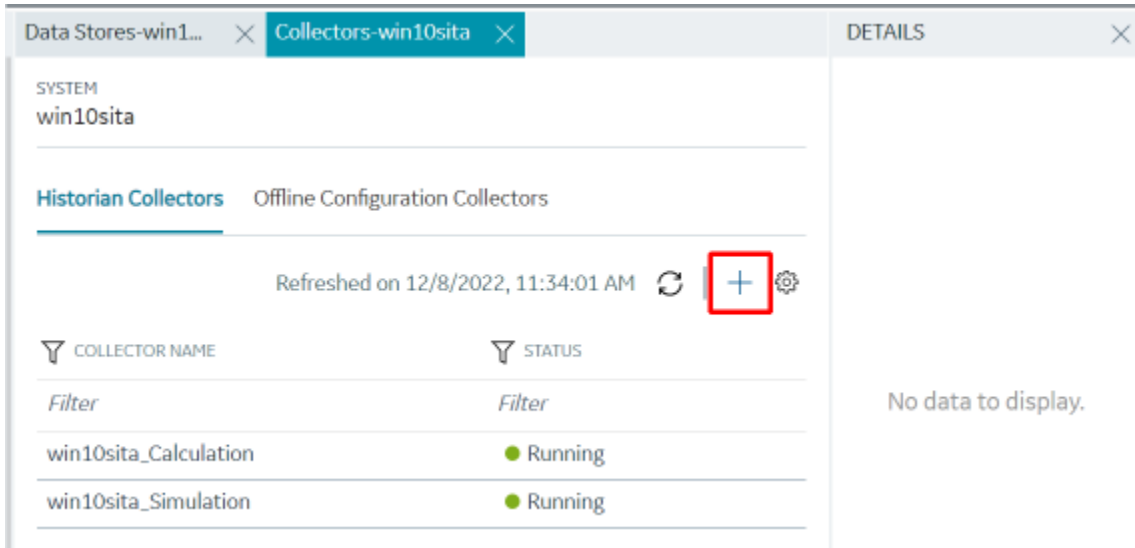
1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.
3. If needed, select the system in which you want to add a collector instance.



The screenshot shows a web interface for managing collectors. At the top left, there is a dropdown menu labeled 'SYSTEM' with 'WIN10TECH' selected. To the right, it says 'Refreshed on 2021-12-21 16:10:40' with refresh, add, and settings icons. Below this is a table with columns: COLLECTOR NAME, STATUS, CONFIGURATION, and MACHINE. Each column has a filter icon and the word 'Filter' below it. The table contains three rows of data.

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

4. In the upper-right corner of the main section, select **+**.



The **Add Collector Instance: <system name>** window appears, displaying the **Collector Selection** section. The **MACHINE NAME** field contains a list of machines on which you have installed collectors.

5. In the **MACHINE NAME** field, select the machine in which you want to add a collector instance.
6. In the **COLLECTOR TYPE** field, select **OPC HDA Collector**, and then select **Get Details**.

The **INSTALLATION DRIVE** and **DATA DIRECTORY** fields are disabled and populated.

7. Select **Next**.

The **Source Configuration** section appears.

8. Enter values as described in the following table.

Field	Description
OPC HDA SERVER	Select the machine on which you have installed the OPC Classic HDA server from which you want to collect data.
MACHINE NAME	Enter the host name or IP address of the OPC server. This field appears only if you have selected a remote OPC server. A value is required.

Field	Description
OPC DA SERVER PROG ID	Enter the prog ID of the OPC server. This field appears only if you have selected a remote OPC server. A value is required.

9. Select **Next**.

The **Destination Configuration** section appears. Under **CHOOSE DESTINATION**, the **Historian Server** option is selected by default.

10. Select the destination to which you want to send data, and then enter values in the available fields.

You can send data to an on-premises Historian server or to a cloud destination such as [Alibaba Cloud \(on page 1122\)](#), [AWS Cloud \(on page 1127\)](#), [Azure Cloud \(on page 1134\)](#), [Google Cloud \(on page 1148\)](#), or [Predix Cloud \(on page 1154\)](#).

11. Select **Next**.

The **Collector Initiation** section appears.

12. If needed, modify the value in the **COLLECTOR NAME** field.

The value that you enter:

- Must be unique.
- Must contain the string `OPCHDA`.
- Must not exceed 15 characters.
- Must not contain a space.
- Must not contain special characters except a hyphen, period, and an underscore.

13. In the **RUNNING MODE** field, select one of the following options.

- **Service - Local System Account:** Select this option if you want to run the collector as a Windows service using the credentials of the local user (that is, the currently logged-in user). By default, this option is selected, and the **USERNAME** and **PASSWORD** fields are disabled.
- **Service Under Specific User Account:** Select this option if you want to run the collector as a Windows service using a specific user account. If you select this option, you must enter values in the **USERNAME** and **PASSWORD** fields.

If you have enabled the **Enforce Strict Collector Authentication** option in Historian Administrator, you must provide the credentials of a user who is added to at least one of the following security groups:

- iH Security Admins
- iH Collector Admins
- iH Tag Admins

You can also configure the collector to start automatically when you start the computer.

14. Select **Add**.

The collector instance is added. The fields specific to the collector section appear in the **DETAILS** section.

15. If needed, under **Collector-Specific Configuration**, modify the value in the **Recovery Time** field.

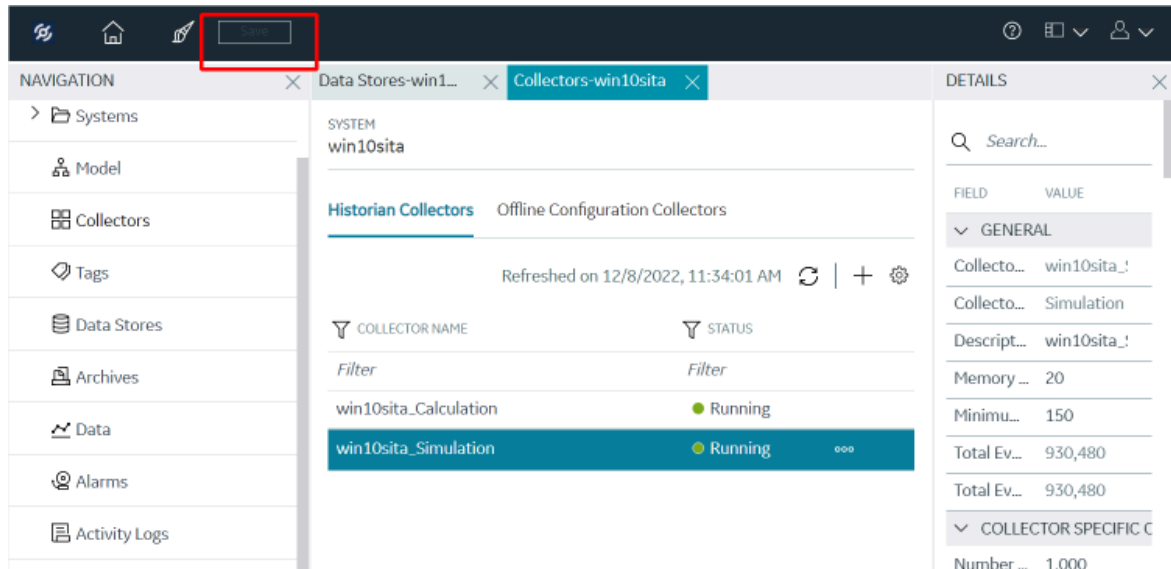
It indicates the maximum time, in hours, for which the collector will attempt to recover data after the collector is started or when connection between the collector and the OPC server is re-established. This time is calculated as the duration between the current time and the last known write time.

Continuous data collection is resumed only after the previous data has been recovered.

You can enter a value between 1 and 150.

16. If needed, enter values in [the other sections \(on page 1114\)](#).

17. In the upper-left corner of the page, select **Save**.



The changes to the collector instance are saved.

18. If needed, restart the collector.

Specify the tags whose data you want to collect using the collector. In the **CHOOSE CONFIGURATION** field,

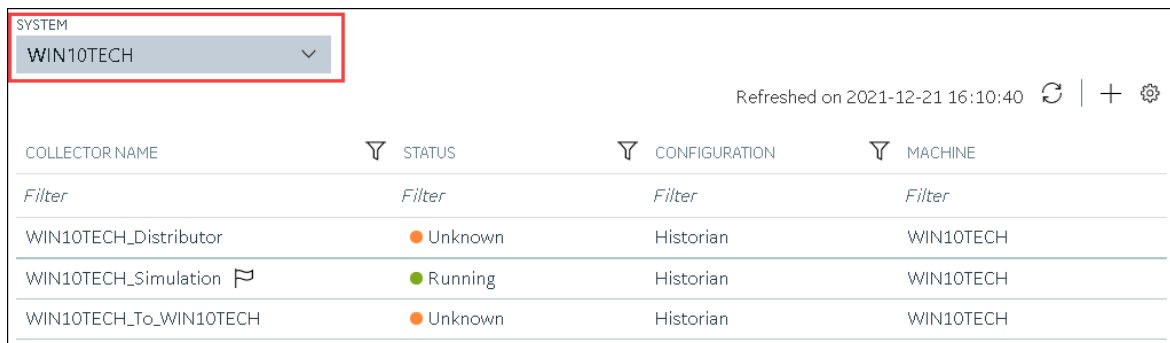
- If you have selected **Historian Configuration**, specify the tags using [Configuration Hub \(on page 909\)](#).
- If you have selected **Offline Configuration**, modify the offline configuration file of the collector. By default, the file is available in the following location: *<installation folder of Historian>\GE Digital\<collector name>*. For information, refer to [Offline Configuration for Collectors](#). This option is applicable only if you have selected a cloud destination.

Add and Configure an OPC UA Data Access Collector

The OPC UA Data Access (DA) collector gathers and collects data from a OPC UA 1.0-compliant OPC UA DA server. For more information, refer to [Configure an OPC UA DA Collector Using Historian Administrator](#).

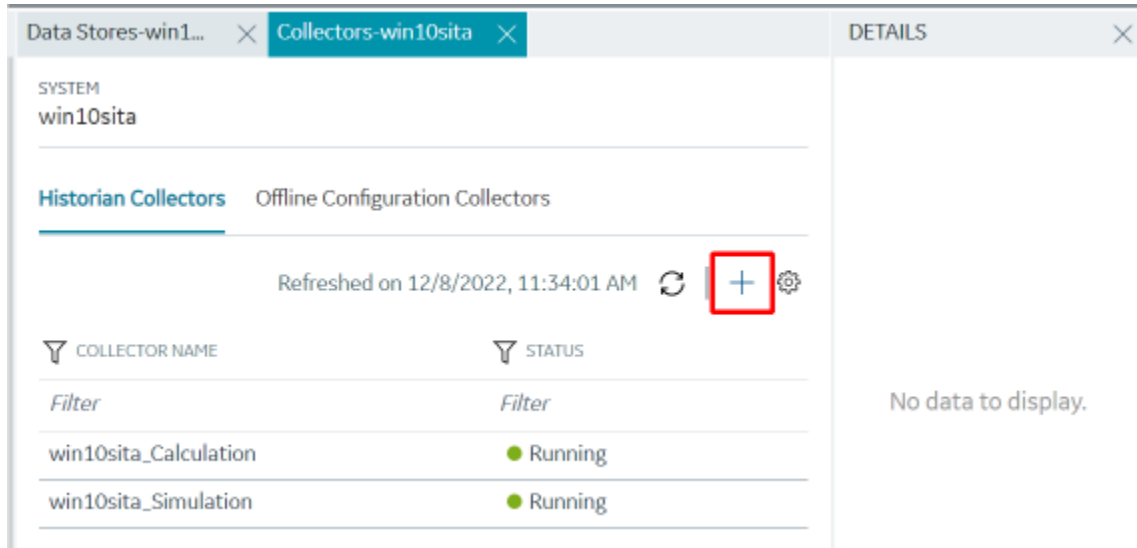
This topic describes how to add a collector instance using Configuration Hub. You can also [add a collector instance using the RemoteCollectorConfigurator utility](#), which does not require you to install Web-based Clients.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**. A list of collectors in the default system appears.
3. If needed, select the system in which you want to add a collector instance.



COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

4. In the upper-right corner of the main section, select **+**.



The **Add Collector Instance: <system name>** window appears, displaying the **Collector Selection** section. The **MACHINE NAME** field contains a list of machines on which you have installed collectors.

5. In the **MACHINE NAME** field, select the machine in which you want to add a collector instance.
6. In the **COLLECTOR TYPE** field, select **OPC UA DA Collector**, and then select **Get Details**.

The **INSTALLATION DRIVE** and **DATA DIRECTORY** fields are disabled and populated.

7. Select **Next**.

The **Source Configuration** section appears.

8. In the **OPC UA SERVER URI** field, enter the URI to connect to the OPC server in the following format:

`opc.tcp://<host name or IP address of the OPC UA server>:<port number>`

9. Select **Next**.

The **Destination Configuration** section appears. Under **CHOOSE DESTINATION**, the **Historian Server** option is selected by default.

10. Select the destination to which you want to send data, and then enter values in the available fields.

You can send data to an on-premises Historian server or to a cloud destination such as [Alibaba Cloud \(on page 1122\)](#), [AWS Cloud \(on page 1127\)](#), [Azure Cloud \(on page 1134\)](#), [Google Cloud \(on page 1148\)](#), or [Predix Cloud \(on page 1154\)](#).

11. Select **Next**.

The **Collector Initiation** section appears. The **COLLECTOR NAME** field is populated with a value in the following format: `<Historian server name>_OPCUACollector_<number>`

12. If needed, modify the value in the **COLLECTOR NAME** field.

The value that you enter:

- Must be unique.
- Must contain the string `OPCUACollector`.
- Must not exceed 15 characters.
- Must not contain a space.
- Must not contain special characters except a hyphen, period, and an underscore.

13. In the **RUNNING MODE** field, select one of the following options.

- **Service - Local System Account:** Select this option if you want to run the collector as a Windows service using the credentials of the local user (that is, the currently logged-in user). If you select this option, the **USERNAME** and **PASSWORD** fields are disabled.
- **Service Under Specific User Account:** Select this option if you want to run the collector as a Windows service using a specific user account. If you select this option, you must enter values in the **USERNAME** and **PASSWORD** fields.

If you have enabled the **Enforce Strict Collector Authentication** option in Historian Administrator, you must provide the credentials of a user who is added to at least one of the following security groups:

- iH Security Admins
- iH Collector Admins
- iH Tag Admins

You can also configure the collector to start automatically when you start the computer.

14. Select **Add**.

The collector instance is added. The fields specific to the collector section appear in the **DETAILS** section.

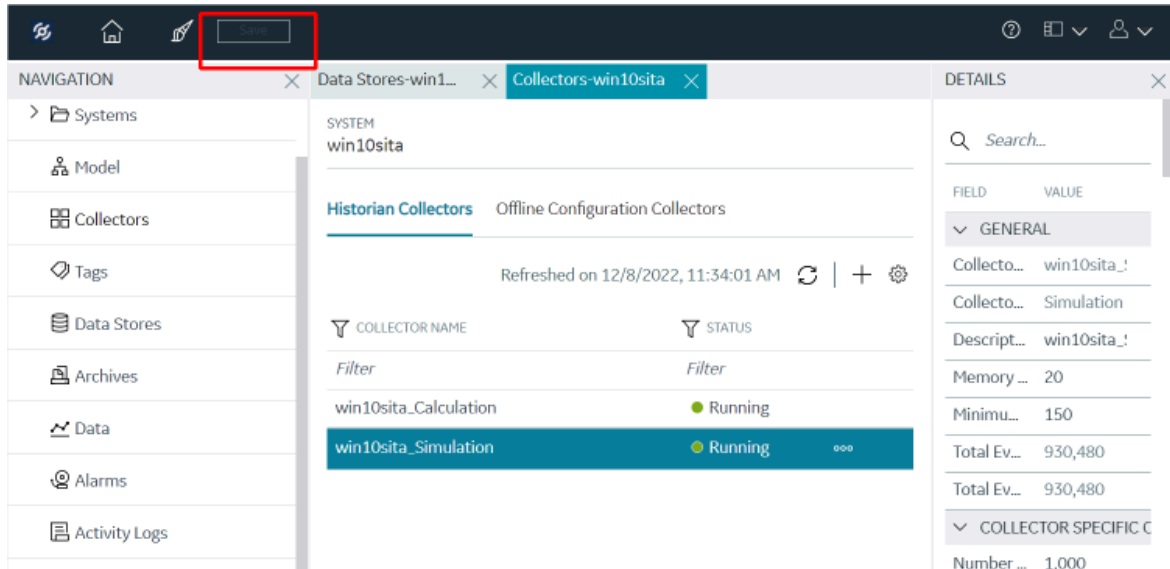
15. Under **Collector-Specific Configuration**, enter values as described in the following table.

Field	Description
OPC UA Server URL	The URI to connect to the OPC UA server. Enter a value in the following format: <code>opc.tcp://<host name or IP address of the OPC UA server>:<port number></code>
Secured Connectivity	Indicates whether you want a secured connection between the OPC UA server and the collector. By default, this field is set to false. You can establish a secured connectivity in one of the following ways:

Field	Description
	<ul style="list-style-type: none"> ◦ Using certificates: To use certificates, switch off the User Security toggle. ◦ Using user authentication: To use user authentication, switch on the User Security toggle.
User Security	<p>This field is enabled only if you have enabled secured connectivity. Switch on this toggle if you want to use user authentication to connect to the OPC server. When you do so, the User Name and Password fields are enabled. You can either enter the user credentials in these fields, or you can use the values in the <code>ClientConfig.ini</code> file. For instructions, refer to Connect with the OPC UA DA Server Securely.</p>
Username	<p>This field is enabled only if you have set the secured connectivity to true and switched on the User Security toggle. Enter the username that you want to use to connect to the OPC server. If you do not provide a value, the username from the <code>ClientConfig.ini</code> file is considered.</p>
Password	<p>This field is enabled only if you have set the secured connectivity to true and selected the Enable User Security check box. Enter the password that you want to use to connect to the OPC server. If you do not provide a value, the password from the <code>ClientConfig.ini</code> file is considered.</p>

16. If needed, enter values in [the other sections \(on page 1114\)](#).

17. In the upper-left corner of the page, select **Save**.



The changes to the collector instance are saved.

18. If needed, restart the collector.

If you have enabled secured connection, [establish a secured connection between the OPC server and the collector](#).

Add and Configure an OSI PI Collector

Install PI AF SDK version 2.7.5 or later.

The OSI PI collector collects data from an OSI PI server. For more information, refer to [Overview of the OSI PI Collector](#).

This topic describes how to add a collector instance using Configuration Hub. You can also [add a collector instance using the RemoteCollectorConfigurator utility](#), which does not require you to install Web-based Clients.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.
A list of collectors in the default system appears.
3. If needed, select the system in which you want to add a collector instance.

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

4. In the upper-right corner of the main section, select **+**.

COLLECTOR NAME	STATUS
<i>Filter</i>	<i>Filter</i>
win10sita_Calculation	Running
win10sita_Simulation	Running

The **Add Collector Instance: <system name>** window appears, displaying the **Collector Selection** section. The **MACHINE NAME** field contains a list of machines on which you have installed collectors.

5. In the **MACHINE NAME** field, select the machine in which you want to add a collector instance.
6. In the **COLLECTOR TYPE** field, select **OSI PI Collector**, and then select **Get Details**.

The **INSTALLATION DRIVE** and **DATA DIRECTORY** fields are disabled and populated.

7. Select **Next**.

The **Source Configuration** section appears.

8. Enter values as described in the following table.

Field	Description
PI SERVER	Enter the host name or IP address of the OSI PI server from which you want to collect data. A value is required.
PI USERNAME	Enter the username to connect to the OSI PI server.
PI PASSWORD	Enter the password to connect to the OSI PI server.

9. Select **Next**.

The **Destination Configuration** section appears. Under **CHOOSE DESTINATION**, the **Historian Server** option is selected by default.

10. Select the destination to which you want to send data, and then enter values in the available fields.

You can send data to an on-premises Historian server or to a cloud destination such as [Alibaba Cloud](#), [AWS Cloud](#), [Azure Cloud](#), [Google Cloud](#), or [Predix Cloud](#).

11. Select **Next**.

The **Collector Initiation** section appears. The **COLLECTOR NAME** field is populated with a value in the following format: `<host name or IP address of the PI server>_PICollector`

12. If needed, modify the value in the **COLLECTOR NAME** field.

The value that you enter:

- Must be unique.
- Must not exceed 15 characters.
- Must not contain a space.
- Must not contain special characters except a hyphen, period, and an underscore.

13. In the **RUNNING MODE** field, select one of the following options.

- **Service - Local System Account:** Select this option if you want to run the collector as a Windows service using the credentials of the local user (that is, the currently logged-in user). By default, this option is selected, and the **USERNAME** and **PASSWORD** fields are disabled.
- **Service Under Specific User Account:** Select this option if you want to run the collector as a Windows service using a specific user account. If you select this option, you must enter values in the **USERNAME** and **PASSWORD** fields.

If you have enabled the **Enforce Strict Collector Authentication** option in Historian Administrator, you must provide the credentials of a user who is added to at least one of the following security groups:

- iH Security Admins
- iH Collector Admins
- iH Tag Admins

You can also configure the collector to start automatically when you start the computer.

14. Select **Add**.

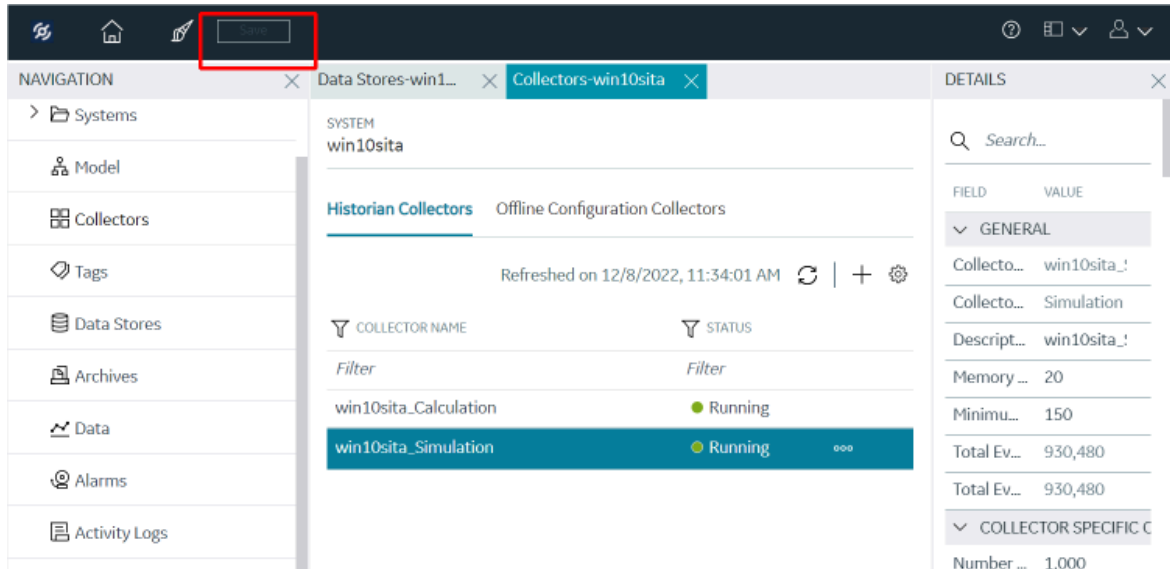
The collector instance is added. The fields specific to the collector appear in the **DETAILS** section.

15. Under **Collector Specific Configuration**, enter values in the following table.

Field	Description
Max Recovery Time (hours)	<p>Enter the maximum time, in hours, for which the collector will attempt to recover data after the collector is started or when connection between the collector and the OSI PI server is re-established. This time is calculated as the duration between the current time and the last known write time.</p> <p>Continuous data collection is resumed only after the previous data has been recovered.</p> <p>The default value is 4 hours.</p>
Data Source	<p>Specify whether you want to collect data from PI archive or PI snapshot:</p> <ul style="list-style-type: none"> ◦ Archive: Stores timeseries-based data. ◦ Snapshot: Stores the most recent values of tags.

16. If needed, enter values in [available fields \(on page 1114\)](#).

17. In the upper-left corner of the page, select **Save**.



The changes to the collector instance are saved.

18. If needed, restart the collector.

Specify the tags whose data you want to collect using the collector. In the **CHOOSE CONFIGURATION** field,

- If you have selected **Historian Configuration**, specify the tags using Configuration Hub (on page 909).
- If you have selected **Offline Configuration**, modify the offline configuration file of the collector. By default, the file is available in the following location: `<installation folder of Historian>\GE Digital\<collector name>`. For information, refer to [offline configuration](#). This option is applicable only if you have selected a cloud destination.

Add and Configure an OSI PI Distributor

Install PI AF SDK version 2.7.5 or later.

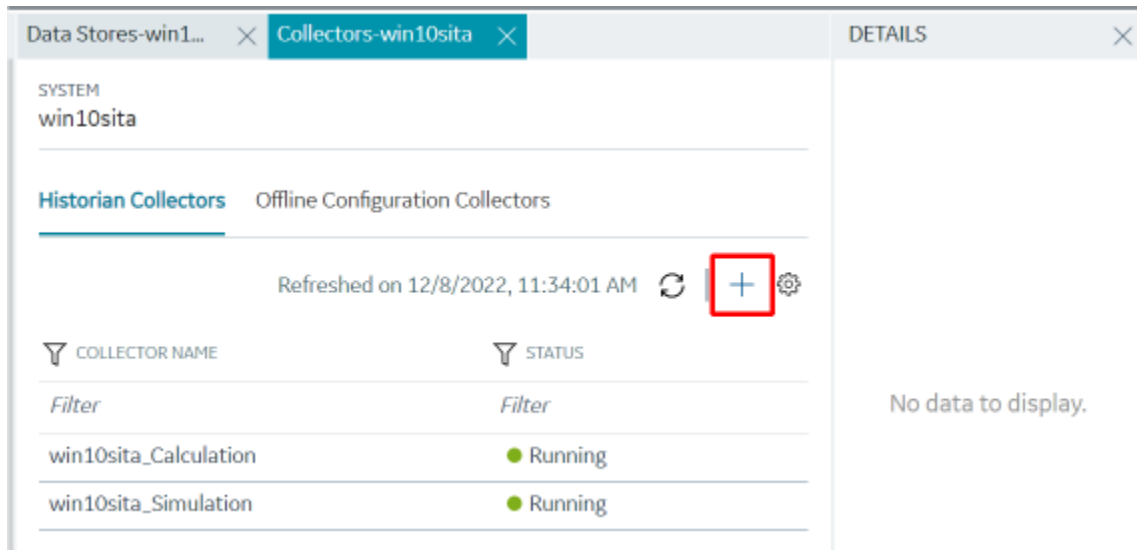
An OSI PI distributor collects data from a Historian server and sends it to an OSI PI server. For more information, refer to [Overview of the OSI PI Distributor](#).

This topic describes how to add a collector instance using Configuration Hub. You can also [add a collector instance using the RemoteCollectorConfigurator utility](#), which does not require you to install Web-based Clients.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.
A list of collectors in the default system appears.
3. If needed, select the system in which you want to add a collector instance.

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

4. In the upper-right corner of the main section, select **+**.



The **Add Collector Instance: <system name>** window appears, displaying the **Collector Selection** section. The **MACHINE NAME** field contains a list of machines on which you have installed collectors.

5. In the **MACHINE NAME** field, select the machine in which you want to add a collector instance.
6. In the **COLLECTOR TYPE** field, select **OSI PI Distributor Collector**, and then select **Get Details**.
The **INSTALLATION DRIVE** and **DATA DIRECTORY** fields are disabled and populated.
7. Select **Next**.

The **Source Configuration** section appears.

8. Enter values as described in the following table.

Field	Description
HISTORIAN SOURCE SERVER	Enter the host name or IP address of the Historian server from which you want to collect data. A value is required.
USERNAME	Enter the username to connect to the Historian server. A value is required.
PASSWORD	Enter the password to connect to the Historian server. A value is required.

9. Select **Next**.

The **Destination Configuration** section appears. Under **CHOOSE DESTINATION**, the **PI Server** option is selected by default; the other options are disabled.

10. Enter values as described in the following table.

Field	Description
PI SERVER	Enter the host name or IP address of the OSI PI server to which you want to send data. A value is required.
PI USERNAME	Enter the username to connect to the OSI PI server.
PI PASSWORD	Enter the password to connect to the OSI PI server.

11. Select **Next**.

The **Collector Initiation** section appears.

12. If needed, modify the value in the **COLLECTOR NAME** field.

The value that you enter:

- Must be unique.
- Must not exceed 15 characters.
- Must not contain a space.
- Must not contain special characters except a hyphen, period, and an underscore.

13. In the **RUNNING MODE** field, select one of the following options.

- **Service - Local System Account:** Select this option if you want to run the collector as a Windows service using the credentials of the local user (that is, the currently logged-in user). By default, this option is selected, and the **USERNAME** and **PASSWORD** fields are disabled.
- **Service Under Specific User Account:** Select this option if you want to run the collector as a Windows service using a specific user account. If you select this option, you must enter values in the **USERNAME** and **PASSWORD** fields.

If you have enabled the **Enforce Strict Collector Authentication** option in Historian Administrator, you must provide the credentials of a user who is added to at least one of the following security groups:

- iH Security Admins
- iH Collector Admins
- iH Tag Admins

You can also configure the collector to start automatically when you start the computer.

14. Select **Add**.

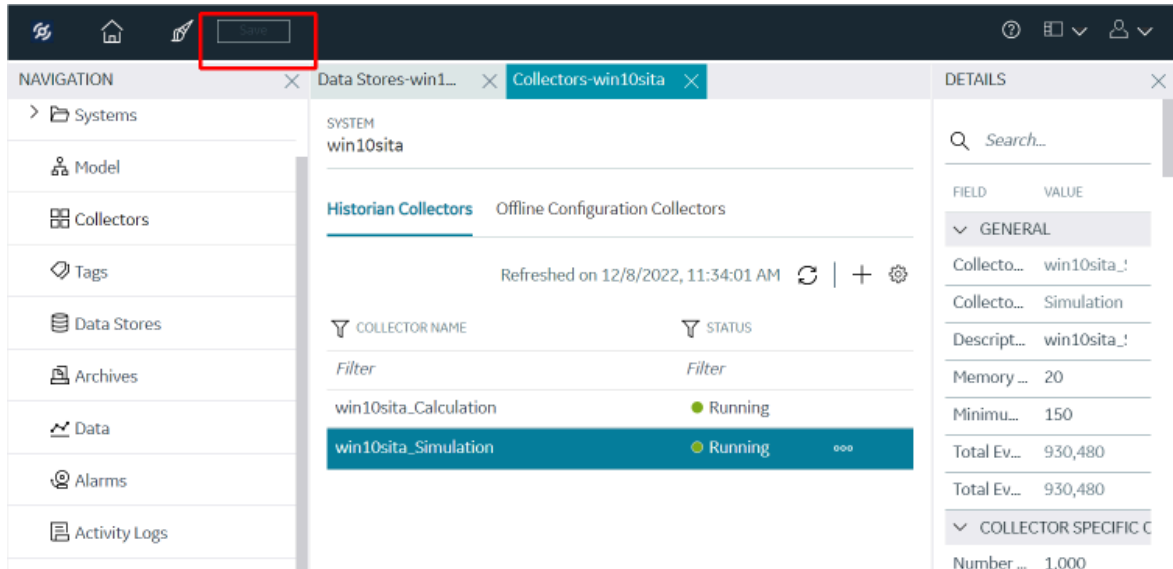
The collector instance is added. The fields specific to the collector instance appear in the **DETAILS** section.

15. Under **Collector Specific Configuration**, enter values in the following table.

Field	Description
Max Recovery Time (hours)	<p>Enter the maximum time, in hours, for which the collector will attempt to recover data after the collector is started or when connection between the collector and the OSI PI server is re-established. This time is calculated as the duration between the current time and the last known write time.</p> <p>Continuous data collection is resumed only after the previous data has been recovered.</p> <p>The default value is 4 hours.</p>
Data Source	<p>Specify whether you want to collect data from PI archive or PI snapshot:</p> <ul style="list-style-type: none"> ◦ Archive: Stores timeseries-based data. ◦ Snapshot: Stores the most recent values of tags.

16. If needed, enter values in [available fields \(on page 1114\)](#).

17. In the upper-left corner of the page, select **Save**.



The changes to the collector instance are saved.

18. If needed, restart the collector.

[Specify the tags \(on page 909\)](#) whose data you want to collect using the collector.

Add and Configure a Server-to-Server Collector

The Server-to-Server collector collects data and messages from a source Historian server to a destination Historian server or a cloud destination. For more information, refer to [Overview of Server-to-Server Collector](#).

This topic describes how to add a collector instance using Configuration Hub. You can also [add a collector instance using the RemoteCollectorConfigurator utility](#), which does not require you to install Web-based Clients.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.
A list of collectors in the default system appears.
3. If needed, select the system in which you want to add a collector instance.

Refreshed on 2021-12-21 16:10:40

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

4. In the upper-right corner of the main section, select **+**.

Refreshed on 12/8/2022, 11:34:01 AM

COLLECTOR NAME	STATUS
<i>Filter</i>	<i>Filter</i>
win10sita_Calculation	Running
win10sita_Simulation	Running

No data to display.

The **Add Collector Instance: <system name>** window appears, displaying the **Collector Selection** section. The **MACHINE NAME** field contains a list of machines on which you have installed collectors.

5. In the **MACHINE NAME** field, select the machine in which you want to add a collector instance.
6. In the **COLLECTOR TYPE** field, select **Server to Server Collector**, and then select **Get Details**.

The **INSTALLATION DRIVE** and **DATA DIRECTORY** fields are disabled and populated.

7. Select **Next**.

The **Source Configuration** section appears.

8. In the **HISTORIAN SOURCE SERVER** field, enter the host name or IP address of the Historian server from which you want to collect data. By default, the local host name appears.

9. Select **Next**.

The **Destination Configuration** section appears. Under **CHOOSE DESTINATION**, the **Historian Server** option is selected by default. In addition, the **DESTINATION HISTORIAN SERVER** field is disabled and populated.

10. Select the destination to which you want to send data, and then enter values in the available fields.

You can send data to an on-premises Historian server or to a cloud destination such as [Alibaba Cloud](#), [AWS Cloud](#), [Azure Cloud](#), [Google Cloud](#), or [Predix Cloud](#).

11. Select **Next**.

The **Collector Initiation** section appears.

12. If needed, modify the value in the **COLLECTOR NAME** field.

The value that you enter:

- Must be unique.
- Must not exceed 15 characters.
- Must not contain a space.
- Must not contain special characters except a hyphen, period, and an underscore.

13. In the **RUNNING MODE** field, select one of the following options.

- **Service - Local System Account:** Select this option if you want to run the collector as a Windows service using the credentials of the local user (that is, the currently logged-in user). If you select this option, the **USERNAME** and **PASSWORD** fields are disabled.
- **Service Under Specific User Account:** Select this option if you want to run the collector as a Windows service using a specific user account. If you select this option, you must enter values in the **USERNAME** and **PASSWORD** fields.

If you have enabled the **Enforce Strict Collector Authentication** option in Historian Administrator, you must provide the credentials of a user who is added to at least one of the following security groups:

- iH Security Admins
- iH Collector Admins
- iH Tag Admins

You can also configure the collector to start automatically when you start the computer.

14. Select **Add**.

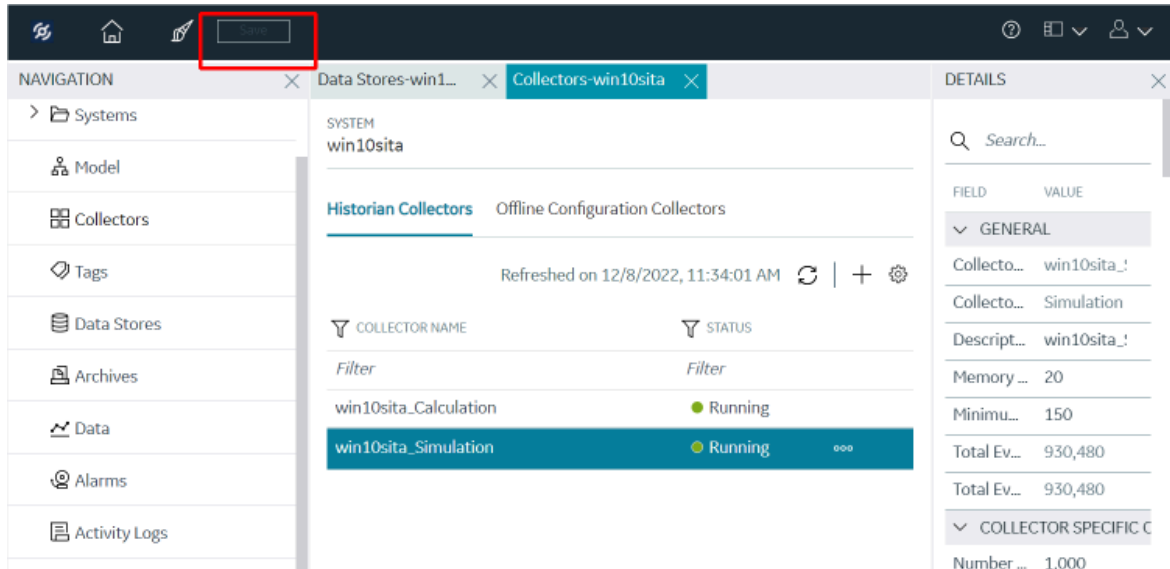
The collector instance is added. The fields specific to the collector section appear in the **DETAILS** section.

15. Under **Collector-Specific Configuration**, enter values as described in the following table.

Field	Description
Alarm Replication	Indicates whether you want to enable or disable alarm replication. If you enable alarm replication, all collected alarm data will be transferred from the source server to the destination server. If you enable alarm replication, you also enable alarm recovery. However, if you set the Max Recovery Time value to zero, alarm recovery does not happen.
Message Replication	Indicates whether you to want to enable or disable message replication. If you enable message replication, messages will be transferred from the source server to the destination server. You can use this data for audits. If you enable message replication, you also enable message recovery. However, if you set the Max Recovery Time value to zero, message recovery does not happen.
Calculation Timeout (sec)	The maximum time allowed for a tag's calculation formula to execute before being terminated. The default value is 10 seconds.
Max Recovery Time (hr)	The maximum duration, in hours, for which the collector will attempt to restore data during recovery logic. The default value is 4 hours.
Add Prefix to Messages	<p>The prefix to identify replicated messages on the destination.</p> <p>Alarms and events data will automatically have a prefix added to it with the following syntax: <code>MachineName_Datasource</code></p> <p>For example, if your alarm is forwarded from the server <code>Almserver12</code> with a data source named <code>OPCAE</code>, the prefix will be <code>Almserver12_OPCAE</code>.</p>

16. If needed, enter values in [the other sections \(on page 1114\)](#).

17. In the upper-left corner of the page, select **Save**.



The changes to the collector instance are saved.

18. If needed, restart the collector.

Specify the tags whose data you want to collect using the collector. In the **CHOOSE CONFIGURATION** field,

- If you have selected **Historian Configuration**, specify the tags using Configuration Hub (on page 909).
- If you have selected **Offline Configuration**, modify the offline configuration file of the collector. By default, the file is available in the following location: `<installation folder of Historian>\GE Digital\<collector name>`. For information, refer to [offline configuration](#). This option is applicable only if you have selected a cloud destination.





Add and Configure a Server-to-Server Distributor


The Server-to-Server distributor is used to send data from a smaller Historian server to a larger, centralized on-premises Historian server or a cloud destination. For more information, refer to [Overview of Server-to-Server Distributor](#).

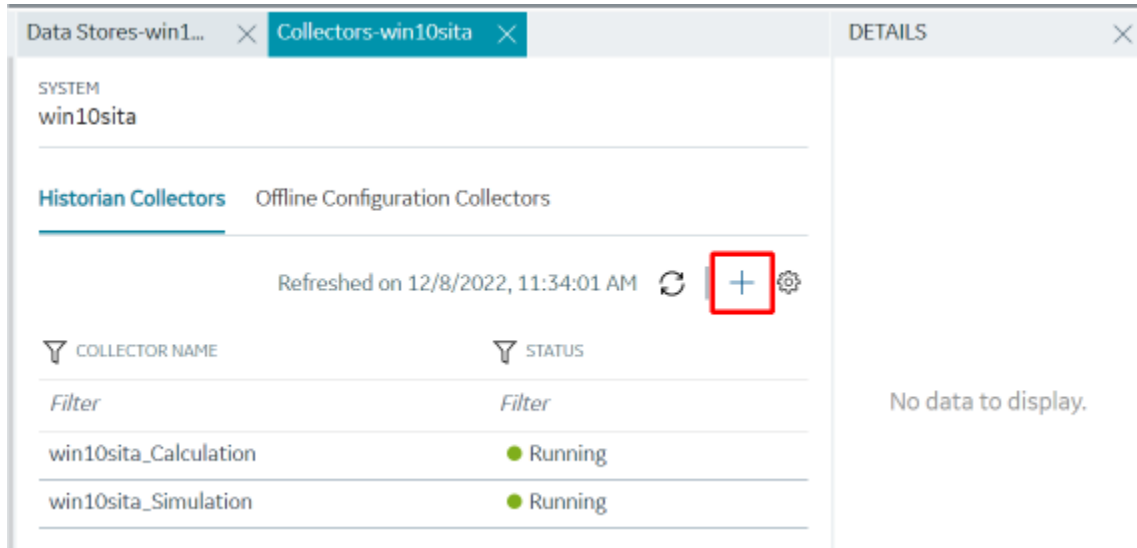
You can use a Server-to-Server distributor only to send data to an on-premises Historian server. If you want to send data to a cloud destination, [use the Server-to-Server collector \(on page 1093\)](#) instead.

This topic describes how to add a collector instance using Configuration Hub. You can also [add a collector instance using the RemoteCollectorConfigurator utility](#), which does not require you to install Web-based Clients.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.
A list of collectors in the default system appears.
3. If needed, select the system in which you want to add a collector instance.

SYSTEM			
COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
Refreshed on 2021-12-21 16:10:40   			
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	● Unknown	Historian	WIN10TECH
WIN10TECH_Simulation 	● Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	● Unknown	Historian	WIN10TECH

4. In the upper-right corner of the main section, select .



The **Add Collector Instance: <system name>** window appears, displaying the **Collector Selection** section. The **MACHINE NAME** field contains a list of machines on which you have installed collectors.

5. In the **MACHINE NAME** field, select the machine in which you want to add a collector instance.
6. In the **COLLECTOR TYPE** field, select **Server to Server Distributor Collector**, and then select **Get Details**.

The **INSTALLATION DRIVE** and **DATA DIRECTORY** fields are disabled and populated.

7. Select **Next**.

The **Source Configuration** section appears.

8. In the **HISTORIAN SOURCE SERVER** field, enter the host name or IP address of the Historian server from which you want to collect data. By default, the local host name appears.
9. Select **Next**.

The **Destination Configuration** section appears. Under **CHOOSE DESTINATION**, the **Historian Server** option is selected by default; the other options are disabled. In addition, the **DESTINATION HISTORIAN SERVER** field is disabled and populated.

10. In the **USERNAME** and **PASSWORD** fields, enter the credentials to access the destination Historian server. Values are required only for a remote Historian server.
11. Select **Next**.

The **Collector Initiation** section appears.

12. If needed, modify the value in the **COLLECTOR NAME** field.

The value that you enter:

- Must be unique.
- Must not exceed 15 characters.
- Must not contain a space.
- Must not contain special characters except a hyphen, period, and an underscore.

13. In the **RUNNING MODE** field, select one of the following options.

- **Service - Local System Account:** Select this option if you want to run the collector as a Windows service using the credentials of the local user (that is, the currently logged-in user). If you select this option, the **USERNAME** and **PASSWORD** fields are disabled.
- **Service Under Specific User Account:** Select this option if you want to run the collector as a Windows service using a specific user account. If you select this option, you must enter values in the **USERNAME** and **PASSWORD** fields.

If you have enabled the **Enforce Strict Collector Authentication** option in Historian Administrator, you must provide the credentials of a user who is added to at least one of the following security groups:

- iH Security Admins
- iH Collector Admins
- iH Tag Admins

You can also configure the collector to start automatically when you start the computer.

14. Select **Add**.

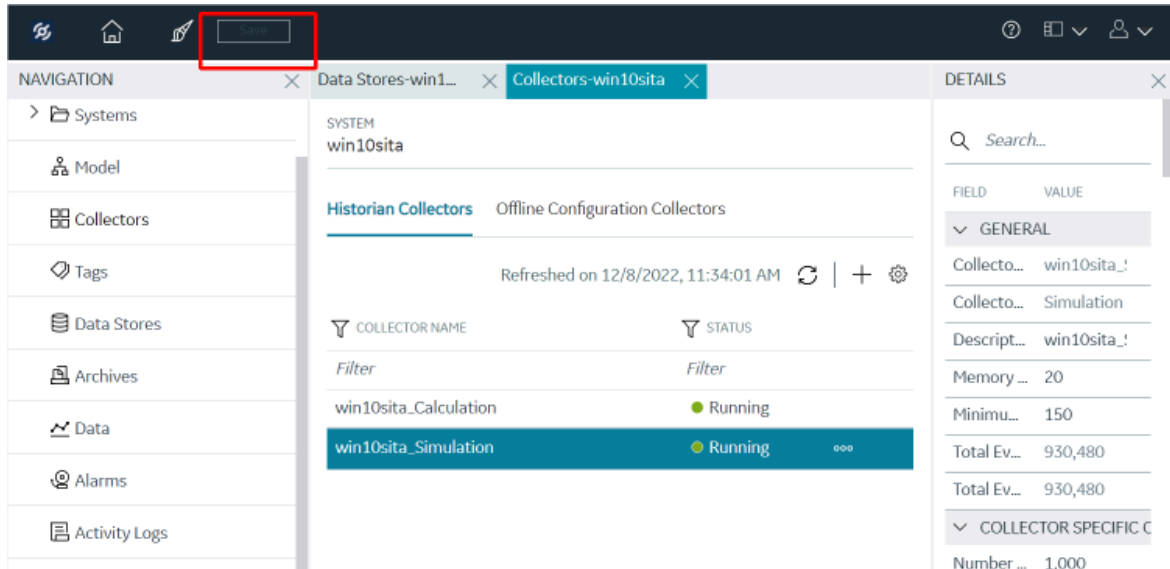
The collector instance is added. The fields specific to the collector section appear in the **DETAILS** section.

15. Under **Collector-Specific Configuration**, enter values as described in the following table.

Field	Description
Alarm Replication	Indicates whether you want to enable or disable alarm replication. If you enable alarm replication, all collected alarm data will be transferred from the source server to the destination server. If you enable alarm replication, you also enable alarm recovery. However, if you set the Max Recovery Time value to zero, alarm recovery does not happen.
Message Replication	Indicates whether you to want to enable or disable message replication. If you enable message replication, you also enable message recovery. However, if you set the Max Recovery Time value to zero, message recovery does not happen.

Field	Description
Calculation Timeout (sec)	The maximum time allowed for a tag's calculation formula to execute before being terminated. The default value is 10 seconds.
Max Recovery Time (hr)	The maximum duration, in hours, for which the collector will attempt to restore data during recovery logic. The default value is 4 hours.
Add Prefix to Messages	<p>The prefix to identify replicated messages on the destination.</p> <p>Alarms and events data will automatically have a prefix added to it with the following syntax:</p> <pre data-bbox="581 657 1421 709">MachineName_Datasource</pre> <p>For example, if your alarm is forwarded from the server <code>Almserver12</code> with a data source named <code>OPCAE</code>, the prefix will be <code>Almserver12_OPCAE</code>.</p>

16. If needed, enter values in [the other sections \(on page 1114\)](#).
17. In the upper-left corner of the page, select **Save**.



The changes to the collector instance are saved.

18. If needed, restart the collector.

[Specify the tags \(on page 909\)](#) whose data you want to collect using the collector.

Add and Configure a Simulation Collector

The Simulation collector generates random numbers and string patterns for demonstration purposes. For more information, refer to [Overview of the Simulation Collector](#).


This topic describes how to add a collector instance using Configuration Hub. You can also [add a collector instance using the RemoteCollectorConfigurator utility](#), which does not require you to install Web-based Clients.


1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.

A list of collectors in the default system appears.

3. If needed, select the system in which you want to add a collector instance.

SYSTEM			
WIN10TECH			
Refreshed on 2021-12-21 16:10:40			
COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

4. In the upper-right corner of the main section, select .

Data Stores-win1...		Collectors-win10sita	DETAILS
SYSTEM		win10sita	
Historian Collectors		Offline Configuration Collectors	
		Refreshed on 12/8/2022, 11:34:01 AM	
			
COLLECTOR NAME	STATUS	No data to display.	
<i>Filter</i>	<i>Filter</i>		
win10sita_Calculation	Running		
win10sita_Simulation	Running		

The **Add Collector Instance: <system name>** window appears, displaying the **Collector Selection** section. The **MACHINE NAME** field contains a list of machines on which you have installed collectors.

5. In the **MACHINE NAME** field, select the machine in which you want to add a collector instance.
6. In the **COLLECTOR TYPE** field, select **Simulation Collector**, and then select **Get Details**.
The **INSTALLATION DRIVE** and **DATA DIRECTORY** fields are disabled and populated.
7. Select **Next**.

The **Source Configuration** section appears. The **COLLECTOR MACHINE NAME** field is disabled and populated.

8. Select **Next**.

The **Destination Configuration** section appears. Under **CHOOSE DESTINATION**, the **Historian Server** option is selected by default. In addition, the **DESTINATION HISTORIAN SERVER** field is disabled and populated.

9. Select the destination to which you want to send data, and then enter values in the available fields. You can send data to an on-premises Historian server or to a cloud destination such as [Alibaba Cloud](#), [AWS Cloud](#), [Azure Cloud](#), [Google Cloud](#), or [Predix Cloud](#).

10. Select **Next**.

The **Collector Initiation** section appears.

11. If needed, modify the value in the **COLLECTOR NAME** field.

The value that you enter:

- Must be unique.
- Must not exceed 15 characters.
- Must not contain a space.
- Must not contain special characters except a hyphen, period, and an underscore.

12. In the **RUNNING MODE** field, select one of the following options.

- **Service - Local System Account:** Select this option if you want to run the collector as a Windows service using the credentials of the local user (that is, the currently logged-in user). If you select this option, the **USERNAME** and **PASSWORD** fields are disabled.
- **Service Under Specific User Account:** Select this option if you want to run the collector as a Windows service using a specific user account. If you select this option, you must enter values in the **USERNAME** and **PASSWORD** fields.

If you have enabled the **Enforce Strict Collector Authentication** option in Historian Administrator, you must provide the credentials of a user who is added to at least one of the following security groups:

- iH Security Admins
- iH Collector Admins
- iH Tag Admins

You can also configure the collector to start automatically when you start the computer.

13. Select **Add**.

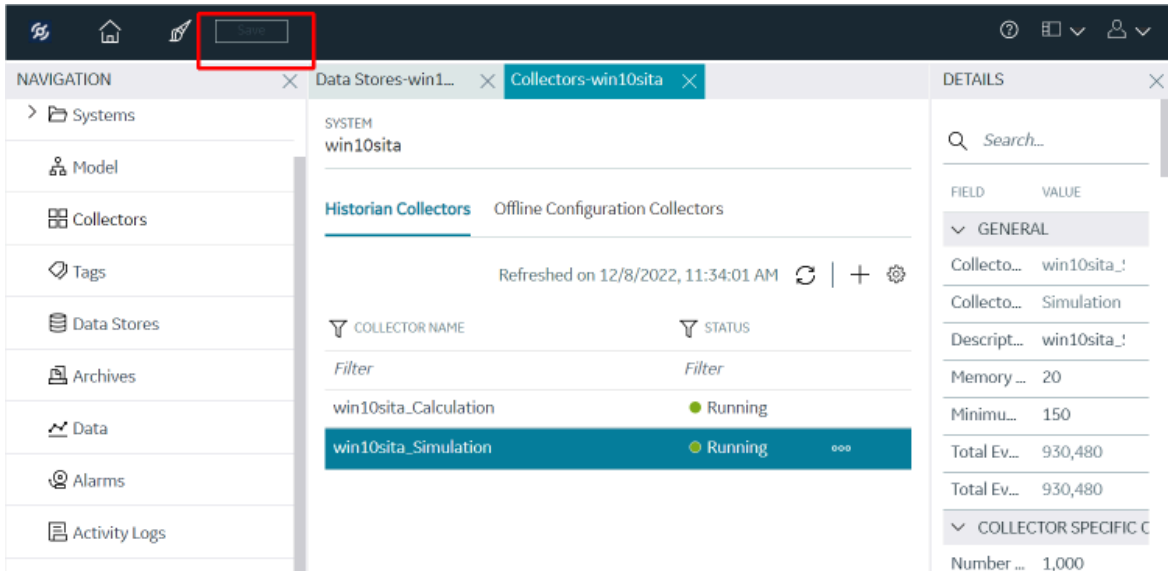
The collector instance is added. The fields specific to the collector section appear in the **DETAILS** section.

14. Under **Collector-Specific Configuration**, enter values as described in the following table.

Field	Description
Number of Tags	The number of Historian tags that you want the create for the collector.
Function Period (seconds)	The period, in seconds, of the <code>SIN</code> , <code>STEP</code> , and <code>RAMP</code> functions implemented in the collector.

15. If needed, enter values in [the other sections \(on page 1114\)](#).

16. In the upper-left corner of the page, select **Save**.



The changes to the collector instance are saved.

17. If needed, restart the collector.

Specify the tags whose data you want to collect using the collector. In the **CHOOSE CONFIGURATION** field,

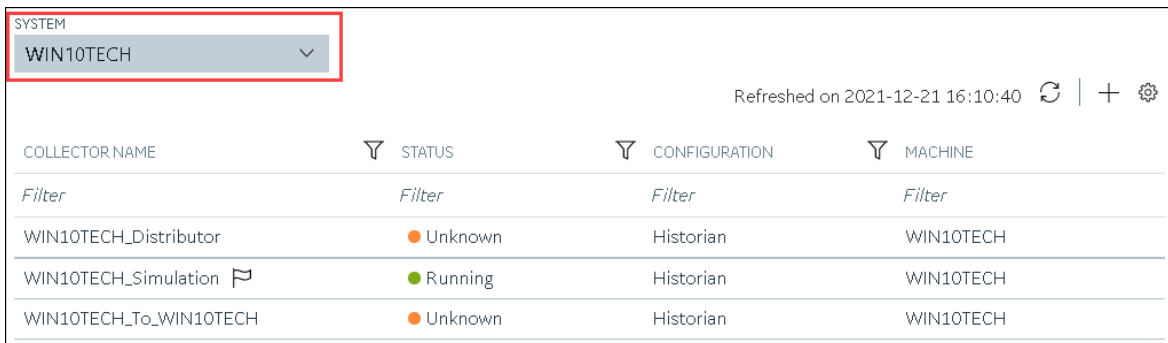
- If you have selected **Historian Configuration**, [specify the tags using Configuration Hub \(on page 909\)](#).
- If you have selected **Offline Configuration**, modify the offline configuration file of the collector. By default, the file is available in the following location: *<installation folder of Historian>\GE Digital\<collector name>*. For information, refer to [offline configuration](#). This option is applicable only if you have selected a cloud destination.

Add and Configure Windows Performance Collector

The Windows Performance collector collects Windows performance counter data. For more information, refer to [Overview of the Windows Performance Collector](#).

This topic describes how to add a collector instance using Configuration Hub. You can also [add a collector instance using the RemoteCollectorConfigurator utility](#), which does not require you to install Web-based Clients.

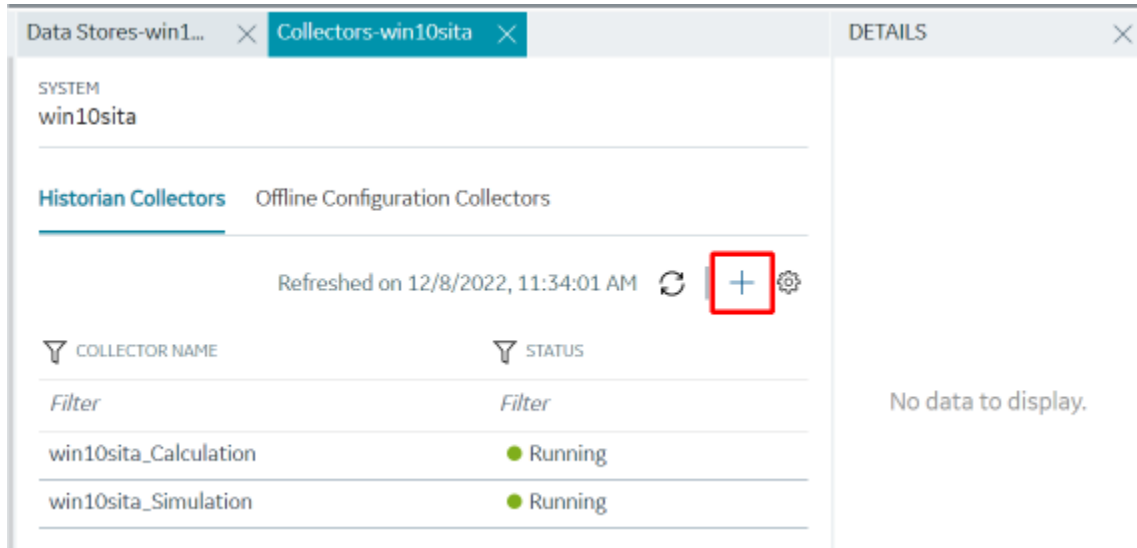
1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**. A list of collectors in the default system appears.
3. If needed, select the system in which you want to add a collector instance.



The screenshot shows a web interface for managing collectors. At the top left, there is a dropdown menu labeled 'SYSTEM' with 'WIN10TECH' selected. To the right, it says 'Refreshed on 2021-12-21 16:10:40' with refresh, add, and settings icons. Below this is a table with columns for Collector Name, Status, Configuration, and Machine. The table contains three rows of data.

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

4. In the upper-right corner of the main section, select **+**.



The **Add Collector Instance: <system name>** window appears, displaying the **Collector Selection** section. The **MACHINE NAME** field contains a list of machines on which you have installed collectors.

5. In the **MACHINE NAME** field, select the machine in which you want to add a collector instance.
6. In the **COLLECTOR TYPE** field, select **Windows Performance Collector**, and then select **Get Details**. The **INSTALLATION DRIVE** and **DATA DIRECTORY** fields are disabled and populated.

7. Select **Next**.

The **Source Configuration** section appears. The **WINDOWS MACHINE NAME** field is disabled and populated.

8. Select **Next**.

The **Destination Configuration** section appears. Under **CHOOSE DESTINATION**, the **Historian Server** option is selected by default.

9. Select the destination to which you want to send data, and then enter values in the available fields.

You can send data to an on-premises Historian server or to a cloud destination such as [Alibaba Cloud](#), [AWS Cloud](#), [Azure Cloud](#), [Google Cloud](#), or [Predix Cloud](#).

10. Select **Next**.

The **Collector Initiation** section appears. The **COLLECTOR NAME** field is populated with a value in the following format: `<Historian server name>_WindowsPerfMon`

11. If needed, modify the value in the **COLLECTOR NAME** field.

The value that you enter:

- Must be unique.
 - Must not exceed 15 characters.
 - Must not contain a space.
 - Must not contain special characters except a hyphen, period, and an underscore.
12. In the **RUNNING MODE** field, select one of the following options.
- **Service - Local System Account:** Select this option if you want to run the collector as a Windows service using the credentials of the local user (that is, the currently logged-in user). By default, this option is selected, and the **USERNAME** and **PASSWORD** fields are disabled.
 - **Service Under Specific User Account:** Select this option if you want to run the collector as a Windows service using a specific user account. If you select this option, you must enter values in the **USERNAME** and **PASSWORD** fields.

If you have enabled the **Enforce Strict Collector Authentication** option in Historian Administrator, you must provide the credentials of a user who is added to at least one of the following security groups:

- iH Security Admins
- iH Collector Admins
- iH Tag Admins

You can also configure the collector to start automatically when you start the computer.

13. Select **Add**.

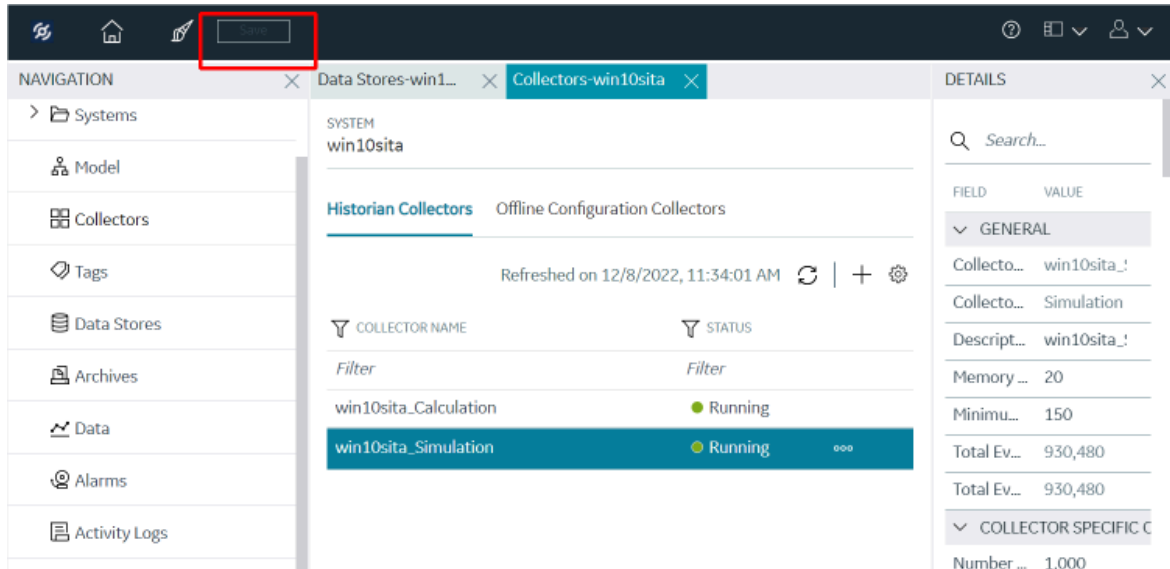
The collector instance is added.

14. Select the collector instance.

The fields specific to the collector section appear in the **DETAILS** section.

15. If needed, enter values in the [available sections \(on page 1114\)](#).

16. In the upper-left corner of the page, select **Save**.



The changes to the collector instance are saved.

17. If needed, restart the collector.

Specify the tags whose data you want to collect using the collector. In the **CHOOSE CONFIGURATION** field,




- If you have selected **Historian Configuration**, specify the tags using Configuration Hub (on page 909).
- If you have selected **Offline Configuration**, modify the offline configuration file of the collector. By default, the file is available in the following location: `<installation folder of Historian>\GE Digital\<collector name>`. For information, refer to [offline configuration](#). This option is applicable only if you have selected a cloud destination.


Add and Configure a Wonderware Collector

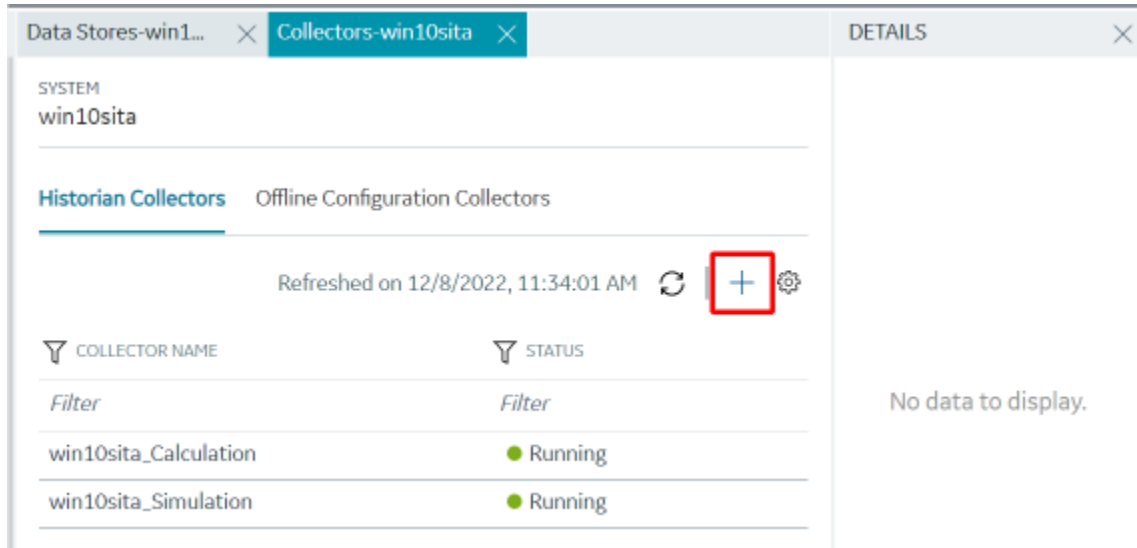
The Wonderware collector gathers data samples from a Wonderware Historian 2014 R2 server and stores it in the Proficy Historian server. For more information, refer to [Overview of the Wonderware Collector](#).

This topic describes how to add a collector instance using Configuration Hub. You can also [add a collector instance using the RemoteCollectorConfigurator utility](#), which does not require you to install Web-based Clients.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.
A list of collectors in the default system appears.
3. If needed, select the system in which you want to add a collector instance.

SYSTEM			
WIN10TECH			
Refreshed on 2021-12-21 16:10:40   			
COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	● Unknown	Historian	WIN10TECH
WIN10TECH_Simulation 	● Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	● Unknown	Historian	WIN10TECH

4. In the upper-right corner of the main section, select  .



The **Add Collector Instance: <system name>** window appears, displaying the **Collector Selection** section. The **MACHINE NAME** field contains a list of machines on which you have installed collectors.

5. In the **MACHINE NAME** field, select the machine in which you want to add a collector instance.
6. In the **COLLECTOR TYPE** field, select **Wonderware Collector**, and then select **Get Details**.

The **INSTALLATION DRIVE** and **DATA DIRECTORY** fields are disabled and populated.

7. Select **Next**.

The **Source Configuration** section appears. The field is disabled and populated.

8. In the **WONDERWARE SERVER** field, enter the host name or IP address of the Wonderware Historian server from which you want to collect data.
9. Enter values in the **USERNAME** and **PASSWORD** fields to connect to the Wonderware Historian server.

10. Select **Next**.

The **Destination Configuration** section appears. Under **CHOOSE DESTINATION**, the **Historian Server** option is selected by default.

11. Select the destination to which you want to send data, and then enter values in the available fields.

You can send data to an on-premises Historian server or to a cloud destination such as [Alibaba Cloud](#), [AWS Cloud](#), [Azure Cloud](#), [Google Cloud](#), or [Predix Cloud](#).

12. Select **Next**.

The **Collector Initiation** section appears. The **COLLECTOR NAME** field is populated with a value in the following format: `<Historian server name>_Wonderware`

13. If needed, modify the value in the **COLLECTOR NAME** field.

The value that you enter:

- Must be unique.
- Must contain the string `Wonderware`.
- Must not exceed 15 characters.
- Must not contain a space.
- Must not contain special characters except a hyphen, period, and an underscore.

14. In the **RUNNING MODE** field, select one of the following options.

- **Service - Local System Account:** Select this option if you want to run the collector as a Windows service using the credentials of the local user (that is, the currently logged-in user). By default, this option is selected, and the **USERNAME** and **PASSWORD** fields are disabled.
- **Service Under Specific User Account:** Select this option if you want to run the collector as a Windows service using a specific user account. If you select this option, you must enter values in the **USERNAME** and **PASSWORD** fields.

If you have enabled the **Enforce Strict Collector Authentication** option in Historian Administrator, you must provide the credentials of a user who is added to at least one of the following security groups:

- iH Security Admins
- iH Collector Admins
- iH Tag Admins

You can also configure the collector to start automatically when you start the computer.

15. Select **Add**.

The collector instance is added.

16. Select the collector instance.

The fields specific to the collector section appear in the **DETAILS** section.

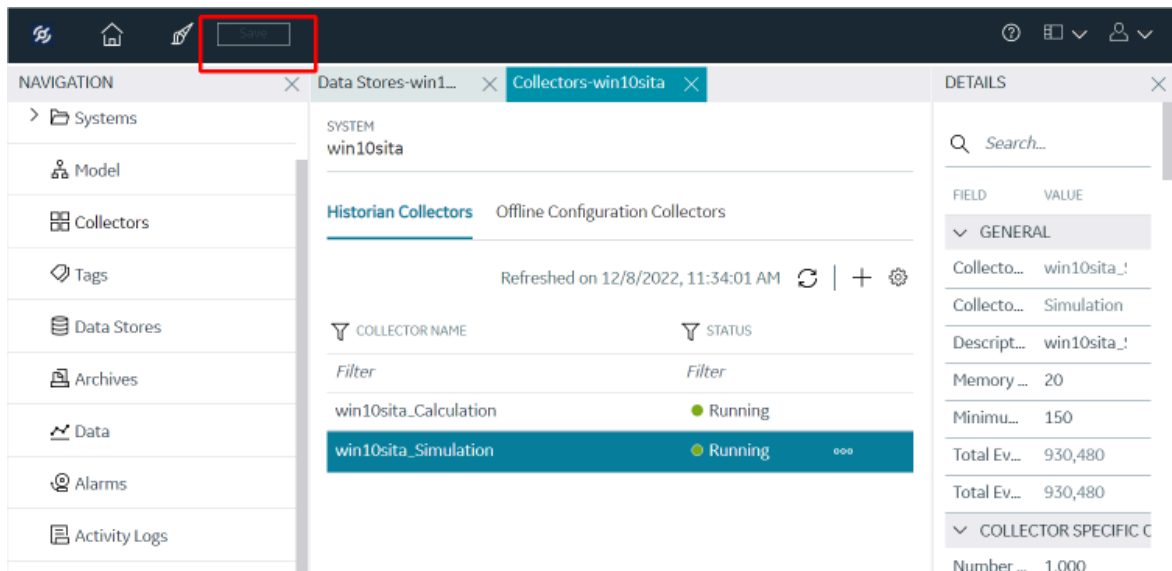
17. Under **Collector Specific Configuration**, enter values as described in the following table.

Field	Description
Recovery Time (hours)	Enter the maximum time, in hours, for which the collector will attempt to recover data after the collector is started or when connection between the collector and the Wonderware Historian server is re-established. This time is calculated as the duration between the current time and the last known write time.

Field	Description
Throttle (Milliseconds)	<p>Continuous data collection is resumed only after the previous data has been recovered.</p> <p>The default value is 0 hours.</p> <p>Enter the frequency of Wonderware data polling. This is to minimize the load on the Wonderware Historian server. By default, GE Wonderware Collector tries to query the tag data every 100 milliseconds based on the collection interval time. You can change this value to any time between 100 milliseconds to 16 hours.</p>

18. If needed, enter values in the [available sections \(on page 1114\)](#).

19. In the upper-left corner of the page, select **Save**.



The changes to the collector instance are saved.

20. If needed, restart the collector.

Specify the tags whose data you want to collect using the collector. In the **CHOOSE CONFIGURATION** field,

- If you have selected **Historian Configuration**, [specify the tags using Configuration Hub \(on page 909\)](#).
- If you have selected **Offline Configuration**, modify the offline configuration file of the collector. By default, the file is available in the following location: `<installation folder of Historian>\GE Digital\<collector name>`. For information, refer to [offline configuration](#). This option is applicable only if you have selected a cloud destination.

Collector Configuration - Common Fields

This topic provides a list of general fields that you can configure for any collector instance. These fields appear in the **DETAILS** section when you select a collector instance. For fields specific to a cloud destination, refer to [Alibaba Cloud](#), [AWS Cloud](#), [Azure Cloud](#), [Google Cloud \(on page 1148\)](#), and [Predix Cloud](#). For fields specific to the collector type, refer to the topics on adding and configuring each individual collector.

After you enter/modify a value in these fields, the changes are saved automatically after you place the cursor in a different field. Until the changes are saved, the values appear in bold formatting.

Table 33. The General Section

Field	Description
Collector Name	The name of the collector instance. This field is disabled.
Collector Type	The type of the collector instance. This field is disabled.
Description	The description of the collector instance. This field is disabled.
Memory Buffer Size (MB)	The size of the memory buffer currently assigned to the store-and-forward function. The memory buffer stores data during short-term or momentary interruptions of the server connection; the disk buffer handles long duration outages. To estimate

Table 33. The General Section (continued)

Field	Description
	<p>the size you need for this buffer, you need to know how fast the collector is trying to send data to the server and how long the server connection is likely to be down. With those values and a safety margin, you can compute the required size of the buffer.</p> <p>The default value is 20.</p>
Minimum Free Space (MB)	<p>The minimum free disk space that must be available on the computer. If the minimum space required is not available when the collector starts, the collector will shut down.</p>
Total Events Collected	<p>This field is disabled.</p>
Total Events Reported	<p>This field is disabled.</p>

Table 34. The Tags section

Field	Description
Tag Prefix	<p>The prefix that will be added to each tag that you configure for the collector instance. This field is disabled and populated with the name of the collector instance.</p> <p>This field applies to all collectors except File and Calculation collectors.</p>
Collection Interval Value	<p>The interval at which the collector collects data for all the tags configured in the collector instance.</p> <ul style="list-style-type: none"> • For polled data collection, this value represents the time required to complete a poll of tags in the collector. • For unsolicited data collection, it represents the frequency at which data is retrieved from tags in the collector. The collection interval can be individually configured for each tag.

Table 34. The Tags section (continued)


Field	Description
	<p>You can set this value for each tag as well.</p> <div data-bbox="820 388 1421 661" style="border: 1px solid orange; border-radius: 10px; padding: 10px;"> <p> Important: For an OPC collector, to avoid collecting redundant values when using device time-stamps, specify a collection interval that is greater than the OPC server update rate.</p> </div>
Collection Interval	The units of measure for the collection interval value.
Collection Type	<p>The type of the data collection:</p> <ul style="list-style-type: none"> • Polled: Data is collected based on a scheduled time interval. This type of data collection is supported only for: <ul style="list-style-type: none"> ◦ The Calculation collector ◦ The HAB collector ◦ The iFIX collector ◦ The OPC Classic DA collector ◦ The OPC UA DA collector ◦ The Simulation collector ◦ The Windows Performance collector • Unsolicited: Data is collected based on an event. This type of data collection is supported only for: <ul style="list-style-type: none"> ◦ The Calculation collector ◦ The HAB collector ◦ The MQTT collector ◦ The ODBC collector ◦ The OPC Classic DA collector ◦ The OPC Classic HDA collector ◦ The OPC UA DA collector ◦ The OSI PI collector ◦ The OSI PI distributor ◦ The Server-to-Server collector

Table 34. The Tags section (continued)

Field	Description
Time Assigned By	<ul style="list-style-type: none"> ◦ The Server-to-Server distributor ◦ The Wonderware collector <p>Indicates whether the timestamp for the collected data is set based on the data source or the collector. For example, for an OSI PI collector, if you select Source, the timestamp of the OSI PI server is considered for the values collected by the collector. If you select Collector, the timestamp of the collector is considered.</p>

Table 35. The Collector Compression Section

Field	Description
Collector Compression	<p>Indicates whether you want to apply collector compression, which is a smoothing filter to data retrieved from the data source. By ignoring small changes in values that fall within a deadband centered around the last reported value, only significant changes are stored in Historian, thus consuming less archive storage space.</p> <p>For more information, refer to About Collector and Archive Compression (on page 1190).</p>
Deadband	<p>Indicates whether you want to apply a deadband based on the percentage of values or on absolute values.</p> <p>For example, if you set the deadband to 20% for a range of 0 to 500 engineering units, the deadband value is 100 units, which is 50 units on each side. Therefore, only if the difference between two values is greater than 50, they are stored in Historian.</p>

Table 35. The Collector Compression Section (continued)


Field	Description
<p>Deadband Value</p>	<div data-bbox="820 319 1421 583" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-bottom: 10px;">  Note: If the data quality changes from good to bad or vice versa, the values are stored in Historian regardless of the deadband value. </div> <p>The deadband value that you want to use for values collected by the collector. Depending on whether you have selected percent or absolute, the deadband value is determined.</p> <p>For example, if you want to set a deadband of 5 units on either side of a value (that is, value +/- 5), enter 10 in the Deadband Value field, and select Absolute in the Deadband field. Similarly, if you want to set a deadband of 5% on either side of a value, enter 10 in the Deadband Value field, and select Percent in the Deadband field.</p> <p>For more information, refer to About Collector and Archive Compression (on page 1190).</p>
<p>Compression Timeout</p>	<p>The time for one poll cycle for which collector compression is not used, thus sending all the samples to Historian.</p> <p>This is used for a Calculation collector or Server-to-Server collector, when calculations fail, you may possibly observe collector compression (even if it is not enabled), thus producing no results or bad quality data. In such cases, you can use compression timeout, thus sending all the samples to Historian.</p> <p>For more information, refer to About Collector and Archive Compression (on page 1190).</p>

Table 35. The Collector Compression Section (continued)

Field	Description
Compression Timeout Interval	The units of measure for compression timeout.
Spike Logic Control	Indicates whether you want to apply spike logic to tag values. When you apply spike logic, in the event of a sudden change in tag values, a data sample is inserted just before the spike. The timestamp of the inserted sample is determined by your polling interval. If samples are collected at 1 second intervals, the inserted sample's timestamp will be 1 second before the spike. This helps clearly identify the spike, and retains a more accurate picture of the data leading up to it.
Multiplier	<p>Specifies how much larger a spike value must be than the deadband range before the spike logic is invoked.</p> <p>For example, if you enter 3 in the Multiplier field, and the deadband is set to 5%, the spike logic will not be invoked until the difference between the spike value and the previously archived data point is 15% of the EGU range.</p>
Interval	Specifies how many samples must have been compressed before the spike logic is invoked. For example, if you enter 4 in the Interval field, and 6 values have been compressed since the last archived data sample, the spike logic will be invoked.

Table 36. The Collector Options Section

Field	Description
Online Tag Configuration Changes	Indicates whether you want tag configuration changes to reflect immediately. If you disable this option, any tag configuration changes will reflect only after you restart the collector instance.

Table 36. The Collector Options Section (continued)


Field	Description
Browse Source Address Space	Indicates whether you want to allow browsing for tags in the source. You may sometimes want to disable this option to reduce processing load on the collector.
Synchronize Timestamps to Server	<p>Indicates whether you want to adjust the timestamp of data to align with the time setting in the Historian server. Note that this does not change the time setting in the collector machine; it only calculates the timestamp based on the difference between the time settings in the server machine and the collector machine, independent of time zone or daylight saving differences.</p> <div data-bbox="820 909 1421 1518" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note:</p> <ul style="list-style-type: none"> This option is applicable only if the timestamp of the collector is considered (instead of that of the data source - as specified in the Time Assigned By field). If this option is disabled, and if the time in the collector machine is more than 15 minutes ahead of the time in the server machine, data will not be stored in Historian. </div>
Delay Collection at Startup (sec)	The duration, in seconds, after which you want the data collection to begin post tag configuration.

Table 37. The Advanced Section


Field	Description
Debug Mode	<p>The debug mode for collector logs. 0 indicates normal log level, whereas 255 indicates that debugging is enabled.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;">  Note: Leaving the debug mode enabled for a long time consumes disk space. </div>
Message Compression	<p>Indicates whether you want to apply message compression.</p>

Table 38. The Collector Status Output Section

Field	Description
Rate Output Address	<p>The address in the source database into which the collector writes the output of events/minute. This will help an operator (or a HMI/SCADA application) learn the performance of the collector. Values are captured once a minute.</p> <p>You must enter the address of a writable analog field.</p> <p>For example, for an iFIX collector, enter the address of an iFIX tag in the following format: <code><node name>.<tag name>.<field name></code> (for example, <code>MyNode.MySIM_AO.F_CV</code>).</p>
Status Output Address	<p>The address in the source database into which the collector writes the current value of its status (for example, running, stopped). This will help an operator (or a HMI/SCADA application) learn the current status of the collector. The value is updated only if the status of the collector changes.</p> <p>You must enter the address of a writable text field of at least eight characters.</p>

Table 38. The Collector Status Output Section (continued)

Field	Description
Heartbeat Output Address	<p>For an iFIX collector, use TX tag for the output address. Enter the address in the following format: <code><node name>.<tag name>.<field name></code> (for example, <code>MyNode.MyCollector_TX.A_CV</code>).</p> <p>The address in the source database into which the collector writes the heartbeat signal output. Values are captured once a minute.</p> <p>You must enter the address of a writable analog field.</p> <p>For an iFIX data collector, use an iFIX tag for the output address. Enter the address in the following format: <code><node name>.<tag name>.<field name></code> (for example, <code>MyNode.MyCollector_TX.A_CV</code>).</p> <p>You can program the iFIX database to generate an alarm if values are not written every minute, notifying you that the collector has stopped.</p>

Sending Data to Cloud

Send Data to Alibaba Cloud

Generate a password using [the utility](#). While generating the password, use the same algorithm that you will use to connect to Alibaba Cloud.

To send data to Alibaba Cloud, you can choose any of the following collectors:

- The iFIX collector
- The MQTT collector
- The ODBC collector
- The OPC Classic DA collector
- The OPC Classic HDA collector
- The OPC UA DA collector
- The OSI PI collector
- The Server-to-Server collector

- The Simulation collector
- The Windows Performance collector
- The Wonderware collector

1. Access Alibaba IoT Platform console.

2. [Create a product](#). When you do so:

- In the **Node Type** field, select **Directly Connected Device**.
- In the **Network Connection Method** field, select **Wi-Fi**.
- In the **Data Type** field, select **ICA Standard Data Format**.

* Product Name
Format.

* Node Type

Directly Connected Device Gateway sub-device Gateway device

Networking and Data Format

* Network Connection Method
Wi-Fi

* Data Type
ICA Standard Data Format (Alink JSON)

✓ Checksum Type

✓ Authentication Mode

More

✓ Product Description

3. Note down the region ID for the region you have selected. For a list of region IDs, refer to <https://www.alibabacloud.com/help/doc-detail/40654.htm>.

4. Access the product certificate, and note down the product secret and product key values.

5. [Create a device](#).

6. [Access Configuration Hub \(on page 902\)](#).

7. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.

A list of collectors in the system appears.

8. If needed, select the system in which you want to add a collector instance.

SYSTEM			
WIN10TECH			
COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

9. In the upper-right corner of the main section, select **+**.

The screenshot shows a window titled 'Collectors-win10sita' with a 'DETAILS' pane on the right. The main area displays the system 'win10sita' and a section for 'Historian Collectors'. Below this, there is a refresh indicator showing 'Refreshed on 12/8/2022, 11:34:01 AM' and a red box around a '+' button. Below the refresh area is a table with columns for 'COLLECTOR NAME' and 'STATUS'.

COLLECTOR NAME	STATUS
<i>Filter</i>	<i>Filter</i>
win10sita_Calculation	Running
win10sita_Simulation	Running

The 'DETAILS' pane on the right contains the text 'No data to display.'

The **Add Collector Instance: <system name>** window appears, displaying the **Collector Selection** section. The **MACHINE NAME** field contains a list of machines on which you have installed collectors.

10. In the **COLLECTOR TYPE** field, select a collector type, and then select **Get Details**.

The **INSTALLATION DRIVE** and **DATA DIRECTORY** fields are disabled and populated.

11. Select **Next**.

The **Source Configuration** section appears, populating the hostname of the collector machine.

12. As needed, enter values in the available fields, and then select **Next**.

The **Destination Configuration** section appears.

13. In the **CHOOSE DESTINATION** field, select **MQTT**, and then provide values as described in the following table.

Field	Description
HOST ADDRESS	Enter a value in the following format: <code><product name>.iot-as-mqtt.<region ID>.aliyuncs.com</code> . A value is required. For example: <code>a23dr53dwrt.iot-as-mqtt.cn-shanghai.aliyuncs.com</code>
PORT	Enter 1883. A value is required.
CLIENT ID	Enter a value in the following format: <code><device name> securemode=<value>,signmethod=<algorithm name></code> . A value is required. <ul style="list-style-type: none"> ◦ For securemode, enter 2 for direct TLS connection, or enter 3 for direct TCP connection. ◦ For signmethod, specify the signature algorithm that you want to use. Valid values are hmacmd5, hmacsha1, hmacsha256, and sha256. You must use the same algorithm to generate the password. For example: <code>MyDevice securemode=3,signmethod=hmacsha1</code>
TOPIC	Enter a value in the following format: <code>/sys/<product name>/<device name>/thing/event/property/post</code> . A value is required.

Field	Description
	For example: <code>/sys/a23dr53dwrt/MyDevice/thing/event/proper-ty/post</code>
USERNAME	Enter a value in the following format: <code><device name><product name></code> . A value is required. For example: <code>MyDevicea23dr53dwrt</code>
PASSWORD	Enter the password that you have generated. A value is required.
CHOOSE CONFIGURATION	Select the type of the configuration to specify the tags whose data you want to collect. Select one of the following options: <ul style="list-style-type: none"> ◦ Historian Configuration: Select this option if you want to add the tags manually using Historian Administrator (on page 1189). If you select this option, the CONFIGURATION HISTORIAN SERVER field appears. ◦ Offline Configuration: Select this option if you want to provide the tag names using the offline configuration file instead of adding tags manually. By default, this file is located in the following location: <code><installation folder of Historian>\GE Digital\<collector name></code>

14. Select **Next**.

The **Collector Initiation** section appears.

The screenshot shows the 'Add Collector Instance' configuration window. On the left, a vertical progress bar indicates the current step: 'Collector Initiation' (WIN10TECH_Simulation) is selected, while previous steps like 'Collector Selection' and 'Source Configuration' are completed. The main configuration area includes:

- COLLECTOR NAME:** WIN10TECH_Simulation
- RUNNING MODE*:** Radio buttons for 'Service - Local System Account' (selected) and 'Service Under Specific User Account'.
- USERNAME:** A text field with the placeholder 'Enter Username'.
- PASSWORD:** A text field with the placeholder 'Enter Password'.

A note below the running mode options states: 'Note: Once an instance of the collector is created, you can run the collector either in Windows service mode or in Command line mode.' At the bottom of the window, there are three buttons: 'Previous', 'Cancel', and 'Add'.

15. Enter a collector name.

The value that you enter:

- Must be unique.
- Must not exceed 15 characters.
- Must not contain a space.
- Must not contain special characters except a hyphen, period, and an underscore.

16. In the **RUNNING MODE** field, select one of the following options.

- **Service - Local System Account:** Select this option if you want to run the collector as a Windows service using the credentials of the local user (that is, the currently logged-in user). If you select this option, the **USERNAME** and **PASSWORD** fields are disabled.
- **Service Under Specific User Account:** Select this option if you want to run the collector as a Windows service using a specific user account. If you select this option, you must enter values in the **USERNAME** and **PASSWORD** fields. If you have enabled the **Enforce Strict Collector Authentication** option in Historian Administrator, you must provide the credentials of a user who is added to at least one of the following security groups:
 - iH Security Admins
 - iH Collector Admins
 - iH Tag Admins

If you choose the first option, you can also configure the collector to start automatically when you start the computer, or, in the case of iFIX collectors, whenever you start iFIX.

17. Select **Add**.

The collector instance is created.

18. Specify the tags for which you want to collect data.

- If you have selected **Historian Configuration** in the **CHOOSE CONFIGURATION** field, [specify the tags manually \(on page 909\)](#).
- If you have selected **Offline Configuration** in the **CHOOSE CONFIGURATION** field, [specify the tags using the offline configuration file](#).

The collector begins sending Historian data to the device that you have created.

Send Data to AWS IoT Core

To send data to an AWS IoT Code, you can choose any of the following collectors:

- The iFIX collector
- The MQTT collector
- The ODBC collector
- The OPC Classic DA collector

- The OPC Classic HDA collector
- The OPC UA DA collector
- The OSI PI collector
- The Server-to-Server collector
- The Simulation collector
- The Windows Performance collector
- The Wonderware collector

1. Access the **AWS Management Console** page.

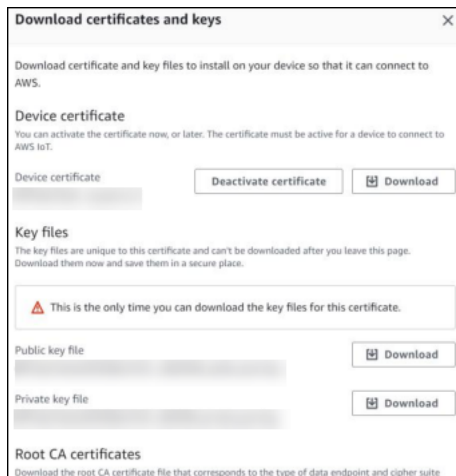
2. Search and select **IoT Core**.

The **AWS IoT** page appears.

3. [Create a policy](#) allowing the permissions that you want to grant on your device (for example, `iot:Connect`, `iot:Publish`, `iot:Subscribe`, `iot:Receive`). For the resource, provide the topic name. If, however, you want to use all topics, enter `*`.

4. [Create a thing](#), linking it with the policy that you have created.

5. Download the certificates and key files for the device to communicate. In addition, download the root CA certificate.

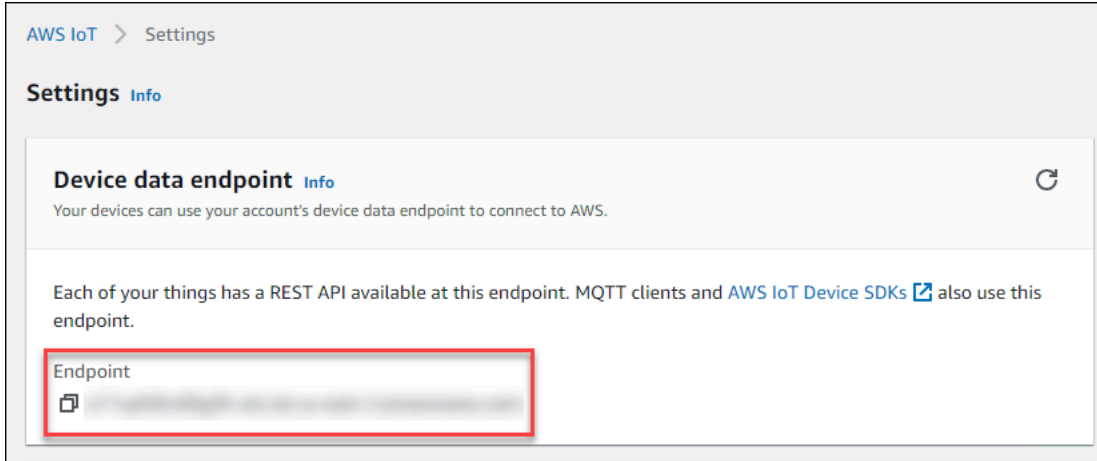


Important:

This is mandatory, and it is the only time you can download the certificates.

6. In the left navigation pane, select **Settings**.

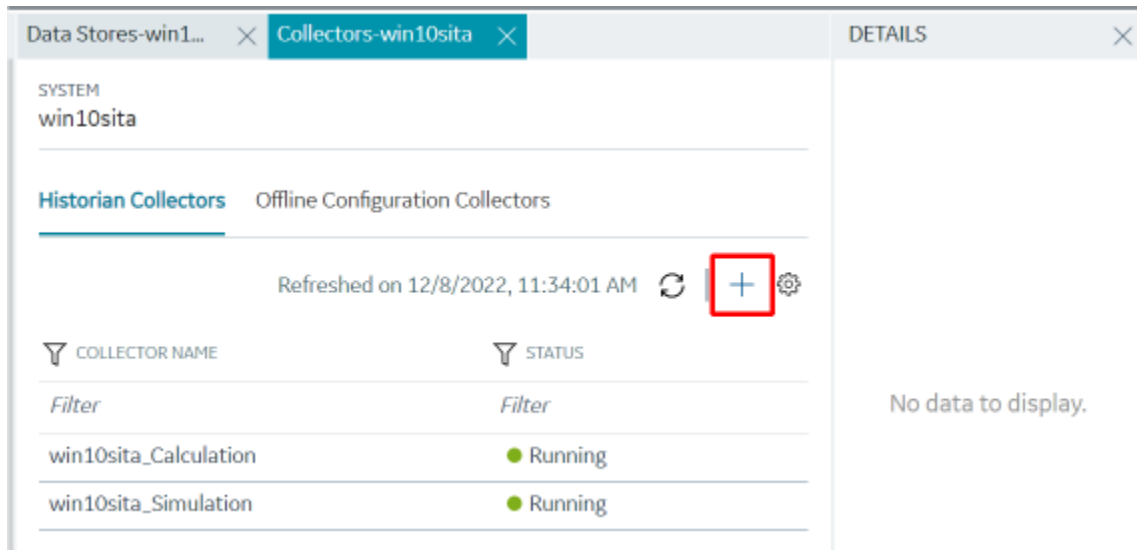
7. Make a note of the endpoint that appears.



8. [Access Configuration Hub \(on page 902\)](#).
9. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.
A list of collectors in the system appears.
10. If needed, select the system in which you want to add a collector instance.

SYSTEM			
COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
Refreshed on 2021-12-21 16:10:40 ↻ + ⚙️			
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	● Unknown	Historian	WIN10TECH
WIN10TECH_Simulation 📄	● Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	● Unknown	Historian	WIN10TECH

11. In the upper-right corner of the main section, select **+**.



The **Add Collector Instance: <system name>** window appears, displaying the **Collector Selection** section. The **MACHINE NAME** field contains a list of machines on which you have installed collectors.

- In the **COLLECTOR TYPE** field, select a collector type (except the File collector and the Server-to-Server collector), and then select **Get Details**.

The **INSTALLATION DRIVE** and **DATA DIRECTORY** fields are disabled and populated.

- Select **Next**.

The **Source Configuration** section appears, populating the hostname of the collector machine.

- As needed, enter values in the available fields, and then select **Next**.

The **Destination Configuration** section appears.

15. In the **CHOOSE DESTINATION** field, select **MQTT**, and then provide values as described in the following table.

Field	Description
HOST ADDRESS	Enter the endpoint that you have noted down. A value is required.
PORT	Enter 8883. A value is required.
CLIENT ID	Enter the thing name. A value is required.
TOPIC	Enter the MQTT topic to which you want the collector to publish data. A value is required. For information on topic names, refer to https://docs.aws.amazon.com/iot/latest/developer-guide/topics.html .
USERNAME	Enter any value. Since we will use a certificate-based authentication, username and password will not be used; however, you must still enter a value.
PASSWORD	Enter any value. Since we will use a certificate-based authentication, username and password will not be used; however, you must still enter a value.

Field	Description
CA SERVER ROOT FILE	Enter the path of the root CA certificate file that you have downloaded.
CLIENT CERTIFICATE	Enter the path of the device certificate that you have downloaded.
PRIVATE KEY FILE	Enter the path of the private key file that you have downloaded.
PUBLIC KEY FILE	Enter the path of the public key file that you have downloaded.
CHOOSE CONFIGURATION	<p>Select the type of the configuration to specify the tags whose data you want to collect. Select one of the following options:</p> <ul style="list-style-type: none"> ◦ Historian Configuration: Select this option if you want to add the tags manually using Historian Administrator (on page 1189). If you select this option, the CONFIGURATION HISTORIAN SERVER field appears. ◦ Offline Configuration: Select this option if you want to provide the tag names using the offline configuration file instead of adding tags manually. By default, this file is located in the following location: <code><installation folder of Historian>\GE Digital\<collector name></code>

16. Select **Next**.

The **Collector Initiation** section appears.

17. Enter a collector name.

The value that you enter:

- Must be unique.
- Must not exceed 15 characters.
- Must not contain a space.
- Must not contain special characters except a hyphen, period, and an underscore.

18. In the **RUNNING MODE** field, select one of the following options.

- **Service - Local System Account:** Select this option if you want to run the collector as a Windows service using the credentials of the local user (that is, the currently logged-in user). If you select this option, the **USERNAME** and **PASSWORD** fields are disabled.
- **Service Under Specific User Account:** Select this option if you want to run the collector as a Windows service using a specific user account. If you select this option, you must enter values in the **USERNAME** and **PASSWORD** fields. If you have enabled the **Enforce Strict Collector Authentication** option in Historian Administrator, you must provide the credentials of a user who is added to at least one of the following security groups:
 - iH Security Admins
 - iH Collector Admins
 - iH Tag Admins

If you choose the first option, you can also configure the collector to start automatically when you start the computer, or, in the case of iFIX collectors, whenever you start iFIX.

19. Select **Add**.

The collector instance is created.

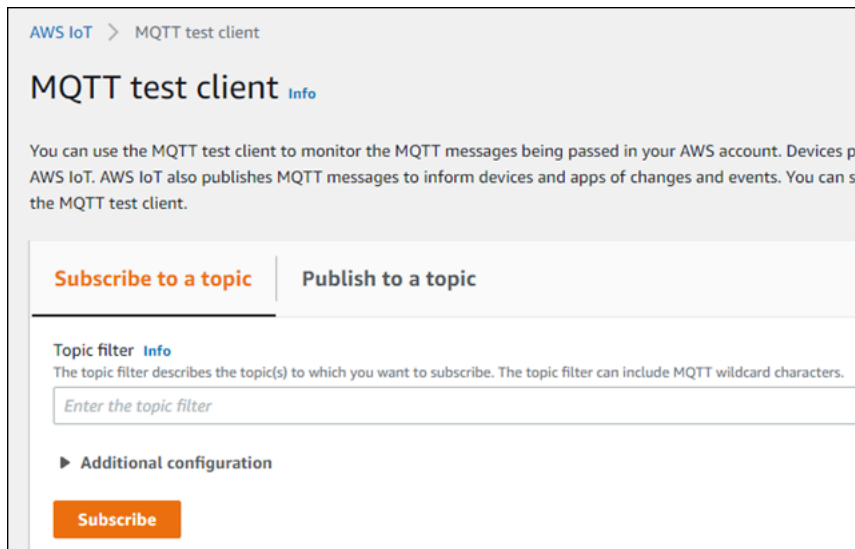
20. Specify the tags for which you want to collect data.

- If you have selected **Historian Configuration** in the **CHOOSE CONFIGURATION** field, [specify the tags manually \(on page 909\)](#).
- If you have selected **Offline Configuration** in the **CHOOSE CONFIGURATION** field, [specify the tags using the offline configuration file](#).

The collector begins sending Historian data to the thing that you have created.

21. Access AWS IoT Core, and in the left pane, select **Test**.

The **MQTT test client** page appears.



22. Subscribe to the topic to which the collector is publishing data, and then select **Subscribe**.

The messages received from the topic appear, indicating that the collector is sending data to the AWS IoT device.

AWS supports a payload of maximum 128 KB. Therefore, if the message size is greater than 128 KB, create a registry key named `CloudMaxSamplesPerMsg` for the collector instance, and decrease the value to 700 or less. If, however, you want to send more data in a message, we recommend that you create another collector instance and send data to another thing resource in AWS.



Tip:

To find out the message size, [modify the collector instance \(on page 1166\)](#) and set the log level to 3 or more.

23. Create a [VPC destination](#) or an [HTTP destination](#) for the messages.
24. [Monitor the data that you have collected](#).

Send Data to Azure Cloud in the Key-Value Format

To send data to an Azure IoT Hub device, you can choose any of the following collectors:

- The iFIX collector
- The MQTT collector
- The ODBC collector
- The OPC Classic DA collector
- The OPC Classic HDA collector
- The OPC UA DA collector
- The OSI PI collector
- The Server-to-Server collector
- The Simulation collector
- The Windows Performance collector
- The Wonderware collector

This topic describes how to send data in the key-value format. In this format, the message size is bigger because names of the tag properties are repeated. However, it provides clarity to novice users. For example: {"body":

```
[{"tagname": "Azure_Iot_simulation_tag_1", "epochtime": 1629730936000, "tagvalue": 7129.124023438, "quality": 3}, {"tagname": "Azure_Iot_simulation_tag_2", "epochtime": 1629730936000, "tagvalue": 123.3738924567, "quality": 3}] , "message": "..."
```

You can also [send data in the KairosDB format \(on page 1142\)](#).



Note:

Data in Azure IoT Hub is stored for maximum seven days, after which it is deleted from the hub. Therefore, you must consume the data within seven days. Based on your requirement, you can store it in a relevant Azure storage. You can then use Azure functions or streaming analytics to analyse the data.

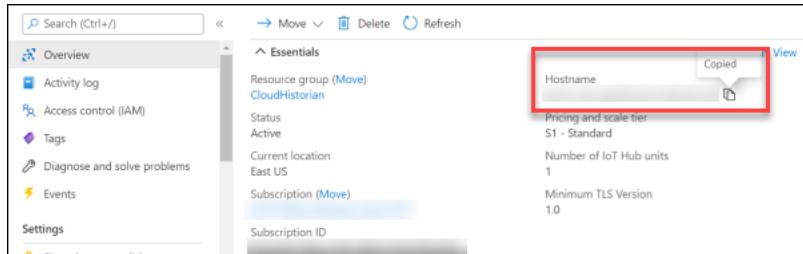
1. [Create Azure IoT Hub](#).



Tip:

To choose the correct Azure IoT Hub tier based on your data throughput, refer to <https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-quotas-throttling>. For guidance on choosing the appropriate subscription, refer to <https://azure.microsoft.com/en-us/pricing/details/iot-hub/>

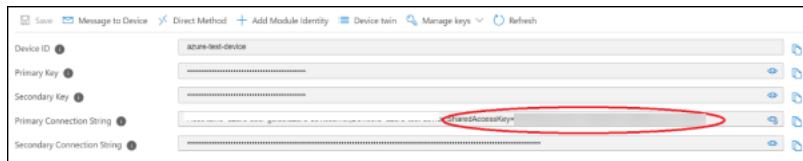
2. After you create Azure IoT Hub, select **Go to resource**, and then note down the hostname:



3. [Create devices in Azure IoT Hub](#) to group related tag information; thus mapping a collector instance to a device. We recommend that you create one device per collector instance. Ensure that the device is running.

When you create a device, use the following guidelines to choose the authentication type:

- **Symmetric Key:** Select this option if you want to use a Shared Access Signature (SAS) authentication.
 - **X.509 Self-Signed:** Select this option if you want to create self-signed certificates using OpenSSL. We recommend that you use these certificates only for testing purposes. For instructions, refer to <https://docs.microsoft.com/en-us/azure/iot-hub/tutorial-x509-self-sign>.
 - **X.509 CA Signed:** Select this option if you want to use CA-signed certificates
4. If you have selected **Symmetric Key** in the previous step, select the link in the **Device ID** column, and note down the shared access key value.



5. [Access Configuration Hub \(on page 902\)](#).
6. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.
A list of collectors in the default system appears.
7. If needed, select the system in which you want to add a collector instance.
8. If needed, select the system in which you want to add a collector instance.

SYSTEM			
WIN10TECH			
Refreshed on 2021-12-21 16:10:40			
COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

9. In the upper-right corner of the main section, select **+**.

The screenshot shows a window titled 'Collectors-win10sita' with a 'DETAILS' pane on the right. The main area displays the system name 'win10sita' and a section for 'Historian Collectors'. Below this, it shows 'Offline Configuration Collectors' and a refresh timestamp 'Refreshed on 12/8/2022, 11:34:01 AM'. A table lists collector instances with their names and statuses. A '+' button is highlighted in a red box in the upper right of the main section.

COLLECTOR NAME	STATUS
<i>Filter</i>	<i>Filter</i>
win10sita_Calculation	Running
win10sita_Simulation	Running

The 'DETAILS' pane on the right contains the text: 'No data to display.'

The **Add Collector Instance: <system name>** window appears, displaying the **Collector Selection** section. The **MACHINE NAME** field contains a list of machines on which you have installed collectors.

10. In the **COLLECTOR TYPE** field, select a collector type, and then select **Get Details**.

The **INSTALLATION DRIVE** and **DATA DIRECTORY** fields are disabled and populated.

11. Select **Next**.

The **Source Configuration** section appears.

12. As needed, enter values in the available fields.

13. Select **Next**.

The **Destination Configuration** section appears.

The screenshot shows a configuration window titled "Add Collector Instance:". On the left, a vertical progress bar indicates the current step is "Destination Configuration" (MQTT). The main area is divided into sections: "CHOOSE DESTINATION*" with radio buttons for Historian Server, Predix Timeseries, Azure IoT Hub, and MQTT (selected); "HOST ADDRESS*" and "PORT*" fields with "Enter Address" and "Enter Port" prompts; "CLIENT ID*" and "TOPIC*" fields with "Enter Client ID" and "Enter Topic" prompts; an "AUTHENTICATION" section with an "AUTO REFRESH" toggle (currently off); "USER CREDENTIAL" fields for "USERNAME*" and "PASSWORD" with "Enter Username" and "Enter Password" prompts; and an "SSL/TLS" section. At the bottom are "Previous", "Cancel", and "Next" buttons.

14. Select **MQTT**, and provide values as described in the following table.

Field	Description
HOST ADDRESS	Enter the host name of the resource that you have noted down in step 2. A value is required and must be in the following format: <code><Azure IoT Hub name>.azure-devices.net</code>
PORT	Enter 8883.
CLIENT ID	Enter the ID of the device that you created in step 3. A value is required and must be unique for an MQTT broker.
TOPIC	Enter <code>devices/<device ID>/messages/events.</code>
AUTO REFRESH	Indicates whether you want to automatically create/refresh the SAS authentication token when it expires. <ul style="list-style-type: none"> ◦ If you switch the toggle off, you must manually provide the token as soon as it expires. ◦ If you switch the toggle on, you must provide the shared access key that you have noted down in step 4. And, you can leave the PASSWORD field blank.

Field	Description
	This is applicable only if you have selected Symmetric Key in step 3.
USERNAME	Enter a value in the following format: <code><host name or IP address>/<device ID>/?api-version=2018-06-30</code>
PASSWORD	<p>Enter the SAS token. This is applicable only if you have selected Symmetric Key in step 3 and if you have switched off the AUTO REFRESH toggle.</p> <p>For instructions on generating a SAS token, refer to https://docs.microsoft.com/en-us/azure/cognitive-services/translator/document-translation/create-sas-tokens?tabs=Containers.</p>
DEVICE SHARED KEY	Enter the shared access key value that you noted down in step 4. A value is required. This is applicable only if you have selected Symmetric Key in step 3 and if you have switched the AUTO REFRESH toggle on.
CA SERVER ROOT FILE	Enter the path of the CA server root file that you want to use. You can find the file here: https://github.com/Azure-Samples/loTMQTTSample/blob/master/loTHubRootCA_Baltimore.pem .
CLIENT CERTIFICATE	<p>Enter the path to the client certificate. A value is required. This is applicable only if you have selected one of these options in step 3:</p> <ul style="list-style-type: none"> ◦ X.509 Self-Signed: If you have selected this option, you can generate the certificate using OpenSSL. ◦ X.509 CA Signed: If you have selected this option, you would receive the certificate from CA.

Field	Description
PRIVATE KEY FILE	<p>Enter the complete path to the private key file. A value is required. This is applicable only if you have selected one of these options in step 3:</p> <ul style="list-style-type: none"> ◦ X.509 Self-Signed: If you have selected this option, you can generate the key file using OpenSSL. ◦ X.509 CA Signed: If you have selected this option, you would receive the key file from CA.
PUBLIC KEY FILE	<p>Enter the path to the public key file. This is applicable only if you have selected one of these options in step 3:</p> <ul style="list-style-type: none"> ◦ X.509 Self-Signed: If you have selected this option, you can generate the key file using OpenSSL. ◦ X.509 CA Signed: If you have selected this option, you would receive the key file from CA.
CHOOSE CONFIGURATION	<p>The type of the configuration to specify the tags whose data you want to collect. Select one of the following options:</p> <ul style="list-style-type: none"> ◦ Historian Configuration: Select this option if you want to add the tags manually (on page 909). If you select this option, the CONFIGURATION HISTORIAN SERVER field appears. ◦ Offline Configuration: Select this option if you want to provide the tag names using the offline configuration file instead of adding tags manually. By default, this file is located in the following location: <i><installation folder of Historian>\GE Digital\<collector name></i>

Field	Description
CONFIGURATION HISTORIAN SERVER	The host name of the machine from which you want to access Historian Administrator to add the tags manually for the collector. This field appears only if you have selected Historian Configuration in the CHOOSE CONFIGURATION field.

15. Select **Next**.

The **Collector Initiation** section appears.

16. Enter a collector name.

The value that you enter:

- Must be unique.
- Must not exceed 15 characters.
- Must not contain a space.
- Must not contain special characters except a hyphen, period, and an underscore.

17. In the **RUNNING MODE** field, select one of the following options.

- **Service - Local System Account:** Select this option if you want to run the collector as a Windows service using the credentials of the local user (that is, the currently logged-in user). If you select this option, the **USERNAME** and **PASSWORD** fields are disabled.
- **Service Under Specific User Account:** Select this option if you want to run the collector as a Windows service using a specific user account. If you select this option, you must enter values in the **USERNAME** and **PASSWORD** fields. If you have enabled the **Enforce Strict**

Collector Authentication option in Historian Administrator, you must provide the credentials of a user who is added to at least one of the following security groups:

- iH Security Admins
- iH Collector Admins
- iH Tag Admins

If you choose the first option, you can also configure the collector to start automatically when you start the computer, or, in the case of iFIX collectors, whenever you start iFIX.

18. Select **Add**.

The collector instance is created.

19. Specify the tags for which you want to collect data.

- If you have selected **Historian Configuration** in the **CHOOSE CONFIGURATION** field, [specify the tags manually \(on page 909\)](#).
- If you have selected **Offline Configuration** in the **CHOOSE CONFIGURATION** field, [specify the tags using the offline configuration file](#).

The collector begins sending Historian data to the Azure IoT Hub device that you have created.

Send Data to Azure Cloud in the KairosDB Format

To send data to an Azure IoT Hub device, you can choose any of the following collectors:

- The iFIX collector
- The MQTT collector
- The ODBC collector
- The OPC Classic DA collector
- The OPC Classic HDA collector
- The OPC UA DA collector
- The OSI PI collector
- The Server-to-Server collector
- The Simulation collector
- The Windows Performance collector
- The Wonderware collector

This topic describes how to send data in the KairosDB format. In this format, the message size is less because names of the tag properties are not repeated. For example: `[{"<tag name>":"Cloud_GCYSS3X2E.Simulation00001","<timestamp, tag value, and quality>":[[1586260104000,132560.203125000,3]]}]`. If you use this format, you can only use SAS-based authentication; you cannot use certificate-based authentication.

You can also [send data in the key-value format \(on page 1134\)](#).



Note:

Data in Azure IoT Hub is stored for maximum seven days, after which it is deleted from the hub. Therefore, you must consume the data within seven days. Based on your requirement, you can store it in a relevant Azure storage. You can then use Azure functions or streaming analytics to analyse the data.

1. [Create Azure IoT Hub](#).



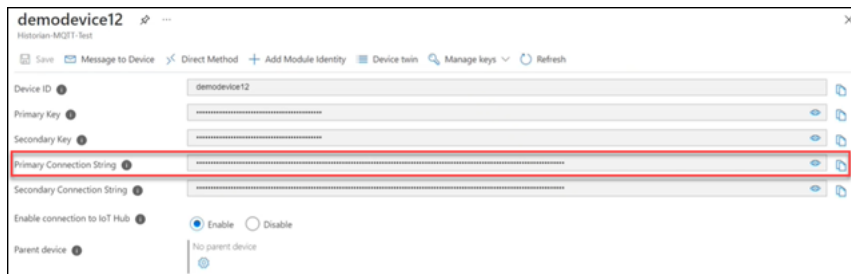
Tip:

To choose the correct Azure IoT Hub tier based on your data throughput, refer to <https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-quotas-throttling>. For guidance on choosing the appropriate subscription, refer to <https://azure.microsoft.com/en-us/pricing/details/iot-hub/>

2. [Create devices in Azure IoT Hub](#) to group related tag information; thus mapping a collector instance to a device. We recommend that you create one device per collector instance. Ensure that the device is running.

When you create a device, use only in the Symmetric Key authentication.

3. Select the link in the **Device ID** column, and note down the primary connection string value.



4. [Access Configuration Hub \(on page 902\)](#).

5. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.

A list of collectors in the default system appears.

6. If needed, select the system in which you want to add a collector instance.

7. If needed, select the system in which you want to add a collector instance.

SYSTEM WIN10TECH			
COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

8. In the upper-right corner of the main section, select **+**.

The screenshot shows a window titled 'Collectors-win10sita' with a 'DETAILS' pane on the right. The main area displays a table of collector instances for system 'win10sita'. The table has columns for 'COLLECTOR NAME' and 'STATUS'. Below the table, a refresh button and a '+' button are visible. The '+' button is highlighted with a red box. The 'DETAILS' pane on the right contains the text 'No data to display.'

COLLECTOR NAME	STATUS
<i>Filter</i>	<i>Filter</i>
win10sita_Calculation	Running
win10sita_Simulation	Running

The **Add Collector Instance: <system name>** window appears, displaying the **Collector Selection** section. The **MACHINE NAME** field contains a list of machines on which you have installed collectors.

9. In the **COLLECTOR TYPE** field, select a collector type, and then select **Get Details**.

The **INSTALLATION DRIVE** and **DATA DIRECTORY** fields are disabled and populated.

10. Select **Next**.

The **Source Configuration** section appears.

11. As needed, enter values in the available fields.

12. Select **Next**.

The **Destination Configuration** section appears.

The screenshot shows a configuration window titled "Add Collector Instance:". On the left, a vertical navigation pane lists four steps: "Collector Selection" (Simulation Collector), "Source Configuration" (WIN10TECH), "Destination Configuration" (MQTT), and "Collector Initiation". The "Destination Configuration" step is currently selected and highlighted in blue. The main area of the window is titled "CHOOSE DESTINATION*" and contains several input fields and a section for authentication. Under "CHOOSE DESTINATION*", there are four radio button options: "Historian Server", "Predix Timeseries", "Azure IoT Hub", and "MQTT". The "MQTT" option is selected. Below this, there are two columns of input fields: "HOST ADDRESS*" with a placeholder "Enter Address", "PORT*" with a placeholder "Enter Port", "CLIENT ID*" with a placeholder "Enter Client ID", and "TOPIC*" with a placeholder "Enter Topic". A section titled "AUTHENTICATION" contains a toggle switch for "AUTO REFRESH" which is turned off. Below this, there are two columns of input fields for "USER CREDENTIAL": "USERNAME*" with a placeholder "Enter Username" and "PASSWORD" with a placeholder "Enter Password". At the bottom of the window, there are three buttons: "Previous", "Cancel", and "Next".

13. Select **Azure IoT Hub**, and provide values as described in the following table.

Field	Description
DEVICE CONNECTION STRING	Identifies the Azure IoT device to which you want to send data. Enter the primary connection string value that you have noted down in step 3.
TRANSPORT PROTOCOL	The protocol that you want to use to send data to Azure IoT Hub. Select one of the following options: <ul style="list-style-type: none"> ◦ HTTP ◦ MQTT ◦ AMQP ◦ MQTT_OVER_WEBSOCKETS ◦ AMQP_OVER_WEBSOCKETS For information on which protocol to use, refer to Protocols and Port Numbers (on page 1159) .
PROXY	Identifies the URL of the proxy server to be used for both the authentication process and for sending data. If the collector is running on a network where proxy servers are used to access web resources outside of the network,

Field	Description
	then you must provide the proxy server settings. However, it does not affect the proxy server used by Windows when establishing secure connections. As a result, you must still configure the proxy settings for the Windows user account under which the collector service runs.
PROXY USERNAME	The username to connect to the proxy server.
PROXY PASSWORD	The password to connect to the proxy server.
CHOOSE CONFIGURATION	<p>The type of the configuration to specify the tags whose data you want to collect. Select one of the following options:</p> <ul style="list-style-type: none"> ◦ Historian Configuration: Select this option if you want to add the tags manually (on page 909). If you select this option, the CONFIGURATION HISTORIAN SERVER field appears. ◦ Offline Configuration: Select this option if you want to provide the tag names using the offline configuration file instead of adding tags manually. By default, this file is located in the following location: <code><installation folder of Historian>\GE Digital\<collector name></code>
CONFIGURATION HISTORIAN SERVER	The host name of the machine from which you want to access Historian Administrator to add the tags manually for the collector. This field appears only if you have selected Historian Configuration in the CHOOSE CONFIGURATION field.

The collector instance is created and connected to the Azure IoT Hub device.

14. Select **Next**.

The **Collector Initiation** section appears.

15. Enter a collector name.

The value that you enter:

- Must be unique.
- Must not exceed 15 characters.
- Must not contain a space.
- Must not contain special characters except a hyphen, period, and an underscore.

16. In the **RUNNING MODE** field, select one of the following options.

- **Service - Local System Account:** Select this option if you want to run the collector as a Windows service using the credentials of the local user (that is, the currently logged-in user). If you select this option, the **USERNAME** and **PASSWORD** fields are disabled.
- **Service Under Specific User Account:** Select this option if you want to run the collector as a Windows service using a specific user account. If you select this option, you must enter values in the **USERNAME** and **PASSWORD** fields. If you have enabled the **Enforce Strict Collector Authentication** option in Historian Administrator, you must provide the credentials of a user who is added to at least one of the following security groups:
 - iH Security Admins
 - iH Collector Admins
 - iH Tag Admins

If you choose the first option, you can also configure the collector to start automatically when you start the computer, or, in the case of iFIX collectors, whenever you start iFIX.

17. Select **Add**.

The collector instance is created.

18. Specify the tags for which you want to collect data.

- If you have selected **Historian Configuration** in the **CHOOSE CONFIGURATION** field, [specify the tags manually \(on page 909\)](#).
- If you have selected **Offline Configuration** in the **CHOOSE CONFIGURATION** field, [specify the tags using the offline configuration file](#).

The collector begins sending Historian data to the Azure IoT Hub device that you have created.

Send Data to Google Cloud

1. Download the Google root CA certificate from <https://pki.google.com/roots.pem>.
2. [Create public/private key pairs](#). Use OpenSSL only for testing purposes.

To send data to a Google Cloud device, you can choose any of the following collectors:

- The iFIX collector
- The MQTT collector
- The ODBC collector
- The OPC Classic DA collector
- The OPC Classic HDA collector
- The OPC UA DA collector
- The OSI PI collector
- The Server-to-Server collector
- The Simulation collector
- The Windows Performance collector
- The Wonderware collector

1. Access Google Cloud Platform.
2. [Create a project](#). Note down the project ID.
3. [Create a registry](#).

When you create the registry:

- Use the MQTT protocol.
- You can choose to provide a CA certificate.

Note down the registry ID and the region values.

4. [Add a device to the registry](#).

When you add the device:

- Allow device communication.
- Upload the public key or enter the details manually.

Note down the device ID.

5. [Access Configuration Hub \(on page 902\)](#).

6. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.

A list of collectors in the default system appears.

7. If needed, select the system in which you want to add a collector instance.

8. If needed, select the system in which you want to add a collector instance.

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

9. In the upper-right corner of the main section, select **+**.

COLLECTOR NAME	STATUS
win10sita_Calculation	Running
win10sita_Simulation	Running

The **Add Collector Instance: <system name>** window appears, displaying the **Collector Selection** section. The **MACHINE NAME** field contains a list of machines on which you have installed collectors.

10. In the **COLLECTOR TYPE** field, select a collector type, and then select **Get Details**.

The **INSTALLATION DRIVE** and **DATA DIRECTORY** fields are disabled and populated.

11. Select **Next**.

The **Source Configuration** section appears.

12. As needed, enter values in the available fields.

13. Select **Next**.

The **Destination Configuration** section appears.

The screenshot shows a configuration window titled "Add Collector Instance:". On the left, a vertical navigation pane lists steps: "Collector Selection Simulation Collector" (checked), "Source Configuration WIN10TECH" (checked), "Destination Configuration MQTT" (selected), and "Collector Initiation". The main area is titled "Destination Configuration" and contains the following fields:

- CHOOSE DESTINATION***: Radio buttons for "Historian Server", "Predix Timeseries", "Azure IoT Hub", and "MQTT" (selected).
- HOST ADDRESS***: Text input field with placeholder "Enter Address".
- PORT***: Text input field with placeholder "Enter Port".
- CLIENT ID***: Text input field with placeholder "Enter Client ID".
- TOPIC***: Text input field with placeholder "Enter Topic".
- AUTHENTICATION**: A section containing an "AUTO REFRESH" toggle switch (disabled) and an information icon.
- USER CREDENTIAL**: A section containing "USERNAME*" and "PASSWORD" text input fields with placeholders "Enter Username" and "Enter Password".
- SSL/TLS**: A section with no visible input fields.

At the bottom of the window are three buttons: "Previous", "Cancel", and "Next".

14. Select **MQTT**, and provide values as described in the following table.

Field	Description
HOST ADDRESS	Enter <code>mqtt.googleapis.com</code> . A value is required.
PORT	Enter 8883 or 443.
CLIENT ID	Enter the ID of the device that you created in the following format: <code>projects/<project ID>/locations/<cloud region>/registries/<registry ID>/devices/<device ID></code> . For example: <code>projects/mygcpproject/locations/asia-east1/registries/testmqttgcpiot/devices/gcptesting</code> A value is required and must be unique for an MQTT broker.
TOPIC	Enter <code>devices/<device ID>/events</code> .
AUTO REFRESH	Indicates whether you want to automatically refresh the authentication token when it expires.

Field	Description
	If you switch the toggle off, you must manually provide the token as soon as it expires. Google Cloud accepts only those tokens that expire in 24 hours or less; therefore, we recommend that you switch the toggle on.
USERNAME	Enter any value. This value is not used, but only if you enter a value, you can proceed.
PASSWORD	If you have switched the AUTO REFRESH toggle on, leave this field blank. Historian generates a JSON Web Token (JWT) and uses it automatically.
CA SERVER ROOT FILE	Enter the path of the Google root CA certificate that you have downloaded.
CLIENT CERTIFICATE	Enter the path to the client certificate.
PRIVATE KEY FILE	Enter the complete path to the private key file. A value is required.
PUBLIC KEY FILE	Enter the path to the public key file. A value is required.
CHOOSE CONFIGURATION	<p>The type of the configuration to specify the tags whose data you want to collect. Select one of the following options:</p> <ul style="list-style-type: none"> ◦ Historian Configuration: Select this option if you want to add the tags manually (on page 909). If you select this option, the CONFIGURATION HISTORIAN SERVER field appears. ◦ Offline Configuration: Select this option if you want to provide the tag names using the offline configuration file instead of adding tags manually. By default, this file is located in the following location:

Field	Description
	<i><installation folder of Historian>\GE Digital\ <collector name></i>
CONFIGURATION HISTORIAN SERVER	The host name of the machine from which you want to access Historian Administrator to add the tags manually for the collector. This field appears only if you have selected Historian Configuration in the CHOOSE CONFIGURATION field.

15. Select **Next**.

The **Collector Initiation** section appears.

16. Enter a collector name.

The value that you enter:

- Must be unique.
- Must not exceed 15 characters.
- Must not contain a space.
- Must not contain special characters except a hyphen, period, and an underscore.

17. In the **RUNNING MODE** field, select one of the following options.

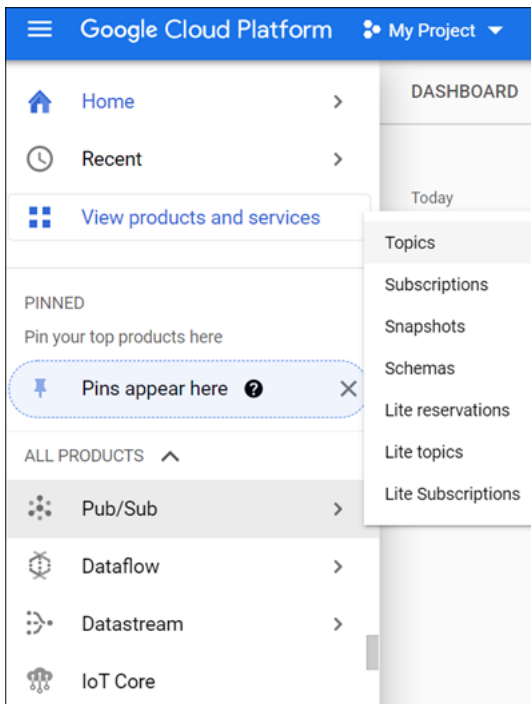
- **Service - Local System Account:** Select this option if you want to run the collector as a Windows service using the credentials of the local user (that is, the currently logged-in user). If you select this option, the **USERNAME** and **PASSWORD** fields are disabled.
- **Service Under Specific User Account:** Select this option if you want to run the collector as a Windows service using a specific user account. If you select this option, you must enter values in the **USERNAME** and **PASSWORD** fields. If you have enabled the **Enforce Strict Collector Authentication** option in Historian Administrator, you must provide the credentials of a user who is added to at least one of the following security groups:
 - iH Security Admins
 - iH Collector Admins
 - iH Tag Admins

If you choose the first option, you can also configure the collector to start automatically when you start the computer, or, in the case of iFIX collectors, whenever you start iFIX.

18. Select **Add**.

The collector instance is created.

19. Access Google Cloud Platform, and select **Pub/Sub > Topics**.



20. Select **Messages > PULL**.





Messages published to the topic that you have created appear. These messages contain the data sent by the collector instance. You can verify that the message content is correct by selecting **Message body**.


Send Data to Predix Cloud

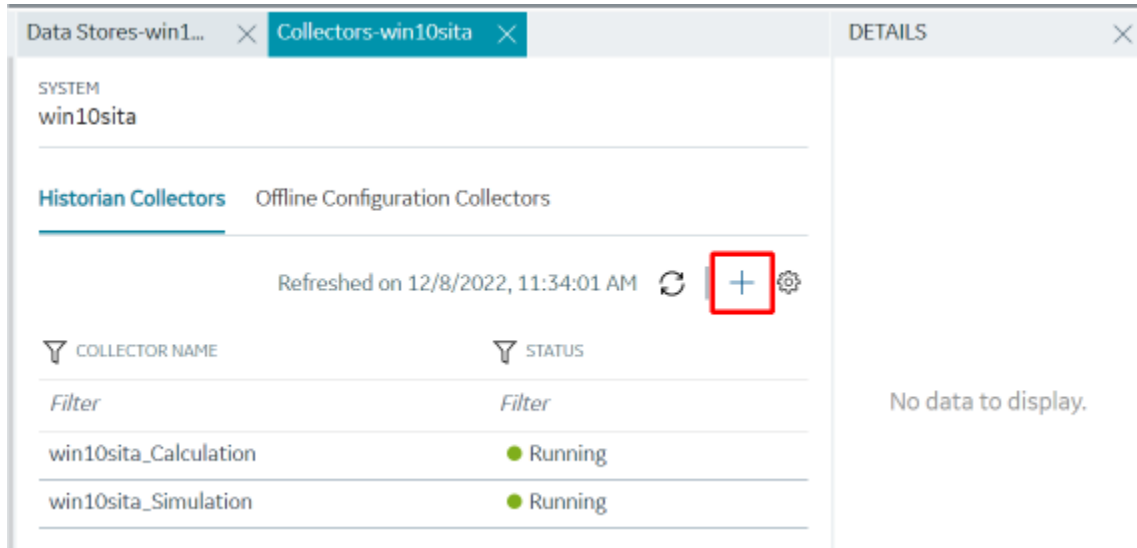
To send data to Predix Cloud, you can choose any of the following collectors:

- The iFIX collector
- The MQTT collector
- The ODBC collector
- The OPC Classic DA collector
- The OPC Classic HDA collector
- The OPC UA DA collector
- The OSI PI collector
- The Server-to-Server collector
- The Simulation collector
- The Windows Performance collector
- The Wonderware collector

1. [Register with the Timeseries service or any UAA service that you want to use](#). Note down the destination address, URI, client ID, client secret, and the zone ID that you have provided.
2. [Access Configuration Hub \(on page 902\)](#).
3. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**. A list of collectors in the system appears.
4. If needed, select the system in which you want to add a collector instance.

SYSTEM			
COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
Refreshed on 2021-12-21 16:10:40   			
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	● Unknown	Historian	WIN10TECH
WIN10TECH_Simulation 	● Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	● Unknown	Historian	WIN10TECH

5. In the upper-right corner of the main section, select .



The **Add Collector Instance: <system name>** window appears, displaying the **Collector Selection** section. The **MACHINE NAME** field contains a list of machines on which you have installed collectors.

- In the **COLLECTOR TYPE** field, select a collector type (except the File collector and the Server-to-Server collector), and then select **Get Details**.

The **INSTALLATION DRIVE** and **DATA DIRECTORY** fields are disabled and populated.

- Select **Next**.

The **Source Configuration** section appears, populating the hostname of the collector machine.

- As needed, enter values in the available fields, and then select **Next**.

The **Destination Configuration** section appears.

9. In the **CHOOSE DESTINATION** field, select **Predix Timeseries**, and then provide values as described in the following table.

Field	Description
CLOUD DESTINATION ADDRESS	The URL of a data streaming endpoint exposed by the Predix Time Series instance to which you want to send data. Typically, it starts with "wss://". This value is used as part of the interface name and default tag prefix of the collector. Your Predix Time Series administrator can provide this URL.
IDENTITY ISSUER	The URL of an authentication endpoint for the collector to authenticate itself and acquire necessary credentials to stream to the Predix Time Series. In other words, this is the issuer ID of the Proficy Authentication instance that you want to use to connect to Predix Time Series. Typically, it starts with https:// and ends with "/oauth/token".
CLIENT ID	Identifies the collector when interacting with Predix Time Series. This is equivalent to the username in many authentication schemes. The client must exist in the Proficy Authentication instance identified by the identity issuer, and the system requires that the <code>timeseries.zones. {ZoneId}.ingest</code> and <code>timeseries.zones. {ZoneId}.query</code> authorities are granted access to the client for the Predix Zone ID specified. Your Predix Time Series administrator can provide this information.

Field	Description
CLIENT SECRET	The secret to authenticate the collector. This is equivalent to the password in many authentication schemes.
ZONE ID	Unique identifier of the instance to which the collector will send data.
PROXY	Identifies the URL of the proxy server to be used for both the authentication process and for sending data. If the collector is running on a network where proxy servers are used to access web resources outside of the network, then you must provide the proxy server settings. However, it does not affect the proxy server used by Windows when establishing secure connections. As a result, you must still configure the proxy settings for the Windows user account under which the collector service runs.
PROXY USERNAME	The username to connect to the proxy server.
PROXY PASSWORD	The password to connect to the proxy server.
DATAPPOINT ATTRIBUTES	The attributes or parameters related to a datapoint that you want the collector to collect. Select Add Attributes to specify the attributes. You can add maximum five attributes for each collector instance.
CHOOSE CONFIGURATION	<p>The type of the configuration to specify the tags whose data you want to collect. Select one of the following options:</p> <ul style="list-style-type: none"> ◦ Historian Configuration: Select this option if you want to add the tags manually (on page 909). If you select this option, the CONFIGURATION HISTORIAN SERVER field appears. ◦ Offline Configuration: Select this option if you want to provide the tag names using the offline configuration file instead of adding tags manually. By default, this file is located in the following location: <i><installation folder of Historian>\GE Digital\<collector name></i>
CONFIGURATION HISTORIAN SERVER	The host name of the machine from which you want to access Historian Administrator to add the tags manually for the collec-

Field	Description
	tor. This field appears only if you have selected Historian Configuration in the CHOOSE CONFIGURATION field.

10. Select **Next**.

The **Collector Initiation** section appears.

11. Enter a collector name.

The value that you enter:

- Must be unique.
- Must not exceed 15 characters.
- Must not contain a space.
- Must not contain special characters except a hyphen, period, and an underscore.

12. In the **RUNNING MODE** field, select one of the following options.

- **Service - Local System Account:** Select this option if you want to run the collector as a Windows service using the credentials of the local user (that is, the currently logged-in user). If you select this option, the **USERNAME** and **PASSWORD** fields are disabled.
- **Service Under Specific User Account:** Select this option if you want to run the collector as a Windows service using a specific user account. If you select this option, you must enter values in the **USERNAME** and **PASSWORD** fields. If you have enabled the **Enforce Strict Collector Authentication** option in Historian Administrator, you must provide the credentials of a user who is added to at least one of the following security groups:
 - iH Security Admins
 - iH Collector Admins
 - iH Tag Admins

If you choose the first option, you can also configure the collector to start automatically when you start the computer, or, in the case of iFIX collectors, whenever you start iFIX.

13. Select **Add**.

The collector instance is created.

14. Specify the tags for which you want to collect data.

- If you have selected **Historian Configuration** in the **CHOOSE CONFIGURATION** field, [specify the tags manually \(on page 909\)](#).
- If you have selected **Offline Configuration** in the **CHOOSE CONFIGURATION** field, [specify the tags using the offline configuration file](#).

The collector begins sending Historian data to Predix Timeseries.

Protocols and Port Numbers

The following table provides a list of protocols that are available to send data to Azure IoT Hub, guidelines on which protocol to choose, and the port number that each protocol uses.

Protocol	When to Use	Port Number
HTTP	Use this protocol if the data that you want to send is not large and/or the default ports for the other protocols are not available.	80
MQTT	MQTT is lightweight compared to AMQP, and is widely used. Use this protocol if you want to send data using low bandwidth and/or you do not want to connect to multiple devices using the same connection.	8883
AMQP	AMQP is more reliable compared to other protocols. It sends data in batches, and hence, the network traffic is less compared to that of MQTT. Use this protocol if you want to send a large amount of data from multiple collectors frequently.	5671
MQTT over web sockets	MQTT is lightweight compared to AMQP, and is widely used. In addition, communication using web sockets is more reliable and secure. Use this protocol if you want to send data using low bandwidth and securely.	443

Protocol	When to Use	Port Number
AMQP over web sockets	AMQP is more reliable compared to other protocols. It sends data in batches, and hence, the network traffic is less compared to that of MQTT. In addition, communication using web sockets is more reliable and secure. Use this protocol if you want to send a large amount of data from multiple collectors frequently and securely.	443

Managing Collector Instances

About Managing Collectors Using Configuration Hub

Collectors are used to collect data from various sources and send it to Historian. For a list of collectors and their usage, refer to [About Historian Collectors](#).

After you install collectors and Remote Management Agent, the following artefacts will be available:

- **Executable files:** These files are required to add a collector instance.
- **Instances of the following collectors:**
 - The iFIX collector
 - The iFIX Alarms & Events collector
 - The OPC Classic Data Access collector for CIMPLICITY
 - The OPC Classic Alarms and Events collector for CIMPLICITY

These instances will be created only if iFIX and/or CIMPLICITY are installed on the same machine as the collectors.

- **The Remote Collector Management agent:** Provides the ability to [manage collectors remotely](#) manage collectors remotely.

You can then add a collector instance. This section describes how to [add a collector instance using Configuration Hub \(on page 909\)](#). You can also [add a collector instance using the RemoteCollectorConfigurator utility](#), which does not require you to install Web-based Clients.



Note:

Using Configuration Hub, you cannot add comments, enable the debug mode, pause data collection, resume data collection, modify, or delete an instance of offline collectors. In addition,



you cannot compress network messages. You can, however, [add](#) or [delete](#) the collector instance using the Collector Manager utility at a command prompt.

Access a Collector Instance

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.

A list of collectors appears, displaying the following columns:

Column	Description
COLLECTOR NAME	The name of the collector instance. If you select the link in this column, the details of the collector instance appears.
STATUS	The status of the collector. Contains one of the following values: <ul style="list-style-type: none"> ◦ Started ◦ Stopped ◦ Running ◦ Paused
CONFIGURATION	The source of the tag configuration for the collector. Contains one of the following values: <ul style="list-style-type: none"> ◦ HISTORIAN: Indicates that tags are configured using Historian Administrator. ◦ OFFLINE: Indicates that tags are configured using an offline configuration file.
MACHINE	The name of the machine on which the collector is installed.
VERSION	The version number of the collector.
REPORT RATE	The average rate at which the collector is sending data. This is a general indicator of load on the collector.
OVERRUNS	The total number of data events not collected. In normal operation and under normal conditions, this value should always be zero. If the value is not zero, which indicates that data is being lost, you must take steps to reduce peak load on the system by increasing the collection interval.

Column	Description
COMPRESSION	The effectiveness of collector compression. If the value is low, you can increase the compression deadbands to pass fewer values and thus increase the effect of compression.
OUT OF ORDER	The total number of out-of-order samples for the collector.
REDUNDANCY	Indicates whether collector redundancy is enabled, which decreases the likelihood of lost data due to software or hardware failures. For information, refer to About Collector Redundancy .
TAG COUNT	The number of tags for which the collector collects data.
COMMENTS	The comments that you have entered for the collector.


**Tip:**


You can also add, reorder, and remove columns from the table. For instructions, refer to [Common Tasks in Configuration Hub \(on page 906\)](#).

3. Select the row containing the collector whose details you want to access.

The details of the collector appear in the **DETAILS** section.

**Note:**

If the **DETAILS** section does not appear, in the upper-right corner of the page, select , and then select **Details**.

4. If you want to access the collector performance, right-click the collector (or select ) , and then select **View Collector Performance**.

SYSTEM			
WIN10TECH			
Refreshed on 2021-12-20 16:10:56			
COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running		WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown		WIN10TECH

Browse Tags
Add Tags
View Collector Performance
Start
Stop
Restart
Pause Data Collection
Resume Data Collection
Clear Buffer
Move Buffer
Change Destination Server
Delete

The **Collector Performance** section appears, displaying the following graphs:

- **REPORT RATE:** The rate at which the collector collects data.
- **TOTAL EVENTS REPORTED:** The total number of events reported to the Historian archive from the collector. This number may not match the total events collected due to collector compression.
- **STATUS:** The status of the collector plotted at regular intervals.
- **COLLECTOR COMPRESSION:** The collector compression (in percentage) applied to tag values plotted at regular intervals.
- **OUT OF ORDER:** The number of samples that have been received out of sequence. Even though data is still stored, a steadily increasing number of out-of-order events indicates a problem with data transmission that you should investigate. For example, a steadily increasing number of out-of-order events when you are using the OPC Collector means that there is an out-of-order between the OPC server and the OPC collector. This may also cause an out-of-order between the OPC collector and the data archiver but that is not what this graph indicates.



- **OVERRUNS:** The number of overruns in relation to the total events collected. Overruns are a count of the total number of data events not collected on their scheduled polling cycle. An overrun occurs when the data source is changing tag values faster than the collector collecting values, which causes it to consistently remain behind the archiver updates. It implies that the collector is running against the hardware and/or network limits and you may consider partitioning the tags into two or more sets, each with separate collector instances.


In a normal operation, this value should be zero. You may be able to reduce the number of overruns on the collector by increasing the tag collection intervals (per tag).

- **MINIMUM EVENT RATE:** Specifies the minimum number of data samples per minute sent to the archiver from all the collector instance.
- **TOTAL EVENTS COLLECTED:** The total number of events collected from the data source by the collector instance.
- **MAXIMUM EVENT RATE:** Specifies the maximum number of data samples per minute sent to the archiver from all the collector instance.

Access the Tags in a Collector Instance

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.
A list of collectors appears.
3. Right-click the collector instance whose tags you want to access (or select **☰**), and then select **Browse Tags**.

Refreshed on 2021-12-20 14:33:05  

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation 	Running	Browse Tags	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Add Tags	WIN10TECH
		View Collector Performance	
		Start	
		Stop	
		Restart	
		Pause Data Collection	
		Resume Data Collection	
		Clear Buffer	
		Move Buffer	
		Change Destination Server	
		Delete	

A list of tags for which the collector instance collects data appears.

- To narrow down your search results, select **Search**, enter the search criteria, and then enter **Search**.

You can add more search criteria by selecting **Add Attribute**.

You can enter a name or a value partially or use the wildcard character asterisk (*).

The list of tags are filtered based on the search criteria.

Add a Collector Instance

Before you begin using a collector, you must add an instance of the collector. You can add multiple instances of the same collector or instances of multiple collectors. To add multiple instances of a collector, perform the steps once again.

You can add and configure the following types of collector instances:

- [The Calculation collector \(on page 1024\)](#)
- [The CygNet collector \(on page 1027\)](#)
- [The File collector \(on page 1031\)](#)
- [The HAB collector \(on page 1035\)](#)
- [The iFIX collector \(on page 1051\)](#)
- [The MQTT collector \(on page 1056\)](#)

- [The ODBC collector \(on page 1062\)](#)
- [The OPC Classic Alarms and Events collector \(on page 1067\)](#)
- [The OPC Classic DA collector \(on page 1070\)](#)
- [The OPC Classic HDA collector \(on page 1076\)](#)
- [The OPC UA DA collector \(on page 1080\)](#)
- [The OSI PI collector \(on page 1084\)](#)
- [The OSI PI distributor \(on page 1088\)](#)
- [The Server-to-Server collector \(on page 1093\)](#)
- [The Server-to-Server distributor \(on page 1098\)](#)
- [The Simulation collector \(on page 1102\)](#)
- [The Windows Performance collector \(on page 1106\)](#)
- [The Wonderware collector \(on page 1110\)](#)

Modify a Collector Instance

This topic describes how to modify a collector instance using Configuration Hub. You can also [modify a collector instance using the RemoteCollectorConfigurator utility](#), which does not require you to install Web-based Clients.



Note:

- If the status of a collector instance is unknown, you cannot modify it.
- You cannot modify the instance of an offline collector.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.
A list of collectors appears.



Tip:

You can filter the collectors by the system name.

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

3. Select the collector instance that you want to modify.

The details of the collector appear in the **DETAILS** section.



Tip:

If the **DETAILS** section does not appear, in the upper-right corner of the page, select and then select **Details**.

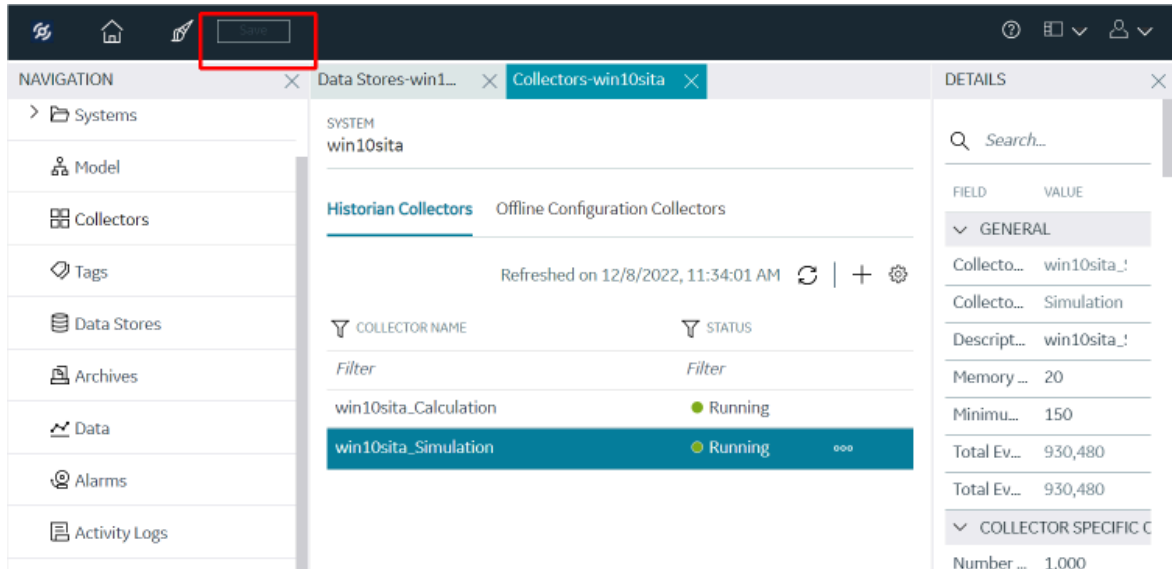
4. As needed, modify values in the [available fields \(on page 1114\)](#).



Note:

You cannot modify the destination of a collector.

5. In the upper-left corner of the page, select **Save**.





The changes to the collector instance are saved.



Note:

For collectors earlier than version 9.0:

- You cannot modify the details in the **INSTANCE CONFIGURATION** section.
- Some of the details, such as the collector type, do not appear.

6. If a  icon appears next to the collector name in the main section, right-click the collector (or select ), and then select **Restart**.

The changes to the collector instance are saved.

Add a Comment to a Collector Instance

This topic describes how to add a comment to a collector instance.

**Note:**

- You cannot modify or delete comments.
- You cannot add comments to offline collectors.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.
A list of collectors appears.


**Tip:**

You can filter the collectors by the system name.

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

3. Select the collector instance to which you want to add a comment.
The details of the collector appear in the **DETAILS** section, along with a list of comments at the end.

**Tip:**

If the **DETAILS** section does not appear, in the upper-right corner of the page, select , and then select **Details**.

4. In the **DETAILS** section, in the text box below **Comments**, enter your comment, and then select **Add Comment**.
The comment is added to the collector instance.

Access a Comment on a Collector Instance

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.

A list of collectors appears.


i Tip:
You can filter the collectors by the system name.


COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

Refreshed on 2021-12-20 14:29:16

3. Select the collector instance whose comments you want to access.

The details of the collector appear in the **DETAILS** section, along with a list of comments at the end.

i Tip:
If the **DETAILS** section does not appear, in the upper-right corner of the page, select , and then select **Details**.

4. To access comments in full screen, select . If you want to search for a comment, enter the search criteria in the **Search** field. You can also filter the comments based on a date and time range by selecting the values in the **FROM** and **TO** fields.
The comments are filtered based on the search criteria.

Start a Collector

You can start a collector using one of the following options:

- **Service:** Select this option if you want to start the collector as a Windows service using the credentials of the local user (that is, the currently logged-in user). If you select this option, the **USERNAME** and **PASSWORD** fields are disabled.
- **Command Line:** Select this option if you want to start the collector at a command prompt using a specific user account. If you select this option, you must enter values in the **USERNAME** and **PASSWORD** fields.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.
A list of collectors appears.

i Tip:
You can filter the collectors by the system name.

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

3. Right-click the collector instance that you want to start (or select **⋮**), and then select **Start**.

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

- Browse Tags
- Add Tags
- View Collector Performance
- Start**
- Stop
- Restart
- Pause Data Collection
- Resume Data Collection
- Clear Buffer
- Move Buffer
- Change Destination Server
- Delete

The **Start: <collector name>** window appears.

4. Under **RUNNING MODE**, select one of the following options:
 - **Service**: Select this option if you want to start the collector as a Windows service using the credentials of the local user (that is, the currently logged-in user). If you select this option, the **USERNAME** and **PASSWORD** fields are disabled.
 - **Command Line**: Select this option if you want to start the collector at a command prompt using a specific user account. If you select this option, you must enter values in the **USERNAME** and **PASSWORD** fields.
5. Select **Start**.

The collector is started, and the data collection begins. The status of the collector in the **Collectors** section changes to Starting and then to Running. If, however, the connection fails, the status changes to Unknown.

**Note:**

If auto-refresh is not enabled, refresh the collector manually.

Stop a Collector

When you stop a collector, the collector stops collecting data, and it is disconnected from the destination. If, however, you want the collector to remain connected to the destination, you can instead [pause data collection \(on page 1175\)](#).

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.
A list of collectors appears.

**Tip:**

You can filter the collectors by the system name.

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

3. Right-click the collector instance that you want to stop (or select **⋮**), and then select **Stop**.

SYSTEM			
WIN10TECH			
Refreshed on 2021-12-20 14:33:05			
COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
Filter	Filter	Filter	Filter
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running		WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown		WIN10TECH

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	<ul style="list-style-type: none"> Browse Tags Add Tags View Collector Performance Start Stop Restart Pause Data Collection Resume Data Collection Clear Buffer Move Buffer Change Destination Server Delete 	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown		WIN10TECH

The **Stop: <collector name>** window appears. The **COLLECTOR MACHINE** and **CURRENT RUNNING MODE** fields are populated and disabled.

- If the collector is running in the command-line mode, enter values in the **USERNAME** and **PASSWORD** fields.
- Select **Stop**.

The collector is stopped, and the data collection is paused. The status of the collector in the **Collectors** section changes to Stopped.

Restart a Collector

You can restart a collector to stop and start it again. You can restart a collector only if it is running.

- [Access Configuration Hub \(on page 902\)](#).
- In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**. A list of collectors appears.



Tip:

You can filter the collectors by the system name.

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

3. Right-click the collector instance that you want to restart (or select **⋮**), and then select **Restart**.

SYSTEM
WIN10TECH

Refreshed on 2021-12-20 14:33:05

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

- Browse Tags
- Add Tags
- View Collector Performance
- Start
- Stop
- Restart**
- Pause Data Collection
- Resume Data Collection
- Clear Buffer
- Move Buffer
- Change Destination Server
- Delete

The **Restart: <collector name>** window appears. The **COLLECTOR MACHINE** and **CURRENT RUNNING MODE** fields are populated and disabled.

4. If the collector is running in the command-line mode, enter values in the **USERNAME** and **PASSWORD** fields.

5. Select **Restart**.

The collector is restarted, and the data collection is resumed.

Pause the Data Collection of a Collector

When you pause data collection, the collector stops collecting the data. However, the collector is still connected to the destination. If you want to disconnect the collector from the destination, [stop the collector \(on page 1172\)](#).



Note:


You cannot pause the data collection of an offline collector.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.
A list of collectors appears.



Tip:

You can filter the collectors by the system name.

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	● Unknown	Historian	WIN10TECH
WIN10TECH_Simulation 	● Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	● Unknown	Historian	WIN10TECH

3. Right-click the collector instance for which you want to pause data collection (or select **⋮**), and then select **Pause Data Collection**.

SYSTEM			
WIN10TECH			
Refreshed on 2021-12-20 14:33:05			
COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
Filter	Filter	Filter	Filter
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running		WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown		WIN10TECH

Historian

- Browse Tags
- Add Tags
- View Collector Performance
- Start
- Stop
- Restart
- Pause Data Collection
- Resume Data Collection
- Clear Buffer
- Move Buffer
- Change Destination Server
- Delete

A message appears, asking you to confirm whether you want to pause data collection.

4. Select **Pause**.

The data collection is paused, and the collector is stopped.

Resume the Data Collection of a Collector

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.
A list of collectors appears.



Tip:

You can filter the collectors by the system name.

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

3. Right-click the collector instance for which you want to resume data collection (or select **...**), and then select **Resume Data Collection**.

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

A message appears, asking you to confirm whether you want to resume data collection.

4. Select **Resume**.

The collector is started, and the data collection is resumed.

Delete the Buffer Files of a Collector

When you delete buffer files, the collector is stopped, and after the buffer files are deleted, it is restarted.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.
A list of collectors appears.

i Tip:
You can filter the collectors by the system name.

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

3. Right-click the collector instance whose buffer files you want to delete (or select **⋮**), and then select **Clear Buffer**.

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH ⋮
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

- Browse Tags
- Add Tags
- View Collector Performance
- Start
- Stop
- Restart
- Pause Data Collection
- Resume Data Collection
- Clear Buffer**
- Move Buffer
- Change Destination Server
- Delete

A message appears, asking you to confirm that you want to clear the buffer files.

4. Select **Clear**.

The **Clear Buffer: <collector name>** window appears.

5. If the collector is running in the command-line mode with a specific user account, enter values in the **USERNAME** and **PASSWORD** fields.

6. Select **Clear**.

The buffer files of the collector are deleted.

Move the Buffer Files of the Collector

We recommend that you move the buffer files to a new folder within the same drive. You cannot move files to a folder on a network shared drive.

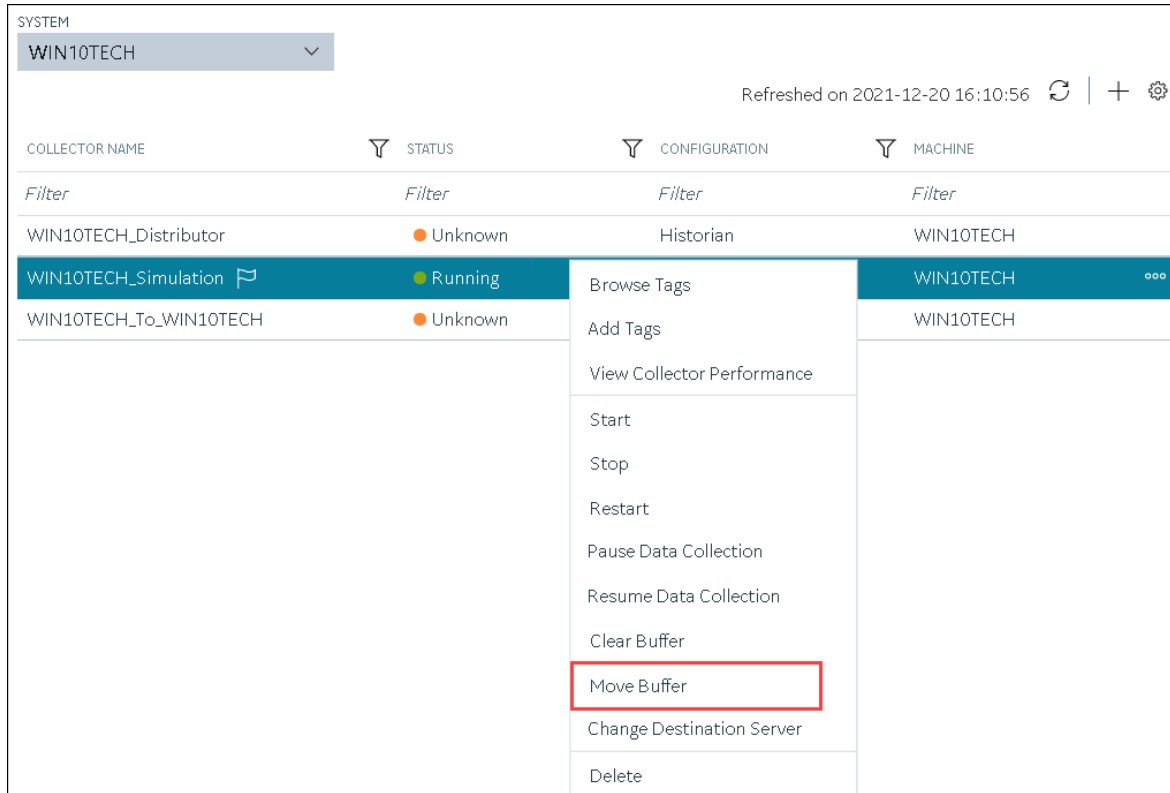
When you move buffer files, the collector is stopped, and after the buffer files are moved, it is restarted.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.
A list of collectors appears.

i Tip: You can filter the collectors by the system name.

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

3. Right-click the collector instance whose buffer files you want to move (or select **⋮**), and then select **Move Buffer**.



The **Move Buffer: <collector name>** window appears. The **CURRENT LOCATION, COLLECTOR MACHINE**, and **RUNNING MODE** fields are populated and disabled.

4. In the **TARGET LOCATION** field, enter the path of the folder to which you want to move the buffer files.
5. If the collector is running in the Windows service mode, select **Move Buffer**. If the collector is running in the command-line mode, enter values in the **USERNAME** and **PASSWORD** fields, and then select **Move Buffer**.

The buffer files are moved, and the collector is started.

Change the Destination Server of a Collector

1. Ensure that Historian is installed on the new destination server to which you want the collector to send data.
 2. Ensure that the collector whose destination server you want to change is running.
1. [Access Configuration Hub \(on page 902\)](#).
 2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.

A list of collectors appears.

i Tip:
You can filter the collectors by the system name.

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

3. Right-click the collector instance whose destination server you want to change (or select **...**), and then select **Change Destination Server**.

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	<ul style="list-style-type: none"> Browse Tags Add Tags View Collector Performance Start Stop Restart Pause Data Collection Resume Data Collection Clear Buffer Move Buffer Change Destination Server Delete 	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown		WIN10TECH

The **Change Destination Server: <collector name>** window appears. The **COLLECTOR MACHINE**, **CURRENT RUNNING MODE**, and **CURRENT DESTINATION SERVER** fields are populated and disabled.

4. In the **NEW RUNNING MODE** field, select one of the following options:
 - **Service:** Select this option if you want to start the collector as a Windows service using the credentials of the local user (that is, the currently logged-in user). If you select this option, the **USERNAME** and **PASSWORD** fields are disabled.
 - **Command Line:** Select this option if you want to start the collector in the command-line mode. If you select this option, you must enter values in the **USERNAME** and **PASSWORD** fields.
 5. In the **NEW DESTINATION SERVER** field, enter the host name or IP address of the new destination server to which you want the collector to send data.
 6. In the **USERNAME** and **PASSWORD** fields, enter the credentials to access the new destination server.
 7. Select **Change Server**.

The destination server of the collector is changed, and the collector is stopped.
1. Update the network message compression of the collector by modifying the collector instance using Configuration Hub.
 2. Reconfigure the collector properties using Historian Administrator.
 3. [Restart the collector \(on page 1173\)](#).

Configure Collector Redundancy

1. [Create the collector instances \(on page 909\)](#) that you want to use for collector redundancy. All these collectors must be of the same type.
2. [Create tags](#) in the primary collector.
3. If you want to use the values of a watchdog tag as a failover trigger, [create the watchdog tag](#) in the primary collector.

Collector redundancy ensures that collection of your data remains uninterrupted. It uses two or more collectors that gather data from a single source. For more information, refer to [About Collector Redundancy](#)



This topic describes how to set up redundancy between two collectors - one primary and the other secondary. You can, however, set up multiple secondary collectors.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.
A list of collectors appears.
3. For the primary collector, in the **DETAILS** section, under **REDUNDANCY**, switch the **Redundant Collector** toggle. And then, in the upper-left corner of the page, select **Save**.
Redundancy is enabled for the primary collector.
4. Repeat the previous step for the secondary collector.
Redundancy is enabled for the secondary collector.
5. For the secondary collector, in the **DETAILS** section, under **REDUNDANCY**, in the **Backup For** field, select the primary collector, and then select **Save**.
The secondary collector is configured as a backup for the primary collector.

**Note:**

If you want to add another collector in the redundancy group, in the **Backup For** field, select the secondary collector.

6. If you want to manually trigger a failover, perform the following steps. Or, if you want to configure automatic triggers, skip to the next step.
 - a. Select the collector that you want to make active.
 - b. In the **DETAILS** section, under **REDUNDANCY**, in the **Make Active Collector** field, select **Active Collector**.
7. For the secondary collector, in the **DETAILS** section, under **REDUNDANCY FAILOVER TRIGGERS**, enter values as described in the following table, and then select **Save**.

Field	Description
Collector Status	Switch the toggle if you want to trigger failover when the primary collector stops collecting data.
Watchdog Tag	Select  , and then select the tag whose values you want to use as a trigger. <div style="border: 1px solid #00a0c0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note: The watchdog tag must be in the primary collector.</p> </div>
Failover on Bad Quality	Switch the toggle if you want to trigger failover when bad data is collected for the watchdog tag.

Field	Description
Failover on value	Specify whether you want to trigger a failover if the value of the watchdog tag is non-zero. You can use this option only if you have not used the No Value change interval field.
No Value change interval	Enter the duration in seconds after which you want to trigger a failover if the values of the watchdog tag do not change for the specified duration. You can use this option only if you have not used the Failover on value field.

The failover triggers are configured. As soon as any of these conditions are satisfied, the secondary collector becomes active and collects data.

Delete a Collector Instance

If you no longer want to use a collector instance to collect data, you can delete it. When you delete a collector instance, the Windows service for the collector, the Registry folder, and the buffer files are deleted as well.

This topic describes how to delete a collector instance using Configuration Hub. You can also [delete a collector instance using the RemoteCollectorConfigurator utility](#), which does not require you to install Web-based Clients.



Note:

When you delete an offline collector instance, the corresponding configuration file is not deleted. However, if another collector instance of the same interface name is created, the existing configuration file is replaced by a template configuration file.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**. A list of collectors appears.



Tip:

You can filter the collectors by the system name.

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Historian	WIN10TECH

3. Right-click the collector instance that you want to delete (or select **☰**), and then select **Delete**.

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation	Running		WIN10TECH ☰
WIN10TECH_To_WIN10TECH	Unknown		WIN10TECH

- Browse Tags
- Add Tags
- View Collector Performance
- Start
- Stop
- Restart
- Pause Data Collection
- Resume Data Collection
- Clear Buffer
- Move Buffer
- Change Destination Server
- Delete**

A message appears, asking you to confirm that you want to delete the collector instance.

4. If you want to delete the tags as well, select the **Delete associated tags** check box.

5. Select **Delete**.

The collector instance is deleted.

Managing Offline Configuration Collector Instances

Access Offline Configuration Collectors

Offline Configuration Collectors are the instances of collectors whose destination is the cloud and display the configuration details as Offline Configuration.

Add Collector Instance: santhoshwin10

<ul style="list-style-type: none"> Collector Selection Simulation Collector Source Configuration santhoshwin10 Destination Configuration Predix Timeseries Collector Initiation 	CLIENT ID*	CLIENT SECRET*
	<i>Enter client ID</i>	<i>Enter secret</i>
	ZONE ID*	PROXY
	<i>Enter zone ID</i>	<i>Enter proxy</i>
	PROXY USERNAME	PROXY PASSWORD
	<i>Enter username</i>	<i>Enter password</i>
DATAPoint ATTRIBUTES (OPTIONAL) ⓘ		
ATTRIBUTE + Add Attributes		
CONFIGURATION DETAILS		
CHOOSE CONFIGURATION*		
<input type="radio"/> Historian Configuration <input checked="" type="radio"/> Offline Configuration		


1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, expand **Systems**, and then select the system whose collectors you want to access.
The system appears in the main section.
3. Right-click the system whose collectors you want to access (or select **☰**), and then select **Browse Collectors**.

This displays the list of Historian collectors and Offline configuration collectors. By default, the Historian collector instances added to the system appear, displaying the following information.



Tip:

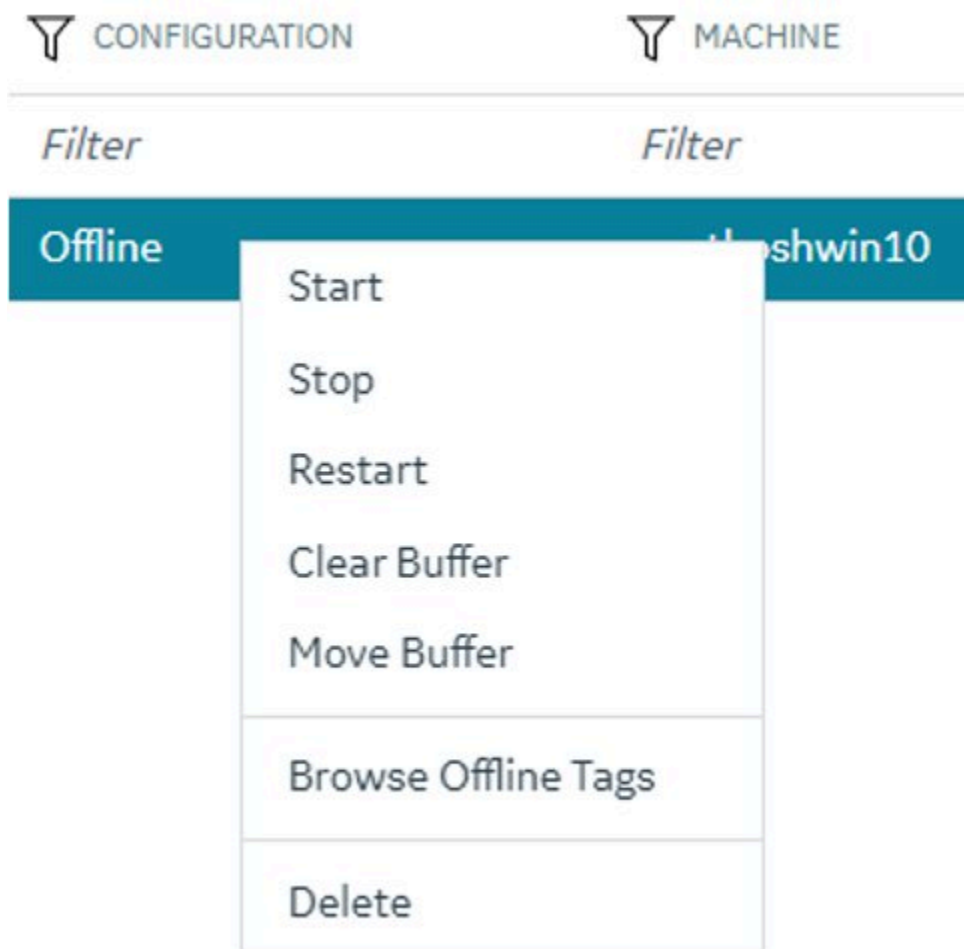
- To access the details of a collector, select the row containing the collector instance. The details appear in the **DETAILS** section.
- You can show/hide/reorder columns in the table. For instructions, refer to [Common Tasks in Configuration Hub \(on page 906\)](#).

 The Details panel for the Offline Configuration Collector Interface contains information regarding the instance configuration provided for the destination while installing software like Predix, MQTT, or Azure. For example, here is an example of the Details panel for the Offline Configuration Collector:

DETAILS ✕	
<input type="text" value="Search..."/>	
FIELD	VALUE
▼ INSTANCE CONFIGURATION	
Historian Server	SANTHOSHWIN10
Destination	Predix Timeseries
Cloud Destination Address	wss://gateway-predix-data-
Identity Issuer	https://9d4d55e0-14e1-4a4
Client ID	HistQA
Client Secret	
Zone ID	d459998a-656c-46c2-b525-
Proxy	http://PITC-Zscaler-America
Proxy Username	
Proxy Password	
Configuration	Offline
Configuration Historian S...	none

Manage Offline Configuration Collectors

Like other Historian collectors, Offline Configuration collectors can also be managed by selecting different options:






Refer to the following sections on how to use these options:

- [Start a Collector \(on page 1170\)](#)
- [Stop a Collector \(on page 1172\)](#)
- [Restart a Collector \(on page 1173\)](#)
- [Delete the Buffer Files of a Collector \(on page 1177\)](#)
- [Move the Buffer Files of the Collector \(on page 1179\)](#)
- [Delete a Collector Instance \(on page 1184\)](#)

Access the Tags in the Offline Configuration Collector Instance

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.
A list of collectors appears.
3. Right-click the Offline Configuration collectors you want to access (or select **☰**), and then select **Browse Tags**.

Refreshed on 2021-12-20 14:33:05  

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
WIN10TECH_Distributor	Unknown	Historian	WIN10TECH
WIN10TECH_Simulation 	Running	Browse Tags	WIN10TECH
WIN10TECH_To_WIN10TECH	Unknown	Add Tags	WIN10TECH
		View Collector Performance	
		Start	
		Stop	
		Restart	
		Pause Data Collection	
		Resume Data Collection	
		Clear Buffer	
		Move Buffer	
		Change Destination Server	
		Delete	

A list of tags for which the Offline Configuration collector instance collects data appears.

4. To narrow down your search results, select **Search**, enter the search criteria, and then enter **Search**.
You can add more search criteria by selecting **Add Attribute**.
You can enter a name or a value partially or use the wildcard character asterisk (*).
The list of tags are filtered based on the search criteria.

Managing Tags

About Tags

A Historian tag is used to store data related to a property.

For example, if you want to store the pressure, temperature, and other operating conditions of a boiler, a tag will be created for each one in Historian.

When you collect data using a collector, tags are created automatically in Historian to store these values. These tags are mapped with the corresponding properties in the source.

For example, suppose you want to store OSI PI data in Historian. You will specify the OSI PI tags for which you want to collect data. The OSI PI collector creates the corresponding tags in Historian, and it stores the values in those tags.

You can also choose to create tags manually (for example, to store the result of a calculation performed by the Calculation collector).

About Array Tags

You can store a set of values with a single timestamp and single quality and then read the elements individually or as an array.

The following conditions apply when using an array tag:

- You need not specify the size of an array tag. Data Archiver will store the number of elements that were written.
- You can change a tag to an array tag later as well. However, when you do so, only the latest data is retrieved. If you want to get the old data, you must change the tag back to its previous type.
- The maximum number of elements that an array tag can store is 10,000.
- You cannot associate an enumerated set or a user-defined data type (UDT) with an array tag.
- Fixed String and Scaled data types are not supported.
- Scaling, collector compression, and archive compression do not apply to an array tag.
- You cannot use an array element as a calculation trigger.
- You cannot plot a trend chart for an array tag.
- TagStats calculation mode is not supported.

About Collector and Archive Compression

Collector Compression

Collector compression applies a smoothing filter to data retrieved from the data source. By ignoring small changes in values that fall within a deadband centered around the last reported value, only significant changes are reported to the archiver. Fewer samples reported yields less work for the archiver and less archive storage space used.

You can specify the deadband value. For convenience, if you enter a deadband percentage, Historian Administrator shows the deadband in engineering units. For example, if you specify a 20% deadband on 0 to 500 EGU span, it is calculated and shown as 100 engineering units. If you later change the limits to 100 and 200, the 20% deadband is now calculated as 20 engineering units.

The deadband is centered around the last reported sample, not simply added to it or subtracted. If your intent is to have a deadband of 1 unit between reported samples, you must enter a compression deadband of 2 so that it is one to each side of the last reported sample. In the previous example of 0 to 500 EGU range, with a deadband of 20%, the deadband is 100 units; This means that only if the value changes by more than 50 units, it is reported.

Changes in data quality from good to bad, or bad to good, automatically exceed collector compression and are reported to the archiver. Any data that comes to the collector out of time order will also automatically exceed collector compression.

It is possible for collected tags with no compression to appear in Historian as if the collector or archive compression options are enabled. If collector compression occurs, you will notice an increase in the percentage of the compression value in the **Collectors** section of the **System Statistics** page in Historian Administrator. When archive compression occurs, you will notice the archive compression value and status bar change on the **System Statistics** page.

Even if collector compression is not enabled, you may notice it in the following scenarios:

- When a succession of bad data quality samples appears, Historian collects only the first sample in the series. No new samples are collected until the data quality changes. Historian does not collect the redundant bad data quality samples, and this is reflected in the collector compression percentage.
- For a Calculation or Server-to-Server collector, when calculations fail, producing no results or bad quality data, collector compression is used. The effect of Collector Compression Timeout is to behave, for one poll cycle, as if the collector compression feature is not being used. The sample collected from the data source is sent to the archiver. Then the compression is turned back on, as configured, for the next poll cycle with new samples being compared to the value sent to the archiver.

**Note:**

Array tags do not support archive and collector compression. If the tag is an array tag, then the **Compression** tab is disabled.

Handling Value Step Changes with Collector Data Compression

If you enable collector compression, the collector does not send values to the archiver any new input values if the value remains within its compression deadband. Occasionally, after several sample intervals inside the deadband, an input makes a rapid step change in value during a single sample interval. Since there have been no new data points recorded for several intervals, an additional sample is stored one interval before the step change with the last reported value to prevent this step change from being viewed as a slow ramp in value. This value marks the end of the steady-state, non-changing value period, and provides a data point from which to begin the step change in value.



Note:

You can configure individual tags can be configured to retrieve step value changes.

The collector uses an algorithm that views the size of the step change and the number of intervals since the last reported value to determine if a marker value is needed. The following is an example of the algorithm:

```
BigDiff=abs(HI_EGU-LO_EGU)*(CompressionDeadbandPercent/(100.0*2.0))*4.0

If ( Collector Compression is Enabled )

If ( Elapsed time since LastReportedValue>=( SampleInterval * 5 ) )

If ( abs(CurrentValue-LastReportedValue) > BigDiff )

Write LastReportedValue,Timestamp=(CurrentTime-SampleInterval)
```

In the example above, if a new value was not reported for at least the last 4 sample intervals, and the new input value is at least 4 deltas away from the old value (where a single delta is equal to half of the compression deadband), then a marker value is written.



Note:

These settings are also adjustable from the Registry. Please contact [technical support](#) for more information.

Value Spike with Collector Compression

For example, a collector reads a value X once per second, with a compression deadband of 1.0. If the value of X is 10.0 for a number of seconds starting at 0:00:00 and jumps to 20.0 at 0:00:10, the data samples read would be:

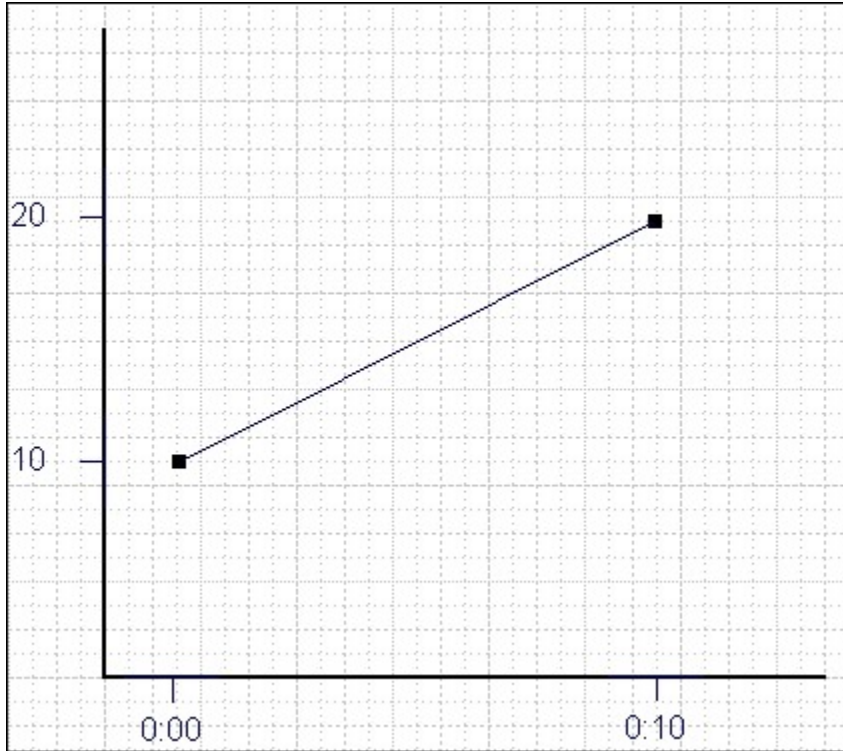
Time	X Value
0:00:00	10.0 (steady state value)

Time	X Value
0:00:01	10.0
0:00:02	10.0
0:00:03	10.0
0:00:04	10.0
0:00:05	10.0
0:00:06	10.0
0:00:07	10.0
0:00:08	10.0
0:00:09	10.0
0:00:10	20.0 (new value after step change)

To increase efficiency, the straightforward compression would store only 2 of these 11 samples.

Time	X Value
0:00:00	10.0 (steady state value)
0:00:10	20.0 (new value after step change)

However, without the marker value, if this data were to be put into a chart, it would look like the data value **ramped** over 10 seconds from a value of 10.0 to 20.0, as shown in the following chart.



The addition of a **marker value** to the data being stored results in the following data values:

Time	X Value
0:00:00	10.0 (steady state value)
0:00:09	10.0 (inserted Marker value)
0:00:10	20.0 (new value after step change)

If you chart this data, the resulting trend accurately reflects the raw data and likely real world values during the time period as shown in the following chart.



Evaluating and Controlling Data Compression

You can achieve optimum performance in Historian by carefully controlling the volume of dynamic data it collects and archives. You need enough information to tell you how the process is running, but you do not need to collect and store redundant or non-varying data values that provide no useful information.

Control Data Flow

You can control the amount of online or dynamic data the system handles at a given time by adjusting certain system parameters. The general principle is to control the flow of data into the archive either by adjusting the rate at which the collectors gather data or by adjusting the degree of filtering (compression) the system applies to the data collected.

Adjust the following parameters to *reduce* the rate of data flow into the server.

- Reduce the polling rate by increasing the collection interval for unsolicited and polled collection.
- Enable collector compression and optionally use compression timeout.
- Set the compression deadband on the collectors to a wider value.
- Use the collector compression timeout.

Adjust the following parameters to *increase the filtering* applied by the archiver in the server.

- Enable archive (trend) compression.
- Set the archive compression deadband to a wider value.
- Where possible, use the scaled data type and enable input scaling on selected tags.
- Where possible, select milliseconds or microseconds rather than seconds for time resolution.
Seconds is optimum for most common devices. This affects disk space.

Evaluate Data Compression Performance

You can determine how effectively data compression is functioning at any given time by examining the system statistics displayed on the **System Statistics** page of Historian Administrator.

The compression field at the top of the page shows the current effect of archive compression. Values for this parameter should typically range from 0 to 9%. If the value is zero, it indicates that compression is either ineffective or turned off. If it shows a value other than zero, it indicates that archive compression is operating and effective. The value itself indicates how well it is functioning. To increase the effect of data compression, increase the value of archive compression deadband so that compression becomes more active.

Archive Compression

Archive compression is used to reduce the number of samples stored when data values for a tag form a straight line in any direction. For a horizontal line (non-changing value), the behavior is similar to collector compression. But, in archive compression, it is not the *values* that are being compared to a deadband, but the *slope of line* those values produce when plotted value against time. Archive compression logic is executed in the data archiver and, therefore, can be applied to tags populated by methods other than collectors.

You can use archive compression on tags where data is being added to a tag by migration, or by the File collector, or by an SDK program for instance. Each time the archiver receives a new value for a tag, the archiver computes a line between this incoming data point and the last archived value.

The deadband is calculated as a tolerance centered about the slope of this line. The slope is tested to see if it falls within the deadband tolerance calculated for the previous point. If the new point does not exceed the tolerance, it is not stored in the archive. This process repeats with subsequent points. When an incoming value exceeds the tolerance, the value held by the archiver is written to disk and the incoming sample is withheld.

The effect of the archive compression timeout is that the incoming sample is automatically considered to have exceeded compression. The withheld sample is archived to disk and the incoming sample becomes the new withheld sample. If the Archive Compression value on the System Statistics page indicates that

archive compression is occurring, and you did not enable archive compression for the tags, the reason could be because of internal statistics tags with archive compression enabled.

About Scaling

Scaling converts a data value from a raw value expressed in an arbitrary range of units, such as a number of counts, to one in engineering units, such as gallons per minute or pounds per square inch. The scaled data type can serve as a third form of data compression, in addition to collector compression and archive compression, if it converts a data value from a data type that uses a large number of bytes to one that uses fewer bytes.

About Condition-Based Collection

Condition based collection is a method to control the storage of data for data tags by assigning a condition. Data is always collected but it is only written to the Data Archiver if the condition is true; otherwise, the collected data is discarded.

This condition is driven by a trigger tag; a tag collected by the collector evaluating the condition. Ideally, Condition based Collection should be used only with tags that are updating faster than the trigger tag. Condition based collection can be used to archive only the specific data which is required for analysis, rather than archiving data at all times, as the collector is running.

For example, if a collector has tags for multiple pieces of equipment, you can stop collection of tags for one piece of equipment during its maintenance. It is typically used on tags that use fast polled collection but you don't want to use collector compression. While the equipment is running, you want all the data but when the equipment is stopped, you don't want any data stored. The trigger tag would also typically use polled collection. But, either tag could use unsolicited collection.

The condition is evaluated every time data is collected for the data tag. When a data sample is collected, the condition is evaluated and data is either queued for sending to archiver, or discarded. If the condition cannot be evaluated as true or false, like if the trigger tag contains a bad data quality or the collector is not collecting the trigger tag, the condition is considered true and the data is queued for sending.

No specific processing occurs when the condition becomes true or false. If the condition becomes true, no sample is stored to the data tag using that condition, but the data tag will store a sample next time it collects. When the condition becomes false, no end of the collection marker is stored until the data tag is collected.

For example, if the condition becomes false at 1:15 and the data tag gets collected at 1:20, the end of collection marker will be created at 1:20 and have a timestamp of 1:20, not 1:15.

Condition based collection is supported by only archiver and collectors of Historian version 4.5 and above. Condition based collection does not apply to alarm collectors. This condition based collection is applicable to the following collectors only:


- Simulation Collector
- OPC Collector
- iFIX Collector
- PI Collector

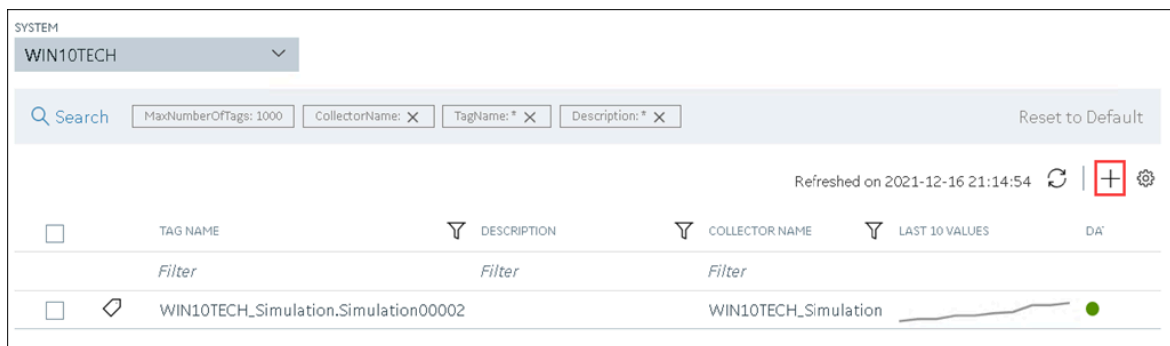
Add Tags for the Data Store Using Configuration Hub

- [Add the collector instance \(on page 909\)](#) using which you want to collect data. Ensure that the collector is running.
- By default, the tag data is stored in the user data store, which is created automatically when you set up Configuration Hub. If, however, you want to store the data in a different data store, [create it \(on page 920\)](#).

This topic describes how to specify the tags for which you want to collect data by browsing through the tags in the data source. For example, for an iFIX collector, if there are 1,00,000 tags in the iFIX server, you must specify the ones for which you want to collect data. Only then data is collected for those tags.

In addition to adding tags from the data source, you can [create tags manually \(on page 1018\)](#).

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Tags**.
3. Select .



The **Add Tag-<system name>** page appears. The **Add Tags from Collector** option is selected by default.

4. Enter values as described in the following table.

Field	Description
COLLECTOR NAME	Select the collector instance that you want to use to collect data. A value is required.
COLLECTED TYPE	Specify whether you want to browse through all the tags in the data source or only from the tags that you have not added yet. A value is required.
SOURCE TAG NAME	Enter the name of the tag (either completely or partially) to narrow down the search results.
SOURCE TAG DESCRIPTION	Enter the description of the tag (either completely or partially) to narrow down the search results.

5. Select **Search Tags**.

A list of tags that match *all* the criteria that you have specified appears. If a tag is already added, it is disabled.

6. Select the check box corresponding to each tag for which you want to collect data.

Add Tags from Collector
 Add Manually

COLLECTOR NAME*
 COLLECTED TYPE*
 SOURCE TAG NAME
 SOURCE TAG DESCRIPTION

SEARCH RESULTS FOR SOURCE TAGS NAMES

<input type="checkbox"/>	TAG NAME	DESCRIPTION
	<i>Filter</i>	<i>Filter</i>
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00001	WIN10TECH_Simulation.Simulation00001
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00002	WIN10TECH_Simulation.Simulation00002
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00003	WIN10TECH_Simulation.Simulation00003
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00004	WIN10TECH_Simulation.Simulation00004
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00005	WIN10TECH_Simulation.Simulation00005
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00006	WIN10TECH_Simulation.Simulation00006
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00007	WIN10TECH_Simulation.Simulation00007
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00008	WIN10TECH_Simulation.Simulation00008
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00009	WIN10TECH_Simulation.Simulation00009
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00010	WIN10TECH_Simulation.Simulation00010
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00011	WIN10TECH_Simulation.Simulation00011
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00012	WIN10TECH_Simulation.Simulation00012

DATASTORE*

7. In the **DATA STORE** field, if you want to store the data in a different data store than the user data store, select the same.
8. Select **Add Tag**.
Data collection begins for the selected tags.

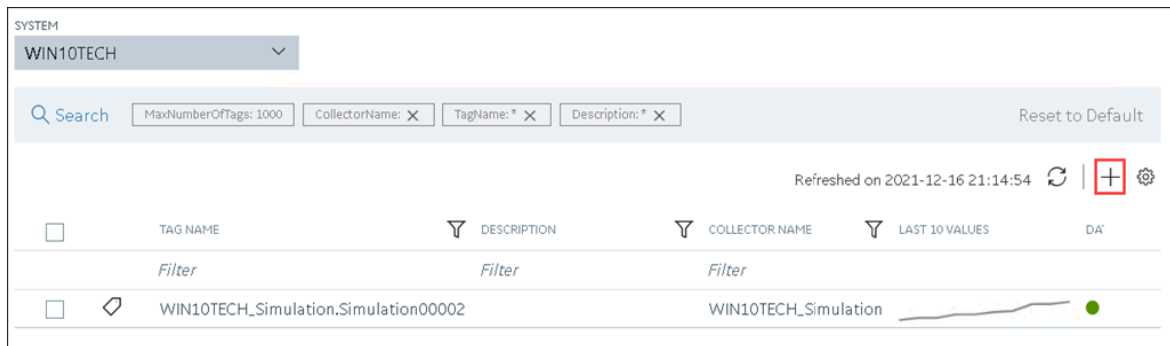
As needed, configure each tag by providing values for the tag properties. For information on the delta query modes, refer to [Counter Delta Queries](#).

Add a Tag Manually

- [Add the collector instance \(on page 909\)](#) using which you want to collect data.
- By default, the tag data is stored in the user data store, which is created automatically when you set up Configuration Hub. If, however, you want to store the data in a different data store, [create it \(on page 920\)](#).

After you create a collector instance, you [specify which tags from the source must be used for data collection \(on page 909\)](#). In addition, if you want to use the same tag twice (say, with a different collection interval or collector compression settings), you can add the tag manually. You can also create a calculation tag or a tag to store the values imported using the Excel Add-in.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Tags**.
3. Select **+**.




The **Add Tag-<system name>** page appears. The **Add Tags from Collector** option is selected by default.

4. Select **Add Manually**.

5. Enter values as described in the following table.

Field	Description
COLLECTOR NAME	Select the collector instance that you want to use to collect data. If, however, this tag is not associated with a collector, you can leave the field blank (for example, you want to ingest this data manually instead of using a collector).
SOURCE ADDRESS	Specify the source tag to which you want to map the one you are creating. This field is enabled only if you select a value in the COLLECTOR NAME field. When you select ☐☐☐ , the Browse Source Tag: <collector name> window appears. Provide the search criteria to find the tag that you want to map.
TAG NAME	Enter a name for the tag. A value is required and must be unique for the Historian server. The value that you enter: <ul style="list-style-type: none"> ◦ Must begin with a letter or a number. ◦ Can contain up to 256 characters.

Field	Description
	<ul style="list-style-type: none"> ◦ Can include any of the following special characters: /! #{}%\$-_ ◦ Must not include a space or any of the following characters: ~`+^;,:?*"={}@
DATA TYPE	<p>Select the data type of the tag data. To find out the data types supported by a collector, refer to the documentation on the collector that you have created.</p> <div style="border: 1px solid #ffc107; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Important: If you select an unsupported data type, you may receive incorrect data or even lose data.</p> </div> <p>If you select Multi-Field, the USER-DEFINED TYPE NAME field appears, and the ENUMERATED SET and ARRAY TAG fields are disabled.</p> <p>If you select Fixed String, the STRING LENGTH field appears.</p>
STRING LENGTH	<p>Enter the maximum character length allowed for the tag data. This field appears only if the value in the DATA TYPE field is Fixed String. A value is required.</p> <p>You can enter a value between 1 and 255. The default value is 8.</p>
USER-DEFINED TYPE NAME	<p>Select the user-defined data type (UDT) (<i>on page 1238</i>) that you want to assign to the tag. This field appears only if the value in the DATA TYPE field is Multi-Field. A value is required.</p>
ENUMERATED SET	<p>Select the enumerated set (<i>on page 1234</i>) that you want to assign to the tag. This field is not applicable for string and multi-field data types (enumerated sets) and for array tags.</p>
ARRAY TAG	<p>Switch the toggle to indicate whether the tag stores an array of data. This field is disabled if you select a value in the ENUMERATED SET field or if the value in the DATA TYPE field is Multi-Field.</p> <p>For information on array tags, refer to About Array Tags (<i>on page 1190</i>).</p>

Field	Description
TIME RESOLUTION	Select the time resolution for the tag. A value is required. For example, if you select Seconds , when you plot the data on a trend chart, the timestamp of the data points will be one second apart.
DATA STORE	If you want to store the data in a different data store than the user data store, select the same.

6. Select **Add Tag**.

Data collection begins for the selected tags.

As needed, configure each tag by providing values for the tag properties.

Access a Tag

To search for a tag, you can choose from the following options:

- Access all the tags in all the systems available in the Historian server.
- Access the tags added to a specific collector instance.
- Access the tags added to all the collector instances in a specific Historian system.

You can narrow down the search results further by performing a search.



Note:

By default, maximum one million tags are retrieved. If the Historian clients are configured to retrieve more than a million tags, to retrieve all of them, add the `MaxTagsToRetrieve` registry key under `HKEY_LOCAL_MACHINE\SOFTWARE\Intellution, Inc.\iHistorian\Services\DataArchiver\`, and then set the maximum number of tags that you want to retrieve. Restart the Historian Data Archiver service for the change to reflect.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Tags**.
A list of all the tags appears, displaying the following information.

Column	Description
TAG NAME	The name of the tag.

Column	Description
DESCRIPTION	The description of the tag.
COLLECTOR NAME	The name of the collector instance to which you have added the tag.
LAST 10 VALUES	The last 10 values collected for the tag, plotted as a trend chart. If you pause over the chart, the minimum, maximum, first, and last values among the 10 values appear.
TAG ALIAS	Indicates whether the tag contains aliases, which are created when you rename the tag using an alias (on page 1224) .

i Tip:
 You can show/hide/reorder columns in the table. For instructions, refer to [Common Tasks in Configuration Hub \(on page 906\)](#).

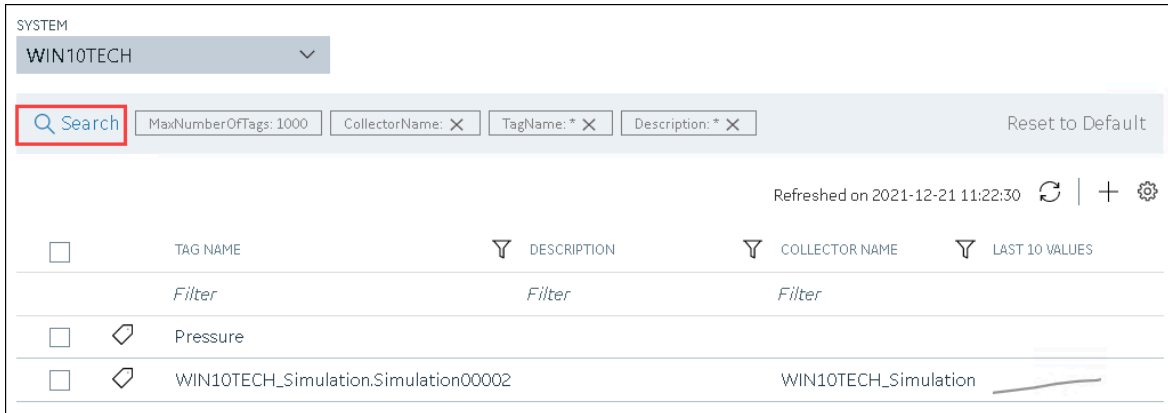
- If you want to access the tags specific to a Historian system, in the drop-down list box in the upper-left corner of the main section, select the system.

The screenshot shows the Configuration Hub interface. At the top left, there is a dropdown menu labeled 'SYSTEM' with 'WIN10TECH' selected. Below this is a search bar with a magnifying glass icon and the text 'Search'. To the right of the search bar are several filter buttons: 'MaxNumberOfTags: 1000', 'CollectorName: X', 'TagName: * X', and 'Description: * X'. A 'Reset to Default' button is located to the right of these filters. Below the search and filter area, there is a refresh indicator showing 'Refreshed on 2021-12-21 11:22:30' and icons for refresh, add, and settings. The main content area displays a table with columns: TAG NAME, DESCRIPTION, COLLECTOR NAME, and LAST 10 VALUES. Each column has a filter icon and the word 'Filter' below it. The table contains two rows of data: one for 'Pressure' and one for 'WIN10TECH_Simulation.Simulation00002'.

Alternatively, you can access the system from the **NAVIGATION** section, right-click the system (or select **☰**), and then select **Browse Tags**.

The list of tags is filtered to display only the tags specific to the system.

- If you want to narrow down the search results, select **Search**.



Enter the search criteria, and then select **Search**. You can add more attributes by selecting **Add Attribute**. You can enter a name or a value partially or use the wildcard character asterisk (*).

The tags are filtered based on the search criteria.

5. Select the row containing the tag that you want to access.



The tag details appear in the **DETAILS** section.


Table 39. The General Section

Field	Description
Tag Name	The name of the tag. This field is disabled and populated.
Description	The description of the tag.
Comment	Comments that apply to the tag.
StepValue	Indicates that the actual measured value changes in a sharp step instead of a smooth linear interpolation. This option is applicable only for numeric data. Enabling this option only affects data retrieval; it has no effect on data collection or storage.
Last Modified Time	The date the last tag parameter modification was made. This field is disabled and populated.
Last Modified User	The name of the person who last modified the tag configuration parameters. This field is disabled and populated.

Table 40. The Collection Section

Field	Description
Collector	The name of the collector that collects data for the selected tag.


Field	Description
Source Address	<p>The address for the tag in the data source. Leave this field blank for tags associated with the Calculation or Server-to-Server collector.</p> <p>For Python Expression tags, this field contains the full applicable JSON configuration, which includes an indication of the source address.</p> <div data-bbox="573 506 1419 772" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: When exporting or importing tags using the Excel Add-in for Historian, the Calculation column, not the SourceAddress column, holds the formulas for tags associated with the Calculation or Server-to-Server collector.</p> </div>
Data Type	<p>The data type of the tag.</p> <p>The main use of the scaled data type is to save space, but this results in a loss of precision. Instead of using 4 bytes of data, it only uses 2 bytes by storing the data as a percentage of the EGU limit. Changing the EGU limits will result in a change in the values that are displayed. For example, if the original EGU values were 0 to 100 and a value of 20 was stored using the scaled data type and if the EGUs are changed to 0 to 200, the original value of 20 will be represented as 40.</p> <div data-bbox="573 1205 1419 1430" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: If you change the data type of an existing tag between a numeric and a string or binary data type (and vice versa), the tag's compression and scaling settings will be lost.</p> </div>
Value	The number of bytes for a fixed string data type. This field is enabled only for fixed string data types.
Enumerated Set Name	The name of the enumerated set (on page 1234) that you want to assign to the tag.
Array Tag	Indicates that the tag is an array tag (on page 1190) .
Location	The distributed location of the system in which the tag data is stored (applicable only for a horizontally scalable system).
Data Store	The data store in which the tag data is stored.

Field	Description
Collection	Indicates whether data collection is enabled or disabled for the tag. If you disable collection for the tag, Historian stops collecting data for the tag, but does not delete the tag or its data.
Collection Type	The type of data collection used for this tag, which can be polled or unsolicited. Polled means that the data collector requests data from the data source at the collection interval specified in the polling schedule. Unsolicited means that the data source sends data to the collector whenever necessary (independent of the data collector polling schedule).
Collection Interval	The time interval between readings of data from this tag. With Unsolicited Collection Type, this field defines the minimum interval at which unsolicited data should be sent by the data source.
Collection Offset	<p>Used with the collection interval to schedule collection of data from a tag. For example, to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), enter a collection interval of 1 hour and an offset of 30 minutes. Similarly, to collect a value each day at 8am, enter a collection interval of 1 day and an offset of 8 hours.</p> <div data-bbox="570 1115 1419 1383" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: If you enter a value in milliseconds, the value must be in intervals of 1000 ms. For example, 1000, 2000, and 3000 ms are valid values, but 500 and 1500 ms are invalid. The minimum value is 1000 ms.</p> </div>
Time Resolution	The precision for timestamps, which can be either seconds, milliseconds or microseconds.
Condition-Based	Indicates whether condition-based data collection (on page 1197) is enabled.
Trigger Tag	The name of the trigger tag used in the condition.
Comparison	The comparison operator that you want to use in the condition. Select one of the following options:

Field	Description
	<ul style="list-style-type: none"> ◦ Undefined: Collection will resume only when the value of the triggered tag changes. This is considered an incomplete configuration, so condition-based collection is turned off and all the collected data is sent to archiver. ◦ < =: Setting condition as trigger tag value less than or equal to the compare value. ◦ > =: Setting condition as trigger tag value greater than or equal to the compare value. ◦ <: Setting condition as trigger tag value less than the compare value. ◦ >: Setting condition as trigger tag value greater than the compare value. ◦ =: Setting condition as trigger tag value equals compare value. ◦ ! =: Setting condition as trigger tag value not the same as compare value.
Compare Value	A target value that you want to compare with the value of the trigger tag. If using = and != comparison parameters, ensure that the format of the compared value and triggered tag are the same. For example, for a float type trigger tag, the compare value must be a float value; otherwise, the condition result is an invalid configuration. When the configuration is invalid, condition-based collection is disabled and all data is sent to archiver.
End of Collection Markers	Indicates whether end-of-collection markers are enabled. This will mark all the tag's values as bad, and sub-quality as ConditionCollectionHalted when the condition becomes false. Trending and reporting applications can use this information to indicate that the real-world value was unknown after this time until the condition becomes true and a new sample is collected. If disabled, a bad data marker is not inserted when the condition becomes false.

Table 41. The Collection Options Section

Field	Description
Data Collection	Indicates whether data collection is enabled or disabled for the tag. If you disable collection for the tag, Historian stops collecting data for the tag, but does not delete the tag or its data.

Field	Description
Collection Type	<p>The type of data collection used for this tag:</p> <ul style="list-style-type: none"> ◦ Polled: The data collector requests data from the data source at the collection interval specified in the polling schedule. ◦ Unsolicited: The data source sends data to the collector whenever necessary (independent of the data collector polling schedule).
Collection Interval	<p>The time interval between readings of data from this tag. For unsolicited collection type, this field defines the minimum interval at which unsolicited data should be sent by the data source.</p>
Collection Offset Value and Collection Offset	<p>Used with the collection interval to schedule collection of data from a tag. For example, to collect a value for a tag every hour at thirty minutes past the hour (12:30, 1:30, 2:30, and so on), enter a collection interval of 1 hour and an offset of 30 minutes. Similarly, to collect a value each day at 8am, enter a collection interval of 1 day and an offset of 8 hours.</p> <div data-bbox="574 919 1419 1184" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note: If you enter a value in milliseconds, the value must be in intervals of 1000 ms. For example, 1000, 2000, and 3000 ms are valid values, but 500 and 1500 ms are invalid. The minimum value is 1000 ms.</p> </div>
Time Resolution	<p>The precision for timestamps, which can be either seconds, milliseconds or microseconds.</p>
Condition based collection	<p>Indicates whether condition-based data collection (on page 1197) is enabled.</p>
Trigger Tag	<p>The name of the trigger tag used in the condition.</p>
Comparison	<p>The comparison operator that you want to use in the condition. This field is enabled only if you have enabled condition-based collection. Select one of the following options:</p> <ul style="list-style-type: none"> ◦ Undefined: Collection will resume only when the value of the triggered tag changes. This is considered an incomplete configuration, so condition-based collection is turned off and all the collected data is sent to archiver. ◦ < =: Setting condition as trigger tag value less than or equal to the compare value.

Field	Description
	<ul style="list-style-type: none"> ◦ > = Setting condition as trigger tag value greater than or equal to the compare value. ◦ <=: Setting condition as trigger tag value less than the compare value. ◦ >: Setting condition as trigger tag value greater than the compare value. ◦ =: Setting condition as trigger tag value equals compare value. ◦ !=: Setting condition as trigger tag value not the same as compare value.
Compare Value	<p>A target value that you want to compare with the value of the trigger tag. If using = and != comparison parameters, ensure that the format of the compared value and triggered tag are the same. For example, for a float type trigger tag, the compare value must be a float value; otherwise, the condition result is an invalid configuration. When the configuration is invalid, condition-based collection is disabled and all data is sent to archiver.</p>
End of Collection Markers	<p>Indicates whether end-of-collection markers are enabled. This will mark all the tag's values as bad, and sub-quality as ConditionCollectionHalted when the condition becomes false. Trending and reporting applications can use this information to indicate that the real-world value was unknown after this time until the condition becomes true and a new sample is collected. If disabled, a bad data marker is not inserted when the condition becomes false.</p>


Table 42. The Scaling Section

Field	Description
EGU Description	The engineering units assigned to the tag.
Hi Engineering Units	<p>The current value of the upper range limit of the span for this tag.</p> <p>Engineering Hi and Lo are retrieved automatically for F_CV fields for iFIX tags; all others are left at default settings. When adding tags from the server using an OPC Collector, the OPC Collector queries the server for the EGU units and EGU Hi/Lo limits. However, not all OPC Servers make this information available. There-</p>

Field	Description
	fore, if the server does not provide the limits when requested to do so, the collector automatically assigns an EGU range of 0 to 10,000.
Lo Engineering Units	The current value of the lower range limit of the span for this tag.
Input Scaling	<p>Indicates whether input scaling is enabled, which converts an input data point to an engineering units value.</p> <p>For example, to rescale and save a 0 - 4096 input value to a scaled range of 0 - 100, enter 0 and 4096 as the low and high input scale values and 0 and 100 as the low and high engineering units values, respectively.</p> <p>If a data point exceeds the high or low end of the input scaling range, Historian logs a bad data quality point with a ScaledOutOfRange subquality. In the previous example, if your input data is less than 0, or greater than 4096, Historian records a bad data quality for the data point.</p> <p>OPC Servers and TRUE Values: Some OPC servers return a TRUE value as -1. If your OPC server is returning TRUE values as -1, modify the following scaling settings:</p> <ul style="list-style-type: none"> ◦ Hi Engineering Units: Enter 0. ◦ Lo Engineering Units: Enter 1. ◦ Hi Scaling Value: Enter 0. ◦ Lo Scaling Value: Enter -1. ◦ Input Scaling: Enable this option.
Hi Scaling Value	The upper limit of the span of the input value.
Lo Scaling Value	The lower limit of the span of the input value.

Table 43. The Collector Compression Section

Field	Description
Collector Compression	Indicates whether collector compression (on page 1190) is enabled.

Field	Description
Collector Deadband and Deadband value	<p>The current value of the compression deadband. This value can be computed as a percent of the span, centered around the data value or given as an absolute range around the data value.</p> <div data-bbox="573 432 1419 743" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: Some OPC servers add and subtract the whole deadband value from the last data value. This effectively doubles the magnitude of the deadband compared to other OPC servers. To determine how your specific server handles deadband, refer to the documentation of your OPC server.</p> </div> <p>Example:</p> <p>Suppose the engineering units are 0 to 200. Suppose the deadband value is 10%, which is 20 units. If the deadband value is 10% and the last reported value is 50, the value will be reported when the current value exceeds $50 + 10 = 60$ or is less than $50 - 10 = 40$. Note that the deadband (20 units) is split around the last data value (10 on either side.)</p> <p>Alternatively, you could specify an absolute deadband of 5. In this case, if the last value was 50, a new data sample will be reported when the current value exceeds 55 or drops below 45.</p> <p>If compression is enabled and the deadband is set to zero, the collector ignores data values that do not change and records any that do change. If you set the deadband to a non-zero value, the collector records any value that lies outside the deadband. If the value changes drastically, a pre-spike point may be inserted.</p>
Engineering Unit	<p>Converts the deadband percentage into engineering units and displays the result. This value establishes the deadband range that is centered around the new value.</p> <p>This field represents a calculated number created to give an idea of how large a deadband you are creating in engineering units. The deadband is entered in percentage and Historian converts the percentage in to engineering units.</p>


Field	Description
Compression Timeout and Compression Timeout Interval	<p>Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver. This time is maintained per tag, as different tags report to the archiver at different times.</p> <p>For polled tags, this value should be in multiples of your collection interval. After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred. For example, if you have a 10-second collection interval, a 1-minute compression timeout, and a collection that started at 2:14:00, if the value has not changed, the value is logged at 2:15:10 and not at 2:15:00.</p> <p>For unsolicited tags, a value is guaranteed in, at most, twice the compression timeout interval.</p> <p>A non-changing value is logged on each compression timeout. For example, an unsolicited tag with a 1-second collection interval and a 30-second compression timeout is stored every 30 seconds.</p> <p>A changing value for the same tag may have up to 60 seconds between raw samples. In this case, if the value changes after 10 seconds, then that value is stored, but the value at 30 seconds (if unchanged) will not be stored. The value at 60 seconds will be stored. This leaves a gap of 50 seconds between raw samples which is less than 60 seconds.</p> <p>Compression timeout is supported in all collectors except the PI collector.</p>

Table 44. The Archive Compression Section

Field	Description
Archive Compression	Indicates whether archive compression (on page 1190) is enabled. If enabled, Historian applies the archive deadband settings against all reported data from the collector.
Archive Deadband and Deadband value	The current value of the archive deadband, expressed as a percent of span or an absolute number.

Field	Description
Engineering Unit	Converts the deadband percentage into engineering units and displays the result. This value establishes the deadband range that is centered around the new value.
Compression Time-out and Compression Timeout Interval	<p>The maximum amount of time from the last stored point before another point is stored, if the value does not exceed the archive compression deadband.</p> <p>The data archiver treats the incoming sample after the timeout occurs as if it exceeded compression. It then stores the pending sample.</p>

Table 45. The Advanced Section

Field	Description
Time Assigned By	<p>The source of the timestamp for a data value is either the collector or the data source.</p> <p>All tags, by default, have their time assigned by the collector. When you configure a tag for a polled collection rate, the tag is updated based on the collection interval. For example, if you set the collection interval to 5 seconds with no compression, then the archive will be updated with a new data point and timestamp every 5 seconds, even if the value is not changing.</p> <p>However, if you set the Time Assigned By field to Source for the same tag, the archive only updates when the device timestamp changes. For example, if the poll time is still 5 seconds, but if the timestamp on the device does not change for 10 minutes, no new data will be added to the archive for 10 minutes.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;">  Note: This field is disabled for Calculation and Server-to-Server tags. </div>
Time Zone Bias	<p>The number of minutes from GMT that should be used to translate timestamps when retrieving data from this tag. For example, the time zone bias for Eastern Standard time is -300 minutes (GMT-5).</p> <p>This field is not used during collection. Use this option if a particular tag requires a time zone adjustment during retrieval other than the client</p>


Field	Description
	or server time zone. For example, you could retrieve data for two tags with different time zones by using the tag time zone selection in the iFIX chart.
Time Adjustment	<p>If the Server-to-Server collector is not running on the source computer, select the Adjust for Source Time Difference option to compensate for the time difference between the source archiver computer and the collector computer.</p> <div data-bbox="573 621 1419 800" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: This field only applies to tags associated with the Server-to-Server collector that use a polled collection type.</p> </div>

Table 46. The Security Section

Field	Description
Read Group	<p>The Windows security group that can retrieve the tag data and plot it in a trend chart.</p> <p>For example, if you select a group with power users, in addition to members of the iH Security Admins group, only a member of the power users group will be able to read data for that tag. Even a member of the iH Readers group will not be able to access data for that tag, unless they are also defined as a member of the power users group.</p>
Write Group	The Windows security group that can write tag data (for example, using the Excel Add-in for Historian).
Administer Group	The Windows security group that can create, modify, and delete the tag.



Note:

If you are using domain groups (instead of local groups), the **Read Group**, **Write Group**, and **Administer Group** fields contain only the groups whose names begin with iH<space> (case-sensitive). Therefore, ensure that the group that you want to use begins with iH<space>.

Table 47. The Delta Query Section

Field	Description
Delta Max Value	The maximum value that a tag can have. It also called the rollover point of the counter or totalizer. If the tag values exceed MaxValue, the counter is reset to the minimum value. If you do not provide MaxValue, the delta query cannot check for a positive counter wrap.
Delta Min Value	The minimum value that a tag can have. If the tag values are less than MinValue (and the counter is going in the negative direction), the tag values are reset to MaxValue. If you do not provide MinValue, 0 is considered.
Delta Max Positive RPH	The maximum rate per hour between two consecutive data points in the positive direction. If two consecutive data points exceed this value, they are not considered in a delta query.
Delta Max Negative RPH	<p>The maximum rate per hour between two consecutive data points in the negative direction. If two consecutive data points exceed this value, they are not considered in a delta query.</p> <p>The Delta Max Positive RPH and Delta Max Negative RPH values are used to determine if a counter wrap has occurred or if the counter has been manually reset. They help ignore data points whose values increase or decrease drastically.</p>

For information on how these values are calculated, refer to [Counter Delta Queries](#).

The Spare Fields section

Spare configuration enables you to add additional configuration to the tag using the **Spare Field 1** to **Spare Field 5** fields in all the collectors except in a Server-to-Server collector, Server-to-Server distributor, and an OSI PI distributor.

- In case of an OSI PI distributor, data is read from the Historian tag displayed in the **Source Address** field and sent to the OSI PI tag name displayed in the **Spare Field 1** field. To control the source and destination tags, change the **Source Address** and **Spare Field 1** values. You can add or update values in the remaining spare fields.
- In case of Server-to-Server collector and Server-to-Server distributor, you can update the **Spare Field 1** to **Spare Field 4** values, but the **Spare Field 5** field is used only for internal purposes. Therefore, do not update the **Spare Field 5** field.

The TAG ALIAS Section

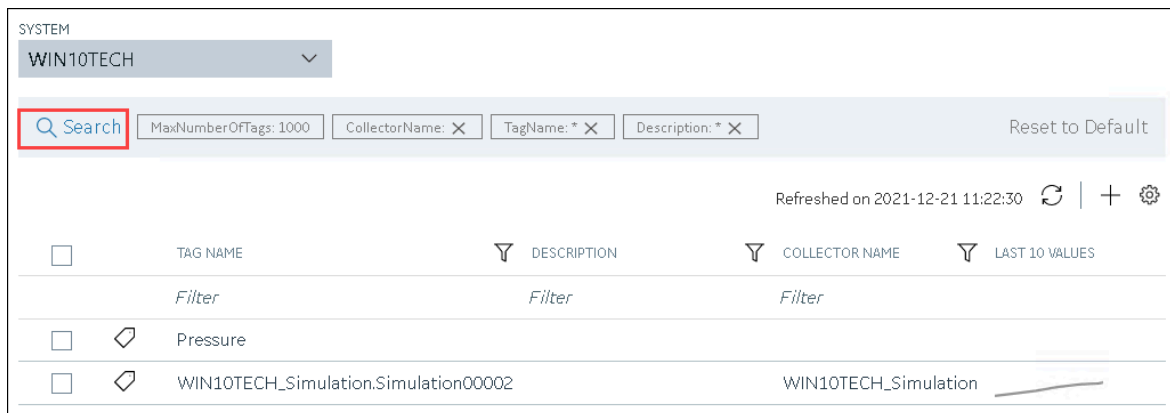
Contains a list of the old names of the tag that you have renamed using an alias. For more information, refer to [Rename a Tag \(on page 1224\)](#).

Access the Trend Chart of Tag Values

This topic describes how to access the values of a tag in a trend chart. The difference in the timestamp of consecutive values depends on the time resolution of the tag. For example, if the time resolution is seconds, the timestamp of consecutive values of the tag will be one second apart.

You can plot the trend chart for up to 10 tags at a time.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Tags**.
A list of all the tags appears.
3. If you want to narrow down the search results, select **Search**.



Enter the search criteria, and then select **Search**. You can add more attributes by selecting **Add Attribute**. You can enter a name or a value partially or use the wildcard character asterisk (*). The list of tags are filtered based on the search criteria.


4. If you want to access the trend chart of a single tag, right-click the tag (or select **☰**), and then select **Trend**.

The screenshot shows the Configuration Hub interface for the 'WIN10TECH' system. At the top, there is a search bar with filters for 'MaxNumberOfTags: 1000', 'CollectorName: X', 'TagName: * X', and 'Description: * X'. Below the search bar, a table lists tags with columns for 'TAG NAME', 'DESCRIPTION', 'COLLECTOR NAME', and 'LAST 10 VALUES'. The tag 'WIN10TECH_Simulation.Simulation00002' is selected, and a context menu is open over it, showing options like 'Trend', 'View Last 10 Values', 'View Aliases', 'Rename', 'Permanent Rename', 'Copy', 'Stop Data Collection', 'Remove Tag From System', and 'Delete'. The 'Trend' option is highlighted with a red box.

If you want to access the trend chart for multiple tags, select the check boxes corresponding to the tags, right-click (or select **☰**), and then select **Trend**. You can select up to 10 tags. The tag values are plotted on a trend chart. You can switch between the trend view and the table view.



Tip:

You can also filter the chart by changing the duration, sampling type, time interval, and so on by selecting .

Access the Last 10 Values of a Tag

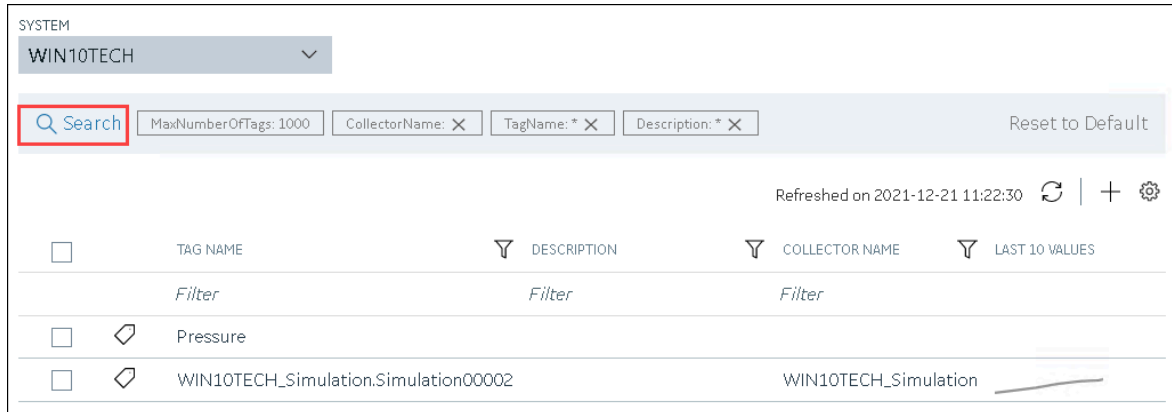
This topic describes how to access the last 10 values of a tag up to the current time. The difference in the timestamp of consecutive values depends on the time resolution of the tag. For example, if the time resolution is seconds, the timestamp of consecutive values of the tag will be one second apart.



Note:

If a tag name contains a comma or a semicolon, you cannot view the last 10 values of the tag.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Tags**.
A list of all the tags appears.
3. If you want to narrow down the search results, select **Search**.



Enter the search criteria, and then select **Search**. You can add more attributes by selecting **Add Attribute**. You can enter a name or a value partially or use the wildcard character asterisk (*). The list of tags are filtered based on the search criteria.

4. If you want to access the last 10 values of a single tag, right-click the tag (or select **Filter**), and then select **View Last 10 Values**.

The screenshot shows the Configuration Hub Historian interface. At the top, the system is set to 'WIN10TECH'. Below this is a search bar and filter options: 'MaxNumberOfTags: 1000', 'CollectorName: X', 'TagName: * X', and 'Description: * X'. A 'Reset to Default' button is on the right. The main area displays a table of tags with columns for TAG NAME, DESCRIPTION, COLLECTOR NAME, and LAST 10 VALUES. The tag 'WIN10TECH_Simulation.Simulation00002' is selected, and a context menu is open over it. The menu options are: Trend, View Last 10 Values (highlighted with a red box), View Aliases, Rename, Permanent Rename, Copy, Stop Data Collection, Remove Tag From System, and Delete. The interface also shows a refresh status: 'Refreshed on 2021-12-21 11:22:30' and a page number '1' at the bottom right.

If you want to access the last 10 values of multiple tags, select the check boxes corresponding to the tags, right-click (or select **☰**), and then select **Trend**. You can select up to 10 tags. The last 10 values of the tag appear, along with the timestamp and quality of each value. You can switch between the trend view and the table view.

In table view you can view data attributes which are introduced to store the 128-bit subquality for every sample.

SCADA applications such as Habitat support data samples with several quality types. To support such SCADA applications, Historian is now enhanced to store up to 128-bit quality types, which are stored in the data attributes. These attributes are extended qualities that you can store more than the regular qualities and subqualities (such as good and bad).

In addition to regular qualities, the HAB collector collects extends qualities such as replaced, suspect, garbage, old, and so on.

The Data Attributes are displayed in the table view along with Timestamp, Value, and Quality.


Data Attributes are supported for Current Value, Raw by Number, Raw by Time, Lab, and Lab to Raw .

In addition:

- For an array tag, all the values in the array appear for each timestamp.
- For a tag using an enumerated set, values of all the states appear for each timestamp.
- For a tag using a user-defined data type (UDT), values for all the fields appear for each timestamp.



Tip:

You can also filter the values by changing the duration, sampling type, time interval, and so on by selecting .

Time Stamp	Value	QUALITY	Data Attributes
<i>Fiber</i>	<i>Fiber</i>	<i>Fiber</i>	<i>Fiber</i>
12/6/2022, 12:40:07 PM	61122.47266	Good	22.21.20.19.14.13.12.11.6.5.4.3
12/6/2022, 12:40:09 PM	28003.78516	Good	22.21.20.19.14.13.12.11.6.5.4.3
12/6/2022, 12:40:11 PM	176995.1406	Good	22.21.20.19.14.13.12.11.6.5.4.3
12/6/2022, 12:40:13 PM	4205.450684	Good	22.21.20.19.14.13.12.11.6.5.4.3
12/6/2022, 12:40:14 PM	174858.8594	Good	22.21.20.19.14.13.12.11.6.5.4.3
12/6/2022, 12:40:16 PM	148283.3281	Good	22.21.20.19.14.13.12.11.6.5.4.3
12/6/2022, 12:40:18 PM	2050.84375	Good	22.21.20.19.14.13.12.11.6.5.4.3
12/6/2022, 12:40:20 PM	158946.5	Good	22.21.20.19.14.13.12.11.6.5.4.3
12/6/2022, 12:40:22 PM	194219.7969	Good	22.21.20.19.14.13.12.11.6.5.4.3
12/6/2022, 12:40:23 PM	96792.50781	Good	22.21.20.19.14.13.12.11.6.5.4.3

Access a Tag Alias

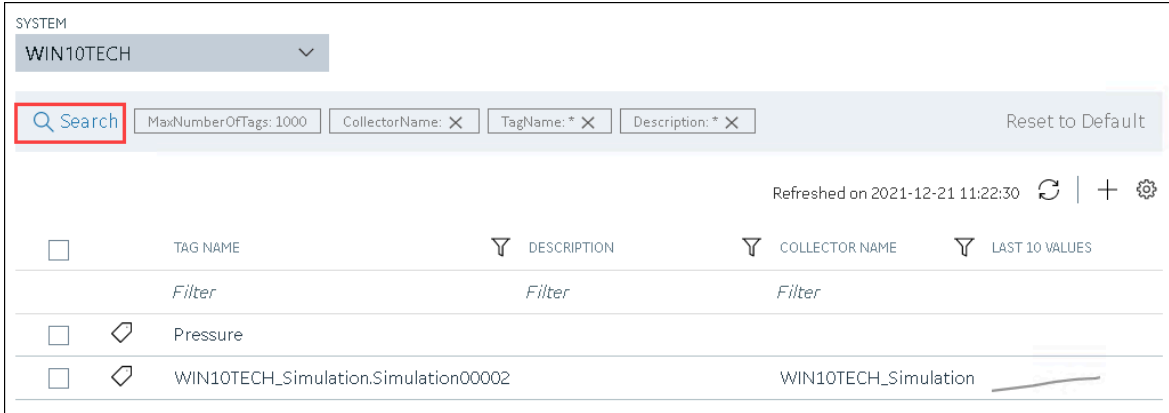
After you rename a tag, the old name is called the tag alias. You can retrieve tag data using the tag alias as well. When you copy a tag, the tag alias is also captured to aid in an audit trail.



Note:

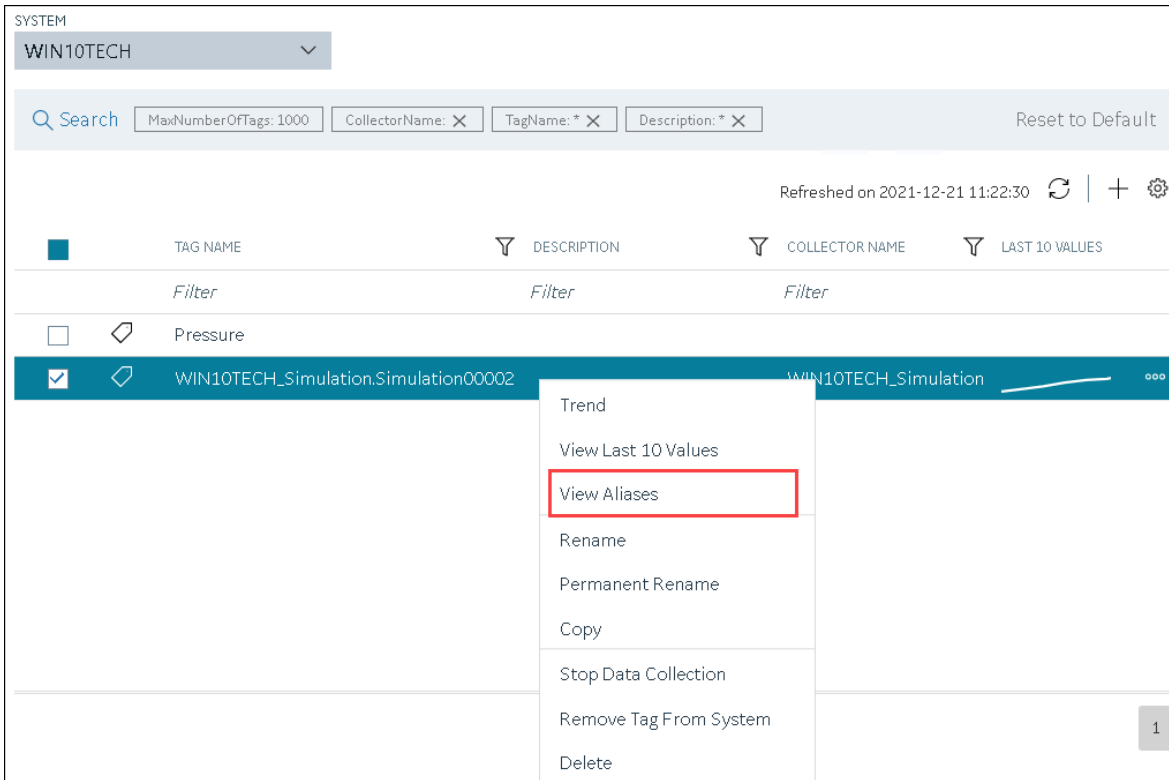
If a tag name contains a comma or a semicolon, you cannot view the tag alias.


1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Tags**.
A list of all the tags appears.
3. If you want to narrow down the search results, select **Search**.



Enter the search criteria, and then select **Search**. You can add more attributes by selecting **Add Attribute**. You can enter a name or a value partially or use the wildcard character asterisk (*). The list of tags are filtered based on the search criteria.

4. Right-click the tag whose alias you want to access (or select **⋮**), and then select **View Aliases**.



Alternatively, you can select  in the **TAG ALIAS** column.
All the tag aliases of the selected tag appear.

Rename a Tag

To rename a tag, you must be a member of the administrator's group with tag-level security.

When you rename a tag, you can choose between the following options:

- **Rename using an alias:** In this case, the old name is called the tag alias. You can retrieve tag data using the tag alias as well. When you copy a tag, the tag alias is captured as well to aid in an audit trail.



Note:

If a tag name contains a comma or a semicolon, you cannot view the tag alias.

- **Rename permanently:** In this case, the old name is no longer captured. Therefore, you can create another tag with this old name. You cannot store and forward data using the old name. This implies that data for the tag is collected separately for the new name.

1. [Access Configuration Hub \(on page 902\).](#)
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Tags**.
A list of all the tags appears.
3. If you want to narrow down the search results, select **Search**.

The screenshot shows the Configuration Hub interface for tags. At the top, there is a 'SYSTEM' dropdown menu set to 'WIN10TECH'. Below this is a search bar with a magnifying glass icon and the text 'Search', which is highlighted with a red box. To the right of the search bar are several filter buttons: 'MaxNumberOfTags: 1000', 'CollectorName: X', 'TagName: * X', and 'Description: * X'. A 'Reset to Default' button is located on the far right of the search bar. Below the search bar, there is a refresh button and a plus sign icon. The main area displays a table of tags with columns for 'TAG NAME', 'DESCRIPTION', 'COLLECTOR NAME', and 'LAST 10 VALUES'. Each row has a checkbox and a tag icon. The first row shows 'Pressure' and the second row shows 'WIN10TECH_Simulation.Simulation00002' with a collector name of 'WIN10TECH_Simulation'.

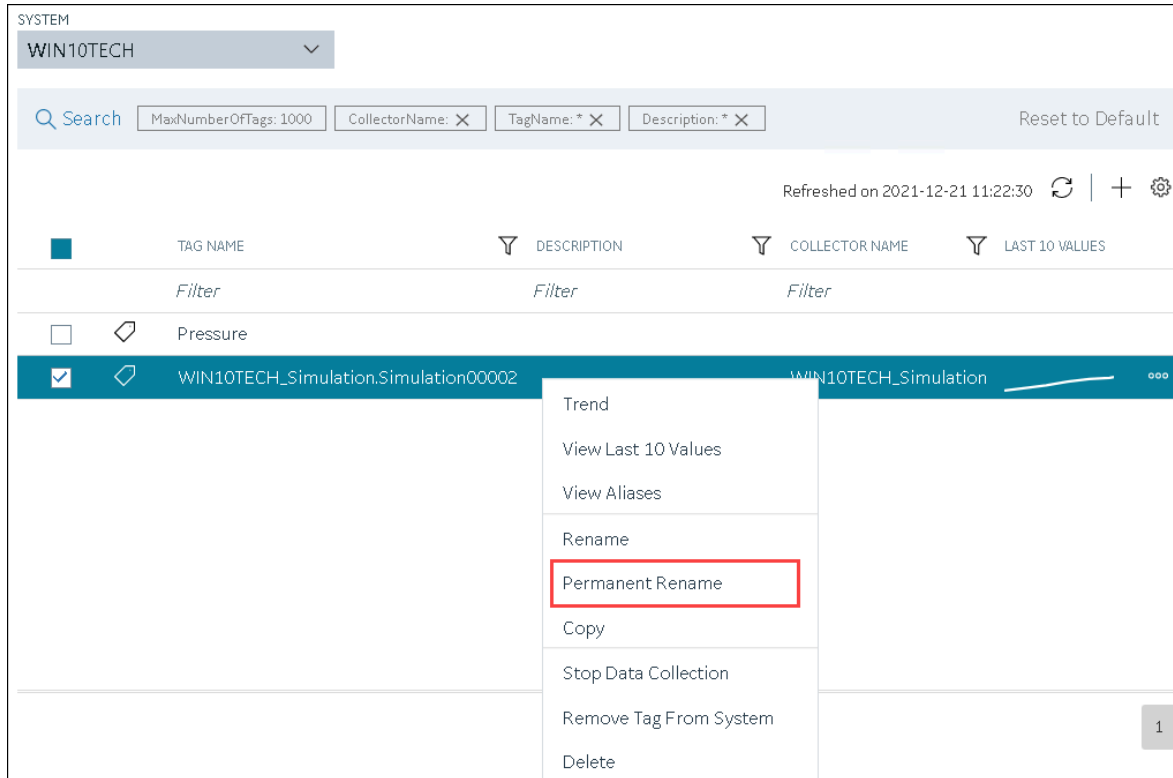
Enter the search criteria, and then select **Search**. You can add more attributes by selecting **Add Attribute**. You can enter a name or a value partially or use the wildcard character asterisk (*).

The list of tags are filtered based on the search criteria.

4. Right-click the tag that you want to rename (or select **☰**).
5. If you want to rename the tag using an alias, select **Rename**.


The screenshot displays the Configuration Hub Historian interface. At the top, the system is identified as 'WIN10TECH'. Below this, there is a search bar and filter controls for 'MaxNumberOfTags: 1000', 'CollectorName: X', 'TagName: * X', and 'Description: * X'. A 'Reset to Default' button is also present. The interface shows a table of tags with columns for 'TAG NAME', 'DESCRIPTION', 'COLLECTOR NAME', and 'LAST 10 VALUES'. The tag 'WIN10TECH_Simulation.Simulation00002' is selected, and a context menu is open over it. The 'Rename' option in the menu is highlighted with a red box. Other options in the menu include 'Trend', 'View Last 10 Values', 'View Aliases', 'Permanent Rename', 'Copy', 'Stop Data Collection', 'Remove Tag From System', and 'Delete'. The page number '1' is visible in the bottom right corner.

If you want to rename the tag permanently, select **Permanent Rename**.



The **Rename Tag: <tag name>** window or the **Permanent Rename Tag: <tag name>** window appears.

6. Enter the new name of the tag, and then select **Rename**. The tag name must be unique in the Historian server.

The tag is renamed. If you have renamed using an alias, the **TAG ALIAS** column displays , indicating that the tag now has an alias.

If you have renamed the tag permanently:

- If the tag is used as a trigger, reassign the trigger.
- [Restart the collector instance \(on page 1173\)](#).

Copy a Tag

If you want to create a tag with the same properties as another one, you can copy it, and then modify the properties as needed. When you copy a tag, the tag alias is captured as well to aid in an audit trail.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Tags**.
A list of all the tags appears.
3. If you want to narrow down the search results, select **Search**.

SYSTEM
WIN10TECH

Q Search MaxNumberOfTags: 1000 CollectorName: X TagName: * X Description: * X Reset to Default

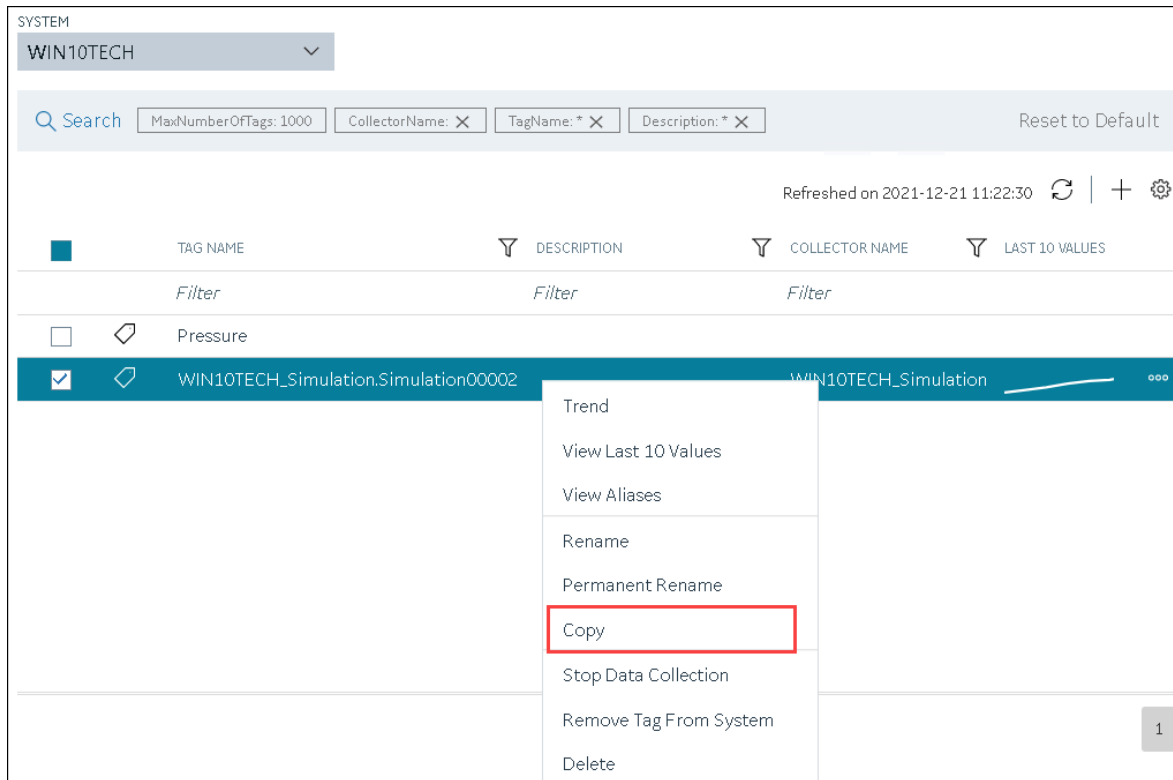
Refreshed on 2021-12-21 11:22:30

<input type="checkbox"/>	TAG NAME	DESCRIPTION	COLLECTOR NAME	LAST 10 VALUES
<input type="checkbox"/>	Pressure			
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00002		WIN10TECH_Simulation	

Enter the search criteria, and then select **Search**. You can add more attributes by selecting **Add Attribute**. You can enter a name or a value partially or use the wildcard character asterisk (*).

The list of tags are filtered based on the search criteria.

4. Right-click the tag that you want to copy (or select **...**), and then select **Copy**.



The **Copy Tag: <tag name>** window appears.

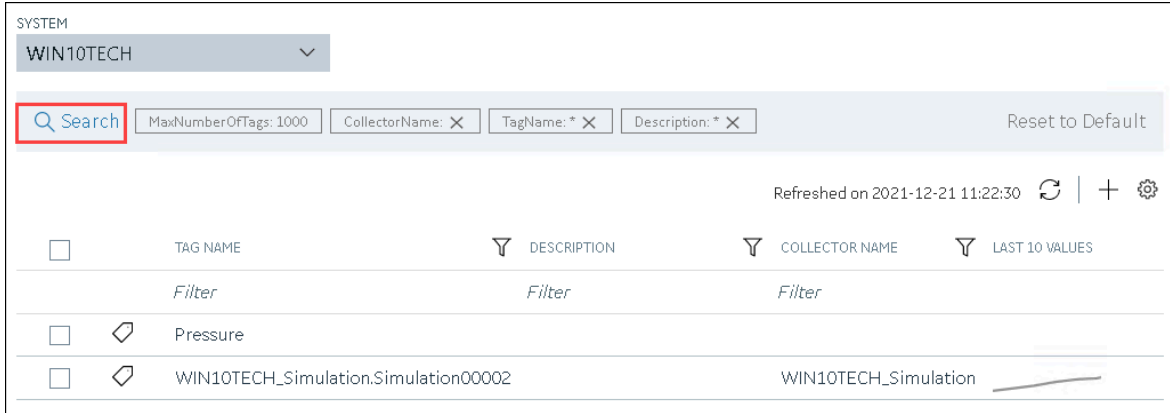
5. In the **NEW TAG NAME** field, provide a name for the tag. A value is required and must be unique for the Historian system.
6. Select **Copy**.

The tag is copied, inheriting the properties of the original tag. In addition, data collection begins for the tag.

Stop the Data Collection of a Tag

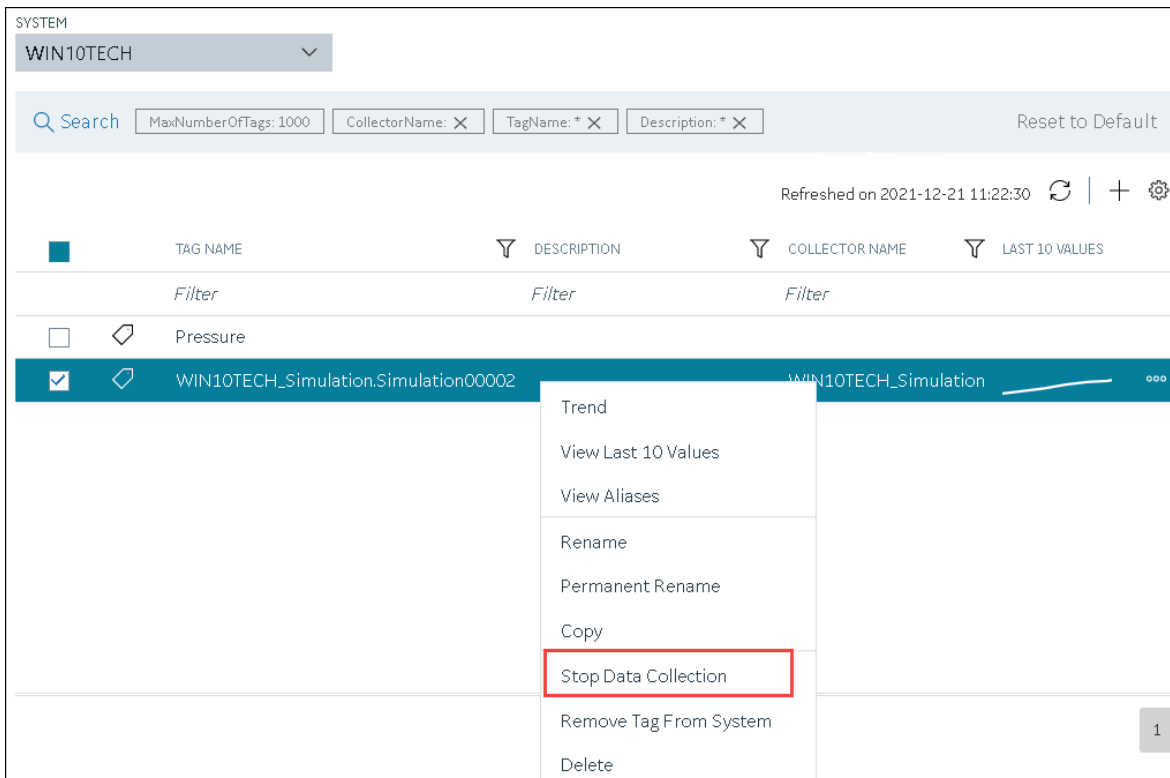
If you want to stop using a tag for a while, you can stop the data collection of the tag, which allows you to resume the data collection later. If, however, you no longer want to use the tag or its data, you can [remove it from the system \(on page 1230\)](#) or [delete it \(on page 1232\)](#).

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Tags**.
A list of all the tags appears.
3. If you want to narrow down the search results, select **Search**.



Enter the search criteria, and then select **Search**. You can add more attributes by selecting **Add Attribute**. You can enter a name or a value partially or use the wildcard character asterisk (*). The list of tags are filtered based on the search criteria.

4. Right-click the tag for which you want to stop data collection (or select **ooo**), and then select **Stop Data Collection**.



A message appears, asking you to confirm that you want to stop the data collection for the tag.

5. Select **Stop**.

Data collection is stopped for the tag.

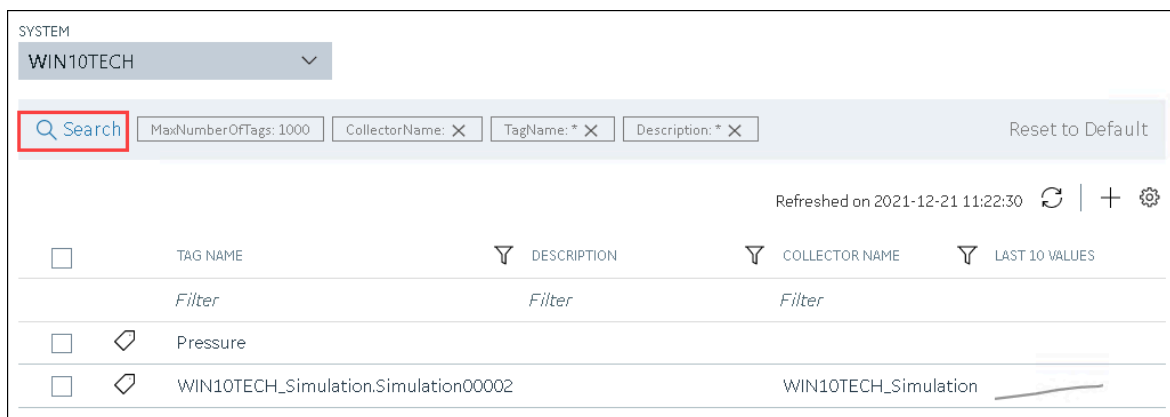
Start the Data Collection of a Tag

1. [Access Configuration Hub \(on page 902\)](#).

2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Tags**.

A list of all the tags appears.

3. If you want to narrow down the search results, select **Search**.



Enter the search criteria, and then select **Search**. You can add more attributes by selecting **Add Attribute**. You can enter a name or a value partially or use the wildcard character asterisk (*).

The list of tags are filtered based on the search criteria.

4. Right-click the tag for which you want to start data collection (or select **⋮**), and then select **Start Data Collection**.

A message appears, asking you to confirm that you want to start the data collection for the tag.

5. Select **Start**.

Data collection is started for the tag.

Remove a Tag from a System

When you remove a tag from a system, the tag and its data will still be available. Therefore, you cannot create a tag with the same name. If, however, you no longer need the tag or its data, you can [delete it \(on page 1232\)](#). Or, you can choose to [stop the data collection \(on page 1228\)](#) for the tag, which allows you to [resume the data collection \(on page 1230\)](#) later.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Tags**.
A list of all the tags appears.
3. If you want to narrow down the search results, select **Search**.

SYSTEM
WIN10TECH

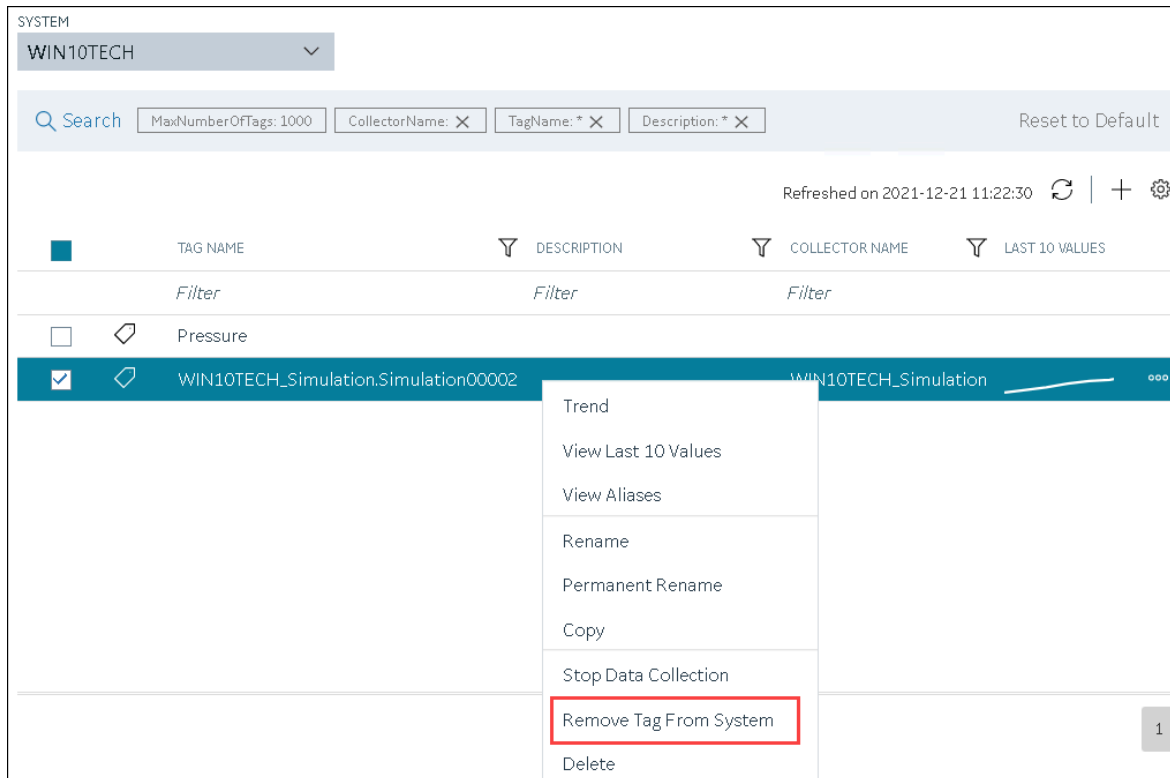
Q Search MaxNumberOfTags: 1000 CollectorName: X TagName: * X Description: * X Reset to Default

Refreshed on 2021-12-21 11:22:30

<input type="checkbox"/>	TAG NAME	DESCRIPTION	COLLECTOR NAME	LAST 10 VALUES
<input type="checkbox"/>	Pressure			
<input type="checkbox"/>	WIN10TECH_Simulation.Simulation00002		WIN10TECH_Simulation	

Enter the search criteria, and then select **Search**. You can add more attributes by selecting **Add Attribute**. You can enter a name or a value partially or use the wildcard character asterisk (*).
The list of tags are filtered based on the search criteria.

4. Right-click the tag that you want to remove (or select **ooo**), and then select **Remove Tag From System**.



A message appears, asking you to confirm that you want to remove the tag from the system.

5. Select **Remove**.

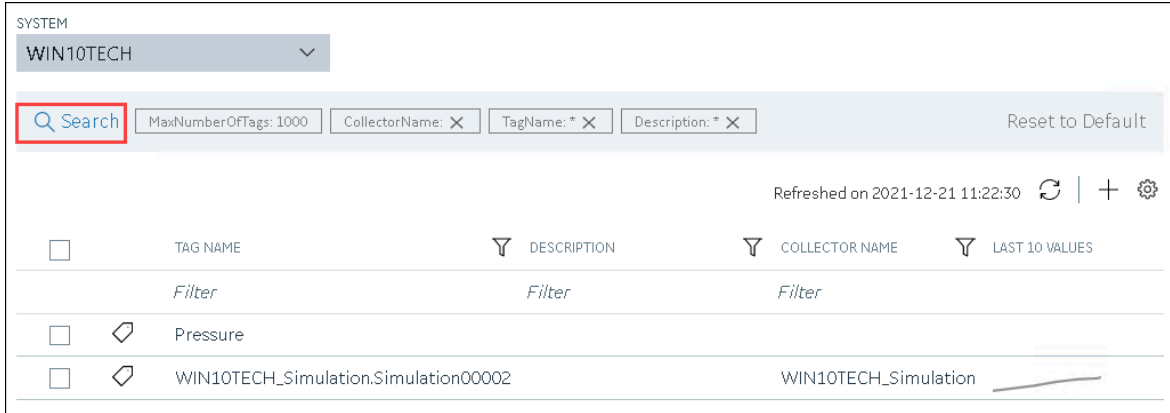
The tag is removed from the system.

Delete a Tag

If the tag that you want to delete is associated with a variable in a Historian model, remove the mapping between the variable and the tag.

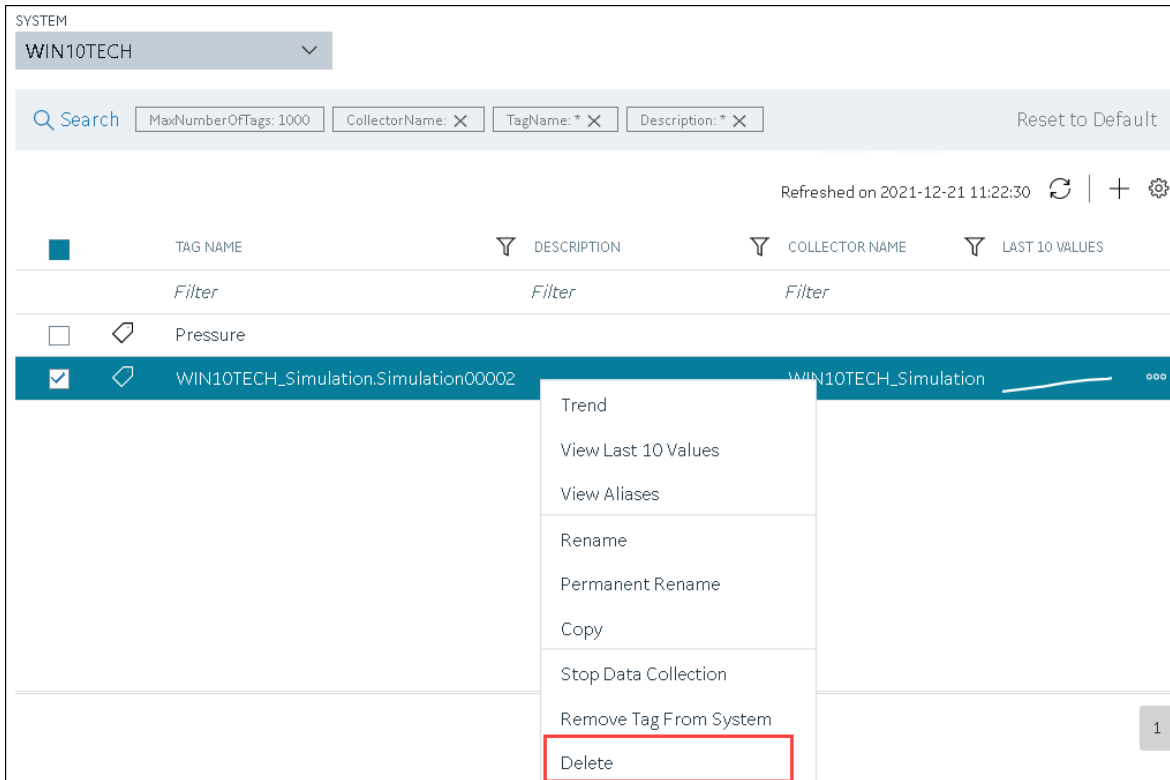
When you delete a tag, it is deleted from Historian, and the tag data will no longer be available. If, however, you want the tag data to be available, instead of deleting the tag, [remove it from the system \(on page 1230\)](#). Or, you can choose to [stop the data collection \(on page 1228\)](#) for the tag, which allows you to [resume the data collection \(on page 1230\)](#) later.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Tags**.
A list of all the tags appears.
3. If you want to narrow down the search results, select **Search**.



Enter the search criteria, and then select **Search**. You can add more attributes by selecting **Add Attribute**. You can enter a name or a value partially or use the wildcard character asterisk (*). The list of tags are filtered based on the search criteria.

4. Right-click the tag that you want to delete (or select **⋮**), and then select **Delete**.



A message appears, asking you to confirm that you want to delete the tag.

5. Select **Delete**.

The tag is deleted.

Managing Enumerated Sets

About Enumerated Sets

An enumerated data set provides an enhanced way of displaying data. It enables you to retrieve numeric data as string state values. You can use the string values in reports, charts, etc.

An enumerated set contains several states. A state is the number-string value pair in a set. It contains a set of numeric values and their corresponding string values. You can define an enumerated set for a single value or a range of values. These state values are defined for data states stored in Data Archiver. Data is retrieved using the value of the state. You have to define state values within a set to assign enumerated values.

Table 48. Example of a Single-Value Enumerated Set

State Name	State Value
Manual	0
Automatic	1

Table 49. Example of a Range-of-Values Enumerated Set:

State Name	State Value
ON	0 to 100
OFF	101 to 200

State names can be duplicated. If duplicated states exist, take precautions to avoid unpredictable results. For example, a tag is associated with an enumerated set defined as follows.

State Name	State Value
0	Open
1	Close
2	Close
2	Open

The server will return unpredictable results due to the State Name duplication for an input of 2.



Note:

You cannot assign an enumerated set to an array tag.

Create an Enumerated Set

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Tags**.
3. Select **☰**, and then select **Manage Enumerated Sets**.
The **Manage Enumerated Sets: <system name>** window appears.
4. Select **New Set**, and enter values as described in the following table.

Field	Description
SET NAME	Enter a name for the set.
DESCRIPTION	Enter a description for the set.
ENUMERATE BY	Specify whether you want to define a single value or a range of values. A single value is best used with integer values because they match exactly. A range of values can be used with floating point values because they may not match exactly due to rounding.
NAME	Enter a name for the state.
VALUE	Enter a numeric value for the state; string values such as on/off are not supported. This field appears only if you select Single Value in the ENUMERATE BY field.
START RANGE and END RANGE	Enter the start and end values of the range. Enter only numeric values; string values are not supported. These fields appear only if you select Range in the ENUMERATE BY field. If you want to assign ON for values 0-100, enter ON in the NAME field, and enter 0 and 100 in the START RANGE and END RANGE fields.
DESCRIPTION (under STATES)	Enter a description for the state.

5. For each state that you want to create, select **Add State**, and repeat the previous step.

6. Select **Save Set**.
7. If needed, add more sets, and then select **Done**.
The enumerated set is created.

[Assign the enumerated set to a tag \(on page 1236\)](#).

Assign an Enumerated Set to a Tag

- [Create the tag \(on page 909\)](#) for which you want to use an enumerated set.
- [Create the enumerated set \(on page 1235\)](#) that you want to assign to a tag.

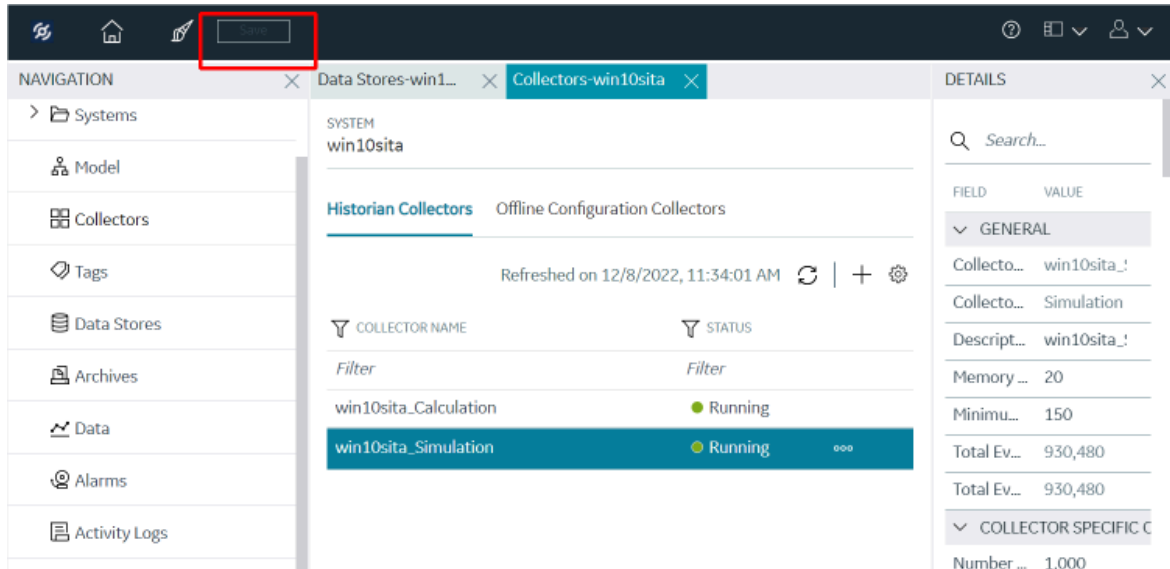
If you assign an enumerated set to a tag, when you retrieve the tag data, instead of the actual values, the corresponding state names appear.

For example, suppose you have created the following states in an enumerated set:

State Name	State Range
ON	0 to 100
OFF	101 to 200

Suppose you assign the enumerated set to a tag. If the tag values are, say, 50, 100, 75, and 104, when you retrieve the tag values, ON, ON, ON, and OFF, respectively, are retrieved instead of the actual tag values.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Tags**.
3. Select the tag to which you want to assign an enumerated set.
The details of the tag appear in the **DETAILS** section.
4. Under **Collection**, in the **Enumerated Set** field, select the enumerated set that you want to assign.
5. In the upper-left corner of the page, select **Save**.



The enumerated set is assigned to the tag. When you now retrieve the tag values, the corresponding state names appear instead of the actual values.

Delete an Enumerated Set

You cannot delete an enumerated set if it is assigned to a tag.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Tags**.
3. Select **...**, and then select **Manage Enumerated Sets**.
The **Manage Enumerated Sets: <system name>** window appears.
4. Select the ENUM set that you want to delete, or select **...**, and then select **Delete**. Or, select next

 to the Set name.

A message appears, asking you to confirm that you want to delete the set.

5. Select **Delete**.

The enumerated set is deleted.

Managing User-Defined Data Types

About User-Defined Data Types

Sometimes, a single tag cannot store all the required details of a parameter. For example, if you want to store the name, address, and phone number of the manufacturer of a machine, it may not be feasible to store all these details in a single tag, which uses a single data type. In such cases, you can create a user-defined data type (UDT), which includes one or more fields, and then apply that type to Historian tags. Each of these fields in a UDT can contain a different data type based on your requirement.

The following conditions apply when working with a UDT:

- You must have appropriate security permissions to create, modify, and delete a UDT. The type can have its own Administrator security group.
- You cannot create an array tag that uses a UDT.
- UDTs cannot have fields of Scaled or FixedString data types.
- Scaling, collector compression, and archive compression do not apply to UDT tags.
- You cannot associate an enumerated set with a UDT tag.
- A UDT supports maximum 100 fields.

Create User-Defined Data Types

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Tags**.
3. Select **☰**, and then select **Manage User-Defined Types**.
The **Manage User-Defined Types: <system name>** window appears.
4. Select **New Type**, and enter values as described in the following table.

Field	Description
TYPE NAME	Enter a name for the user-defined data type (UDT).
DESCRIPTION	Enter a description for the UDT.
ADMINISTER GROUP	Specify the Windows Security Group that you want to assign to the UDT.
DATA QUALITY	Select one of the following options:

Field	Description
	<ul style="list-style-type: none"> ◦ Store Individual Quality: Select this option to store field-level quality. Storing individual qualities consumes more disk space. ◦ Store Master Field Quality: Select this option if you want to assign the same quality as the master field to all the other fields in the UDT. If you select this option, the data sample will have a single quality similar to how an array tag works.
MASTER	Select the radio button corresponding to the field that you want to set as master. When you do so, the data type of this field is used for all the remaining fields in the UDT as well. Only one field can be the master in a UDT. The MASTER column appears only if you select Store Master Field Quality under DATA QUALITY .
NAME	Enter a name for the field.
DESCRIPTION (under FIELD)	Enter a description for the field.
DATA TYPE	Select the data type for the field. If you select Store Master Field under DATA QUALITY , and if you set this field as master, the data type of this field will be applied to the remaining fields in the UDT as well.

5. For each field that you want to create, select **Add Field**, and provide the required details.
6. Select **Save Type**.
7. If needed, add more UDTs, and then select **Done**.
The UDT is created.

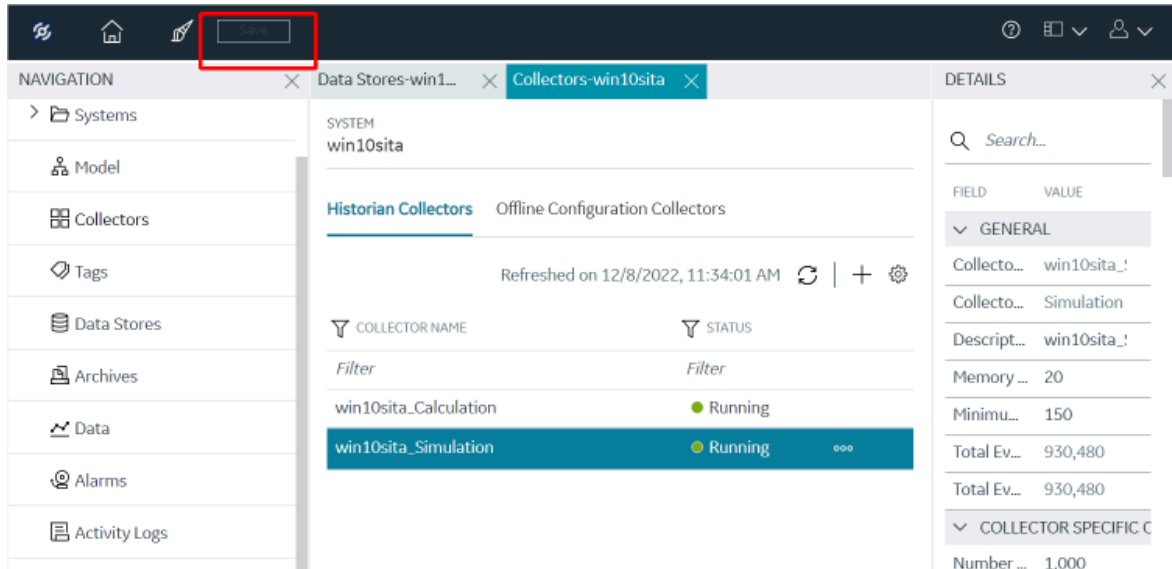
[Assign the UDT to a tag \(on page 1239\)](#).

Assign a User-Defined Data Type to a Tag

- [Create the tag \(on page 909\)](#) for which you want to assign a user-defined data type (UDT).
- [Create the UDT \(on page 1238\)](#) that you want to assign to the tag.

When you assign a UDT to a tag, the tag can collect data of various data types.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Tags**.
3. Select the tag for which you want to assign a UDT.
The details of the tag appear in the **DETAILS** section.
4. Under **Collection**, in the **User Defined Type Name** field, select the UDT that you want to assign.
5. In the upper-left corner of the page, select **Save**.





The UDT is assigned to the tag.

Delete a User-Defined Data Type

You cannot delete a user-defined data type (UDT) if it is assigned to a tag.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Tags**.
3. Select **☰**, and then select **Manage User-Defined Types**.

The **Manage User-Defined Types: <system name>** window appears.

4. Select the UDT that you want to delete, select , and then select **Delete**. Or, select  next to the UDT name.

A message appears, asking you to confirm that you want to delete the UDT.

5. Select **Delete**.

The UDT is deleted.

Managing Archives

About Archives

Historian archives are data files, each of which contains data gathered from all data sources during a specific period of time.

Types of Archive Files:

- ***machine name_Config.ihc***: Contains information about the archiver, tag configuration, and collector configuration.
- ***machine name_ArchiveXXX.iha***: Contains tag data, where x is a number indicating the place of the file in a time-based sequence.

Creation of Archive Files Automatically

Archive files grow to a user-configured maximum size as data is recorded by the server. When data starts loading into an archive file, Historian will automatically create a new blank archive file. When the current archive file becomes full, Historian will immediately serve data to the newly created archive file. This significantly reduces archive creation and transition time.

If, however, the option to automatically create archive files is not enabled, you must [create an archive file manually](#).

**Note:**

If the option to automatically create an archive is not enabled and you do not create a new archive manually, or if the available disk space is less than the required amount of free disk space, a new archive file will not be created.

Overriding Old Archive Files

If you enable the **Overwrite Old Archives** option, the system replaces the oldest archived data with new data when the latest archive default size has been reached. Since this action deletes historical data,

exercise caution in using this feature. Be sure that you have a backup of the archive so that you can restore it later. Best practice is to create an additional archive to prevent premature loss of data due to overwriting. For example, if you want to save 12 months of data into 12 archives, create 13 archives.

During archiver startup and every 60 seconds while the server is running, Historian verifies that you have configured enough free disk space to save the archives, buffer files, and log files. If there is insufficient disk space, the Data Archiver shuts down and a message is logged into the log file. By default, you can view the Historian archiver log file in `C:\Historian Data\LogFiles`.

```
[03/03/10 15:28:41.398] Insufficient space available in [d:\Historian\Archives\]
    [03/03/10 15:28:41.399] The server requires a minimum of [5000 MB] to continue
    [03/03/10 15:28:41.679] USER: DataArchiver TOPIC: ServiceControl MSG: DataArchiver(DataArchiver)
    Archiver shutdown at 03/03/10 15:28:41.653
    [03/03/10 15:28:41.807] DataArchiver Service Stopped.
    [03/03/10 15:28:41.809] [d:\Historian\LogFiles\DataArchiver-34.log] Closed.
```

Guidelines for Setting Archive Size

Since archived data files can become quite large, you must adjust system parameters carefully to limit data collection to meaningful data only and thus minimize the required size of system storage. You can allocate up to 256 GB per archive.

For each archive, you need approximately 1MB of archive space for every 1000 tags to store tag information. Archive size is a function of the rate at which you archive data and the time period you want the archive to cover. A typical user wants the archive to cover a time period of, say, 30 days.

The following factors affect the rate at which you archive data:

- Number of tags
- Polling frequency of each tag
- Compression settings
- Data types

Based on these parameters, the archive size is calculated as follows:

$$\#Tags \times \frac{Values}{Tag} \times \frac{Tags}{Second} \times \%PassComp \times \frac{Bytes}{Value} \times \frac{Seconds}{Hour} \times \frac{Hours}{Day} \times \frac{MB}{Bytes} = \frac{MB}{Day}$$

Calculating Archive Size

Suppose you want to store data, and you have the following parameters:

- Number of tags: 5000
- Polling rate: 1 value/5 seconds
- Pass compression: 5%.

Pass compression is the number of data values archived relative to the number of values read.

- Bytes/value: 4
- Duration: 30 days

Based on the preceding formula, for the given parameters, the archive size is calculated as follows:

$$5000 \times \frac{1}{1} \times \frac{1}{5} \times \frac{5}{100} \times \frac{4}{1} \times \frac{3600}{1} \times \frac{24}{1} \times \frac{1}{1024 \times 1024} \times 30 = 494 \frac{MB}{Month}$$

The calculation shows that a file size of 500 MB is adequate for archiving one month of data for this application.

Therefore, we recommend that you set the default archive size to 500 MB for systems with 1000 tags or more. If you believe the computed size is too large for your application, you can modify parameters as follows:

- Decrease the polling frequency.
- Increase compression deadband, reducing the pass percentage.
- Reduce the number of tags.
- Add more disk capacity to your computer.

Archive Size Calculator

An archive size calculator tool is available to estimate archive size and collector compression based on a tag that has already been configured or based on your inputs. Log on to <http://digitalsupport.ge.com> to download this tool and other GE Intelligent Platforms freeware product solutions.

Access an Archive

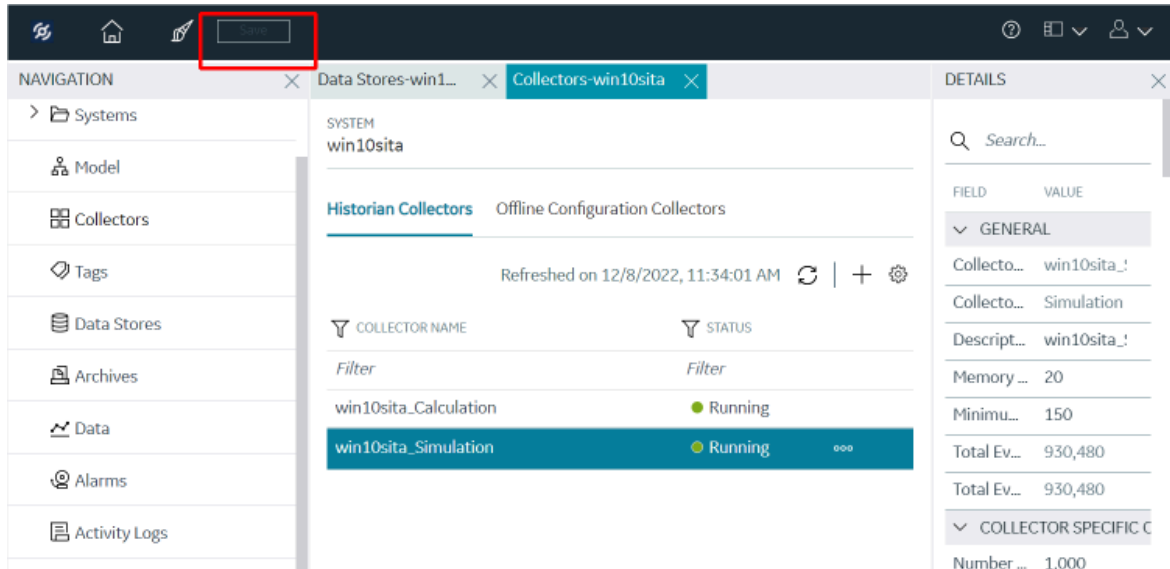
1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Archives**. The **Archives** section appears. By default, only the archives of the default data store appear. If you want to access archives from another data store, select it in the **DATA STORE** field.

3. Select the archive whose details you want to access.

The **DETAILS** section displays the following information of the archive.

Field	Description
Status	Identifies the status of the archive. Contains one of the following values: <ul style="list-style-type: none">◦ Current: The archive is actively accepting data.◦ Active: The archive contains data but is not currently accepting data.◦ Empty: The archive was created but has never accepted data.
Start Time	The time at which writing data to the archive has begun.
End Time	The time at which writing data to the archive has ended.
Last Backup	The time at which the archive has been backed up last.
Backup User	The user who created the last backup of the archive.
File Name	The name and folder path of the archive file.
File Size (MB)	The size of the archive file.
File Attribute	Indicates whether the archive file is read-only or read/write.

4. If needed, change the values in the **Filename** and **File Attribute** fields. You cannot, however, change the file attribute for the current archive.
5. In the upper-left corner of the page, select **Save**.



The archive is modified.

Create Archives Automatically

Historian can automatically create archives for you if the current archive reaches a specific size or after a specific duration. This topic describes how to set these options. You can, however, choose to [create archives manually \(on page 1247\)](#).

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Archives**.
The **Data Stores** section appears.
3. Select the data store in which you want to create archives automatically.
The **DETAILS** section displays the details of the data store.
4. Under **Archive Creation**, enter values as described in the following table.

Field	Description
Automatically Create Archives	Switch the toggle on to indicate that you want Historian to create archive files automatically when the current one is full.
Create Archive By	<p>Select whether you want to create a new archive automatically after the current one reaches a specific <i>size</i> or after a specific <i>duration</i>. This field is enabled only if you switch the Automatically Create Archives toggle on.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> ◦ Size: Select this option if you want to create a new archive when the current one reaches a specific size. Specify the size in the Default Size (MB) field (which appears only if you select Size). ◦ Days or Hours: Select one of these options if you want to create a new archive after a specific duration. Specify the duration in the Archive Duration field (which appears only if you select Days or Hours).
Default Size (MB)	The default size of an archive after which a new one will be automatically created. This field appears only if you select Size in the Create Archive By field.
Archive Duration	The duration after which a new archive will be automatically created. This field appears only if you select Days or Hours in the Create Archive By field.

If needed, you can switch the **Overwrite Old Archives** toggle on. If you enable this option, the oldest archived data is replaced with the latest one when the latest archive default size is reached. Since this action deletes historical data, exercise caution in using this feature. Be sure that you have a backup of the archive so that you can restore it later. Best practice is to create an additional archive

to prevent premature loss of data due to overwriting. For example, if you want to save 12 months of data into 12 archives, create 13 archives.

5. In the upper-left corner of the page, select **Save**.

The screenshot shows the Configuration Hub interface. In the top-left corner, a button (likely 'Save') is highlighted with a red box. The main content area displays the 'Historian Collectors' section for the system 'win10sita'. It shows a table of collectors with columns for 'COLLECTOR NAME' and 'STATUS'. The 'win10sita_Simulation' collector is highlighted in blue and shows a 'Running' status. The right sidebar shows details for the selected collector, including a search bar and a table of fields and values.

FIELD	VALUE
GENERAL	
Collecto...	win10sita_!
Collecto...	Simulation
Descript...	win10sita_!
Memory ...	20
Minimu...	150
Total Ev...	930,480
Total Ev...	930,480
COLLECTOR SPECIFIC C	
Number ...	1,000


Archives will now be created automatically based on the criteria you specified.

Create Archives Manually

This topic describes how to create an archive file manually. You can create multiple archives at the same time. You can, however, choose to [create archives automatically \(on page 1245\)](#).

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Archives**.
The **Archives** section appears.
3. In the upper-right corner of the section, select **+**.
The **Add Archives** window appears.

4. Enter values as described in the following table.

Field	Description
ARCHIVE NAME	Identifies the name of the archive. A value is required. By default, it is in the following format: <i><data store name>_<system name>-Archive<number></i> . The number is used to name the archives sequentially. You can only add a suffix to the archive name.
DATASTORE	Select the data store in which you want to create the archives. A value is required.
FILE LOCATION	Enter the folder path in which you want to store the archives. A value is required. By default, it is <code>C:\Proficy Historian Data\Archives</code>
EACH ARCHIVE SIZE	Enter the size, in MB, that you want to allocate to each archive. A value is required. This field is populated with the value in the Default Size (MB) field in the data store (if applicable).
NUMBER OF ARCHIVES	Enter the number of archives that you want to create. A value is required. The default value is 1.
ALLOCATE SPACE	<p>Specify the disk space that you want to allocate for archives. A value is required.</p> <div data-bbox="862 1360 1419 1675" style="border: 1px solid orange; border-radius: 10px; padding: 10px;"> <p> Important:</p> <p>If there is insufficient disk space, Data Archiver is shut down and a message is logged into the log file. By default, you can view the log file in <code>C:\Historian Data\LogFiles</code>.</p> </div>

5. Select **Add**.

The archives are created.

Back up an Archive

Ensure you have enough disk space.

You must back up archive files periodically to ensure that your data is protected. These backup files contain tag data as well as alarms and events data. You can send these files to a shared network location or to physical media.

Always back up archives before a planned Historian software product upgrade. Use Microsoft® Volume Shadow Copy Service when backing up archive files that are more than 2 GB in size or when backing up more than the last two archives. For more information, refer to [Back Up Archives with Volume Shadow Copy Service \(on page 1250\)](#).

This topic describes how to back up an archive manually. You can also [back up an archive automatically](#).

Important points to remember:

- The .IHC file is automatically backed up when, and only when, you back up the current archive .IHA file. By default, the .IHC backup path is the same as the archives path.
- The .IHC backup file uses the following naming convention: `<system name>_Config-Backup.ihc`. If the default backup path is different from the archives counterpart, the .IHC file is copied to the backup folder with the standard .IHC naming convention: `ComputerName_Config.ihc`.
- In the mirroring system, Client Manager sends a backup message to Data Archiver located on the Client Manager node to which you are connected. The back up, then, happens in the specified location on that node. If that Data Archiver is not running, a NOT_CONNECTED error message appears, and the backup will not happen.
- If you back up an archive more than once, the backup tool will (by default) attempt to use the same name for the backup file and will detect that an archive with the same name already exists. Rename the backup archive file or move the original backup archive file to a different folder.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Archives**. The **Archives** section appears.
3. Right-click the archive that you want to back up (or select **☰**), and then select **Backup Archive**. The **Backup Archives** window appears. The **ARCHIVE NAME** field is disabled and populated. The **BACKUP FILE PATH** field is disabled and populated with the value in the **DEFAULT BACKUP PATH** field of the data store.
4. Select **OK**.
The archive file is backed up.

Back up Archives with Volume Shadow Copy Service

Use the Microsoft® Volume Shadow Copy Service to back up large archive files, or if you want to back up more than the last two archives, as it allows you to backup and restore archives reliably and in a short period of time without affecting the data collection.

The Volume Shadow Copy feature is provided by Windows Operating System, and the instructions to use backup and restore vary depending on the backup application that is used in the Windows operating system.

VSS provides fast volume capture of the state of a disk which is called a snapshot or shadow copy. When the snapshot is taken, disk writes are suspended for a brief period of time, typically on the order of milliseconds. After the snapshot, disk writes can resume, but the original state of the files are maintained by a difference file. The difference file allows the state of the original file at the time of the snapshot to be reconstructed. This behavior allows files to be backed up while new data is being written to files.

If you are using `ihArchiveBackup.exe` before the upgrade, your backup will continue to work in the same or similar manner as it did before the upgrade. There is no change in the backup procedure and the Auto Recovery Backup Files option remains unchanged.

**Note:**

Though you could use either `ihArchiveBackup.exe` or VSS for backup, VSS is a better choice for both larger archives or if you are backing up more than the last two archives to reduce the load on the Data Archiver service.

Microsoft uses a backup format called Virtual Hard Disk (VHD) to back up files.

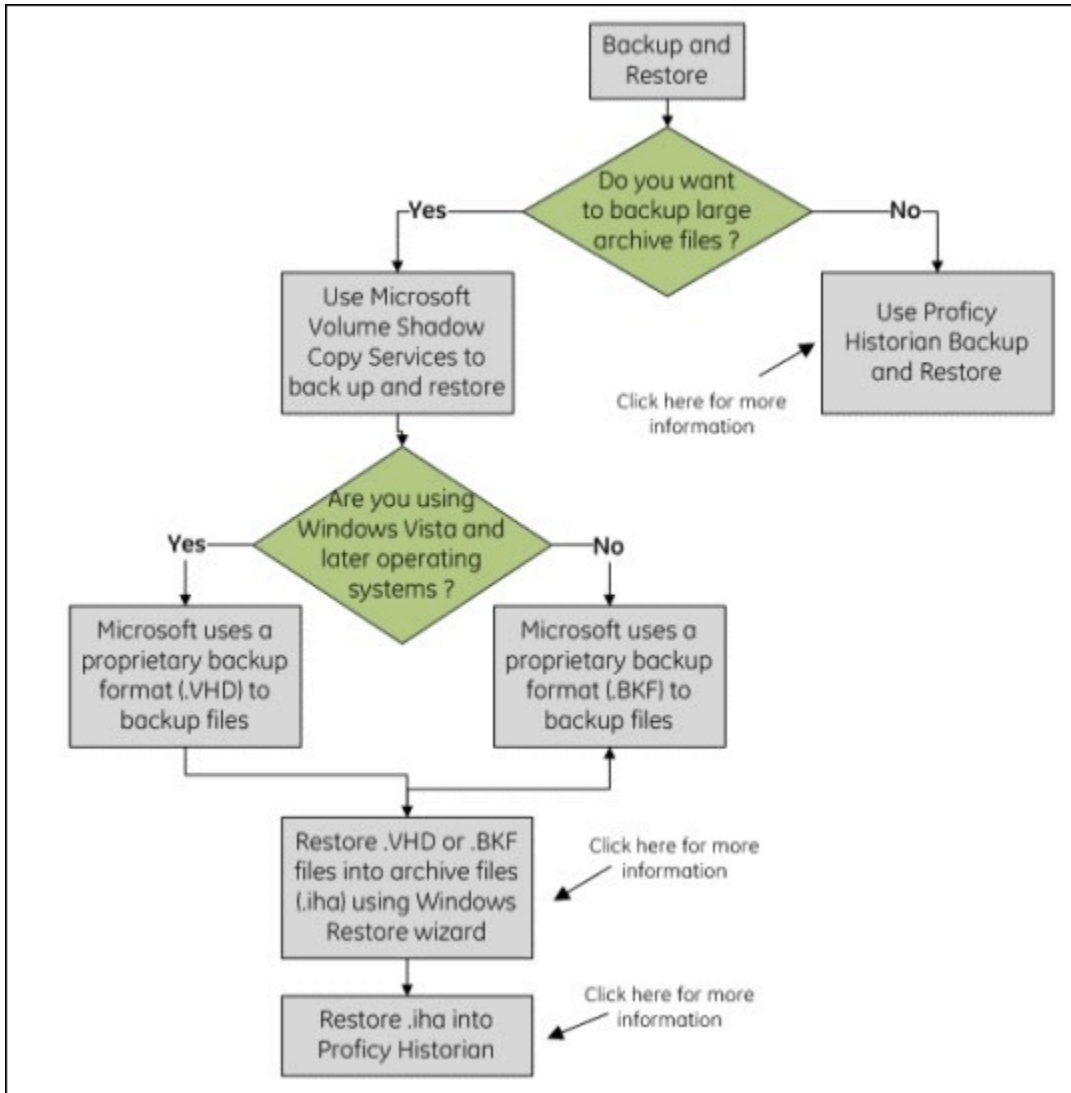
When you create archives backup using Microsoft® Volume Shadow Copy Service, you must first restore the archives files (that is, `.bkf` or `.vhd` into `.iha`) using the Windows Restore wizard, and then restore the archives (`.iha`) into Historian. For more information on restoring an archive (`.iha`) into Historian, refer to the Restoring an Archive topic.

**Note:**

It is recommended that you:



- Use Microsoft® Volume Shadow Copy Service when you want to back up archive files that are more than 2 GB in size, or if you are backing up more than your last two archives.
- Ensure you have enough hard drive space on your default backup location before backing up your archives.



Important:

For optimum performance, it is recommended you to save paging file of the operating system, Historian archives, and scheduled backup directory on separate drives.

Restore an Archive

- Before restoring an archive from a removable disk, copy the archive file to the normal archive path and then restore the archive from that location. Leave the original backup file in the backup file folder.
- Ensure that the current archive is online.


Under certain circumstances, you may want to restore tag and alarms and events data to Historian. This may be after an unplanned shutdown, or you may need to retrieve data from an old, inactive archive.



Important:

Restoring an archive is a resource-intensive operation and should be scheduled for non-peak usage times.

Archives that have been previously removed from Historian can be found in the `\Archives\Offline` directory.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Archives**.
The **Archives** section appears.
3. In the upper-right corner of the section, select .
The **Restore Archives** window appears.
4. Enter values as described in the following table.

Field	Description
FILE LOCATION	This field is populated with the value in the DEFAULT BACKUP PATH field of the data store. Append the name of the .zip file of the archive that you want to restore. The ARCHIVE NAME field is populated with the .zip file name that you enter.
DATASTORE	Select the data store in which you want to restore the archive.

5. Select **Restore**.
The archive is restored; it is moved to the `Archive` folder and is made available for querying.

Close an Archive

By default, an archive is closed when it is full. However, you can manually close an archive before it is full.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Archives**.
The **Archives** section appears.
3. Right-click the archive that you want to back up (or select **ooo**), and then select **Close Archive**.
A message appears, asking you to confirm that you want to close the archive.
4. Select **Yes**.
The archive file is closed, and another one is used for writing data.

Remove an Archive

When you remove an archive, it no longer appears in Configuration Hub. However, it exists in the Archives folder (by default, C:\Proficy Historian Data\Archives).

You cannot remove the current archive. If you want to remove it, you must first close it. When you do so, another archive is used for writing data.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Archives**.
The **Archives** section appears.
3. Right-click the archive that you want to remove (or select **ooo**), and then select **Remove Archive**.
A message appears, asking you to confirm that you want to remove the archive.
4. Select **Yes**.
The archive file is removed.


Reading/Writing Data

Query Data

Using Configuration Hub, you can query the data of selected tags. This data is then plotted in a trend chart. You can also export this data into a PDF, SVG, PNG, or a JPEG file.

Querying data involves the following steps:

1. **Selecting the tags:** You can select tags from all the tags in the system. While selecting tags, you can view them in a hierarchical object model view or in a flat list.
2. **Applying conditions and filters:** You can select the sampling mode, size, query modifiers, and so on. You can also select the calculation modes for the calculated sampling mode.
3. **Generating the report:** You can plot the query results in a trend chart or view them in a table. You can also export the data.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Data**. The **Data** section appears, displaying a list of object instances and the underlying variables and contained types hierarchically. If you want to view a flat list of all the tags, select .
3. Select the tags for which you want to query data, select Read data operation, and then select **Next**. You can select up to 10 tags.
4. Enter values as described in the following table.

Field	Description
START DATE/TIME	Enter the start date and time for the query.
END DATE/TIME	Enter the end date and time for the query.
SAMPLING MODES	Select the sampling mode for the query: <ul style="list-style-type: none"> ◦ Calculated: Returns the result of a calculation on tag values (for example, count, maximum, delta). ◦ Current Value: Returns a single sample containing the current value of the tag. Retrieves the timestamp, value, and quality. ◦ Interpolated: Returns the interpolated tag values. ◦ Interpolated to Raw ◦ Lab: Returns only collected values. Each collected value is repeated until the next collected value, resulting in a jagged step plot instead of a smooth curve. ◦ Lab to Raw ◦ Raw By Number: Returns the specified number of raw samples of all qualities beginning with the start time and moving in the specified direction. ◦ Raw By Time: Returns all raw samples of all qualities with a timestamp greater than the start time and less

Field	Description
	<p>than or equal to the end time. It will not return a raw sample with same time stamp as the start time.</p> <ul style="list-style-type: none"> ◦ Trend: Returns significant points, which are raw samples. These points are determined by finding the raw minimum and raw maximum values within each interval. ◦ Trend to Raw ◦ Trend to Raw2 ◦ Trend2: Splits up a given time period into a number of intervals (using either a specified number of samples or specified interval length), and returns the minimum and maximum data values that occur within the range of each interval, together with the timestamps of the raw values. This sampling mode is suitable for analysis of minimum and maximum values and for plotting programs that can handle unevenly spaced data.
CALCULATION MODE	<p>Select the calculation mode that you want to use. This field appears only if you select Calculated in the SAMPLING MODES field. For information on calculation modes, refer to Calculation Modes.</p>
SAMPLING DIRECTION	<p>The direction in which you want to retrieve the query results:</p> <ul style="list-style-type: none"> ◦ Forward: Returns query results starting from the start data to the end date. ◦ Backward: Returns query results starting from the end date to the start data.
SAMPLE INCREMENT	<p>Identifies the amount of data samples in each sample:</p> <ul style="list-style-type: none"> ◦ By Size: Select this option if you want each sample to contain a specific number of data points, and then enter the number of data points. ◦ By Time: Select this option if you want each sample to contain data points collected for a specified duration, and then enter the duration.
QUERY MODIFIERS	<p>Used for retrieving a specific set of data. For information, refer to Query Modifiers.</p>

Field	Description
Filters	<p>You can enter your filter conditions using the Filter tag, the Filter Condition, and the Filter Comparison Value.</p> <p>In the Filter Tag Name field, select the tag you want to enable filtering with.</p> <p>In the Condition field, select your comparison condition.</p> <p>In the Value field, enter your filter condition value.</p>

5. Select **Generate Report**.

The query results for the selected tags are plotted on a trend chart.




You can narrow down the start and end dates by dragging the timeline below the trend chart.


[Query_Results.mp4](#)


The Tags and query criteria appear in the **Summary** section; you can edit them if needed.

Select the Edit beside Tag Selection and Query Builder to modify tags and query criteria.

If you want to view the results in a table, select **Table**.

If you want to export the results into a .csv file, select . The results are exported.

If you want to print the trend, select , and then select **Print**.

To export into other formats (such as a .pdf, .svg, .png, or .jpeg), select , and then select the format.


Write Data

Using Configuration Hub, you can write data for selected tags. This helps you verify that data is being sent to Data Archiver.

Writing data involves the following steps:

1. **Selecting the tags:** You can select tags from all the tags in the system. While selecting tags, you can view them in a hierarchical object model view or in a flat list.
2. **Entering the data:** You can enter data for each selected tag, along with the data type and quality.
3. **Generating the report:** You can plot the query results in a trend chart or view them in a table. You can also export the data.

1. [Access Configuration Hub \(on page 902\)](#).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Data**.

The **Data** section appears, displaying a list of object instances and the underlying variables and contained types hierarchically. If you want to view a flat list of all the tags, select .

3. Under **DATA OPERATION**, select **Write Data**.
4. Select the tags for which you want to write data, and then select **Next**.
5. For each tag that you have selected, enter values as described in the following table.

Column	Description
VALUE	Enter the value of the tag. A value is required.
DATA TYPE	If Hierarchical tags are selected, select the data type of the tag value. A value is required. If normal tags are selected, the data type will be automatically populated.
DATA QUALITY	Select the data quality of the tag value from Good or Bad from the list. A value is required.

6. Select **Write Data**, and then select **Next**.
7. Select **Generate Report**.

The query results for the selected tags are plotted on a trend chart.



You can narrow down the start and end dates by dragging the timeline below the trend chart.

[Query_Results.mp4](#)

The query criteria appear in the **Summary** section; you can edit them if needed.

The screenshot shows the 'Summary' section of the Configuration Hub interface. It includes a 'New Query' button in the top right corner. Below it, there is a 'Tag Selection' section with an 'Edit' link and a list of tags: 'Maruthi>Mileage', 'Maruthi>SidestandIndicator', 'srinivas2020_Simulation.Simulation00002', and 'srinivas2020_Simulation.Simulation00003'. The 'Query Builder' section has an 'Edit' link and displays the following settings: TIME (2022-06-07 10:34:34), END DATE (2022-06-14 10:35:11), MODE (Interpolated), SAMPLING MODE (Interpolated), SAMPLE DIRECTION (Forward), and SAMPLES (1000). The 'QUERY MODIFIERS' section includes a 'QUERY MODIFIER' (Exclude Bad DQ Values) and a 'FILTER' field.

If you want to view the results in a table, select **Table**.

The screenshot shows the 'Table' view selected in the Configuration Hub interface. The 'Table' button is highlighted with a red box. Below it, there is a table with columns for 'Timestamp', 'Value', and 'Quality'. The table contains four rows of data, each with a chevron icon on the left:

Timestamp	Value	Quality
> TAG NAME: MARUTHI>MILEAGE		
> TAG NAME: MARUTHI>SIDESTANDINDICATOR		
> TAG NAME: MARUTHI>SPEED		
> TAG NAME: SRINIVAS2020_SIMULATION.SIMULATION00002		

Managing Alarms and Events

About Alarms and Events

Using Configuration Hub, you can manage alarms and events data from any OPC-compliant alarms and events server.



Note:

The Alarm Archiver must be available and running to access this feature.

Alarms: Alarms are generally defined as tags going into an abnormal condition. For example, you can set an alarm on a boiler when it reaches a specified temperature. Alarms usually have a well-defined life cycle, which is defined by the individual data sources from which the alarms data is collected. They enter an alarm state, are generally acknowledged, then return to normal.

To collect alarms and events data, you can use any of the following collectors:

- iFIX Alarms and Events collector
- OPC Classic Alarms and Events collector

Historian handles alarm data in two ways. You can view the entire Alarm as a single record that contains all information about the alarm, or you can view the Alarm History, which shows the transitions of the alarm as individual records.

Events: Events are generally defined as activities in a system that occur once only. For example, a user logging on to a device is an event. When viewing this data in Historian, each event is returned as a record.

Alarms and Events Requirements

To generate alarms and events data, you can use any OPC-compliant alarms and events server such as:

- CIMPLICITY
- iFIX

To collect alarms and events data, [install collectors](#), and then add any of the following collector instances:

- [iFIX Alarms and Events collector \(on page 1051\)](#)
- [OPC Classic Alarms and Events collector \(on page 1067\)](#)

To store alarms and events data, [install Historian Alarms and Events](#). During the installation, provide the credentials of Microsoft SQL server 2012 or later.

To view and analyze alarms and events data, you can use any of the following applications:

- Configuration Hub
- Historian Administrator
- Crystal Reports 11 or later
- The OLEDB Provider
- REST APIs




Note:

Before starting the Alarm Archive service, ensure that "NT AUTHORITY/SYSTEM" has "SysAdmin" privileges.


Create an Alarm

This topic describes how to create an alarm manually. You can use it to verify that Historian is collecting alarm data. You can then use the iFIX Alarms and Events collector or the OPC Classic Alarms and Events collector to collect alarm data and store it in Historian.

1. [Access Configuration Hub \(on page 902\)](#)
2. In the **NAVIGATION** section, under the Configuration Hub for Historian, select **Alarms**.
The **Alarms** section appears.
3. In the upper-right corner of the page, select .

**Note:**

To select hierarchical model tags you must need to have the valid license.

The **Add Alarm** window appears, displaying a list of tags in a hierarchical view. If you want to view a flat list of all the tags, select .

4. Select the check boxes corresponding to the tags for which you want to create an alarm, and then select **Next**.
The **Alarm Attributes** section appears, displaying the selected tags. The **TAG NAME** and **TIMESTAMP** columns are automatically populated.
5. For each tag, enter values as described in the following table.

Column	Description
SEVERITY	Specify whether you want to record high or low severity for the alarm.
DATA QUALITY	Specify whether you want to record good or bad quality for the alarm.
MESSAGE	Enter a message for the alarm.

6. Select **Write Alarm**.
The alarm is created.

Access/Filter Alarms

1. [Access Configuration Hub \(on page 902\)](#)
2. In the **NAVIGATION** section, under the Configuration Hub for Historian, select **Alarms**.
The **Alarms** section appears.
3. To filter for alarms, enter values as described in the following table.

Field	Description
GENERATED FROM	Enter the start date and time for which you want to filter alarms. By default, ten minutes earlier than the current time is considered. A value is required.
GENERATED TO	Enter the end date and time for which you want to filter alarms. By default, the current time is considered. A value is required.
COLLETOR NAME	Select the collector that collects the alarms and events data.

4. Select **Apply**.

The alarms and events data is filtered based on the criteria. To access the events data, select **Events**. The list of events is also filtered based on the criteria.



Tip:

You can show/hide/reorder columns in the table. For instructions, refer to [Common Tasks in Configuration Hub \(on page 906\)](#).

Back up Alarms Using Configuration Hub

1. [Access Configuration Hub \(on page 902\)](#)

2. In the **NAVIGATION** section, under the Configuration Hub for Historian, select **Alarms**.


The **Alarms** section appears.

3. Select **☰**, and then select **Backup Alarms**.

The **Backup Alarms** window appears.

4. Enter values as described in the following table.

Field	Description
GENERATED FROM	Enter the start time for which you want to back up alarms.
GENERATED TO	Enter the end time for which you want to back up alarms.
PROVIDE FILE NAME	Enter the file name and location of the back up file that you want to create. By default, the backup location of the default data store is considered. And, the file name is in the following format: <code>mm_dd_yyyy_hh_mm_ss</code> . For example: 11_25_2022_11_23_26.zip. The time format followed is the 24-hour time notation.

Field	Description
	<div data-bbox="667 262 1425 531" style="border: 1px solid #0070c0; border-radius: 10px; padding: 10px; background-color: #e6f2ff;">  Note: This file naming convention for alarm backup is standard to Historian. Even if you use other date settings such as dd-mm, the file name will still be saved in the mm-dd format. </div> <p data-bbox="667 562 1425 921">The end time stamp in the file name indicates the time at which the alarms have been backed up but not the time till when the alarms are backed up. For example, suppose, at 8:00 am, you back up alarms for the past two hours, the backup will contain alarms from 6:00 am to 8:00 am but may not contain an alarm generated at 8:00 am. The last alarm may have been at 7:50 am. But the backup file name will have the time stamp of 8:00:00 along with the date.</p>

5. Select **Backup**.

The alarms data is backed up.

Restore Alarms Using Configuration Hub

Restoring alarms to a running system makes them available for query and analysis. You can restore alarms that have been backed up or deleted previously.

1. [Access Configuration Hub \(on page 902\)](#)
2. In the **NAVIGATION** section, under the Configuration Hub for Historian, select **Alarms**.
The **Alarms** section appears.
3. Select **☰**, and then select **Restore Alarms**.
The **Restore Alarms** window appears.
4. In the **PROVIDE FILE NAME** field, provide the backup file in the .zip format that you want to restore.



Note:

Remember to include .zip at the end of the file name.

5. Select **Restore**.

The alarm data is restored.

About Purging Alarms

Purging alarm data involves deleting the data from the database.



Note:

- Even after purging, the data is not lost; a backup is created to maintain an audit trail. You can restore the data if needed.
- When using circular archives (that is, archives that roll over), alarms are purged automatically.

You can choose to purge alarm data for any of the following reasons:

- To maintain alarm data efficiently
- The data is outdated or redundant
- The disk space is limited

Data in the following tables is purged:

- Alarm Attribute Values
- Alarm Attribute Value History
- Delete from Alarm History
- Delete from Alarm Table esignatures
- comments

You can purge data using one of the following methods:

- Purge data within a specified duration. You can do this [using Configuration Hub \(on page 1265\)](#), [using the Proficy Historian Alarm and Event Data Migration utility](#) or [at a command prompt](#).
- Purge data related to a specific alarm ID. You can do this [using `Alarms.PurgeAlarmsById`](#) to develop an SDK program.

Purging is performed in batches. You can check the log data in the `Proficy.Historian.AandE.Migration.log` file. By default, this file is located in the `C:\Program Files(x86)\Proficy` folder.

In the case of a failure:

- The batch size is changed to 10. That is, the collector receives an acknowledgement after sending 10 messages, thus reducing the load on the server.
- The waiting time for receiving an acknowledgement is automatically incremented after each failure per batch, starting from 90 seconds to 270 seconds. This gives more time for the server to respond.

**Note:**

After the acknowledgement is received, the batch size and the waiting time are reset for the subsequent batches.

If the time taken to purge exceeds the timeout limit, instead of reverting the entire purging operation, only the current batch, which is still under processing, is purged.


Best Practices:

- Restart the Alarms and Events services before purging data.

Purge Alarms Using Configuration Hub

1. [Access Configuration Hub \(on page 902\)](#)
2. In the **NAVIGATION** section, under the Configuration Hub for Historian, select **Alarms**.
The **Alarms** section appears.
3. Select **☰**, and then select **Purge Alarms**.
The **Purge Alarms** window appears.
4. In the **PROVIDE FILE NAME** field, pro
5. Enter values as described in the following table.

Field	Description
GENERATED FROM	Enter the start time for which you want to purge alarms.
GENERATED TO	Enter the end time for which you want to purge alarms.
PROVIDE FILE NAME	Enter the file name and location of the back up file that you want to create. This field is enabled only if you select the BACKUP ALARMS BEFORE PURGE? check box. By default, the backup location of the default data store is considered. And, the file name is in the following format: <code>mm_dd_yyyy_hh_mm_ss</code> . For example: 11_25_2022_11_23_26.zip. The time format followed is the 24-hour time notation.

Field	Description
	<div data-bbox="667 262 1421 531" style="border: 1px solid #0070c0; border-radius: 10px; padding: 10px; background-color: #e6f2ff;">  Note: This file naming convention for alarm backup is standard to Historian. Even if you use other date settings such as dd-mm, the file name will still be saved in the mm-dd format. </div> <p>The end time stamp in the file name indicates the time at which the alarms have been backed up but not the time till when the alarms are backed up. For example, suppose, at 8:00 am, you back up alarms for the past two hours, the backup will contain alarms from 6:00 am to 8:00 am but may not contain an alarm generated at 8:00 am. The last alarm may have been at 7:50 am. But the backup file name will have the time stamp of 8:00:00 along with the date.</p>
BACKUP ALARMS BEFORE PURGE?	Select the check box if you want to back up alarms before purging.

6. Select **Purge**.

The alarms data is purged. A backup file is created if you have selected the **BACKUP ALARMS BEFORE PURGE?** check box.

Access Activity Logs

Activity logs are generated when activities are performed in the Historian system.

Examples:

- When a tag is created, modified, or deleted
- When a collector instance is created, modified, or deleted
- When data collection for a tag or a collector begins or ends
- When an archive is created or will be closed soon


You can access these logs for each tag/collector or for all the tags and collectors in a system. You can filter these logs based on the start and end dates, priority, topics, and the content in the logs. You can also export all the logs or selected ones.

1. [Access Configuration Hub \(on page 902\)](#).
2. If you want to access activity logs for all the tags and collectors in a system, in the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Activity Logs**.

A list of activity logs appears.

3. If you want to access the activity logs of a collector instance:
 - a. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Collectors**.
A list of collectors in the system appears.
 - b. Right-click the collector whose activity log you want to access (or select **☰**), and then select **Browse Activity Log**.
A list of activity logs for the collector appears.
4. If you want to access the activity logs of a tag:
 - a. In the **NAVIGATION** section, select **Historian_<system_name> > Tags**.
A list of tags in the system appears.
 - b. Right-click the tag whose activity log you want to access (or select **☰**), and then select **Browse Activity Log**.
A list of activity logs for the tag appears.

5. If you want to filter the list of activity logs:

- a. In the upper-right corner of the main section, select .
- b. Enter values as described in the following table.

Field	Description
START DATE/TIME	Select the start date and time for the activity logs.
END DATE/TIME	Select the end date and time for the activity logs.
PRIORITY	Specify whether you want to see only alerts or messages or both.
TOPIC	Select the topic based on which you want to filter the logs: <ul style="list-style-type: none"> ▪ Configuration: Includes modifying a collector instance or a tag configuration. ▪ Connections: Includes system connections and creating a collector interface.

Field	Description
	<ul style="list-style-type: none"> ▪ General: Includes pausing or resuming data collection. ▪ Performance: Includes creating or closing an archive and moving buffer files. ▪ ServiceControl: Includes starting or stopping a collector interface. <p>This list is not comprehensive.</p>
ACTIVITY CONTAINS	Enter the content of the logs based on which you want to filter them.

c. Select **Apply**.

The logs are filtered based on the criteria.

If you want to export the logs, select . The logs are exported into a CSV file.

Troubleshooting Historian and Configuration Hub

This topic contains solutions/workarounds to some of the common issues encountered with Configuration Hub. This list is not comprehensive. If the issue you are facing is not listed on this page, refer to [Troubleshooting Web-based Clients](#) and [Troubleshooting the Historian Server](#).

Unable to Access Configuration Hub After Upgrading Web-based Clients

Workaround: Clear your browser cache.

Even after installing Web-based Clients, you cannot access Configuration Hub.

Workaround: Start the GE Operations Hub Httpd Reverse Proxy and the Data Archiver services.

Unable to Access External Configuration Hub if Public Https Port is Different

Issue: During Web-based Clients installation, if you provide an existing Proficy Authentication and Configuration Hub details, and if the public https port numbers of these two machines do not match, you cannot access the external Configuration Hub from the current machine.

For example, suppose you have installed Web-based Clients on machine A, which points to the Proficy Authentication and Configuration Hub installed on machine B. If the public https port numbers of machines A and B do not match, you cannot access Configuration Hub of machine B from machine A (although you can access it locally from machine B).

Workaround: Perform the following steps on the machine on which you have installed Configuration Hub (machine B):

1. Access the following folder: `C:\Program Files (x86)\GE\ConfigurationHub\Web\conf\confi`
`hub`
2. Access the file that contains the details of the machine from which you want to access external Configuration Hub (machine A). The file name begins with the host name of machine A.
3. In the line that contains the details of the Proficy Authentication server (for example, `proxy_pass https://machine_B.Domain.com:Port/uaa/`), change the port number to match the public https port number of machine B.
4. Save and close the file.
5. Restart the following services:
 - ConfigHubContainerService
 - ConfigHubNGINXService
 - ConfigHubStorageService

Error Occurs When Historian Plugin is Registered with an External Configuration Hub

Description: If you install Configuration Hub using iFIX, then install Web-based Clients on another machine with local Proficy Authentication, and then register the Historian plugin with Configuration Hub, testing the connection to Configuration Hub fails. Even after you add the IP addresses of both the machines to the hosts file, the issue is not resolved.

Error Message: Error while getting token in ConfigAuth App

Workaround: [Register the Historian plugin](#) on the machine on which you have installed Web-based Clients, [install the Proficy Authentication certificate](#), and then restart the browser.

Cannot Access the Collectors Section or Add a Collector Instance

Possible Cause: User credentials not provided while installing collectors or Remote Collector Manager:

If installing collectors and the Historian server on the same machine, the collectors installer does not mandate the entry of username and password because it not required for Remote Collector Management Agent to connect to a local Historian server. But if Historian security or strict authentication is enabled, it is mandatory to enter the username and password.

Workaround:

- **Option 1:** Disable the strict collector authentication using Historian Administrator, and then restart the Historian Remote Collector Management Agent service.
- **Option 2:** Reinstall Remote Management Agents, providing the user credentials.

Cannot Access or Add a System in Configuration Hub

Possible Causes:

- **User does not have security privileges:** During installation of the Historian server, if you have allowed the installer to create security groups, you must create a user with the name in the following format: <Proficy Authentication host name>.admin. Verify that this user has been created and added to the ihSecurityAdmins group.

If the Proficy Authentication server hostname is long, resulting in a username longer than 20 characters, Windows does not allow you to create the user. In that case, you can create a Proficy Authentication user, and then create the corresponding Windows user, using the Proficy Authentication Configuration utility:

1. Access the Proficy Authentication Configuration utility. By default, it is located at C:\Program Files\GE Digital\Historian Config\uaa_config_tool.
2. Run the following command: `uaa_config_tool add_user -u <username> -p <password> -s <the client secret you provided while installing the Historian server> -c`

Example: `uaa_config_tool add_user -u adminuser -p Password123 -s pwd@123 -c`

- **Incorrect Proficy Authentication details:** You must provide the host name of the Proficy Authentication server while installing the Historian server. In the Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Intellution, Inc.\iHistorian\SecurityProviders\OAuth2 registry path, verify that the URI value is in the following format: `https://<Proficy Authentication host name>:<port number>/uaa/check_token.`

If needed, modify the value, and then restart the Data Archiver service.

Error Appears When Creating a Collector Instance

Description: When you add a collector instance, the following error message appears: `The server encountered an error processing the request. Please try again.` The collector instance is added successfully, but it does not appear in the **Collectors** section.

Possible causes: When you add a collector instance, the collector service is started and stopped so that it is connected to the Historian server. The collector then appears in the table in the **Collectors** section. Sometimes, however, the collector service does not respond to these commands on time, resulting in the

error message. If you attempt to add the same collector instance again, a message appears, stating that it exists.

Workaround: Select **Cancel**, and refresh the **Collectors** section. If the collector instance still does not appear, access the collector machine, and start the collector manually.

Data Archiver is Shut Down

Possible causes: If there is insufficient disk space, the Data Archiver shuts down and a message is logged into the log file. By default, you can view the Historian archiver log file in C:\Historian Data\LogFiles.

Workaround: Allocate more disk space for archives, or remove old archives. You can also configure Historian to overwrite old archives automatically by switching the **Overwrite Old Archives** toggle on. If you enable this option, the oldest archived data is replaced with the latest one when the latest archive default size is reached. Since this action deletes historical data, exercise caution in using this feature. Be sure that you have a backup of the archive so that you can restore it later. Best practice is to create an additional archive to prevent premature loss of data due to overwriting. For example, if you want to save 12 months of data into 12 archives, create 13 archives.

For instructions, refer to [Access a Data Store \(on page 1005\)](#).

Chapter 5. Operations Hub

Operations Hub and the Integrated Installer

This topic describes how to use the integrated installer to install Operations Hub.

The latest version of Operations Hub is distributed as follows:

- **Dedicated installer:** Enables to install the common components and Operations Hub.

See [Install Operations Hub from a Dedicated Installer \(on page 1282\)](#).

- **iFIX or CIMPLICITY installer suite:** Enables to install the common components and Operations Hub along with additional Proficy applications.

See [Install Operations Hub for SCADA \(on page 1277\)](#).



Note:

It is highly recommended to first install common components (Configuration Hub and Proficy Authentication) followed by any additional product installations. See [Install Common Components \(on page 1273\)](#).



Note:

If installing Operations Hub remotely from Configuration Hub, make sure that the Operations Hub certificate is trusted by Configuration Hub. If not trusted, then the request to load plugins gets blocked. Refer to the *Install the Certificate on your Clients* topic in the Operations Hub documentation.

About Upgrading Operations Hub

If Proficy Authentication version is older than Operations Hub version you are upgrading to, then you will be requested to first upgrade or uninstall Proficy Authentication. The request does not appear if Proficy Authentication version is same or greater than Operations Hub upgrade version.

Do not uninstall Proficy Authentication if other Proficy products are using the application. Choose to upgrade to the latest version.

Install Common Components

This topic describes how to install Configuration Hub and Proficy Authentication from an integrated installer.

You must be an Administrator to perform these steps.

You can install the common components, Configuration Hub and Proficy Authentication, from any of these install packages:

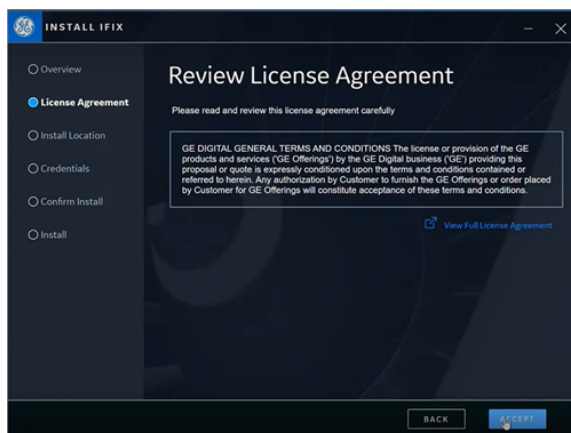
- Dedicated installer for Operations Hub
- iFIX integrated installer
- CIMPLICITY integrated installer

In the following steps, we run the iFIX integrated installer to install the common components. You can refer to these steps while installing from any other install package.

1. Select **Common Components > START**.



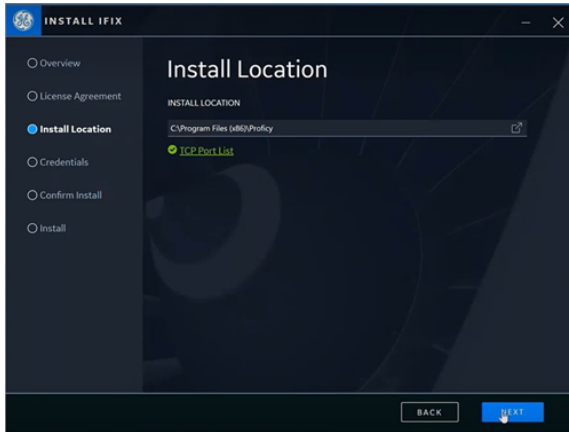
2. Accept the license agreement to continue with the install.



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

- Continue to the next screen with the default install location.

If port conflicts are detected, you must fix them before proceeding to the next screen.



If there are no conflicts, the **Credentials** screen for Configuration Hub and Proficy Authentication appears.

- Complete the following and proceed to the next screen.




Note:

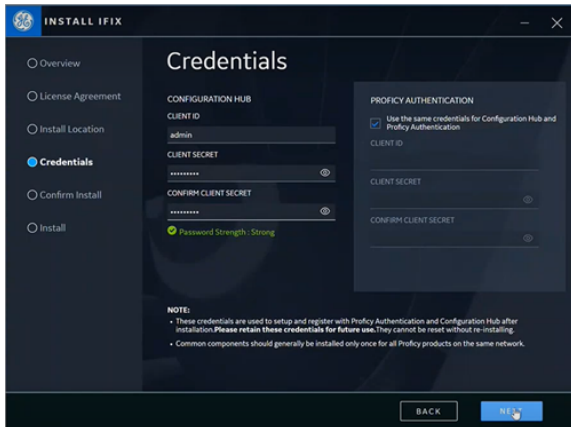
Remember the information you enter here, as you shall need it later for logging in to the applications. If you lose the credentials, you will have to reinstall common components to set them up again.

- Create these login credentials for Configuration Hub:

CLIENT ID	Enter a client id, which you can use to login to the Configuration Hub application. For example, <code>admin</code>
CLIENT SECRET	Enter a secret password for your Configuration Hub client id.
CONFIRM CLIENT SECRET	Enter the secret password again to confirm.

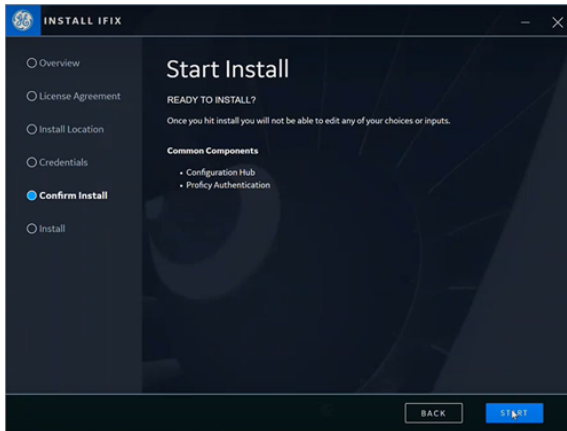
- Create these login credentials for Proficy Authentication:

<p>Use the same credentials for Configuration Hub and Proficy Authentication</p>	<p>If you select this check box, then you do not have to enter any additional credentials for Proficy Authentication. The login credentials you entered for Configuration Hub is automatically applied to Proficy Authentication.</p> <p>This is a useful feature if you do not want to remember two sets of login credentials.</p> <p>However, if you want to set unique login credentials for Proficy Authentication, then clear the check box and proceed to enter additional details.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note: It is recommended to install common components (Configuration Hub, Proficy Authentication) with the same client id/secret.</p> </div>
<p>CLIENT ID</p>	<p>Enter a client id, which you can use to login to the Proficy Authentication application.</p>
<p>CLIENT SECRET</p>	<p>Enter a secret password for your Proficy Authentication client id.</p>
<p>CONFIRM CLIENT SECRET</p>	<p>Enter the secret password again to confirm.</p>



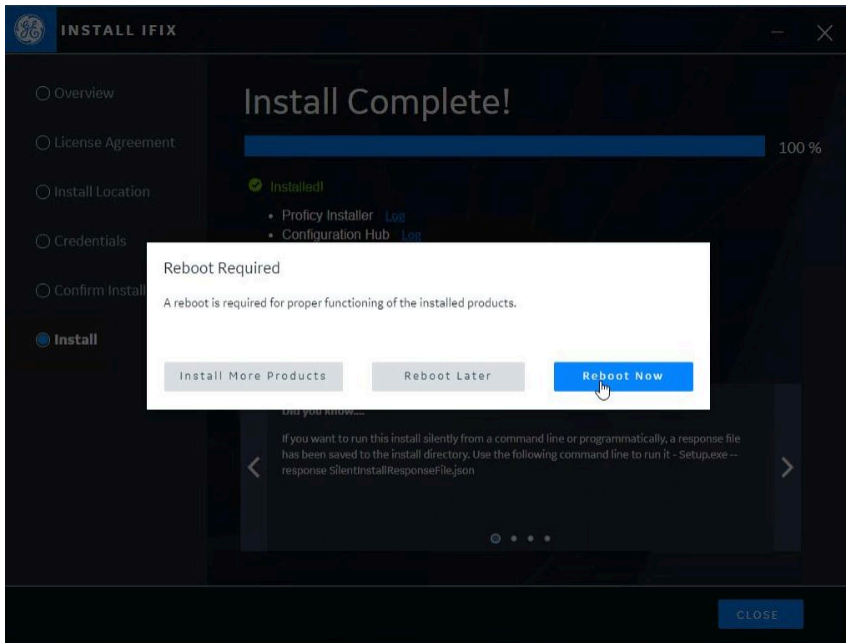
The **Start Install** screen appears.

5. Select **START** to start installing the products.




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

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



Select from these options:

<p>Install More Products</p>	<p>You are redirected to the installation welcome screen, from where you can choose to install more applications.</p>
<p>Reboot Later</p>	<p>Closes the installation setup screen without restarting your computer.</p>

Reboot Now	<p>Restarts your computer.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;">  Note: You must reboot for applications to function properly. You may choose to do this after installing all the applications, or at a later time. </div>
-------------------	--

Install Operations Hub for SCADA

This topic describes how to install Operations Hub from the iFIX integrated installer.

- Ensure that the machine on which you want to install Operations Hub meets the system requirements.
- Use a machine that does not host any applications that are bundled with Operations Hub.
- Run a Windows update (including security updates).
- Use a host name that contains up to 24 characters and any of the following characters:
 - Alphabetic characters
 - Numeric characters
 - Minus
 - Period
- Ensure that you have administrative privileges to the machine on which you want to install Operations Hub.

In the following steps, we run the iFIX integrated installer to install Operations Hub. Consider these points during installation:

- **First time installation:** You can choose to provide the same user name and password for Operations Hub tenant admin and Configuration Hub. This will allow you to use the same credentials to log in to both the applications.
- **Re-installation:** If re-installing Operations Hub without DB purge, provide the same user name and password as the earlier install. If you provide a different set of credentials other than the tenant admin credentials used in the initial install, the user ID will not match what already exists in Proficiency Authentication (UAA). As a result, users will not be able to log into Operations Hub.

1. Download the iFIX 2023 ISO install media from the Salesforce and mount the file.
2. From the ISO folder, double-click `Setup.bat` to run the file.
The welcome screen appears.

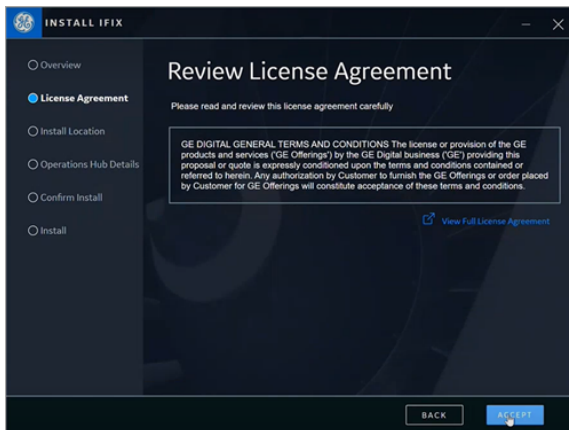
3. On the welcome screen, you must first install Configuration Hub and Proficiency Authentication before installing Operations Hub.

For step-by-step instructions, refer to [Install Common Components \(on page 1273\)](#).

4. On the welcome screen, select **Operations Hub > START**.



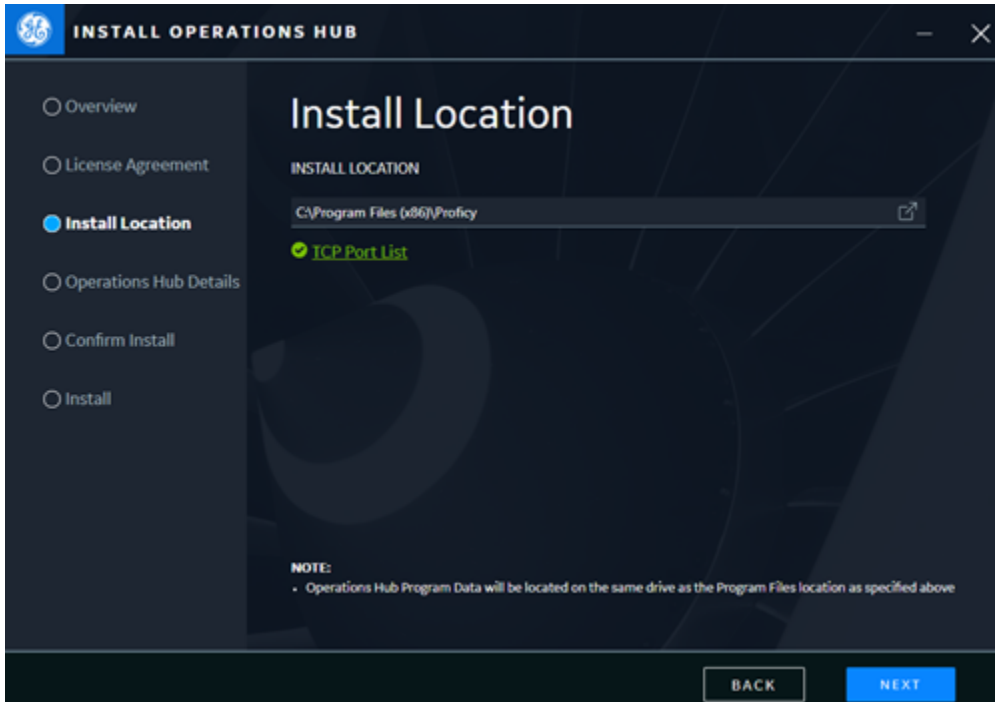
5. Accept the license agreement to continue with the install.



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

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

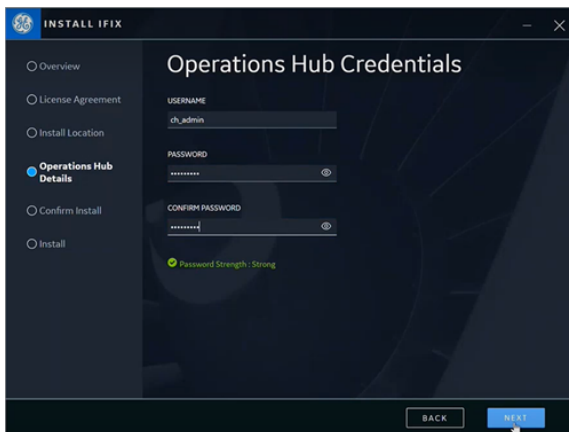
If port conflicts are detected, you must fix them before proceeding to the next screen.



If there are no conflicts, the **Operations Hub Credentials** screen appears.

7. Create these login credentials for Operations Hub and proceed to the next screen.

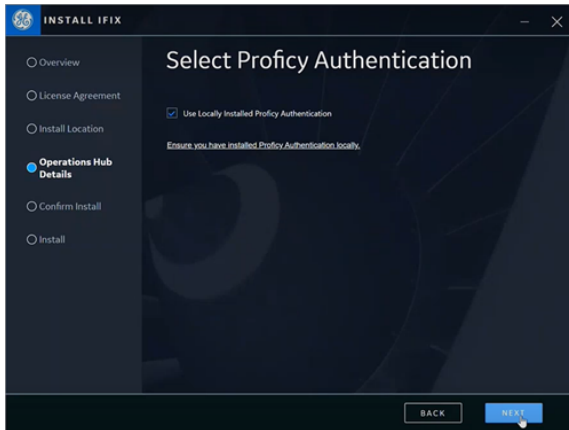
USERNAME	Enter a user name, which you can use to login to the Operations Hub application. For example, <code>ch_admin</code>
PASSWORD	Enter a password for your Operations Hub user login.
CONFIRM PASSWORD	Enter the password again to confirm.



The **Select Proficy Authentication** screen appears.

8. Select the check box for **Use Locally Installed Proficy Authentication** and proceed to the next screen.

Proficy Authentication was locally installed during the [installation of common components \(on page 1273\)](#).



Note:

Prior to Operations Hub installation, you must have a local or remote instance of Proficy Authentication installed. The Operations Hub installation will not be allowed to continue if you select **Use Locally Installed Proficy Authentication** and it is not detected.

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

9. Complete the following and proceed to the next screen.

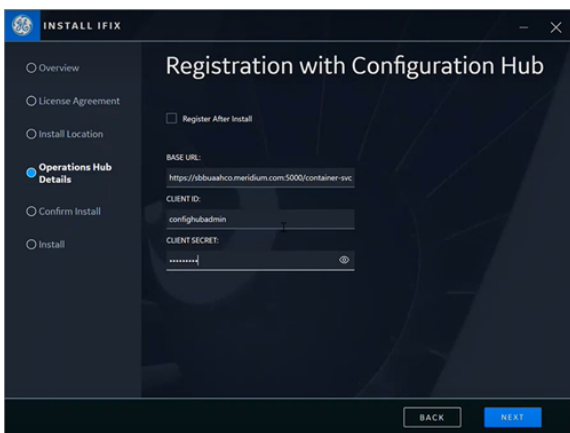


Note:

We provide Configuration Hub login credentials that we already created. Refer to step 4a in the [Install Common Components \(on page 1273\)](#) topic.

<p>Register After Install</p>	<p>If you select this check box, then you can skip registering Operations Hub with the Configuration Hub application for now. You will then need to register after the current Operations Hub installation using the application shortcut on the Desktop. Refer to Register Operations Hub with Configuration Hub (on page 1289).</p>
--------------------------------------	---

	If you choose to register along with the current Operations Hub installation, then leave this check box blank and proceed to provide more details.
BASE URL	Enter the url address to access the Configuration Hub application. For example, <code>https://sbbuaahco.meridium.com:5000/container-svc</code>
CLIENT ID	Enter the client id created for logging in to Configuration Hub. For example, <code>admin</code>
CLIENT SECRET	Enter the secret password created for your Configuration Hub client id.



The **Start Install** screen appears.

10. Select from the following install options:

Silent Install	Select this option if you want to run a silent installation of products without any further user interaction or input. Refer to the <i>Install Operations Hub in Unattended Mode</i> topic in the Operations Hub documentation.
Interactive Install	Select this option if you want to install the following: <ul style="list-style-type: none"> ◦ Refer to the <i>Install Dataflow Editor</i> topic in the Operations Hub documentation.

11. Select **START** to start the installation.

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

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

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

After installation, shortcut icons of the installed applications are created on your desktop.



Important:

If a firewall is running on the server, configure the firewall to make sure the public https port used by Operations Hub Public is not blocked. Typically, the port is 443, but can be a different value that you have selected or that was changed to avoid a conflict. If you are not sure of the port number, the shortcut (URL) placed on the desktop should contain it.

Refer to [Operations Hub documentation](#).

- [Install the Certificate on your Clients](#) (on each client that you will use to access Operations Hub).
- [Install Site Administration Addon](#).

Install Operations Hub from a Dedicated Installer

This topic describes how to install Operations Hub from its dedicated installer.

- Ensure that the machine on which you want to install Operations Hub meets the system requirements.
- Use a machine that does not host any applications that are bundled with Operations Hub.
- Run a Windows update (including security updates).
- Use a host name that contains up to 24 characters and any of the following characters:
 - Alphabetic characters
 - Numeric characters
 - Minus
 - Period
- Ensure that you have administrative privileges to the machine on which you want to install Operations Hub.

Consider these points during installation:

- **First time installation:** You can choose to provide the same user name and password for Operations Hub tenant admin and Configuration Hub. This will allow you to use the same credentials to log in to both the applications.
- **Re-installation:** If re-installing Operations Hub without DB purge, provide the same user name and password as the earlier install. If you provide a different set of credentials other than the tenant admin credentials used in the initial install, the user ID will not match what already exists in Proficy Authentication (UAA). As a result, users will not be able to log into Operations Hub.

1. Download the Operations Hub 2023 ISO install media from the Salesforce and mount the file.
2. From the ISO folder, double-click `Setup.bat` to run the file.

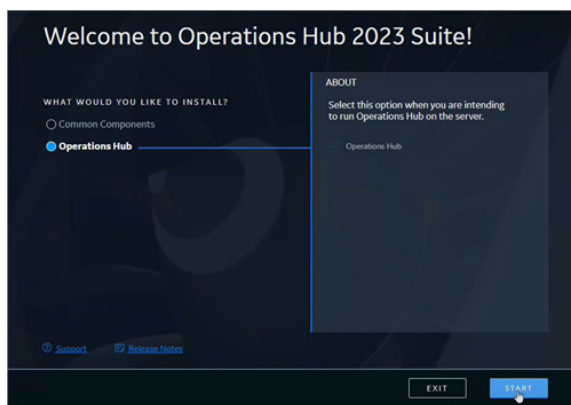
The welcome screen appears.

3. On the welcome screen, you must first install Configuration Hub and Proficy Authentication before installing Operations Hub.

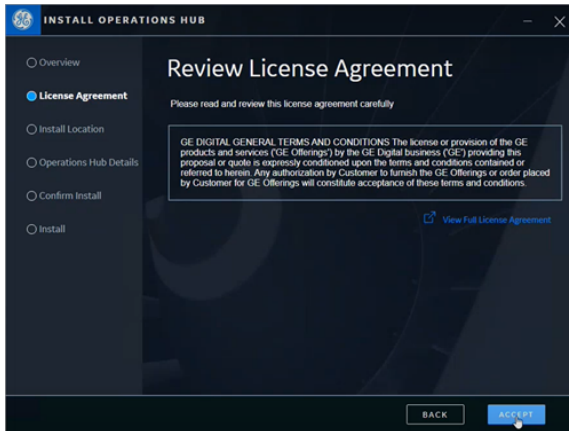
For step-by-step instructions, refer to [Install Common Components \(on page 1273\)](#).



4. On the welcome screen, select **Operations Hub**.



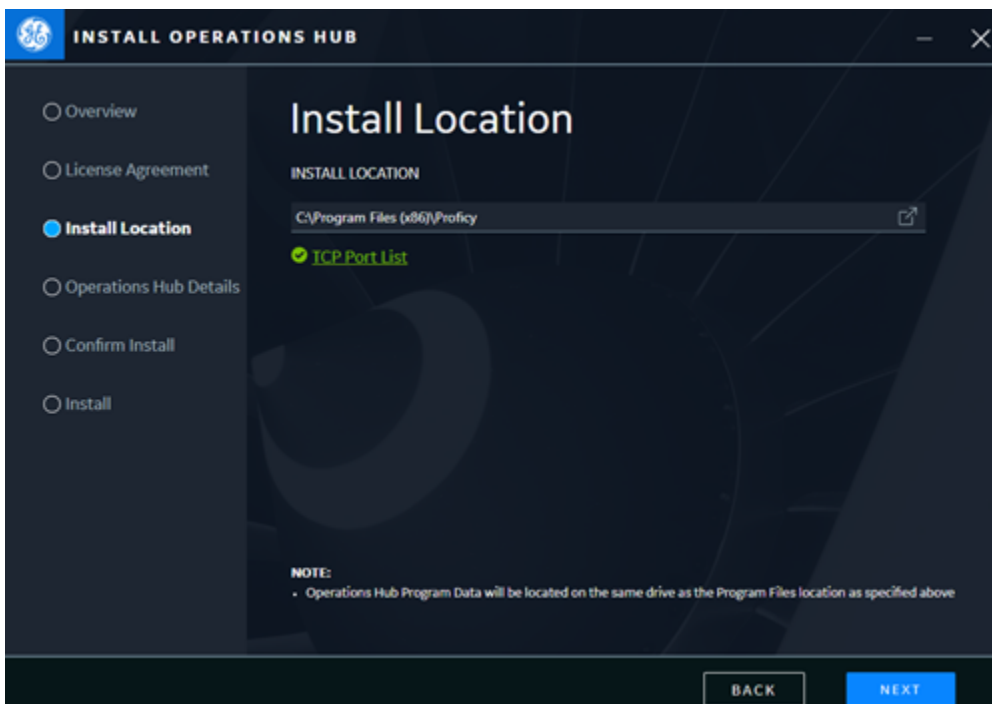
5. Accept the license agreement to continue with the install.



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

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

If port conflicts are detected, you must fix them before proceeding to the next screen.

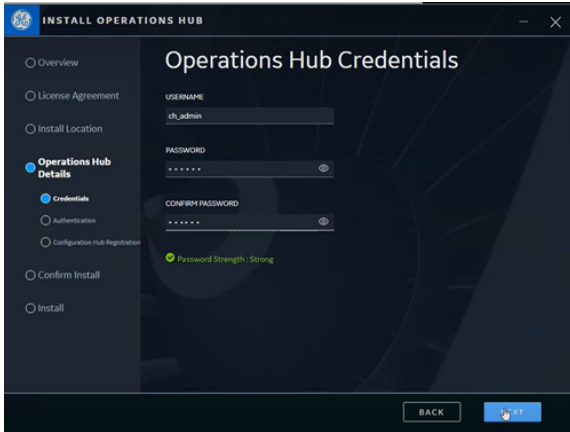


If there are no conflicts, the **Operations Hub Credentials** screen appears.

7. Create these login credentials for Operations Hub and proceed to the next screen.


USERNAME	<p>Enter a user name, which you can use to login to the Operations Hub application.</p> <p>For example, <code>ch_admin</code></p>
-----------------	---

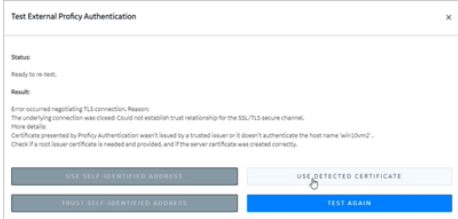
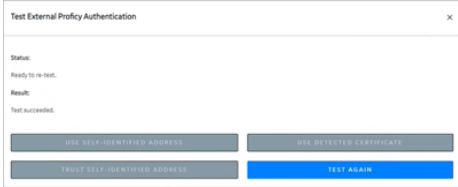
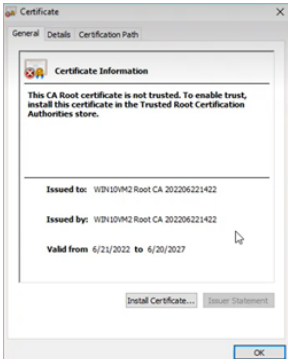
PASSWORD	Enter a password for your Operations Hub user login.
CONFIRM PASSWORD	Enter the password again to confirm.

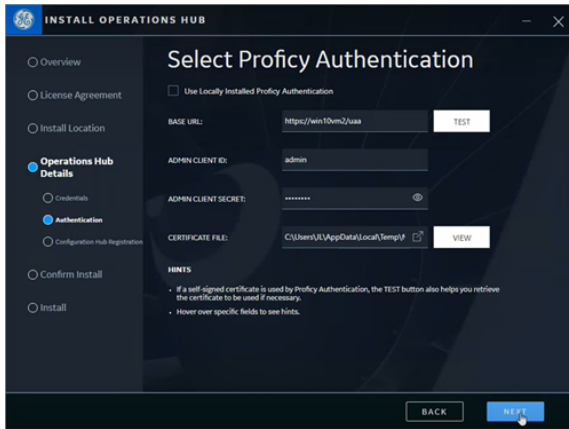


The **Select Proficity Authentication** screen appears.

8. Complete the following and proceed to the next screen.

<p>Use Locally Installed Proficity Authentication</p>	<p>If you select this check box, then the local instance of Proficity Authentication will be used.</p> <p>If you want to use an external Proficity Authentication (UAA), then leave this check box blank and proceed to provide more details.</p> <div style="border: 1px solid #0070c0; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p> Note:</p> <p>Prior to Operations Hub installation, you must have a local or remote instance of Proficity Authentication installed. The Operations Hub installation will not be allowed to continue if you select Use Locally Installed Proficity Authentication and it is not detected.</p> </div>
<p>BASE URL</p>	<p>Enter the url address to access the Proficity Authentication application.</p> <p>For example, <code>https://win10vm2/uaa</code></p>
<p>ADMIN CLIENT ID</p>	<p>Enter the administrator client id to login to Proficity Authentication.</p> <p>For example, <code>admin</code></p>

<p>ADMIN CLIENT SECRET</p>	<p>Enter the secret password for the Proficy Authentication administrator client id.</p>
<p>CERTIFICATE FILE</p>	<p>You can browse and select the security certificate, (or) let the system do it for you.</p> <p>When you test for validation, the system provides you with an option to use a detected certificate as shown here:</p> 
<p>TEST</p>	<p>Select this option to validate all your field entries.</p> <p>The validation results appear on the Test External Proficy Authentication screen, wherein you can do the following:</p> <ul style="list-style-type: none"> ◦ Add and trust self-identified base url ◦ Add detected security certificate <p>Proceed to next only after the validation test is successful as shown here:</p> 
<p>VIEW</p>	<p>Select this option if you want to open and check the added security certificate.</p> 



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

9. Complete the following and proceed to the next screen.

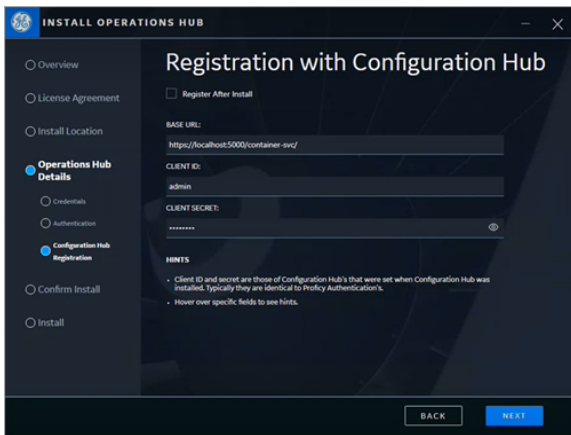


Note:

We provide Configuration Hub login credentials that we already created. Refer to step 4a in the [Install Common Components \(on page 1273\)](#) topic.

<p>Register After Install</p>	<p>If you select this check box, then you can skip registering Operations Hub with the Configuration Hub application for now. You will then need to register after the current Operations Hub installation using the application shortcut on the Desktop. Refer to Register Operations Hub with Configuration Hub (on page 1289).</p> <p>If you choose to register along with the current Operations Hub installation, then leave this check box blank and proceed to provide more details.</p>
<p>BASE URL</p>	<p>Enter the url address to access the Configuration Hub application.</p> <p>For example, <code>https://sbbuahco.meridium.com:5000/container-svc</code></p>
<p>CLIENT ID</p>	<p>Enter the client id created for logging in to Configuration Hub.</p> <p>For example, <code>admin</code></p>

CLIENT SECRET	Enter the secret password created for your Configuration Hub client id.
----------------------	---



The **Start Install** screen appears.

10. Select from the following install options:

Silent Install	Select this option if you want to run a silent installation of products without any further user interaction or input. Refer to the <i>Install Operations Hub in Unattended Mode</i> topic in the Operations Hub documentation.
Interactive Install	Select this option if you want to install the following: <ul style="list-style-type: none"> ◦ Refer to the <i>Install Dataflow Editor</i> topic in the Operations Hub documentation.

11. Select **START** to start the installation.

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

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

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

After installation, shortcut icons of the installed applications are created on your desktop.



Important:

If a firewall is running on the server, configure the firewall to make sure the public https port used by Operations Hub Public is not blocked. Typically, the port is 443, but can be a different value that you have selected or that was changed to avoid a conflict. If you are not sure of the port number, the shortcut (URL) placed on the desktop should contain it.

Refer to [Operations Hub documentation](#).

- [Install the Certificate on your Clients](#) (on each client that you will use to access Operations Hub).
- [Install Site Administration Addon](#).

Register Operations Hub with Configuration Hub

This topic describes how to register Operations Hub with Configuration Hub post installation.

You should perform the following steps only if you select the **Register After Install** option on the **Registration with Configuration Hub** screen.

1. On your desktop, double-click the **Register Operations Hub with Configuration Hub** shortcut icon.
The registration screen appears.
2. Enter the following details.



Note:

You must provide the same Configuration Hub credentials entered when installing Configuration Hub as part of common components.

CONFIGURATION HUB BASE URL	Enter the url address to access the Configuration Hub application.
CLIENT ID	Enter the client id created for logging in to Configuration Hub.
CLIENT SECRET	Enter the secret password created for your Configuration Hub client id.

3. Select **Register**.

The screenshot shows a web browser window with the address bar displaying "localhost:3000/chregister". The page content is organized into three main sections:

- Configuration Hub Info:** This section contains three input fields:
 - Configuration Hub Base URL: `https://localhost:5000/container-svc/`
 - Client ID: `confighubadmin`
 - Client Secret: `.....`
- Operations Hub Plugins:** This section features a "Designer Plugin:" label and two buttons: "Register" (highlighted in blue) and "Unregister".
- Result:** This section displays the message "Response: OK. Expand for the response details." and a button labeled "Details" with a right-pointing arrow.

Getting Started with Operations Hub

This topic describes how to work with Operations Hub using the latest (HMI powered designer) and the classic version. For more complete details on how to use Operations Hub, refer to the [Operations Hub help](#).

With 2023 release, Operations Hub is now available as a plug-in in Configuration Hub. The latest version is equipped with a HMI designer layout, and has enhanced plug-in functionality. All the features from the classic version of Operations Hub are also available in this latest version.

1. Install the latest version of Operations Hub. Refer to [Operations Hub and the Integrated Installer \(on page 1272\)](#).
2. Log in to the Operations Hub classic and set up the following:
 - Data Sources (required)
 - Queries
 - Entities
 - Themes (optional)
3. Log in to the latest version of Operations Hub via Configuration Hub.

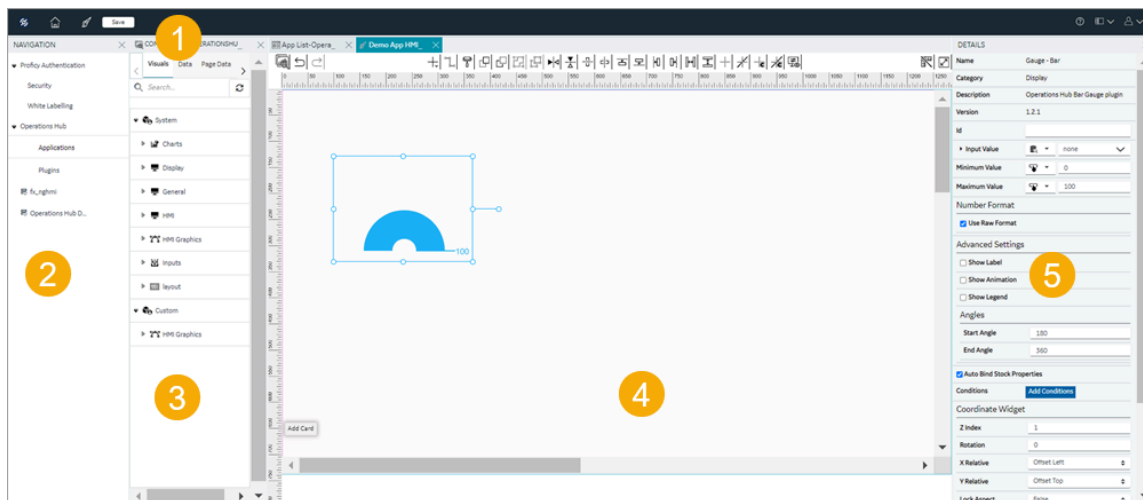
- a. Double-click the Configuration Hub desktop shortcut.
 - b. Log in with the credentials that you specified during installation.
 - c. On the Configuration Hub navigation panel, navigate to the Operations Hub home page. For more information on using the Operations Hub new layout, refer to [Panels Layout \(on page 1291\)](#).
4. [Create an application.](#)
 5. [Create pages for your application.](#)
 6. Use the following features to design your application pages:
 - [Page Grid Details \(on page 1312\)](#)
 - [Design a layout using the coordinate card \(on page 1321\)](#).
 - [Design a layout using the flexbox card \(on page 1314\)](#).
 - [Apply format tools to design your pages \(on page 1307\)](#).
 - [Connect plug-ins with a line connector \(on page 1308\)](#).
 - [Animate HMI graphics \(on page 1325\)](#).
 - [Bind data to your plug-ins \(on page 1300\)](#).
 7. Save the application pages, and preview the end application.

Operations Hub (New Layout)

Panels Layout

This topic provides an overview of the latest Operations Hub application layout.







Log in to the latest version of Operations Hub via Configuration Hub and access the Operations Hub home page. The following screen provides an overview of all the panels that appear in the Operations Hub new layout.



1	Toolbar Menu (on page 1292)
2	Navigation Panel (on page 1292)
3	Components Panel (on page 1294)
4	Display Panel (on page 1305)
5	Details Panel (on page 1310)

Toolbar Menu

The toolbar contains the following menus:

	Select this icon to reload the application.
	Select this icon to work in the configuration mode, wherein you are connected to the Configuration Hub navigation panel.
	Select this icon to work in the Operations Hub designer mode. The Configuration Hub navigation panel is disconnected to allow more work area for Operations Hub designer.
Save	The Save button on the toolbar is highlighted whenever you modify settings.
	Select this icon to access Operations Hub online documentation.
	Select the icon to open/close Navigation and Details panels for a clutter-free workspace.
	Select this icon to logout of the application.

Navigation Panel

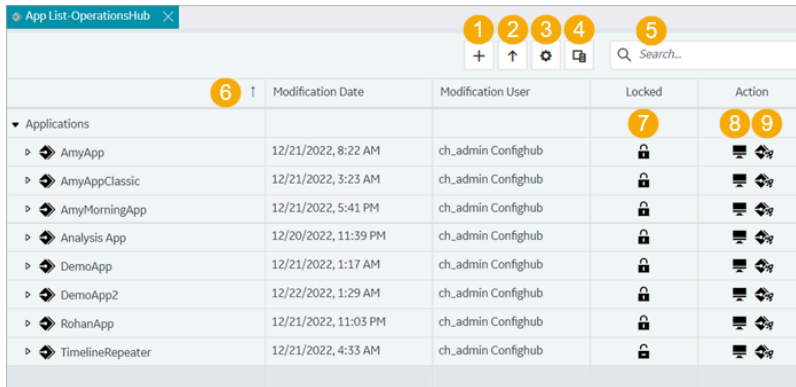
This topic provides an overview of the navigation panel from Configuration Hub in the Operations Hub new layout.

On this panel, you can navigate to other Proficy applications installed within your Configuration Hub environment. Under Operations Hub, you have access to the following areas:


- [Applications \(on page 1293\)](#)
- [Plug-ins \(on page 1294\)](#)

Applications

On the applications homepage, you can perform tasks as described in the following table.



1	Creates a new application.
2	Imports an application.
3	Allows to perform the following actions: <ul style="list-style-type: none"> • App Actions: A selection check box appears next to the applications and allows to perform related operations. • Page Actions: A selection check box appears next to the pages and allows to perform page related operations. You must select the app to show page check box. • Clear: Clears all selection check boxes.
4	Opens a Column Chooser dialog, where you can select the columns you want to appear on the applications homepage.
5	Enter keywords to search for applications or pages.
6	Sorts columns in ascending or descending order. The status is indicated by the up/down arrow on each sortable column header.
7	Indicates whether the application is in a locked or unlocked state.
8	Allows to perform tasks on the selected application or page. You can either: <ul style="list-style-type: none"> • Select this icon for the app/page to access task actions, (OR) • Right-click the app/page to access task actions. <p>Existing app/page names are quickly editable on the homepage itself.</p>

	<div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: Applications/pages created in the Operations Hub Classic version cannot be modified in the new Operations Hub layout. Such applications are marked as legacy apps. You can only preview them. </div> <p>For more information on applications and pages, refer to Operations Hub documentation.</p>
9	Opens the end application.

Plug-ins

On the plug-ins homepage, you can perform tasks as described in the following table:



1	Enter keywords to search for plug-ins.
2	Expand System to view the system plug-ins available in Operations Hub. See also Visuals Tab (on page 1295) .
3	Expand Custom to view custom plug-ins. If you have saved any customized plug-ins, then they appear under custom plug-ins.
4	Reloads the plug-ins screen.

For a high-level panel layout, see [Panels Layout \(on page 1291\)](#).

Components Panel

This topic provides an overview of the components panel in the Operations Hub new layout.

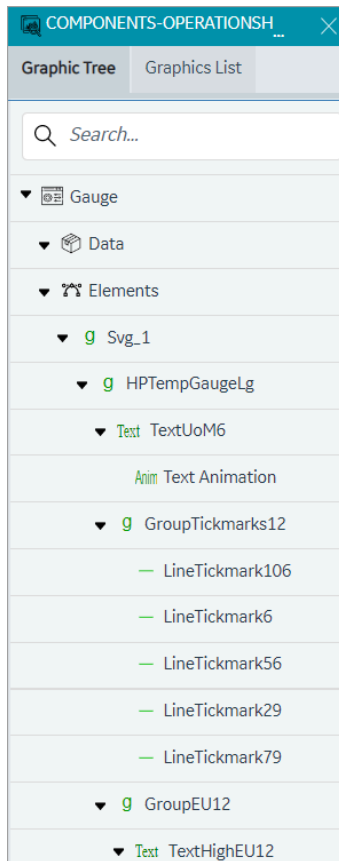
On Operations Hub components panel, you can access the following tabs for designing application pages:

- [Visuals \(on page 1295\)](#)
- [Data \(on page 1300\)](#)

- [Page Data \(on page 1303\)](#)
- [Page Visuals \(on page 1305\)](#)

On Operations Hub components panel, you can access the following tabs while working with the SVG editor:

- **Graphic Tree:** On this tab, expand the tree-view structure to review the properties currently configured for the graphic.
- **Graphics List:** On this tab, you can access all the plug-ins listed under the custom category.



For a high-level panel layout, see [Panels Layout \(on page 1291\)](#).

Visuals Tab

This tab provides access to system and custom plug-ins in Operations Hub.

You can configure the plug-ins to work with the components of an application, such as entities and queries.

1. Open an application page.
2. Select the **Visuals** tab.
3. Drag-and-drop the plug-ins to design your page.

You can also double-click a plug-in to add to the page.

Following list of plug-in categories are available as **System** plug-ins:

- [Charts \(on page 1296\)](#)
- [Display \(on page 1297\)](#)
- [General \(on page 1298\)](#)
- [HMI \(on page 1298\)](#)
- [HMI Graphics \(on page 1298\)](#)
- [Inputs \(on page 1299\)](#)
- [Layout \(on page 1300\)](#)

The **Custom** plug-ins contains the list of plug-ins saved with custom functionality. Refer to [About HMI Graphics \(on page 1325\)](#).

Plug-in Enhanced Preview


Enhanced preview enables to access the real-time data preview within the page designer itself. Some of the plug-ins under [Charts \(on page 1296\)](#), [Display \(on page 1297\)](#), and [Inputs \(on page 1299\)](#) are powered with an enhanced preview feature. This means that the plug-in preview (within the designer) is the same as the result that appears in the end application. Refer to the respective plug-in categories for a full list of plug-ins that support enhanced preview.

Currently, the enhanced preview feature works only when the data is bound to the plug-in using the [manual \(on page 1312\)](#) option. Data binding via other methods does not support enhanced preview.

Charts

Except timeline, spider chart, trend card, and histogram, the enhanced preview feature is available for all the charts category plug-ins.

Bullet Graph	Compares a single value to a target value. Available variants are bullet graph and bar graph.
Histogram	Creates a visual representation of data distribution.

Spider Chart	Visualizes data in a web-like pattern to compare and analyze multiple data sets.
Trend Card	Helps to analyze data trends over a time period. <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; background-color: #e6f2ff;">  Note: Do not rotate the trend card plug-in in the page designer. </div>
Variwide Chart	Each column in a variwide chart has a separate width to represent the third dimension. Helps to analyze multi-dimensional data.
Sparkline	Visualizes events over a time span. The chart displays each data point of a set of time series data as a separate event along a horizontal line. Creates tiny data charts that can fit into compact areas in your application.
Line Chart	Use a line chart to visualize data using data points.
Pareto Chart	Graphically summarize and display the relative importance of the differences between groups of data.
Pie Chart	Visualize data using data points that belong to different categories.
Timeline	Create visual charts that help to monitor the progress of your events.


Display

Except Datagrid and Pivot Grid, the enhanced preview feature is available for all the display category plug-ins.

Gauge Bar	Presents data in simple bar format.
Gauge Circular	Measure data values on a radial scale.
Gauge Linear	Measure data values on a linear scale.
Solid Gauge	Displays data in six different styles with alert and color limits.
Datagrid	Displays data in a tabular format. Supports grouping, filtering, and sorting column data. You can also animate the data cells.
Pivot Grid	Visualize data in a multi-dimensional format. You can apply conditions to format cells, filter rows/columns by value, and export data to a CSV file.
Image	Insert images in your application.
Indicator	Indicator with range limits and styling.

Simple Indicator	Simple indicator is a lighter version of the indicator plug-in.
List	Display data in bullet points.
Text	Create display-only text in your application.
Value Display	Displays data values with a variety of configurable properties.

General

Favorite Organizer	Create folders and organize your favorite trend charts.
iFrame	Load information from external sources.
Breadcrumb	Shows the hierarchy to the current asset and allows the user to select any item in the list to trigger a change of context to that asset. Use a breadcrumb for easy navigation in your application. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: Do not rotate the breadcrumb plug-in in the page designer. </div>
HTML Editor	Helps to create and edit HTML code.

HMI

Alarm Card	Provides details of the active alarms by their severity levels in the HMI/SCADA system for the selected asset.
Alarm Count	Provides the total alarm count by their severity levels in the whole HMI/SCADA system.
CIMPLICITY HMI Web-space	Opens an instance of the Webspace remote access application.
Mimic Card	Displays mimics from the SCADA systems.
iFIX HMI Webspace	Opens an instance of the Webspace remote access application.

HMI Graphics

Use the following list of graphics based on your specific application and industry requirements. See [About HMI Graphics \(on page 1325\)](#).

Gauge	High performance HMI graphic to represent pressure, flow, temperature or level gauges.
Mixer	High performance HMI graphic to represent agitators or batch mixers.
Motor	High performance HMI graphic to represent AC/DC motors, etc.
Pump	High performance HMI graphic can be configured to provide real-time feedback on the pump's status, such as flow rate, pressure, temperature, etc.
Tank	High performance HMI graphic to represent storage, mixing, or pressure tanks.
Valve	High performance HMI graphic to represent centrifugal, displacement, or gear pumps.

Inputs

The enhanced preview feature is available for all the input category plug-ins.

Button	Trigger an action in your application.
Checkbox	Create mutually exclusive data options.
Date Picker	Display date and time in a variety of formats.
Dropdown	Create a drop-down list from which operators can select between multiple choices.
DateTime Range Picker	Display and edit beginning and ending date time pairs.
Radio Button	Create radio button selection list.
Slider	Generate a slider selection format.
Text Area	Create a text area in your application.
Textbox	Insert a text box wherein the operator can enter data that goes in to the database.
Toggle	Create a toggle switch.

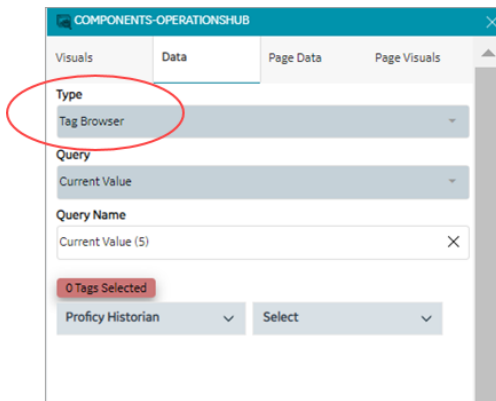
Layout

Interactive Map (on page 1322)	Create a coordinate/flex interactive map layout.
Repeater (on page 1324)	Create a flex repeater layout.

Data Tab

This tab displays the data types you can apply to the plug-ins.

Select your data type from the **Type** drop-down field.



Choose from the following data types:

- [Tag Browser \(on page 1300\)](#)
- [Query \(on page 1301\)](#)
- [Globals \(on page 1301\)](#)
- [Admin Functions \(on page 1302\)](#)
- [M2M Functions \(on page 1302\)](#)
- [Asset Management Functions \(on page 1303\)](#)

Tag Browser

You can browse a data source and select the properties/tags.

1. From **Type**, select `Tag Browser`.
2. From **Query**, select an extension query.

The selected query is populated in **Query Name**.

3. Browse the data source and select the check box for the tag/s you want add.
4. Drag and drop the tags on the plug-in to bind data.

Query

1. From **Type**, select `Query`.
2. From **Query Type**, select the query type you want to use. The query types appear in the list box based on the queries you created in the Operations Hub classic version. For example, if you select `Extension` or `Entity`, additional selection fields appear.

<code>Extension</code>	<p>Populates extension type of queries in the Query field.</p> <p>Select an extension query to add to the plug-in. The selected query is populated in Query Name.</p>
<code>Entity</code>	<p>Populates entities in the Query field.</p> <p>Select an entity to add to the plug-in. The selected entity is populated in Query Name.</p>

3. Select **+ Add**.

Globals

1. From **Type**, select `Globals`.
2. From **Globals**, select any of these options:

<code>System</code>	<p>Is associated to a computer's settings. Populates system date/time variables.</p>
<code>Output</code>	<p>Is associated to query data fields. Populates available queries in the Query field.</p> <ol style="list-style-type: none"> a. Select a query to populate its date fields. b. Select a data field from Outputs.
<code>Custom</code>	<p>Allows you create your own customized global variable.</p> <ol style="list-style-type: none"> a. Enter a name for the variable. b. Choose from the available data types to define the variable.
<code>URL Parameters</code>	<p>Is associated to a URL address. Enter a name for the variable.</p>

3. Select **+ Add Global**. All added globals appear on the **Page Data** tab.
4. Go to **Page Data** tab and select the global. The global details appear on the details panel.

5. On the details panel, you can specify the **Global Type** as `App` or `Page` global.
6. For custom and URL parameter global, enter the **Initial Value**.

Admin Functions

Use these functions to perform system administration tasks.

1. From **Type**, select `Admin Functions`.
2. Select from:

<code>Send Email</code>	Sends an email to specified recipient/s using the email sender service.
<code>DeleteAlertInstance</code>	Deletes the alert set for an asset object instance.
<code>StartStopAlertInstance</code>	Starts and stops the alert set for an asset object instance.
<code>Get all apps</code>	Retrieves a list of all applications in Operations Hub.
<code>Get all apps for user id</code>	Retrieves a list of all applications in Operations Hub that are associated with a specific user ID.
<code>Delete image on hard disk</code>	Deletes the image file on the logged-in user's hard disk.
<code>GetAllAlerts</code>	Retrieves a list of all alerts in Operations Hub.
<code>appGetCurrentUser</code>	Retrieves the current user of the application.
<code>GetEventByName</code>	Retrieves an event by its name.

3. Select **+ Add**.

M2M Functions

Perform machine-to-machine functions to control and manage devices remotely.

1. From **Type**, select `M2M Functions`.
2. Select from:

<code>Send_MQTT_Command</code>	Sends a command to a device using the MQTT (Message Queuing Telemetry Transport) protocol. The device must be configured with IQP MQTT.
--------------------------------	---

Send_REST_Command	Sends a command to a device using the REST (Representational State Transfer) protocol.
-------------------	--

3. Select **+ Add**.

Asset Management Functions

Use these functions to manage and track assets, such as devices and systems.

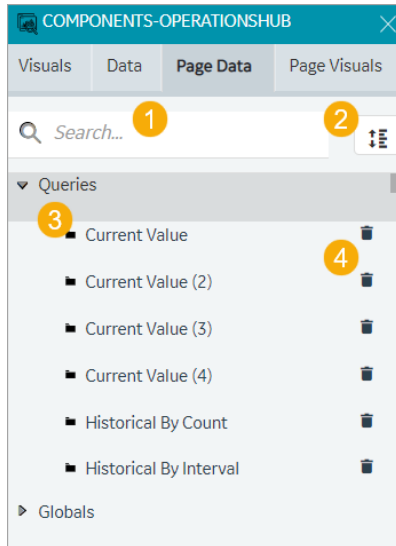
1. From **Type**, select `Asset Management Functions`.
2. Select from:



Add new device type	Creates a new category to classify similar type of devices.
Add new metric to device type	Adds a new measurement unit to the device type.
Add new device	Adds a new device (for example, Pump).
Add new thing	Adds a new thing (IoT devices)
Add new group	Creates a new group to gather and manage similar devices or things.
Add device or thing to group	Assigns a device or thing to a group.
Add new device cloud	Adds a new device cloud, which can be used to host and manage devices remotely.
Add new cloud account	Adds a new cloud account, which can be used to manage devices that are hosted on a cloud service.

3. Select **+ Add**.

Page Data Tab

This tab displays the data applied to the page.



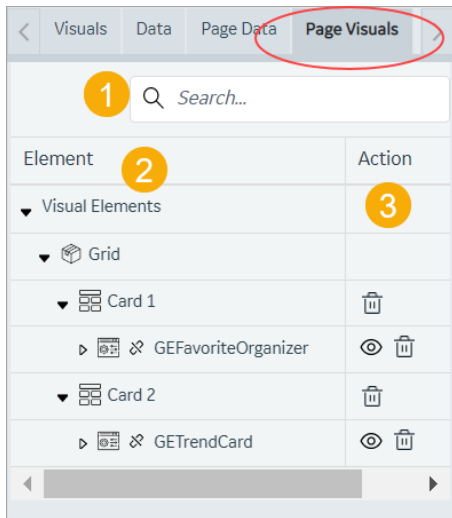
1	Enter keywords to search within the data (queries, globals, etc.) that is bound to the page.
2	<p>Enable/Disable the icon to determine the functionality of drag-and-drop action.</p> <p> When disabled, it is white in color. In this mode, you can drag-and-drop a global on the plug-in to perform auto binding of data. The drag-and-drop action invokes a list of plug-in properties to choose from, and binds data to the selected property.</p> <div data-bbox="540 1234 769 1520" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Bind System - Date - Current Date (Local) ✕</p> <p>Sources ▼</p> <p>Minimum Value</p> <p>Maximum Value</p> <p>Input Value</p> <p style="text-align: center; margin-top: 10px;">Cancel</p> </div> <p> When enabled, it turns blue. In this mode, you can drag and rearrange the order of queries. To move a query up/down in a ordered list, simply select and drag the query item, and then drop it on the new location (up/down).</p>
3	A tree-view of the data that is bound to the page.

4	Option to delete the data bound to the page.
---	--

Page Visuals Tab

This tab displays a visual overview of all the elements or objects on the page.

1. Open an application page.
2. Select **Page Visuals** tab.
3. Select any object on the page to locate its hierarchy in the tree layout.











1	Enter keywords to search within the elements added to the page.
2	<p>Elements added to the page appear in a tree data structure showing their hierarchical relationship.</p> <p>To sort the elements in ascending/descending order, select the Element column header.</p>
3	<p>You can perform the following actions:</p> <ul style="list-style-type: none"> • Delete at card-level. The card and the plug-ins within the card are deleted from the page. • Delete a plug-in added to the page. • Show/Hide a plug-in on the page.

Display Panel

The display panel serves as the display area for working with applications and their pages within Operations Hub.

Before you start to design your page, you can set up the page grid. Open the page and select anywhere outside of the card to access the settings for the page grid. Refer to [Page Grid Details \(on page 1312\)](#).

	Select the data panel icon to show or hide the components panel (on page 1294) and increase the display panel work area.
	Select this icon to show or hide the ruler. The ruler appears by default when you create a page.
Add Card 	<p>Adds a card on the page. A card is a container that holds the plug-in objects.</p> <ul style="list-style-type: none"> • See Coordinate Card (on page 1321) • See Flexbox Card (on page 1314)
	<p>The page refresh icon appears when you edit a page. If the layout gets distorted, refresh the page.</p> <p>During user interface operations (in particular when using Flexbox layout, or after Undo/Redo operations), the display panel's canvas area might get distorted or misaligned. To recover the page, select the refresh icon to reload the view.</p>
	Select the full screen icon to display in the full screen mode.
Page Building Tools	A tools menu that you can use to format plug-in objects on a page. See Page Building Tools (on page 1307) .
	Undo an action on the page.
	Redo an action on the page.
Launch 	Launches the end application.

For a high-level panel layout, see [Panels Layout \(on page 1291\)](#).

Keyboard Shortcuts Keys

These are the computer keyboard shortcut keys to perform UI operations:

UI Operation	Windows	Mac
Copy	Ctrl+C	Command+C
Paste	Ctrl+V	Command+V
Duplicate	Ctrl+D	Command+D
Toggle line connector mode	L	L
Toggle ruler	Ctrl+R	Command+R
Redo	Ctrl+Y	Command+Y
Undo	Ctrl+Z	Command+Z

Page Building Tools

Use these tools to design visually appealing application pages.



Tool	Description
Line Connector On/Off	Activates or deactivates the line connector. Use the line connector tool to connect and draw a relationship between two plug-in objects on the page. See Line Connector (on page 1308) .
Bring Front	When objects overlap on the page, brings the selected object to the front.
Send Back	When objects overlap on the page, sends the selected object to the back.
Group	Groups two or more selected objects on the page.
Un Group	Ungroups a grouped object.
Horizontal Flip	Turns the object to create its mirror image.
Vertical Flip	Turns the object upside-down.
Align Horizontally Center	Horizontally aligns all the objects towards the center of the page.
Align Vertically Center	Vertically aligns all the objects towards the center of the page.
Align Vertically Top	Vertically aligns all the objects towards the top of the page.
Align Vertically Bottom	Vertically aligns all the objects towards the bottom of the page.

Tool	Description
Align Left	Aligns all the objects to the left side of the page.
Align Right	Aligns all the objects to the right side of the page.
Distribute Horizontally	Horizontally aligns the selected objects and evenly distributes the space between them.
Distribute Vertically	Vertically aligns the selected objects and evenly distributes the space between them.
Guide On	Shows the guidelines on the page.
Guide Off	Hides the guidelines on the page.
Guide and Snap On	Shows the page guidelines, and object snap points.
Guide and Snap Off	Hides the page guidelines, and object snap points.

Line Connector


A line connector is a tool to show a connection between two or more objects.

Place two visual objects next to each other on a page, and draw a line connector to link them. You can draw straight line connectors or angle line connectors to link visual objects. You can use the [line connector properties \(on page 1309\)](#) to:

- Customize line connector arrowheads to help explain the direction of the flow from one object to the other.
- Apply varied line styles.
- Add a unique color and thickness to the lines.

Draw Line Connector

To draw a line connector, follow these steps:

1. On the page designer [toolbar \(on page 1307\)](#), select  to activate the line connector.
2. Single-click/mouse-click on the page where you want to draw.
3. Start to draw the line by dragging the mouse in the direction you want the line to go. To add a vertex in line, single-click.

4. To end the line connector, Shift-click. (On the keyboard, hold down the `Shift` key and release the mouse-click.)

5. To deactivate the line connector, select  on the page designer [toolbar \(on page 1307\)](#).


Add Vertex

A vertex is a node/point on the line connector. You can add a vertex on the line connector to help demonstrate the relationships between multiple objects. To add a vertex to any line connector:

1. Select the line connector, for which you want to add a vertex.
2. Double-click to select the area on the line connector where you want to add a vertex.
3. Drag the vertex to create an angle.

Delete Line Connector

To delete a line connector:

1. Select the line connector you want to delete.
2. Select  that appears next to the line connector. You can also select the `Delete` key on the keyboard to delete the line connector.

Line Connector Properties

Property	Description
Color	Use the color palette to apply a color to the line.
Width	Enter a width to set the thickness of the line.
Stroke Type	Define how you want the line to appear: <ul style="list-style-type: none"> • <code>solid</code>: Creates a solid line. • <code>dots</code>: Creates a dotted line. • <code>dashes</code>: Creates a dashed line.
Start Marker End Marker	Define a start/end line marker from these options: <ul style="list-style-type: none"> • <code>smallArrowMarker</code>: Adds a small-sized arrowhead. • <code>mediumArrowMarker</code>: Adds a medium-sized arrowhead. • <code>largeArrowMarker</code>: Adds a large-sized arrowhead.

Property	Description
	<ul style="list-style-type: none"> • <code>vertexMarker</code>: Adds a circle. • <code>none</code>: No line marker is added.
Middle Marker	Define a line marker for the points in the middle of the line: <ul style="list-style-type: none"> • <code>circle</code>: Adds a circle. • <code>none</code>: No line marker is added.
Layer	These layers are defined for line connectors so that they appear either above or behind the plug-ins in the end application. <ul style="list-style-type: none"> • <code>back</code>: The line connector is sent to the back, when overlapped by any object on the page. • <code>front</code>: The line connector is brought to the front, when overlapped by any object on the page.
Rounded Corners	Select this check box if you want a round corner instead of a pointed corner.

Details Panel

All the properties/settings specific to your current selection appear on the details panel.

- Access application settings.
- Access page settings.
- You can modify and save plug-in properties.
- Select source/target data. See [Bind Your Data to Plug-ins \(on page 1310\)](#).
- Access animation properties in the SVG editor mode.

For a high-level panel layout, see [Panels Layout \(on page 1291\)](#).

Bind Your Data to Plug-ins

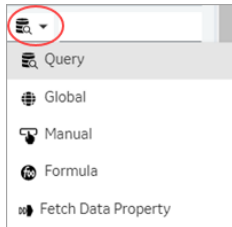
This topic describes the available options to configure source and target data.

In Operations Hub, you can select from the following options to pass values to the plug-in from your data source. You can also specify a target data source to receive data from a plug-in.

- [Query \(on page 1311\)](#)
- [Global \(on page 1312\)](#)

- [Manual \(on page 1312\)](#)
- [Formula \(on page 1312\)](#)
- [Fetch Data Property \(on page 1312\)](#)

On the plug-in's details panel, you can choose the options from a drop-down menu.



Query

When using a query to configure **source data**, select at least one output field.

Alias	Option to enter a temporary name for the query's output field.
Output Field	<p>Lists all the data fields available in the selected query.</p> <p>On executing the query, data is retrieved from the data source for the selected output fields.</p> <p>For example, a weather application might use a query to retrieve the current temperature, humidity, and precipitation levels for a particular location, and use these fields as the basis for its output.</p>
+Add	To include additional query output fields, select this option.
+Add All	If you want to include all the query output fields, then select this option.

When using a query to configure **target data**, select at least one input field.

Input Field	<p>Lists all the data fields available in the selected query.</p> <p>The selected input fields are used to execute the query to retrieve data.</p> <p>For example, a weather application might include input fields where you can specify the location, temperature unit, or forecast duration.</p>
+Add	To include additional query input fields, select this option.

Global

This option allows you to select a global variable to configure source data and target data.

Manual

This option allows you to manually enter the values for the plug-in. You can also access [enhanced preview \(on page 1296\)](#) of the real-time data within the page designer. The plug-in preview is the same as the result that appears in the end application.

Formula

Select **Add Formula** to create a formula that returns values for the plug-in.

Fetch Data Property

This option is view-only. It applies when you drag-and-drop tag data on a plug-in. The drag-and-drop action automatically fetches the data from the data source, and updates values to a list of applicable properties.

On drag-and-drop, the **Fetch Data Property** label appears for:

- Minimum and Maximum scale values
- Engineering unit
- Data range values

In case you drag-and-drop multiple tags on a plug-in, then values fetched from the first tag are applicable to the above listed properties.

Page Grid Details

This topic describes the page grid properties.

A page is divided into grids, wherein multiple card layouts can be added. Select outside of the card layout to access the page's grid properties. By default, the page grid has 12 rows and 12 columns.

Properties

Field Name	Description
Grid Type	Choose from these grid types:

Field Name	Description
	<ul style="list-style-type: none"> • <code>fit</code>: The grid fits to the size of the available space irrespective of the specified number of rows and columns. • <code>fixed</code>: This is the default option. The grid appears in a fixed size based on the specified number of column and rows. • <code>verticalFixed</code>: The grid's row height is fixed. Column width is adjustable to fit to the size of the available space. • <code>horizontalFixed</code>: The grid's column width is fixed. Row height is adjustable to fit to the size of the available space.
Mobile Breakpoint	This value determines the page grid layout adjustment on a mobile device.
Margin	This value determines the size of the gap between the rows and columns.
Display Grid	<p>Choose how you want to display the grid on the page:</p> <ul style="list-style-type: none"> • <code>always</code>: Shows the grid lines on the page. • <code>onDrag&Resize</code>: Allows to drag and resize grid columns and rows. • <code>none</code>: Hides the grid lines on the page.
Fixed Col Width	<p>Appears when Grid Type is <code>fixed</code> and <code>horizontalFixed</code>.</p> <p>Enter a value to set a fixed width for the grid columns.</p>
Fixed Row Height	<p>Appears when Grid Type is <code>fixed</code> and <code>verticalFixed</code>.</p> <p>Enter a value to set a fixed width for the grid rows.</p>
Min Cols	<p>Appears when Grid Type is <code>fit</code> and <code>verticalFixed</code>.</p> <p>Enter a value to set minimum width for the grid columns.</p>
Max Cols	<p>Appears when Grid Type is <code>fit</code> and <code>verticalFixed</code>.</p> <p>Enter a value to set maximum width for the grid columns.</p>
Min Rows	<p>Appears when Grid Type is <code>fit</code> and <code>horizontalFixed</code>.</p> <p>Enter a value to set minimum width for the grid rows.</p>
Max Rows	<p>Appears when Grid Type is <code>fit</code> and <code>horizontalFixed</code>.</p> <p>Enter a value to set maximum width for the grid rows.</p>
Row Height Ratio	Appears when Grid Type is <code>fit</code> .

Field Name	Description
Outer Margin	Appears when Grid Type is <code>fit</code> , <code>verticalFixed</code> , and <code>horizontalFixed</code> .

Flexbox Card

This layout offers a flexible and responsive design structure.

A flexbox card aligns and distributes the items along a main axis. Objects placed within a flexbox card are laid out next to each other, row-wise or column-wise. When we drag and drop plug-in objects, they get rearranged to follow the one-dimensional layout concept.

The ideal way to use a flexbox card is when you have objects that require flexibility to grow and shrink, and fit within the layout. Use the flexbox properties to control the alignment and distribution of the objects (items).

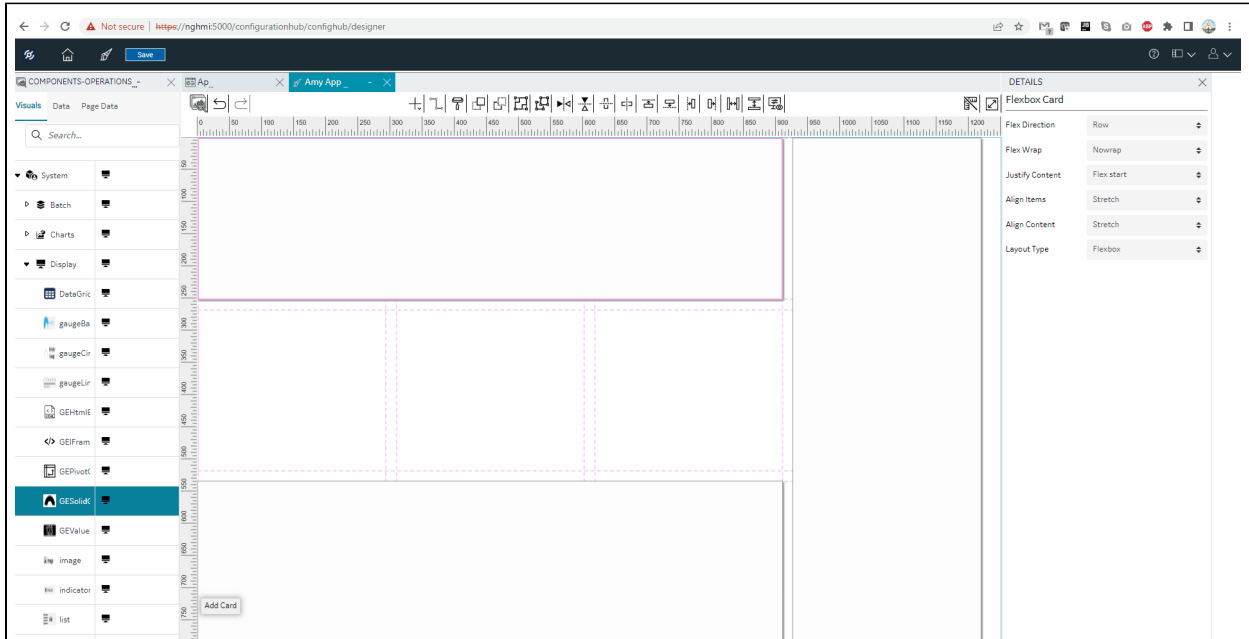
Flexbox Properties

Field Name	Description
Columns	The card occupies the specified number of columns on the page grid (on page 1312) .
Rows	The card occupies the specified number of rows on the page grid (on page 1312) .
Position X	Applies to the horizontal placement of the card on the page. When the value is <code>0</code> , the card is placed on the left-most side of the page. As you increase the value, the card moves away from the left side of the page.
Position Y	Applies to the vertical placement of the card on the page. When the value is <code>0</code> , the card is placed at the top of the page. As you increase the value, the card moves away from the top of the page.
Flex Direction	The objects are arranged next to each other based on these placement directions: <ul style="list-style-type: none"> <code>Row</code>: The objects within the card are placed horizontally, from left to the right. <code>Column</code>: The objects within the card are placed vertically, from top to bottom.

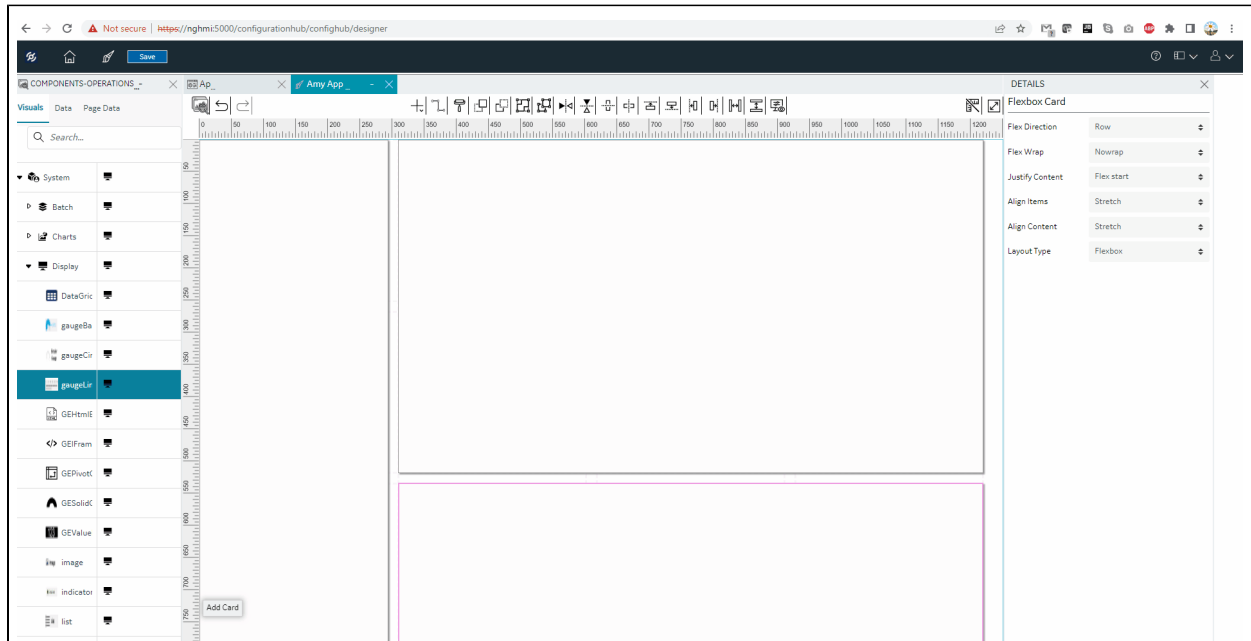
Field Name	Description
	<ul style="list-style-type: none"> • <code>Row reverse</code>: The objects within the card are placed horizontally, from right to left. • <code>Column reverse</code>: The objects within the card are placed vertically, from bottom to top. <p>See Flex Row (on page 1317), Flex Row and Column (on page 1318).</p>
Flex Wrap	<p>By default, objects within the card are not wrapped.</p> <ul style="list-style-type: none"> • <code>Nowrap</code>: All the objects within the card try to fit into a single line, as per the flex direction. • <code>Wrap</code>: The objects are evenly spaced, and are arranged in multiple lines, as per the flex direction. The wrap orientation is from top to bottom. • <code>Wrap reverse</code>: The objects are evenly spaced, and are arranged in multiple lines, as per the flex direction. The wrap orientation is from bottom to top. <p>See Flex Wrap (on page 1319).</p>
Justify Content	<p>You can choose from these options to align objects along the main axis (left to right):</p> <ul style="list-style-type: none"> • <code>Flex start</code>: Objects are pushed towards the start of the direction (left). • <code>Flex end</code>: Objects are pushed towards the end of the direction (right). • <code>Center</code>: Objects are pushed towards the center of the direction (horizontal center). • <code>Space between</code>: Objects are evenly spaced on a single line. • <code>Space around</code>: Objects are evenly spaced on a single line, with equal amount of space around them.
Align Items	<p>You can choose from these options to align objects along the cross axis (top to bottom):</p> <ul style="list-style-type: none"> • <code>Flex start</code>: Objects are pushed towards the start of the direction (top). • <code>Flex end</code>: Objects are pushed towards the end of the direction (bottom). • <code>Center</code>: Objects are pushed towards the center of the direction (vertical center).

Field Name	Description
	<ul style="list-style-type: none"> • Baseline: Objects choose a baseline (for example, title of the object) and align accordingly. • Stretch: Objects stretch to fill the card.
Layout Type	<p>Choose from the following card layouts before starting to design your pages:</p> <ul style="list-style-type: none"> • Coordinate: Objects dropped on this layout stay where they are on the page. See Coordinate Card (on page 1321). • Flexbox: Objects dropped on this layout are automatically arranged on a single line.
Flex Grow	Enter a value for the object to grow in size with the flexbox layout. The value determines how much the object will grow in comparison to other objects within the layout.
Flex Shrink	Enter a value for the object to shrink in size with the flexbox layout. The value determines how much the object will shrink in comparison to other objects within the layout.
Flex Basis	This default property is the initial size of the objects within the flexbox layout. You can grow/shrink this size.
Style	<p>Select these check boxes to format the objects:</p> <ul style="list-style-type: none"> • Rounded Corners: Adds a rounded corner instead of a pointed corner. • Custom Colors: Adds color.
Function	<p>Layout functionalities:</p> <ul style="list-style-type: none"> • Card: This is the regular flexbox layout option without any additional functionalities. • Interactive Map: This flexbox layout includes an interactive map functionality. See Interactive Map (on page 1322). • Repeater: This flexbox layout includes a repeater functionality. You can create multiple instances of a plug-in dropped in a repeater layout. Refer to Repeater (on page 1324) layout properties.
Show/Hide	Select +Add Conditions to create conditions to show or hide the card.

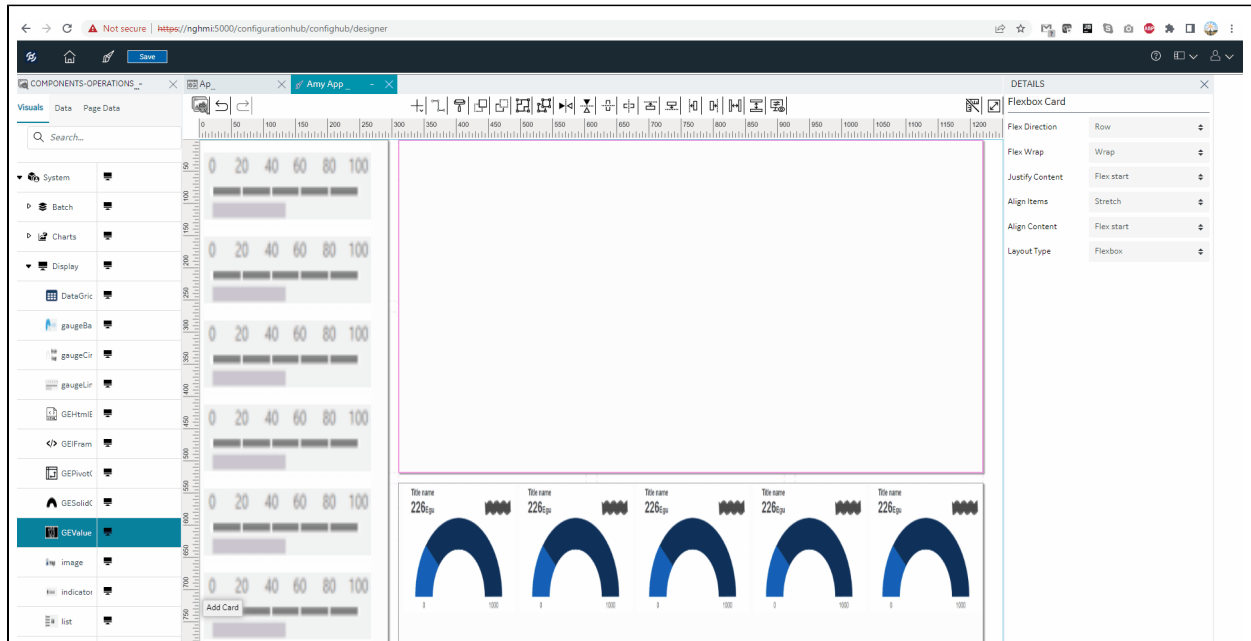
Flex Row



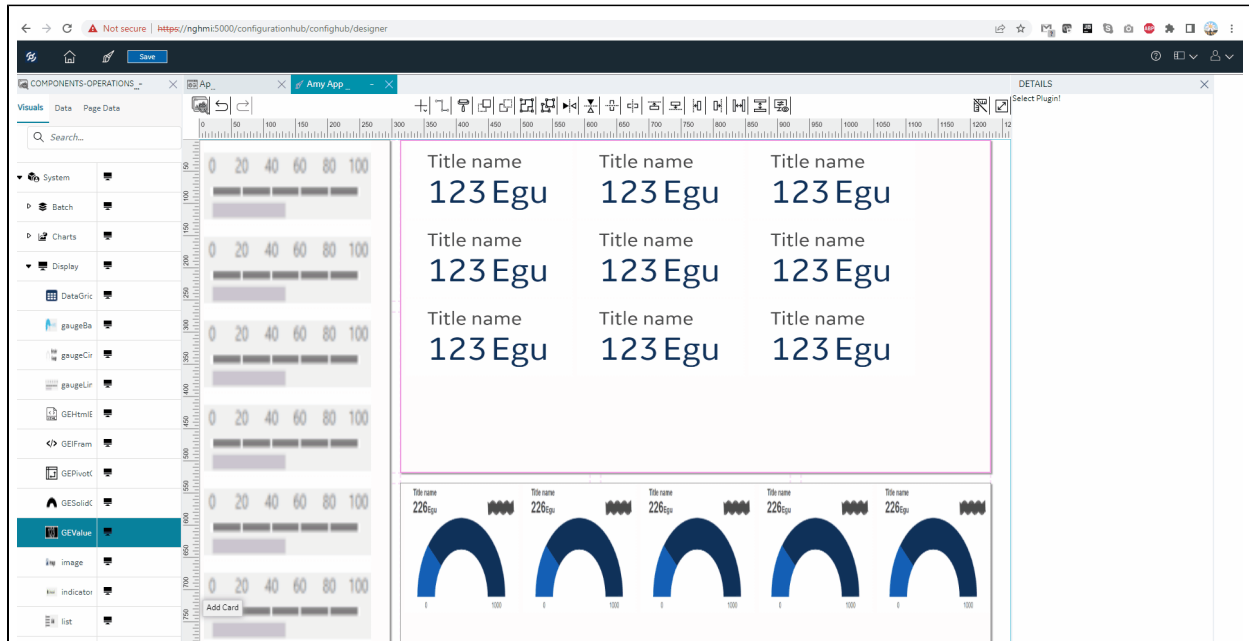
Flex Row and Column



Flex Wrap



Resizing the Flexbox Layout



Coordinate Card

This layout offers an absolute layout design structure.

This is the default card layout when you start to design application pages. You can drag and drop plug-in objects to an absolute position on the card. The end application reflects the same as in the coordinate card page design.

Field Name	Description
Columns	The card occupies the specified number of columns on the page grid (on page 1312) .
Rows	The card occupies the specified number of rows on the page grid (on page 1312) .
Position X	Applies to the horizontal placement of the card on the page. When the value is 0, the card is placed on the left-most side of the page. As you increase the value, the card moves away from the left side of the page.
Position Y	Applies to the vertical placement of the card on the page. When the value is 0, the card is placed at the top of the page. As you increase the value, the card moves away from the top of the page.
Layout Type	Choose from the following card layouts before starting to design your pages: <ul style="list-style-type: none"> • Coordinate: Objects dropped on this layout stay where they are on the page. • Flexbox: Objects dropped on this layout are automatically arranged on a single line. See Flexbox Card (on page 1314).
Style	Select these check boxes to format the objects: <ul style="list-style-type: none"> • Rounded Corners: Adds a rounded corner instead of a pointed corner. • Custom Colors: Adds color.
Function	Layout functionalities: <ul style="list-style-type: none"> • Card: This is the regular flexbox layout option without any additional functionalities. • Interactive Map: This flexbox layout includes an interactive map functionality. See Interactive Map (on page 1322).

Field Name	Description
scale Line Connector	Scale Line Connectors checkbox option: - We need to set 'Scale Line' connector option at card level and with this setting the line connector will work similar to %. All the other plugins that are connected using line connector needs to be in % when user is expecting to scale based on browser page dynamic height and width changes.
Show/Hide	Select +Add Conditions to create conditions to show or hide the card.

Scroll bars will display for the card when card size is smaller than the plugin size.

Value display: - In new designer, Height & width will consider from widget properties not from the plugin manifest/properties (Height & Width).

Breadcrumb: - Breadcrumb combination with any other plugins used in coordinated layout , should follow the higher z-index properties than breadcrumb. (Ex: Set the Breadcrumb z-index '0' and Alarm Card/Trend card should be z-index '1')

Interactive Map

This topic describes properties for an interactive map layout.

The interactive map functionality is available in both coordinate and flexbox card layout types.

1. Upload an image.
2. Double-click the image areas where you want to create a marker.
3. Select the marker you want to update.
4. On the details panel, select **+Add Marker State**, and update the properties.
5. Similarly update all markers on the image.
6. You can also delete markers on the image.

If you selected an interactive map functionality for your layouts, then configure these details:

Field Name	Description
Map Image	Select Upload Image to browse and select an image. The option to upload an image is also available within the interactive map card layout.
Coordinates	Enter these coordinates to position the image within the card. The value should be less than or equal to 99.

Field Name	Description
	<ul style="list-style-type: none"> • Top Offset: The margin between the top of the card and top of the image. • Left Side Offset: The margin between the left side of the card and left side of the image. <p>You can also set the coordinates by moving the image on the layout. The values in the text box are adjusted based on the set position.</p>
Marker Type	<p>You can select one of the following options:</p> <ul style="list-style-type: none"> • Shape • Image
Color	If you selected Shape as the marker type, specify a fill color.
Shape	<p>If you selected Shape as the marker type, select one of the following options:</p> <ul style="list-style-type: none"> • Round • Square
Marker Image	<p>If you selected Image as the marker type, upload an image for the marker.</p> <p>For example, if the marker identifies the position of a radiator fan, you can upload the image of a fan instead of using a predefined round or square shape for the marker.</p>
Size	<p>Enter the size to multiply the default size of the marker shape or image size.</p> <p>For example, if you enter 2, the marker size is double the default size. By default, the value in this field is 1. The marker size can have a value greater than or equal to 100.</p>
Label	If you want a label to appear for the marker, then enter the label name.
Label Color	Choose a color for the label text.
Data Label	<p>You can choose to pass the data to the interactive map using a query, global, formula, or enter the value manually.</p> <p>For example, suppose the interactive map plots the temperature of various components of a car. For a marker that identifies the position of a radiator fan in a car, you can map the data label with the output of the query that re-</p>

Field Name	Description
	trieves the temperature of the fan. When you access the application, the temperature value retrieved from the query is displayed for the radiator fan.
Number Format	<ul style="list-style-type: none"> • Use Raw Format: Select the check box to display numbers in raw format. For example, a numeric value with 5 or more decimal places is shown as it is, and not rounded off. • Number of decimals: This option appears if you do not want to display numbers in raw format. In that case, enter the decimal places (0-7) to consider after the decimal point to format large numbers. Based on the decimals, the value is rounded off to the nearest whole number.
Data Label Color	Identifies the color and opacity of the data label.
Show/Hide	Select +Add Conditions to create conditions that show or hide the interactive map.
BEHAVIOR	You can set actions to be performed when a marker is selected. <ol style="list-style-type: none"> 1. Select +Add. 2. Select from the list of available actions for the marker.
Delete Marker	Select the marker you want to delete, and select the Delete icon.

Repeater

A repeater layout displays a set of repeating objects.

The repeater functionality is available only in the flexbox card layout.

If you selected a repeater functionality for your [flex layout \(on page 1314\)](#), then configure these details:

Field Name	Description
Repeater Source	Select a query to retrieve data, which is displayed in the repeater.
Multi Select	<p>This property is used in combination with a map or a graph plug-in. Select this check box if you want to insert a check box for multi-selection.</p> <p>In the end application, a check box appears in each row of the repeater, allowing you to select which items should appear on the map or the graph.</p>

Field Name	Description
Checked	<p>This property applies only if you enabled multi-selection check boxes.</p> <p>Select this check box if you want multi-selection check boxes selected by default.</p> <p>When you open the end application, the check box that appears in each row of the repeater remains selected by default.</p>
Load	Select this check box if you want to add rows that appear by default in the repeater.
Page Size	Enter the number of rows that should appear by default in the repeater.
Paging Style	<p>Choose from these options:</p> <ul style="list-style-type: none"> • Paging: Each page in the repeater will contain the number of rows that you specify. You can navigate to the other pages to access the rest of the rows. • Load More: The repeater will initially contain the number of rows that you specify. A Load more button appears in the application, which allows you to retrieve additional rows in the same page.

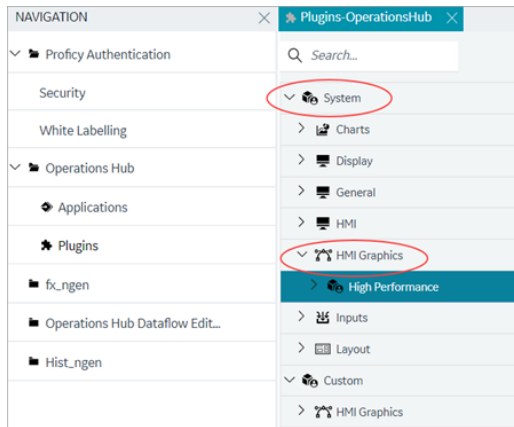
HMI Graphics

About HMI Graphics

HMI graphics are accessible only in the latest version of Operations Hub layout.

Use the HMI graphic plug-ins to design a pictorial setup of your industrial system. The plug-ins can be animated based on their configured tag data values. Operators can experience a real world layout while monitoring the changing status of the system. The HMI graphics are scalable, and can be resized to fit into your application design.

With the Operations Hub installation, you get a list of [out-of-the-box HMI Graphics \(on page 1298\)](#) (not available in Operations Hub Classic). You can use the system HMI graphics to get started, and create custom graphics for varied applications.



Refer to the following topics to work with HMI graphics.

- [Duplicate Graphic \(on page 1327\)](#)
- [Create New Graphic \(on page 1328\)](#)
- [Rename Graphic \(on page 1329\)](#)
- [Edit Graphic \(on page 1329\)](#)
- [Export Graphic \(on page 1331\)](#)
- [Import Graphic \(on page 1332\)](#)
- [Delete Graphic \(on page 1333\)](#)

Under custom, you can also create varied categories to efficiently organize your HMI graphics.

- [Create Category \(on page 1333\)](#)
- [Rename Category \(on page 1334\)](#)
- [Delete Category \(on page 1334\)](#)

With the in-built SVG graphic editor, you can configure and animate the HMI graphics to meet your specific requirements.

- [Create Data Item \(on page 1335\)](#)
- [Add Datalink Animation \(on page 1336\)](#)
- [Add Color Animation \(on page 1337\)](#)
- [Add Fill Animation \(on page 1338\)](#)
- [Add Visibility Animation \(on page 1340\)](#)
- [Delete Animation \(on page 1341\)](#)

Add/Update Graphics to a Page

When designing application pages in Operations Hub, you can drag-and-drop graphics to the page designer area.

In case you modified animation for a graphic that is already used in an application, then you need to update those graphic instances to render the data accurately. For example, to update an instance of a graphic called `speedometer`, do the following:

1. Open the application page where the `speedometer` is used.
2. Delete the `speedometer`. You have deleted the old instance of the `speedometer`.
3. On the **Visuals** tab under custom graphics, drag-and-drop or double-click the `speedometer` to add it back to the page. You have added the updated instance of the `speedometer`.
4. On the toolbar, select **Save**.

You don't need to update graphic instances if you modified color, size, position, or shape of a graphic.

Duplicate Graphic

This topic describes how to duplicate and create a new HMI graphic.

You cannot create a graphic with duplicate names in the same folder.

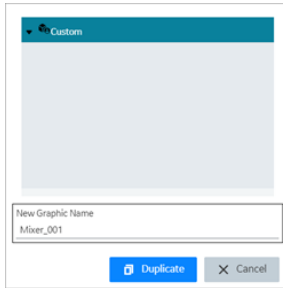
1. You can duplicate all HMI graphics under system and custom.

Go to System > HMI Graphics > High Performance .
Go to Custom > HMI Graphics

A list of HMI graphics appear.

2. Right-click the graphic you want to duplicate, and select **Duplicate Graphic**.
A pop-up screen appears.
3. Do the following:

- a. Select a custom location path to save the new graphic.
- b. Enter a new name for the graphic.
- c. Select **Duplicate**.



You can access the newly created graphic under the custom plug-ins category.

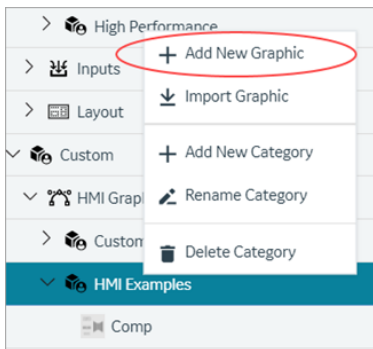
Create New Graphic

This topic describes how to create a new HMI graphic.

Using the SVG editor, you can create new HMI graphics from scratch apart from [duplicating existing graphics \(on page 1327\)](#).

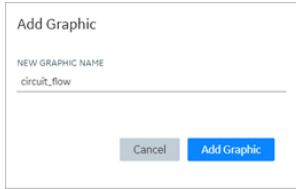
The following steps create a new SVG file. You can open the file in the editor to create interactive elements of an HMI graphic using the basic shapes, lines, etc.

1. Under custom graphics, select the folder category where you want to create and save the new graphic.
2. Right-click the folder and select **Add New Graphic**.



The **Add Graphic** screen appears.

3. Enter a name for the new graphic.
4. Select **Add Graphic**.



A blank SVG file is created with the name.

The newly created file is saved to the selected folder category.

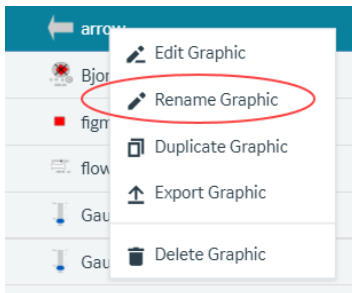
1. Use the [edit option \(on page 1329\)](#) to open the file in the SVG editor.
2. Use the [SVG editor tools \(on page 1342\)](#) to create HMI graphics.

Rename Graphic

This topic describes how to rename a newly created HMI graphic plug-in.

[Duplicate Graphic \(on page 1327\)](#)

1. Under **Custom** plug-ins, right-click the graphic you want to rename.
2. Select **Rename Graphic**.



A confirmation dialog appears.

3. Enter a new name for the graphic.
4. Select **Rename** to save.

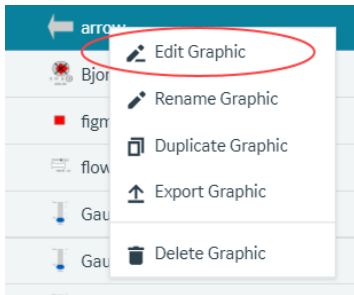
The graphic is updated with a new name.

Edit Graphic

This topic describes how to modify a HMI graphic plug-in.

You can modify custom HMI graphics only.

1. Under **Custom** plug-ins, right-click the graphic you want to modify.
2. Select **Edit Graphic**.



The graphic opens in an SVG editor.

3. On the components panel, access the following tabs to modify the graphic:

<p>Graphic Tree</p>	<p>On this tab, you can view the hierarchy of SVG elements and corresponding animations. You can add or delete animations from this tree only. Refer to the following topics:</p> <ul style="list-style-type: none"> ◦ Add Datalink Animation (on page 1336) ◦ Add Color Animation (on page 1337) ◦ Add Fill Animation (on page 1338) ◦ Add Visibility Animation (on page 1340) ◦ Delete Animation (on page 1341)
<p>Graphics List</p>	<p>On this tab, you can access all the plug-ins listed under the custom category. Refer to the following topics:</p> <ul style="list-style-type: none"> ◦ Create Category (on page 1333) ◦ Rename Category (on page 1334) ◦ Delete Category (on page 1334)

4. Save the changes made to the graphic.



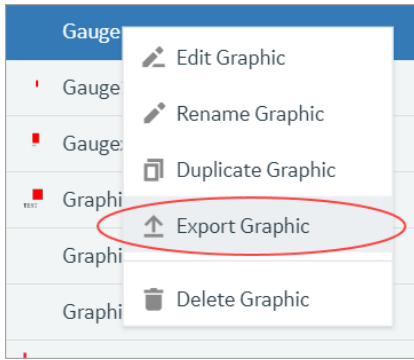
Export Graphic

This topic describes how to export a HMI graphic.

You can export and save graphics to re-use them across different systems. For example, a system integrator builds a valve graphic and implements it for various customers.

To import/export SVGs, refer to [SVG Editor Tools \(on page 1342\)](#).

1. Under **Custom** plug-ins, right-click the graphic you want to export.
2. Select **Export Graphic**.



The export graphic screen appears.

3. Select **Export**.

The file is exported and saved as a JSON file.

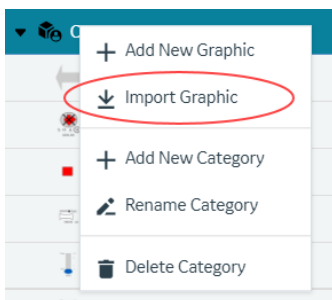
Import Graphic

This topic describes how to import a HMI graphic.

HMI graphics are a combination of SVGs (visual shapes/text, etc.) and animated content stored in a JSON file. This file can be distributed across different Operations Hub systems using the export/import feature. Invalid JSON files will not get imported to Operations Hub.

To import/export SVGs, refer to [SVG Editor Tools \(on page 1342\)](#).

1. Under **Custom** plug-ins, right-click the folder where you want to import a graphic.
2. Select **Import Graphic**.



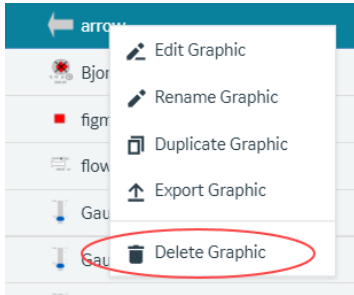
3. Browse the system and locate the JSON file you want to import.
4. Select **Import**.

The file is imported to the folder.

Delete Graphic

This topic describes how to delete a HMI graphic plug-in.

1. Under **Custom** plug-ins, right-click the graphic you want to delete.
2. Select **Delete Graphic**.



A confirm dialog appears.

3. Select **Yes**

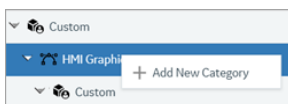
The graphic is deleted from Operations Hub.

Create Category

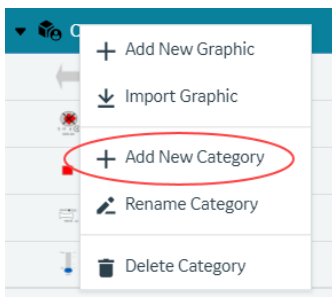
This topic describes how to create folders and sub-folders to categorize custom graphics.

You can also create categories on the components panel while [editing graphics \(on page 1329\)](#).

1. To create a category for the first time under **Custom**, right-click **HMI Graphics** and select **Add New Category**.



Hereafter, you can create categories at every level. Right-click the folder where you want to create a category and select **Add New Category**.



The **Add Category** screen appears.

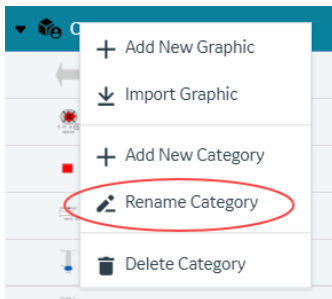
2. Enter a name for the new category.
3. Select **Add Category**.
A folder with the given name is created.

Rename Category

This topic describes how to rename the folder categories.

[Create Category \(on page 1333\)](#)

1. Right-click the folder you want to rename and select **Rename Category**.



- A screen appears with the current folder name.
2. Enter a new name and select **Rename**.
The folder category is saved with the new name.

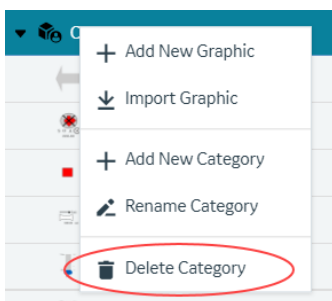
Delete Category

This topic describes how to delete the folder categories.

[Create Category \(on page 1333\)](#)

If you want to delete any custom folder/sub-folder, first delete the graphics within the folder.

1. Right-click the folder you want to delete and select **Delete Category**.



A confirmation screen to confirm the delete action appears.

2. Select **Yes**.

The folder category is deleted.

Create Data Item

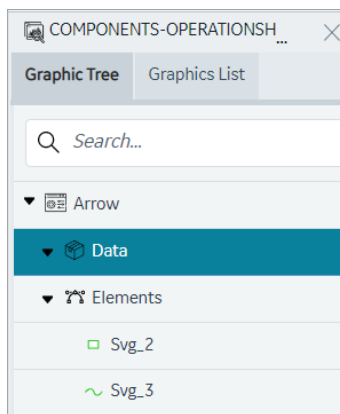
This topic describes how to create data items for SVG graphics.

Data items are used to configure SVG graphic properties. You can create only one data item for each graphic. By default, every graphic has a data item attached to it. You can modify or delete the default data item. In the following steps, you can create a data item in case you deleted the default data item.

1. Open a graphic in the SVG editor.

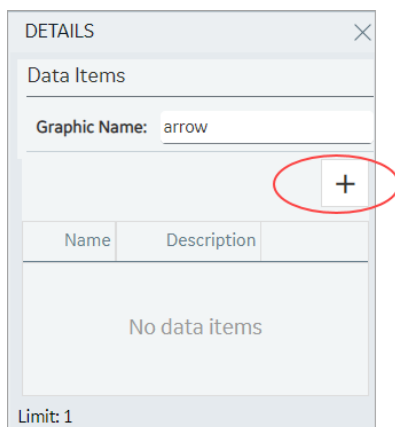
Refer to [Edit Graphic \(on page 1329\)](#).

2. On the components panel > **Graphic Tree** tab, select **Data**.



Data Items appears on the details panel.

3. Select **+** icon.



4. Enter a **Name** and **Description** for the data item.

5. Select **Update**.

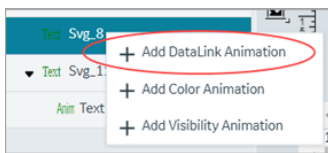
The data item is created with options to modify and delete the item.

Add Datalink Animation

This topic describes how to animate text for SVG graphics.

In SVG, you can create text elements and animate them. You can also use input data to create dynamic and interactive animations by linking data to the animation properties. At runtime, the animation is executed based on the data. For example, change in color of an element based on data values.

1. Right-click the element you want to animate.
2. Select **Add DataLink Animation**.



Adds an entry for text animation under the element.

3. On the Details panel, access the text animation properties for the entry.
4. Enter information in the following fields:

Field Name	Description
Animation Name	Provide a name for reference.
Data Type	Choose from these data types to configure animation properties: <ul style="list-style-type: none"> ◦ Text ◦ Decimal ◦ Integer
Data Item	Select the data item you want to apply to the element. See Create Data Item (on page 1335) .
Attribute	The drop-down list contains several attributes, which can be associated with the data item in order to animate the HMI Graphic. The animation will apply to the selected attribute.
Default Value	Enter a default value for the selected attribute. This default value is used only when the data source is set to Manual in page designer. See Bind Your Data to Plug-ins (on page 1310) .
Zero Fill	Select this check box if you want to fill unused digits with zeroes.

Field Name	Description
	For example, if the graphic can display a maximum of four digits and the current value is 25, it is displayed as "0025" when zero fill is enabled.
Integer Digits	If Zero Fill is enabled, enter the number of digits for display.
Group Digits	Select this check box if you want to group the digits in a graphic display making it easy to read. For example, 123456 can be grouped as "123,456".
Scientific	Select this check box if you want to display numbers in scientific notation. This option is useful for displaying very large numbers in a more compact and readable format.
Decimal Digits	Enter the number of decimal places to display a number. This option helps to avoid displaying unnecessary decimal places or rounding errors.

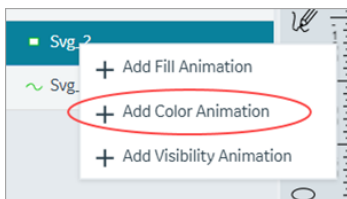
5. On the toolbar, select **Save**.

Add Color Animation

This topic describes how to create color animation for SVG graphics.

You can animate to change the color of the SVG graphic element.

1. Right-click the element you want to animate.
2. Select **Add Color Animation**.



Adds an entry for color animation under the element.

3. On the Details panel, access the color animation properties for the entry.
4. Enter information in the following fields:

Field Name	Description
Animation Name	Provide a name for reference.
Data Item	Select the data item you want to apply to the element. See Create Data Item (on page 1335) .
Attribute	The drop-down list contains several attributes, which can be associated with the data item in order to animate the HMI Graphic. The animation will apply to the selected attribute.
Default Value	Enter a default value for the selected attribute. This default value is used only when the data source is set to Manual in page designer. See Bind Your Data to Plug-ins (on page 1310) .
Color Table	Configure one or more colors to change the color based on a specific value. To configure a color: <ul style="list-style-type: none"> a. Select the + icon. b. Select a logical Operator. For example, < c. Enter a Value. For example, 50 d. Choose a Color. For example, green. e. Select Update. Result: If the value is less than 50, the color remains green. Configured colors appear in a table with options to modify and delete the colors. You can also drag-to-reorder the list of colors in a table.

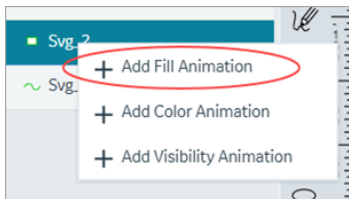
5. On the toolbar, select **Save**.

Add Fill Animation

This topic describes how to create fill animation for SVG graphics.

You can animate the fill color of the SVG graphic element.

1. Right-click the element you want to animate.
2. Select **Add Fill Animation**.



Adds an entry for fill animation under the element.

3. On the Details panel, access the fill animation properties for the entry.
4. Enter information in the following fields:

Need to make distinction between level, min, and max. Each of these three properties have ability to define data item, attribute, and default

Field Name	Description
Animation Name	Provide a name for reference.
Color	Select a color to fill the SVG element. For example, sets the color of the liquid or the substance represented by the SVG tank.
Fill Direction	Select from these directional modes, in which a gauge or pump is filled with data: <ul style="list-style-type: none"> ◦ left-to-right ◦ right-to-left ◦ bottom-to-top ◦ top-to-bottom
Level	The values entered in this section apply to an object's fill-level, such as the progress of a loading bar or the level of a liquid in a container.
Minimum	The values entered in this section apply to minimum values of a range. For example, minimum levels of a gauge.
Maximum	The values entered in this section apply to maximum values of a range. For example, maximum levels of a gauge.
Data Item	Select the data item you want to apply to the element. See Create Data Item (on page 1335) .
Attribute	The drop-down list contains several attributes, which can be associated with the data item in order to animate the HMI Graphic. The animation will apply to the selected attribute.

Field Name	Description
Default Value	Enter a default value for the selected attribute. This default value is used only when the data source is set to Manual in page designer. See Bind Your Data to Plug-ins (on page 1310) .

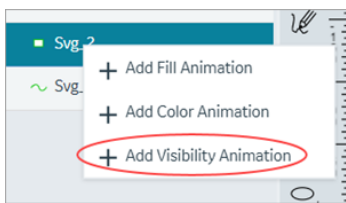
5. On the toolbar, select **Save**.

Add Visibility Animation

This topic describes how to create visibility animation for SVG graphics.

Lets you control the visibility of graphical elements.

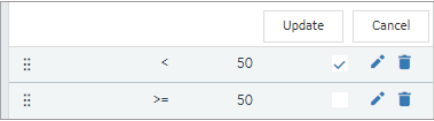
1. Right-click the element you want to animate.
2. Select **Add Visibility Animation**.



Adds an entry for visibility animation under the element.

3. On the Details panel, access the visibility animation properties for the entry.
4. Enter information in the following fields:

Field Name	Description
Animation Name	Provide a name for reference.
Data Item	Select the data item you want to apply to the element. See Create Data Item (on page 1335) .
Attribute	The drop-down list contains several attributes, which can be associated with the data item in order to animate the HMI Graphic. The animation will apply to the selected attribute.
Default Value	Enter a default value for the selected attribute. This default value is used only when the data source is set to Manual in page designer. See Bind Your Data to Plug-ins (on page 1310) .

Field Name	Description
Visibility Table	<p>Configure one or more values to animate the visibility status of the element.</p> <p>To configure visibility status:</p> <ol style="list-style-type: none"> Select the + icon. Select a logical Operator. For example, < Enter a Value. For example, 50 Select the check box for Visible. Select Update. <p>Similarly, add another value to the table that is >= 50 with visible check box cleared.</p>  <p>Result: The element is visible only when the value is less than 50. If the value is greater than or equal to 50, the element is hidden.</p> <p>The visibility configuration values appear in a table with options to modify and delete them. You can also drag-to-reorder the visibility list.</p>

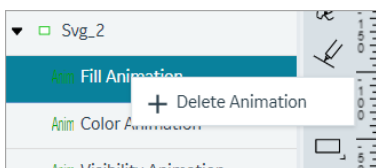
5. On the toolbar, select **Save**.

Delete Animation

This topic describes how to delete animation for SVG graphics.

You can delete text, color, fill, and visibility animation.

1. Right-click the animation you want to delete.
2. Select **Delete Animation**.



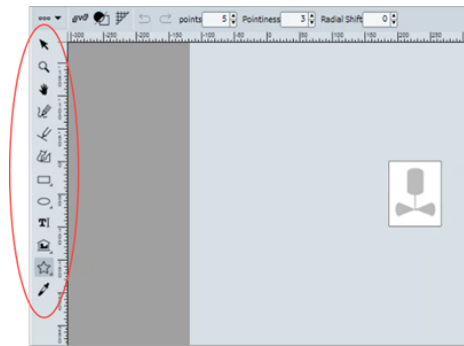
The animation is deleted.

SVG Editor Tools

This topic describes SVG editor tools.

You can modify SVG files using the SVG editor's user-friendly interface.

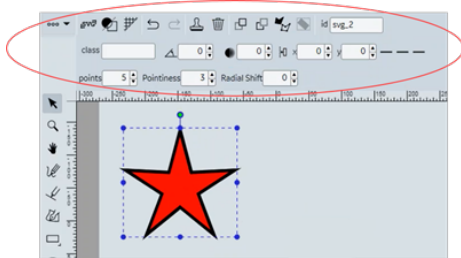
Side Toolbar Options



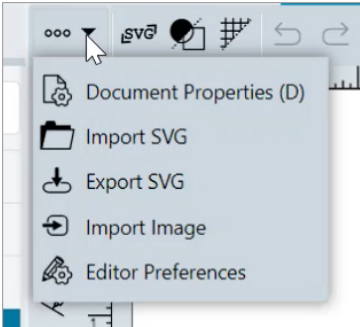
Tool	Description
Select Tool	Allows you to select and move objects within the editing area.
Zoom Tool	Zoom in/out to view objects at different levels of detail. It helps to perform precise edits and adjustments.
Panning	Helps to pan around when used along with the zoom tool.
Pencil Tool	Use this tool to create any shape or design. You can draw and create custom shapes by dragging the mouse.
Line Tool	To create a perfectly vertical or horizontal straight line, hold down the Shift key while drawing the line.
Path Tool	Use the tool to draw a path creating additional points along the way. A path has a start point, end point, and curve parameters of the path. To create the shape you want, mouse-click and drag. To end the path, double-click.
Square/Rectangle Tool	Create squares or rectangles of different sizes. Useful for creating basic geometric shapes. Hold down the Shift key while drawing to create a perfect shape.
Ellipse/Circle Tool	Create ellipses or circles of different sizes.
Text Tool	Allows you to add and edit text within the editing area. Useful for adding labels, annotations, etc.

Tool	Description
Shape library	Contains ready-to-use shapes such as geometric shapes, mathematical shapes, flowchart shapes, etc.
Polygon/Star Tool	<p>The polygon tool allows you to create polygon shapes.</p> <p>The star tool allows you to create star shapes. You can resize these shapes without losing their sharpness and quality.</p>
Eye Dropper Tool	Use the tool to pick a color from an existing object. You can now use the picked color for other elements as well.

Top Toolbar Options



The options in the top toolbar may vary based on the selected objects.

Tool	Description
Document Properties	<p>In the document properties dialog, you can modify the SVG document settings.</p> 
Import SVG	Allows to select and import an SVG file containing shapes, text, and/or images to Operations Hub and add interactive animation using our SVG editor.

Tool	Description
	<p>This option allows you to use SVG files created using third party tools, such as Microsoft Powerpoint, Adobe Illustrator, Inkscape, Figma, etc. These are fixed SVG images and do not contain any animation. Such SVGs when imported may get slightly altered to match our SVG format. For example, <code>tspan</code> elements are converted to <code><text></code> elements.</p> <p>You can also modify third party SVGs by editing its source code.</p>
Export SVG	Allows to export the SVG file and save as HMI graphic.
Import Image	Allows to import an image file. For example, PNG, JPEG, etc.
Editor Preferences	In the editor preferences dialog, you can modify the SVG background, units of measurement, and grid settings.
Edit Source	Opens a code editor, wherein you can make changes to the source code and save it.
Wireframe Mode	When you switch to the wireframe mode, visual distractions such as color, texture, and other design elements are removed. This helps to focus on the layout, positioning, and hierarchy of elements, and make adjustments as necessary. Once the basic structure is in place, you can switch back to the normal mode, and continue working on other design elements.
Show/Hide Grid	Shows/hides the grid layout.
Undo and Redo	These buttons allow you to undo or redo changes you've made to the canvas.
Duplicate Element	Duplicates the selected element.
Delete Element	Deletes the selected element.
Bring to Front	When objects overlap on the page, brings the selected object to the front.
Send to Back	When objects overlap on the page, sends the selected object to the back.
Convert to Path	You can convert an object to a path. This option is used along with the path editing tools to turn a simple shape/text into a complex vector shape. Consider these points when using the tool:

Tool	Description
	<ul style="list-style-type: none"> • Once you convert an object to a path, you cannot easily convert it back to its original form. • Converting an object to a path can make the file size larger.
Reorient Path	Allows you to change the orientation or direction of a path for the selected object, either clockwise or counterclockwise. It is useful when you want to change the starting point or direction of a path without having to redraw it.
Identify the element	When using multiple objects in SVG, this option identifies the selected object within the editing area.
Element class	You can use defined classes to apply styles or behaviors to various elements in SVG file.
Change rotation angle	Rotates the selected object to the selected degrees.
Change gaussian blur value	Increases the blur effect on the object based on the increasing value.
Align	Use the alignment options to position objects within the editing area. Select one or more objects you want to align, and then choose the appropriate alignment option.
Change X/Y coordinate	<p>Enter the X and Y coordinates of an object to move it to a new position within the editing area.</p> <ul style="list-style-type: none"> • X coordinate represents the horizontal position of the object. • Y coordinate represents the vertical position of the object.
Link Control Points	Applies to curved paths. You can link the control points to create complex curves and adjust the shape of a path.
Change node's X/Y coordinate	Applies to nodes in a path. Nodes are the points that define the shape of a path. This option allows you to select a node and set its X and Y coordinates within the path.
Clone Node	Clones the selected node.
Delete Node	Deletes the selected node.
Text formatting tools	Select the text element to access tools to perform the following functions:

Tool	Description
	<ul style="list-style-type: none"> • Choose from a variety of fonts available in the editor. • Adjust the size of your text to make it larger or smaller. • Change the style of your text to bold, italic, underlined, etc. • Align your text. • Adjust the spacing between letters and lines.

Bottom Toolbar Options



Tool	Description
Change zoom Level	Allows you to zoom in and out of the editing area for more precise editing. Use the preset options to apply the zoom level.
Change fill Color	To change the fill color, select the shape/object and from the color palette, choose a color to fill the shape/object.
Change stroke Color	To change the stroke color, select the shape/object and from the color palette, choose a color to apply to the shape/object.
Change stroke width by 1, shift-click to change by 0.1	Allows to change the width of the stroke.
Change stroke dash style	Select the line/shape to change its stroke dash style and apply a new style (dots, dashes, etc.) from the available preset options.
Linejoin	<p>You can set any of these linejoin options to set the corners of a shape/line:</p> <ul style="list-style-type: none"> • Miter: At the meeting point of two lines, applies a pointed corner. • Round: At the meeting point of two lines, applies a rounded corner. • Bevel: At the meeting point of two lines, applies a flat and beveled corner.
Linecap	You can set any of these linecap options to set the ends of a line:

Tool	Description
	<ul style="list-style-type: none">• Butt: Applies a flat end to the line that is perpendicular to the direction of the line.• Square: Applies a flat end to the line that is slightly wider than the line itself.• Round: Applies a rounded end to the line.
Change selected item opacity	Select the item (shape, line, group of objects, or any other element in your SVG file) for which you want to modify the opacity. Set the opacity percentage for the item.
Click to change fill color, shift-click to change stroke color	Allows to change the color.

Chapter 6. Webpace

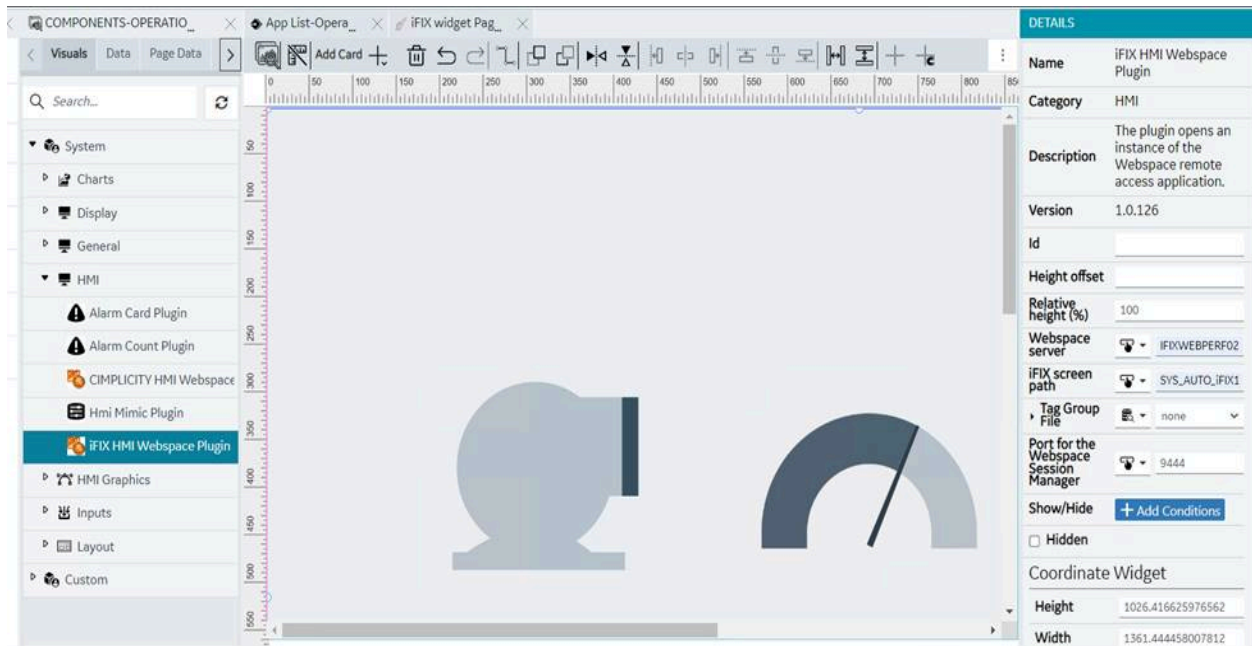
Overview of Webpace with Configuration Hub

This topic provides an overview of Webpace within Configuration Hub. For more details on the Webpace Admin app configuration that can be done on the Webpace Server, refer to the [Webpace documentation](#).

Overview

Use the Webpace widget along with other Operations Hub widgets for better consolidation and visualization of data.

The iFIX HMI Webpace Plugin is available in Configuration Hub from the **Operations Hub > Applications > HMI** page. To add an iFIX HMI Webpace Plugin widget, drag-and-drop the widget to a container application and configure its properties.



Limitations

Be aware of the following limitations when using the iFIX HMI Webpace Plugin with Operations Hub and Configuration Hub:

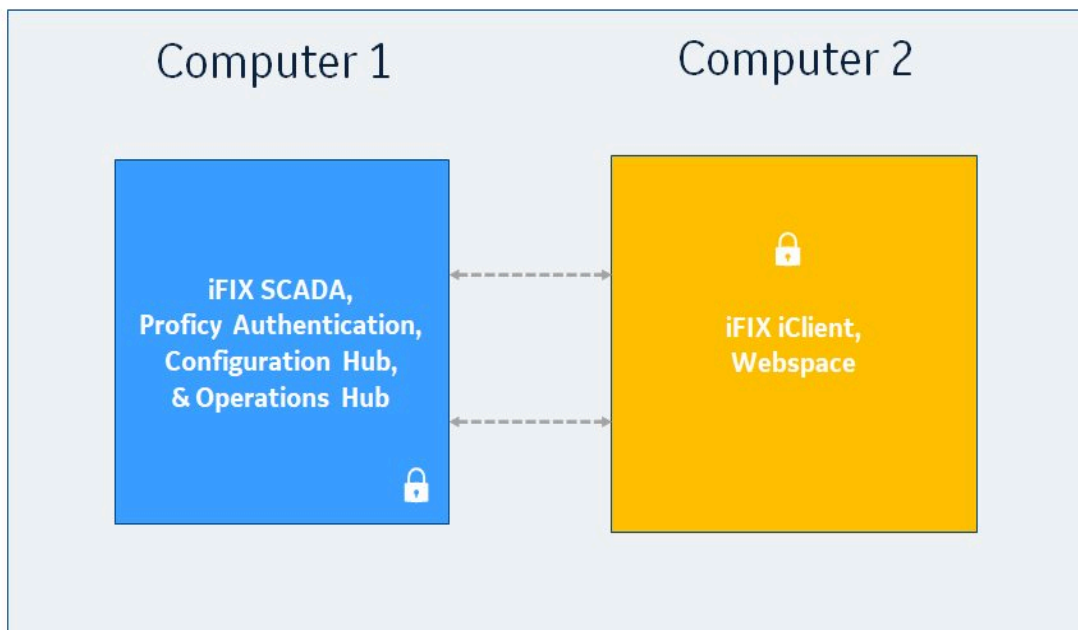
- The Webspaces Server should not be installed on a Failover pair, or on the Operations Hub server or Configuration Hub server.
- Webspaces sessions require credentials for logging into the windows server Webspaces is running on.
- When Webspaces sessions are started, the iFIX Default Project Node Name get updated with the last run iFIX Project Node Name/SCU file. Since you cannot update or start an iFIX with a specific Node Name from Configuration Hub, you should manually start iFIX in this instance. To start iFIX with correct Node Name manually, use the iFIX Startup screen (and not Configuration Hub).

Sample Webspaces Deployment Architecture

The following figure shows a sample deployment architecture for Configuration Hub with Webspaces. It is recommended that the Webspaces server is not located on the same machine as the Configuration Hub or Operations Hub server.

The following figure shows an example of a simple two node scenario with Webspaces and Configuration Hub.

Simple Example: Configuration Hub with Webspaces

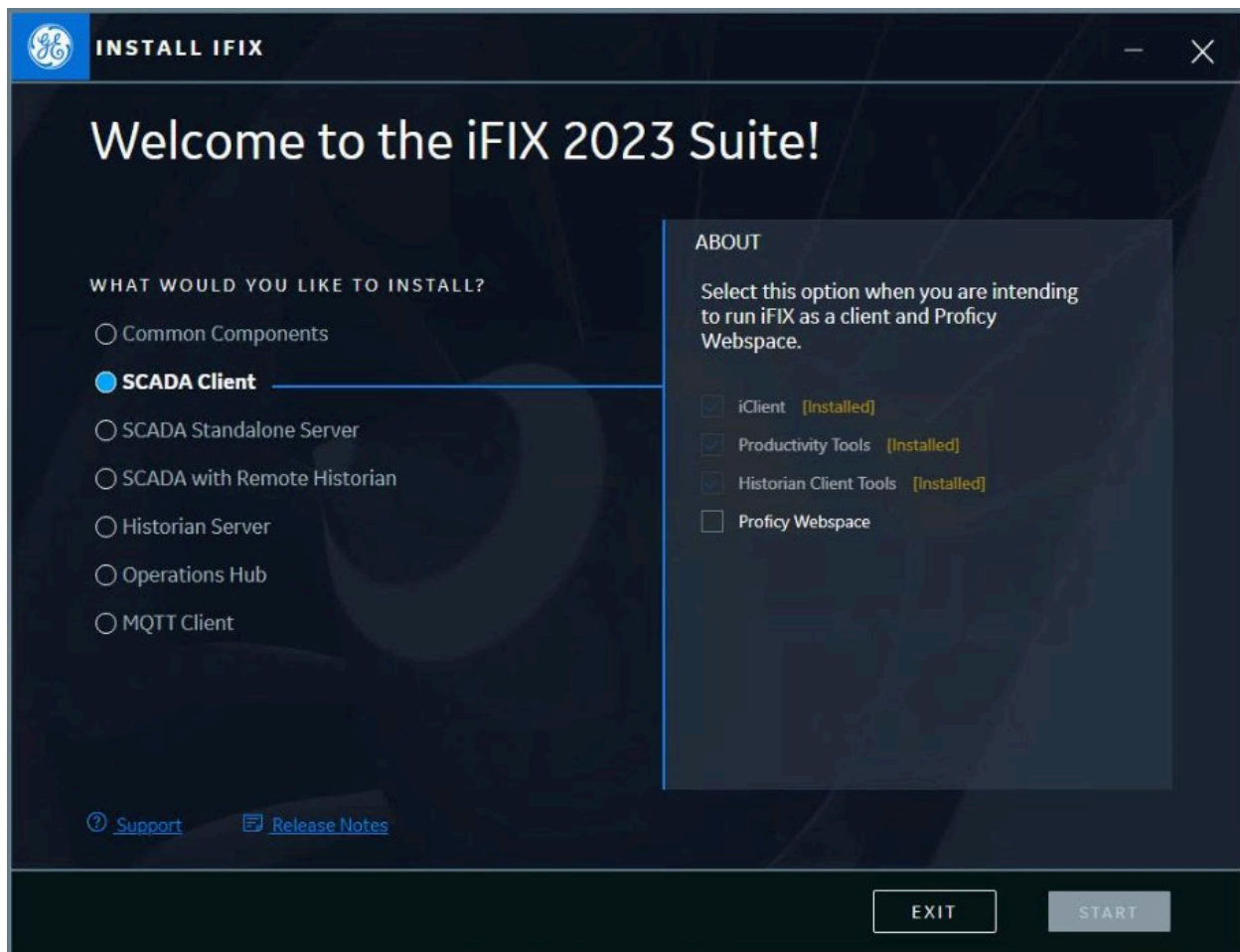


How to Install a Webspaces Server

Use the SCADA Client install option on the Integrated Installer to install Webspaces. The option to install Webspaces can be found on the SCADA Client install option, as shown in the following figure.

**Note:**

After you install Webspaces, you need to register iFIX with Configuration Hub using the registration tool. For steps, see [Registration with Configuration Hub for Webspaces \(on page 1355\)](#).



1. From the SCADA Client, select **Proficy Webspaces** to install the Webspaces Server.
2. Click **Start**. The License Screen appears.
3. Select **Accept** to continue the install and accept the terms and conditions. Next the Install Location screen appears.
4. Leave the default path and port and click **Next**. The Start Install screen appears.

5. Click **Install**. After the Install completes, a message appears.
6. Click **Close** to exit the installer.
7. Export the Webspaces certificate and then import it on to the Configuration Hub server. For steps, refer to these topics: [Exporting the Root Certificate for Webspaces Setup \(on page 1351\)](#) and [Importing the Certificate for Webspaces Setup \(on page 1353\)](#).
8. Register Webspaces with your existing Configuration Hub. For steps, refer to this topic: [Registration with Configuration Hub for Webspaces \(on page 1355\)](#).

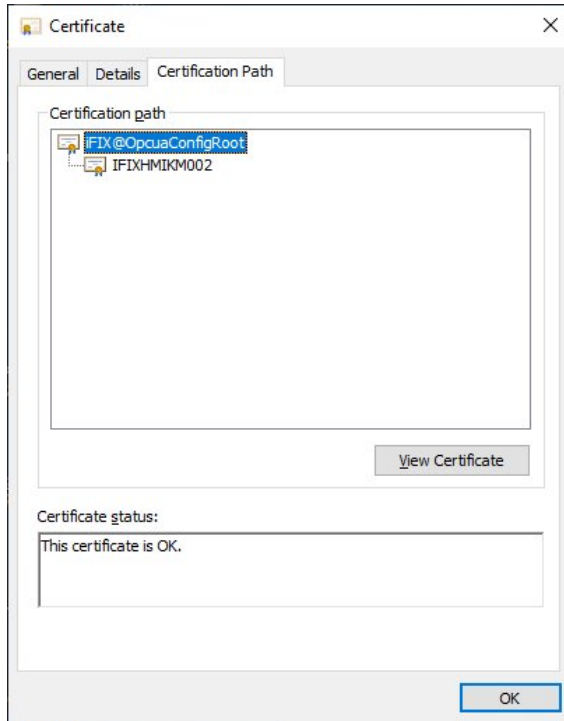
This video provides an overview of the install steps above:

[video/webspaces.mp4](#)

Exporting the Root Certificate for Webspaces Setup

Use the following steps to export a root certificate from the Webspaces server, so that you can install the certificate on the Configuration Hub Server machine.

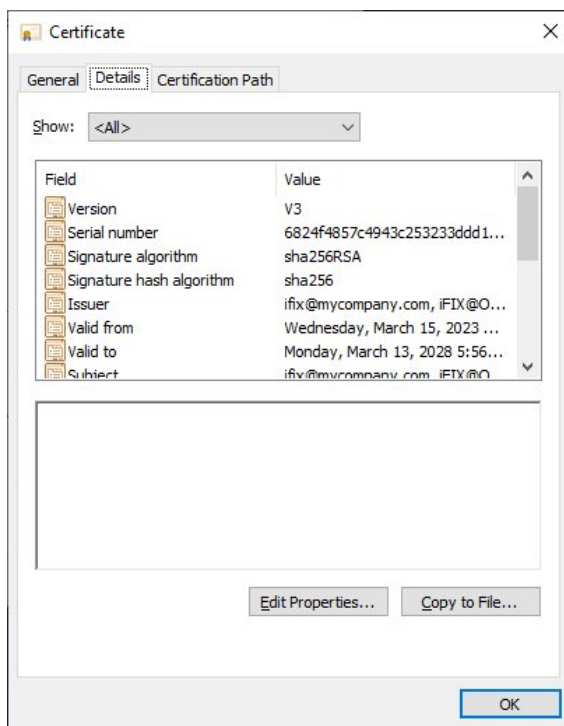
1. On the Webspaces server, navigate to the `C:\Program Files (x86)\Proficy\iFIX\web\conf` folder.
2. Double-click the `iFIX_OpcuaConfigServer.crt` file.
The Certificate Details dialog box appears.
3. Select the **Certificate Path** tab.



4. In the Certificate Path box, select iFIX@OpcuaConfigRoot (if it is not already selected) and then click the **View Certificate** button.

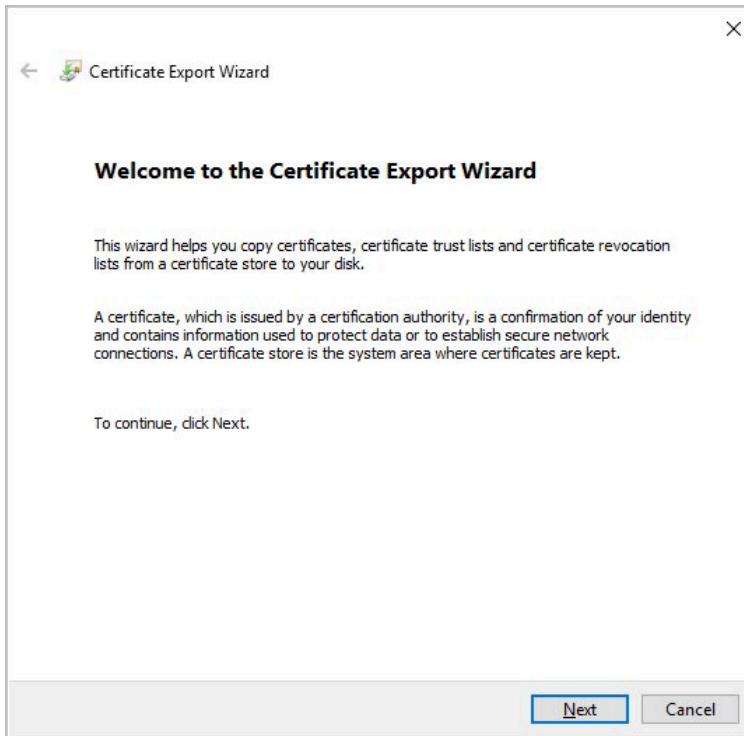
The Certificate Information dialog box appears.

5. Select the **Details** tab, as shown in the following figure.



6. Click **Copy to File**.

The Certificate Export wizard appears, as shown in the following figure.



7. Click **Next**.

The first screen of the wizard appears.

8. Leave the default of **No, do not export the private key**, and then click **Next**.

9. On the Export File format, select **DER encoded binary X.509 (.CER)**, and click **Next**.

10. On the File to Export screen, browse to the location where you want to save the file, and enter a name.

11. Click **Finish**.

The Certificate is generated in the specified folder.

12. Next, copy the root certificate from the output folder to the Configuration Hub machine so that [you can install it. \(on page 1353\)](#)

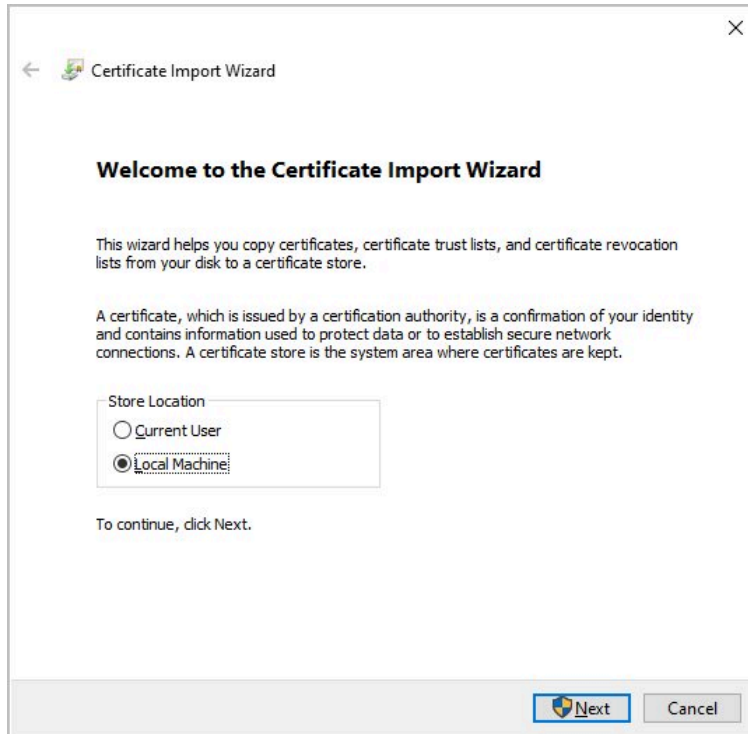
Importing the Certificate for Webspaces Setup

Use the following steps to install a root certificate from the Webspaces server, so that you can install the certificate on the Configuration Hub Server machine.

1. Take the certificate that you exported from the [Webspaces server \(on page 1351\)](#) and copy it to your [Configuration Hub server machine. \(on page 1349\)](#)

2. Double-click the certificate file to install it.

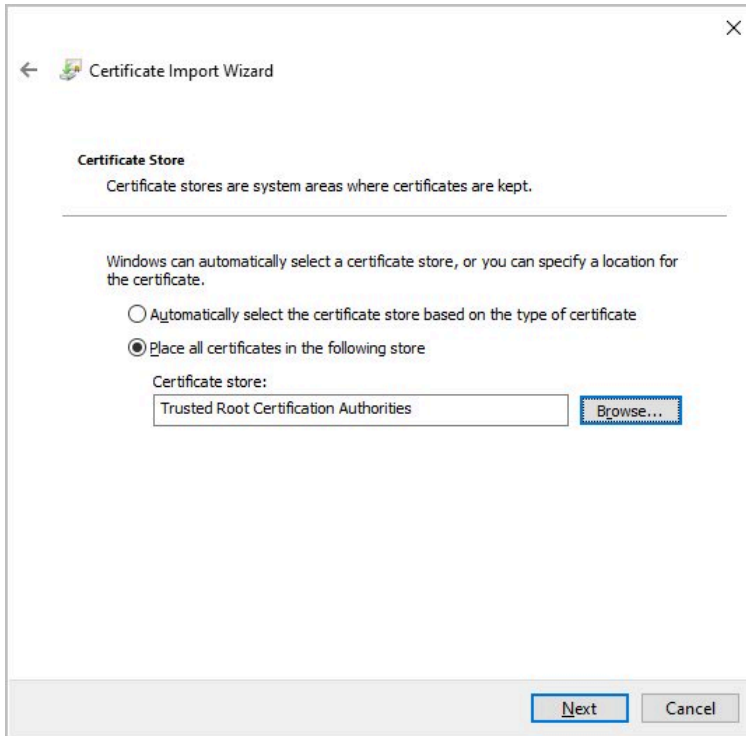
The Certificate Import Wizard appears.



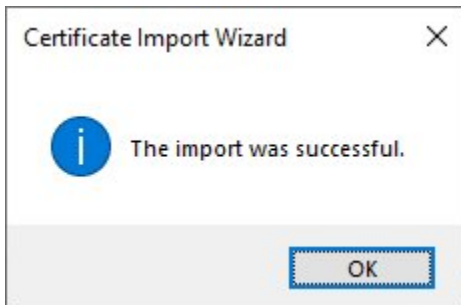
3. Select the **Local Machine** option and click **Next**.

The Import File screen appears in the wizard with your certificate selected.

4. Confirm that the folder and file name are correct, and click **Next**.
5. On the Private Key Protection screen, enter the password and click **Next**.
6. On the Certificate Store screen, select the **Place All Certificates in the following store** option, and click **Browse**.
7. Select the **Trusted Root Certification Authorities** option, and click **OK**.



8. Click **Next**, and then click **Finish** to import the certificates.



A message appears that "The import was successful" when the certificate installs correctly.

Registration with Configuration Hub for Webspaces

After you install Webspaces, you must launch the iFIX registration page to register it with the existing Configuration Hub server. Use these steps to register iFIX with Configuration Hub after Webspaces is installed.

1. On the machine where Webspaces/iFIX is installed, launch the registration tool, and trust and register the certificate:

- a. On the desktop, click the **Register iFIX plugin** icon on the desktop (as shown in the following figure). Or, from the iFIX Workspace, on the Applications tab, in the Configuration Hub area, click **Register** to open the login screen.



- b. Enter the iFIX user name and password, and click **Login**. On successful login, the Configuration Hub Server Registration page appears.
- c. For both Configuration Hub and Proficy Authentication, test the connection by clicking the **Test Server Connection** button. (Enter the server's name and port number if required. If on a domain, use the fully qualified domain name.) Confirm that you can connect to both servers, by clicking the **Test Server Connection** button for both servers.

Configuration Hub Server Registration

Configuration Hub

SERVER NAME 


SERVER PORT

Create User Friendly Plug-in Name

PLUG-IN ALIAS NAME

Configuration Hub Administration Credentials

CLIENT ID

CLIENT SECRET 

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

Proficy Authentication


SERVER NAME 

SERVER PORT

Proficy Authentication Credentials

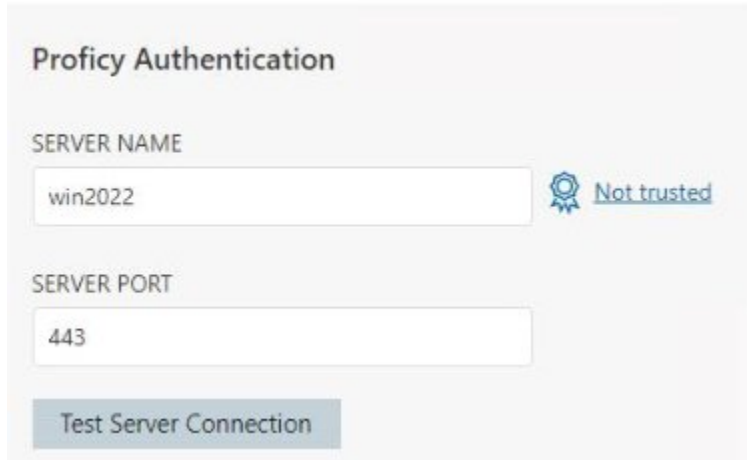
Use Configuration Hub Authentication Credentials for Proficy Authentication.

CLIENT ID

CLIENT SECRET 

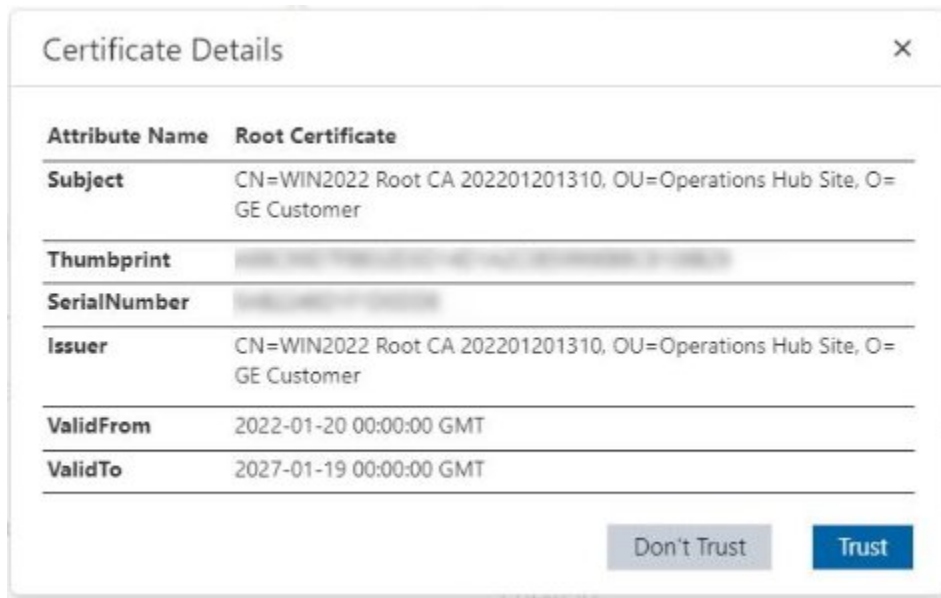
NOTE: These credentials are used to register iFIX plug-in with Proficy Authentication.

If the server certificate shows as **Not Trusted** (in blue next to the server's name), click the Not Trusted link next to the server name to establish the trust. Here is an example of what the Not Trusted link looks like next to the Proficy Authentication Server Name field:



The screenshot shows a configuration form for Proficy Authentication. The title is "Proficy Authentication". There are two input fields: "SERVER NAME" containing "win2022" and "SERVER PORT" containing "443". To the right of the "SERVER NAME" field is a blue icon of a ribbon with a checkmark and the text "Not trusted". Below the fields is a button labeled "Test Server Connection".

After clicking Not Trusted, the Certificate Details window appears. From the Certificate Details window, click **Trust** to trust the certificate.



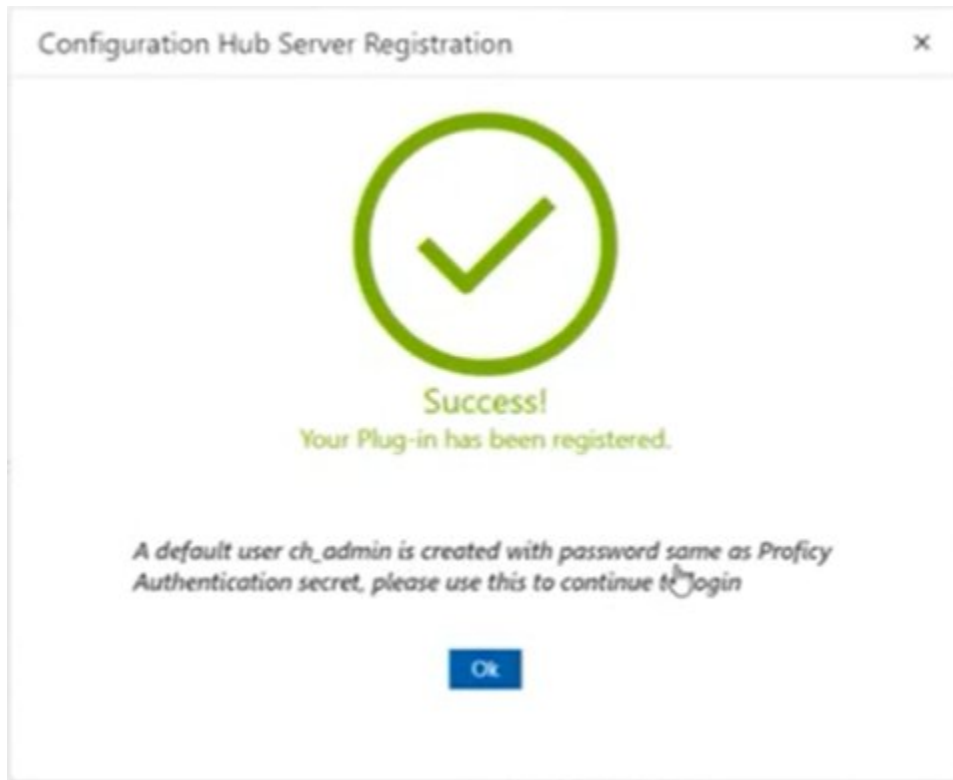
The screenshot shows a "Certificate Details" dialog box with a close button (X) in the top right corner. The dialog contains the following information:

Attribute Name	Root Certificate
Subject	CN=WIN2022 Root CA 202201201310, OU=Operations Hub Site, O=GE Customer
Thumbprint	[REDACTED]
SerialNumber	[REDACTED]
Issuer	CN=WIN2022 Root CA 202201201310, OU=Operations Hub Site, O=GE Customer
ValidFrom	2022-01-20 00:00:00 GMT
ValidTo	2027-01-19 00:00:00 GMT

At the bottom right of the dialog are two buttons: "Don't Trust" (disabled) and "Trust" (active).

Both Configuration Hub and Proficy Authentication must have Trusted certificates before proceeding to register.

- d. To complete the registration for Configuration Hub and Proficy Authentication, for both servers, supply the client IDs and client secrets entered during the common component install, and then click **Register**. When registration is complete, the following screen appears.

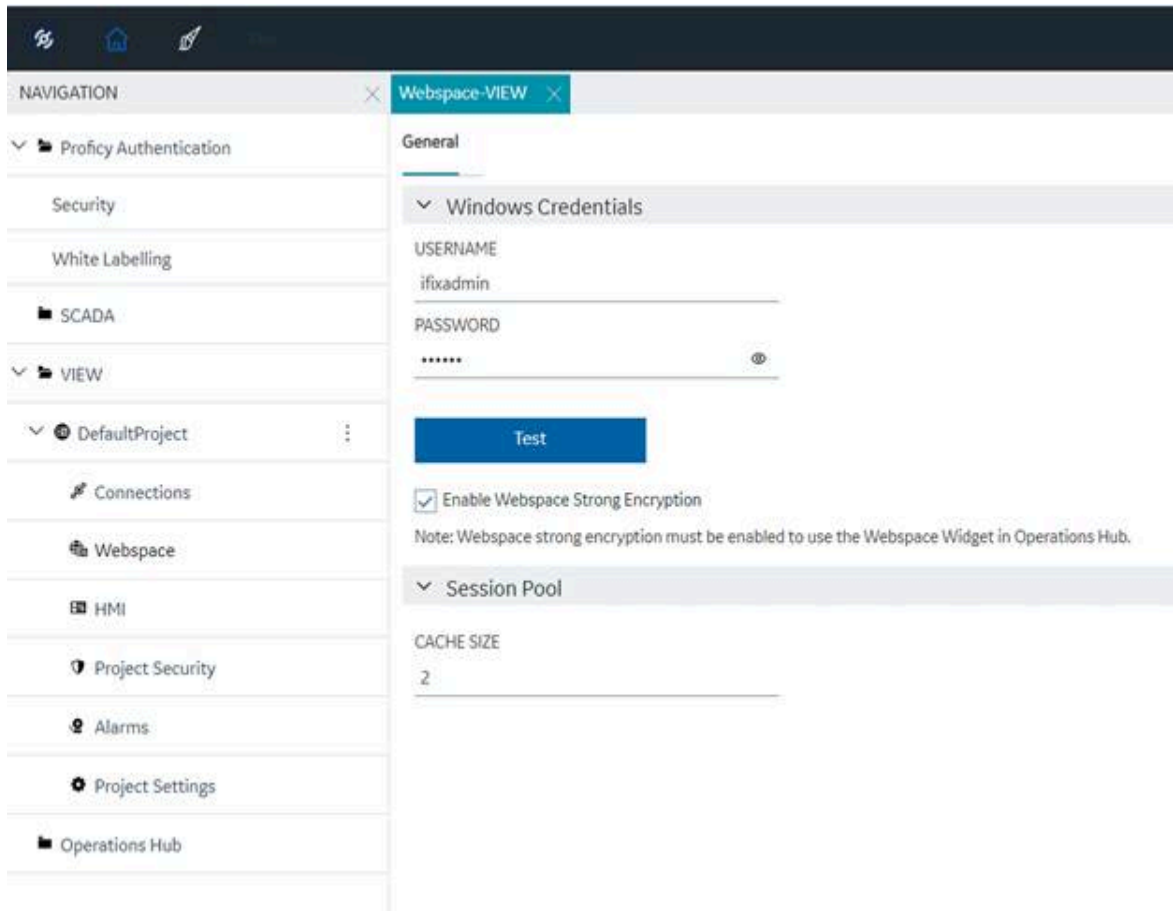


2. Next, on the Webspaces server machine, launch the Registration tool and repeat the previous steps. Trust and register the certificate using the Configuration Hub and Proficy Authentication Server names specified in step 1, from the location of when you installed the product.

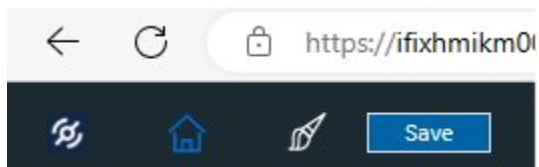
Webspaces Settings in Configuration Hub

Use these steps to setup Webspaces in Configuration Hub after you installed the certificate from the Webspaces Server and registered your Configuration Hub and Proficy Authentication Servers.

1. Click the Configuration Hub icon on the desktop to login to Configuration Hub.
2. Enter a valid user name and password (that you entered when you installed Configuration Hub), and click **Sign-in**.
3. Navigate to Webspaces panel, as shown in the following figure. In the navigation tree, locate the Webspaces Server machine on the View node.



4. Enter the valid Windows credentials for the user name and password.
5. Select the **Enable Webspaces Strong Encryption** option.
6. Click **Test** to confirm that you can connect to the Webspaces Server.
7. In the Session Pool area, leave the default Cache Size.
8. Click **Save**.

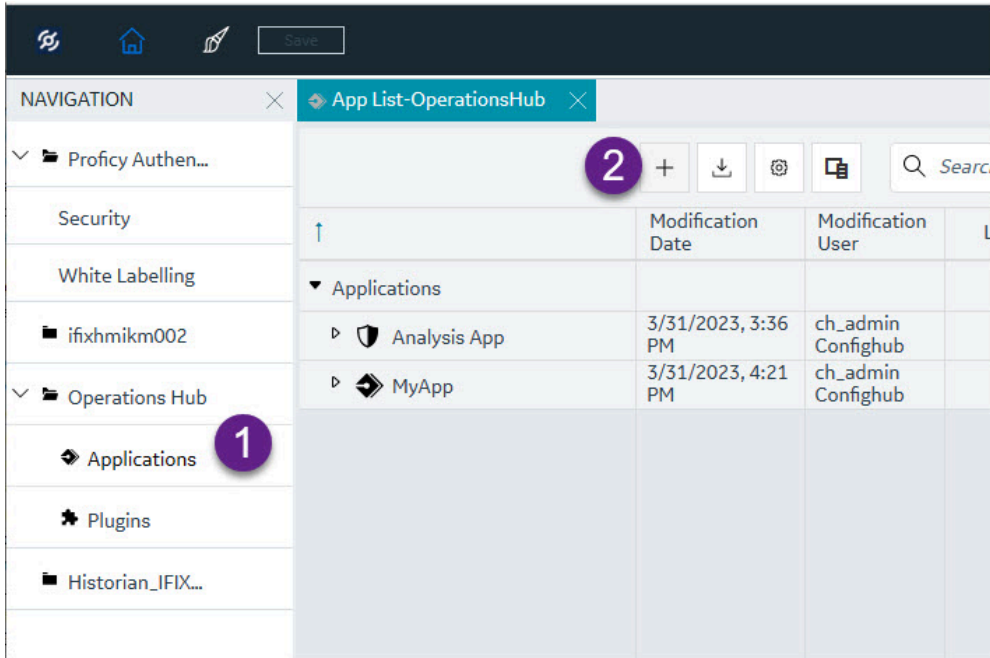


iFIX Webspaces Plugin in Operations Hub

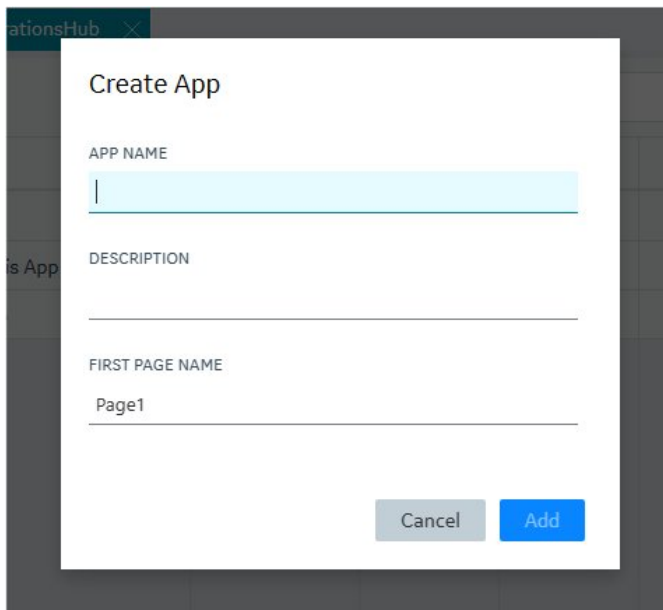
Use the following steps from Configuration Hub to add the iFIX Webspaces to an Operations Hub application.

Create a New Application with the Webpace plugin

1. In Configuration Hub, from the Navigation pane, browse to Operations Hub and then Applications.
2. Next, click the + icon to add application, as shown in step 2 below.




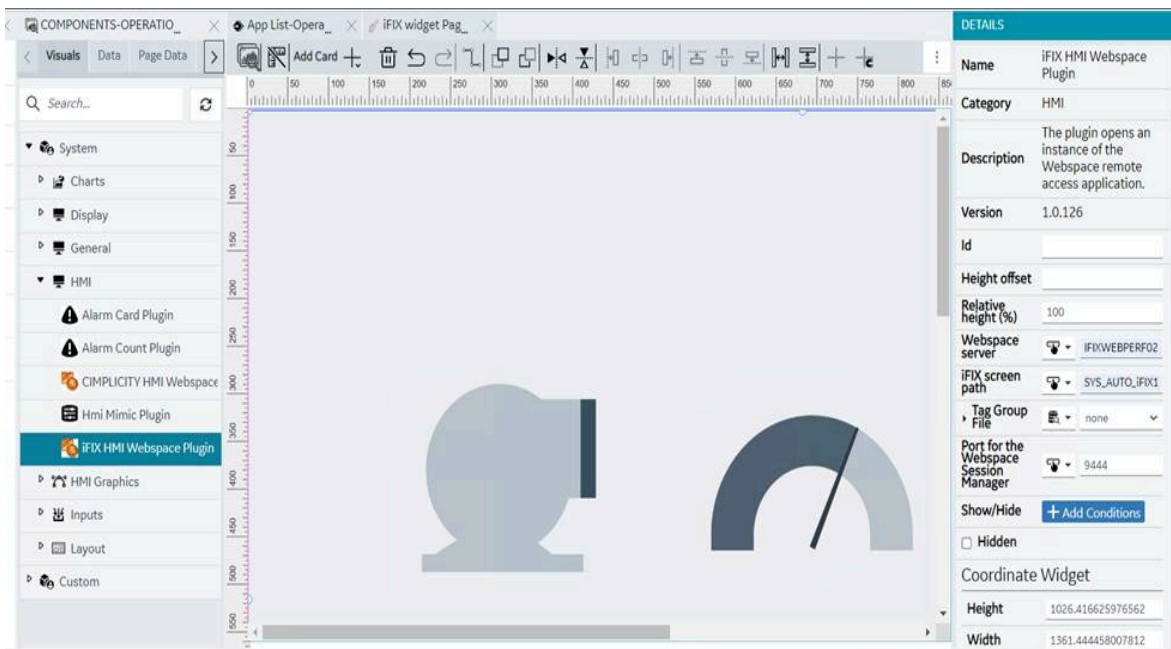
The Create App dialog box appears, as shown in the following figure.



3. In the App Name field, enter a name.

4. Optionally, provide a description.
5. Click **Add**.
6. From Operations Hub, navigate to the **HMI** folder.
7. Drag-and-drop the **iFIX HMI Webservice Plugin** to the workspace. Resize the plug-in as needed.
8. On the Details pane, provide the **Webservice Server Name** path and the **Port for the Webservice Session Manager**.

 **Note:**
The other Webservice details are listed in the table that follows the graphic.



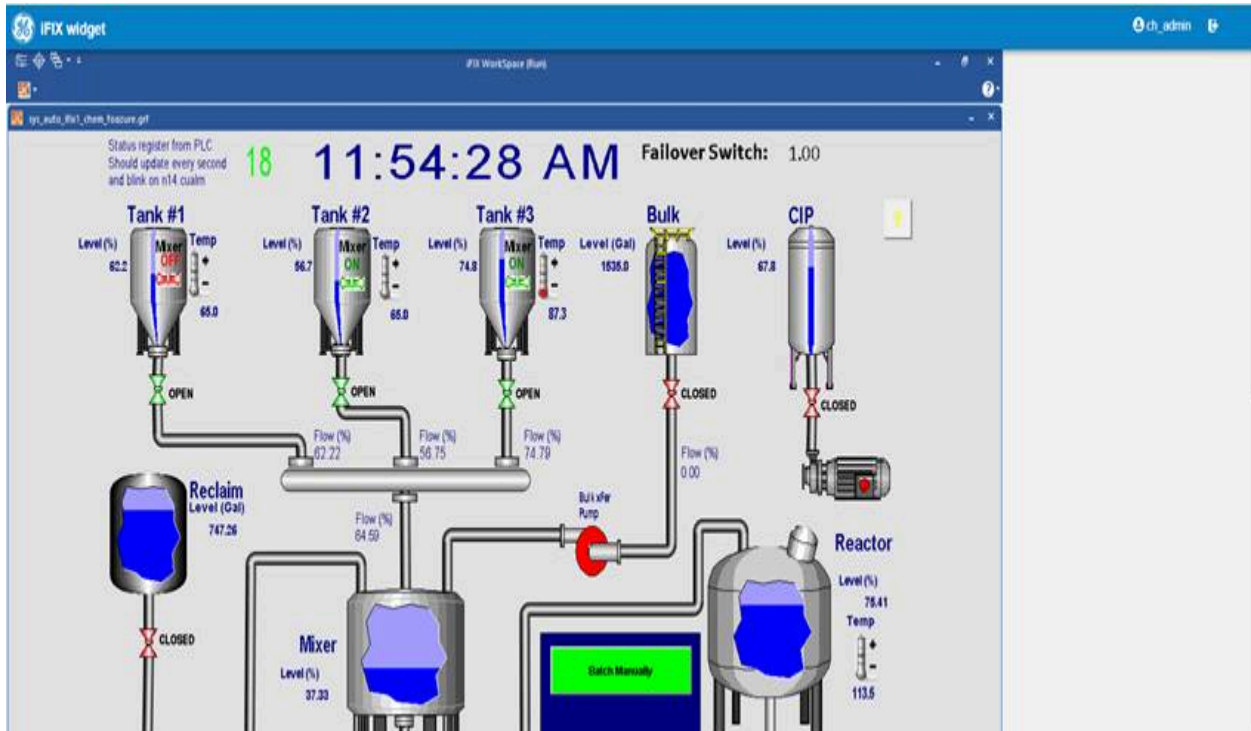
9. Click on **Save** button.
10. Launch the App.

iFIX Webservice Plugin Properties

Field Name	Description
ID	The ID name you choose to give your Webservice plugin instance in your application.
Height offset	Webservice frame will take the proportion specified in Relative height of the browser window minus this offset. It is useful when there are other widgets on the page above or below the Webservice frame.

Field Name	Description
Relative height (%)	Webspaces frame will take this proportion of the height of the browser window minus the Height offset. It is useful when there are multiple Webspaces widgets placed vertically on the page.
Webspaces server	Specify the machine that has iFIX Webspaces running on it.
iFIX screen path	Specify the path to the screen to load. This path is where the file resides on the Webspaces system.
Tag Group File	Specifies the tag of the tag group to open with the picture.
Port for the Webspaces Session Manager	The port configured on the Webspaces system for the Webspaces Session Manager service. 9444 is the default port setting.
Show/Hide	Click the Add Conditions button to add conditions to run when the iFIX Webspaces widget runs.
Hidden	Select the check box if you want to hide the iFIX Webspaces plugin on screen.

Example of Run Mode iFIX Webspaces Widget



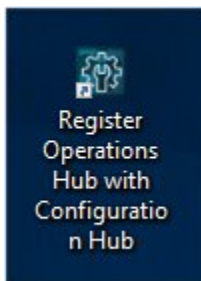
Troubleshooting Webspaces with Configuration Hub

This topic describes how to troubleshoot connection issues with the iFIX Webspaces widget in Configuration Hub, with Operations Hub installed.

What to do if Operations Hub Does Not Display in Configuration Hub in the Navigation Pane

If you cannot see the Operations Hub widget in the Configuration Hub navigation pane, try re-registering Operations Hub:

1. On the Configuration Hub server, double-click the **Register Operations Hub with Configuration Hub** shortcut on the desktop.



2. In the screen that appears, enter the base URL for Configuration Hub, and the client id and secret.

Configuration Hub Info

Configuration Hub Base URL:

Client ID:

Client Secret:

Operations Hub Plugins

Designer Plugin:

Result:

3. Click **Register** to re-register Operations Hub with Configuration Hub.

Contents

- Chapter 11. Getting Started..... 15**
 - Introduction to the Configuration Hub Framework..... 15
 - Sample Deployment Architectures..... 16
 - Install and Uninstall Options..... 20
 - Available Product Plugins..... 27
 - Common Panels..... 28
 - Common Panels..... 28
 - Application Bar 29
 - Navigation Panel..... 30
 - Details Panel..... 32
 - Concurrency Management..... 35
 - Server Certificates for Configuration Hub 36
 - Client Certificates for Configuration Hub..... 39
 - Proficy Authentication Certificate..... 48
 - Known Issues and Limitations 48
 - High Availability for Configuration Hub..... 50
 - Overview..... 50
 - Configure High Availability for Configuration Hub..... 51
 - Install Failover Clustering Feature..... 54
 - Create Failover Cluster..... 55
 - Create Role..... 58
 - Create Client Access Point (Virtual IP)..... 60
 - Add Dependencies to Role..... 62
 - Create Network Attached Storage..... 63
 - Install Configuration Hub on Cluster Nodes..... 65
 - Handling Silent Installation..... 67
- Chapter 12. Proficy Authentication 70**

About Proficy Authentication.....	70
Set up Proficy Authentication.....	70
Navigation in Proficy Authentication.....	75
Manage Identity Providers.....	76
Add LDAP Identity Provider.....	76
Enable SAML.....	79
Add SAML Identity Provider.....	88
Enable Multi-Factor Authentication.....	90
Modify LDAP Identity Provider.....	92
Modify SAML Identity Provider.....	94
Delete Identity Provider.....	95
Manage Groups.....	96
Overview of iFIX Groups in Proficy Authentication.....	96
Overview of Historian Groups in Proficy Authentication.....	97
Create Groups.....	97
Modify Groups.....	98
Map Groups.....	99
Add/Remove Users in a Group.....	102
Add/Remove Sub-Groups in a Group.....	103
Delete Group.....	104
Manage Users.....	105
Create Users.....	105
Add/Remove Groups for a User.....	107
Reset User Password.....	109
Delete User.....	110
Windows Integrated Authentication / Auto-login.....	110
Configure Security Policy.....	113
Create Service Principal Name.....	115
Generate Keytab File.....	118

Proficy Authentication Service Configuration.....	121
Configure Browser.....	122
Troubleshooting Error Logs.....	123
High Availability.....	128
Configure High Availability for Proficy Authentication.....	128
Configure iSCSI Target.....	129
Configure iSCSI Initiator.....	130
Create a Virtual Disk.....	131
Initialize a Virtual Disk.....	133
Create a Cluster.....	135
Configure Role.....	138
Configure Proficy Authentication Installation.....	142
Prerequisites for Installing Operations Hub with External Proficy Authentication.....	146
Customize Login Screen.....	150
Chapter 13. iFIX.....	152
Overview	152
Introduction to iFIX Web Configuration.....	152
Integrated Development Environment.....	154
Prerequisites to Use Configuration Hub with iFIX.....	154
Configuration Information.....	155
Access iFIX Web Configuration.....	169
Connections	171
Connections Overview.....	171
OPC UA Connections	171
IGS Connections.....	183
Drivers.....	191
Network Connections.....	193
Special Considerations for SCADA Enhanced Failover.....	198
SQL Connections.....	200

Model	203
Model Overview.....	203
Model Panel.....	204
Type Creation.....	206
Type Variables	208
Template Overview.....	211
Template Management.....	211
Substitutions.....	214
Expression Builder.....	216
Object Creation.....	216
Model Import and Export.....	217
Model Tags in iFIX.....	218
Database.....	221
Database Overview.....	221
Database Management.....	227
Tag Management.....	279
Validations.....	281
Custom Editors.....	282
Tag Properties.....	283
Project Security	823
Overview of Project Security.....	823
Add or Modify Users.....	824
Add or Modify Groups for Proficy Authentication.....	827
Add or Modify Security Areas.....	828
Auto Login Configuration.....	830
Alarms	832
Defining Alarm Areas.....	832
Alarm Services.....	834
Alarm Printers.....	839

Alarm Events.....	841
Alarm Queue Configuration.....	843
Common Message Format Configuration.....	845
Common Alarm Areas Configuration.....	846
Alarm Clients.....	847
Project Settings	848
Overview of Project Settings.....	848
Starting and Stopping iFIX Projects.....	851
Add a New Project.....	853
Add an Existing Project.....	855
General Settings.....	856
Startup Options.....	858
Startup Schedules.....	861
Startup Pictures.....	862
Historian.....	863
SCADA Failover.....	864
Task Configuration.....	868
Deployment.....	872
Project Deployment.....	872
Save and Publish.....	874
Chapter 14. Historian.....	877
Overview of Historian with Configuration Hub.....	877
About Historian in Configuration Hub.....	877
Configuration Hub Workflow for Historian.....	878
Setting up Configuration Hub for Historian.....	879
About Setting up Configuration Hub with Historian.....	879
Install the Historian Server.....	880
Install Web-based Clients.....	885
Install Collectors.....	898

Perform Post-Installation Tasks.....	901
Upgrade.....	902
Access Configuration Hub.....	902
Common Tasks.....	906
Setting up a Stand-Alone System.....	907
About Setting up a Stand-Alone Historian System.....	907
Add a Collector.....	909
Add Tags for the Data Store Using Configuration Hub.....	909
Setting up a Horizontally Scalable System.....	911
About Setting up a Horizontally Scalable System.....	911
Add a Server.....	913
Add a Collector.....	914
Add Tags.....	915
Setting up High Availability.....	917
About Data Mirroring	917
Create.....	918
Create a Data Store.....	920
Creating a Model.....	921
About a Historian Model.....	921
About Object Templates.....	927
Workflow for Creating a Historian Model.....	930
Create an Object Type.....	931
Include a Contained Type.....	936
Create an Object Instance.....	939
Provide Data for a Static Variable.....	941
Collect Data for a Direct Variable.....	944
Collect Data for an Indirect Variable.....	947
Export an Object Type/Instance.....	951
Import an Object Type/Instance.....	953

Copy an Object Type.....	954
Delete a Template.....	959
Delete an Object Instance.....	961
Delete an Object Type.....	962
Managing Historian Systems.....	963
Access a System.....	963
Access the Collectors in a System.....	971
Access Offline Configuration Collectors.....	973
Access the Tags in a System.....	976
Add a System.....	978
Add a Server.....	979
Set Up a Mirror of Mirror.....	980
Remove a Server.....	990
Set a Default Location.....	990
Modify a System.....	991
Configure Advanced Settings.....	992
Configure Labels of Spare Fields.....	995
Set a Default System.....	996
Delete a System.....	996
Managing Mirror Locations.....	997
Create.....	997
Rename.....	998
Add a Machine.....	1000
Remove a Machine.....	1001
Delete.....	1002
Managing Data Stores.....	1003
About Data Stores	1003
Create a Data Store.....	1004
Access a Data Store.....	1005

Rename a Data Store.....	1009
Set as Default.....	1013
Access Archives.....	1014
Access Activity Logs.....	1015
Access Tags.....	1015
Specify Tags for Data Collection.....	1016
Add a Tag Manually.....	1018
View Performance.....	1021
Delete.....	1023
Adding a Collector Instance.....	1024
The Calculation Collector.....	1024
CygNet Collector.....	1027
The File Collector.....	1031
The HAB Collector.....	1035
Collection Definitions of a HAB Collector.....	1041
About Adding an iFIX Collector Instance.....	1047
The iFIX Collector.....	1051
The MQTT Collector.....	1056
The ODBC Collector.....	1062
The OPC Classic Alarms and Events Collector.....	1067
The OPC Classic DA Collector.....	1070
The OPC Classic HDA Collector.....	1076
The OPC UA DA Collector.....	1080
The OSI PI Collector.....	1084
The OSI PI Distributor.....	1088
The Server-to-Server Collector.....	1093
The Server-to-Server Distributor.....	1098
The Simulation Collector.....	1102
The Windows Performance Collector.....	1106

The Wonderware Collector.....	1110
Collector Configuration - Common Fields.....	1114
Sending Data to Cloud.....	1122
Alibaba Cloud.....	1122
AWS Cloud.....	1127
Azure Cloud (Key-Value Format).....	1134
Azure Cloud (KairosDB Format).....	1142
Google Cloud.....	1148
Predix Cloud.....	1154
Protocols and Port Numbers.....	1159
Managing Collector Instances.....	1160
Managing Collectors Using Configuration Hub.....	1160
Access a Collector.....	1161
Access Tags.....	1164
Add a Collector.....	1165
Modify a Collector.....	1166
Add a Comment.....	1168
Access Comments.....	1169
Start a Collector.....	1170
Stop a Collector.....	1172
Restart a Collector.....	1173
Pause Data Collection.....	1175
Resume Data Collection.....	1176
Clear Buffer.....	1177
Move Buffer.....	1179
Change Destination.....	1180
Configure Collector Redundancy.....	1182
Delete a Collector.....	1184
Managing Offline Configuration Collector Instances.....	1186

Access Offline Configuration Collectors.....	1186
Manage Offline Configuration Collectors.....	1188
Access Tags.....	1189
Managing Tags.....	1189
About Tags.....	1189
About Array Tags.....	1190
About Collector and Archive Compression.....	1190
About Scaling.....	1197
About Condition-Based Collection.....	1197
Specify Tags for Data Collection.....	1198
Add a Tag Manually.....	1200
Access a Tag.....	1204
Access Trend Chart.....	1218
Access Last 10 Values.....	1219
Access a Tag Alias.....	1222
Rename a Tag.....	1224
Copy a Tag.....	1226
Stop Data Collection.....	1228
Resume Data Collection.....	1230
Remove a Tag.....	1230
Delete a Tag.....	1232
Managing Enumerated Sets.....	1234
About Enumerated Sets.....	1234
Create an Enum Set.....	1235
Assign to Tag.....	1236
Delete an Enum Set.....	1237
Managing User-Defined Data Types.....	1238
About UDTs.....	1238
Create UDT.....	1238

Assign to Tag.....	1239
Delete UDT.....	1240
Managing Archives.....	1241
About Archives.....	1241
Guidelines for Archive Sizing.....	1242
Access an Archive.....	1243
Create Archives Automatically.....	1245
Create Archives Manually.....	1247
Back up an Archive.....	1249
Back up Archives with Volume Shadow Copy Service.....	1250
Restore an Archive.....	1252
Close an Archive.....	1253
Remove an Archive.....	1253
Reading/Writing Data.....	1253
Query Data.....	1253
Write Data.....	1257
Managing Alarms and Events.....	1259
About Alarms and Events.....	1259
Requirements.....	1260
Create an Alarm.....	1260
Access/Filter Alarms.....	1261
Back up Alarms.....	1262
Restore Alarms.....	1263
About Purging Alarms.....	1264
Accessing Activity Logs.....	1266
Troubleshooting Historian and Configuration Hub	1268
Chapter 15. Operations Hub.....	1272
Operations Hub and the Integrated Installer.....	1272
Install Common Components.....	1273

Install Operations Hub for SCADA.....	1277
Install Operations Hub from a Dedicated Installer.....	1282
Register Operations Hub with Configuration Hub.....	1289
Getting Started with Operations Hub.....	1290
Operations Hub (New Layout).....	1291
Panels Layout.....	1291
Navigation Panel.....	1292
Components Panel.....	1294
Display Panel.....	1305
Details Panel.....	1310
HMI Graphics.....	1325
Chapter 16. WebSpace	1348
Overview of WebSpace with Configuration Hub.....	1348
Sample WebSpace Deployment Architecture.....	1349
How to Install a WebSpace Server.....	1350
Exporting the Root Certificate for WebSpace Setup.....	1351
Importing the Certificate for WebSpace Setup.....	1353
Registration with Configuration Hub for WebSpace.....	1355
WebSpace Settings in Configuration Hub.....	1358
iFIX WebSpace Plugin in Operations Hub.....	1359
Troubleshooting WebSpace with Configuration Hub.....	1363
Chapter 18. MQTT Client.....	1378
Getting Started.....	1378
Introduction.....	1378
Prerequisites and Hardware Requirements.....	1379
Sample Deployment Architectures.....	1380
Installation.....	1384
Registration and Proficy Authentication.....	1390
Utilities.....	1397

Changing Admin Credentials.....	1397
Port Changes.....	1398
Configuration.....	1399
MQTT Client in Configuration Hub.....	1399
Chapter 19. Settings.....	1442
Switch Users.....	1442
Modify Layout.....	1442
Host Name Changes.....	1442
Port Changes for Configuration Hub.....	1445
Chapter 20. Troubleshooting.....	1447
Log Files.....	1447
Frequently Asked Questions.....	1450

Chapter 7. MQTT Client

Getting Started

Introduction

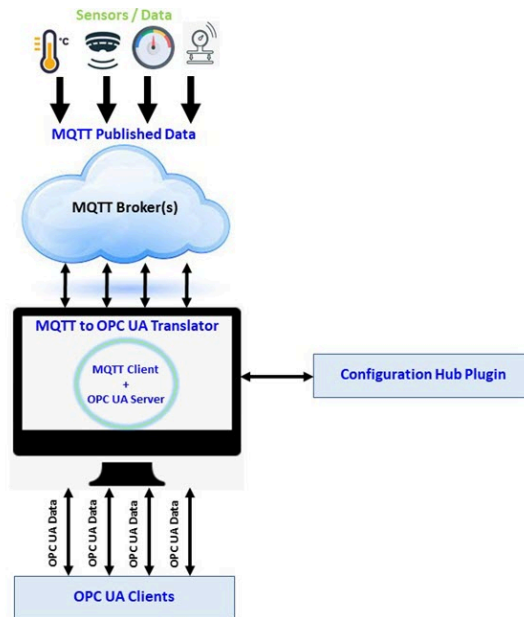
This document describes the importance of the MQTT Client application and its purpose in the Proficy product suite. The MQTT Client application can be installed along with the SCADA products using the iFIX Integrated installer.

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

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

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

MQTT in Configuration Hub helps you to configure the MQTT Client and OPC UA Server. For more information, refer to [MQTT Client in Configuration Hub \(on page 1399\)](#).



Prerequisites and Hardware Requirements

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

- Proficy Authentication 2023
- Configuration Hub 2023
- iFIX 2023



Note:

The Proficy products can be installed using the iFIX Integrated installer.

Hardware Requirements

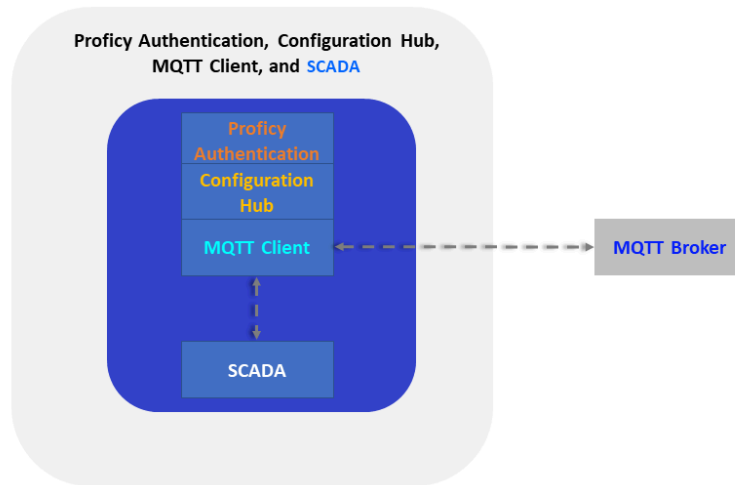
- Operating System Windows 2019 Server, Windows 2022 Server, Windows 10, and Windows 11
- RAM - 8 GB
- CPU - Quad Core

Sample Deployment Architectures

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

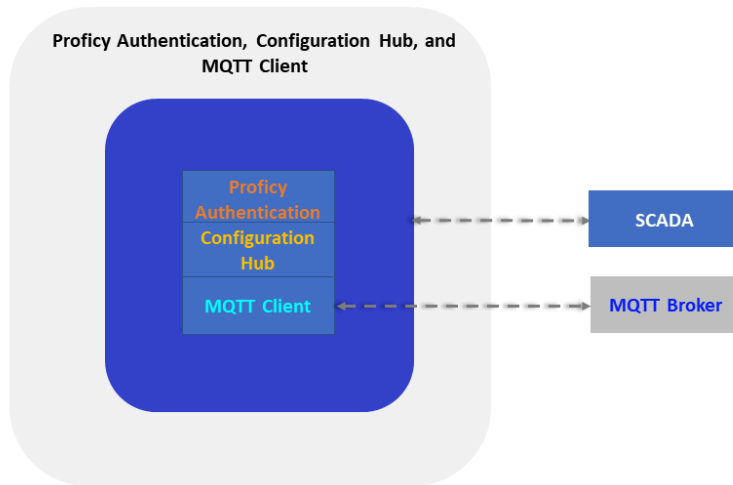
Example 1

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



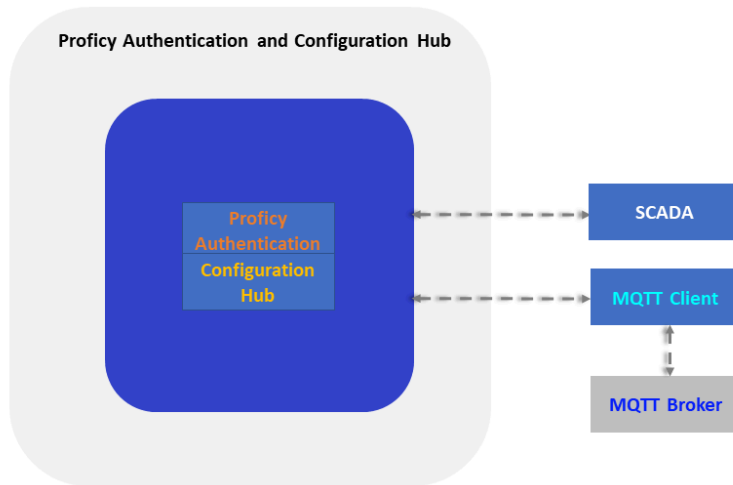
Example 2

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



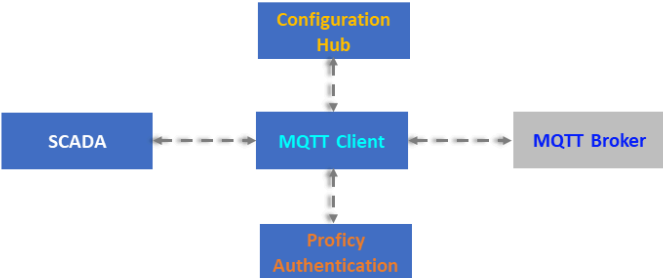
Example 3

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



Example 4

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



Installation

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

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

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

**Note:**

- When you select MQTT Client from the iFIX 2023 Integrated installer, along with the MQTT Client software installation, the License Client will also be installed silently. The License Client helps you manage the license for the MQTT Client software and authenticates you to use the application on your machine.
- Configuration of the MQTT Client requires Configuration Hub to be installed on the SCADA network. Refer to the Configuration Hub documentation for more details.
- Setting up Proficy Authentication provides access to all the products (iFIX, CIMPLICITY, and others) registered with Configuration Hub. You use the same Proficy Authentication server to authenticate the user of all the products. Refer to the Proficy Authentication documentation for more details.

To install the MQTT Client using the iFIX 2023 Integrated installer:

1. Double-click the `<Integrated_Installer>.iso` disc file or select **Mount** from the context menu.
2. Double-click the **Setup.bat** windows batch file, which will launch the iFIX 2023 Integrated installer.

**Note:**

You can also navigate through the **Setup** folder, and then double-click the `setup.exe` application to launch the iFIX 2023 Integrated installer.


The welcome screen for the iFIX 2023 suite appears.

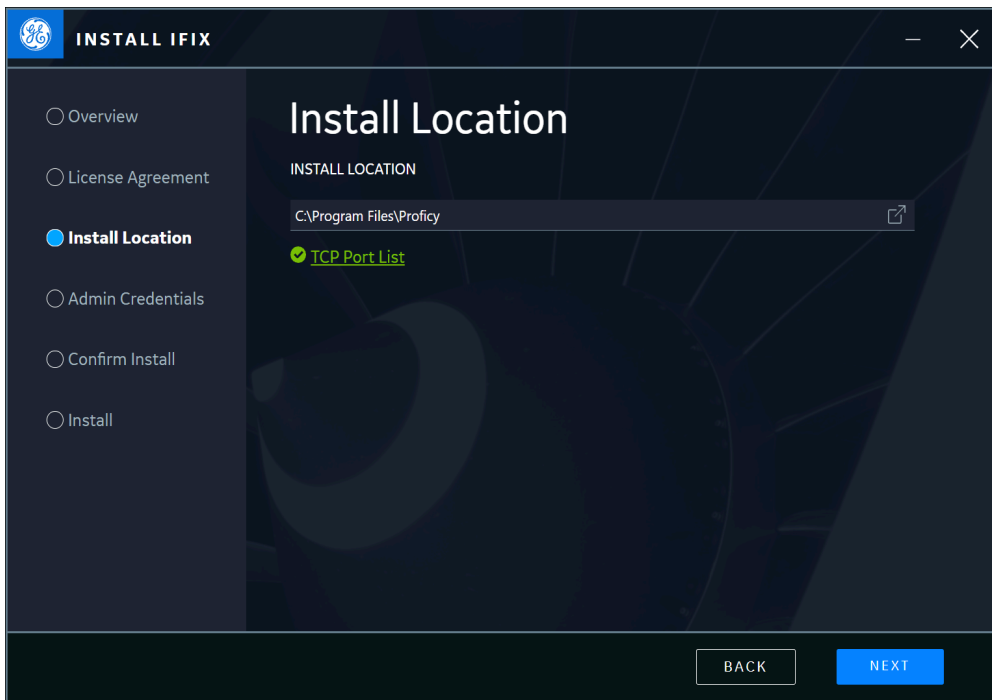
3. Select **MQTT Client**, and then click **START**.



4. Click **ACCEPT** to proceed with the License Agreement.

5. Click **NEXT** to install the MQTT Client in the default location C:\Program Files\Proficy or

click  to modify the install location.

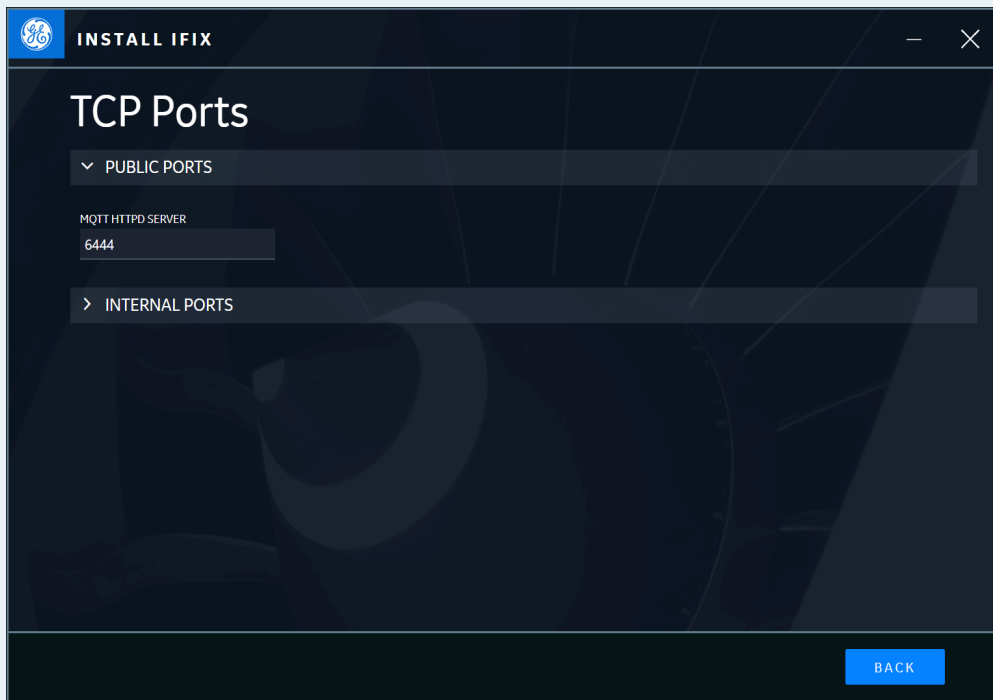


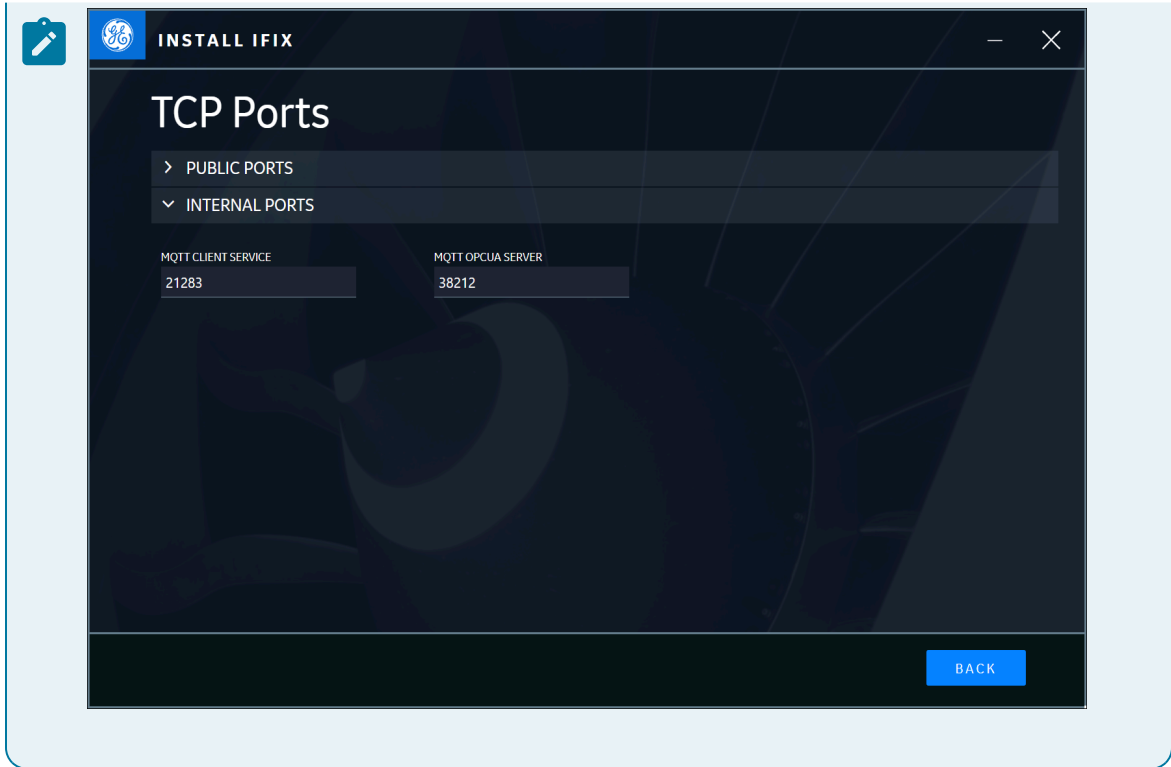
**Note:**

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

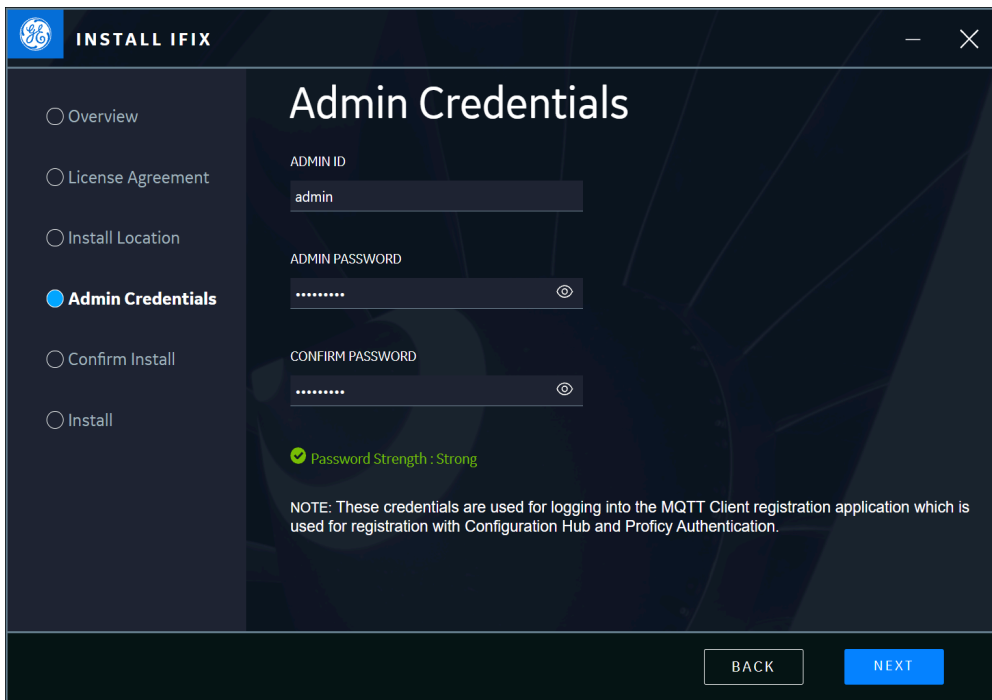
**Note:**

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





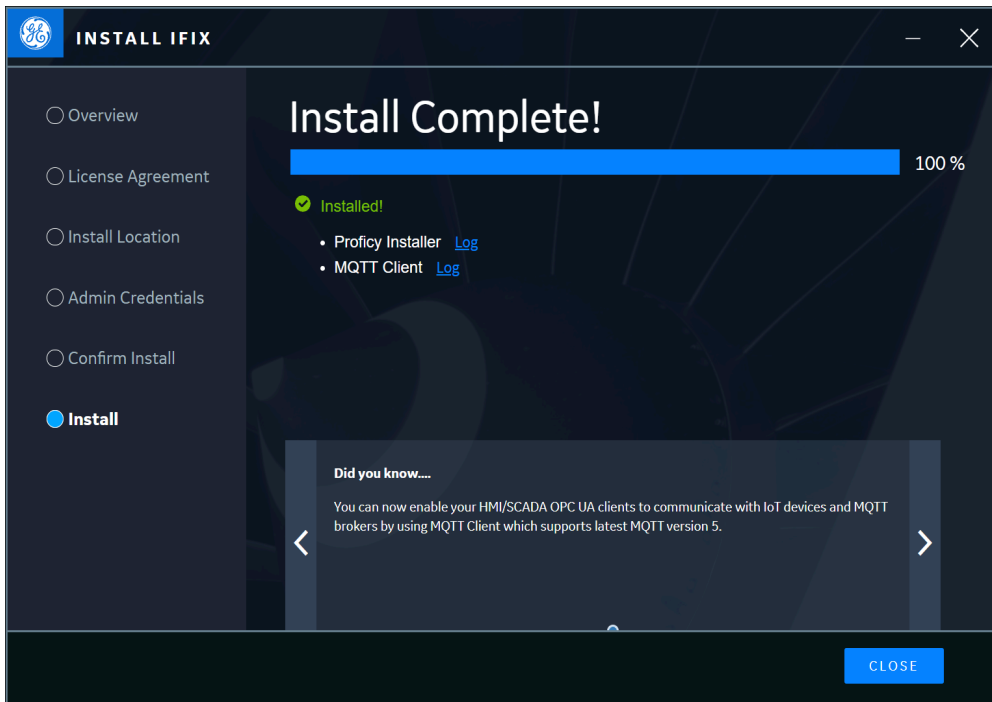
6. Create login credentials for MQTT Client, and then click **NEXT**.



**Note:**

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

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



The MQTT Client application is installed on your machine.

**Note:**

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

8. Click **CLOSE**.

**Note:**


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

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



Note:

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

10. Double-click the  **MQTT Client Registration** desktop shortcut to register the MQTT Plug-in with the Proficy Authentication and the Configuration Hub servers. Refer to [Registration and Proficy Authentication \(on page 1390\)](#) for more information.

Registration and Proficy Authentication

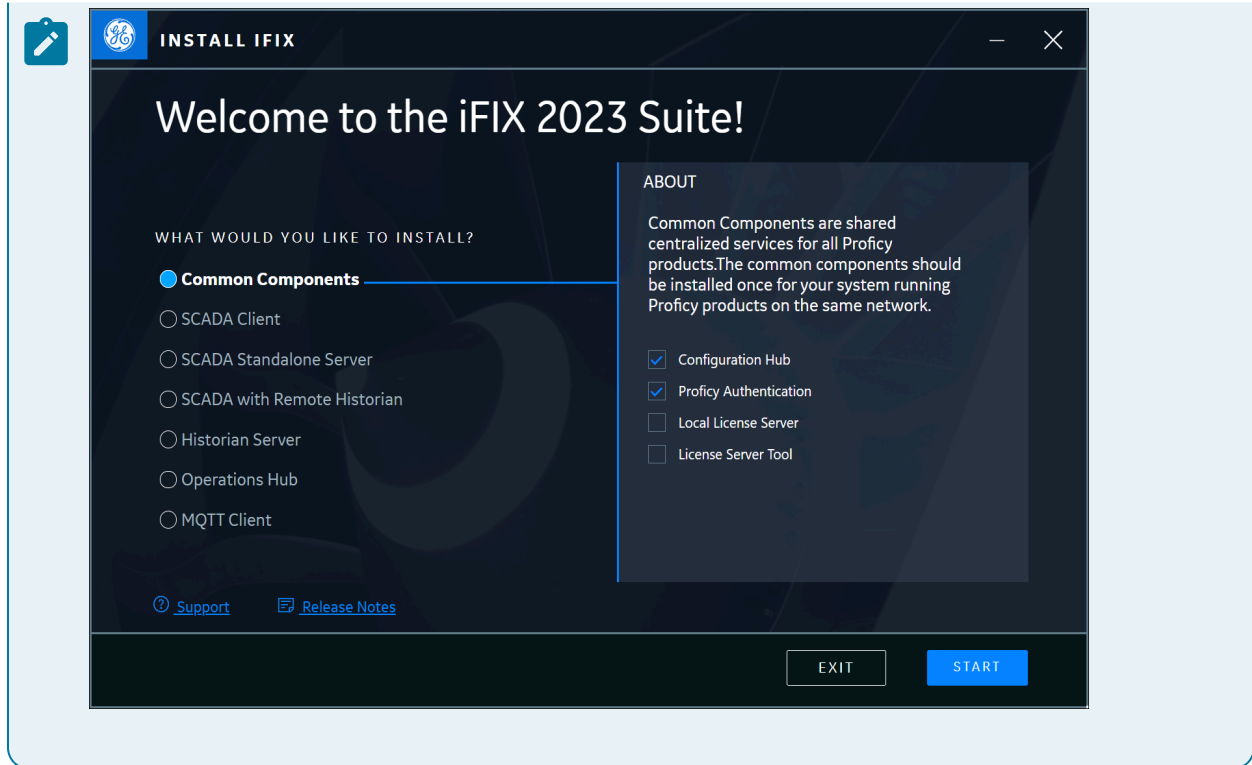
You must register the MQTT Client with the Proficy Authentication server and the Configuration Hub server.

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



Note:

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



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

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

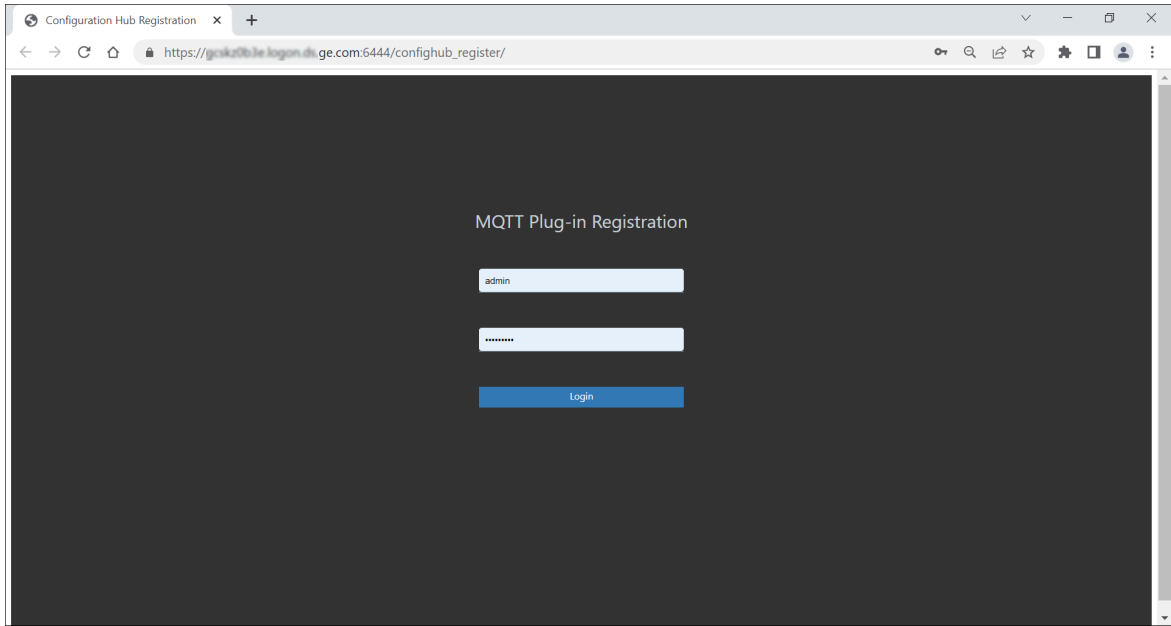
1. Double-click the  **MQTT Client Registration** desktop shortcut.



Note:

The MQTT Client Registration desktop shortcut appears only after you install the MQTT Client application from the <Integrated Installer>.iso disc file. Refer to MQTT Client [Installation \(on page 1384\)](#) for more information.

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



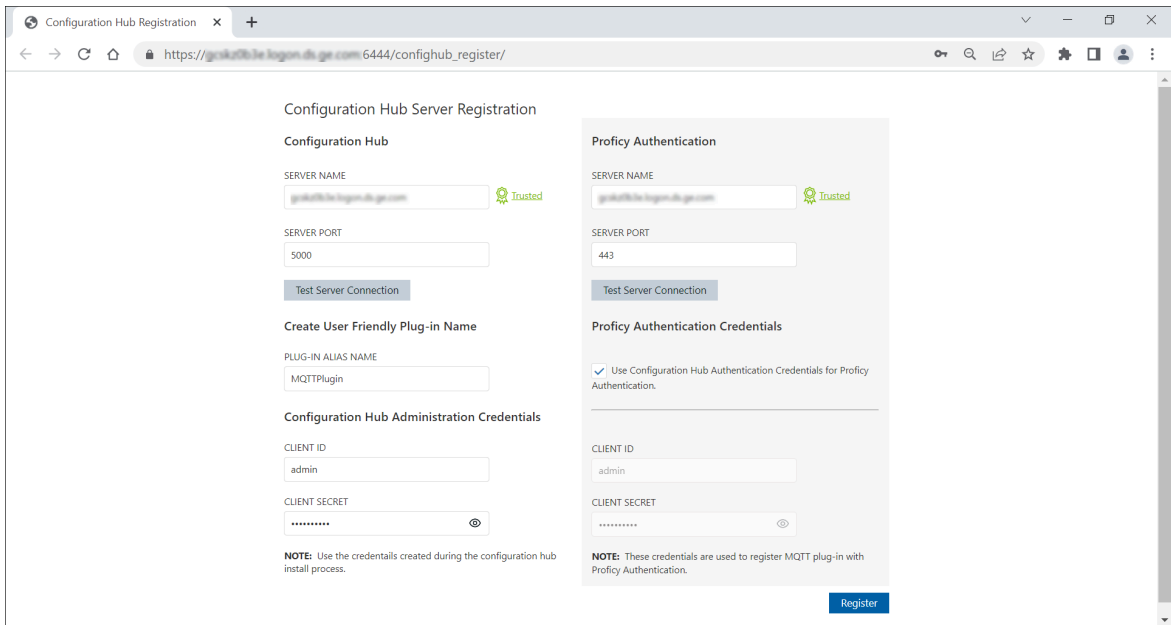
2. Enter your login credentials and then, click **Login**.





Note:

Enter the login credentials you created during the MQTT Client installation.

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



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

Field	Description
SERVER NAME	The name of the Configuration Hub server to which you want to register. In the <Fully qualified domain name> format.
SERVER PORT	The port number of the Configuration Hub server to which you want to register.
PLUG-IN ALIAS NAME	<p>The alias name for the MQTT plugin that you want to see in the Configuration Hub.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note: By default, the name populated is the machine name where the MQTT Client is installed. However, you can update it to how you want to see the MQTT plugin name in the Configuration Hub.</p> </div> <div style="border: 1px solid #FFC000; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Important: Do not use the dot (.) character for the MQTT plugin alias name.</p> </div>
CLIENT ID	The client ID of the Configuration Hub server that you provided during the Configuration Hub installation.
CLIENT SECRET	The client secret of the Configuration Hub server that you provided during the Configuration Hub installation.

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

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

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

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

- Click **Not trusted**.

The **Certificate Details** page appears.

- Click **Trust**.

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

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

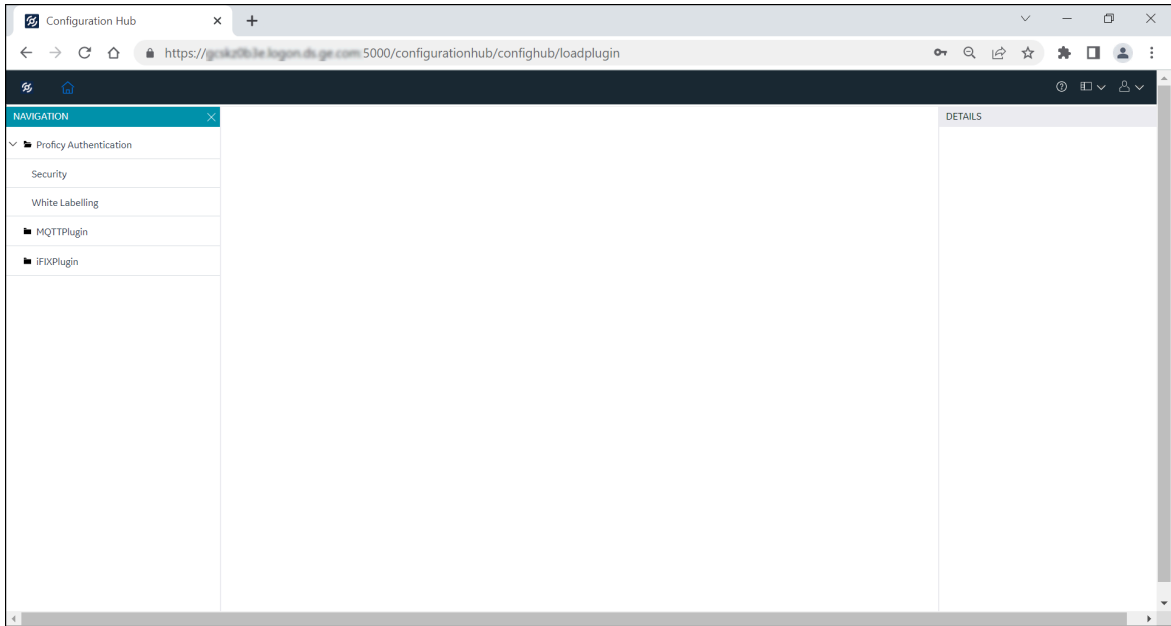
If the connection to the Configuration Hub or the Proficy Authentication server is successful, you will receive a success dialog. If your connection is unsuccessful, retry to connect to another valid Configuration Hub or Proficy Authentication server.

7. Click **Register**.

The Configuration Hub Server registration success message appears.

By default, the ch_admin user is created with a password the same as the Proficy Authentication secret, and the required Group Membership is assigned to the ch_admin user to access the MQTT Client. For more information, refer to [Manage Identity Providers, Groups, and Users \(on page 1400\)](#).

8. Click **OK**.



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




Note:

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

Demo license expired. Restart the MQTTClient service.

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

Service unavailable. Restart the MqttClient service.

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

**Important:**


If you run the MQTT Client application in Demo license mode, OPC UA write permissions are not supported. As a result, the OPC UA clients can only read the values of OPCUA tags but cannot write to or modify them.

Utilities

Changing Admin Credentials

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

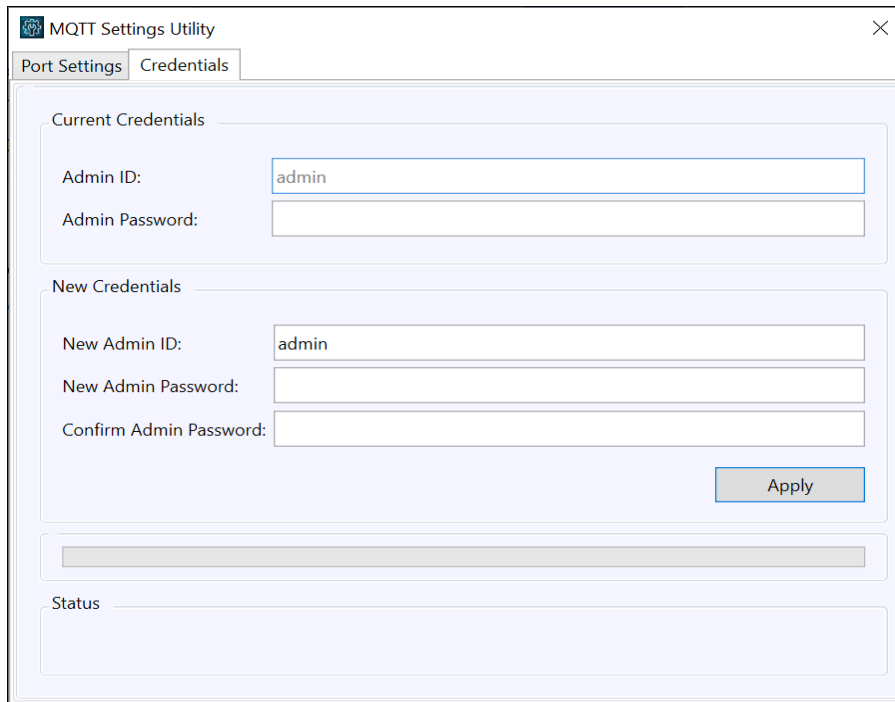
**Note:**

Before you make any changes, you must stop the GE MQTT Client Httpd Service and GE MQTT Client Service from  **Services**.

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

The **MQTT Settings Utility** dialog appears.

3. Select the **Credentials** tab.




4. In **Current Credentials**, enter:

- **Admin Password:** The password you created during MQTT Client installation.

In **New Credentials**, enter:

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

5. Click **Apply**.


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

Port Changes

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



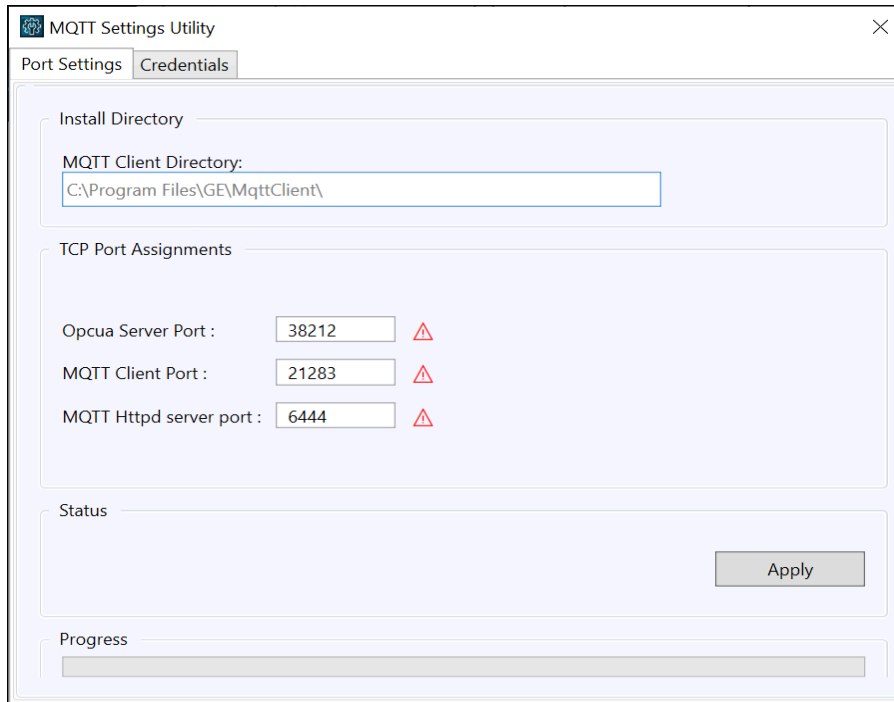
Note:


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

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

The **MQTT Settings Utility** dialog appears.

3. Select the **Port Settings** tab.



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

Configuration

MQTT Client in Configuration Hub

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

To take advantage of the configuration of different data parameters from the MQTT broker(s), you must register the MQTT Client with the Configuration Hub server. Refer to [Registration and Proficy Authentication \(on page 1390\)](#) on how to register the MQTT client connections.

For more information on configuration, refer to [MQTT Client Configuration \(on page 1400\)](#).


MQTT Client Configuration

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

1. [Manage Identity Providers, Groups, and Users \(on page 1400\)](#).
2. [Add MQTT Server for Broker Connection \(on page 1401\)](#).
3. [Add Subscriptions to Broker Connection \(on page 1407\)](#).
4. [Add Tags to Subscription \(on page 1418\)](#).

Manage Identity Providers, Groups, and Users

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

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

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

For more information on MQTT groups and access provisions, refer to [MQTT Groups in Proficy Authentication \(on page 1400\)](#).

MQTT Groups in Proficy Authentication

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

Table 50. Group Membership

MQTT Group Membership	Access Provision
protocoltranslators.mqtt.<PLUG-IN ALIAS NAME>.config.read	Retrieve the list of broker, subscriptions, and tags on the specific MQTT client node that has the Alias name registered with Configuration Hub.

Table 50. Group Membership (continued)

MQTT Group Membership	Access Provision
<code>protocoltranslators.mqtt.<PLUG-IN ALIAS NAME>.config.write</code>	<ul style="list-style-type: none"> Retrieve/modify/add/delete the list of broker, subscriptions, and tags on the specific MQTT client node that has that Alias name registered with Configuration Hub. Save and Publish the data.
<code>protocoltranslators.mqtt.<PLUG-IN ALIAS NAME>.opcua.read</code>	This group provides read access to OPC UA clients, so that the OPC UA clients can connect to the MQTT OPC UA server and read the OPC UA data on the specific node.
<code>protocoltranslators.mqtt.<PLUG-IN ALIAS NAME>.opcua.write</code>	This group provides read/write access to OPC UA clients, so that the OPC UA clients can connect to the MQTT OPC UA server and read/write the OPC UA data on the specific node.

**Note:**

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

- `protocoltranslators.mqtt.shared.config.read`
- `protocoltranslators.mqtt.shared.config.write`
- `protocoltranslators.mqtt.shared.opcua.read`
- `protocoltranslators.mqtt.shared.opcua.write`

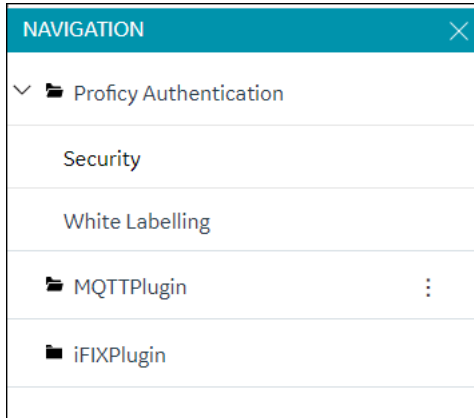
**Important:**

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

Add MQTT Server for Broker Connection

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

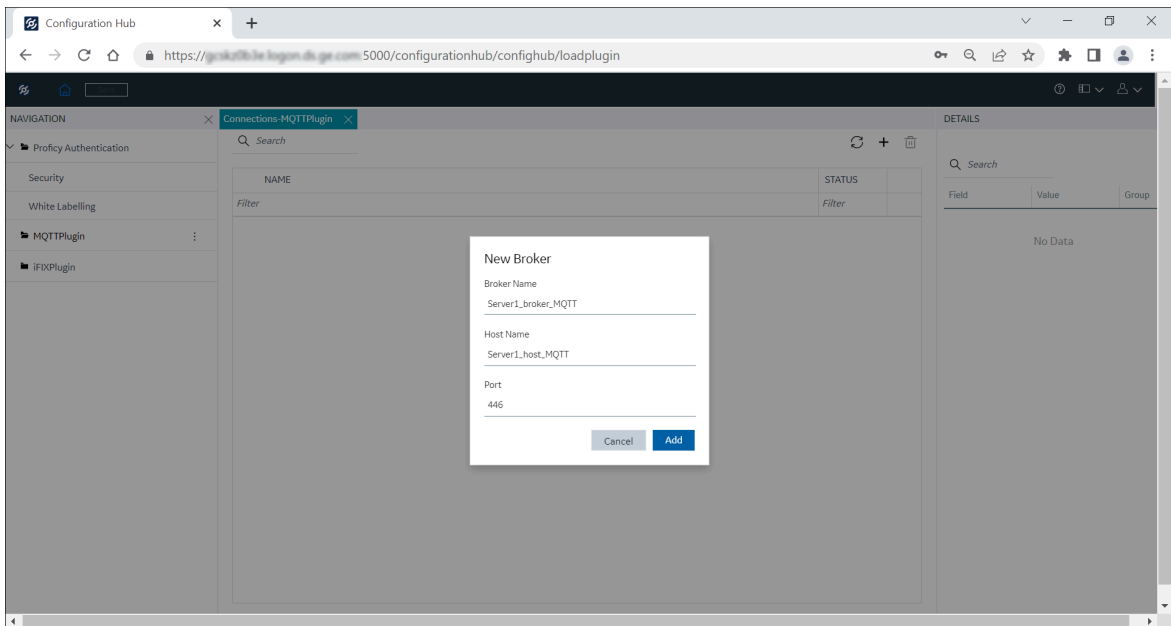
To add the Server for Broker Connection, you must log into Configuration Hub with Proficy Authentication credentials. After you login, the enabled connections appear in the **Navigation** panel.



To add the Server for Broker Connection:

1. Click **+** to add a new broker.

The **New Broker** dialog appears.



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



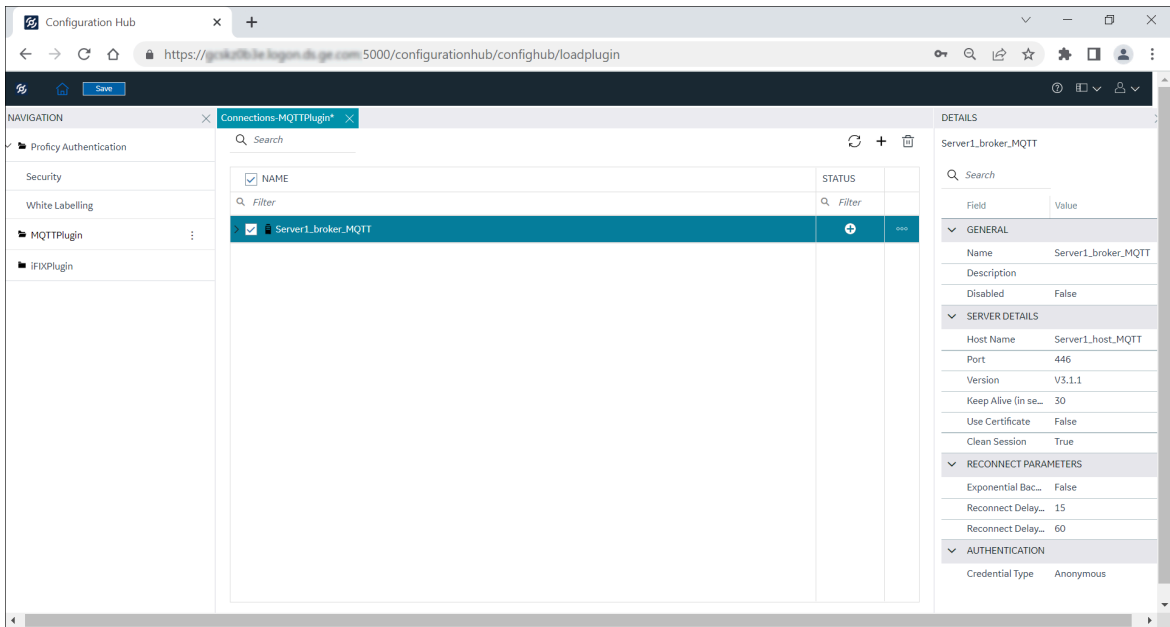
Note:

- Adhere to the following rules when entering information:
 - The broker name must start with a letter and cannot exceed 255 characters.
 - Do not include spaces in between names.



- Names cannot have leading or trailing spaces.
- The only special characters allowed in the broker name are '-' and '_'.
- All special characters and numbers are allowed in a Host name. Spaces are not allowed.
- The port name field cannot include letters. The port number must be in the range 1 to 65535.
- Field names cannot be left blank. Duplicate names are not allowed.

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




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


Table 51. MQTT Server Details

Field	Value
GENERAL	
Name	Enter a name for the broker connection.
Description	Enter the description for the broker connection.
Disabled	You can enable or disable the broker connection with the client.

Field	Value
	<ul style="list-style-type: none"> ◦ True: The client is disabled from connecting to the MQTT broker. ◦ False: The client is enabled to connect to the MQTT broker. This is the default value.
SERVER DETAILS	
Host Name	Host name of the server on which the MQTT broker is installed.
Port	The port number of the MQTT broker.
Version	The MQTT version (V5 or, V3.1.1 or, V3.1) used to connect to the MQTT broker.
Keep Alive (in seconds)	<p>When there is no exchange of messages or no data flow between the client and the broker for a certain time period, the client will generate a PING request to the broker and the broker will reciprocate by sending a PING response to the client. This confirms the connection is active and the time period to confirm the active connection is the <i>Keep Alive</i> period. By default, the <i>Keep Alive</i> period is set to 30 seconds. You can modify the <i>Keep Alive</i> default value as required to establish the connection.</p>
Use Certificate	<p>To establish a secure connection with the broker, you must import the broker certificate and trust the certificate.</p> <ul style="list-style-type: none"> ◦ If set to True, the following message appears: <p><i>'Use certificate' field is set to true, Please upload your certificate by clicking on 'Import certificate' option in the broker context menu.</i></p> <p>This indicates that you must import the certificate to enable a secure connec-</p>

Field	Value
	<p>tion with the MQTT broker. Refer to Secure Connection with Broker (on page 1425) to import the certificate. Similarly, the MQTT broker must import the client certificate to enable a secure connection with the client. Refer to the broker documentation to import the client certificate. The MQTT Client root certificate is available at <Installation Path>/Pki/own/MqttClientRootCA.crt</p> <ul style="list-style-type: none"> ◦ If set to False, the MQTT broker connection is not secured.
Clean Session	<ul style="list-style-type: none"> ◦ True: The broker does not store any information about the client and disconnects the existing session (for the topic subscribed). However, a new session will be created, and this session will remain active until the network connection is active. The client must re-subscribe to the topics in the new session. This is the default value. ◦ False: The broker stores the client information for the topic subscribed so that when the client disconnects and reconnects, the client does not have to re-subscribe to the topics because the information is stored by the broker. Also, the broker stores the QoS1 and QoS2 messages subscribed to by the client when the session is disconnected.
Session Expiry Interval	<p>The Session Expiry Interval is the period after disconnection (client to broker or, broker to client session) during which the messages are persisted.</p>

Field	Value
	<div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: The Session Expiry Interval is applicable only when you connect to the broker using MQTT version V5, and if the Clean Session is set to False. </div>
RECONNECT PARAMETERS	
Exponential BackOff	The Exponential Backoff helps minimize the number of retries during the connection establishment process. <ul style="list-style-type: none"> ◦ True: Requests or retries to reconnect to the broker are sent as the time increases exponentially. ◦ False: Requests are sent according to the reconnect delay parameters.
Reconnect Delay (in seconds)	By default, the Reconnect Delay value is set to 15 seconds. That means, after a connection fails to the server, reconnection to the server will connect every 15 seconds.
Reconnect Delay Max (in seconds)	By default, the reconnect delay maximum value is set to 60 seconds. That means reconnection is attempted as per the values specified in Reconnect Delay until the Reconnect Delay Max is reached. Subsequently, the reconnection is attempted at the interval specified in the Reconnect Delay Max parameter.
AUTHENTICATION	
Credential Type	Valid entries are: <ul style="list-style-type: none"> ◦ Anonymous ◦ UserName/Password ◦ PreShared Key

Field	Value
	<p>It is recommended that you select User-Name/Password or PreShared Key to provide optimum security. If the UserName/Password option is selected, enter the username and password to connect to the MQTT server.</p> <div data-bbox="862 516 1419 737" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: The Anonymous credential type does not provide any access protection for the data.</p> </div>

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

In addition to editing a broker connection, the connection panel supports creating subscriptions under the broker connections. For more details, refer to [Add Subscriptions to Broker Connection \(on page 1407\)](#).

Add Subscriptions to Broker Connection

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

The following subscription types are supported:

1. JSON
2. Sparkplug-B



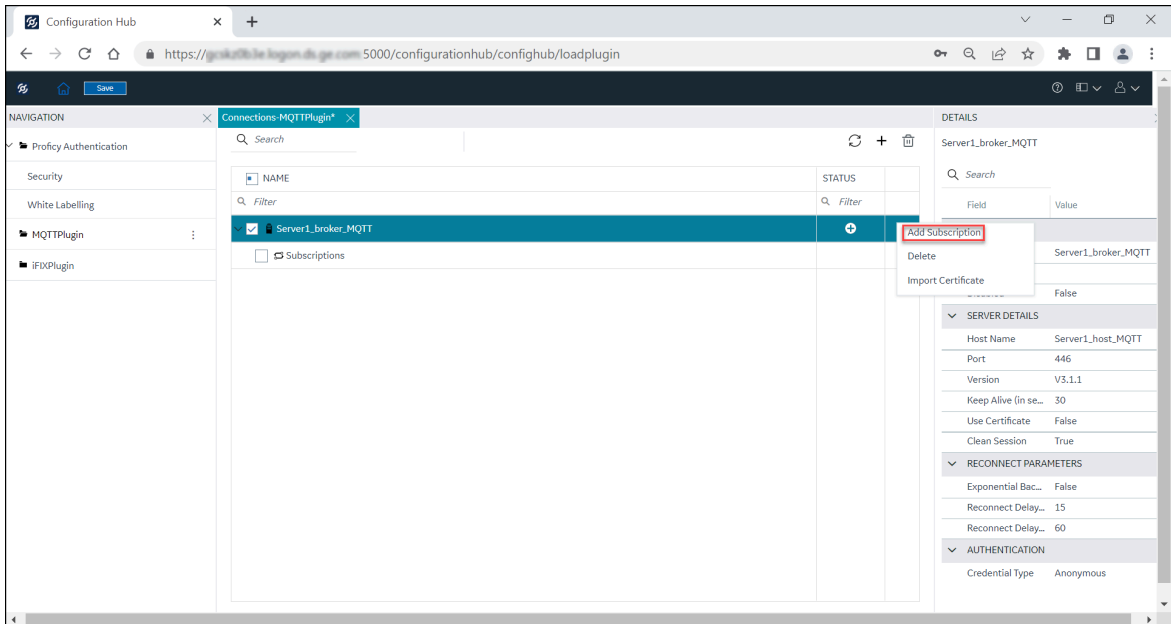
Note:

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

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

To add a Subscription to a Broker Connection:

1. Select **Add Subscription**.



The **New Subscription** dialog appears.

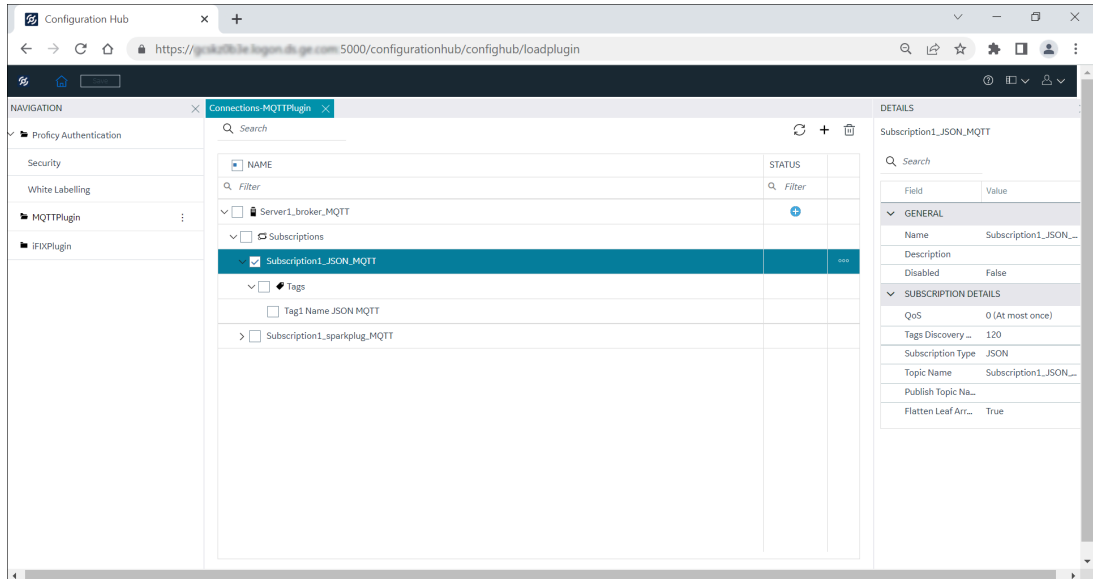
2. Select **Subscription Type** (JSON or Sparkplug Bv1.0).

- If you select JSON, enter a **Subscription Name**, and a **Topic Name**, and then click **Add**.



Note:

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



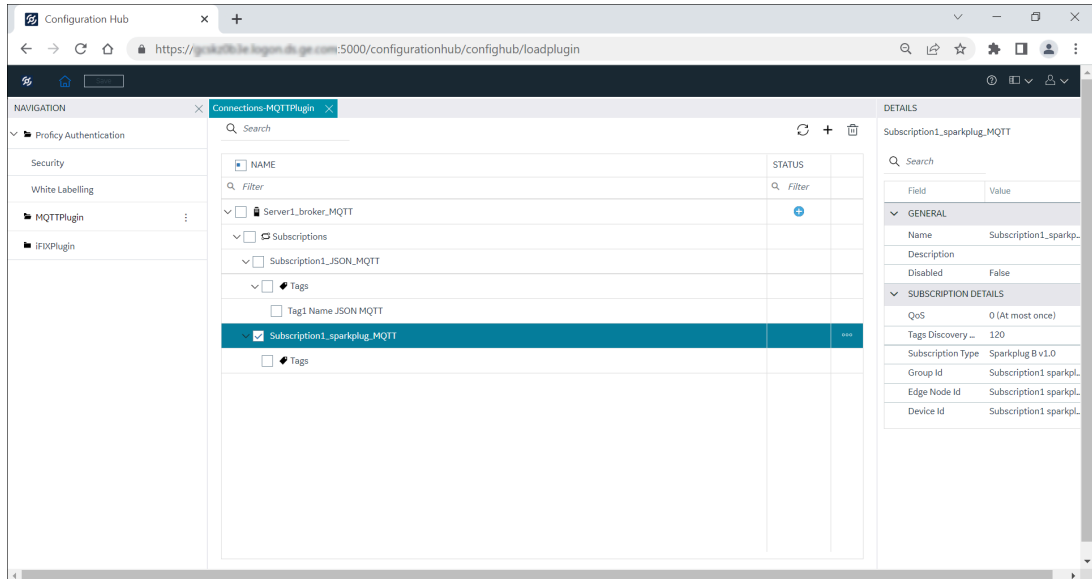
The JSON subscription is added to the broker connection. Click **Save**.

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



Note:

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









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



Table 52. Subscription Details



Field	Value
GENERAL	
Name	Enter a name for the subscription.
Description	Enter the description for the subscription.
Disabled	Enables or disables the subscription with the client: <ul style="list-style-type: none"> ▪ True: The subscription is disabled. ▪ False: The subscription is enabled.
SUBSCRIPTION DETAILS	
QoS	The Quality of Service (QoS) specifies three levels (QoS0, QoS1, and QoS2) at which the messages are delivered between the publishing client (sender) to the broker (receiver) and from the broker (sender) to the subscribing client (receiver). The QoS level selection provides easy communication even when the network is not reliable.


Field	Value
	<ul style="list-style-type: none"> ▪ QoS0: At most once <ul style="list-style-type: none"> ▪ No assurance of message delivery. ▪ Best efforts to deliver message only once. ▪ No acknowledgement receipt of the message from the receiver, message is not transmitted back to the sender, and the message is not stored. ▪ QoS1: At least once <ul style="list-style-type: none"> ▪ Ensures message delivery at least once to the receiver. ▪ Does not prevent delivering the messages multiple times to the receiver. ▪ Receiver acknowledges the message, and the sender stores the message. ▪ QoS2: Exactly once <ul style="list-style-type: none"> ▪ Ensures each message is delivered to the receiver only once. ▪ Receiver confirms the message delivery for each message from the sender. ▪ Requires two request/response flows between the sender and the receiver. ▪ Receiver acknowledges the message, and the sender stores the messages. ▪ Acknowledgement of delivered messages are received

Field	Value
	<p>by the sender until the published messages are available to use.</p> <div data-bbox="980 426 1419 646" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: QoS2 level is most reliable, but the quality of service is slower than QoS0 and QoS1.</p> </div>
<p>Tags Discovery Duration (in sec)</p>	<p>The Tags Discovery Duration is the duration period to fetch the tags. Tags fetched after the discovery are then added to the topic subscribed. This parameter helps the user to dynamically fetch the tags for a specific topic name and for a specific time duration. By default, the tags discovery duration is set to 120 seconds. You can modify the value as required.</p> <div data-bbox="899 1098 1419 1890" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note:</p> <ul style="list-style-type: none"> ▪ You can select Start Tag Discovery, Stop Tag Discovery, and Show Discovered Tags by using the overflow icon  , next to the subscription. ▪ If you select Start Tag Discovery, the Time Remaining in seconds is displayed. ▪ After the time remaining ends, or if you prematurely stop the tag discovery, select Show Discovered Tags to view the published tags. You can modify the Data Type and Read Write parameters. If modified, select the spe- </div>

Field	Value
	<div data-bbox="901 268 1421 464" style="border: 1px solid #0070c0; border-radius: 10px; padding: 10px;">  <p>cific tag, and then click Add to view the modified tag to the tags list for the topic subscribed.</p> </div>
Subscription Type	Displays the subscription type.
JSON Subscription	
Topic Name	<p>Enter a topic name to which you want to subscribe.</p> <p>Example:</p> <ul style="list-style-type: none"> ▪ Entering test1/# indicates that the client can listen to any topic that starts with test1/. <div data-bbox="982 932 1421 1423" style="border: 1px solid #0070c0; border-radius: 10px; padding: 10px; margin-top: 10px;">  <p>Note: The character # is a key word that has to be the last value. You can choose to enter any topic name in place of the key word # to differentiate multiple topics. That is, if you enter test1/test2, the client can listen explicitly to test1/test2.</p> </div> <ul style="list-style-type: none"> ▪ Entering test1/+temperature indicates that the client can listen to any topic name used in place of + to differentiate a single topic. <div data-bbox="982 1661 1421 1856" style="border: 1px solid #0070c0; border-radius: 10px; padding: 10px; margin-top: 10px;">  <p>Note: The character + is a key word between test1 and temperature. If you enter test1/</p> </div>

Field	Value
	<div data-bbox="980 260 1427 428" style="border: 1px solid #ccc; border-radius: 10px; padding: 10px;">  test2/temperature, the client can listen explicitly to test1/test2/temperature. </div>
Publish Topic Name	<p data-bbox="896 445 1421 701">Publish Topic Name, if provided by the user, will be used by the MQTT client when publishing the data; that is, when a user writes to a specific tag in the subscription using the OPC UA client, the data will be published with that specific publish topic name.</p> <div data-bbox="896 735 1421 1003" style="border: 1px solid #ccc; border-radius: 10px; padding: 10px;"> <p data-bbox="912 751 1042 793"> Note:</p> <p data-bbox="977 810 1404 974">If the Publish Topic Name field is left empty, then no data will be published to the broker even though the user modifies on the OPC UA side.</p> </div>
Flatten Leaf Arrays	<p data-bbox="896 1029 1421 1373">The Flatten Leaf Array parameter is used to consider the array tags as a whole or flatten the tag arrays (for example, if you have 100 elements in a JSON array, then you can choose to create a single array tag or, create 100 unique tags each pointing to an array element). By default, Flatten Leaf Arrays is set to True.</p> <ul data-bbox="961 1390 1404 1734" style="list-style-type: none"> <li data-bbox="961 1390 1404 1470">▪ True: A unique tag for each element of the array will be created. <li data-bbox="961 1478 1404 1734">▪ False: A single array tag for all the elements will be created. Also, the Configure Leaf Array Elements are enabled to configure the respective tag elements in TAG DETAILS section.

Field	Value
	<div data-bbox="980 260 1419 663" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;">  Note: The Configure Leaf Array Elements (that is, Leaf Array Rank, Leaf Array Dimensions, and Leaf Array Data Type) are able to be configured only if the Data Type is set to DataSet. </div>
Sparkplug Subscription	
Group Id	Enter a Group Id for the topic subscribed.
Edge Node Id	Enter an Edge Node Id for the topic subscribed.
Device Id	Enter a Device Id for the topic subscribed. The topic device id is the identification of a device attached to the MQTT Edge node. The device id field is optional. <div data-bbox="899 1150 1419 1507" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;">  Note: <ul style="list-style-type: none"> ▪ If the Device ID field is left empty, it will be considered an Edge node. ▪ If you enter the Device ID field, it will be considered as a Device node. </div>

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

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

Tags are added under the Subscriptions to store specific data from the subscription. Refer to [Add Tags to Subscription \(on page 1418\)](#) to add Tags under each Subscription.

JSON Supported Payload

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

The following are examples of JSON supported payloads:

Simple JSON

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

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

Nested JSON

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

In the above payload, the tags created are: *IntVal*, *DoubleVal*, *BoolVal*, *StringVal*, *parent/child*, *FirstLevel1Obj/IntVal*, *FirstLevel1Obj/DoubleVal*, *FirstLevel1Obj/BoolVal*, *FirstLevel1Obj/StringVal*, *FirstLevel1Obj/SecondLevelObj/IntVal*, *FirstLevel1Obj/SecondLevelObj/DoubleVal*, *FirstLevel1Obj/SecondLevelObj/BoolVal*, and *FirstLevel1Obj/SecondLevelObj/StringVal*.

- The `Is Hierarchical` parameter in the *parent/child* tag must be set to **False** to indicate that it is not a nested level tag.
- The `Is Hierarchical` parameter in the tags starting with *FirstLevel1Obj* and *FirstLevel1Obj/SecondLevel1Obj* must be set to **True** to indicate that they are nested level tags. The '/' is considered a delimiter that separates the first level *parent* and the second level *child* tags.

JSON Payload with Arrays

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

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

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

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

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

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

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

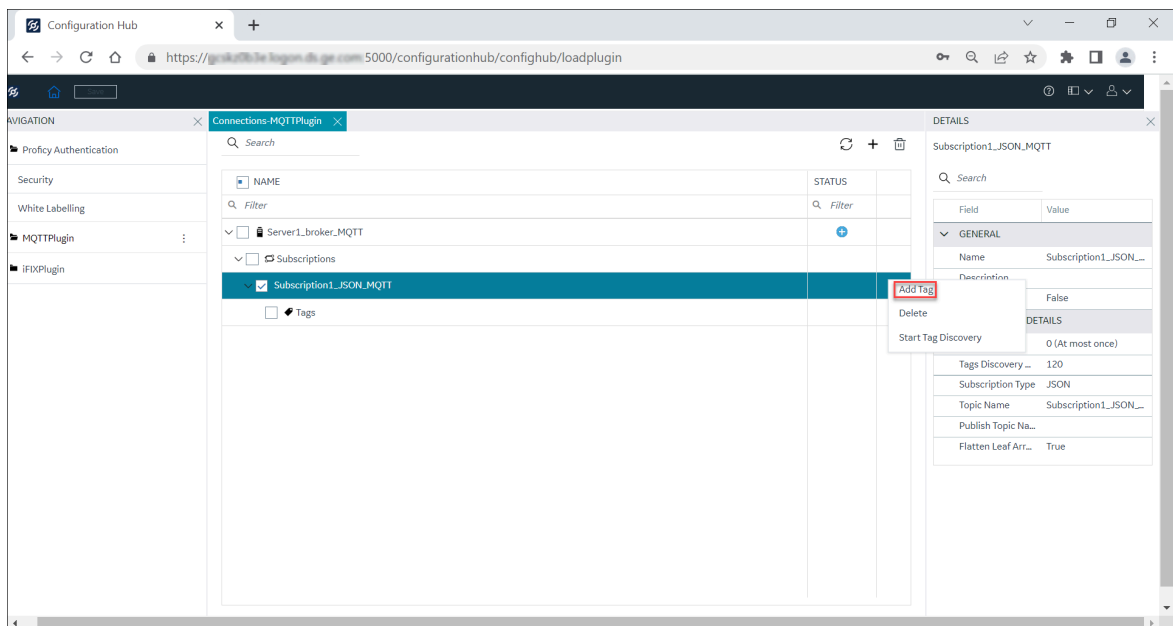
Add Tags to Subscription

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

To add Tags for a JSON or Sparkplug Subscription:


Tag for JSON Subscription

1. Select **Add Tag**.



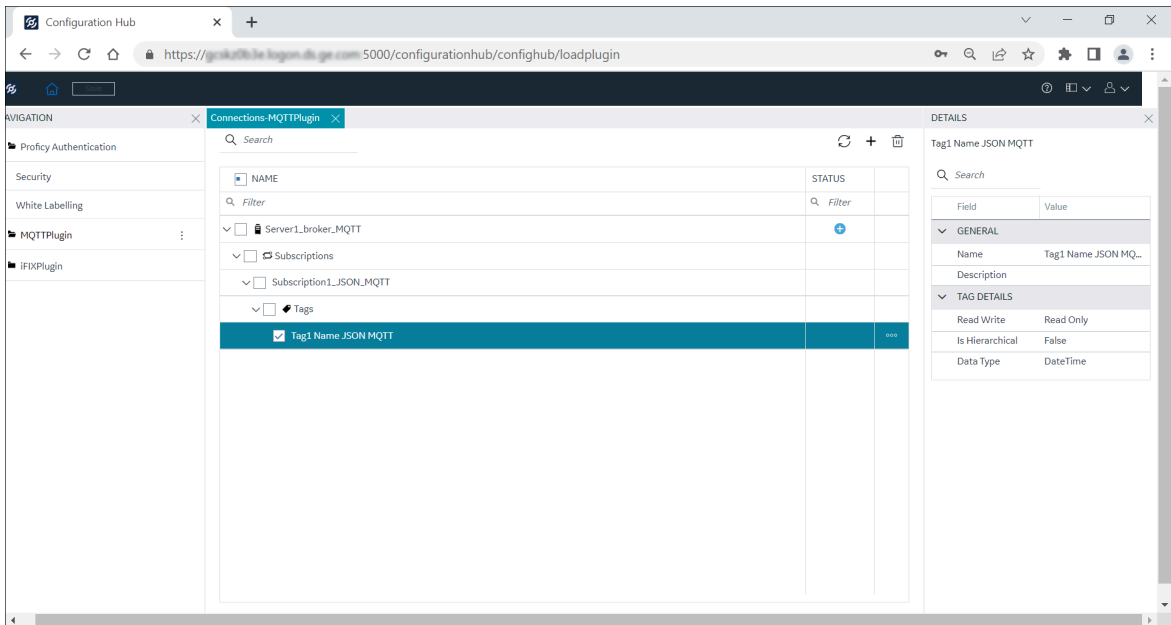
The **New Tag** dialog appears.

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


 **Note:**

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

3. Click **Add**.



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

 **Note:**

You can modify the Data Type value for the JSON Subscription.

Table 53. JSON Tag Details

Field	Value
GENERAL	

Table 53. JSON Tag Details (continued)

Field	Value
Name	Enter a tag name.
Description	Enter the tag description.
TAG DETAILS	
Read Write	<p>You can set the value to Read Only or Read and Write.</p> <p>Read Only: You can only read the tag values from the OPC UA client.</p> <p>Read and Write: You can read and write/modify the tag values from the OPC UA client.</p>
Is Hierarchical	<p>Is Hierarchical parameter helps to indicate whether the tag is at the root level of a JSON object or at a nested level. Nested tags are represented using a complete tag name delimited using a forward slash (/).</p> <p>By default, this parameter is set to False.</p> <ul style="list-style-type: none"> • True: It is a nested tag. • False: It is not a nested tag. <p>For a JSON object:</p> <ul style="list-style-type: none"> • <pre>{ "level1":{ "level2":68 } }</pre> <p>If you want to refer to the level2 tag embedded in a level1 object, the tag name will be represented as level1/level2 where / is the delimiter. The Is Hierarchical parameter</p>

Table 53. JSON Tag Details (continued)

Field	Value
	<p>must be set to True to indicate that it is a nested tag.</p> <ul style="list-style-type: none"> <pre>{ "level1/level2": "my string" }</pre> <p>If you want to refer to a level1/level2 tag at the root level, then the tag name will be represented as level1/level2. The Is Hierarchical parameter must be set to False to indicate that it is not a nested tag.</p>
Data Type	You can select the data type value from the list of available data type entries.



Note:

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



▼ SUBSCRIPTION DETAILS

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

▼ TAG DETAILS

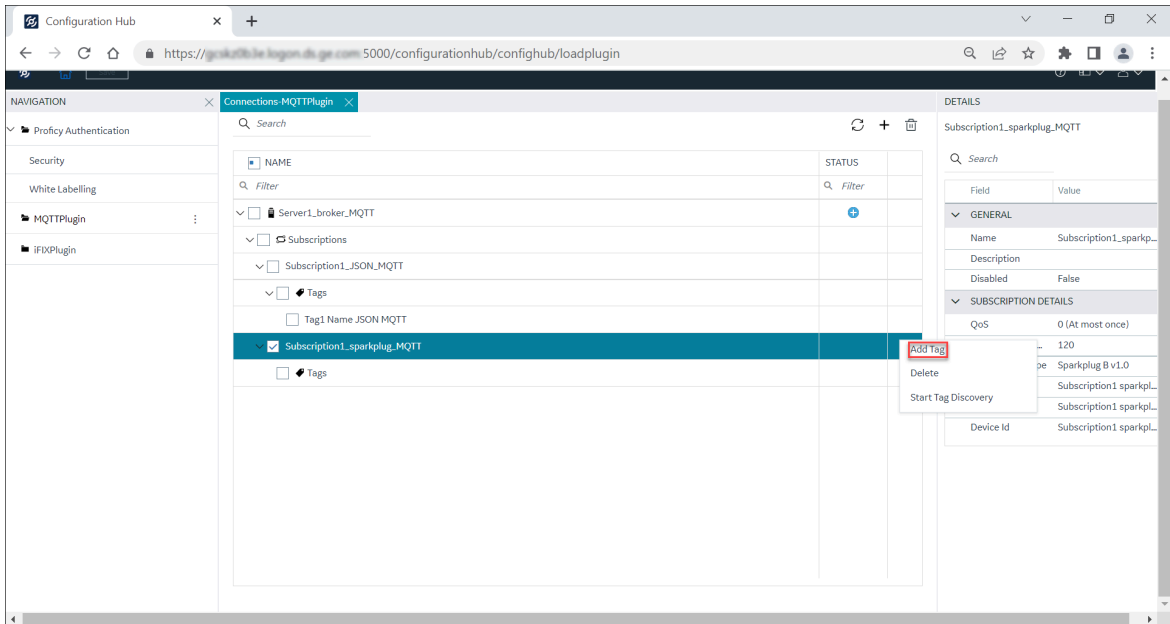
Read Write	Read Only
Is Hierarchical	False
Data Type	DataSet
Leaf Array Rank :	1
Leaf Array Dimensions	[1]
Leaf Array Data Type	["Int8"]
Configure Leaf Array Elements	

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

Leaf Array Elements	Description
Leaf Array Rank	<p>The Leaf Array Rank value is the number of dimensions of an array.</p> <ul style="list-style-type: none"> • 1 - One dimensional • 2 - Two dimensional <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;">  Note: The Leaf Array Rank is set up to two ranks only. </div>
Leaf Array Dimensions	<p>Number of elements in each dimension available corresponding to the Leaf Array Rank number.</p>
Leaf Array Data Type	<p>Select the Data Type as required.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;">  Note: When you select the Variant data type, the Leaf Array Data Types table is displayed with the Index of Elements and its Data Types. That is, you will be populated with the heterogeneous data types in the multi-dimensional array. You can modify the data type per each index in an array. </div>

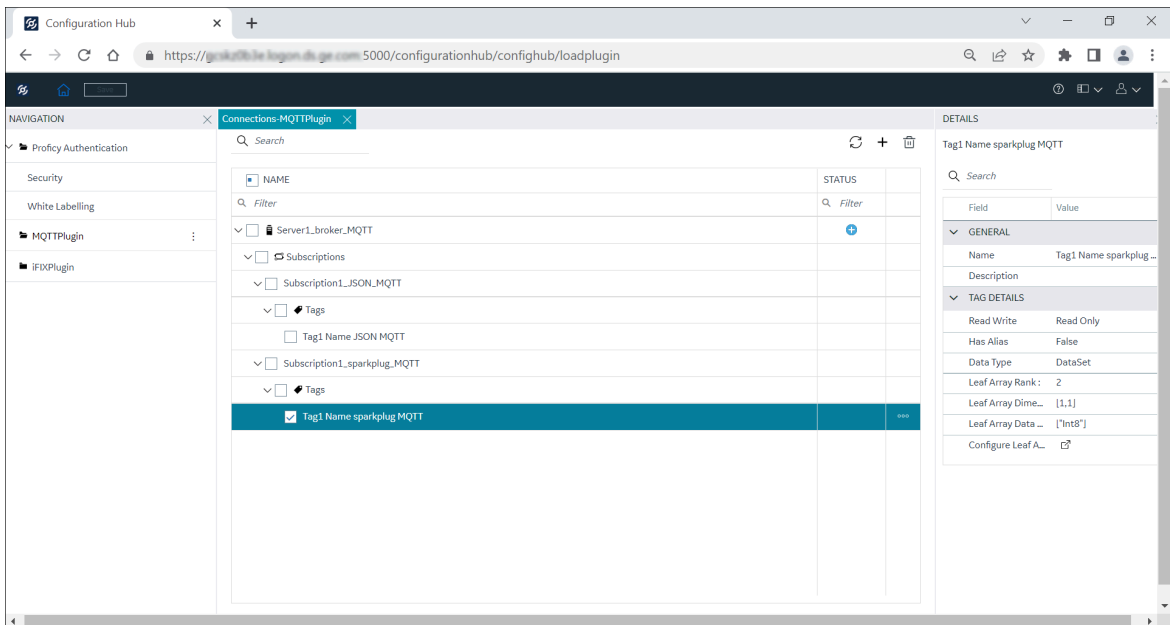
Tag for Sparkplug Subscription

1. Select **Add Tag**.



The **New Tag** dialog appears.

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



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

**Note:**

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

Table 54. Sparkplug Tag Details

Field	Value
GENERAL	
Name	Enter a tag name.
Description	Enter the tag description.
TAG DETAILS	
Read Write	<p>You can set the value to Read Only or Read and Write.</p> <p>Read Only: You can only read the tag values from the OPC UA client.</p> <p>Read and Write: You can read and write/modify the tag values from the OPC UA client.</p>
Has Alias	<p>Has Alias is an integer value that is used as a substitute name to reduce the long and repeated usage of the same tag name. By default, this parameter is set to False.</p> <ul style="list-style-type: none"> • True: The Alias field is displayed. Enter the publisher provided integer value in the Alias field. • False: The tag has no Alias name.
Data Type	Displays the data type.

**Note:**

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

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

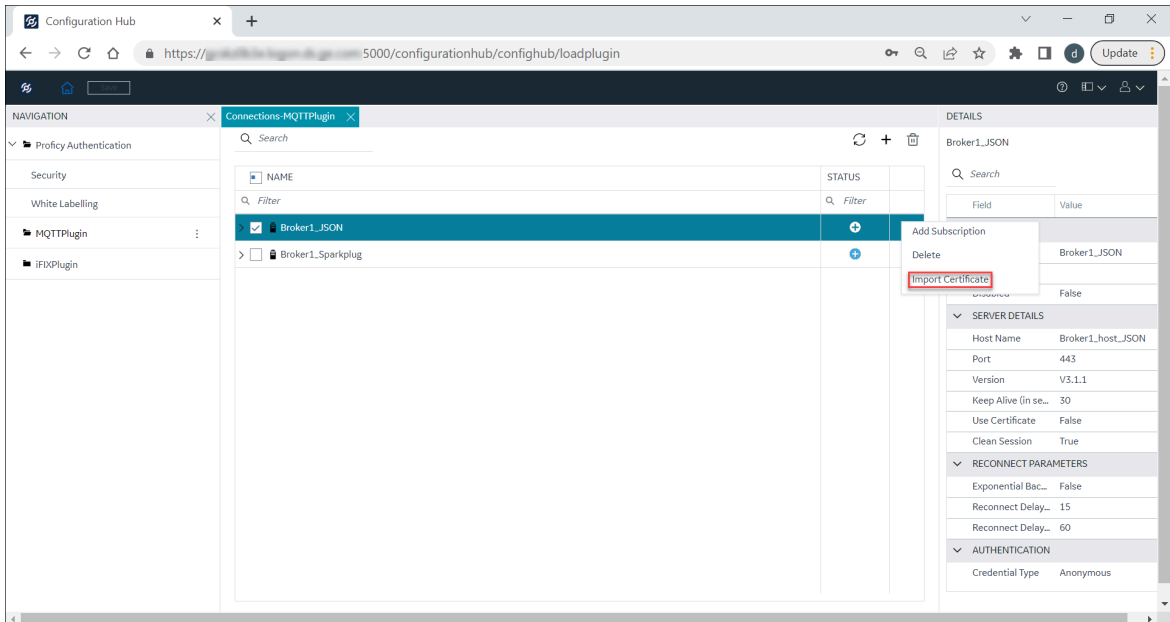
Refer to the above table for more information on Leaf Array Elements.

Secure Connection with Broker

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

To import the broker certificate:

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



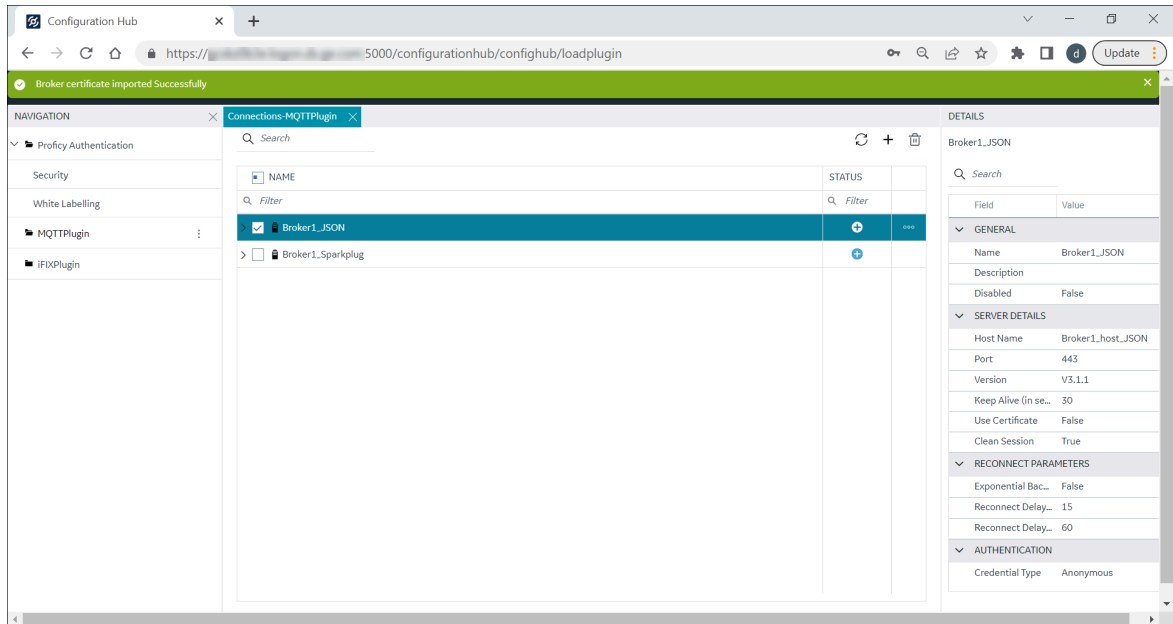
The **Import Service Certificate** dialog appears.

2. Click **Browse** and navigate to the source location of the broker certificate.

3. Double-click the broker root certificate.
4. Click **View** to view the certificate details.

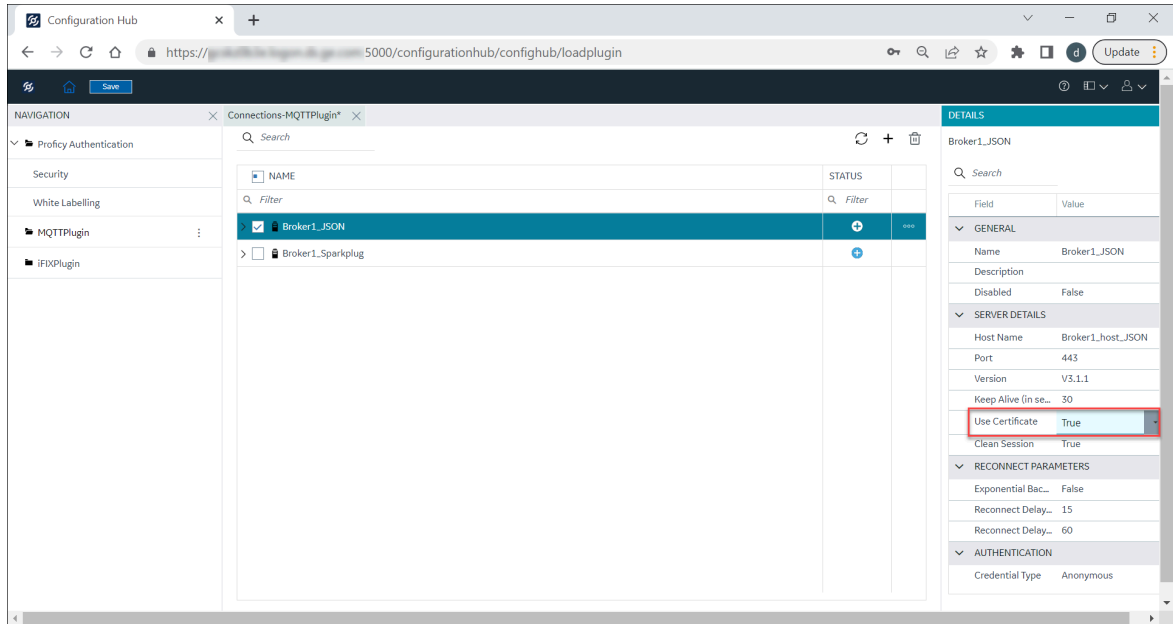
The **Certificate Details** page appears.

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



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

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

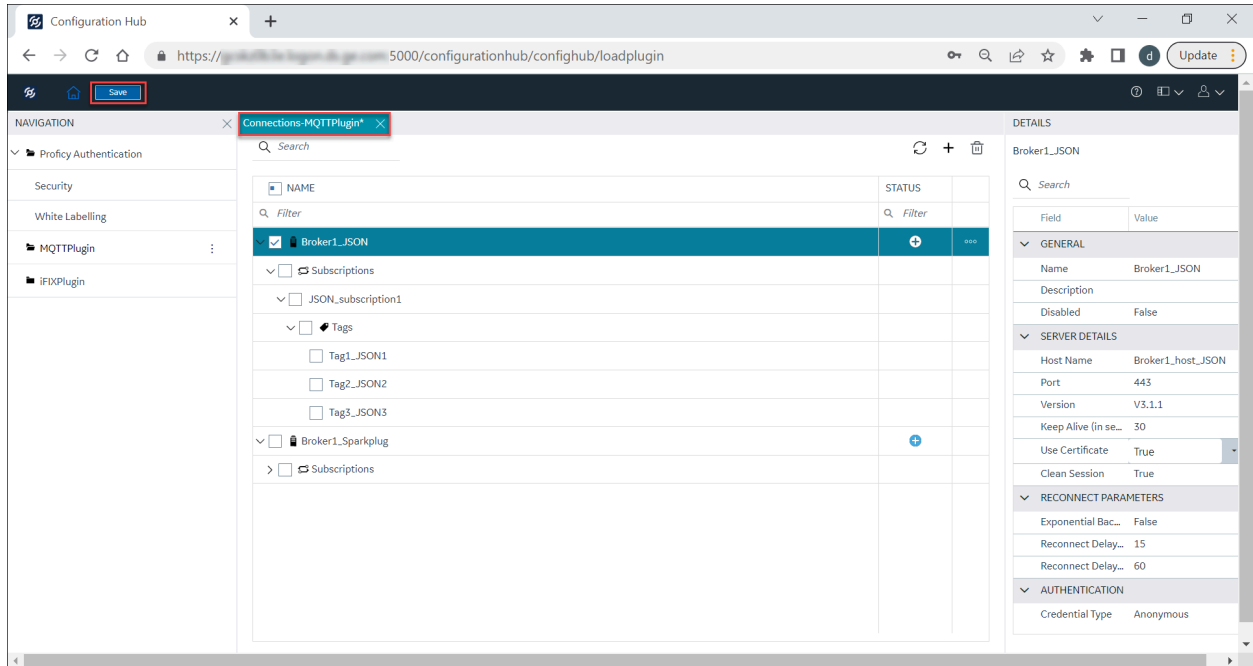


9. Click **Save** and then **Publish**.


Refer to [Save and Publish \(on page 1427\)](#) for more details.

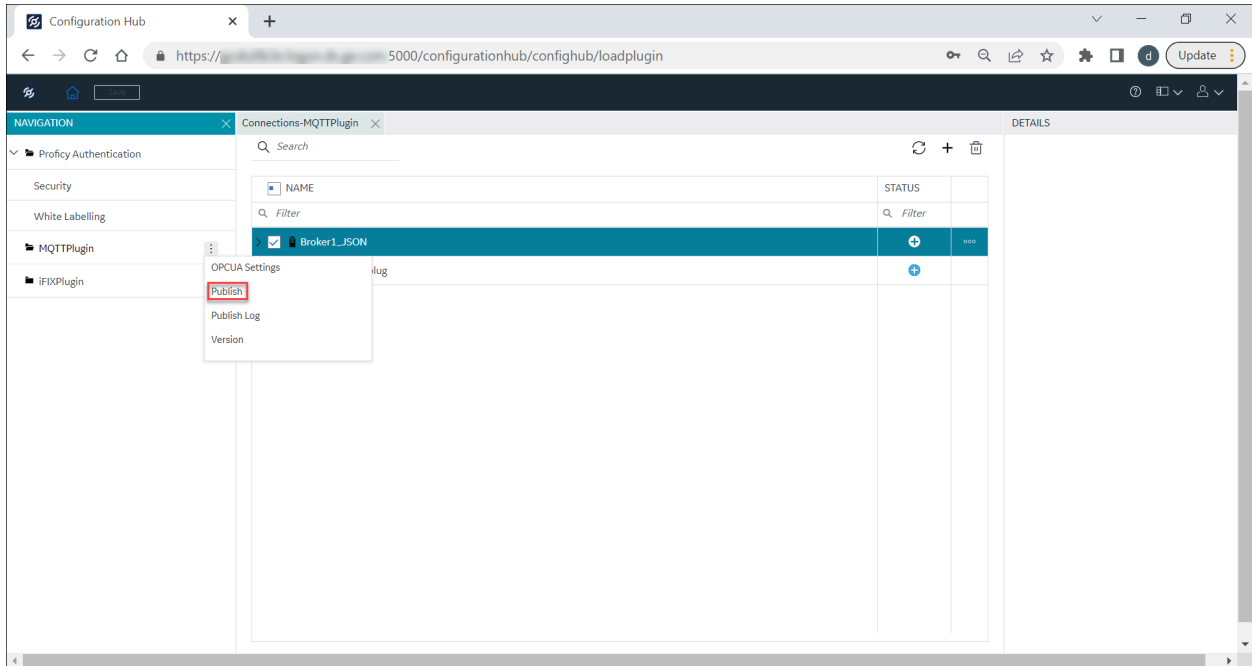
Save and Publish

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



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

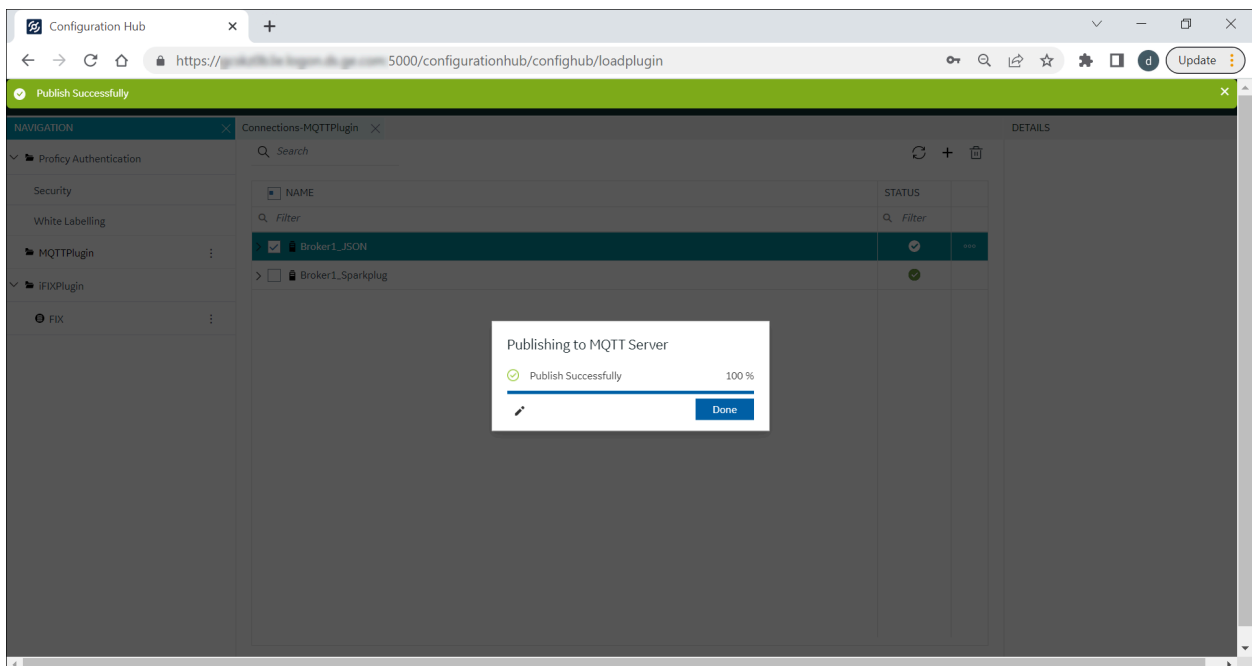
When you are ready to apply the changes to the running system, select **Publish** from the MQTT connection plugin overflow icon  to push the changes to the server.




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

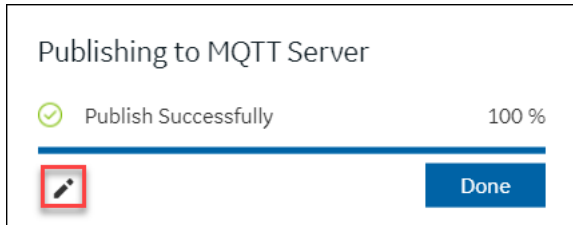
The publish operation begins, after you click the publish button. It may take a while depending on the number of tags being published to the active MQTT node.

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




Publish Log and Version

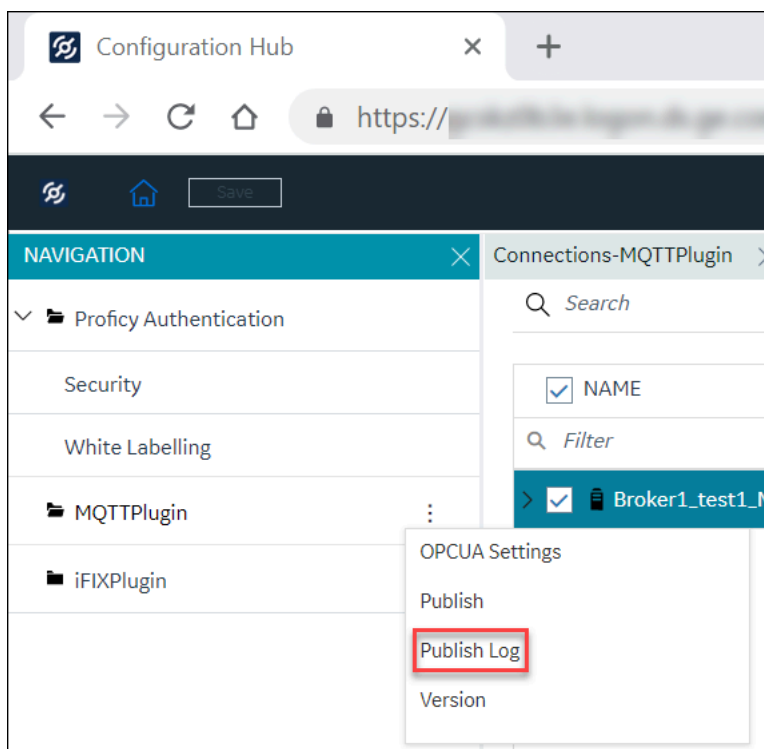
After you publish the MQTT plugin changes, you can directly view the published log reports by clicking the  icon.



Publish Log

To view the publish log reports:

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



The **Publish Report** dialog appears.

Publish Report

MQTT OPC UA

Type ▼	Operati... ▼	Broker Name ▼	Subscription Na... ▼	Timestamp (YY-MM-... ▼
🔍 <i>Filter</i>	🔍 <i>Filter</i>	🔍 <i>Filter</i>	🔍 <i>Filter</i>	🔍 <i>Filter</i>
✔	Add	Broker1_test1_...	Sub3_JSON_test3...	2023-02-07 16:58:17

Download Log
Close

Table 55. MQTT Publish Log Report

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

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

Publish Report

MQTT **OPC UA**

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

Download Log
Close

Table 56. OPC UA Publish Log Report

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



Note:

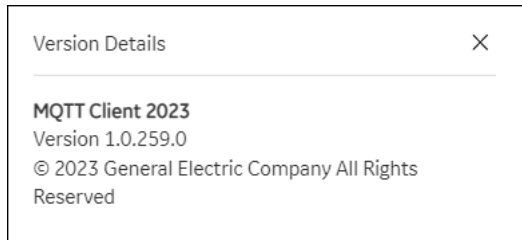
- You can click the icon to filter the data as required.
- You can click the **Download Log** button to download the log information.

**Important:**

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

Version

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



The **Version Details** dialog appears.

The MQTT Client application version details are displayed.

OPC UA

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


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

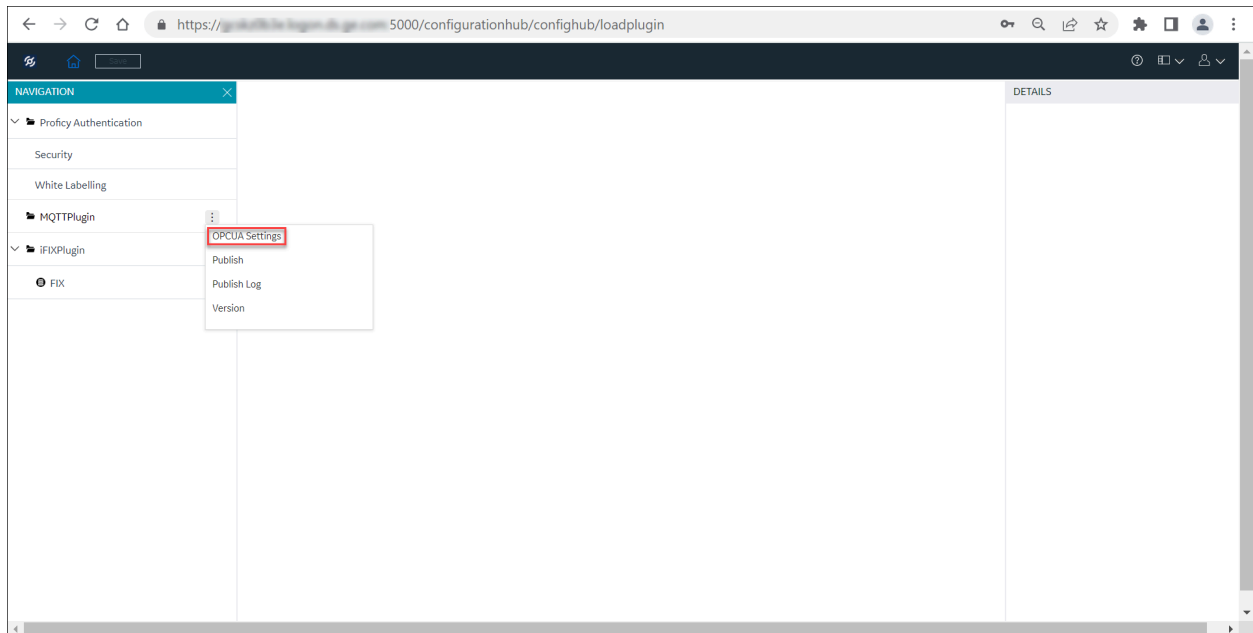
The MQTT client application is used as a two-way data communication. You can also write from OPC UA clients to MQTT clients or from IIoT devices.

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

Refer to [OPC UA Settings \(on page 1434\)](#) to configure the OPC UA settings page.

OPC UA Settings

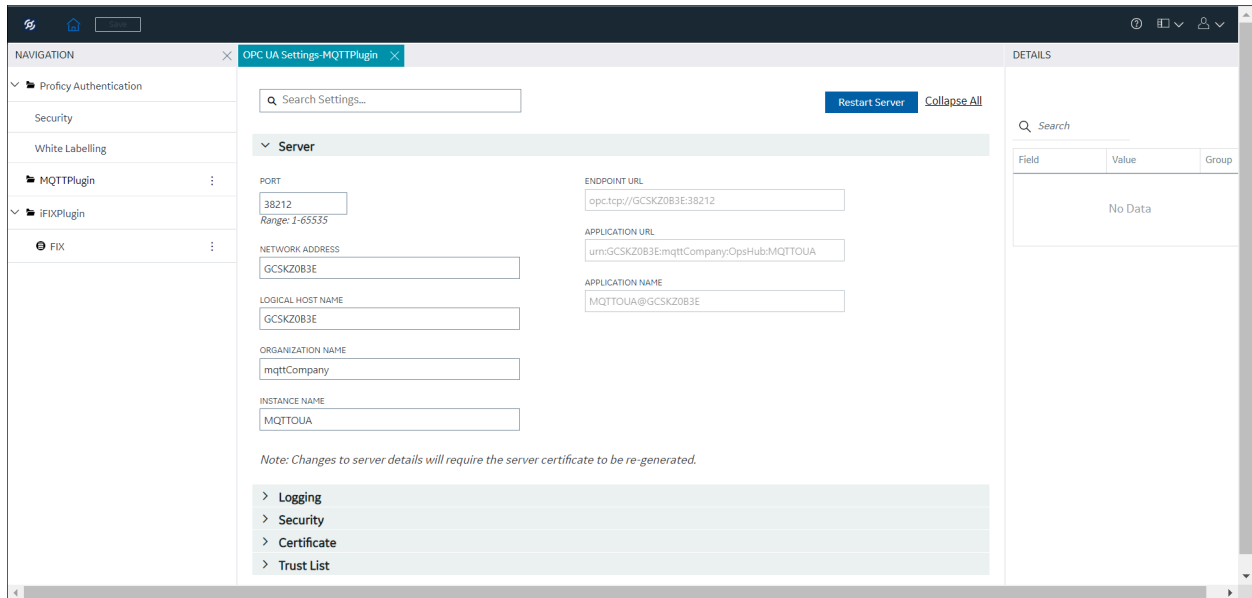
After establishing broker connections, subscriptions, and tags information, click the overflow icon  of the MQTT plugin, and then select **OPC UA Settings** to connect to the OPC UA server and establish the OPC UA client connection.



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

- Server
- Logging
- Security
- Certificate
- Trust List

Server




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

Table 57. OPC UA Server Details

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

Table 57. OPC UA Server Details (continued)

Field	Description
	<div data-bbox="820 325 1421 1108" style="border: 1px solid #0070c0; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p> Note:</p> <ul style="list-style-type: none"> • An endpoint is a physical address available on a network that allows clients to access one or more services provided by a server. • An OPC UA Endpoint URL (Uniform Resource Locator) is a formatted text string that consists of three or four parts (substrings): <ol style="list-style-type: none"> 1. Network protocol ((must be opc.tcp (case sensitive))). 2. Host name or IP address. 3. Port number. 4. (Optional) File or resource location. </div> <p>The OPC UA specific URL, it shows as:</p> <pre data-bbox="831 1199 1409 1241" style="background-color: #f0f0f0; padding: 5px;">opc.tcp://hostname:38212/<file or resource location></pre>
APPLICATION URL	The unique address reference on the Internet. Also, referred to as the web address.
APPLICATION NAME	Name of the application.

**Note:**

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

OPC UA Server successfully restarted.

Logging

The screenshot shows the configuration interface for the MQTTPlugin. The 'Logging' section is expanded, showing the following settings:

- ENABLE LOGGING:** A toggle switch is turned on (Enabled).
- NUMBER OF LOG FILES (MAX 100):** A text input field containing the value '5'.
- MAXIMUM ENTRIES PER LOG FILE:** A text input field containing the value '100000'.
- OPTIMIZE LOG WRITES:** An unchecked checkbox.
- APPLICATION TRACE LEVEL:** A drop-down menu set to 'Error'.
- STACK TRACE LEVEL:** A drop-down menu set to 'Error'.
- LOG FILE PATH:** A text input field containing the path '<Mqtt Client Installation Drive>\Program Files\Proficy\MQTTClient\Lo...'

On the right side of the interface, there is a 'DETAILS' panel with a search bar and a table with columns 'Field', 'Value', and 'Group'. The table currently displays 'No Data'.

Logging helps you to record the error reports. The logging section displays the number of log files, maximum entries per log file, application trace level, stack trace level, and log file path fields. You can select the application level and stack level log files as required from the respective drop-down list.

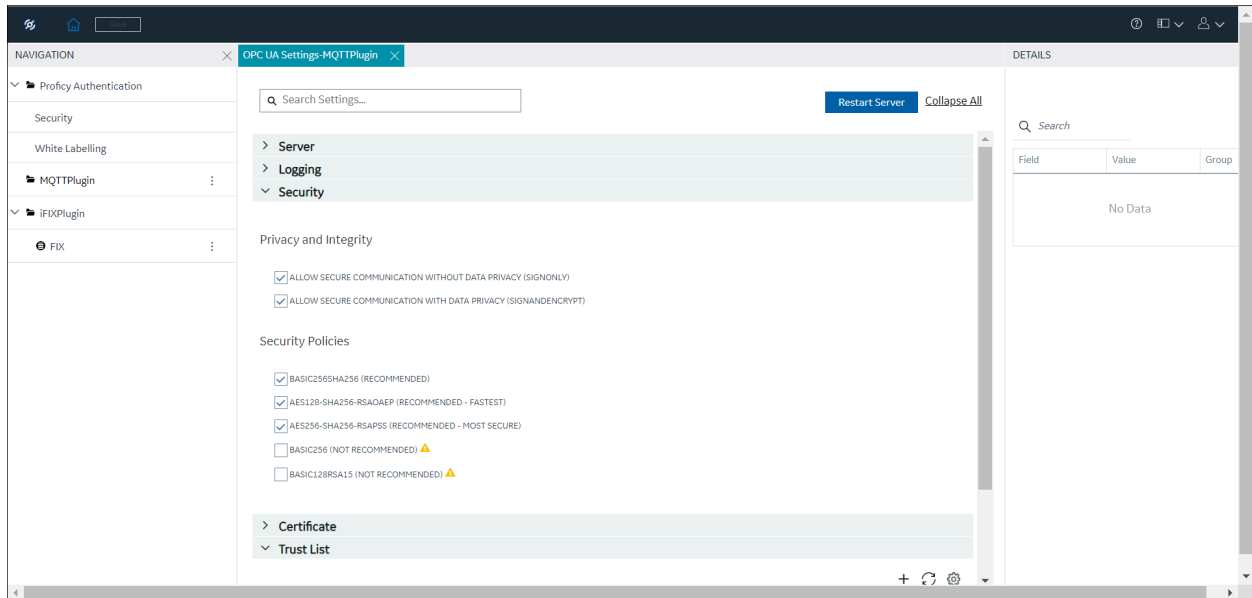
**Note:**

You can enable or disable logging using the toggle switch in the **Logging** section.

Table 58. Logging Configuration

Field	Description
NUMBER OF LOG FILES (MAX 100)	The number of files for log backups (range is from 1 to 100).
MAXIMUM ENTRIES PER LOG FILE	The number of entry per log file (range is from 0 to 1000000000).
APPLICATION TRACE LEVEL	<p>You can trace the errors or warnings to generate the trace messages.</p> <p>From the application trace level, you can select None, Error, Errors and Warnings, Error, Warnings and Information or, Detailed (may impact performance) as required.</p>
STACK TRACE LEVEL	<p>You can trace the information about frequently used operations. The stack trace helps to find out the debugs in an operation and to figure out the problems for any bug generated in the operation.</p> <p>From the application trace level, you can select None, Error, Errors and Warnings, Error, Warnings and Information or, Detailed (may impact performance) as required.</p>
LOG FILE PATH	<p>Location of the log file.</p> <pre data-bbox="818 1346 1414 1465"><Installation Location Drive>\Program Files\Proficy\MQTTClient\Logs\OpcUa-Server.log</pre>
<input type="checkbox"/> OPTIMIZE LOG WRITES	Select the Optimize Log Writes check box to optimize log events, use structured logging, exclude sensitive information, and to store the data.

Security



Use the check boxes in the **Privacy and Integrity** and **Security Policies** sections to ensure data is secured and protected from unauthorized access. Only authorized users can access the data to view and modify as per user access privileges.

Privacy and Integrity	
ALLOW SECURE COMMUNICATION WITHOUT DATA PRIVACY (SIGNONLY)	Encryption is still used in the initial handshake. This mode is not appropriate when legal requirements prohibit the use of encryption.
ALLOW SECURE COMMUNICATION WITH DATA PRIVACY (SIGNANDENCRYPT)	All messages are signed and encrypted.
Security Policies	
BASIC256SHA256 (RECOMMENDED)	For configurations that require high security.
AES128-SHA256-RSAOAE (RECOMMENDED - FASTEST)	For configurations that require high speed with average security.
AES256-SHA256-RSAPSS (RECOMMENDED - MOST SECURE)	For configurations that require very high security.

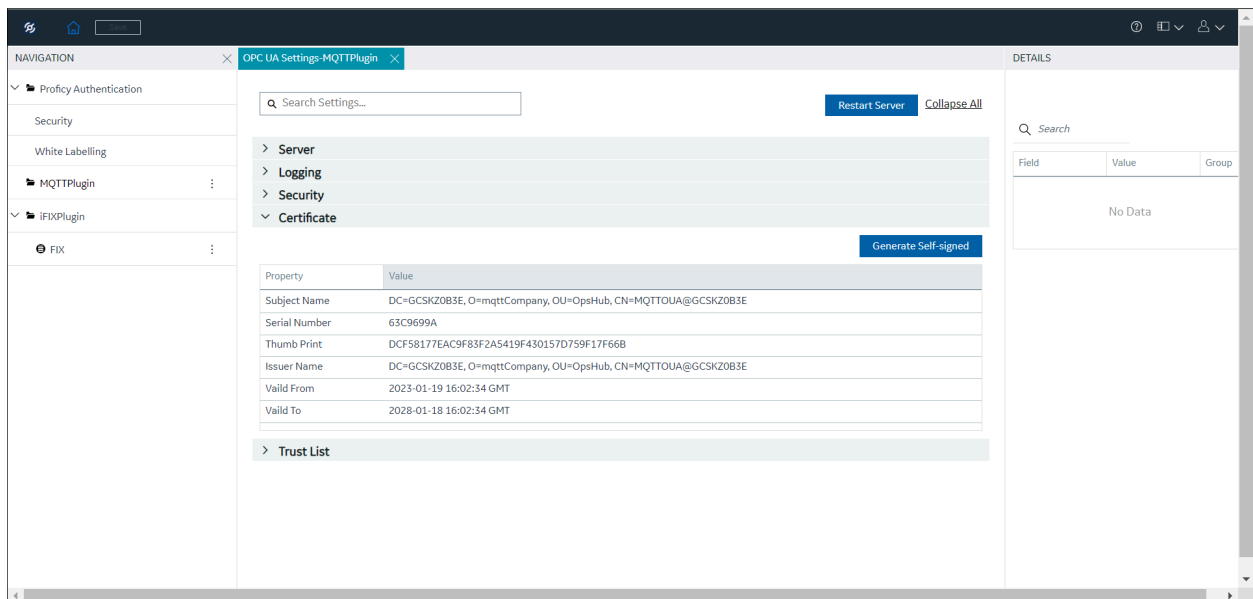


Note:

- BASIC256 and BASIC128RSA15 are deprecated due to vulnerability and theoretical issues.
- You can verify the security permissions at the following location.

```
<Installation Location Drive>\Program Files\Proficy\MQTTClient
  \ServerConfig.xml
```

Certificate



To establish the trusted connection with the OPC UA client, you must generate the self-signed certificate.

1. Select **Generate Self-signed** certificate.
2. A prompt message appears. Click **Yes** to regenerate the server certificate.



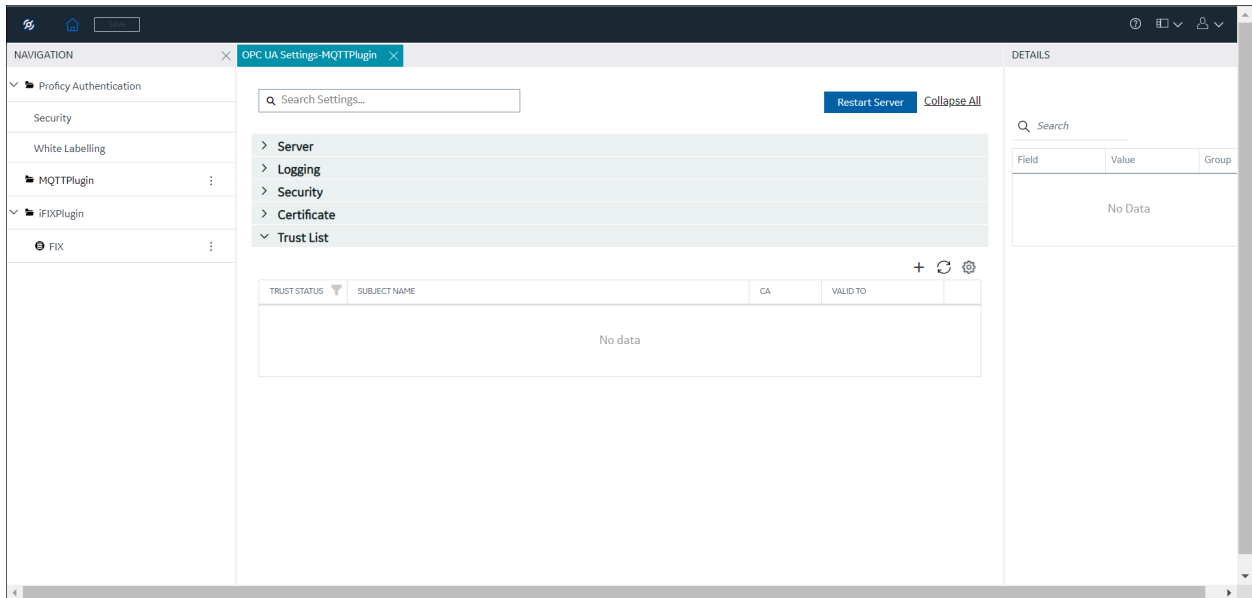
Important:

All previous server settings will be removed, and new details are updated.

OPC UA certification created successfully message appears.



3. Select **Restart Server** to use the certificate. The new server certificate details are populated in the **Certificate** section.
4. To view the server certificate, navigate to <Install Location Drive>\Proficy\MQTTClient\UA\pkiserver\own\certs.

Trust List



The trust list will display the certificate status (trusted and rejected) and its validity period. Use the overflow icon **⋮** and select **Trust** to trust the rejected certificate, or select **Reject** to reject the already trusted certificate, and select **Delete** to delete the certificate from the trust list.

If a client certificate is not displayed in the Trust List table:

- Select the **Refresh**  icon. This will load the client certificate to the Trust List table or,
- Select the **Add Certificate**  icon. The **Import Trust Certificate** dialog appears. You can then browse to the client certificate location and Trust the certificate.

After the OPC UA settings information is saved, you can select the overflow icon **⋮** of the MQTT plugin and select **Publish** to publish the changes to the MQTT server. Refer to [Save and Publish \(on page 1427\)](#) for more details.

Chapter 8. Settings

Switch Users

1. Locate the user button on the top right of the toolbar.
2. Select Logout.
3. Login again under the new user name.



Modify Layout

You can modify the layout in Configuration Hub by:

- Using the split bar to resize panels.
- Open or closing tabs.
- Open or closing panels.
- Resizing the browser window to resize all open panels.

Host Name Changes

This section describes the steps to follow if you need to change the host name of the Configuration Hub server or the iFIX server (or both when the Configuration Hub server is local to the iFIX server). Be aware that the iFIX plugin will only be accessible in Configuration Hub if the certificates are valid. If the host name is changed (in either Configuration Hub or iFIX) and you did not update the certificates, then iFIX plugin may not be accessible in Configuration Hub, as the certificates are not valid anymore. Use the following steps to update your certificates.

Steps for Self-Signed Certificate Creation Due to Configuration Hub Server Host Name Change

During the Configuration Hub install, self-signed certificates are created and stored in the C:\Program Files (x86)\Proficy\ConfigurationHub\ConfigHubPki folder. The Configuration Hub server certificates are stored in the C:\Program Files (x86)\Proficy\ConfigurationHub\Web\conf directory. If you want to change the web server name after the Configuration Hub install, you need to update the self-signed certificates.

Use the following steps to update your self-signed certificates for Configuration Hub:

1. Either remove or backup the certificate files in C:\Program Files (x86)\Proficy\ConfigurationHub\ConfigHubPki folder.
2. Open a command prompt as an administrator in the C:\Program Files (x86)\Proficy\ConfigurationHub\ConfigHubPki directory.
3. Enter the following command to create new self-signed certificates:

```
restart_confighub.bat "C:\Program Files (x86)\Proficy\ConfigurationHub" "C:\Program Files  
(x86)\Proficy\ConfigurationHub\Web" 5678 4890 htclab.ge.com
```

where "C:\Program Files (x86)\Proficy\ConfigurationHub" is the Configuration Hub install directory, C:\Program Files (x86)\Proficy\ConfigurationHub\Web is the directory where the Configuration Hub server resides, 5678 is the Configuration Hub authentication service port (Not used any more), and 4890 is the Configuration Hub server port.

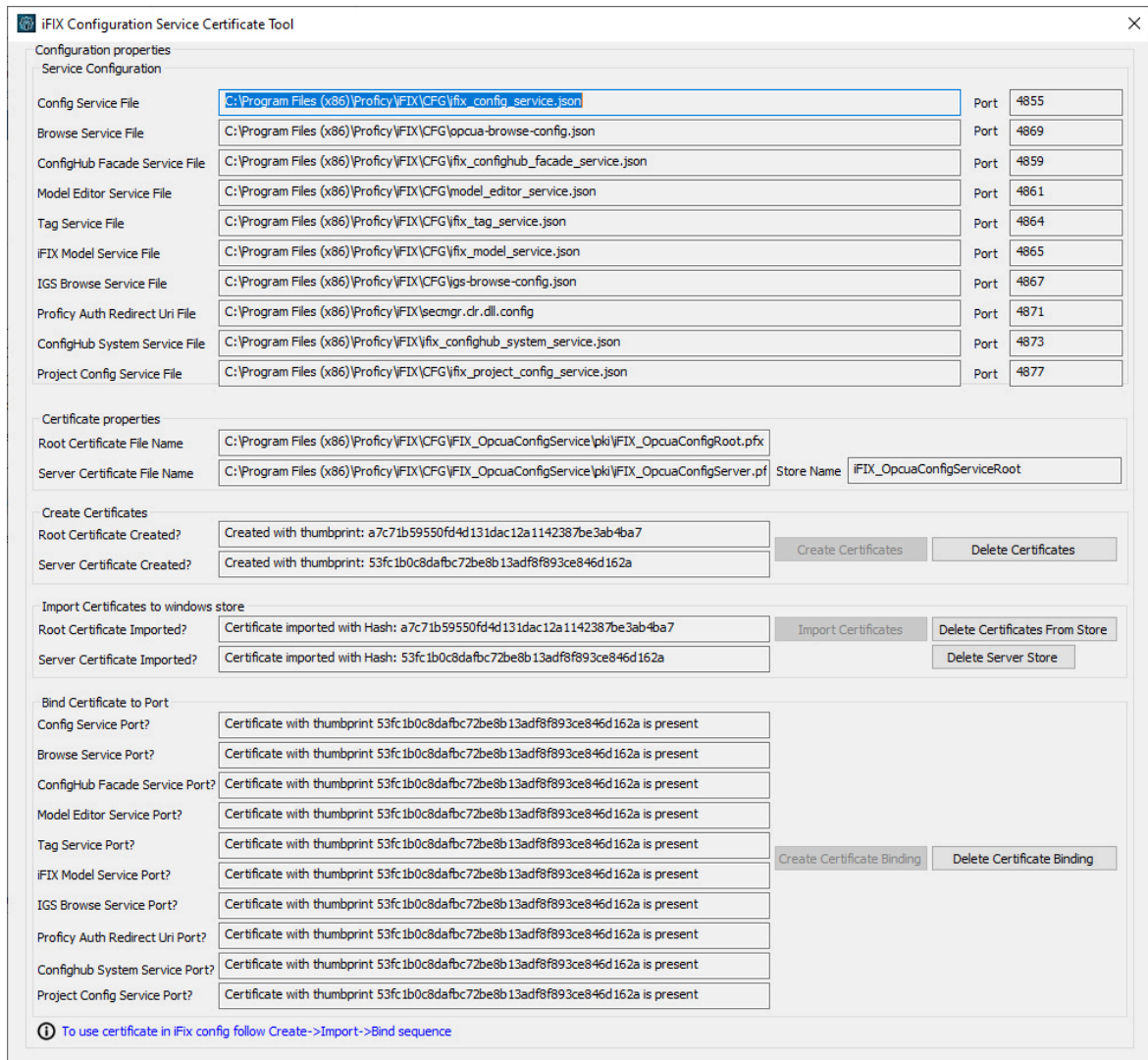
4. Copy the server_cert.crt and server_cert.key files the from C:\Program Files (x86)\Proficy\ConfigurationHub\ConfigHubPki folder to the C:\Program Files (x86)\Proficy\ConfigurationHub\Web\conf folder.
5. Restart the computer.

Steps for Self-Signed Certificate Creation Due to iFIX Server Host Name Change

On the iFIX side, during install, self-signed certificates are created and stored in the C:\Program Files (x86)\Proficy\iFIX\CFG\iFIX_OpcuaConfigService\pki folder. The iFIX HTTPD server certificates are stored in the C:\Program Files (x86)\Proficy\iFIX\web\conf directory. When the host name changes you will also need to update your iFIX certificates.

Use the following steps to update your self-signed certificates for iFIX:

1. Open iFixConfigServiceCertTool.exe as an administrator. This tool is found in the C:\Program Files (x86)\Proficy\iFIX\ folder. The iFIX Configuration Service Certificate Tool appears, similar to the following figure.



2. Click Delete Certificates, and then click Delete Certificate Binding.
3. From the Windows File Explorer, remove or backup the certificate files in C:\Program Files (x86)\Proficy\iFIX\CFG\iFIX_OpcuaConfigService\pki directory.
4. From iFIX Configuration Service Certificate Tool, create the new certificates by clicking on the Create Certificates button.
5. After the new set of certificates are created, ensure that the certificate thumbprint is different in the iFIX Configuration Service Certificate Tool. If they are not different, the new certificates are not created. The following figure shows an example of the before and after:

Before host name change the certificate thumbprint from utility is:

Create Certificates	
Root Certificate Created?	Created with thumbprint: 036d4b98ec62bb34bde7bc4dbb3939486c4d7f48
Server Certificate Created?	Created with thumbprint: ec46567e1aa811fcdc003eea72387bfe1b4e4fb6
<input type="button" value="Create Certificates"/> <input type="button" value="Delete Certificates"/>	

After the new certificate creation, the thumbprint is:

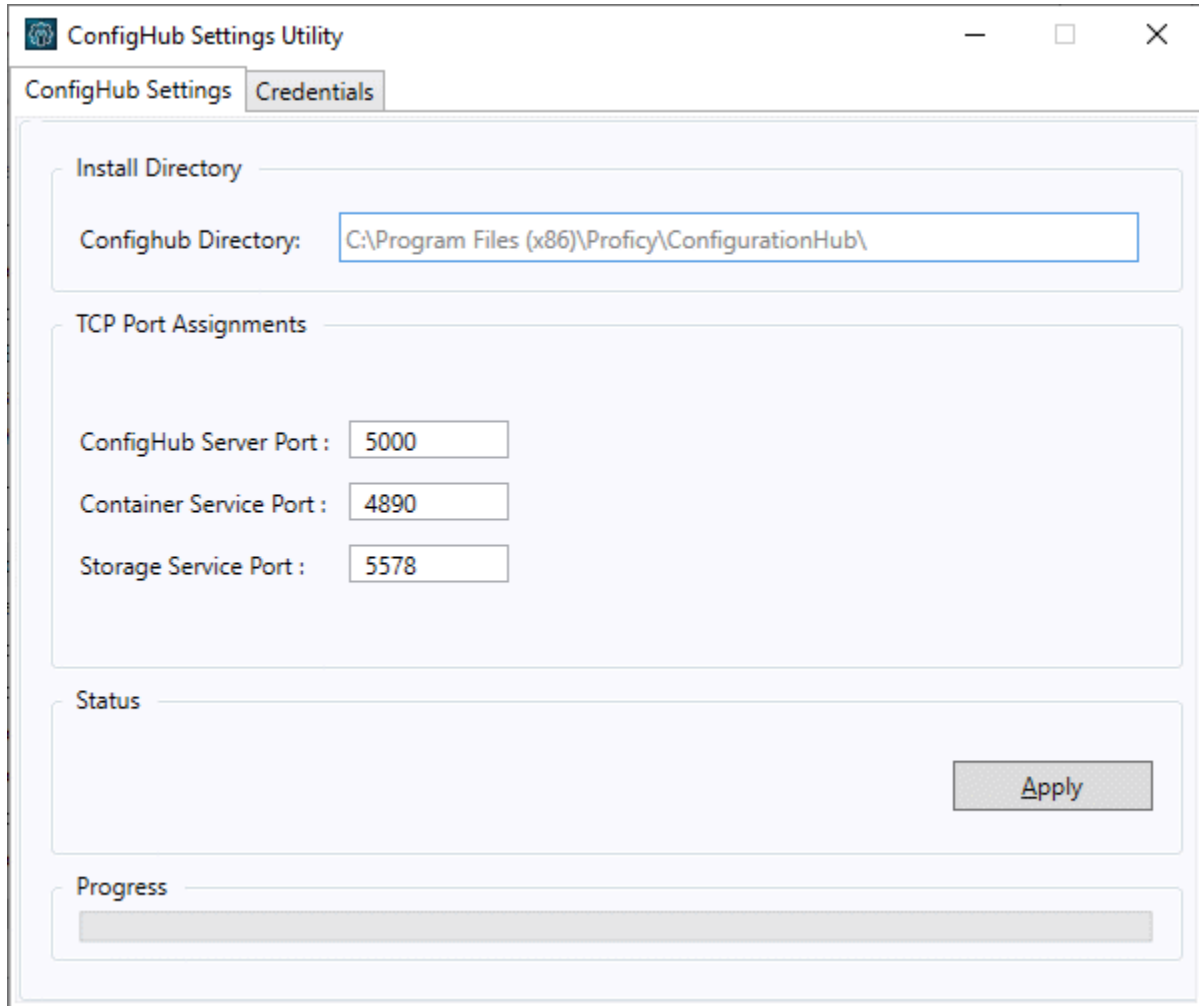
Create Certificates	
Root Certificate Created?	Created with thumbprint: 7091c4ce055de61d6abe15cb31aef94d9e5ab22f
Server Certificate Created?	Created with thumbprint: 607ae61c30566ba29b8c7d53a4f58285eabd624f
<input type="button" value="Create Certificates"/> <input type="button" value="Delete Certificates"/>	

6. Copy the iFIX_OpcuaConfigServer.crt and iFIX_OpcuaConfigServer.key files from C:\Program Files (x86)\Proficy\iFIX\CFG\iFIX_OpcuaConfigService\pki into the C:\Program Files (x86)\Proficy\iFIX\web\conf directory.
7. Restart the computer.

Port Changes for Configuration Hub

If you need to change the ports used by Configuration Hub web server after install, use the

`ConfigHubSettingsUtility.exe` utility found in the Configuration Hub folder (by default this folder is here: `C:\Program Files (x86)\Proficy\ConfigurationHub`) to reset them.



The screenshot shows the 'ConfigHub Settings Utility' window with the 'Credentials' tab selected. The window is divided into several sections:

- Install Directory:** A text box labeled 'Confighub Directory:' contains the path 'C:\Program Files (x86)\Proficy\ConfigurationHub\'. The text box is highlighted with a blue border.
- TCP Port Assignments:** Three text boxes are stacked vertically:
 - 'ConfigHub Server Port : 5000'
 - 'Container Service Port : 4890'
 - 'Storage Service Port : 5578'
- Status:** A large empty text box with an 'Apply' button located at the bottom right.
- Progress:** A horizontal progress bar at the bottom of the window, currently empty.

**Note:**

If you are planning to update the ConfigHub Server port number which is the Configuration Hub web server, then you must update all plugins to update ConfigHub Server port change. Otherwise, the plugins cannot communicate with the Configuration Hub. To update your iFIX plugin post install, use the Registration tool available in the iFIX WorkSpace; see [iFIX Plugin Registration \(on page 158\)](#) for more information. To update your Historian plugin post install, use the Web_Clients_Configuration_Tool.exe tool available in the C:\Program Files\GE Digital \Historian Config folder.

Chapter 9. Troubleshooting

Log Files

Install Log Files

When installed with the integrated installer, the log for the Configuration Hub portion of the install is named ConfigHubInstaller.log. This log appears in the `C:\Users\Admin\AppData\Local\Temp` folder and can be used to troubleshoot any issues that occur during install. You will need to show hidden files, folders, and drives to view this file.

Configuration Hub Log Files

By default, the log for Configuration Hub is saved to the following location: `C:\Program Files (x86)\Proficy\ConfigurationHub\Logs`, and this folder for the web server logs: `C:\Program Files (x86)\Proficy\ConfigurationHub\Web\httpd\logs`.

IGS Log File

For IGS, a log file named `igs-browse-config.log` is located in the `C:\Program Files (x86)\Proficy\iFIX\LOCAL\Logs` folder, by default. There is also an `Industrial Gateway Server.log` file in the `C:\Program Files (x86)\Proficy\Industrial Gateway Server` folder, by default.

Historian Log Files

For Historian, the logs are saved in this folder, by default: `C:\Proficy Historian Data\LogFiles`, or custom install path as specified during the Historian installation.

MQTT Client Log Files

For MQTT Client, the logs are stored in the default install path. By default, this path is: `C:\Program Files\Proficy\MQTTClient\Logs`.

Proficy WebSpace Log Files

For WebSpace, the logs are stored in the WebSpace default install path. By default, this path is: `C:\Program Files\Proficy\Proficy WebSpace\Log`.

WebSpace messages are recorded within log files prefixed with `aps` and followed by the date and time (to the nearest millisecond) the WebSpace Application Publishing Service was started (for example: `aps_2023-03-31_15-14-34.html`). A new log file is created each time the Proficy WebSpace Application

Publishing Service is started. The log file with the latest date and time stamp contains messages for the current or most recent instance of the Proficy WebSpace Application Publishing Service.

The WebSpace session manager logs are stored to the `C:\Program Files\Proficy\Proficy WebSpace\Programs\web-space-session-manager` folder, by default. The `web-space-session-manager.log` file is the name of the log file.

Proficy Authentication Log Files

The default location for the Proficy Authentication log files is the `CC:\ProgramData\ProficyAuthenticationLogs` folder. If However, if Operations Hub has installed Proficy Authentication than it may be the `C:\ProgramData\OphubLogs` folder.

iFIX Web Server Log Files

For the iFIX Web Server, the log files are located in the `C:\Program Files (x86)\Proficy\iFIX\web\logs` folder, by default.

iFIX Log Files

For iFIX, the associated logs are in `C:\Program Files (x86)\Proficy\iFIX\LOCAL\Log` folder, by default. The names of these files are:

Log Name	Description
<code>ifix_config_service.log</code>	iFIX OPCUA Config Service log file.
<code>ifix_config_service_cert.log</code>	iFIX Configuration Hub certificate service log file.
<code>ifix_confighub_facade_service.log</code>	iFIX ConfigHub Facade service log file.
<code>ifix_model_editor_service.log</code>	Model editor service log file.
<code>ifix_model_service.log</code>	iFIX model service which is used for publishing model information to iFIX.
<code>ifix_project_config_service.log</code>	iFIX project configuration service log file.
<code>ifix_tag_service.log</code>	iFIX tag service log file.
<code>ifix_tag_validators.log</code>	iFIX tag validator log file.
<code>ifix_webpace.log</code>	Proficy WebSpace log file.
<code>igs-browse-config.log</code>	IGS browsing log file.

The following list are the .json files located in the iFIX\CFG folder that are associated with the log files in the previous table:

- ifix_config.service.json
- ifix_confighub_facade_service.json
- ifix_confighub_system_service.json
- ifix_model_service.json
- ifix_project_config_service.json
- ifix_tag_service.json
- ifix_tag_validators.json
- igs-browse-config.json
- model_editor_service.json

Each of these .json files have an entry called "level" that accepts various values in lower case to capture greater detail of information. iFIX must be restarted after any modification of any of the levels in the json files.

**Important:**

If you change any of the logging levels for the .json files, after you've finished capturing the logs, be sure to set the level back to the default of "info". Otherwise, leaving the log at a level of "info" can impact performance.

Example of Modified .json File for Logging

Below is an example of the ifix_model_service.json file. Note that the "level" is currently set to "info." This value can be changed to any of the values in the following list. Note, that all values set for the level must be lower case.

```
{
  "port": "4865",
  "secure": true,
  "log": {
    "enable": true,
    "name": "ifix_model_service.log",
    "level": "info",
    "max-size": 5242880,
    "max-files": 3,
    "flush-seconds": 10
  },
}
```

```

"publishResponseUri": {
  "file": "ifix_confighub_facade_service.json",
  "uri_path": "/ifix-confighub-facade/v1/ifix/publish/response"
},
"unpublishModelFilename": "model_editor.sqlite",
"createModelInfoCommand": "CREATE TABLE IF NOT EXISTS model_info ( model_version INTEGER(8) NOT NULL, lastPublishTime
DATETIME, lastPublishUser TEXT(64) )"
}

```

The log level goes from off to trace. The default level is "info". The recommendation is to set the level to "trace" when troubleshooting the logs. After changed, iFIX will need to be restarted. The log files are located in the iFix\LOCAL\Log directory.



Important:

After you've finished capturing the logs, be sure to set the level back to the default of "info". Otherwise, leaving the log at a level of "info" can impact performance.

Error Logging Levels for iFIX .json Files

Acceptable entries for "level" are listed below:

- **off** – To disable logging for the REST service.
- **critical** – For this value the REST services do not have any messages implemented. This setting will output log messages for critical level only.
- **error** – This level captures any error logs. This setting will output log messages for critical and error levels.
- **warning** – Some warning messages are implemented in the REST. This setting will output log messages for critical, error, and warning levels.
- **info** – This is the default value set in the JSON files. This setting will output log messages for critical, error, warning, and info levels.
- **debug** – This setting will output log messages for critical, error, warning, info, and debug levels.
- **trace** – This log level will output every log message implemented in the REST service. This setting will output log messages for critical, error, warning, info, debug, and trace levels.

Frequently Asked Questions

When Would I Use the Database Import/Export vs. the Model Import/Export?

Use the Database import/export when you want to import/export tags to your iFIX database. These tags can be regular tags (non-model), or both model and non-model tags.

Use the Model import and export to help you move the model from one node to another, to make bulk changes to the model itself, or to use your model in Operations Hub.