Proficy Configuration Hub 2022

User Guide

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

doc@ge.com

Contents

Chapter 1. Getting Started

Introduction to the Configuration Hub Framework

Welcome to TestConfiguration Hub. TestConfiguration 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 from within Configuration Hub: Proficy Authentication, iFIX, and Historian.

The following graphic shows an example of TestConfiguration Hub with Proficy Authentication selected:
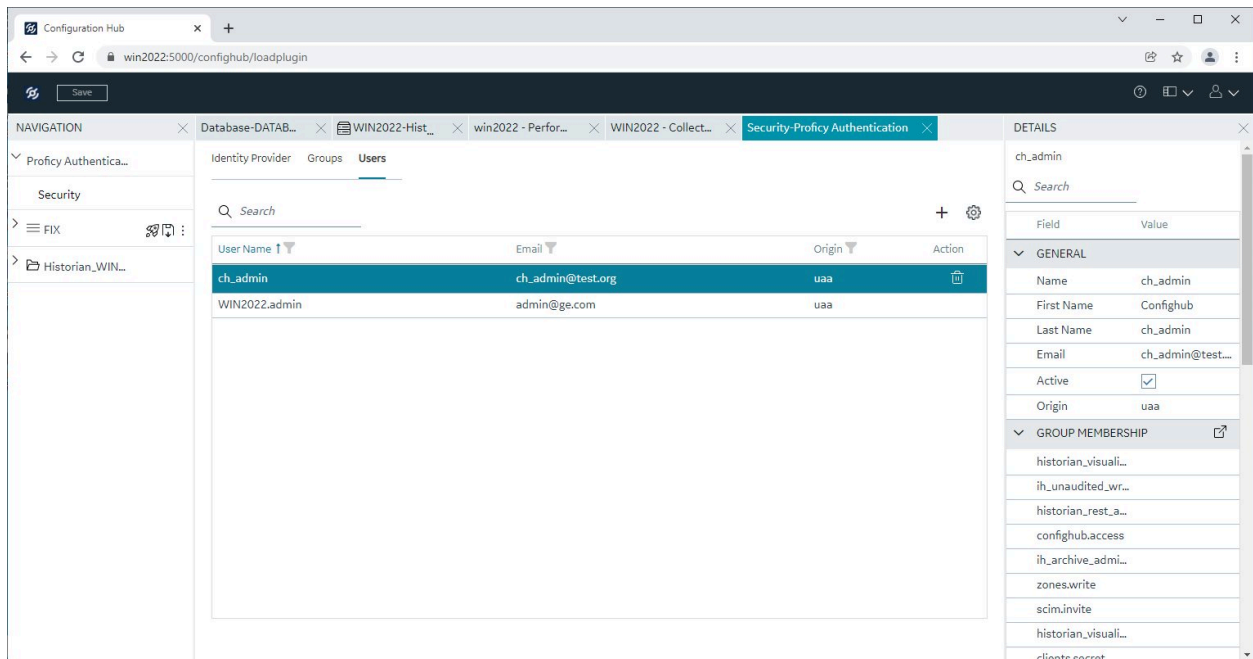
The following graphic shows an example of TestConfiguration Hub with the iFIX Database panel selected:
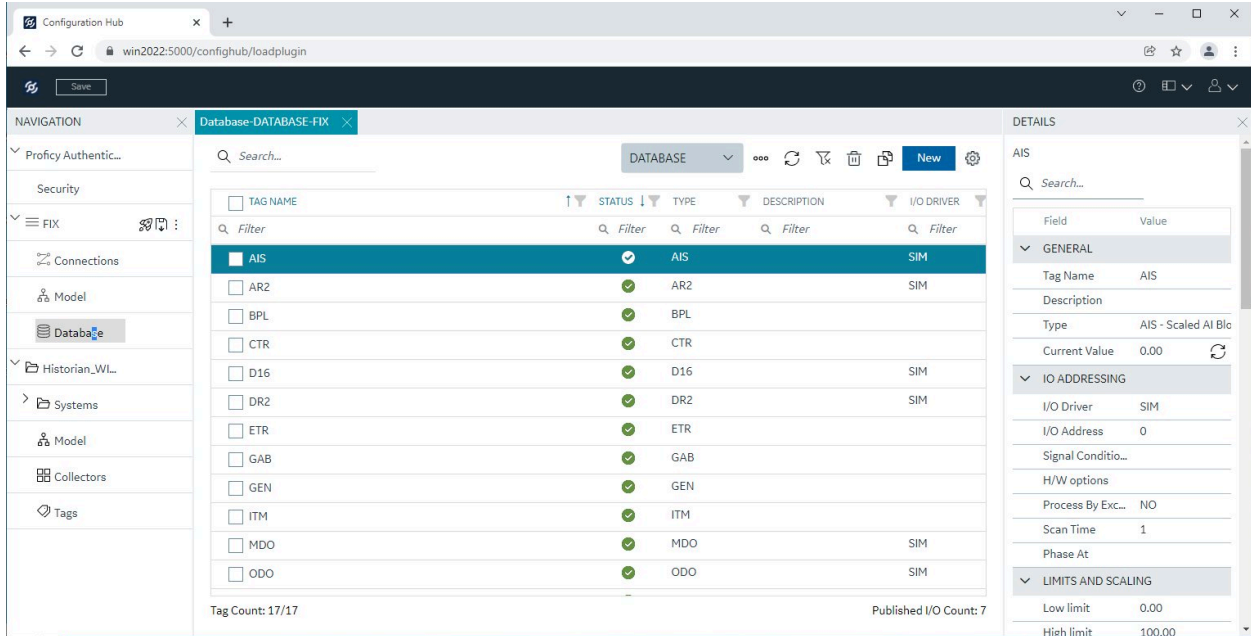
The following graphic shows an example of TestConfiguration Hub with Historian with a Server selected from the Historian Systems panel:
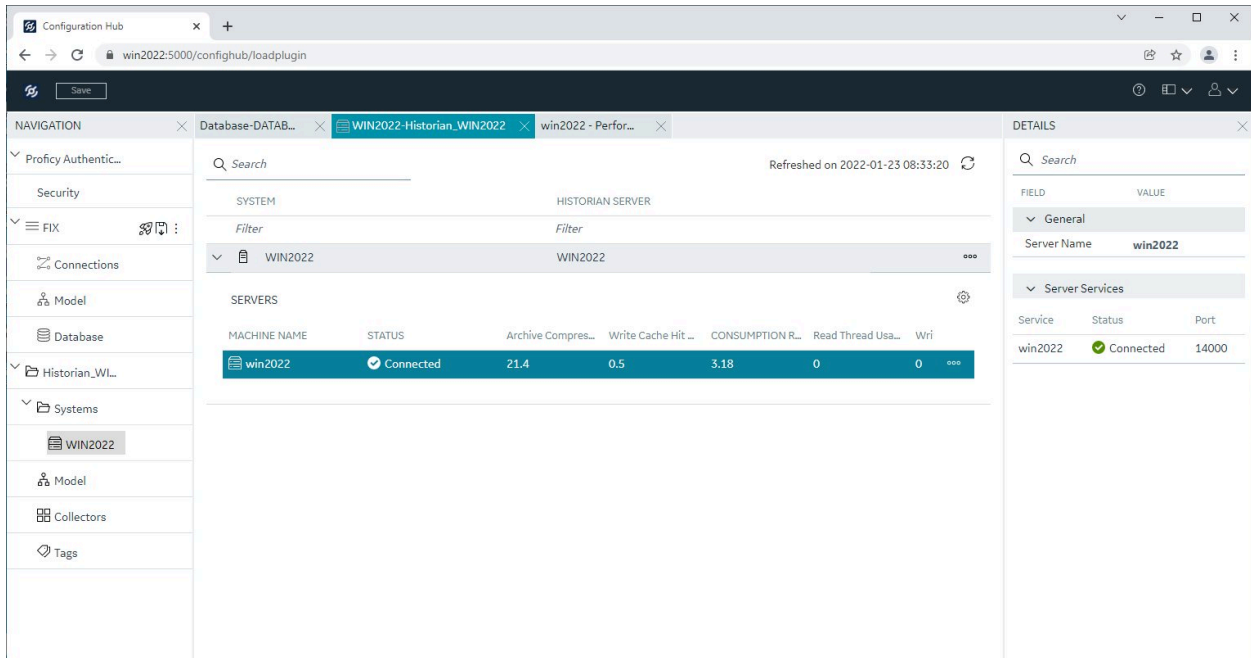
Sample Deployment Architectures

The following examples show different types of deployment architectures you may choose to use with Configutation Hub. In each of the architectures Configuration Hub and Proficy Authentication are only installed ONE TIME.

> ⚠️ **Important:**
> If Historian and iFIX are registered with the same Configuration Hub, the Historian Model editor will be disabled. In this case, use the iFIX model editor to create your model.

Example 1

The following example shows Configuration Hub and Proficy Authentication installed with iFIX (SCADA1) and other SCADAs (SCADA2 and SCADA3) on different computers connecting to that existing node.
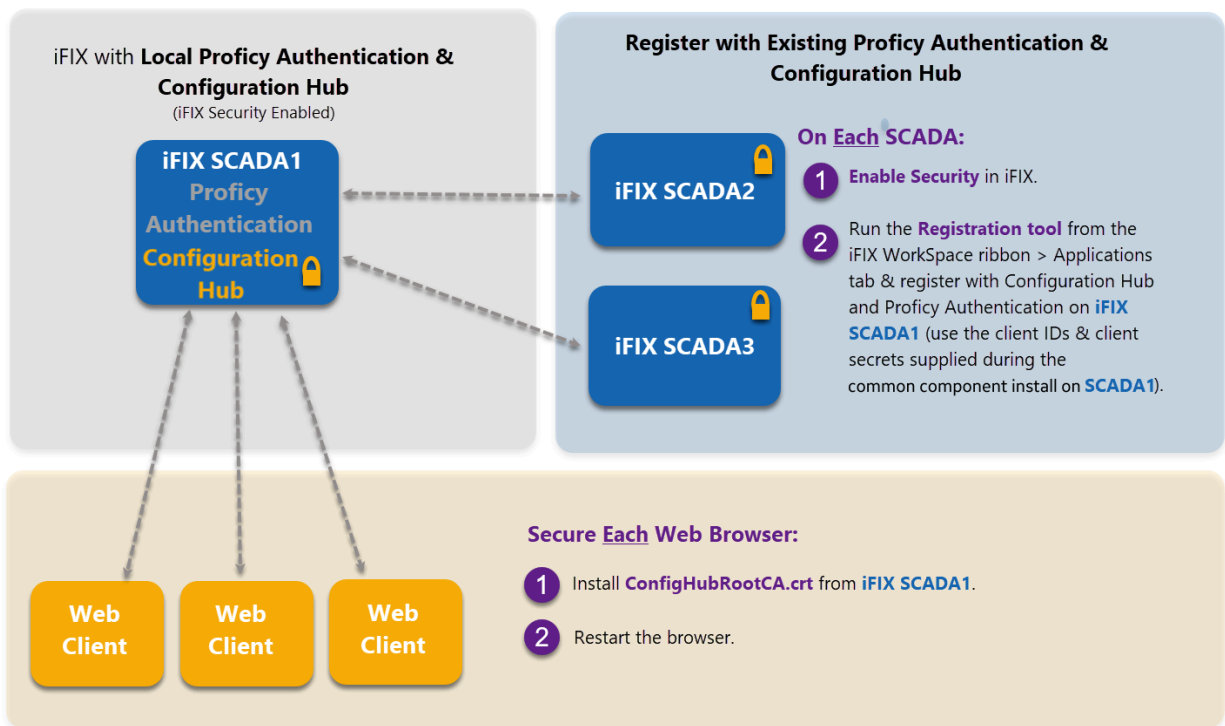
Example 2

The following example shows Configuration Hub and Proficy Authentication installed along with a Historian Server and Web-based Clients (Historian1) and SCADAs (SCADA1 and SCADA2) on different computers connecting to that existing Historian node.

Historian with **Local Configuration Hub & Proficy Authentication**

Historian1 — Proficy Authentication — Configuration Hub — Historian Web-based Clients

Register with Existing Proficy Authentication & Configuration Hub

iFIX SCADA 1

iFIX SCADA2

On Each SCADA:

1. **Enable Security** in iFIX.

2. Run the **Registration tool** from the iFIX WorkSpace ribbon > Applications tab & register with Configuration Hub and Proficy Authentication on **Historian1** (use the client IDs & client secrets supplied during the **Historian1** web-based clients install).

Web Client   Web Client   Web Client

Secure Each Web Browser:

1. Install **ConfigHubRootCA.crt** from **Historian1**.

2. Enable Trust for Self-signed Certificate in Chrome for **Historian1**.

3. Restart the browser.

Example 3

The following example shows Configuration Hub and Proficy Authentication installed with iFIX (SCADA1) and other computers with iFIX (SCADA2 and SCADA3) or a Historian Server (Historian1) with Web-basec Clients connecting to that existing node.

iFIX with Local Configuration Hub & Proficy Authentication
(iFIX Security Enabled)

iFIX SCADA1
Proficy Authentication
Configuration 🔒 **Hub**

Register with Existing Configuration Hub & Proficy Authentication

On the Historian Server:

Historian1 **Historian Web-based Clients**

1. Install **Historian Web-based Clients** from Historian Install, and when prompted, register with the existing Configuration Hub and Proficy Authentication on **iFIX SCADA1** (use the client IDs & client secrest supplied during the common component install on **SCADA1**).

Register with Existing Configuration Hub & Proficy Authentication

iFIX SCADA2 🔒

iFIX SCADA3 🔒

On Each SCADA:

1. **Enable Security** in iFIX.

2. Run the **Registration tool** from the iFIX WorkSpace ribbon > Applications tab & register with the Configuration Hub and Proficy Authentication on **iFIX SCADA1** (use the client IDs & client secrets supplied during the common component install on **SCADA1**).

Secure Each Web Browser:

1. Install **ConfigHubRootCA.crt** from **iFIX SCADA1**.

2. Enable Trust for Self-signed Certificate in Chrome for **Historian1**.

3. Restart the browser.

Web Client **Web Client** **Web Client**

Example 4

The following deployment architecture illustrates Configuration Hub, Proficy Authentication, the iFIX SCADA, and Proficy Historian all installed on separate computers.
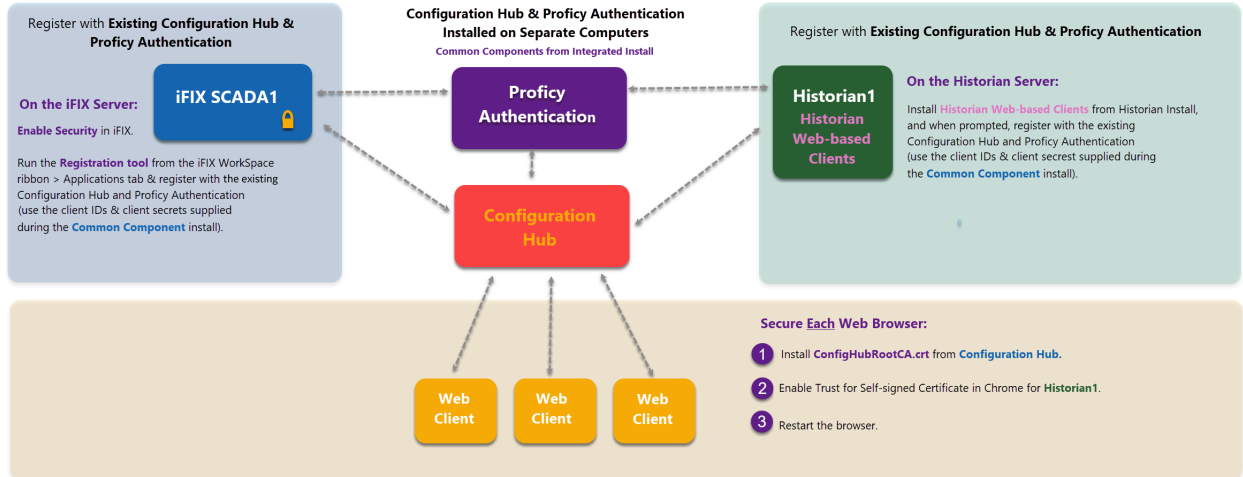
Available Product Plugins

TestConfiguration Hub is a framework where more than one Proficy product can be configured. Currently, you are able to register Proficy Authentication, iFIX and Historian "plugins" with TestConfiguration 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.
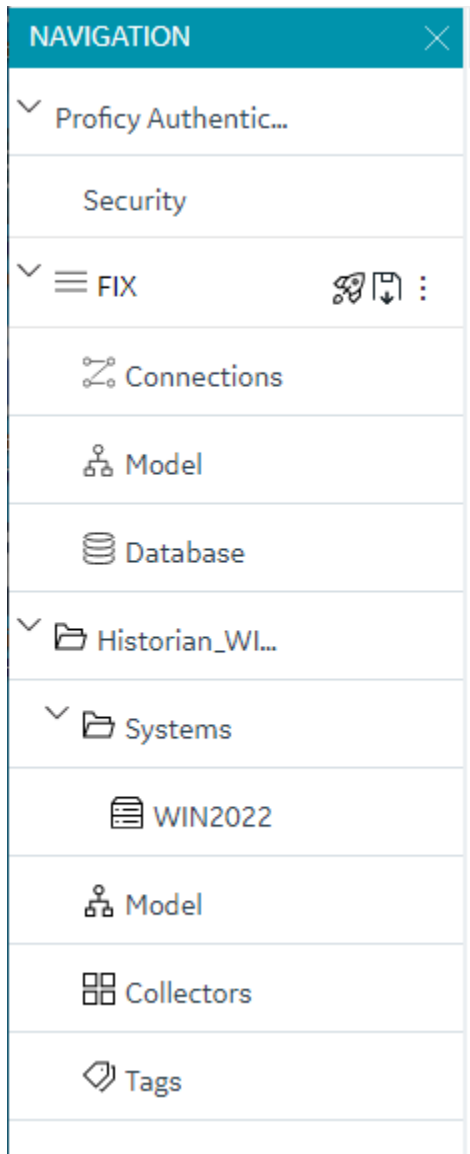
Common Panels

Common Panels

In the TestConfiguration 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:
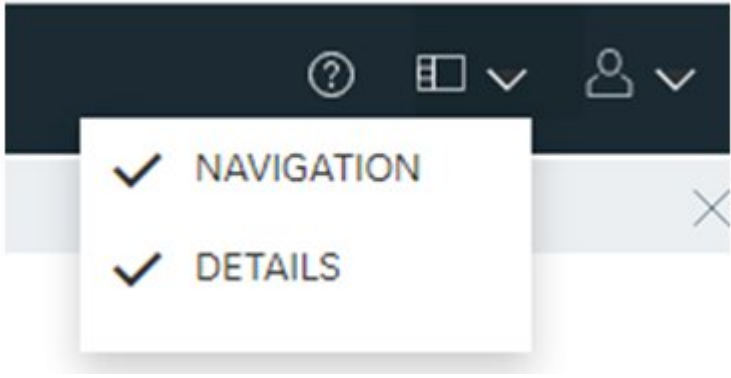
Application Bar

TestConfiguration 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 Save and Publish button also appear in this toolbar.

Item	Description
Publish	Use this button to push any locally saved changes to the iFIX server. This button is not applicable to Historian, and does not display on the Historian toolbar.
Save	Click to save your changes locally. These changes will not get pushed to the iFIX server until you click the Publish button. This button is not applicable to Historian, and does not display on the Historian toolbar.
⑦	Click to access the online help.
▣ ∨	Use this button to open or close a Navigation or Details panel.
👤 ∨	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 ses-

Item	Description
	sion, 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.

Navigation panel

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

- In Historian, the Navigation panel includes the Systems configured by user. Systems will have a Server details displayed. By default, there will be one system created.
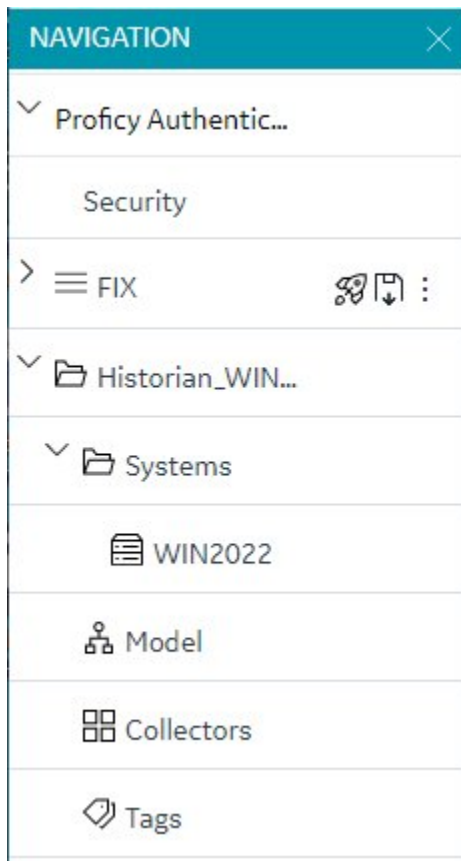
- In the case of iFIX, the plugin name is the Node name of your iFIX node. Under the node name, you will get Connections, Model, and Database panels.
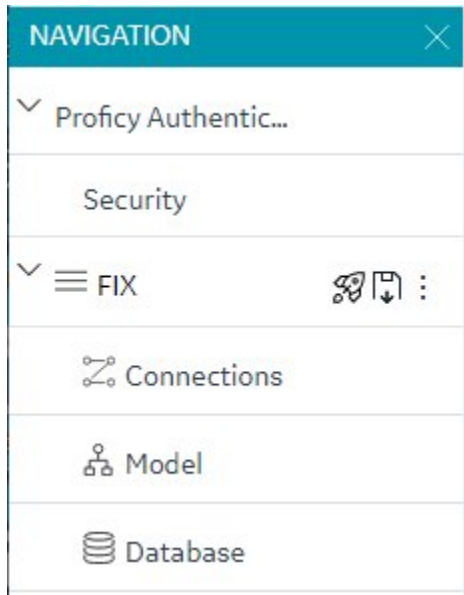
Depending on the product, this instance will have different sub panels available to open and configure.

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.

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.

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:

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. TestConfiguration 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 others 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 TestConfiguration Hub web server. The SSL certificate for TestConfiguration 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 TestConfiguration Hub
Use the following steps to update your self-signed certificates for TestConfiguration Hub:

1. Either remove or backup the certificate files in C:\Program Files (x86)\GE\ConfigurationHub \ConfigHubPki folder.
2. Open a command prompt as an administrator in the C:\Program Files (x86)\GE\ConfigurationHub directory.

3. Enter the following command to create new self-signed certificates:

```
restart_confighub.bat "C:\Program Files (x86)\GE\ConfigurationHub" "C:\Program Files

 (x86)\GE\ConfigurationHub\Web" 5678 4890 htclab.ge.com
```

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

4. Copy the server_cert.crt and server_cert.key files the from C:\Program Files (x86)\GE \ConfigurationHub\ConfigHubPki folder to the C:\Program Files (x86)\GE\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)\GE\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)\GE \iFIX\LOCAL\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)\GE\iFIX\LOCAL\iFIX_OpcuaConfigService\pki into the C:\Program Files (x86)\GE\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 TestConfiguration 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. The web server used by TestConfiguration Hub, Nginx, uses base-64 encoded PEM files for certificates and keys. For more information, refer to the following links:

   http://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_certificate

   http://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_certificate_key

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 TestConfiguration Hub, copy the root and server certificates and key files into the C:\Program Files (x86)\GE\ConfigurationHub\ConfigHubPki folder, and the server certificate and key files to the C:\Program Files (x86)\GE\ConfigurationHub\Web\conf folder. (In TestConfiguration Hub the nginx server certificate files are named: server.crt and server.key.)

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

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

> **Note:**
>
> If there is a name change, then the nginx.conf file in the C:\Program Files (x86)\GE
> \ConfigurationHub\Web\conf\nginx.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)\GE\iFIX
   \LOCAL 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 TestConfiguration Hub, the TestConfiguration 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 TestConfiguration 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)\GE\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)\GE\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.
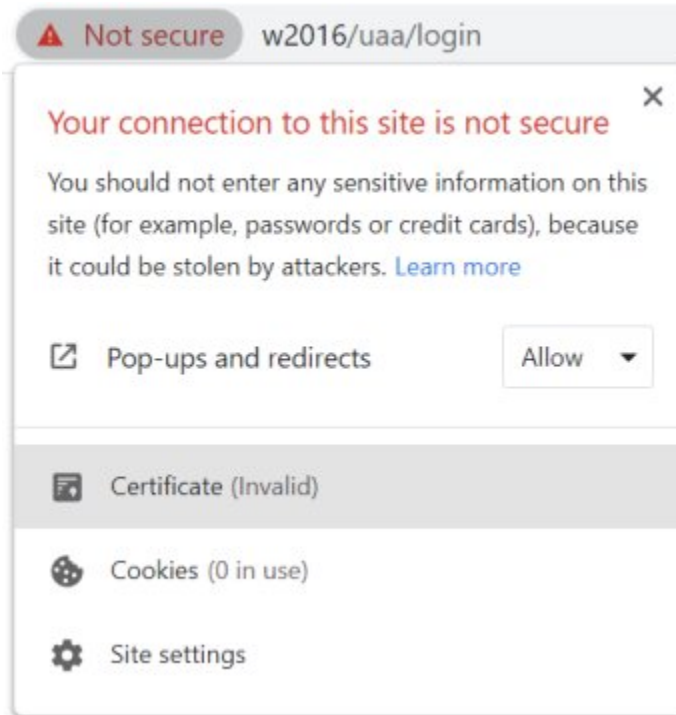
3. Select the **Certification Path** tab, and then select the **root certificate**.
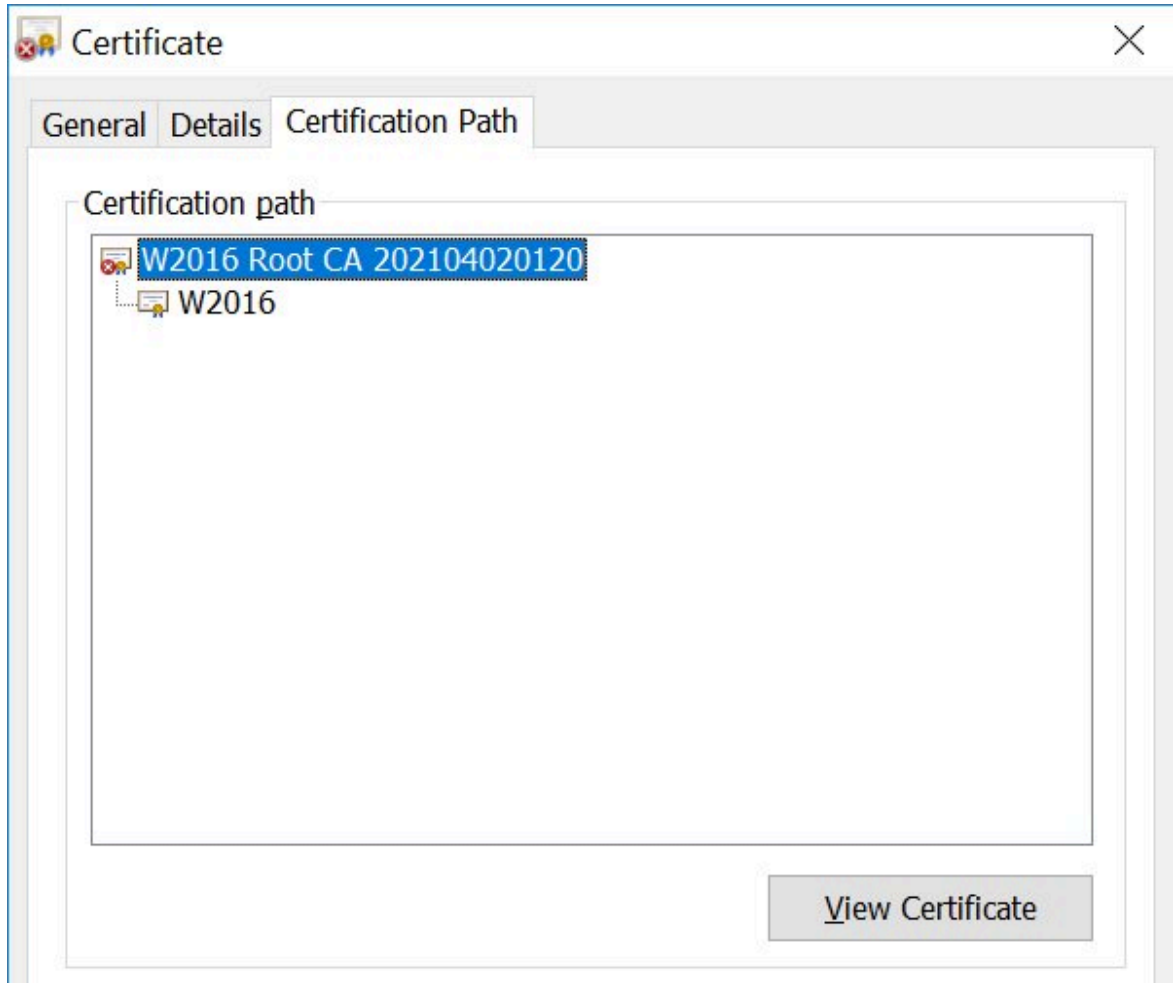
4. Select **View Certificate** The Certificate window appears, displaying the General, Details, and Certification Path sections. Select Details, and then select Copy to Files.
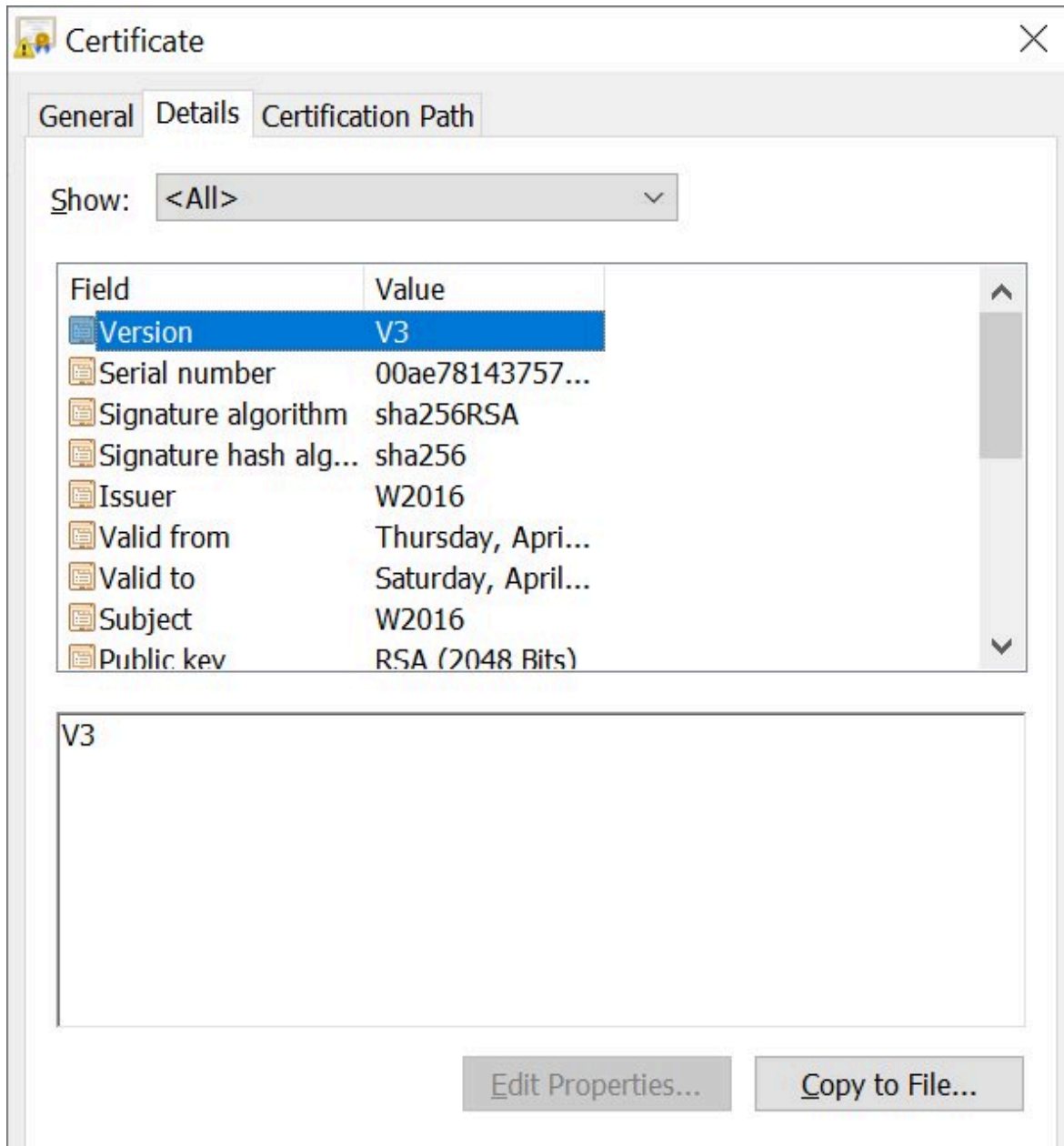
5. Follow the on-screen instructions to save the certificate to a local file. Use the default format: DER encoded binary X.509 (.CER).
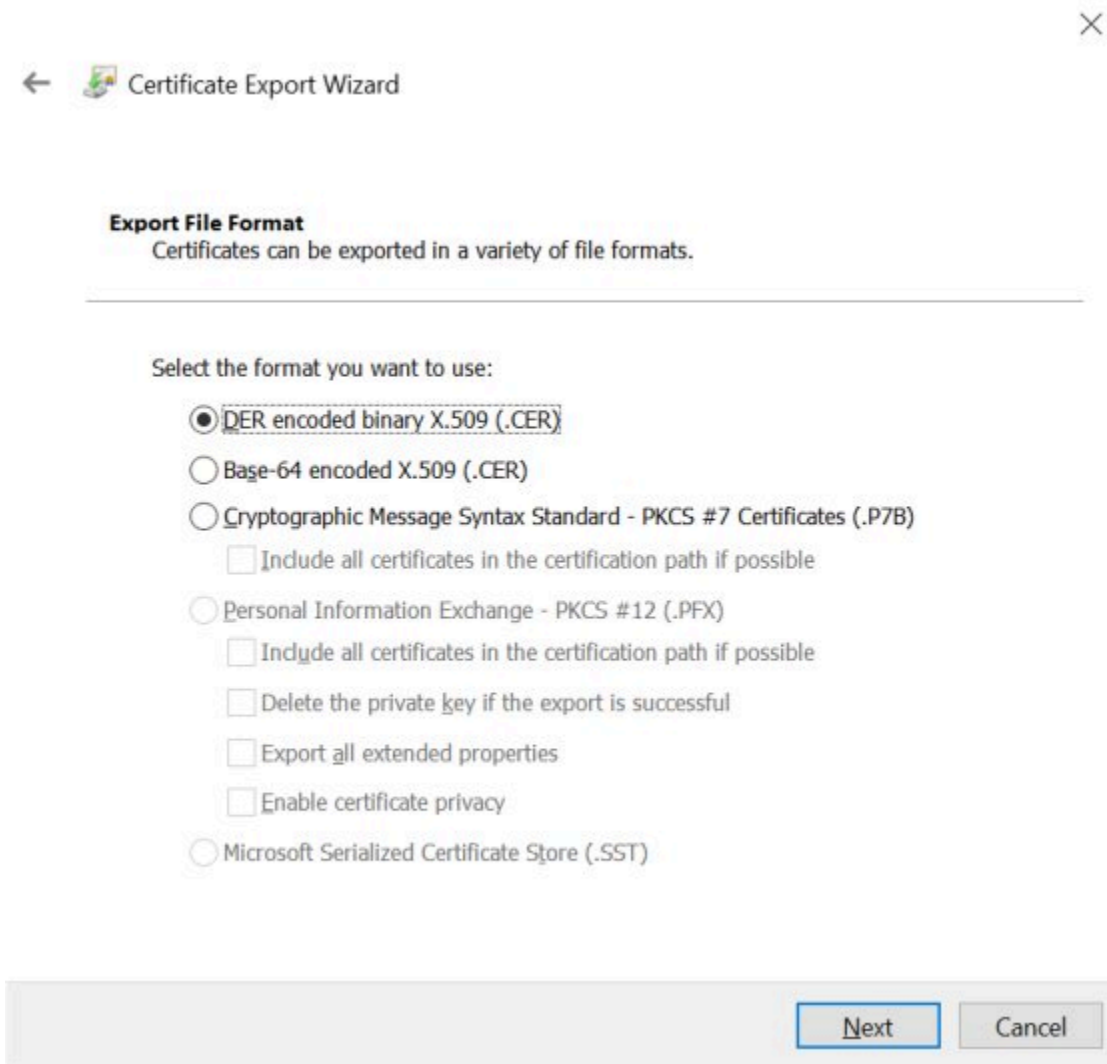
6. Right-click the .CER file that you have exported, and select **Install Certificate**. The Certificate Import Wizard window appears.

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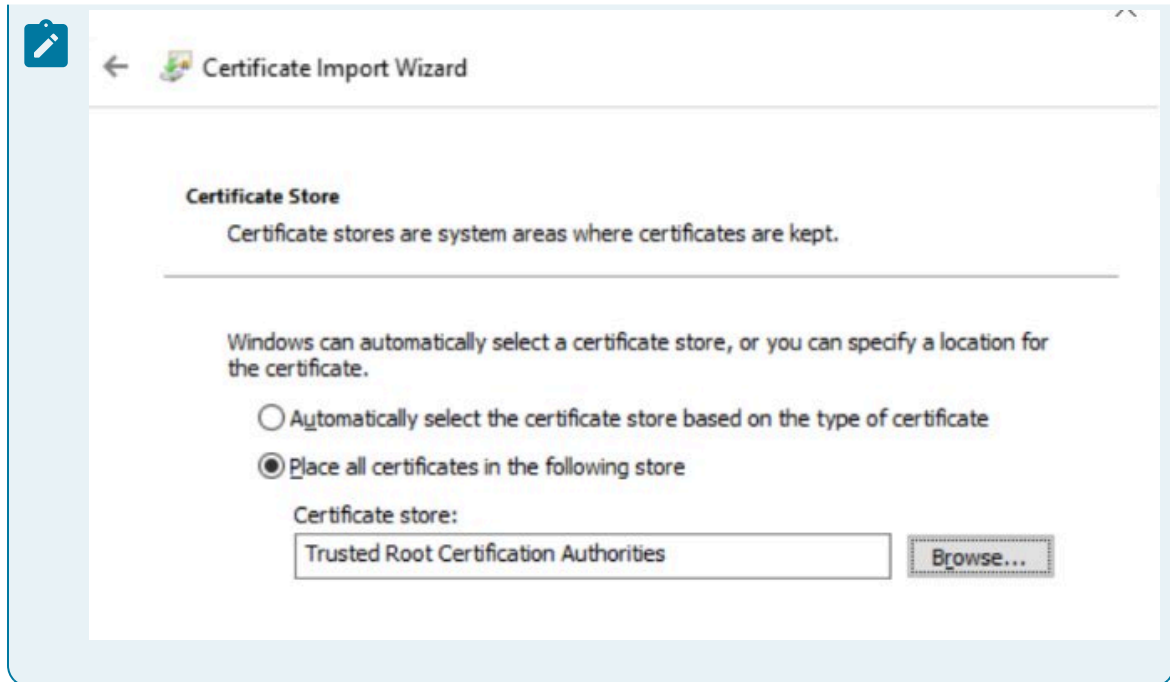
A Security Warning window may appear. If it does, ignore the message by selecting Yes. The certificate is installed.

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.

Known Issues and Limitations

The following limitations apply to using TestConfiguration 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 TestConfiguration Hub.
- For Historian, if only one machine remains in a mirror group, you cannot remove it.
- If you install TestConfiguration Hub and the Historian Web Admin console on the same machine, and use self-signed certificates for both of them, the login page for TestConfiguration 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.
- 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)\GE\iFIX\CFG \iFIX_OpcuaConfigService\pki folder into the C:\Program Files (x86)\GE\iFIX\web\conf directory, and restart iFIX.

Chapter 2. Proficy Authentication

Set up Authentication

Set up authentication for 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**.
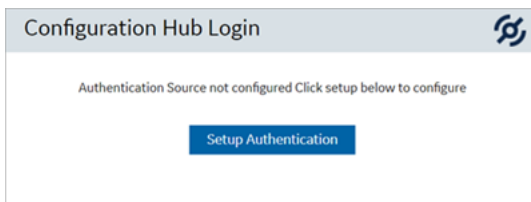
   The **Configuration Hub Administrator Credentials** screen appears.
3. Enter the details for logging in to the Configuration Hub application.

Field	Description
Client ID	The client ID provided during installing Configuration Hub. Example: `confighubadmin`
Client Secret	The client secret provided during installing Configuration Hub.
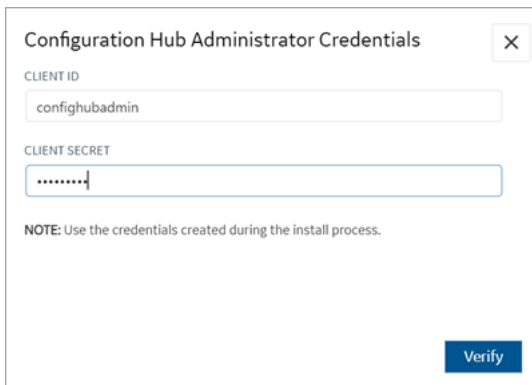
4. Select **Verify**.

   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, `desktop-sahfg5f.logon.ds.ge.com` Refer to step 6 to establish a trust with this server connection.
Server Port	The port number to communicate with the host machine. The default port where UAA is installed is `443`. The server connection is automatically tested on entering the port. You can also select **Test** to test the connection.
Use Configuration Hub Administration credentials for Proficy Authentication	Select this check box to populate the same login credentails you entered for Configuration Hub Admin account. If you want to use unique login credentials for Proficy Authentication, clear the check box and enter **CLIENT ID** and **CLIENT SECRET**.
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.

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

   The **Certificate Details** screen appears.

7. Select **Trust**.

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

8. Select **Register**.

9. Select **Ok**.

The **Configuration Hub Login** screen appears. Refer to .

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

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

Log in to Configuration Hub *(on page 39)* and perform operations related to Proficy Authentication.

Log in to Configuration Hub

Log in as a user or client.

Set up Authentication *(on page 35)*

You can log in to Configuration Hub with user credentials or as a client administrator *(on page 40)*.

1. On the Configuration Hub Login screen, select **Continue to Login**.
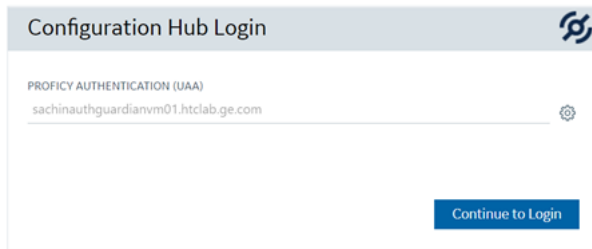
2. Enter your user login credentials.

3. Select **SIGN IN**.

You are now logged in as a user.

Log in as Client Administrator

1. On the Configuration Hub Login screen, select **Login as Proficy Authentication (UAA) admin**.
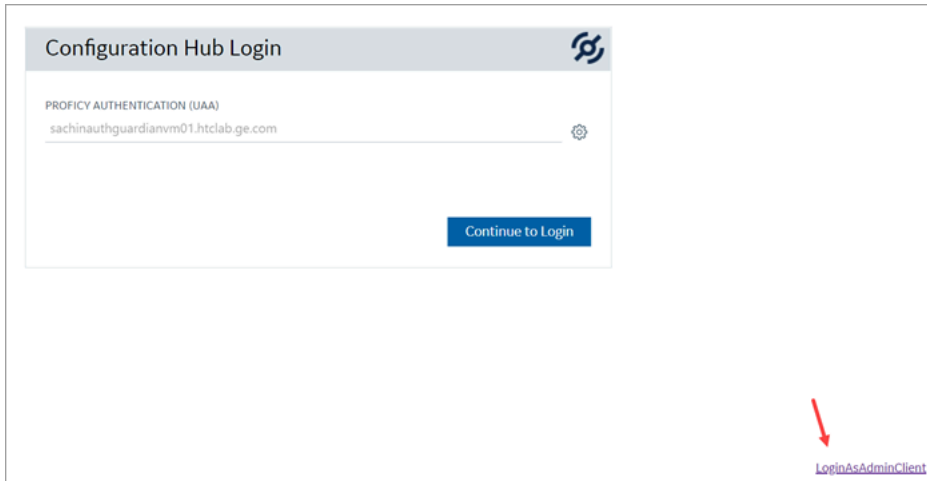
2. Enter **Admin Client ID** and **Client Secret**.

3. Select **SIGN IN**.

You are now logged in as a client.

Proficy Authentication Overview

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 seacrh for existing accounts in Proficy Authentication. You can also filter account details using search keywords.

Enable SAML

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

To enable SAML for Proficy Authentication, you will need to download the Proficy Authentication service provider's metadata file. Visit `https://enter FQDN of the machine where Proficy Authentication is`

`installed/uaa/saml/metadata` to download the `saml-sp.xml` file. This file contains all the information to fulfill the mandatory details for generating the metadata XML file from identity providers.

See Configure Okta as SAML IDP *(on page 42)*.

Configure Okta as SAML IDP

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**.
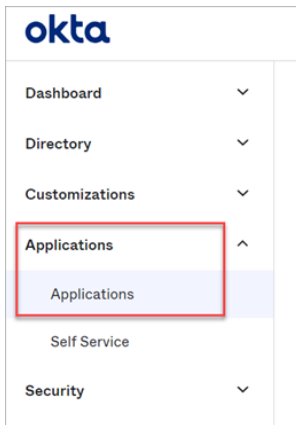
4. Select **Create App Integration**.
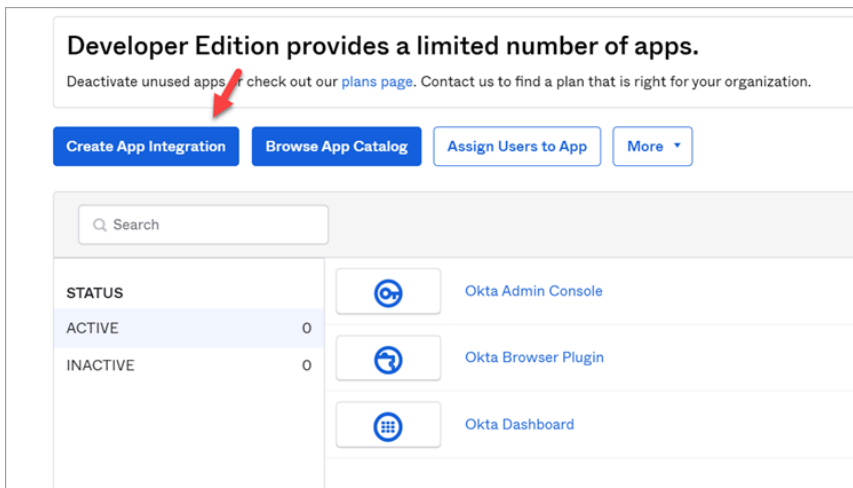
The **Create a new app Integration** screen appears.
5. Select **SAML 2.0**, then select **Next**.
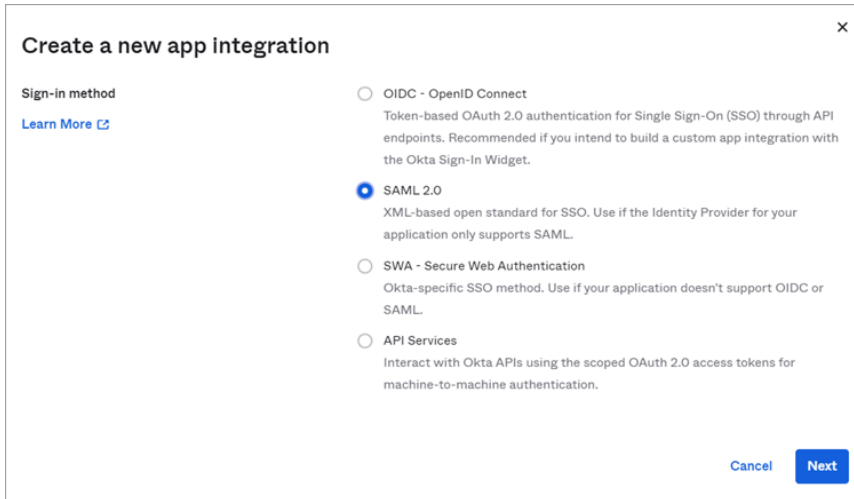
The **Create SAML Integration** screen appears.
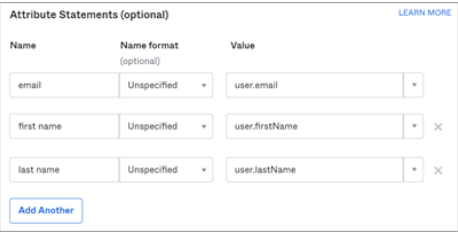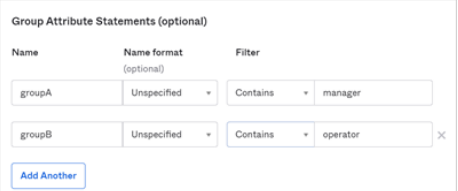
6. Under **General Settings**, provide a name and logo for your application, then select **Next**.
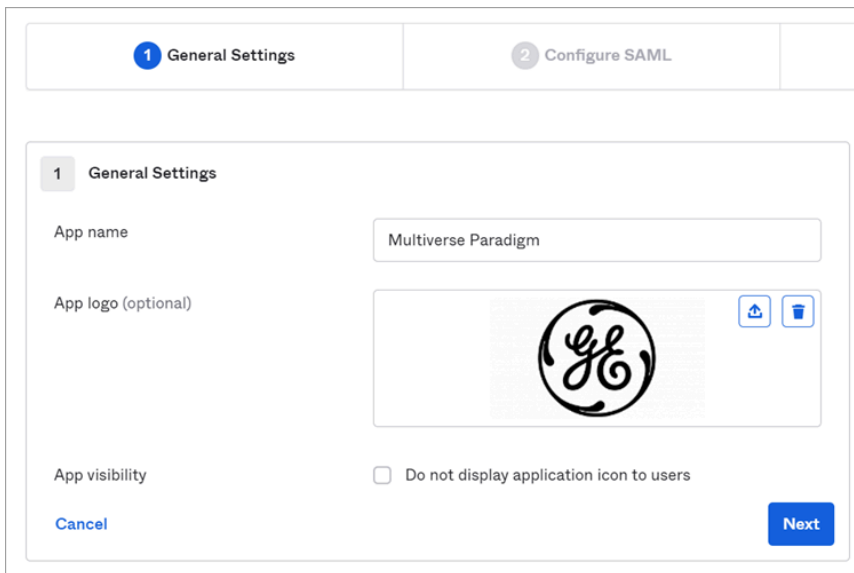
7. Under **Configure SAML**, fill out these details:

Single sign on URL	Use the downloaded Proficy Authentication metadata file *(on page 41)* `saml-sp.xml` to get the URL for this field. It should look something like this:

Audience URI (SP Entity ID)	Refer to `saml-sp.xml` to get the logout URL. It should look something like this:
	
	`<?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#">`

Enable Single Logout	a. Select **Show Advanced Settings**.
	b. Select the check box for **Allow application to initiate Single Logout**.
	c. Enter **Single Logout URL**. Refer to `saml-sp.xml` to get the logout URL. It should look something like this:
	
	`</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"/>`

Attribute Statements (optional)	Add user attribute statements such as email, first name, and last name as shown here:
Group Attribute Statements (optional)	Add group attribute statements such as groupA and groupB as shown here:

> **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 48)* 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.

Manage Identity Providers

Configure LDAP Identity Provider

You can add more than one LDAP connection.

Log in to Configuration Hub *(on page 39)* with user/client having write access for admin and clients.

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
URL	The URL of the LDAP server. The trailing slash (/) must be included at the end of the URL. You can use LDAP with or without secure authentication in the following format: ◦ Insecure port: `ldap://100.100.100.2:389/` ◦ Secure port: `ldaps://100.100.100.2:636/` You can also use a fully qualified domain name instead of an IP address. For a secure port, provide user credentials.
Bind User Distinguished Name	Distinguished LDAP user name. Describes the part of the hierarchy the user belongs to on the active directory network.

Field	Description
	CN=Common Name. DC=Domain Component. OU= Organization Unit Name. The CN and DC is typically required, and the OU is optional. For example: `CN=John Smith,OU=Factory,DC=Company,DC=COM`
Password	The password to log in to the LDAP server if you choose secure authentication.
Test	Tests the connection to the LDAP server. If the URL and login details are correct, you will receive a test successful message.
Skip SSL Verification	This option appears only when you choose a secure port for LDAP. Select this check box if you want to skip establishing a secure connection between client and server for exchanging LDAP data. Clear the check box to allow SSL verification. Refer to step 4.

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.

If the certificate is not added automatically, a message appears allowing you to manually add it.

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

5. **Optional:** Select to view the certificate.
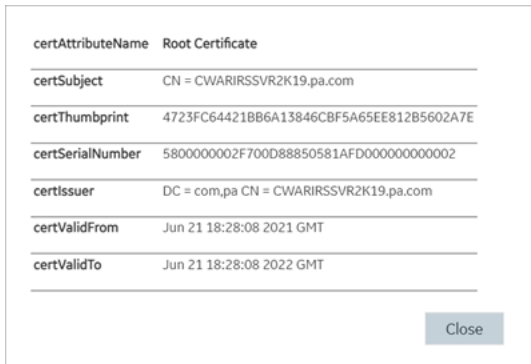
6. Select **Save**.
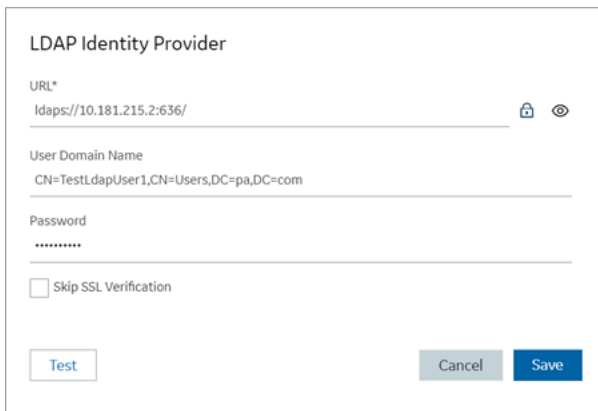
The LDAP identity provider is created.

Configure SAML Identity Provider

You can add multiple SAML connections.

Log in to Configuration Hub as an administrator.

1. Go to **Proficy Authentication > Security > Identity Provider**.

2. Select , then select **SAML**.
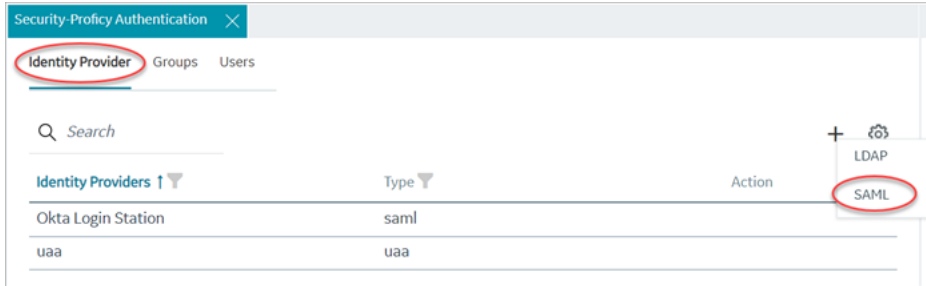
The **SAML Identity Provider** screen appears.

3. Enter the following details:

Field	Description
Metadata Location	Select **Metadata XML** to upload the XML document and populate the location URL in this field. 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 42)*.
Name	Name of the SAML identity provider.
Attribute Name	The attribute that contains the group membership information about a user in a SAML assertion.
Name ID	SAML Name ID and associated fields that you want to use in a link test.
Enable SAML Link	Select the check box.

    4. 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.
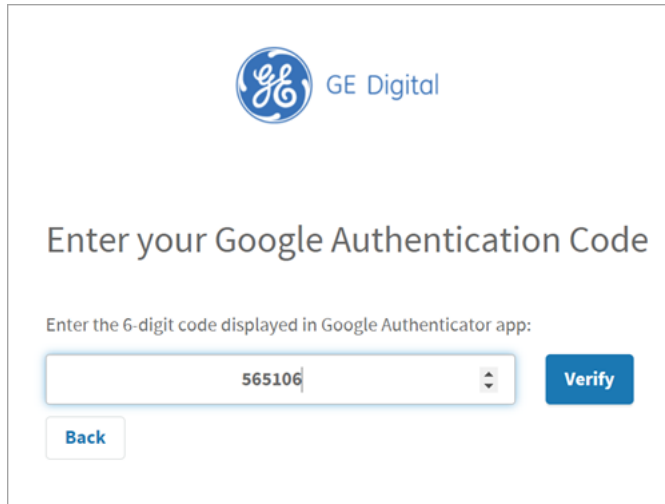
The authentication app validates the user login and displays a 6-digit code. Barcode scanning appears only for the first time validation for every user login.

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.

Configure LDAP Identity Provider *(on page 46)*

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 LDAP identity provider.

    The existing information for the identity provider appears on the **DETAILS** panel.
4. Select ⬚ to display the details in a pop-up screen.
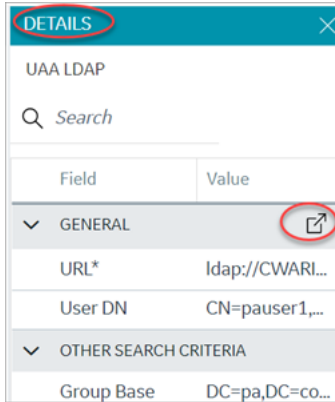
The **LDAP Identity Provider** screen appears.

5. You can modify the existing information and save the changes.
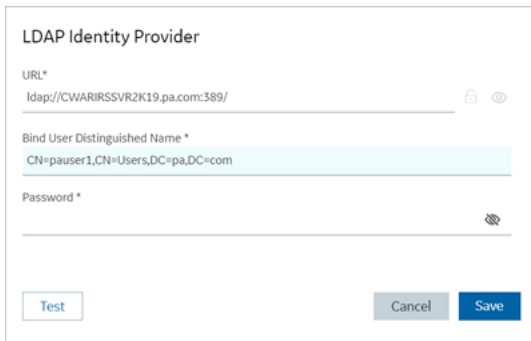
6. To modify existing search criteria values, place your cursor and enter the new value for the respective criteria.

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

Search Criteria	Example Value	Description
Group Base	`OU=Sales,OU=Groups,OU=Enter-prise,DC=company,DC=com`	Defines the starting point for the LDAP group search in the active directory tree.
		CN=Common Name. DC=Domain Component. OU= Organization Unit Name. The CN and DC is typically required, and the OU is optional.
		If you use only `DC=Ge,DC=com`, timeout may occur due to slow

Search Criteria	Example Value	Description
		system response. Use the exact `OU` to avoid timeout.
User Base	`OU=Sales,OU=Users,OU=Enter-prise,DC=company,DC=com`	Defines the starting point for the LDAP group user search in the active directory tree.
		If you use only `DC=pa,DC=com`, timeout may occur due to slow system response. Use the exact `OU` to avoid timeout.
User Filter	`cn={0}`	Allows the LDAP user (active directory user) to login with their display name. This is field is populated by default.
	`sAMAccountName={0}`	Allows the LDAP user (active directory user) to login with their account name (Windows login name). This is field is populated by default.
Group Filter	`member={0}`	Retrieves the `memberOf` attribute values for the specific user. This is field is populated by default.
Max Filter	`10`	Defines the maximum depth for searching the LDAP groups. The default value is `10`.

Search Criteria	Example Value	Description
		For very large systems, set the value to 2 as it may impact system performance.

Modify SAML Identity Provider

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

Configure SAML Identity Provider *(on page 48)*

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 [icon] to display the details in a pop-up screen.
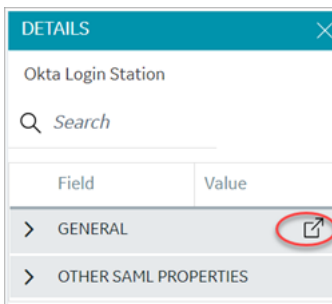
The **SAML Identity Provider** screen appears.

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.

Log in to Configuration Hub as an administrator.

1. Go to **Proficy Authentication > Security > Identity Provider**.

   The existing list of identity providers appear.

2. Select the identity provider you want to delete.

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

3. Select ⚬⚬⚬, then **Delete**.
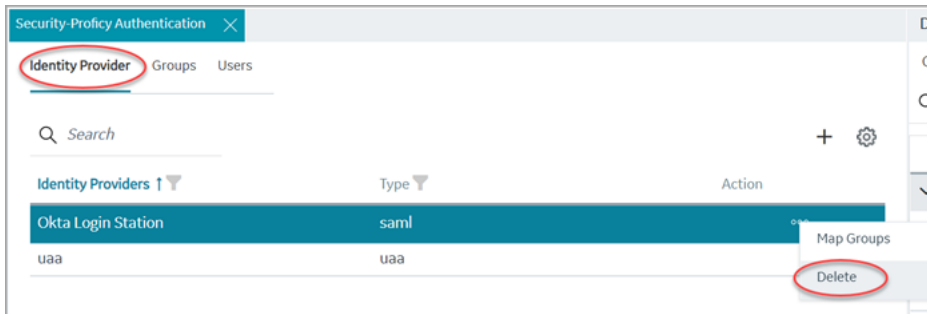
   A message appears to confirm the delete action.

4. 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, and scada.fix.shared.SUPERVISORS.

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.

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

- **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.

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 ＋
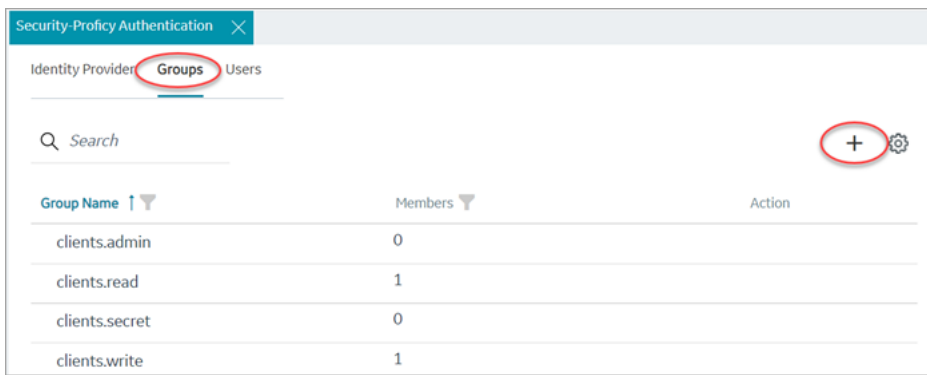
   The **Add Group** screen appears.
3. Enter the following details for the new group.

Field	Description
Group Name	A unique name of the group that does not match with any existing Proficy Authentication groups. For example, `Supervisors_LineA`
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 63)*
- Add/Remove Sub-Groups in a Group *(on page 64)*
- Map Groups *(on page 60)*

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.
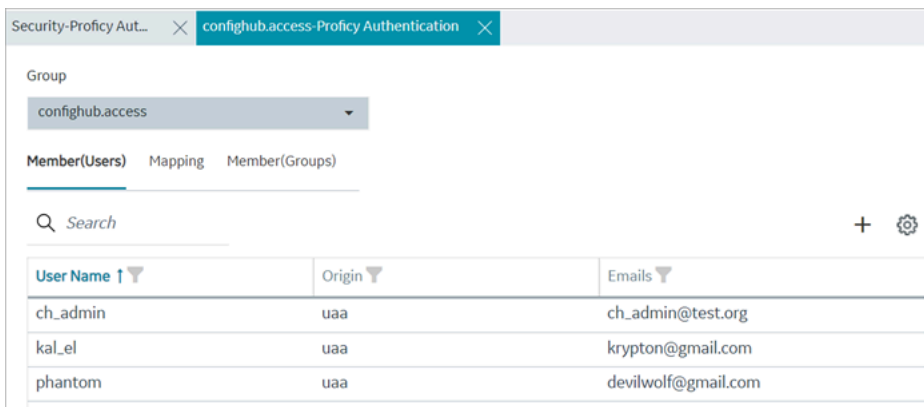
3. You can modify the following:

Tab	Description
Member (Users)	Displays the list of users added to this group. Add/Remove Users in a Group *(on page 63)*.

Tab	Description
Mapping	Displays the list of mapped groups for this group. You can add/remove mapped groups *(on page 60)*.
Member (Groups)	Displays the list of sub-groups added to this group. Add/Remove Sub-Groups in a Group *(on page 64)*.

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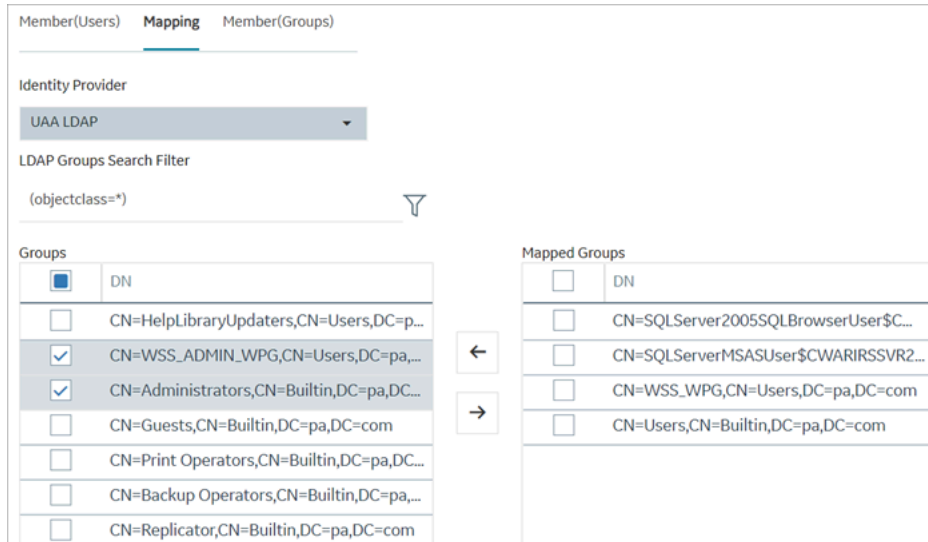
The users belonging to the mapped LDAP groups are now a member of the Proficy Authentication group selected in step 2.

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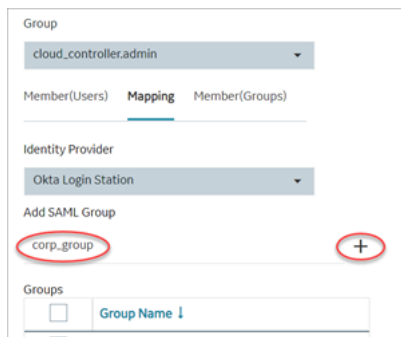
   c. Select the check box for the groups you want to map to the Proficy Authentication group selected in step 2.

   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

Modify a group *(on page 59)* 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.
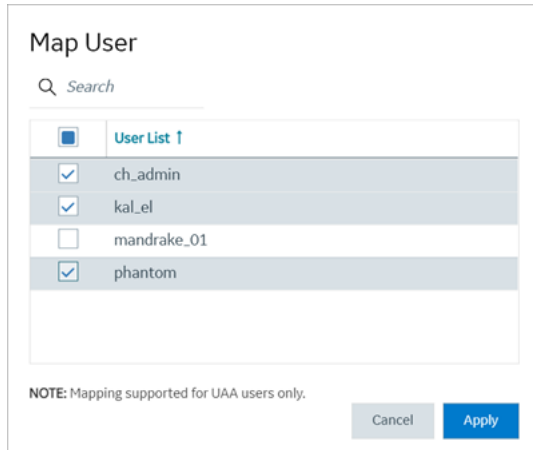
4. Select **Apply**.

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

Add/Remove Sub-Groups in a Group

Modify a group 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.
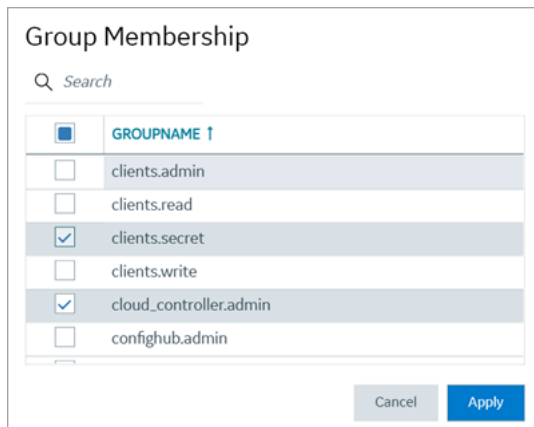
4. Select **Apply**.

   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.
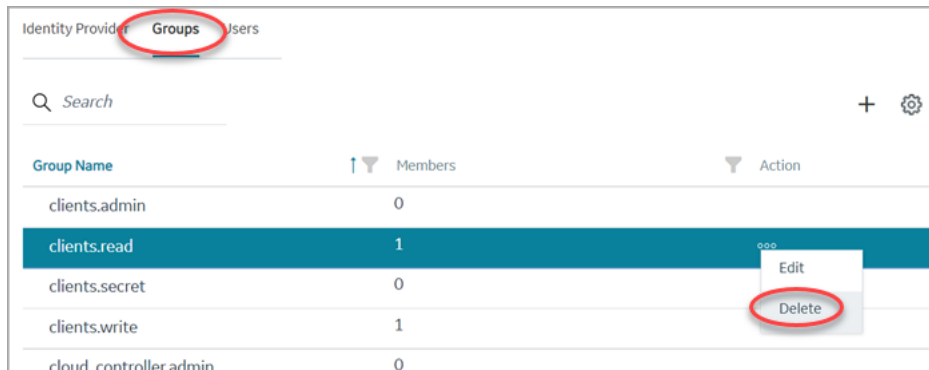
1. Go to **Proficy Authentication > Security > Groups**.
   The existing list of groups appear.
2. Select the group you want to delete.
   Additional options appear under the **ACTION** column.
3. Select ⠿, then **Delete**.

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. Log in to Configuration Hub as an administrator.
2. Go to **Proficy Authentication > Security > Users**.
3. Select +
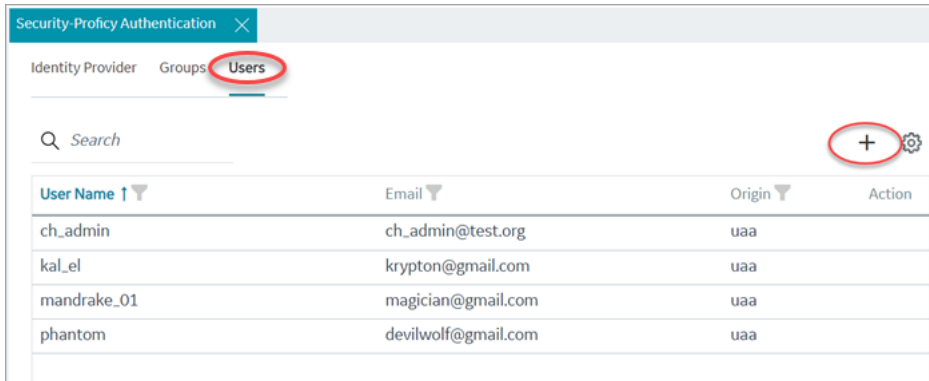
The **Add User** screen appears.

4. 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.

5. 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 plugin via. Configuration Hub. If these scopes are not added, then a warning message alerts the user to contact Admin.

Scope	Description
`uaa.admin`	This scope indicates that this is a superuser.
`clients.write`	This scope resets the Security plugin's admin client secret.
`password.write`	This admin scope enables to change the user password. ✏️ **Note:** This scope is assigned to all the UAA/LDAP/SAML users by default without the need to assign manually.

Default `ch_admin` has all the three scopes.

For user accounts originating from LDAP or SAML, refer to

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.

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.
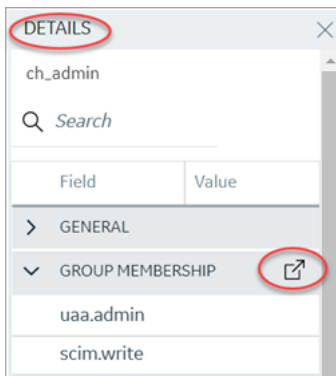
   The **Group Membership** screen appears.
4. Select the check box for the groups you want to add the user as a member.

   To remove a group, clear the check box.
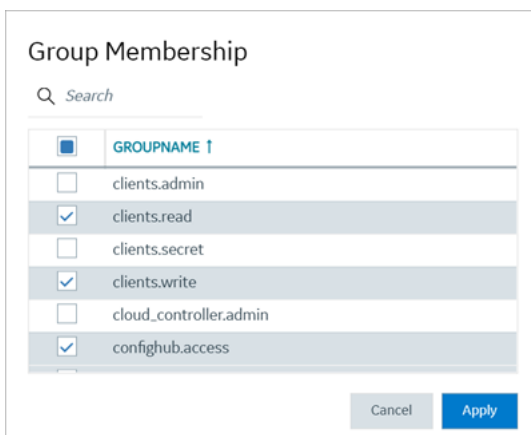
5. Select **Apply**.

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

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.
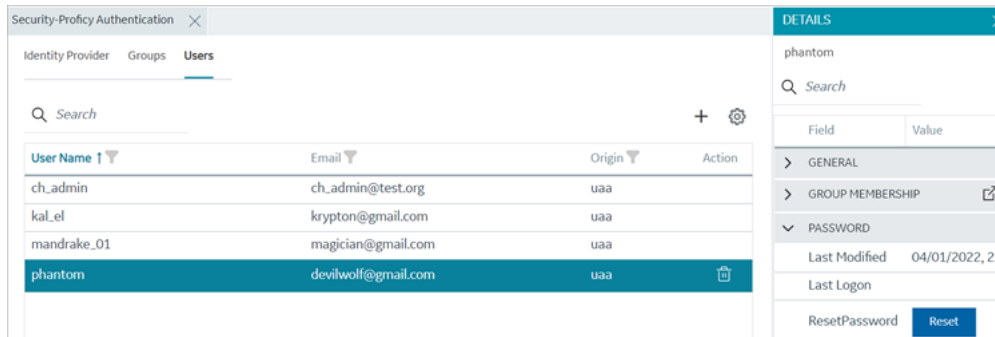
3. Select **RESET**.

   The **Password Reset** screen appears.

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

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.
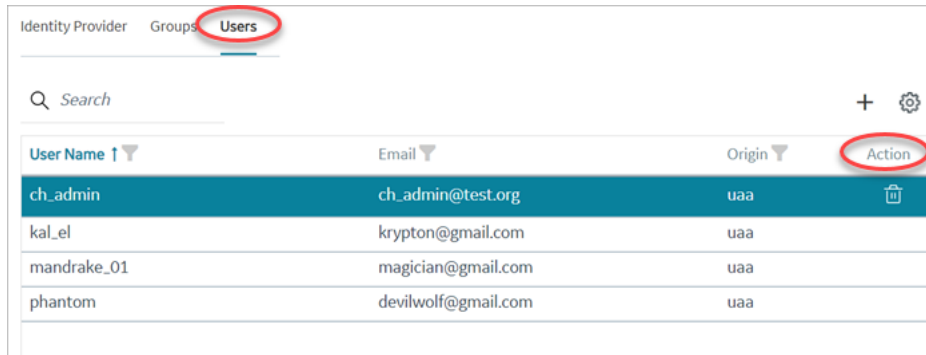
Log in to Configuration Hub as an administrator.

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.

3. Select .

   A message appears to confirm the delete action.
4. Select **Delete**.

The user account is deleted from the Proficy Authentication database.

Windows Auto-login

This topic describes how to configure the Windows system so that the currently logged-in user is automatically log into Proficy products when launched.

With Windows Auto-login configured, once you log in to your system, you are not required to enter your login credentials again to access the Proficy Authentication application on the same machine.

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 71)*.
2. Create a service principal for your user account *(on page 73)*.
3. Generate the Kerberos keytab file *(on page 74)*.
4. Update the Proficy Authentication .yml file *(on page 77)*.

5. Configure LDAP Identity Provider *(on page 46)* 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 78)*.

Figure 1. Windows Auto-login - Deployment Topology and Configuration
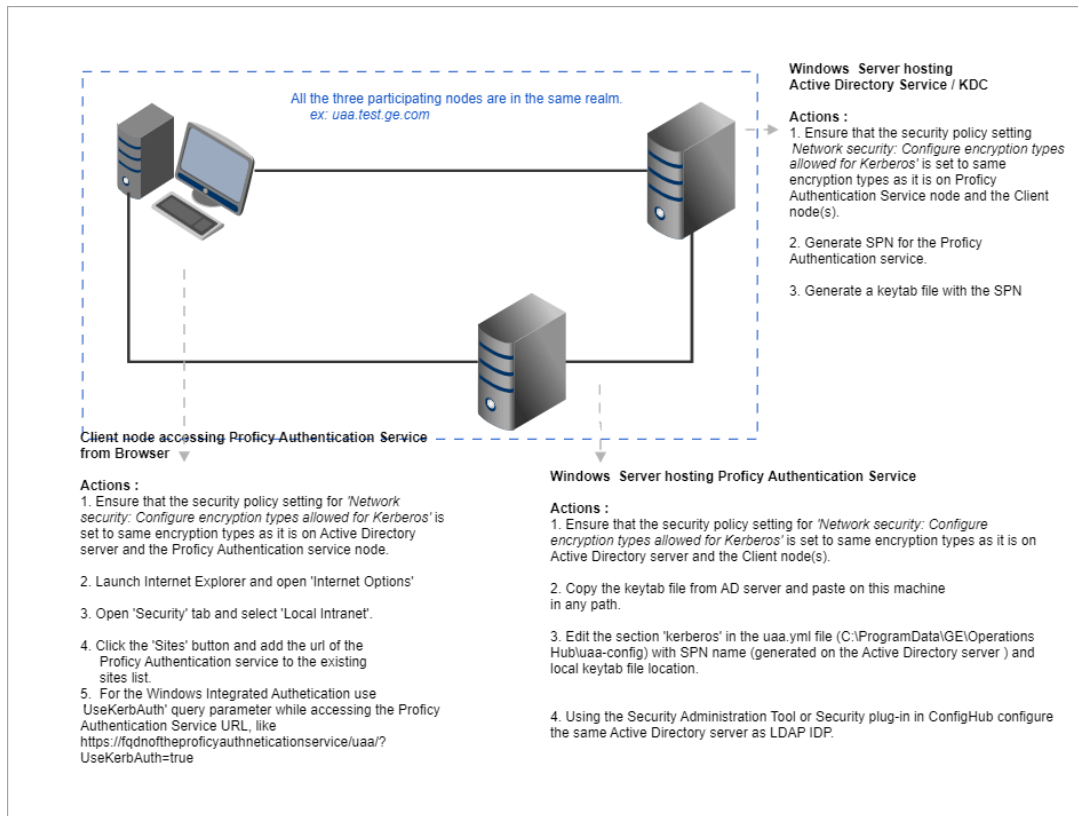
Configure Security Policy

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**.
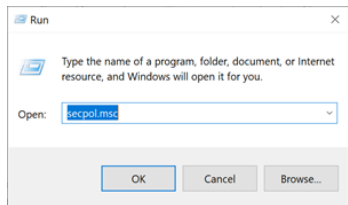
2. Navigate to **Security Settings > Local Policies > Security Options**.
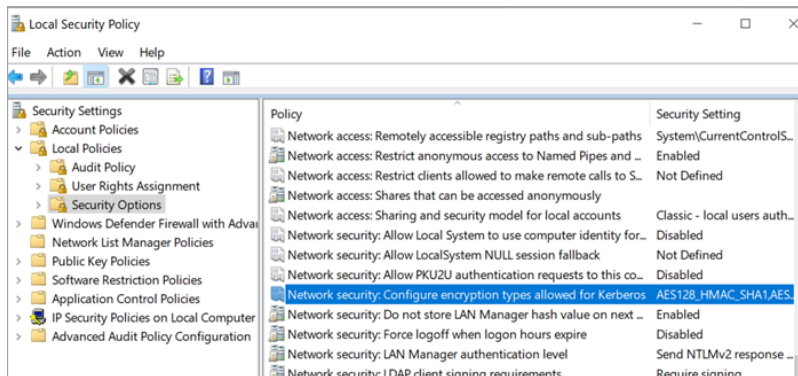
3. Double-click and open `Network security: Configure encryption types allowed for Kerberos` security policy setting.
4. Select the valid encryption types that you want to use as shown in the figure. Ensure that the selection is same across all the participating nodes.
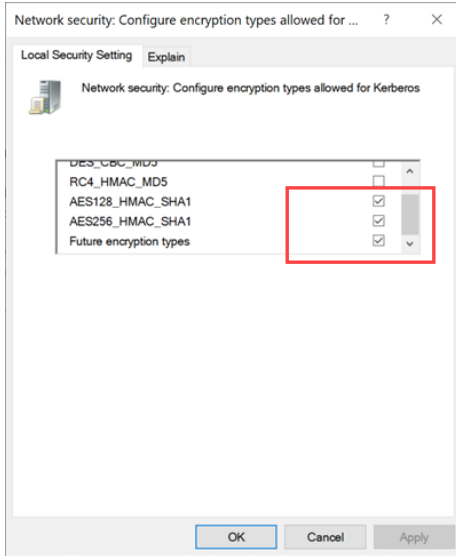
> **Note:**
>
> In our current documentation, we use `AES256_HMAC_SHA1` encryption type in our example
> code to generate the keytab file.

For more information refer to Microsoft documentation on security policy settings.

Create Service Principal

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.
- Configure Security Policy *(on page 71)*

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
	For example, `HTTP/win16-phantomhost.uaatestad.ge.com`
`<user account>`	Dedicated dummy user account created for Proficy Authentication service. For example, `ghost1`.

The service principal name is created.

Generate Keytab File

Generate the Kerberos keytab file.

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 pincipal name> -mapUser <user account> -mapOp set -pass <password> -crypto AES256-SHA1 -pType KRB5_NT_PRINCIPAL`

Code	Replace With
`<filename>`	Name of the keytab file. The file is created at the default location. You also have the option to specify an absolute path for file creation. For example, `-out c:\Documents\myskullcave.keytab`.
`<service pincipal name>`	Enter the service principal name that was created in the following format: `HTTP/win16-phantomhost.uaatestad.ge.com@UAATESTAD.GE.COM`
`<User account>`	Enter the same dummy user account that was used during creating the service principal name.

Code	Replace With
	For example, `ghost1`.
`<password>`	Proficy Authentication dummy user account password.
`AES256-SHA1`	Encryption algorithm you want to use.
`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 Gei321itc -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 (0x8b551a22050935e9ace848cacbacc86a4eb845e63b6461d4f31b7d815158cf6c)
```

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.
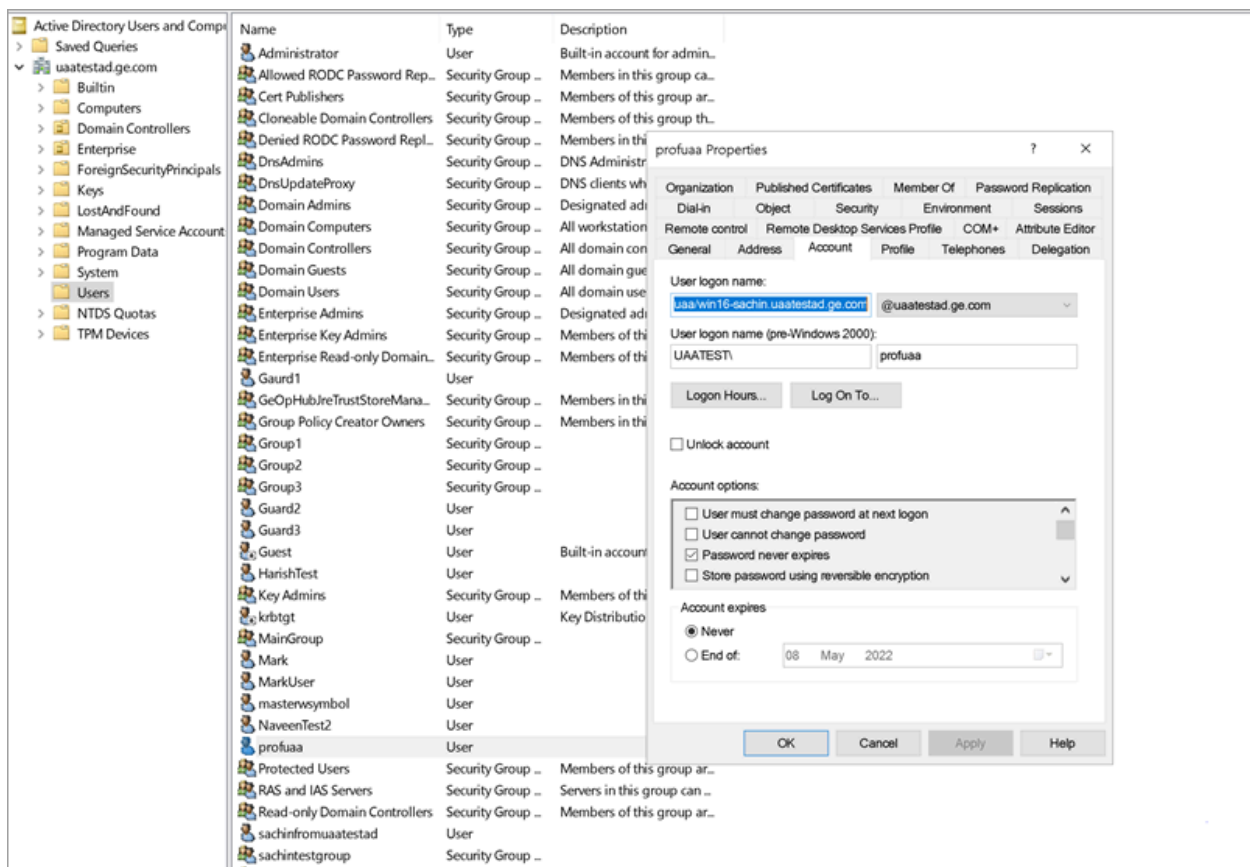
- Copy the keytab file on the machine, where Proficy Authentication is installed.
- Update the Proficy Authentication .yml file *(on page 77)*.

Update YAML File

Update the Proficy Authentication .yml file.

- Generate Keytab File *(on page 74)*.
- 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\GE\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 *(on page 73)*.
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 .yml file is updated .

Configure Browser

Configure the browser settings for Kerberos authentication.

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

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.

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

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

 TlRMTVNTUAABAAAAl4II4gAAAAAAAAAAAAAAAAAAAAAKADk4AAAADw==

org.springframework.security.authentication.BadCredentialsException: Bad Credentials excpetion. 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
```

Client is using a URL with a FQDN of the UAA host, but the DNS server does not have a record for that FQDN.

--[to be updated]--

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)
```

Chapter 3. iFIX in Configuration Hub

Overview

Introduction to iFIX Web Configuration

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

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

Use the Navigation panel to open any of the configuration panels.
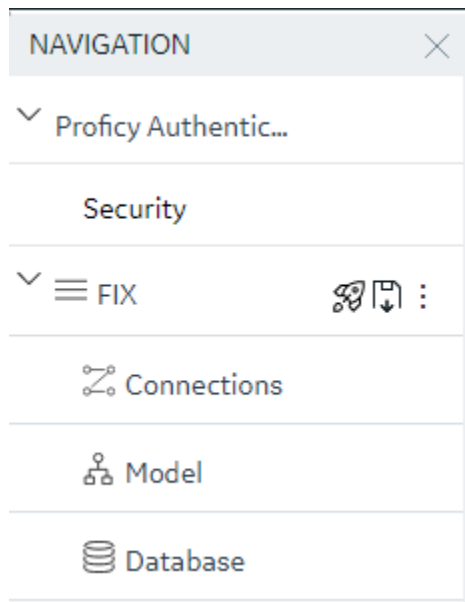
The Navigation panel can be closed to give you more real estate in your IDE and can be re-opened again from the common toolbar on the top right.
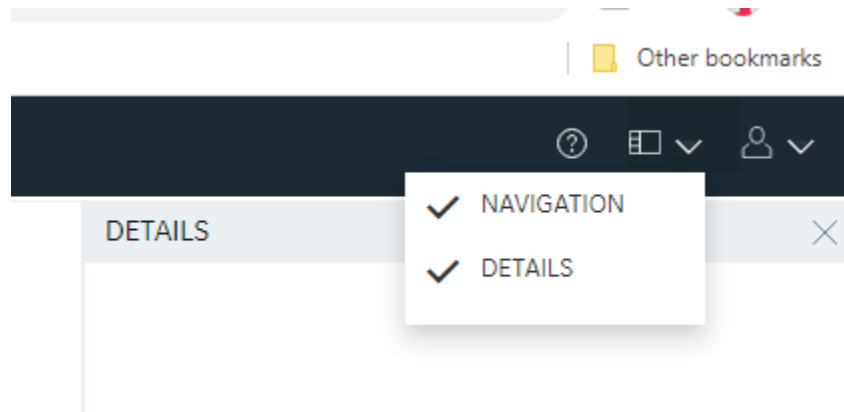
Integrated Development Environment

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.

TestConfiguration 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.
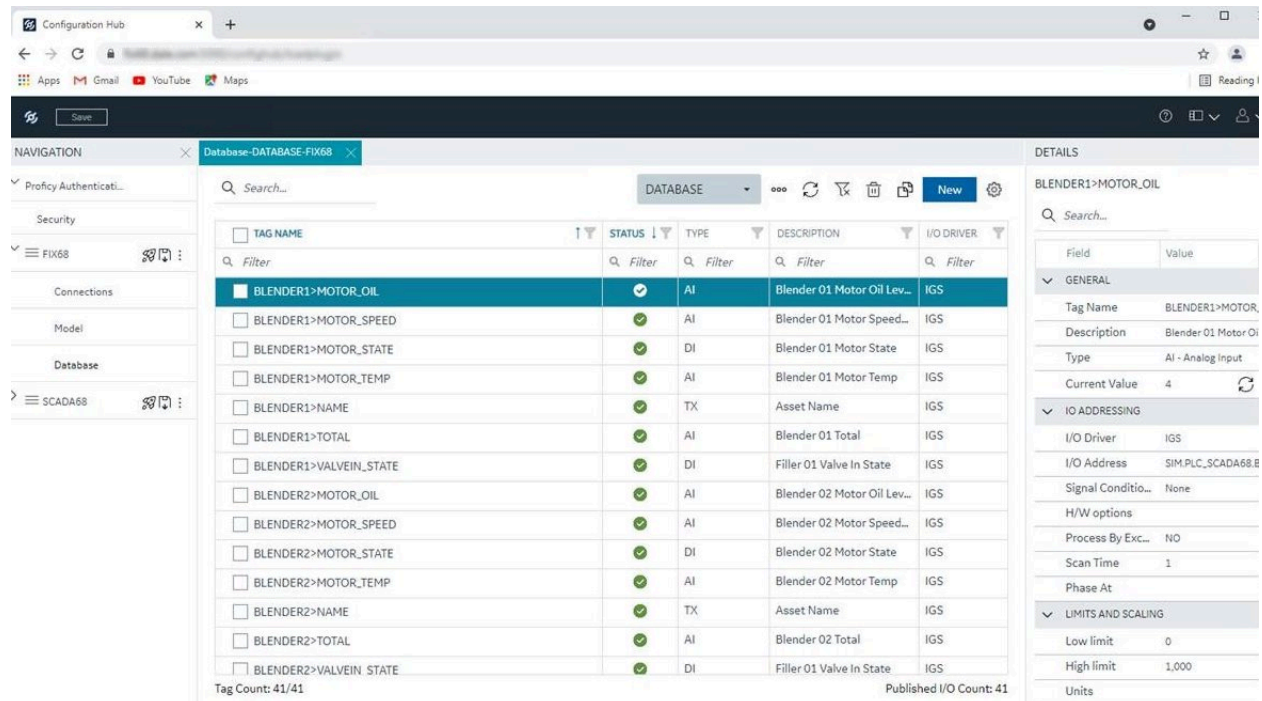
Prerequisites to Use Configuration Hub with iFIX

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

1. You must enable security before you can log in to TestConfiguration 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 logged in user should belong to the Application Designer group or have all of the iFIX application features that the Application Designer group. In Proficy Authencication, this group is named the **scada.fix.shared.APPLICATION_DESIGNER** group. The Application Designer group contains the following iFIX application features:
   - Database Block Add-Delete
   - Database Manager
   - Database Reload
   - Database Save
   - Enable Task Switching
   - OPC UA Configuration Tool
   - Runtime Visual Basic Editor Access
   - WorkSpace Configure
   - WorkSpace Runtime
   - WorkSpace Runtime Exit
4. You can use either a user's login name or the Full Name to login to TestConfiguration Hub.
5. TestConfiguration Hub can only be run with iFIX SCADA or Historian Server nodes.
6. An iFIX node configured to use TestConfiguration Hub should be registered using the Registration tool (available from Applications menu in Workspace) if TestConfiguration Hub is not installed along with iFIX. See the iFIX Plugin Registration *(on page 88)* 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 TestConfiguration 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 TestConfiguration 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

TestConfiguration Hub supports product registrations local to the same machine as TestConfiguration Hub and as remote plugins. For a remote plugin registration, you do NOT need to install TestConfiguration 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 TestConfiguration 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 TestConfiguration Hub instead of installing TestConfiguration Hub again. This allows you to open TestConfiguration Hub centrally from a browser and be able to see and configure multiple product instances from that one installed instance of TestConfiguration Hub.

iFIX – When you use the integrated installer to install TestConfiguration 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 88)* for more details.

Historian – To register with an existing TestConfiguration Hub during the Historian Web-based Clients install, when prompted, enter the client IDs & client secrets supplied during the original TestConfiguration 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 TestConfiguration Hub. TestConfiguration 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 TestConfiguration 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 TestConfiguration Hub to complete the registration.

Configuration Hub Server Registration

Configuration Hub

SERVER NAME

[   ] 🎖 Trusted

SERVER PORT

[5000]

[Test Server Connection]

Create User Friendly Plug-in Name

PLUG-IN ALIAS NAME

[FIX]

Configuration Hub Administration Credentials

CLIENT ID

[Enter confighub server client id...]

CLIENT SECRET

[Enter confighub server client secret... 👁]

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

Proficy Authentication

SERVER NAME

[   ] 🎖 Trusted

SERVER PORT

[443]

[Test Server Connection]

Proficy Authentication Credentials

☐ Use Configuration Hub Authentication Credentials for Proficy Authentication.

CLIENT ID

[Enter Proficy Authentication server client id...]

CLIENT SECRET

[Enter Proficy Authentication server cli... 👁]

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

[Register]

Remote Registration Overview

Remote registration uses the same iFIX Registration process. However, you will most likely need to snter 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 TestConfiguration Hub), or re-register your iFIX product plugin with TestConfiguration Hub when and if your setup changes. iFIX security must be enabled before you can register TestConfiguration Hub.

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

Before you can Register TestConfiguration 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 TestConfiguration 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 TestConfiguration Hubon a domain, you may need to update the HOSTS files on your network with the name of the TestConfiguration 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 clients machine so it can connect properly to the Configuration Hub machine.

Access the Registration Tool

You can access the TestConfiguration Hub Registration tool from the iFIX WorkSpace, on the Applications tab, in the Configuration Hub area. Click **Register** to open the tool.
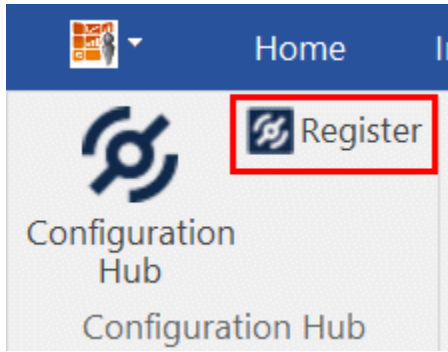
After you launch it, the following login screen appears.
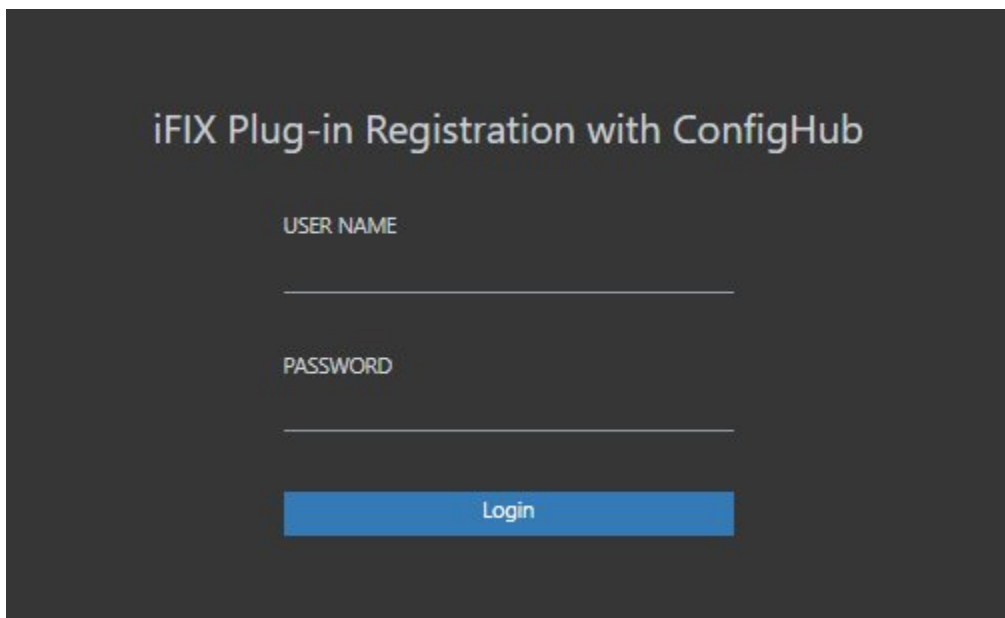
Enter your iFIX user name and password for authentication. The Registration the tool appears, as shown in the following figure.

Configuration Hub Server Registration

Configuration Hub

SERVER NAME

[blurred] 🏅 Trusted

SERVER PORT

5000

[Test Server Connection]

Create User Friendly Plug-in Name

PLUG-IN ALIAS NAME

FIX

Configuration Hub Administration Credentials

CLIENT ID

Enter confighub server client id...

CLIENT SECRET

Enter confighub server client secret... 👁

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

Proficy Authentication

SERVER NAME

[blurred] 🏅 Trusted

SERVER PORT

443

[Test Server Connection]

Proficy Authentication Credentials

☐ Use Configuration Hub Authentication Credentials for Proficy Authentication.

CLIENT ID

Enter Proficy Authentication server client id...

CLIENT SECRET

Enter Proficy Authentication server cli... 👁

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

[Register]

Test the Connection

For both Configuration Hub and Proficy Authentication, first test the connection. Enter the server 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 successfully connected and the server certificate shows as **Not Trusted** (in blue next to the server 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:

After clicking Not Trusted, the Certificate Details window appears. From the Certificate Details window, click **Trusted** in order 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, in the Configuration Hub Server Registration diaog box, 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 TestConfiguration Hub Registration tool:

Field	Description
Server Name	The server name for the TestConfiguration 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 TestConfiguration Hub or Proficy Authentication server. The Client ID and Client Secret was created when you installed the TestConfiguration Hub product.
Client Secret	The client secret associated with the TestConfiguration Hub or Proficy Authentication server. The Client ID and Client Secret was created when you installed the product. You will need to enter the Client Secret if you want to change the server name (update), unregister, or register your TestConfiguration Hub web server. **Note:** If you forget your client ID or secret, you will not be able to register/unregister plug-ins with TestConfiguration Hub or Proficy Authentication. In this case, you would need to reinstall TestConfiguration Hub and/or Proficy Authentication and register all of all the plug-ins again in order to change them.
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	Click to register your TestConfiguration Hub and Proficy Authentication server. This button is only available if the TestConfiguration Hub or Proficy Authentication web server is in an unregistered state. To register TestConfiguration Hub and Proficy Authentication , you'll need the Client ID and Client Secret information that you entered when you installed the product.
Unregister button	Click to unregister your TestConfiguration Hub web server. This button is only available if the TestConfiguration Hub or Proficy Authentication web server is in a registered state. To unregister TestConfiguration Hub, you'll need the Client ID and Client Secret information that you entered when you installed the product.

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)\GE\iFIX) to reset them. This change must be done only when iFIX is NOT running.
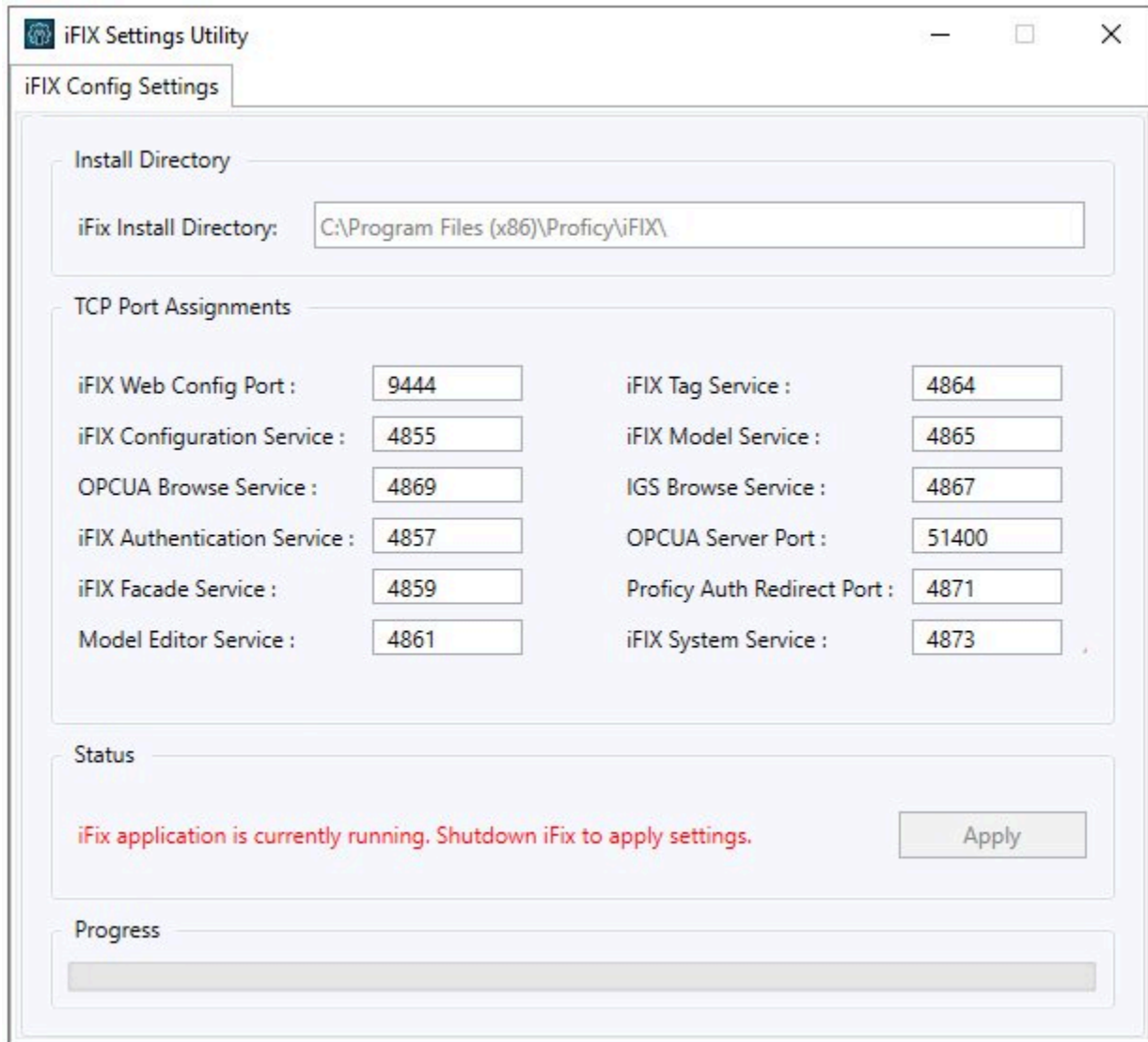
> **Note:**
>
> If you are planning to update iFIX Web Config Port, you must first unregister the iFIX Plugin with ConfigHub. If any of the other service ports are changed, then there is no unregister/register needed.
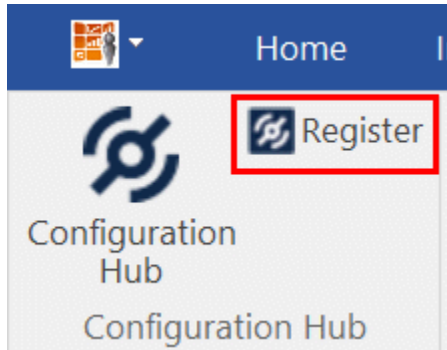
If the iFIX Web Config Port changed, then you must register the iFIX plugin again with TestConfiguration Hub using the Register button in the iFIX WorkSpace. See the iFIX Plugin Registration *(on page 88)* for more details.

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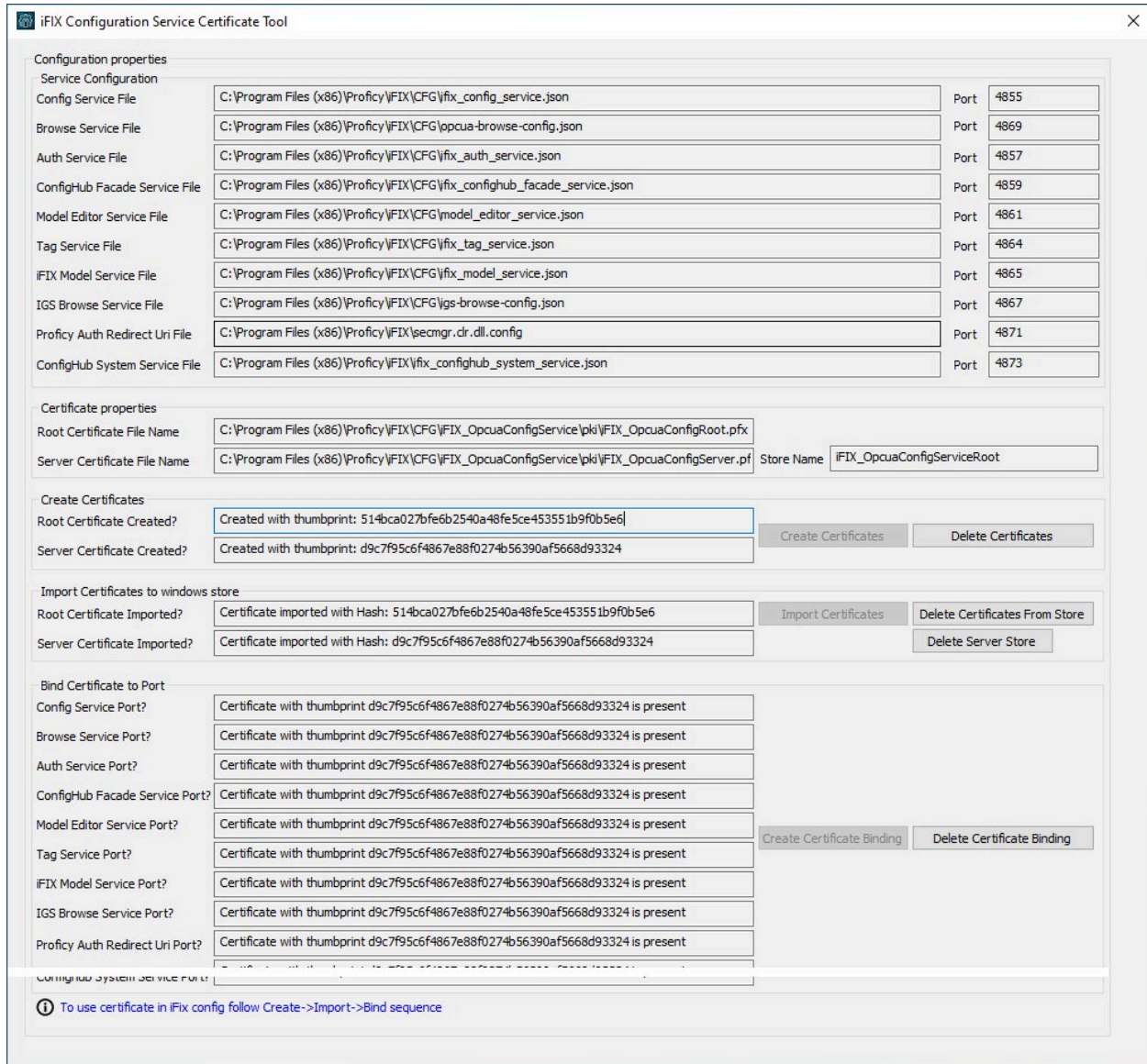
After the binding is complete, close the utility and restart iFIX. The changed ports then will be used by the iFIX.

Access iFIX Web Configuration

1. In the iFIX WorkSpace, select the Applications ribbon and click TestConfiguration Hub Or, on the desktop, click the TestConfiguration 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 e **scada.fix.shared.APPLICATION_DESIGNER** group in Proficy Authentication to have all the permissions necessary to use TestConfiguration Hub.

The TestConfiguration 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 TestConfiguration 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 and IGS.

In the Navigation panel, select Connections, and then select either OPC UA or IGS at the top of the Main
Panel.
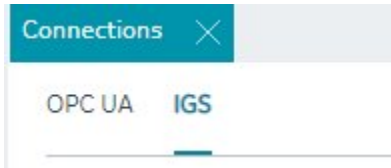
For more detailed information, see:

- OPC UA Connections *(on page 101)*
- IGS Connections *(on page 111)*

OPC UA Connections

OPC UA Connections

iFIX offers an OPC UA Client Driver option that allows you to connect to OPC UA Servers. To use this feature in TestConfiguration Hub, your running iFIX SCADA node must be licensed for this option.

> ✏️ **Note:**
> At this time, TestConfiguration Hub does not support browsing the OUA driver in the Database panel.

Click New to create a new connection. Type in a unique server name and the end point URL of your OPC UA Server. To test the connection, click the Test button. Click the Create button to create the connection for use.

After your connection is created, it appears in the table. Click the ellipsis (...) to the right of your entry to interact with the server.
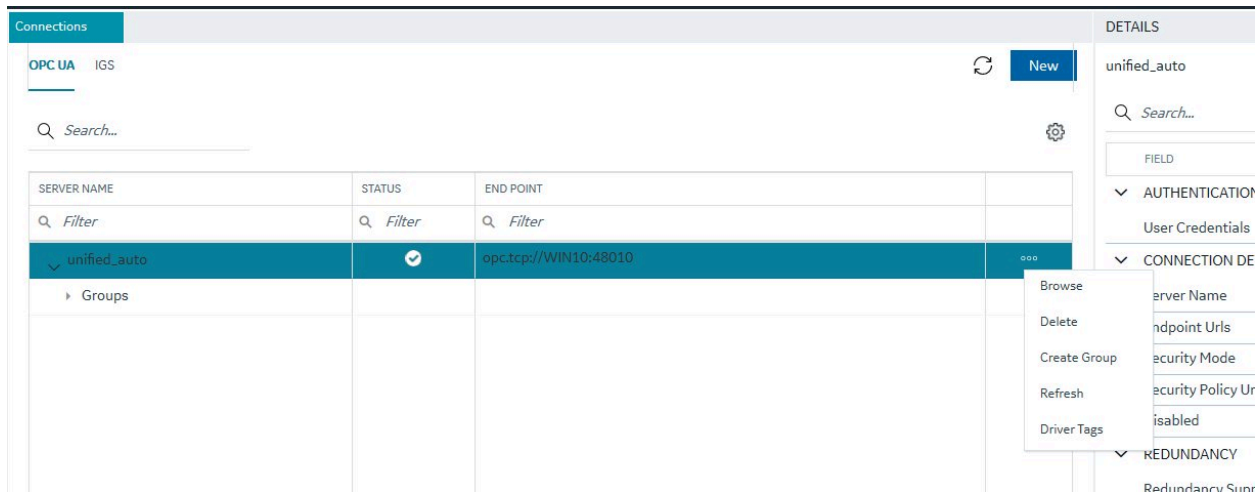
From the popup menu, select Browse to browse the hierarchy available in the OPC UA Server.

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.
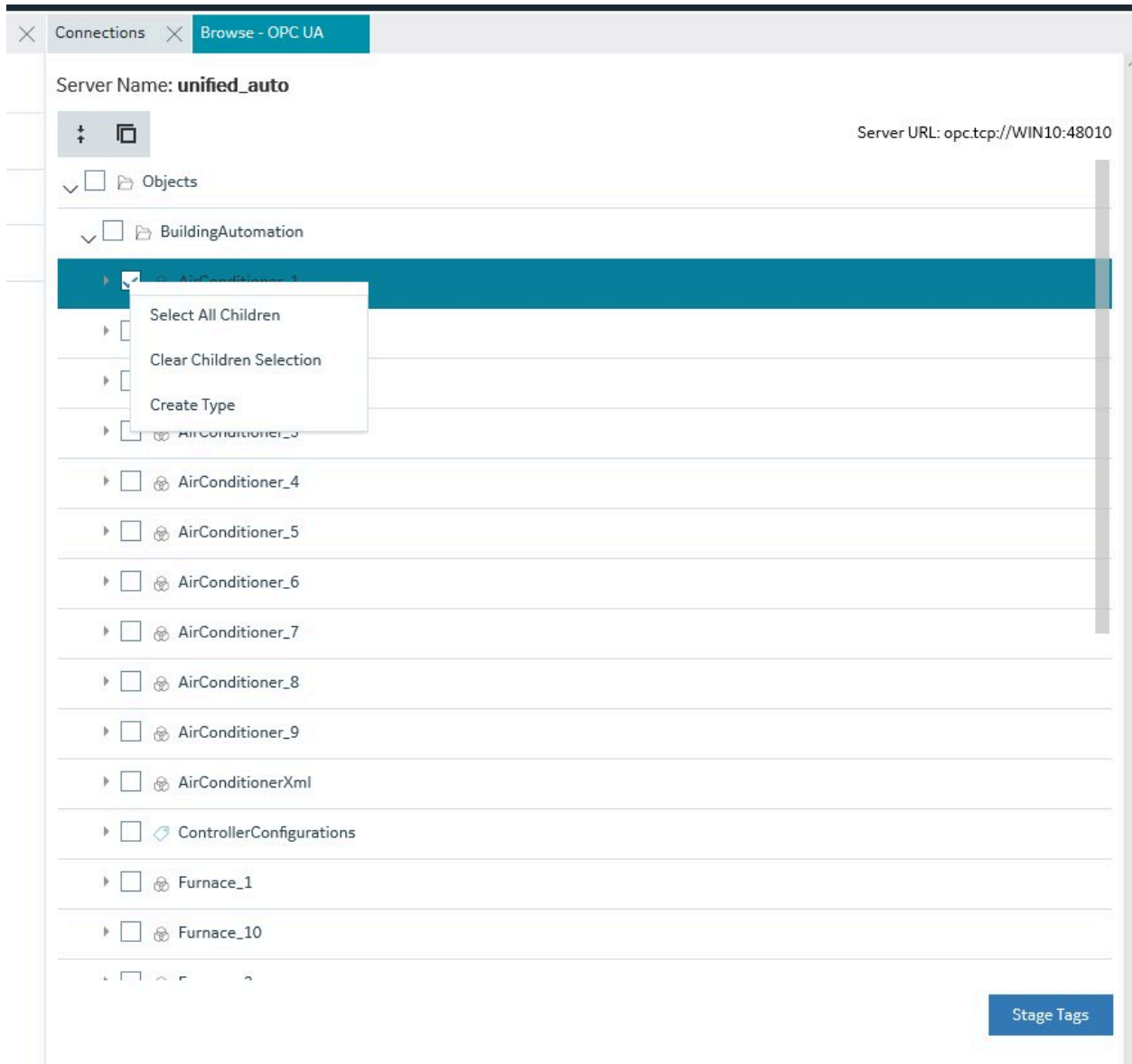
Server Management

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 (-).

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 in to 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

🔍 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	false
∨ REDUNDANCY	
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.

> ✏️ **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.

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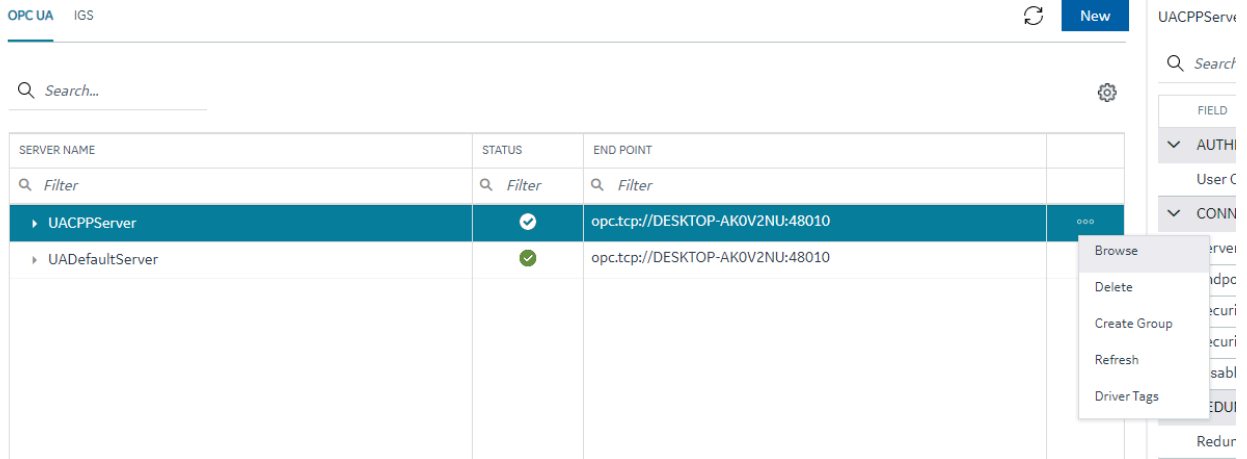
The first step in the tag creation process is to browse the OPC UA Server device and select the tags from the browse content. A parent node's right-click menu can be used to selected bulk child tags for creation.

The next step is to stage the tags and preparing the tags for creation into the iFIX database.
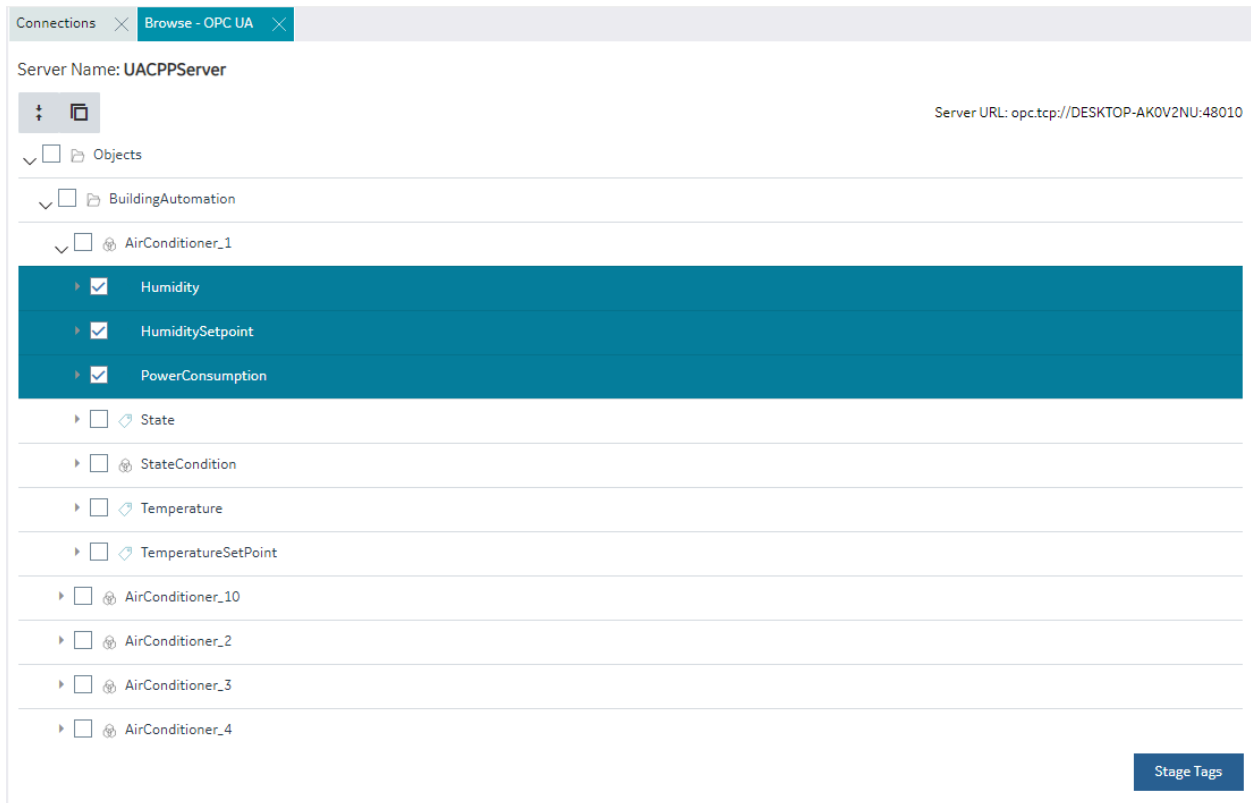
The staging environment allows for modifications to tag names, selection of iFIX block type (default mapped on staging) and selecting a tag for Historian collection.

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

Similar to process of creating tags from an OPC UA sever browse, a model type definition can also be created from the same browse operation. From the OPC UA server browse, an object definition can be selected to create an object type from it.

On selecting an object, the right-click menu provides an option to create a type.
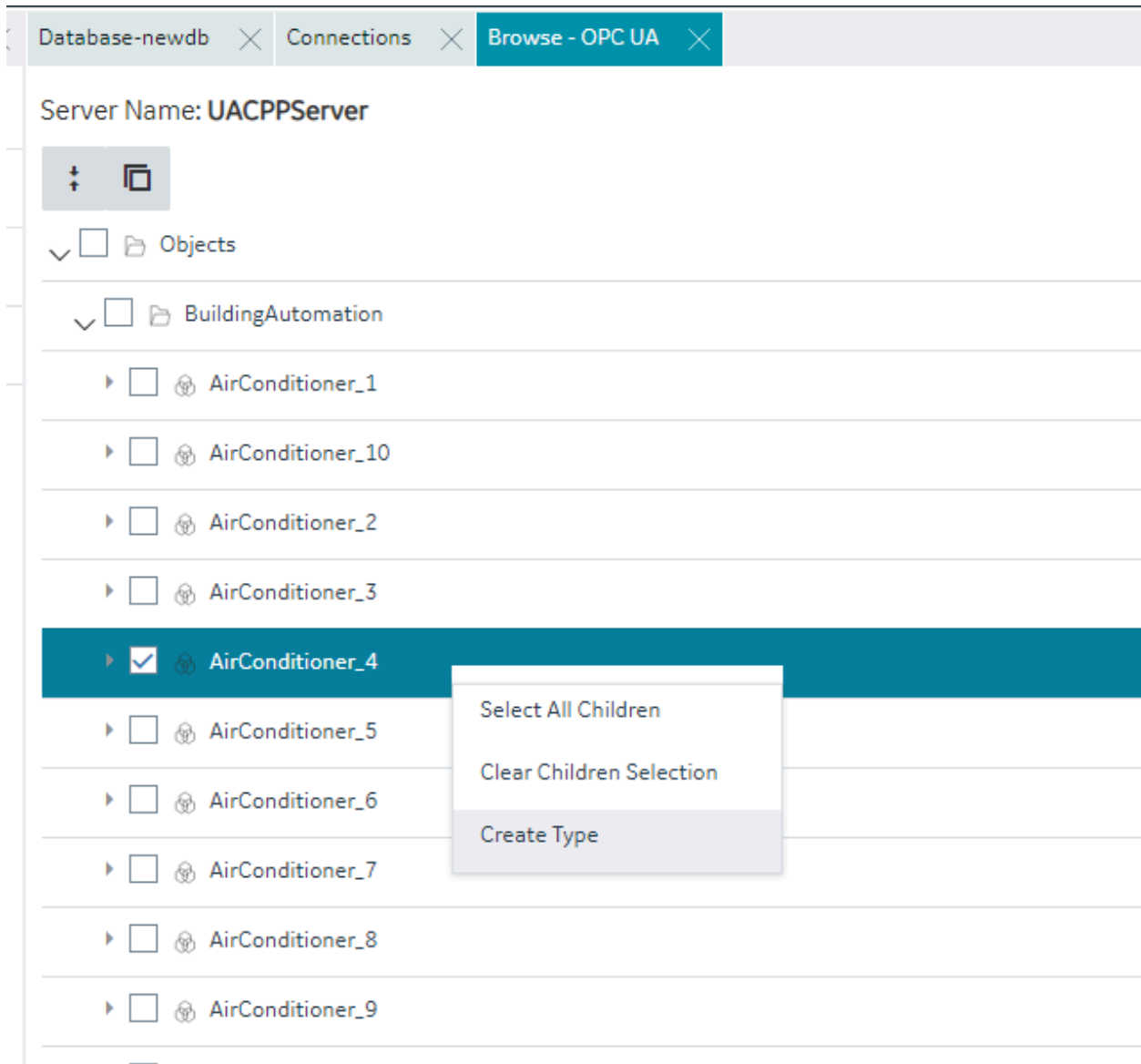
Selection of this menu item displays a pop-up to take the type name as input. New Object Type pop-up shows the class name of the selected object for OPC UA.

New Object Type

NAME

AirConditionerControllerType

DESCRIPTION

Cancel   Create

On clicking Create, the type is created into the model along with tags in the object as variables and values are populated in to the default template of the type.

IGS Connections

IGS Connections

Overview

To use the IGS feature in TestConfiguration 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.
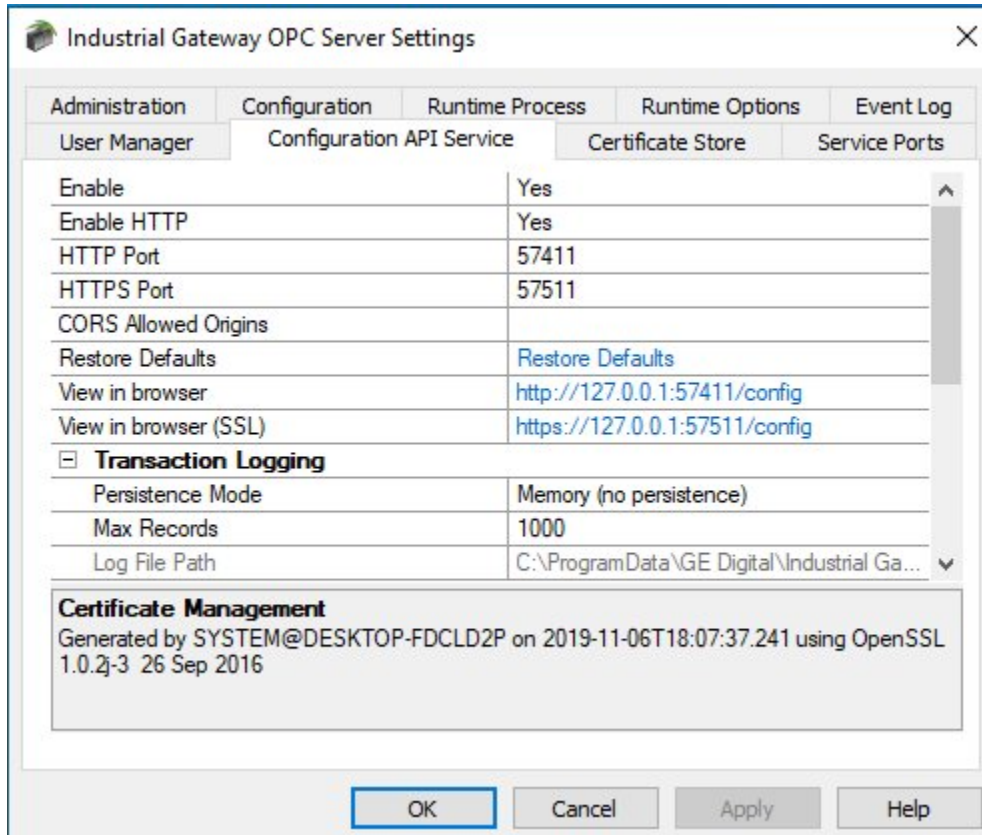
Steps to Add the IGS to the iFIX SCU

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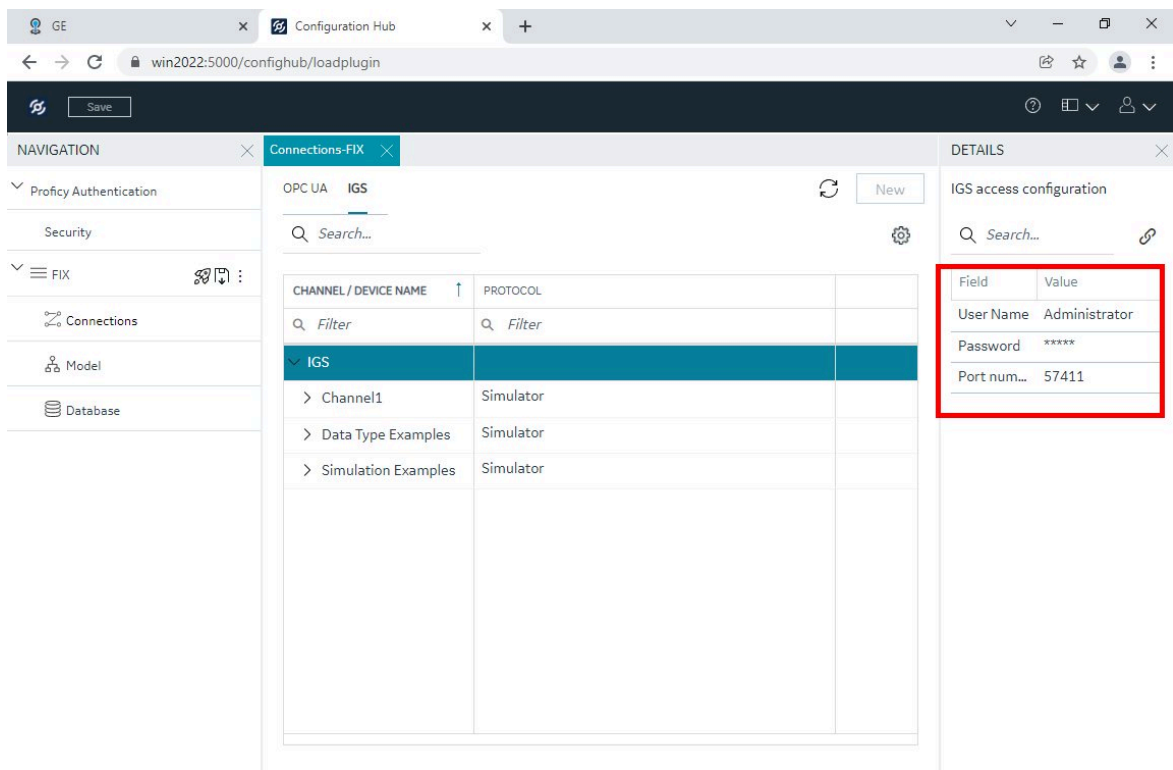
> ℹ️ **Tip:**
> If you need to troubleshoot IGS issues, you can find the IGS log file (igs-browse-config.log) located in the C:\Program Files (x86)\GE\iFIX\ folder, by default.

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

Configuration Example

The following example shows how to access the Settings for the IGS.
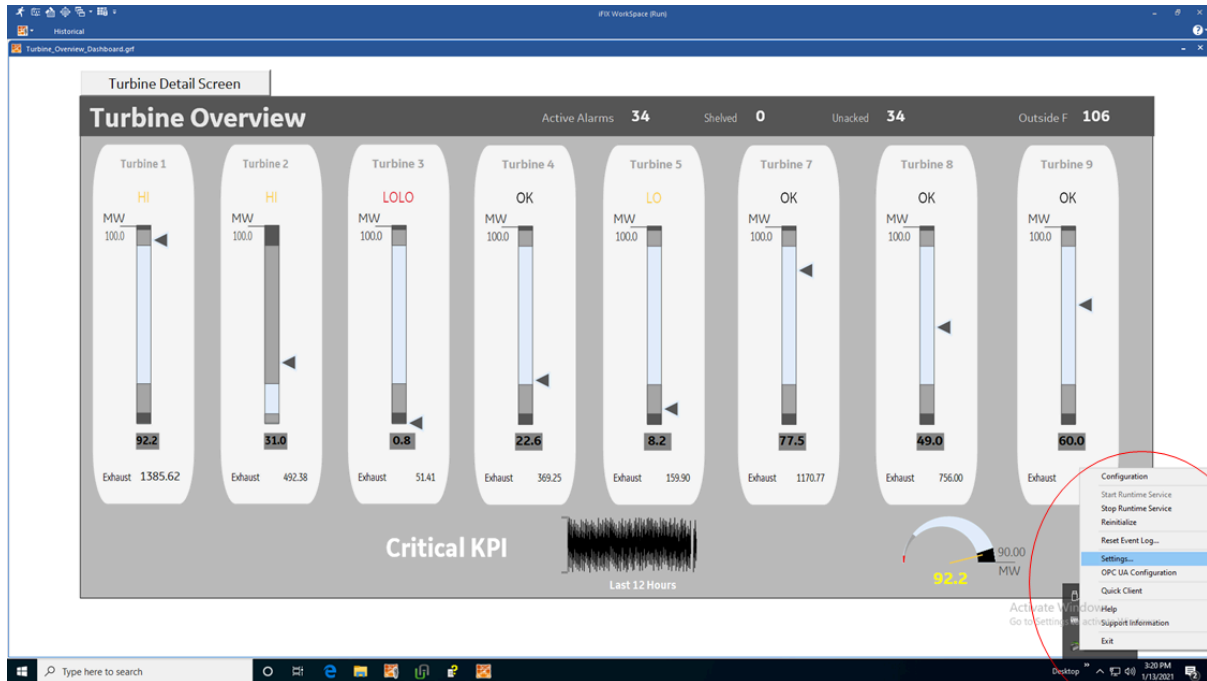
This is the Settings screen for the IGS driver:
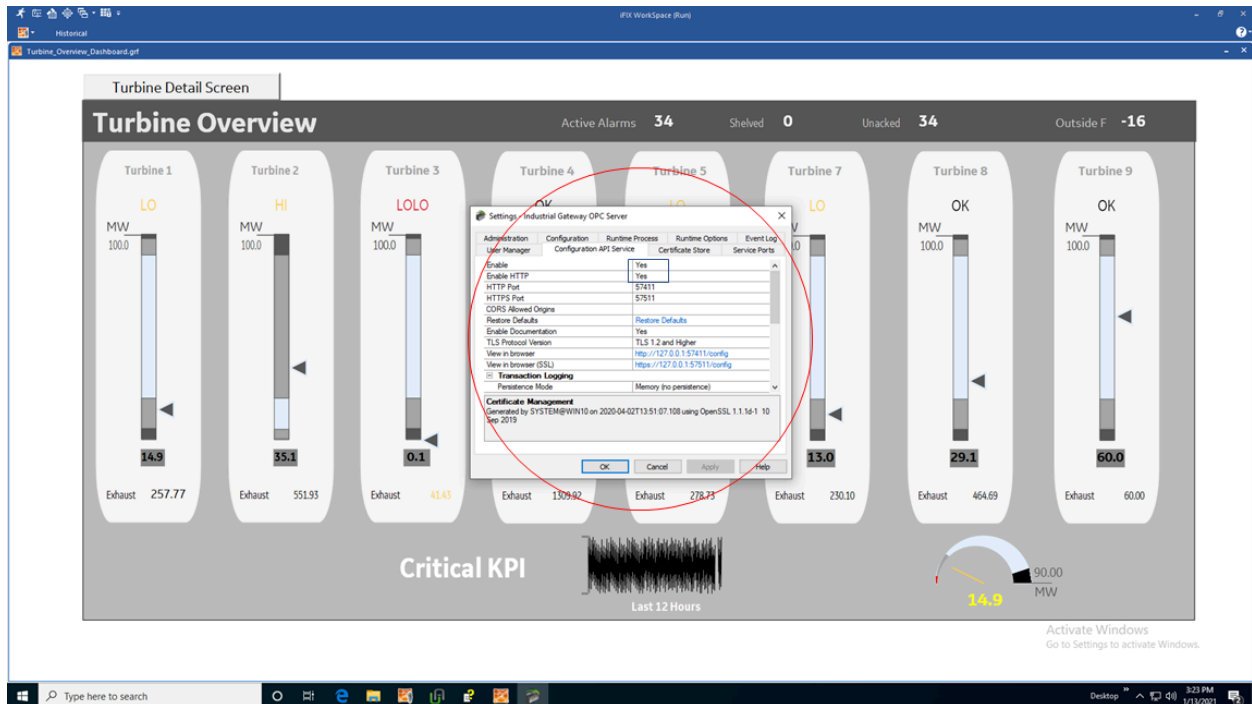
Prerequisites for IGS

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.

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.
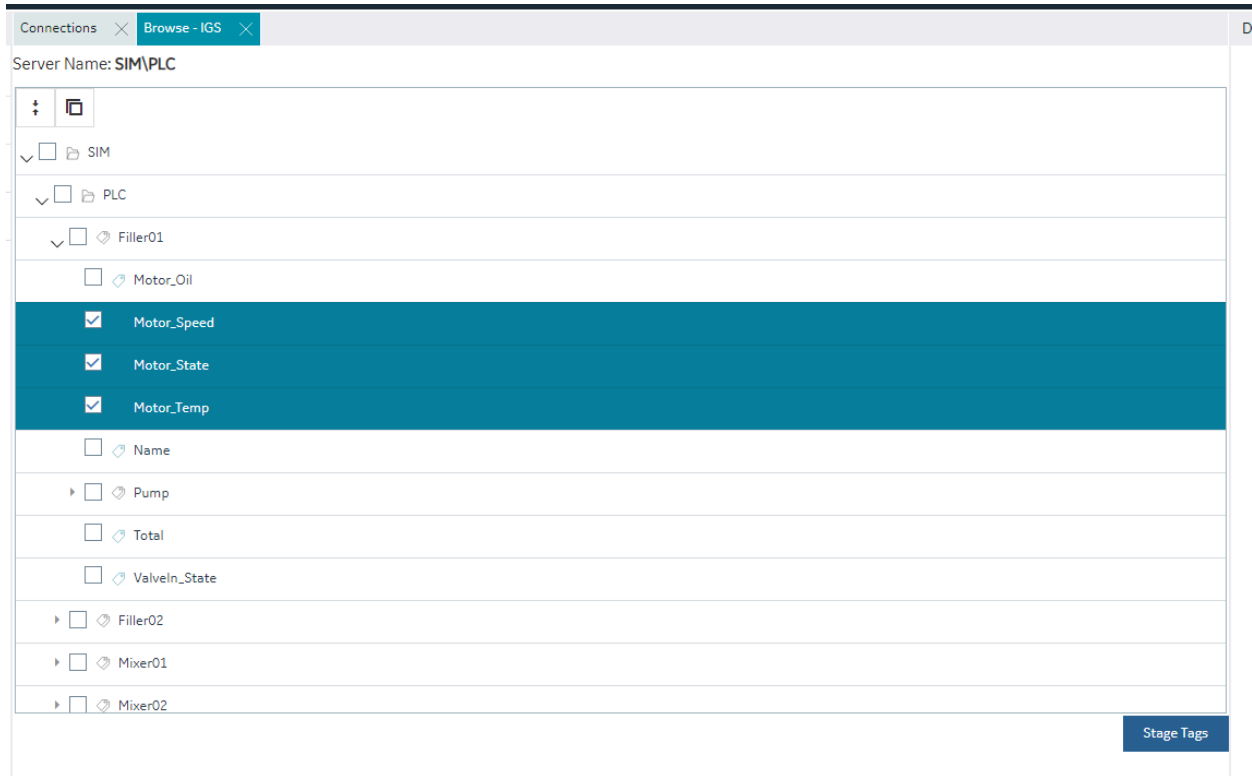
Browse and Create Tags for IGS

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.

Browse and Create Types for IGS

Similar to process of creating tags from an IGS device browse, a model type definition can also be created from the same browse operation. A tag group can be selected to create the object type.

On selecting a tag group, the right-click menu provides an option to create a type. Selection of this menu item displays a pop-up to take the type name input. New Object Type pop-up shows the selected tag group name.

On clicking create, the type is created into the model along with tags in the tag group as variables and values are populated into the default template of the type.
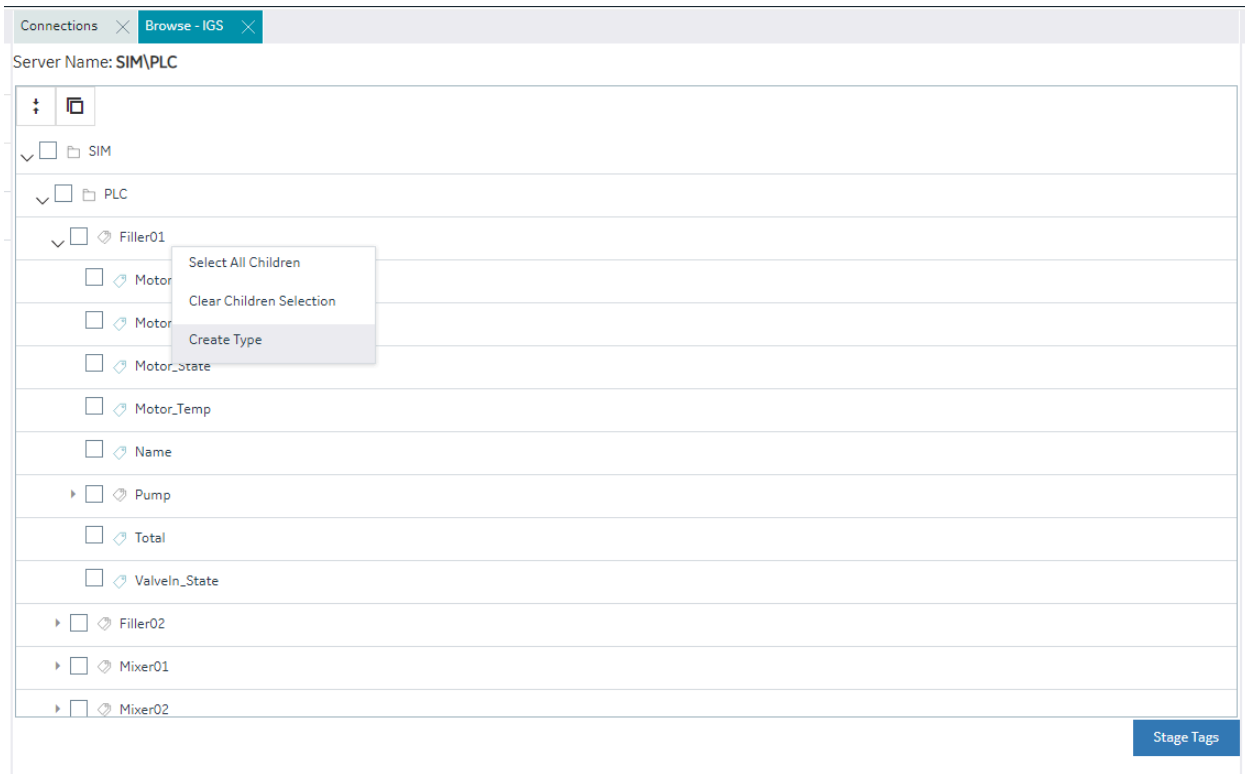
Special Considerations for Enhanced Failover

If using Enhanced Failover, you must be in Maintenance Mode before you log to TestConfiguration 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.

TestConfiguration Hub will not allow you to make changes unless the primary node you are configuring is in Maintenance Mode. It will also not allow any configuration on the Secondary node (you cannot login). All changes to a Failover pair in TestConfiguration Hub must be made on the Primary node.

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 TestConfiguration 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

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 TestConfiguration 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 TestConfiguration Hub on the secondary SCADA.

Server and Group configuration files are found in the PDB\iFixUaClient folder, in Servers and Groups folders, respectively. Each server and group has 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.

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.

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
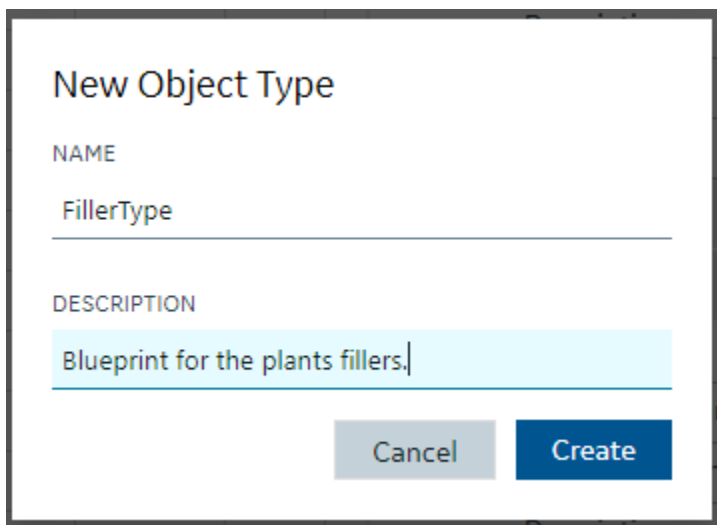
> ⚠ **Warning:**
>
> In the Model panel, when Object Instances or variables under an Object Instance are selected, the properties are populated on the Details panel. When changes are made to the properties of an instance or variable, these changes are saved on a selection change in the model tree.

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.

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.
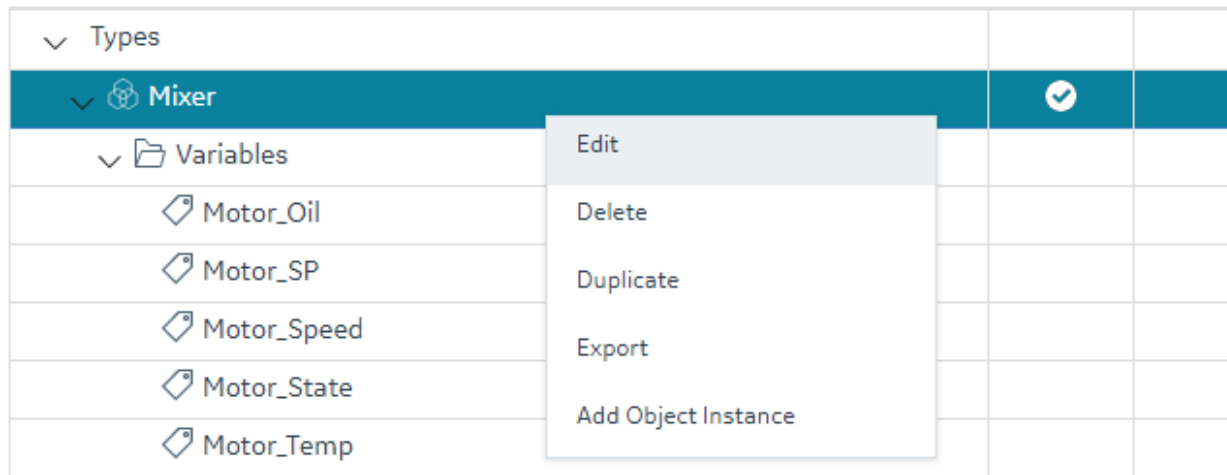
This can be accessed from the context menu in the Type's row in the grid or the Right-Click menu. Double-clicking the Type's row will open the Type Edit panel.
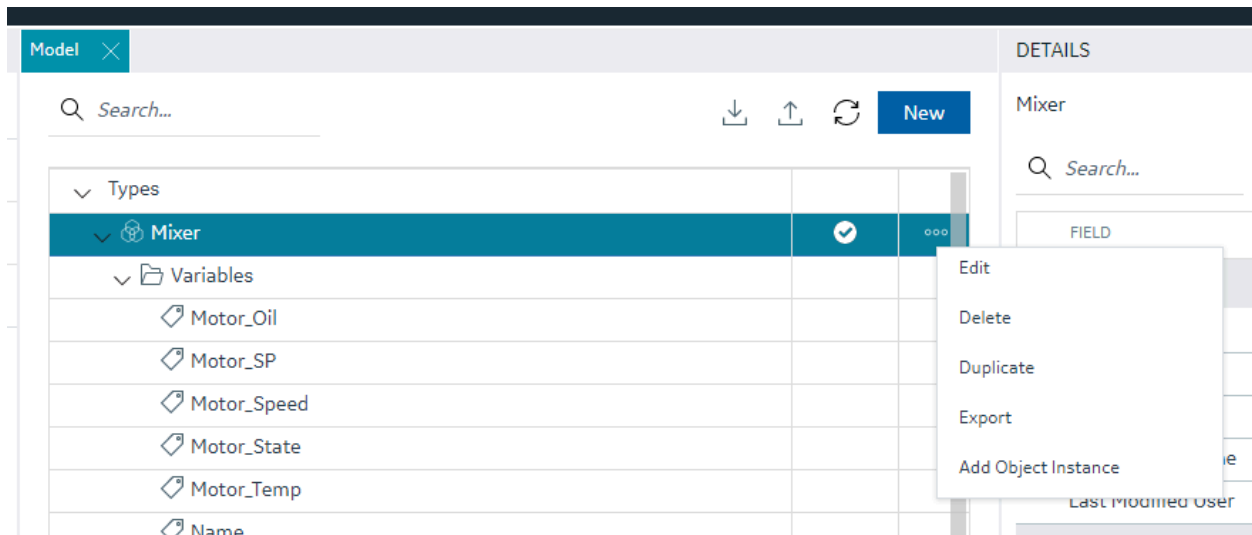
> ✏️ **Note:**
>
> When saving a type, any updates will be automatically pushed to existing Object Instances of type. Depending on the number of instances associated with the type, it could take a long time to update. This may result in the save taking a long time.

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.

Supported Tag Types for Variable Configuration

The iFIX model supports the following tag types for variable configuration:

- Direct Variables *(on page 124)* - Direct variables when instantiated, become tags in your iFIX database.
- Indirect Variables *(on page 125)* - 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 126)* - 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

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.

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.
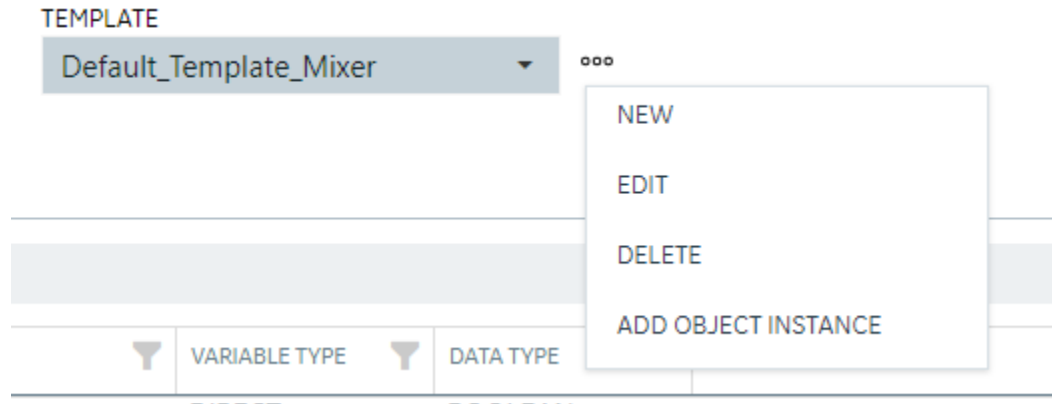
What's Stored in a Template

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.

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.
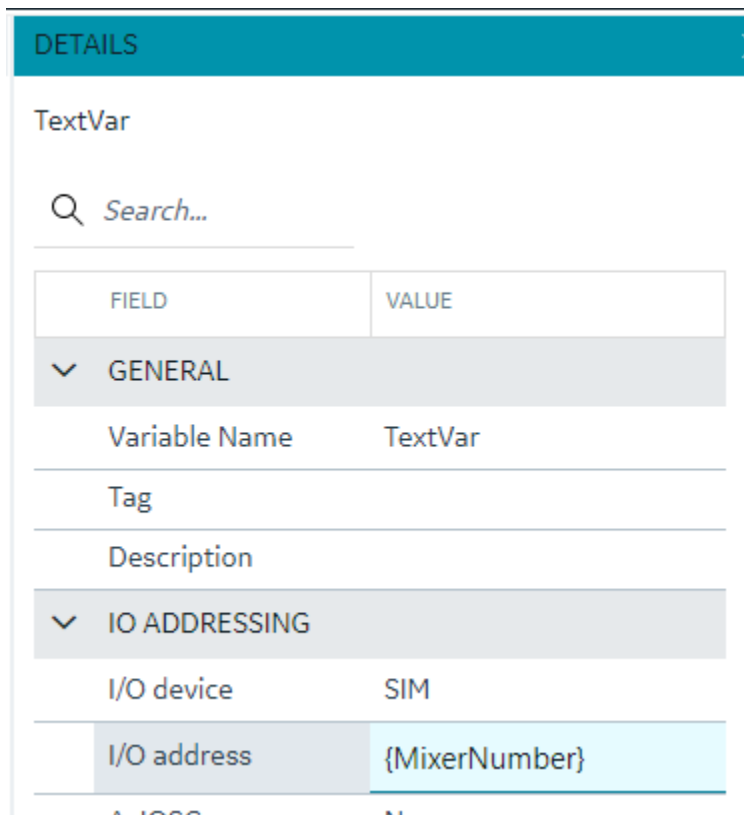
Substitutions

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 placeholder inputs through substitutions. 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.

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.
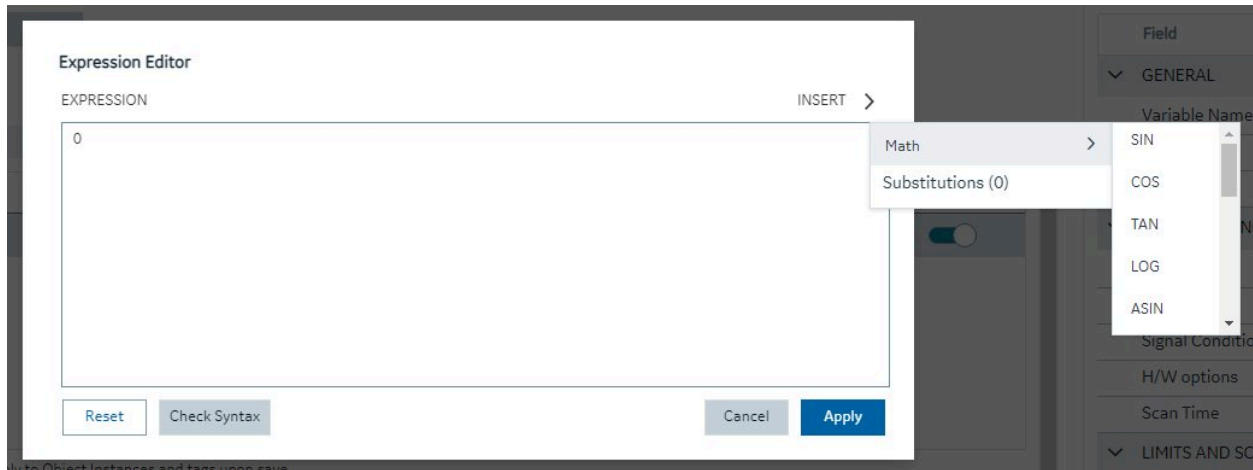
You could also launch expression editor from the property value cell to build the expression.
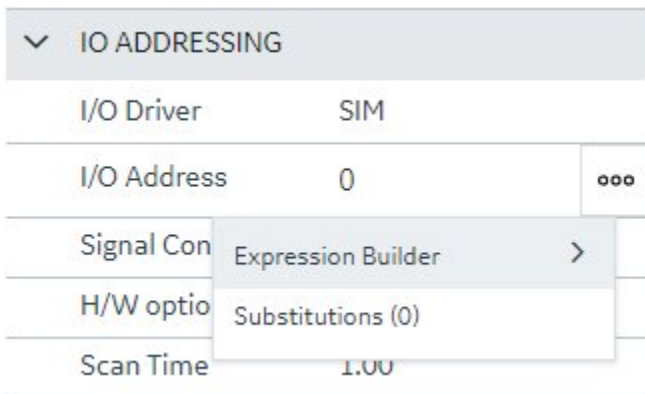
For example, if you were defining a Pump type and create a variable called RPM, you could create a substitution for High Limit called "RPM_HighLimit" to define alarm limit values for this variable, and you could use an expression like Alarm Hi – "{RPM_HighLimit – 20}". The substitution value can be set 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.

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

Overview

The Model can be exported or imported for working on outside of TestConfiguration 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.
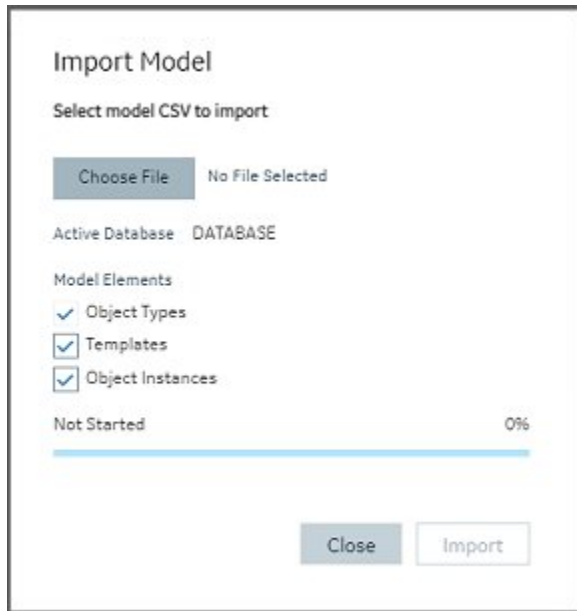
Exporting a Model

To export a model click the export button (⤒). The Export Model dialog box appears where you can specify
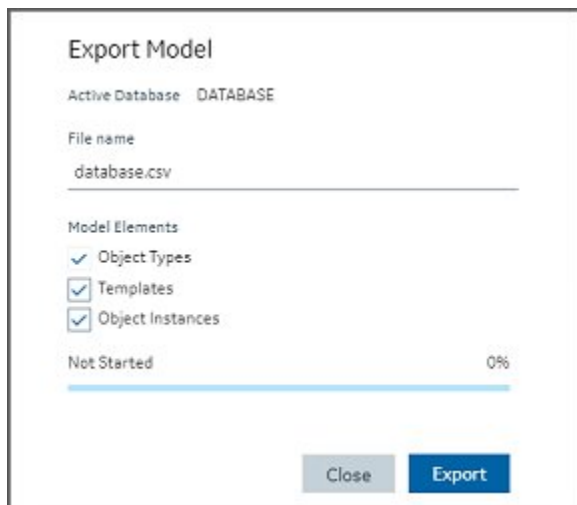
Model Tags in iFIX

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
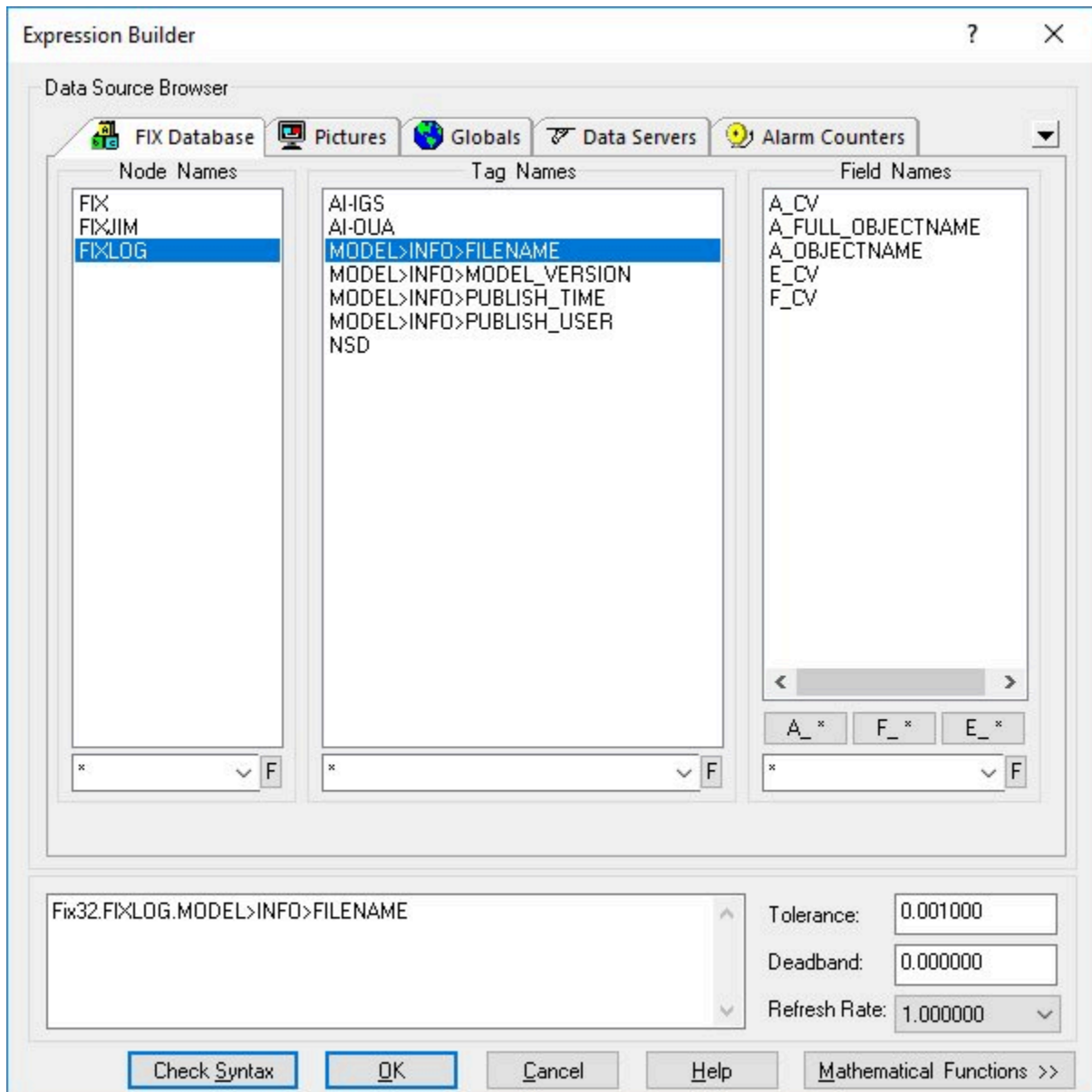
Notes on the Example

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 TestConfiguration 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.
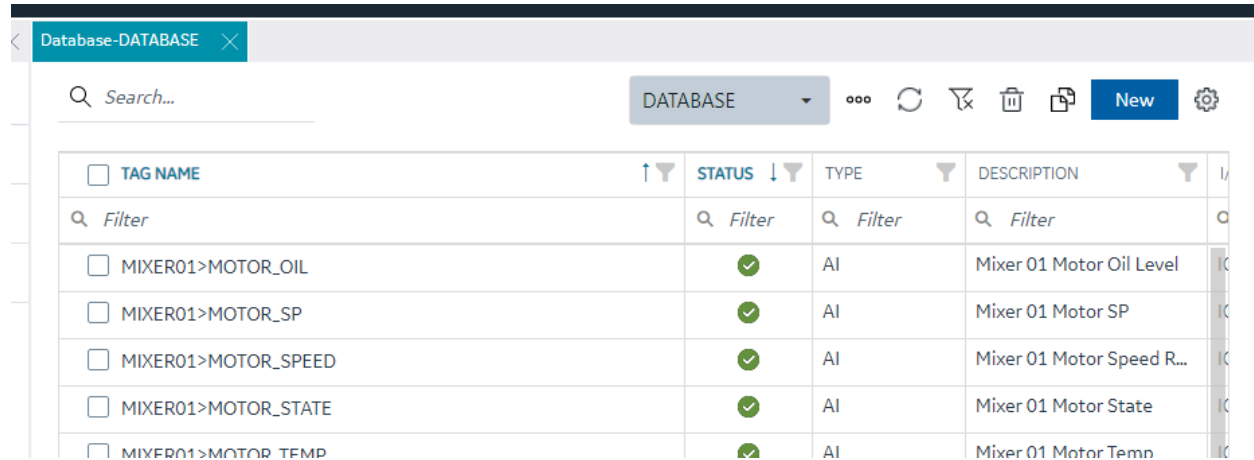
The currently active iFIX database is what will show in TestConfiguration Hub and is what will receive all operations. This is true regardless of how many users are connected to and configuring the same database. Changes to the database, both published and unpublished, are shared across users and browser sessions.

Refer to the following sections for more information about the iFIX Database panel:

Grid Features

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.

When the active database changes from anywhere, the grid should notify you and ask you to refresh. If at anytime 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.
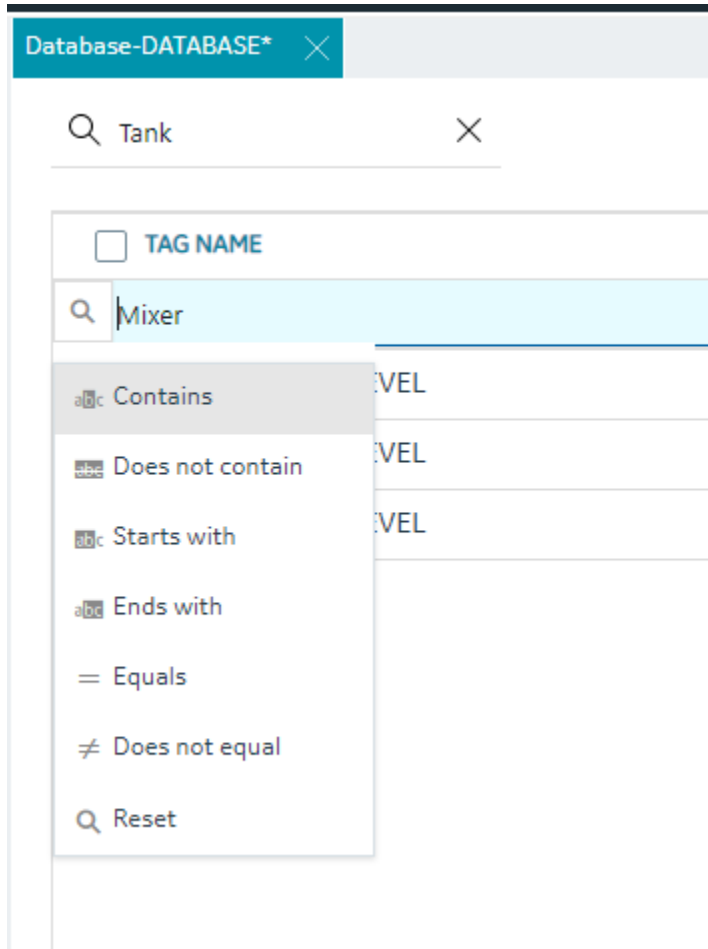
Filtering

Each column also has the ability to 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:
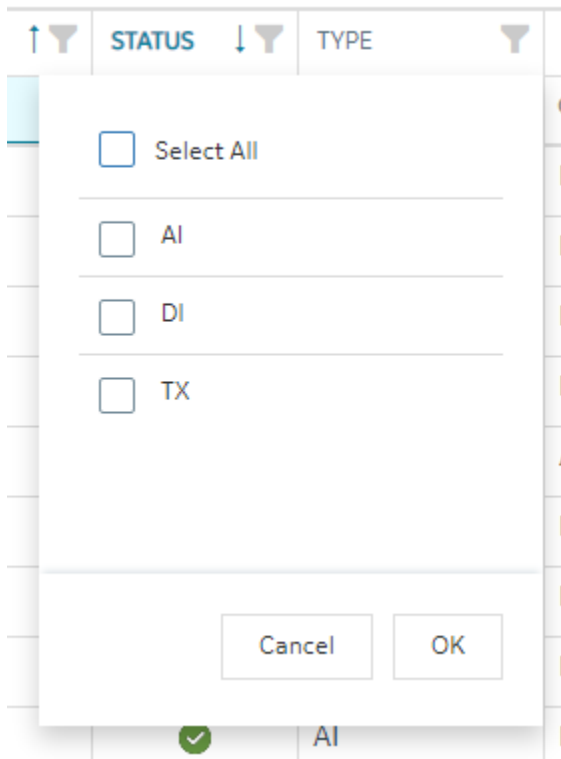
Sorting

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:
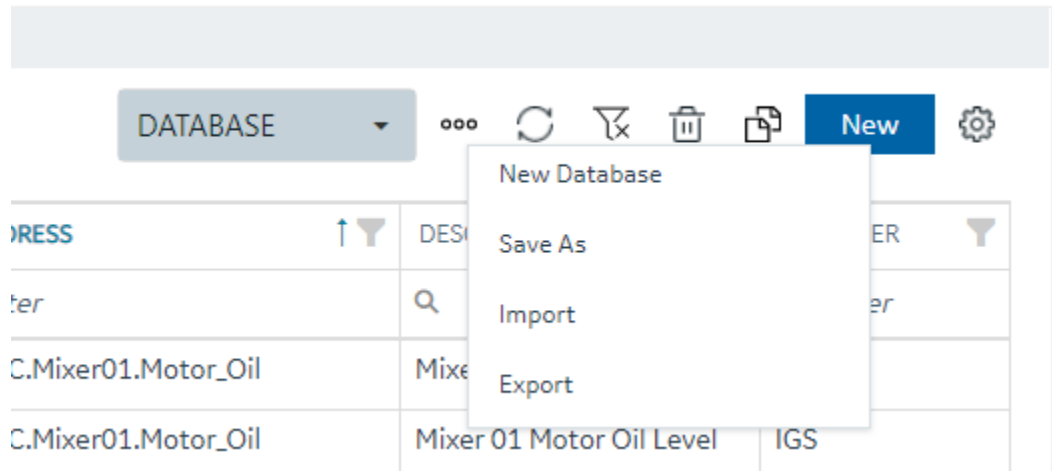
For more information on these icons, refer to the following table.

Item	Description
test ▾	Click the drop-down to switch to another database.
ᵒᵒᵒ	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.
New	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 (e.g. AI, AA, MDI, etc)
- 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.
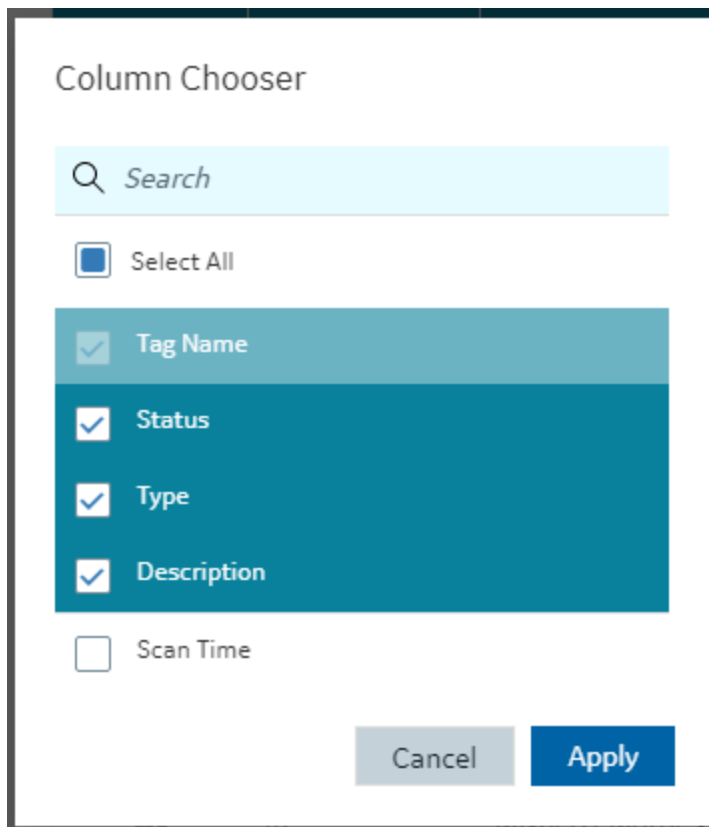
Database Details Panel

Editing database tags is done via the Details panel after selecting a particular tag in the Database panel.

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 type 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.
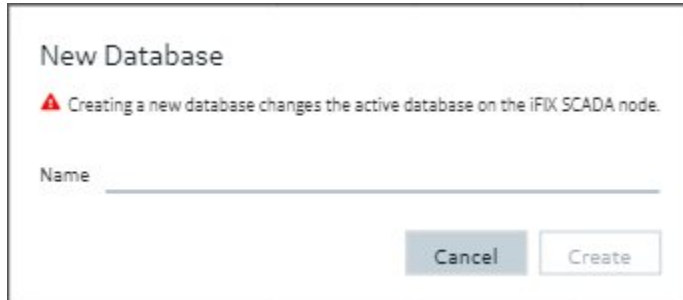
Database Management

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.

New Database

⚠ Creating a new database changes the active database on the iFIX SCADA node.

Name _____

Cancel   Create

Switching Databases
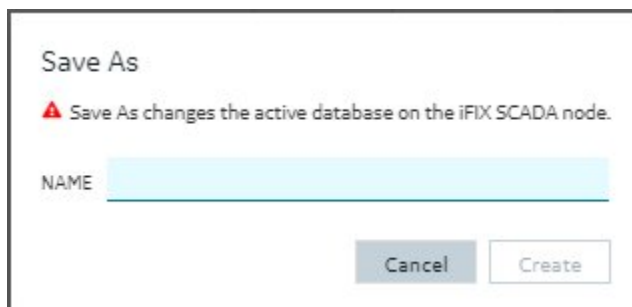
The drop down in the toolbar lets you quickly switch your currently active iFIX database.

Switch to - db1

Switching the database changes the active database on the iFIX SCADA node.

Yes   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.

Save As

⚠ Save As changes the active database on the iFIX SCADA node.

NAME _____

Cancel   Create

Import or Export a Database

See Import a Database *(on page 145)* or Export a Database *(on page 144)*.

Export a Database

Import and Export of your database in CSV format is available and supported from the Database panel by clicking the ellipsis (…) icon, and using the drop-down beside the database selector in the toolbar.
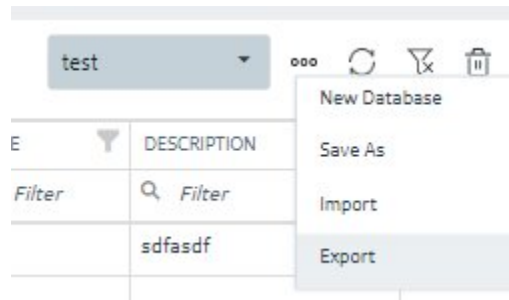
When you select the Export option, the Export iFIX Database dialog box appears where you select the options you want and click Export.
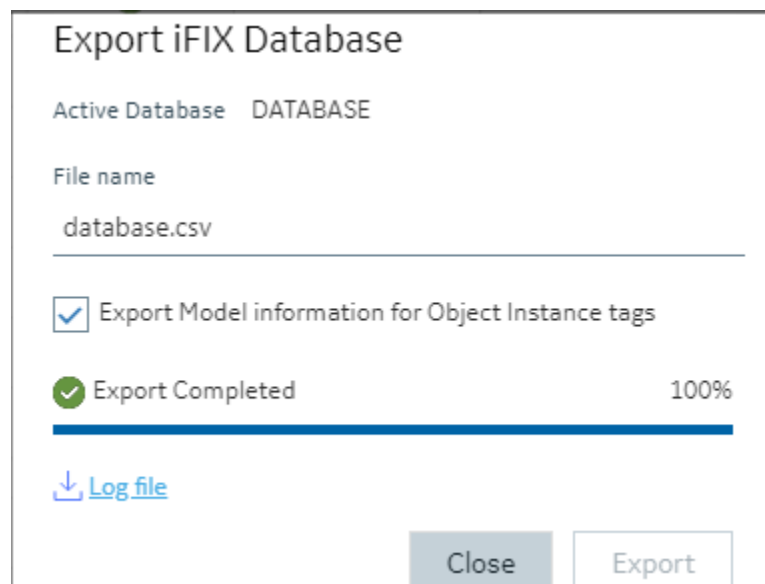
The exported file will be automatically downloaded to your browsers in the specified download folder with "export.csv" as the name.

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 backup 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

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. TestConfiguration Hub, on the Database panel, click the ellipsis (...) icon to open the shortcut menu.
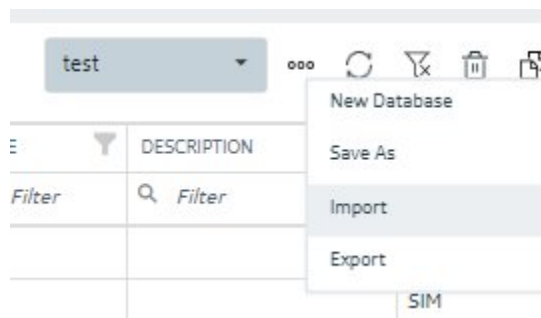
2. Click Import.
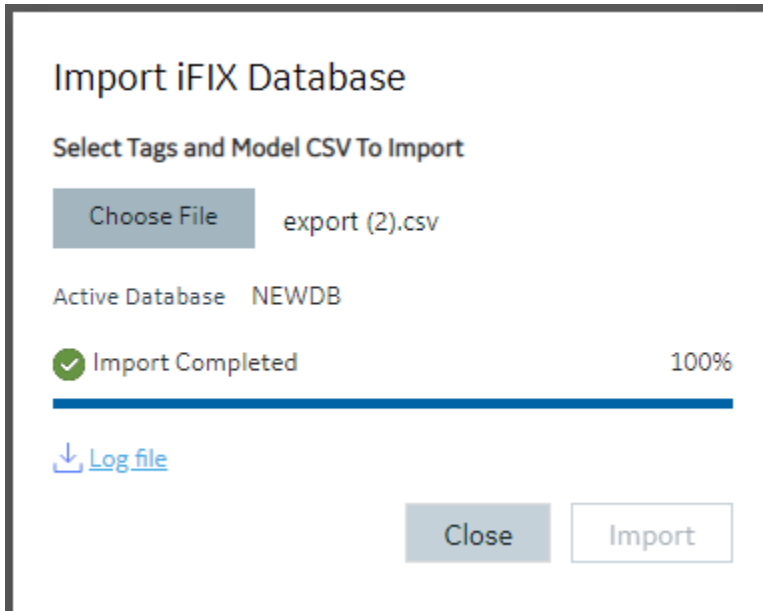
The Import iFIX Database dialog box appears.

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)\GE\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_Addressing`, `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 Databasemanager 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 Databasemanager. 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 Databasemanager 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",

                            "TagCommonValidators.minValue",

                            "TagCommonValidators.maxValue"

                        ]

                    }

                },
```

```
            {
                "A_TS6": {
                    "default": "",
                    "enum": "",
                    "datatype": "string",
                    "validators": [
                        "TagCommonValidators.maxLength"
                    ]
                }
            },
            {
                "TR7": {
                    "default": "128",
                    "field_min": "1",
                    "field_max": "65535",
                    "enum": "",
                    "datatype": "number",
                    "validators": [
                        "TagCommonValidators.maxLength",
                        "TagCommonValidators.isIntegerValidation",
                        "TagCommonValidators.minValue",
                        "TagCommonValidators.maxValue"
                    ]
                }
            },
            {
                "A_TS7": {
                    "default": "",
                    "enum": "",
                    "datatype": "string",
                    "validators": [
                        "TagCommonValidators.maxLength"
                    ]
                }
            },
            {
                "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": [
```

```json
                {
                    "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"

                ]

            }

        },

        {
```

```json
                    "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",
```
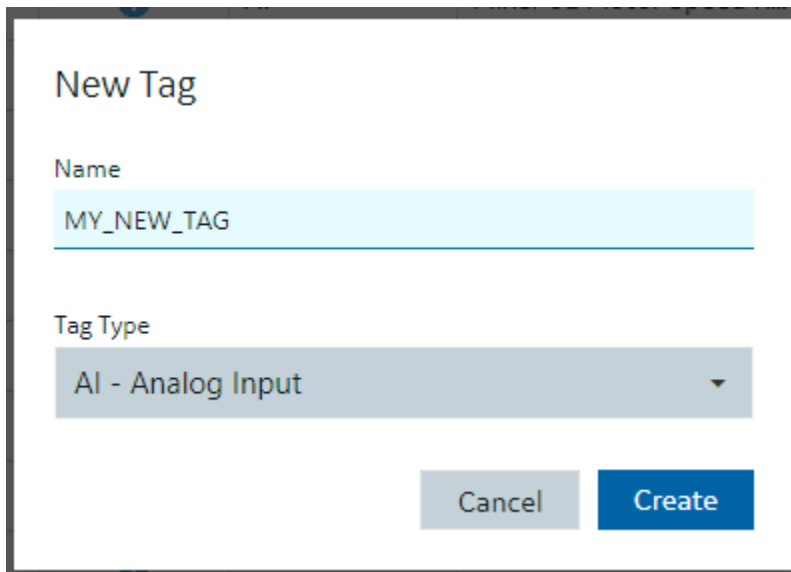
```
                        "PERFONLY",

                        "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"

                }

            },

            {
```

```
                        "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.

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 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
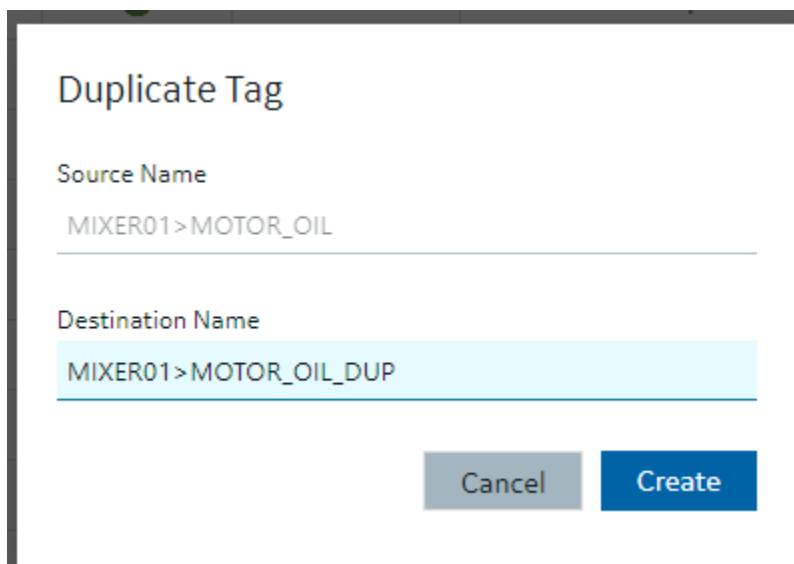
Deleting tags from the Database panel can be accomplished in a few different ways:

- 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:

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.

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.
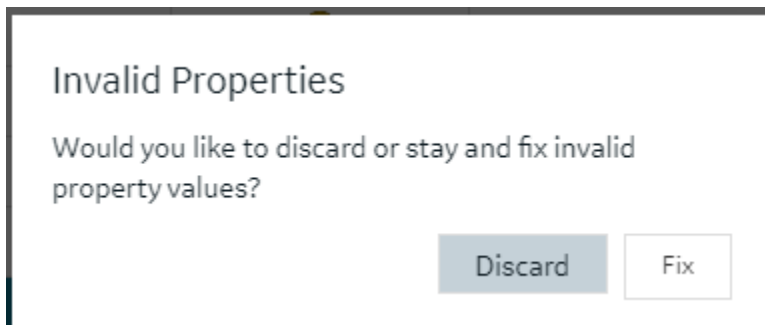
Custom Editors

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.
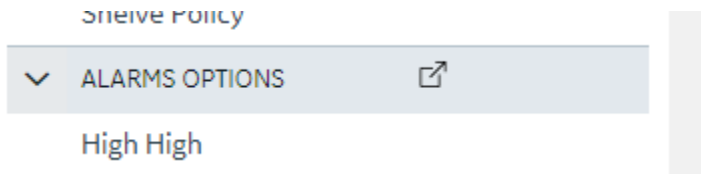
Here is an example of the dialog box that opens Alarm Options for the AA tag:

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 TestConfiguration 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 204)*	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, close a contact when an alarm occurs, and automatically reissue and acknowledge alarms.
AI Tag *(on page 229)*	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 262)*	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 278)*	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 300)*	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 313)*	The Boolean (BL) tag calculates a single true/false output from multiple inputs.

Tag Type	Description
CA Tag *(on page 331)*	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. ✎ **Note:** The precision of calculations is fifteen digits. Round-off errors can occur in the sixteenth digit.
DA Tag *(on page 365)*	The Digital Alarm (DA) tag sends and receives digital data (1 or 0) from an I/O driver, OPC server, or 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.
DC Tag *(on page 381)*	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.
DI Tag *(on page 395)*	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.
DO Tag *(on page 408)*	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. Because iFIX processes Digital Output tags whenever a new value is sent to the hardware, they gen-

Tag Type	Description
	erally 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.
DR Tag *(on page 418)*	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.
DT Tag *(on page 435)*	The Dead Time (DT) tag can delay the transfer of an input value to the next tag in the chain.
ETR Tag *(on page 444)*	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. 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. **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.

Tag Type	Description
EV Tag *(on page 455)*	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 *(on page 465)*	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 destination tag is in Manual mode, the update is instantaneous.
HS Tag *(on page 484)*	The Histogram (HS) tag records how frequently a value occurs during a specified period.
LL Tag *(on page 502)*	The Lead Lag (LL) tag allows you to simulate process dynamics by combining the advantages of lead and lag compensation strategies. **ⓘ 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. The Lead Lag formula is: Output=C3[C1(Input-Prior Output)+(Input*Scan time)+C2(Prior Output)] where: $\quad$ C1 = Lead Time $\qquad\qquad$ C2 = Lag Time $\qquad\qquad$ C3 $= \dfrac{K}{C2 + Scan\ Time}$

Tag Type	Description
	C1, C2, and the scan time (of the primary tag) are in seconds. K is the constant defined in the tag's Constant field.
MDI Tag *(on page 512)*	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.
PA Tag *(on page 540)*	The Pareto (PA) tag can accept up to eight inputs and calculate percentages for them.
PG Tag *(on page 555)*	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.
PID Tag *(on page 573)*	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. 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.
RB Tag *(on page 590)*	The Ratio Bias (RB) tag lets you change an incoming signal by adding a constant (bias) and/or by

Tag Type	Description
	multiplying by a constant (ratio). The tag calculates the constant by subtracting an offset from the signal. The following equation illustrates this method: Output = Ratio (Input - Offset) + Bias > ✎ **Note:** > This is a variation of y = mx + b.
RM Tag *(on page 600)*	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 615)*	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 625)*	The Statistical Data (SD) tag collects and performs statistical calculations on data.
SQD Tag *(on page 641)*	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 650)*	The SQL Trigger (SQT) tag lets iFIX execute SQL commands.
SS Tag *(on page 666)*	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.

Tag Type	Description
TM Tag *(on page 683)*	The Timer (TM) tag functions as a time counter by incrementing or decrementing its value.
TR Tag *(on page 694)*	The Trend (TR) tag can collects 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. 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 dead time (transportation delay) to the next downstream tag immediately.
TT Tag *(on page 704)*	The Totalizer (TT) tag maintains a floating-point total for values passed to it from upstream tags.
TX Tag *(on page 713)*	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	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
	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.
	Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($).
	Invalid Entries
	You cannot use the following special characters in a tag name:
	~ ` + ^ : ? " * = { } . , ; ? @
	Examples
	AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag.
	Valid Entries
	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	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. 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.
I/O Address	Lets you enter the location in the process hardware where data for this tag is saved and where output is sent. **Valid Entries** Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations. ⚠️ **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. ⚠️ **CAUTION:** TestConfiguration 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.

Field	Description
Signal Conditioning	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range. **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. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.
H/W Options	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range. **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. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.
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. **Valid Entries**

Field	Description
	• 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 **Example** 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	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. **Valid Entries** 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	Lets you enter the tag's minimum value. **Valid Entries**

Field	Description
	• 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 (un-signed integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). **Note:** The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more informa-tion. 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. If you want to display a value of 1.236 from the Calculation tag, you must enter three or more deci-mal places in the Low Limit field. If you are using scientific notation, up to six deci-mal places may be configured with precision, and the range may be positive or negative.
High Limit	Lets you enter the tag's maximum value. **Valid Entries** You can enter a high limit in one of three formats: • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999.

Field	Description
	• 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). **Note:** The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. 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. 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. If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
Units	Lets you enter text describing the engineering units range. **Valid Entries** Up to 33 characters. **Example** Kilograms per square meter, Liters per minute, degrees Celsius,

Field	Description
	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.
Scale Enabled	Lets you enable or disable scaling for this tag. Enabling scaling allows the system to convert the data received from input sensors to designated data ranges. **Note:** Linear scaling and signal conditioning cannot be applied simultaneously. If you select Linear Scaling, verify that Signal Conditioning is set to NONE. **Example** Scaling allows conversion of temperature data received in Fahrenheit to an output which uses Celsius values.
Scale Clamping	Lets you enable or disable clamping for this tag. 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. **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.

Field	Description
Raw Low	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. **Valid Entries** • 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	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. **Valid Entries** • 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	Enables the tag to use the range specified in the Engineering Units fields as the output values. Typically, EGU values normally reflect the expected operating ranges, or the Scale Low and Scale High

Field	Description
	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. **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.
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 is received. This field is only available if you did not enable Use EGU. **Valid Entries** • 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
	Note: Changes made to this field are not reflected in the data until after the next tag scan.
Scale High	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. **Valid Entries** • 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). **Note:** Changes made to this field are not reflected in the data until after the next tag scan.

Alarm Settings

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**

Field	Description
	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 to show alarm conditions, and enabling other tags to detect alarms from the tag. **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.
Remote Ack Tag	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. **Valid Entries** Any floating point tag and field name (F_CV) pair in the tag.field format. 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.
Alarm Suspension Tag	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

Field	Description
	Analog Alarm block processes alarms. When the value is other than zero, either a positive or negative number, the tag suspends alarms and generates a suspend alarm message. **Valid Entries** Any floating point tag and field name (F_CV) pair in the block.field format. > ✎ **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.
Target Value	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. **Valid Entries** 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. > ✎ **Note:** > Target Value is an optional field and is used only with deviation alarms.
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:hh: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:hh: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:hh: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:hh: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:hh: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:hh: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:hh: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:hh: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:hh: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
	Valid Entries Numeric value within the EGU range. **Example** 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.
Const Contact Output	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. > **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.
Suppress COMM Alarm	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.

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	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**

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	Used with the collection interval to schedule collection of data from a tag. **Valid Entries** Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples** 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. 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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector. Select either Milliseconds or Seconds.
Collector Compression	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. Select Disabled to prevent the tag from being compressed.
Collector Deadband	Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values

Field	Description
	that fall within a deadband centered around the last reported value. Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage. Select Absolute to set the Collector Deadband value to an absolute value. 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)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver. After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred. The Collector Compression Timeout value should be in increments of your collection interval, and not less. **Valid Entries** Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature:

Field	Description
	• 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.
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. The Perform by Comments Required check box appears in every tag configuration where Electron-

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	Lets you select whether the tag is initially placed on or off scan. 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.
Smoothing	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: Output = (S/16)X1 + ((16-S)/16)X2 where:

Field	Description
	• 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	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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. **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.
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 down-

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.

AI 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
	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. Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name: ~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries** 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	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. 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.
I/O Address	Lets you enter the location in the process hardware where data for this tag is saved and where output is sent. **Valid Entries** Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations. ⚠️ **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. ⚠️ **CAUTION:** TestConfiguration 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.

Field	Description
Signal Conditioning	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range. **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. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.
H/W Options	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range. **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. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.
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. **Valid Entries**

Field	Description
	• 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 **Example** 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	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. **Valid Entries** 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	Lets you enter the tag's minimum value. **Valid Entries**

Field	Description
	• 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).
	Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information.
	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.
	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.
	If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
High Limit	Lets you enter the tag's maximum value.
	Valid Entries
	You can enter a high limit in one of three formats:
	• Standard Integer.
	• Expanded Decimal Notation, ranging from -9999999 to 9999999.

Field	Description
	• 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). **Note:** The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. 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. 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. If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
Units	Lets you enter text describing the engineering units range. **Valid Entries** Up to 33 characters. **Example** Kilograms per square meter, Liters per minute, degrees Celsius,

Field	Description
	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.
Scale Enabled	Lets you enable or disable scaling for this tag. Enabling scaling allows the system to convert the data received from input sensors to designated data ranges. **Note:** Linear scaling and signal conditioning cannot be applied simultaneously. If you select Linear Scaling, verify that Signal Conditioning is set to NONE. **Example** Scaling allows conversion of temperature data received in Fahrenheit to an output which uses Celsius values.
Scale Clamping	Lets you enable or disable clamping for this tag. 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. **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.

Field	Description
Raw Low	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. **Valid Entries** • 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	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. **Valid Entries** • 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	Enables the tag to use the range specified in the Engineering Units fields as the output values. Typically, EGU values normally reflect the expected operating ranges, or the Scale Low and Scale High

Field	Description
	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. **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.
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 is received. This field is only available if you did not enable Use EGU. **Valid Entries** • 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
	Note: Changes made to this field are not reflected in the data until after the next tag scan.
Scale High	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. **Valid Entries** • 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). **Note:** Changes made to this field are not reflected in the data until after the next tag scan.

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**

Field	Description
	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 to show alarm conditions, and enabling other tags to detect alarms from the tag. **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.
Priority	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. **Valid Entries** INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL **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).

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	Lets you enter the tag's critically low values. When the tag's value falls below this limit, the tag generates an alarm. **Valid Entries** A critically low value within the tag's engineering units range. **Example** 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.
Low	Lets you enter the tag's low process values. When the tag's value falls below this limit, the tag generates an alarm. **Valid Entries** 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. **Example** If a temperature of 35 degrees indicates that ice crystals are forming in a cooling water flow, you

Field	Description
	could enter a value of 40 degrees for your Low alarm.
High	Lets you enter the tag's high process values. When the tag's value exceeds this limit, the tag generates an alarm. **Valid Entries** 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. **Example** If a bearing temperature of 80 degrees indicates machine wear, you could enter a value of 75 degrees for your High alarm.
High High	Lets you enter the tag's critically high values. When the tag's value exceeds this limit, the tag generates an alarm. **Valid Entries** A critically high value within the tag's engineering units range. **Example** If a bearing temperature of 90 degrees indicates imminent seizure, you could enter a value of 85 degrees for your High High alarm.
Rate of Change	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. **Valid Entries**

Field	Description
	A value within the tag's engineering units range, to be checked per scan period. Enter 0 to disable this alarm. **Example** 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.
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 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. **Valid Entries** Numeric value within the EGU range. **Example** 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.

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.

Field	Description
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** Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples** 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. 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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector. Select either Milliseconds or Seconds.
Collector Compression	Lets you select if the tag is set for compression. Compression applies a smoothing filter to incom-

Field	Description
	ing data by ignoring incremental changes in values that fall within a deadband centered around the last reported value. Select Disabled to prevent the tag from being compressed.
Collector Deadband	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. Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage. Select Absolute to set the Collector Deadband value to an absolute value. 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)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver. After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred. The Collector Compression Timeout value should be in increments of your collection interval, and not less. **Valid Entries**

Field	Description
	Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature: • 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.

Field	Description
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.
	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.

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	Lets you select whether the tag is initially placed on or off scan.
	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.

Field	Description
Smoothing	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: Output = (S/16)X1 + ((16-S)/16)X2 where: • 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	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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. > 📝 **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.
Previous Block	Displays the name of the previous (upstream) tag. **Valid Entries**

Field	Description
	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 down-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.

AIS 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** 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. Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name: ~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries**

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	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. 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.
I/O Address	Lets you enter the location in the process hardware where data for this tag is saved and where output is sent. **Valid Entries** Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations. **⚠ CAUTION:** Do not assign the same I/O address to tags when using exception-based and time-based processing. Doing so will

Field	Description
	⚠ cause the exception-based tags to occasionally miss a value.
	⚠ **CAUTION:** TestConfiguration 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.
Signal Conditioning	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range. ✎ **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. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.
H/W Options	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range. ✎ **Note:** Signal conditioning and linear scaling cannot be applied simultaneously. If you se-

Field	Description
	✎ lect a value for Signal Conditioning verify that Linear Scaling is not selected. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.
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. **Valid Entries** • 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 **Example** 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	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. **Valid Entries**

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	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. ⚠️ **CAUTION:** This option should generally be CLEAR (the default state) to prevent unwanted values from being sent to equipment.

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
	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 to show alarm conditions, and enabling other tags to detect alarms from the tag. **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.
Priority	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. **Valid Entries** INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL

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.

Alarm Limits

Field	Description
Low Low	Lets you enter the tag's critically low values. When the tag's value falls below this limit, the tag generates an alarm. **Valid Entries** A critically low value within the tag's engineering units range. **Example** 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.
Low	Lets you enter the tag's low process values. When the tag's value falls below this limit, the tag generates an alarm. **Valid Entries** 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. **Example** 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.

Field	Description
High	Lets you enter the tag's high process values. When the tag's value exceeds this limit, the tag generates an alarm. **Valid Entries** 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. **Example** If a bearing temperature of 80 degrees indicates machine wear, you could enter a value of 75 degrees for your High alarm.
High High	Lets you enter the tag's critically high values. When the tag's value exceeds this limit, the tag generates an alarm. **Valid Entries** A critically high value within the tag's engineering units range. **Example** If a bearing temperature of 90 degrees indicates imminent seizure, you could enter a value of 85 degrees for your High High alarm.
Rate of Change	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. **Valid Entries** A value within the tag's engineering units range, to be checked per scan period. Enter 0 to disable this alarm. **Example** 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.
Dead-band	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 nui-

Field	Description
	sance alarms. Once the alarm falls below the dead band and then exceeds the alarm limits, the tag generates another alarm. **Valid Entries** Numeric value within the EGU range. **Example** 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.

E-Signature

Field	Description
Type	The Type of Electronic Signature: • 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
	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. 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. 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.
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	Lets you select whether the tag is initially placed on or off scan.

Field	Description
	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.
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. > ✎ **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.
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 down-

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.

AO 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
	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.
	Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($).
	Invalid Entries
	You cannot use the following special characters in a tag name:
	~ ` + ^ : ? " * = { } . , ; ? @
	Examples
	AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag.
	Valid Entries
	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	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. 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.
I/O Address	Lets you enter the location in the process hardware where data for this tag is saved and where output is sent. **Valid Entries** Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations. ⚠️ **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. ⚠️ **CAUTION:** TestConfiguration 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.

Field	Description
Signal Conditioning	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range. **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. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.
H/W Options	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range. **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. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.

Limits and Scaling

Field	Description
Low Limit	Lets you enter the tag's minimum value. **Valid Entries**

Field	Description
	• 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). **✎ Note:** The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. 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. 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. If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
High Limit	Lets you enter the tag's maximum value. **Valid Entries** You can enter a high limit in one of three formats: • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999.

Field	Description
	• 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). **Note:** The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. 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. 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. If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
Units	Lets you enter text describing the engineering units range. **Valid Entries** Up to 33 characters. **Example** Kilograms per square meter, Liters per minute, degrees Celsius,

Field	Description
	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.
Scale Enabled	Lets you enable or disable scaling for this tag. Enabling scaling allows the system to convert the data received from input sensors to designated data ranges. **Note:** Linear scaling and signal conditioning cannot be applied simultaneously. If you select Linear Scaling, verify that Signal Conditioning is set to NONE. **Example** Scaling allows conversion of temperature data received in Fahrenheit to an output which uses Celsius values.
Scale Clamping	Lets you enable or disable clamping for this tag. 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. **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.

Field	Description
Raw Low	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. **Valid Entries** • 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	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. **Valid Entries** • 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	Enables the tag to use the range specified in the Engineering Units fields as the output values. Typically, EGU values normally reflect the expected operating ranges, or the Scale Low and Scale High

Field	Description
	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. **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.
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 is received. This field is only available if you did not enable Use EGU. **Valid Entries** • 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
	Note: Changes made to this field are not reflected in the data until after the next tag scan.
Scale High	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. **Valid Entries** • 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). **Note:** Changes made to this field are not reflected in the data until after the next tag scan.

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**

Field	Description
	ALL or up to 15 alarm area names.
Enable Event	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. Analog Output, Analog Register, Digital Output, Digital Register, Digital Input, and Text tags have event messaging capabilities. **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.

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.

Field	Description
	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** Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples** 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. 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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector. Select either Milliseconds or Seconds.
Collector Compression	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.

Field	Description
	Select Disabled to prevent the tag from being compressed.
Collector Deadband	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. Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage. Select Absolute to set the Collector Deadband value to an absolute value. 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)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver. After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred. The Collector Compression Timeout value should be in increments of your collection interval, and not less. **Valid Entries** Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature: • 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.
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

Field	Description
	run mode. Comments in the Verify Comment section are optional. 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.

Advanced Options

Field	Description
Output Reverse	Lets you specify the maximum rate of change you want to allow between successive outputs. **Valid Entries** A value between the Low and High Limit (EGU) fields or a 0 to allow any amount of change.
Initial Value	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. **Valid Entries** A value between the Low and High Limit (EGU) fields.
Low Operator Limit	Lets you specify the lowest value that the tag accepts from another tag or from an operator. **Valid Entries** A value between the Low and High Limit (EGU) fields. If appropriate, you can use the Low Limit (EGU) for this value.
High Operator Limit	Lets you specify the highest value that the tag can accept from another tag or from an operator.

Field	Description
	Valid Entries A value between the Low and High Limit (EGU) fields. If appropriate, you can use the High Limit (EGU) for this value.
Rate Limit	Lets you specify the maximum rate of change you want to allow between successive outputs. **Valid Entries** A value between the Low and High Limit (EGU) fields or a 0 to allow any amount of change.
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. > ✏️ **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.
Previous Block	Displays the name of the previous (upstream) tag. **Valid Entries** None. This is a read-only field.

Field	Description
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.

AR 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** 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. Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name: ~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries**

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	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. 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.
I/O Address	Lets you enter the location in the process hardware where data for this tag is saved and where output is sent. **Valid Entries** Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations. ⚠️ **CAUTION:** Do not assign the same I/O address to tags when using exception-based and time-based processing. Doing so will

Field	Description
	⚠ cause the exception-based tags to occasionally miss a value. ⚠ **CAUTION:** TestConfiguration 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.
Signal Conditioning	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range. 📝 **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. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.
H/W Options	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range. 📝 **Note:** Signal conditioning and linear scaling cannot be applied simultaneously. If you se-

Field	Description
	📝 lect a value for Signal Conditioning verify that Linear Scaling is not selected. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.

Limits and Scaling

Field	Description
Low Limit	Lets you enter the tag's minimum value. **Valid Entries** • 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). 📝 **Note:** The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. 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.

Field	Description
	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. If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
High Limit	Lets you enter the tag's maximum value. **Valid Entries** You can enter a high limit in one of three formats: • 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). 📝 **Note:** The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. 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. 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.

Field	Description
	If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
Units	Lets you enter text describing the engineering units range. **Valid Entries** Up to 33 characters. **Example** Kilograms per square meter, Liters per minute, degrees Celsius, > ✏️ **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.
Scale Enabled	Lets you enable or disable scaling for this tag. Enabling scaling allows the system to convert the data received from input sensors to designated data ranges. > ✏️ **Note:** > Linear scaling and signal conditioning cannot be applied simultaneously. If you select Linear Scaling, verify that Signal Conditioning is set to NONE. **Example** Scaling allows conversion of temperature data received in Fahrenheit to an output which uses Celsius values.

Field	Description
Scale Clamping	Lets you enable or disable clamping for this tag. 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. **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.
Raw Low	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. **Valid Entries** • 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	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. **Valid Entries**

Field	Description
	• 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	Enables the tag to use the range specified in the Engineering Units fields as the output values. 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. 📝 **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.
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
	is received. This field is only available if you did not enable Use EGU. **Valid Entries** • 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 (un-signed integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). > 📝 **Note:** > Changes made to this field are not reflect-ed in the data until after the next tag scan.
Scale High	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. **Valid Entries** • 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 (un-signed integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary).

Field	Description
	Note: Changes made to this field are not reflected in the data until after the next tag scan.

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.

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.

Field	Description
	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
	Any numeric value that does not exceed the collection interval. The value is in seconds.
	Examples
	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.
	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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.
	Select either Milliseconds or Seconds.
Collector Compression	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.
	Select Disabled to prevent the tag from being compressed.
Collector Deadband	Lets you select if the tag is set for compression. Compression applies a smoothing filter to incom-

Field	Description
	ing data by ignoring incremental changes in values that fall within a deadband centered around the last reported value. Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage. Select Absolute to set the Collector Deadband value to an absolute value. 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)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver. After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred. The Collector Compression Timeout value should be in increments of your collection interval, and not less. **Valid Entries** Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature:

Field	Description
	• 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.
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. The Perform by Comments Required check box appears in every tag configuration where Electron-

Field	Description
	ic Signature settings are available. By default, this check box is disabled.

Advanced Options

Field	Description
Output Enable	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.
Enable Event	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. Analog Output, Analog Register, Digital Output, Digital Register, Digital Input, and Text blocks have event messaging capabilities. **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.
I/O Address Type	Lets you specify the number format of the block's starting address. **Valid Entries**

Field	Description
	Hex, Octal, or Decimal
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. > 📝 **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.
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**

Field	Description
	Text, up to 80 characters.

AR2 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
	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.
	Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($).
	Invalid Entries
	You cannot use the following special characters in a tag name:
	~ ` + ^ : ? " * = { } . , ; ? @

Field	Description
	Examples AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries** 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	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. 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.
I/O Address	Lets you enter the location in the process hardware where data for this tag is saved and where output is sent. **Valid Entries** Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations.

Field	Description
	⚠️ **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. ⚠️ **CAUTION:** TestConfiguration 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.
H/W Options	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range. ✏️ **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. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.

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	The Type of Electronic Signature: • 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
	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. 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. 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.
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.
Enable Event	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

Field	Description
	as alarms for a given block but do not appear in the Alarm Summary object. Analog Output, Analog Register, Digital Output, Digital Register, Digital Input, and Text blocks have event messaging capabilities. > **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.
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. > **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.
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
	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.

BB 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** 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

Field	Description
	databases, single quotes are not supported in tag names. Tag names can also include dashes (-), under-scores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name: ~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries** 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
Activate High Contact	Enables or disables the High Contact Data fields.

Field	Description
High Contact Driver	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. 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.
High Contact Driver I/O Address	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. **Valid Entries** Depends on your driver. Consult your I/O driver manual for details on the proper input/output addresses and configurations. ⚠️ **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.
High Contact Hardware Options	Lets you select any specific device control addressing format that the block uses to communicate with process hardware on the plant floor. **Valid Entries** For most process hardware, this field is usually left blank. Consult your I/O driver manual for the applicable hardware code if necessary.

Field	Description
High Contact - Turn On Above	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.
	Valid Entries
	Enter the number that represents this value according to the Low and High Limits (EGU) of the analog input.
High Contact - Turn On Below	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.
	Valid Entries
	The number that represents this value according to the Low and High Limits (EGU) of the analog input.
Activate Low Contact	Enables or disables the Low Contact Data fields.
	Valid Entries
	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.
Low Contact Driver	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.
	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.
Low Contact I/O Address	Lets you enter the location in the process hardware where data for this block is saved and where out-

Field	Description
	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. **Valid Entries** Depends on your driver. Consult your I/O driver manual for details on the proper input/output addresses and configurations. ⚠️ **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.
Low Contact Hardware Options	Lets you select any specific device control addressing format that the block uses to communicate with process hardware on the plant floor. **Valid Entries** For most process hardware, this field is usually left blank. Consult your I/O driver manual for the applicable hardware code if necessary.
Low Contact - Turn On Above	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. **Valid Entries** Enter the number that represents this value according to the Low and High Limits (EGU) of the analog input.

Field	Description
Low Contact - Turn On Below	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. **Valid Entries** Enter the number that represents this value according to the Low and High Limits (EGU) of the analog input.

Limits and Scaling

Field	Description
Low Limit	Lets you enter the tag's minimum value. **Valid Entries** • 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). > **Note:** > The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. In a Calculation or Signal Select tag, if the output of the tag is 10 and the Low Limit is 15, the tag

Field	Description
	clamps the value at 15. You must enter a Low Limit of 10 or less to output a value of 10. 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. If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
High Limit	Lets you enter the tag's maximum value. **Valid Entries** You can enter a high limit in one of three formats: • 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). > **Note:** > The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. 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.

Field	Description
	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. If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
Units	Lets you enter text describing the engineering units range. **Valid Entries** Up to 33 characters. **Example** Kilograms per square meter, Liters per minute, degrees Celsius, **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.

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.

Field	Description
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 to show alarm conditions, and enabling other tags to detect alarms from the tag. ✏️ **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.

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**

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	Used with the collection interval to schedule collection of data from a tag. **Valid Entries** Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples** 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. 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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector. Select either Milliseconds or Seconds.
Collector Compression	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. Select Disabled to prevent the tag from being compressed.
Collector Deadband	Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values

Field	Description
	that fall within a deadband centered around the last reported value. Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage. Select Absolute to set the Collector Deadband value to an absolute value. 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)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver. After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred. The Collector Compression Timeout value should be in increments of your collection interval, and not less. **Valid Entries** Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature:

Field	Description
	• 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.
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. The Perform by Comments Required check box appears in every tag configuration where Electron-

Field	Description
	ic Signature settings are available. By default, this check box is disabled.

Advanced Options

Field	Description
One Shot	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.
Invert Output	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. Alternatively, to return a closed contact as a logical 1 (normal conditions) and an open contact as a logical 0, clear the check box.
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. **Note:** Read access for database tags is available to all users regardless of security area.

Field	Description
	📝 This allows users to retrieve data from a specific security area even if they cannot write to that area.
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.

BL 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.

Field	Description
	Valid Entries 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. Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name: ~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries** 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.

Inputs

Field	Description
Input A	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. **Valid Entries** A label of up to 16 characters. **Examples** Open, Off
Input B	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. **Valid Entries** A label of up to 16 characters. **Examples** Open, Off
Input C	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. **Valid Entries** A label of up to 16 characters. **Examples** Open, Off
Input D	Lets you enter a descriptive label for the logical 0 value received by the tag. You can display this label

Field	Description
	in the iFIX WorkSpace through a Data link to aid operators in interpreting the value for the contact. **Valid Entries** A label of up to 16 characters. **Examples** Open, Off
Input E	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. **Valid Entries** A label of up to 16 characters. **Examples** Open, Off
Input F	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. **Valid Entries** A label of up to 16 characters. **Examples** Open, Off
Input G	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. **Valid Entries**

Field	Description
	A label of up to 16 characters. **Examples** Open, Off
Input H	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. **Valid Entries** A label of up to 16 characters. **Examples** Open, Off
Output Calculation	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. **Valid Entries** 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. **Example** (C+(A+B))

Limits and Scaling

Field	Description
Open Tag	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.

Field	Description
	Valid Entries A label of up to 16 characters. **Examples** Close, On.
Close Tag	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. **Valid Entries** A label of up to 16 characters. **Examples** Open, Off

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.

Alarm Limits

Field	Description
Low Low	Lets you enter the tag's critically low values. When the tag's value falls below this limit, the tag generates an alarm.

Field	Description
	Valid Entries A critically low value within the tag's engineering units range. **Example** 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.
Low	Lets you enter the tag's low process values. When the tag's value falls below this limit, the tag generates an alarm. **Valid Entries** 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. **Example** 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.
High	Lets you enter the tag's high process values. When the tag's value exceeds this limit, the tag generates an alarm. **Valid Entries** 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. **Example**

Field	Description
	If a bearing temperature of 80 degrees indicates machine wear, you could enter a value of 75 degrees for your High alarm.
High High	Lets you enter the tag's critically high values. When the tag's value exceeds this limit, the tag generates an alarm. **Valid Entries** A critically high value within the tag's engineering units range. **Example** If a bearing temperature of 90 degrees indicates imminent seizure, you could enter a value of 85 degrees for your High High alarm.
Rate of Change	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. **Valid Entries** A value within the tag's engineering units range, to be checked per scan period. Enter 0 to disable this alarm. **Example** 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.
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 tag issues an alarm once, eliminating nuisance alarms. Once the alarm falls below the dead band and then

Field	Description
	exceeds the alarm limits, the tag generates another alarm. **Valid Entries** Numeric value within the EGU range. **Example** 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.

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	Used with the collection interval to schedule collection of data from a tag. **Valid Entries** Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples** 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. 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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector. Select either Milliseconds or Seconds.
Collector Compression	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. Select Disabled to prevent the tag from being compressed.
Collector Deadband	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.

Field	Description
	Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.
	Select Absolute to set the Collector Deadband value to an absolute value.
	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)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.
	After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.
	The Collector Compression Timeout value should be in increments of your collection interval, and not less.
	Valid Entries
	Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature:
	• 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
	• 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.
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. 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.

Advanced Options

Field	Description
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. > ✏️ **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.
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.

Field	Description
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 block.
Scan Time	Lets you specify how often the Scan, Alarm, and Control (SAC) program processes the tag and any blocks chained to it. **Valid Entries** • 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 **Example** 0.15 specifies a 15-subsecond scan time. 5 specifies a 5-second scan time, 10M specifies a 10-

Field	Description
	minute scan time, 16H specifies a 16-hour scan time.
Phase At	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.
	Valid Entries
	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.

BPL 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
	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.
	Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($).
	Invalid Entries
	You cannot use the following special characters in a tag name:
	~ ` + ^ : ? " * = { } . , ; ? @
	Examples
	AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag.
	Valid Entries
	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 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	The Type of Electronic Signature: • 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. 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes.

Field	Description
	Unsigned writes can originate from scripts, recipe downloads, and other data sources. 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
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.

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
	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** 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. Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name: ~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries** 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.

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	Lets you specify the inputs to the Calculation tag.

Valid Entries

The following are valid entries for defining your equation with Input entries:

- 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.

> ✏️ **Note:**
>
> If you enter a tag name without entering a field name, iFIX automatically enters F_CV as the default field name.

Tag and field pairs represent the value of the specified field. For example, PID1.F_TV1 to access the tag's set point.

> ✏️ **Note:**
>
> Input field A always represents the output of the upstream block (previous block).

Example

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.
Input B	Lets you specify the inputs to the Calculation tag. **Valid Entries** The following are valid entries for defining your equation with Input entries: • 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. **Note:** If you enter a tag name without entering a field name, iFIX automatically enters F_CV as the default field name. Tag and field pairs represent the value of the specified field. For example, PID1.F_TV1 to access the tag's set point. **Note:** Input field A always represents the output of the upstream block (previous block). **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.
Input C	Lets you specify the inputs to the Calculation tag.

Field	Description
	Valid Entries The following are valid entries for defining your equation with Input entries: • 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. **Note:** If you enter a tag name without entering a field name, iFIX automatically enters F_CV as the default field name. Tag and field pairs represent the value of the specified field. For example, PID1.F_TV1 to access the tag's set point. **Note:** Input field A always represents the output of the upstream block (previous block). **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.
Input D	Lets you specify the inputs to the Calculation tag. **Valid Entries** The following are valid entries for defining your equation with Input entries:

Field	Description
	• 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. 📝 **Note:** If you enter a tag name without entering a field name, iFIX automatically enters F_CV as the default field name. Tag and field pairs represent the value of the specified field. For example, PID1.F_TV1 to access the tag's set point. 📝 **Note:** Input field A always represents the output of the upstream block (previous block). **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.
Input E	Lets you specify the inputs to the Calculation tag. **Valid Entries** The following are valid entries for defining your equation with Input entries: • 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
	Note: If you enter a tag name without entering a field name, iFIX automatically enters F_CV as the default field name. Tag and field pairs represent the value of the specified field. For example, PID1.F_TV1 to access the tag's set point. **Note:** Input field A always represents the output of the upstream block (previous block). **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.
Input F	Lets you specify the inputs to the Calculation tag. **Valid Entries** The following are valid entries for defining your equation with Input entries: • 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. **Note:** If you enter a tag name without entering a field name, iFIX automatically enters F_CV as the default field name.

Field	Description
	Tag and field pairs represent the value of the specified field. For example, PID1.F_TV1 to access the tag's set point. **Note:** Input field A always represents the output of the upstream block (previous block). **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.
Input G	Lets you specify the inputs to the Calculation tag. **Valid Entries** The following are valid entries for defining your equation with Input entries: • 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. **Note:** If you enter a tag name without entering a field name, iFIX automatically enters F_CV as the default field name. Tag and field pairs represent the value of the specified field. For example, PID1.F_TV1 to access the tag's set point.

Field	Description
	Note: Input field A always represents the output of the upstream block (previous block). **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.
Input H	Lets you specify the inputs to the Calculation tag. **Valid Entries** The following are valid entries for defining your equation with Input entries: • 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. **Note:** If you enter a tag name without entering a field name, iFIX automatically enters F_CV as the default field name. Tag and field pairs represent the value of the specified field. For example, PID1.F_TV1 to access the tag's set point. **Note:** Input field A always represents the output of the upstream block (previous block). **Example**

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	Lets you specify the Calculation block equation. **Valid Entries** An equation using the input letters (A - H) that correspond to the defined Input fields. The input letters may be used more than once. **Note:** A mathematical overflow (value >1038), underflow (below 10-37), or division by zero causes a Calc error status in the upstream block.

Limits and Scaling

Field	Description
Low Limit	Lets you enter the tag's minimum value. **Valid Entries** • 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
	Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. 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. 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. If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
High Limit	Lets you enter the tag's maximum value. **Valid Entries** You can enter a high limit in one of three formats: • 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). **Note:** The I/O driver can set certain limitations on the engineering units range. Consult

Field	Description
	📝 your I/O driver manual for more information.
	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. 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. If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
Units	Lets you enter text describing the engineering units range. **Valid Entries** Up to 33 characters. **Example** Kilograms per square meter, Liters per minute, degrees Celsius, 📝 **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.

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 to show alarm conditions, and enabling other tags to detect alarms from the tag. **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.

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.

Field	Description
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** Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples** 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. 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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector. Select either Milliseconds or Seconds.
Collector Compression	Lets you select if the tag is set for compression. Compression applies a smoothing filter to incom-

Field	Description
	ing data by ignoring incremental changes in values that fall within a deadband centered around the last reported value. Select Disabled to prevent the tag from being compressed.
Collector Deadband	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. Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage. Select Absolute to set the Collector Deadband value to an absolute value. 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)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver. After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred. The Collector Compression Timeout value should be in increments of your collection interval, and not less. **Valid Entries**

Field	Description
	Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature: • 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.

Field	Description
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. 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.

Advanced Options

Field	Description
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. 📝 **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.
Previous Block	Displays the name of the previous (upstream) tag. **Valid Entries**

Field	Description
	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.

CTR 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
	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.
	Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($).
	Invalid Entries
	You cannot use the following special characters in a tag name:
	~ ` + ^ : ? " * = { } . , ; ? @
	Examples
	AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag.
	Valid Entries

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	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 to show alarm conditions, and enabling other tags to detect alarms from the tag. 📝 **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.
Priority	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. **Valid Entries**

Field	Description
	INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITI-CAL 📝 **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.

E-Signature

Field	Description
Type	The Type of Electronic Signature: • 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	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. 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. 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
Mode	Count on transition to OPEN, CLOSE or COS (any transition).
Passed Value	INPUT passes raw input (converted to 0/1). ALM passes Current Alarm (converted to 0/1). LIMIT passes 'Limit Reached' (as 0/1 which is checked regardless of Alarm Enable, Auto and Gate states).

Field	Description
	COUNT passes current value of Counter. Note that the counter value is converted to Float. Precision may be lost. Also note that some downstream blocks (such as AO) may clamp this to their EGU or OPERATOR limits.
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	If set to YES, the NEXT block will execute only if a transition is counted (requires AUTO and GATE are true). **Note:** A manual change to count via the A_-COUNT field will NOT satisfy this condition.
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.

Field	Description
	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.
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 down-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.

Field	Description
	Valid Entries Text, up to 80 characters.

D16 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** 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. Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name:

Field	Description
	~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries** 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
Mode	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. 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. Exception based processing is NOT supported in DIGITAL mode.

Field	Description
I/O Driver	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. 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.
I/O Address	Lets you enter the location in the process hardware where data for this tag is saved and where output is sent. **Valid Entries** Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations. ⚠️ **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. ⚠️ **CAUTION:** TestConfiguration 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.

Field	Description
Bitcount	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).
H/W Options	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range. **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. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.
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. **Valid Entries** • 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 **Example**

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	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. **Valid Entries** 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.

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	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 to show alarm conditions, and enabling other tags to detect alarms from the tag. 📝 **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.
Priority	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-

Field	Description
	pear in Data links configured to display current and latched alarms. **Valid Entries** INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL 📝 **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.

E-Signature

Field	Description
Type	The Type of Electronic Signature: • 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	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. 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. 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	Lets you select whether the tag is initially placed on or off scan. 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

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	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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. 📝 **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.
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.

Field	Description
	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.

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
	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** 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. Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name: ~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries** 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.

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	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. 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.
I/O Address	Lets you enter the location in the process hardware where data for this tag is saved and where output is sent. **Valid Entries** Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations. ⚠️ **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. ⚠️ **CAUTION:** TestConfiguration Hub currently does not do I/O address validations before publish. If you enter an invalid IO address into a tag

Field	Description
	⚠️ 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.
Signal Conditioning	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range. 📝 **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. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.
H/W Options	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range. 📝 **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. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.
Process by Exception	Enables exception-based processing for the tag.

Field	Description
Scan Time	Lets you specify how often the Scan, Alarm, and Control (SAC) program processes the tag and any tags (blocks) chained to it. **Valid Entries** • 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 **Example** 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	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. **Valid Entries** 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
Open Tag	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. **Valid Entries** A label of up to 16 characters. **Examples** Open, Off
Close Tag	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. **Valid Entries** A label of up to 16 characters. **Examples** Close, On.

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.

Field	Description
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 to show alarm conditions, and enabling other tags to detect alarms from the tag. **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.
Priority	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. **Valid Entries** INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL **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).

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	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. **Valid Entries** Open, Close, Change of State, None
Contact Tag	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. **Valid Entries** A Digital Output or Digital Input block, in Manual mode.
Contact Mode	Lets you specify when to open the digital tag entered in the Contact Name field. **Valid Entries** Acknowledge, Return, All Clear, and Never
Cont Contact Output	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.

Field	Description
	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.
Remote Ack Tag	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. **Valid Entries** Any floating point block and field name pair in the tag.field format. **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.
Alarm Suspension Tag	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

Field	Description
	and generates a suspend message to the enabled alarm destinations. **Valid Entries** Any floating point tag and field name (F_CV) pair in the tag.field format. **Note:** 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.
Delay Time	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. **Valid Entries** 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. For exception-based processing, leave the default entry, 00:00:00:00. This disables any delay. **Note:** The value in the Delay Time field does not apply to Change of State (COS) alarms.
Realarm Time	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

Field	Description
	re-issues the alarm. Any contact associated with each alarm type is closed. **Valid Entries** 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. For exception-based processing, leave the default entry, 00:00:00:00. This disables any delay.
Suppress COMM Alarm	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. 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.
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	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** Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples** 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.

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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector. Select either Milliseconds or Seconds.
Collector Compression	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. Select Disabled to prevent the tag from being compressed.
Collector Deadband	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. Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage. Select Absolute to set the Collector Deadband value to an absolute value. Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.

Field	Description
Compression Time-out (ms)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver. After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred. The Collector Compression Timeout value should be in increments of your collection interval, and not less. **Valid Entries** Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature: • 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes.
	Unsigned writes can originate from scripts, recipe downloads, and other data sources.
	When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.
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.
	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.

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	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	Lets you select whether the tag is initially placed on or off scan. 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.
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. > 📝 **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.
Previous Block	Displays the name of the previous (upstream) tag. **Valid Entries**

Field	Description
	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 down-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.

DC 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** 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. Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name: ~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries**

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	Displays the commands and arguments for each Device Control block. Use the Browse (...) button to select from a list of valid commands. **Valid Entries** The list box can include up to 12 programming statements each containing up to 34 alphanumeric characters.
Step 1 Command	Displays the commands and arguments for each Device Control block. Use the Browse (...) button to select from a list of valid commands. **Valid Entries** The list box can include up to 12 programming statements each containing up to 34 alphanumeric characters.
Step 2 Command	Displays the commands and arguments for each Device Control block. Use the Browse (...) button to select from a list of valid commands. **Valid Entries**

Field	Description
	The list box can include up to 12 programming statements each containing up to 34 alphanumeric characters.
Step 3 Command	Displays the commands and arguments for each Device Control block. Use the Browse (...) button to select from a list of valid commands. **Valid Entries** The list box can include up to 12 programming statements each containing up to 34 alphanumeric characters.
Step 4 Command	Displays the commands and arguments for each Device Control block. Use the Browse (...) button to select from a list of valid commands. **Valid Entries** The list box can include up to 12 programming statements each containing up to 34 alphanumeric characters.
Step 5 Command	Displays the commands and arguments for each Device Control block. Use the Browse (...) button to select from a list of valid commands. **Valid Entries** The list box can include up to 12 programming statements each containing up to 34 alphanumeric characters.
Step 6 Command	Displays the commands and arguments for each Device Control block. Use the Browse (...) button to select from a list of valid commands. **Valid Entries**

Field	Description
	The list box can include up to 12 programming statements each containing up to 34 alphanumeric characters.
Step 7 Command	Displays the commands and arguments for each Device Control block. Use the Browse (...) button to select from a list of valid commands. **Valid Entries** The list box can include up to 12 programming statements each containing up to 34 alphanumeric characters.
Step 8 Command	Displays the commands and arguments for each Device Control block. Use the Browse (...) button to select from a list of valid commands. **Valid Entries** The list box can include up to 12 programming statements each containing up to 34 alphanumeric characters.
Step 9 Command	Displays the commands and arguments for each Device Control block. Use the Browse (...) button to select from a list of valid commands. **Valid Entries** The list box can include up to 12 programming statements each containing up to 34 alphanumeric characters.
Step 10 Command	Displays the commands and arguments for each Device Control block. Use the Browse (...) button to select from a list of valid commands. **Valid Entries**

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	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. 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.
Input Address 1 - 16	Lets you specify the addresses of the digital input points that the Device Control block monitors. **Valid Entries** 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. 📝 **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.
Input Hardware Options	Lets you select any specific device control addressing format that the block uses to communicate with process hardware on the plant floor. **Valid Entries**

Field	Description
	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.
Output Driver	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. 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.
Output Address 1 - 8	Lets you specify the addresses of the digital output points that the Device Control block monitors. **Valid Entries** 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. > ✏️ **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.
Output Hardware Options	Lets you select any specific device control addressing format that the tag uses to communicate with process hardware on the plant floor. **Valid Entries** For most process hardware, this field is usually left blank. Consult your I/O driver, OPC, or OPC UA

Field	Description
	manual for the applicable hardware code if necessary.

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.
Priority	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. **Valid Entries** INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL > **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).

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** Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples** 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.

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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.
	Select either Milliseconds or Seconds.
Collector Compression	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.
	Select Disabled to prevent the tag from being compressed.
Collector Deadband	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.
	Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.
	Select Absolute to set the Collector Deadband value to an absolute value.
	Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.

Field	Description
Compression Time-out (ms)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver. After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred. The Collector Compression Timeout value should be in increments of your collection interval, and not less. **Valid Entries** Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature: • 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.
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. 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.

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	Lets you select whether the tag is initially placed on or off scan. Click On Scan to place the tag on scan as soon as the Scan, Alarm, and Control (SAC) program starts

Field	Description
	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.
Initial Value	Controls the status of digital points on the hardware when the Scan, Alarm, and Control (SAC) program is first started. **Valid Entries** A valid contact pattern. **Example** A typical contact pattern entry in the Initial Value Field would look like the following example: OOCCXXXX 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.
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. **Note:** Read access for database tags is available to all users regardless of security area.

Field	Description
	✎ This allows users to retrieve data from a specific security area even if they cannot write to that area.
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.
Scan Time	Lets you specify how often the Scan, Alarm, and Control (SAC) program processes the block and any tags chained to it. **Valid Entries** • 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 **Example**

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	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. **Valid Entries** 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.

DI 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.

Field	Description
	Valid Entries
	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.
	Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($).
	Invalid Entries
	You cannot use the following special characters in a tag name:
	~ ` + ^ : ? " * = { } . , ; ? @
	Examples
	AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag.
	Valid Entries
	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	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. 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.
I/O Address	Lets you enter the location in the process hardware where data for this tag is saved and where output is sent. **Valid Entries** Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations. ⚠️ **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. ⚠️ **CAUTION:** TestConfiguration 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.

Field	Description
Signal Conditioning	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range. **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. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.
H/W Options	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range. **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. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.
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. **Valid Entries**

Field	Description
	• 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 **Example** 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	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. **Valid Entries** 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
Open Tag	Lets you enter a descriptive label for the logical 0 value received by the tag. You can display this label

Field	Description
	in the iFIX WorkSpace through a Data link to aid operators in interpreting the value for the contact. **Valid Entries** A label of up to 16 characters. **Examples** Open, Off
Close Tag	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. **Valid Entries** A label of up to 16 characters. **Examples** Close, On.

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
	to show alarm conditions, and enabling other tags to detect alarms from the tag. **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.
Enable Event	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. Analog Output, Analog Register, Digital Output, Digital Register, Digital Input, and Text blocks have event messaging capabilities. **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.
Priority	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

Field	Description
	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. **Valid Entries** INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL **✎ 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).
Alarm Type	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. **Valid Entries** Open, Close, Change of State, None
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.

Field	Description
	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** Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples** 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. 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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector. Select either Milliseconds or Seconds.

Field	Description
Collector Compression	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. Select Disabled to prevent the tag from being compressed.
Collector Deadband	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. Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage. Select Absolute to set the Collector Deadband value to an absolute value. 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)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver. After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred. The Collector Compression Timeout value should be in increments of your collection interval, and not less.

Field	Description
	Valid Entries Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature: • 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.

Field	Description
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. 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.

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.
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	Lets you select whether the tag is initially placed on or off scan. 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

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	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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. **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.
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.

Field	Description
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.

DO 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** Tag names must begin with a letter or number and can be up to 256 characters, including certain spe-

Field	Description
	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. Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name: ~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries** 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	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. 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.
I/O Address	Lets you enter the location in the process hardware where data for this tag is saved and where output is sent. **Valid Entries** Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations. ⚠️ **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. ⚠️ **CAUTION:** TestConfiguration 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.

Field	Description
H/W Options	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range. **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. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.

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 in the iFIX WorkSpace through a Data link to aid operators in interpreting the value for the contact. **Valid Entries** A label of up to 16 characters. **Examples** Open, Off
Close Tag	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. **Valid Entries** A label of up to 16 characters.

Field	Description
	Examples Close, On.

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 Event	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. Analog Output, Analog Register, Digital Output, Digital Register, Digital Input, and Text tags have event messaging capabilities. **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.

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** Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples** 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.

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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector. Select either Milliseconds or Seconds.
Collector Compression	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. Select Disabled to prevent the tag from being compressed.
Collector Deadband	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. Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage. Select Absolute to set the Collector Deadband value to an absolute value. Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.

Field	Description
Compression Time-out (ms)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver. After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred. The Collector Compression Timeout value should be in increments of your collection interval, and not less. **Valid Entries** Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature: • 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.
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. 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.

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
	Initial Value is not defined, SAC does not output a value during initialization. **Valid Entries** A value between the Low and High Limit (EGU) fields.
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. > ✏️ **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.
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 down-

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.

DR 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
	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.
	Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($).
	Invalid Entries
	You cannot use the following special characters in a tag name:
	~ ` + ^ : ? " * = { } . , ; ? @
	Examples
	AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag.
	Valid Entries
	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	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. 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.
I/O Address	Lets you enter the location in the process hardware where data for this tag is saved and where output is sent. **Valid Entries** Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations. ⚠️ **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. ⚠️ **CAUTION:** TestConfiguration 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.

Field	Description
H/W Options	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range. ✏️ **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. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.

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 in the iFIX WorkSpace through a Data link to aid operators in interpreting the value for the contact. **Valid Entries** A label of up to 16 characters. **Examples** Open, Off
Close Tag	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. **Valid Entries** A label of up to 16 characters.

Field	Description
	Examples Close, On.

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.

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**

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	Used with the collection interval to schedule collection of data from a tag. **Valid Entries** Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples** 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. 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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector. Select either Milliseconds or Seconds.
Collector Compression	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. Select Disabled to prevent the tag from being compressed.
Collector Deadband	Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values

Field	Description
	that fall within a deadband centered around the last reported value. Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage. Select Absolute to set the Collector Deadband value to an absolute value. 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)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver. After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred. The Collector Compression Timeout value should be in increments of your collection interval, and not less. **Valid Entries** Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature:

Field	Description
	• 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.
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. The Perform by Comments Required check box appears in every tag configuration where Electron-

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.
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	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. Analog Output, Analog Register, Digital Output, Digital Register, Digital Input, and Text blocks have event messaging capabilities. **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.

Field	Description
IO Address Type	Lets you enter the base number system used by the I/O Address field. **Valid Entries** 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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. > 📝 **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.
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 down-

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.

DR2 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
	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.
	Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($).
	Invalid Entries
	You cannot use the following special characters in a tag name:
	~ ` + ^ : ? " * = { } . , ; ? @
	Examples
	AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag.
	Valid Entries
	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	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.
	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.
I/O Address	Lets you enter the location in the process hardware where data for this tag is saved and where output is sent.
	Valid Entries
	Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations.
	⚠ **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.
	⚠ **CAUTION:** TestConfiguration 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.

Field	Description
H/W Options	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range. 📝 **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. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.

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 in the iFIX WorkSpace through a Data link to aid operators in interpreting the value for the contact. **Valid Entries** A label of up to 16 characters. **Examples** Open, Off
Close Tag	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. **Valid Entries** A label of up to 16 characters.

Field	Description
	Examples Close, On.

E-Signature

Field	Description
Type	The Type of Electronic Signature: • 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. The Perform by Comments Required check box appears in every tag configuration where Electron-

Field	Description
	ic Signature settings are available. By default, this check box is disabled.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. 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.
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	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. Analog Output, Analog Register, Digital Output, Digital Register, Digital Input, and Text blocks have event messaging capabilities.

Field	Description
	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.
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. **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.
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
	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.

DT 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** 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. Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points

Field	Description
	(!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name: ~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries** 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	Lets you enter the tag's minimum value. **Valid Entries** - Standard Integer. - Expanded Decimal Notation, ranging from -9999999 to 9999999.

Field	Description
	• 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). ✎ **Note:** The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. 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. 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. If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
High Limit	Lets you enter the tag's maximum value. **Valid Entries** You can enter a high limit in one of three formats: • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38.

Field	Description
	• Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (un-signed integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). 📝 **Note:** The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more informa-tion. In a Calculation or a Signal Select tag, if the out-put 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. If you want to display a value of 1.236 from the Calculation tag, you must enter three or more deci-mal places in the High Limit field. If you are using scientific notation, up to six deci-mal places may be configured with precision, and the range may be positive or negative.
Units	Lets you enter text describing the engineering units range. **Valid Entries** Up to 33 characters. **Example** Kilograms per square meter, Liters per minute, de-grees Celsius, 📝 **Note:** This entry does not affect the calculation or function of any variables in iFIX. It is

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	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** Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples**

Field	Description
	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.
	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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.
	Select either Milliseconds or Seconds.
Collector Compression	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.
	Select Disabled to prevent the tag from being compressed.
Collector Deadband	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.
	Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.
	Select Absolute to set the Collector Deadband value to an absolute value.

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)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver. After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred. The Collector Compression Timeout value should be in increments of your collection interval, and not less. **Valid Entries** Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature: • 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.
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. 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.

Advanced Options

Field	Description
Dead Time	Lets you specify the length of the delay in seconds before transferring the value of upstream tag to the next tag in the chain. **Valid Entries**

Field	Description
	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. **Examples** 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. 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.
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. **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.
Previous Block	Displays the name of the previous (upstream) tag.

Field	Description
	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 down-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.

ETR 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** 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. Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name: ~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries**

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	Lets you enter the tag's minimum value. **Valid Entries** - 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). **Note:** The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. In a Calculation or Signal Select tag, if the output of the tag is 10 and the Low Limit is 15, the tag

Field	Description
	clamps the value at 15. You must enter a Low Limit of 10 or less to output a value of 10. 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. If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
High Limit	Lets you enter the tag's maximum value. **Valid Entries** You can enter a high limit in one of three formats: • 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). > **Note:** > The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. 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.

Field	Description
	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. If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
Units	Lets you enter text describing the engineering units range. **Valid Entries** Up to 33 characters. **Example** Kilograms per square meter, Liters per minute, degrees Celsius, ✏️ **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.

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.

Field	Description
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** Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples** 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. 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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector. Select either Milliseconds or Seconds.
Collector Compression	Lets you select if the tag is set for compression. Compression applies a smoothing filter to incom-

Field	Description
	ing data by ignoring incremental changes in values that fall within a deadband centered around the last reported value. Select Disabled to prevent the tag from being compressed.
Collector Deadband	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. Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage. Select Absolute to set the Collector Deadband value to an absolute value. 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)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver. After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred. The Collector Compression Timeout value should be in increments of your collection interval, and not less. **Valid Entries**

Field	Description
	Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature: • 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. The Perform by Comments Required check box appears in every tag configuration where Electron-

Field	Description
	ic Signature settings are available. By default, this check box is disabled.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. 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
Buffer Clear Status	Lets you clear the block's data buffers every time the block is put on scan. **Valid Entries** Select the check box to clear data buffers. Clear it to suppress this feature.
Input Tag	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. **Valid Entries** A block and field name pair in the tag.field (F_CV) format. > 📝 **Note:** > To chain Extended Trend blocks, enter the Extended Trend tag's name and the field F_INP.

Field	Description
Compression Factor	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. **Valid Entries** A value from 1 - 255 that represents the number of samples to collect. **Example** 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). > ✎ **Note:** > Using this field does not affect or delay the value passed by the Next tag field to the downstream tag.
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.

Field	Description
	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.
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 down-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.

Field	Description
	Valid Entries Text, up to 80 characters.

EV 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** 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. Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name:

Field	Description
	~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries** 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.

Event Definitions

Field	Description
If Condition 1	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. > ✏️ **Note:** > The command is latched. This means that the tag remembers the last operation and only performs a new operation if the condition has changed. **Valid Entries** An expression in the following format:

Field	Description
	Value or Alarm operator condition
	Example
	Value = 83.2
	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.
Then	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.
	Valid Entries
	An expression in the following format:
	command tag
	Example
	RUN PROG1
	Note: 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.
Else	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.

Field	Description
	Valid Entries An expression in the following format: command tag **Example** CLOSE DO3 ⚠️ **Note:** 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.
If Condition 2	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. ⚠️ **Note:** The command is latched. This means that the tag remembers the last operation and only performs a new operation if the condition has changed. **Valid Entries** An expression in the following format: Value or Alarm operator condition **Example** Value = 83.2

Field	Description
	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.
Then	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. **Valid Entries** An expression in the following format: command tag **Example** RUN PROG1 **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.
Else	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. **Valid Entries** An expression in the following format: command tag

Field	Description
	Example CLOSE DO3 📝 **Note:** 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.

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	Used with the collection interval to schedule collection of data from a tag. **Valid Entries** Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples** 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. 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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector. Select either Milliseconds or Seconds.
Collector Compression	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. Select Disabled to prevent the tag from being compressed.
Collector Deadband	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.

Field	Description
	Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage. Select Absolute to set the Collector Deadband value to an absolute value. 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)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver. After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred. The Collector Compression Timeout value should be in increments of your collection interval, and not less. **Valid Entries** Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature: • 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
	• 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.
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. 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.

Advanced Options

Field	Description
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. **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.
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.

Field	Description
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.

FN 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** Tag names must begin with a letter or number and can be up to 256 characters, including certain spe-

Field	Description
	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. Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name: ~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries** 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	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.

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.

Field	Description
	Valid Entries
	Any numeric value that does not exceed the collection interval. The value is in seconds.
	Examples
	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.
	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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.
	Select either Milliseconds or Seconds.
Collector Compression	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.
	Select Disabled to prevent the tag from being compressed.
Collector Deadband	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.
	Select Disabled to prevent the tag from being compressed.

Field	Description
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage. Select Absolute to set the Collector Deadband value to an absolute value. 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)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver. After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred. The Collector Compression Timeout value should be in increments of your collection interval, and not less. **Valid Entries** Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature: • 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
	• 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.
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. 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.

Advanced Options

Field	Description
Output Areas A, B, C, D	Lets you specify the destinations of the Fanout tag. **Valid Entries** A tag name (F_CV is appended automatically) or specific tag and field name pair in the tag.field format. **Example** 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. **ⓘ 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.
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. **✎ Note:** Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a

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 down-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.

GAB 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
	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.
	Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($).
	Invalid Entries
	You cannot use the following special characters in a tag name:
	~ ` + ^ : ? " * = { } . , ; ? @
	Examples
	AI1, CA_10, DI#, 4PID, 'TEST'

Field	Description
Description	Lets you enter optional descriptive text about the tag. **Valid Entries** 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 Tags

Field	Description
Tag 0-15	The tag of another block to monitor for alarms.

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.

E-Signature

Field	Description
Type	The Type of Electronic Signature:

Field	Description
	• 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. 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources.

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	Lets you select whether the tag is initially placed on or off scan. 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.
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. > ✏️ **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.
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
	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.
Scan Time	Lets you specify how often the Scan, Alarm, and Control (SAC) program processes the tag and any tags (blocks) chained to it. **Valid Entries** 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 **Example** 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.

Field	Description
Phase At	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. **Valid Entries** 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.

GEN 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** 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

Field	Description
	least one non-numeric character. For iFIX internal databases, single quotes are not supported in tag names. Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name: ~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries** 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 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	The Type of Electronic Signature: • 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. The Perform by Comments Required check box appears in every tag configuration where Electron-

Field	Description
	ic Signature settings are available. By default, this check box is disabled.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes.
	Unsigned writes can originate from scripts, recipe downloads, and other data sources.
	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
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	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.
	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

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	Lets you select whether the tag is initially placed on or off scan. 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.
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. 📝 **Note:** Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a

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 down-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.
Process by Exception	Enables exception-based processing for the tag.

Field	Description
Scan Time	Lets you specify how often the Scan, Alarm, and Control (SAC) program processes the tag and any tags (blocks) chained to it. **Valid Entries** • 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 **Example** 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.

HS 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
	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.
	Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($).
	Invalid Entries
	You cannot use the following special characters in a tag name:
	~ ` + ^ : ? " * = { } . , ; ? @
	Examples
	AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag.
	Valid Entries
	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	Lets you enter the tag's minimum value. **Valid Entries** • 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 (un-signed integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). > **✎ Note:** > The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. 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. 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. If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
High Limit	Lets you enter the tag's maximum value. **Valid Entries**

Field	Description
	You can enter a high limit in one of three formats: • 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 (un-signed integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). **Note:** The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. 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. 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. If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
Units	Lets you enter text describing the engineering units range. **Valid Entries** Up to 33 characters.

Field	Description
	Example Kilograms per square meter, Liters per minute, degrees Celsius, > ✎ **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.

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.

Field	Description
	Valid Entries
	Any numeric value that does not exceed the collection interval. The value is in seconds.
	Examples
	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.
	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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector.
	Select either Milliseconds or Seconds.
Collector Compression	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.
	Select Disabled to prevent the tag from being compressed.
Collector Deadband	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.
	Select Disabled to prevent the tag from being compressed.

Field	Description
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage. Select Absolute to set the Collector Deadband value to an absolute value. 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)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver. After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred. The Collector Compression Timeout value should be in increments of your collection interval, and not less. **Valid Entries** Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature: • 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
	• 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.
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. 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.

Advanced Options

Field	Description
Auto Clear Status	Lets you specify when the Histogram tag clears the histogram chart. **Valid Entries** 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. 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.
Interval	Lets you specify the range of values represented by each column in the bar graph. **Valid Entries** A number within the EGU range. > 🛈 **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.
Group Size	Lets you specify: • How often the Histogram updates the associated chart. The tag calculates the update period by multiplying the Group value by the

Field	Description
	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. • The number of occurrences displayed on the histogram and the maximum height of the display bars. **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. **Valid Entries** A time in seconds from 1 to 1000.
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. **Note:** Read access for database tags is available to all users regardless of security area.

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	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
	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.
	Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($).
	Invalid Entries
	You cannot use the following special characters in a tag name:
	~ ` + ^ : ? " * = { } . , ; ? @
	Examples
	AI1, CA_10, DI#, 4PID, 'TEST'

Field	Description
Description	Lets you enter optional descriptive text about the tag. **Valid Entries** 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.

Timer and Total Options

Field	Description
Pass	**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.
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 internal 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 *	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). **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.
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	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 to show alarm conditions, and enabling other tags to detect alarms from the tag. **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.
Priority	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. **Valid Entries**

Field	Description
	INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL **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).

E-Signature

Field	Description
Type	The Type of Electronic Signature: • 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
	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.
	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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes.
	Unsigned writes can originate from scripts, recipe downloads, and other data sources.
	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
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.
Clear	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.
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 Man-

Field	Description
	ager or the iFIX WorkSpace, the operator must have access to that tag's security area. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. **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.
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 down-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**

Field	Description
	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.

LL 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** 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. Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([),

Field	Description
	close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name: ~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries** 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	Lets you enter the tag's minimum value. **Valid Entries** • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999.

Field	Description
	• Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. • Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (un-signed integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). **Note:** The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. 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. 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. If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
High Limit	Lets you enter the tag's maximum value. **Valid Entries** You can enter a high limit in one of three formats: • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38.

Field	Description
	• Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (un-signed integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). 📝 **Note:** The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. 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. 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. If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
Units	Lets you enter text describing the engineering units range. **Valid Entries** Up to 33 characters. **Example** Kilograms per square meter, Liters per minute, degrees Celsius, 📝 **Note:** This entry does not affect the calculation or function of any variables in iFIX. It is

Field	Description
	✏️ used strictly as a display label to identify the engineering units.

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.

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**

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	Used with the collection interval to schedule collection of data from a tag. **Valid Entries** Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples** 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. 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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector. Select either Milliseconds or Seconds.
Collector Compression	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. Select Disabled to prevent the tag from being compressed.
Collector Deadband	Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values

Field	Description
	that fall within a deadband centered around the last reported value. Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage. Select Absolute to set the Collector Deadband value to an absolute value. 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)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver. After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred. The Collector Compression Timeout value should be in increments of your collection interval, and not less. **Valid Entries** Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature:

Field	Description
	• 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.
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. The Perform by Comments Required check box appears in every tag configuration where Electron-

Field	Description
	ic Signature settings are available. By default, this check box is disabled.

Advanced Options

Field	Description
Scaling Factor	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. **Valid Entries** A value from -100.00 to +100.00. Enter 1 to disable this function.
Lead Time Constant	Lets you specify the lead time constant. **Valid Entries** A value from 0.00 to +100.00 minutes. Enter 0 to disable this function. 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.
Lag Time Constant	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. **Valid Entries** A value from 0.00 to +100.00 minutes. Enter 0 if you do not want to use any lag time.

Field	Description
	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.
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. **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.
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 down-

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
	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. Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name: ~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries** 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
Driver	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. 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.
I/O Address	Lets you enter the location in the process hardware where data for this tag is saved and where output is sent. **Valid Entries** Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations. ⚠️ **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. ⚠️ **CAUTION:** TestConfiguration 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.

Field	Description
H/W Options	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range. **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. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.
Enable Driver 1-2	Allows you to enable or disable the second or third digital input value. **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.
Driver 1-2	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. 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.
I/O Address 1-2	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

Field	Description
	closed based on the Turn on Above and Turn off Below values. **Valid Entries** Depends on your driver. Consult your I/O driver manual for details on the proper input/output addresses and configurations. ⚠️ **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 blocks to occasionally miss a value.
H/W Options 1-2	Lets you select any specific device control addressing format that the tag uses to communicate with process hardware on the plant floor. **Valid Entries** For most process hardware, this field is usually left blank. Consult your I/O driver manual for the applicable hardware code if necessary.
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. **Valid Entries** • 0 (one shot processing) • 0.05 to .95 in .05 increments (subsecond scan times) • 1 to 60 in 1 second increments

Field	Description
	• 1M to 60M in 1 minute increments • 1H to 24H in 1 hour increments **Example** 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	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. **Valid Entries** 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.

Device States

Field	Description
Alarm 0-7 Enable	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.

Field	Description
	📝 **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.
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
	to show alarm conditions, and enabling other tags to detect alarms from the tag. **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.
Realarm	Enables or disables the re-alarm status of the tag. **Valid Entries** 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.
Priority	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. **Valid Entries** INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL

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	Used with the collection interval to schedule collection of data from a tag. **Valid Entries** Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples** 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. 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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector. Select either Milliseconds or Seconds.
Collector Compression	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. Select Disabled to prevent the tag from being compressed.
Collector Deadband	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.

Field	Description
	Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.

Select Absolute to set the Collector Deadband value to an absolute value.

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) | Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.

After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.

The Collector Compression Timeout value should be in increments of your collection interval, and not less.

Valid Entries

Any numeric value. |

E-Signature

Field	Description
Type	The Type of Electronic Signature:

- 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
	• 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.
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. 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.

Advanced Options

Field	Description
Initial Scan	Lets you select whether the tag is initially placed on or off scan. 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.
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. > **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.
Previous Block	Displays the name of the previous (upstream) tag. **Valid Entries** None. This is a read-only field.

Field	Description
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 down-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.

MDO 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** 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. Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name: ~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries**

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	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. 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.
I/O Address	Lets you enter the location in the process hardware where data for this tag is saved and where output is sent. **Valid Entries** Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations. ⚠️ **CAUTION:** Do not assign the same I/O address to tags when using exception-based and time-based processing. Doing so will

Field	Description
	⚠ cause the exception-based tags to occasionally miss a value. ⚠ **CAUTION:** TestConfiguration 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.
H/W Options	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range. ✎ **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. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.
Normally Closed	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.
Retry Output	If SET then the initial 'CLOSE' output is sent every scan cycle until a confirming CLOSE is read back

Field	Description
	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.
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. **Valid Entries** • 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 **Example** 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	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

Field	Description
	or longer, SAC offsets the initial scan starting at midnight. **Valid Entries** 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
Open Tag	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. **Valid Entries** A label of up to 16 characters. **Examples** Open, Off
Close Tag	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. **Valid Entries** A label of up to 16 characters. **Examples** Close, On.

E-Signature

Field	Description
Type	The Type of Electronic Signature: • 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. 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes.

Field	Description
	Unsigned writes can originate from scripts, recipe downloads, and other data sources. 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
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	Lets you select whether the tag is initially placed on or off scan. 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.
Duty Cycle	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.
Timeout	This is the maximum number if 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-

Field	Description
	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.
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. ✏️ **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.
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
	Valid Entries Text, up to 80 characters.

ODO 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** 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. Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name:

Field	Description
	~ ` + ^ : ? " * = { } . , ; ? @
	Examples
	AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag.
	Valid Entries
	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	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.
	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.
I/O Address	Lets you enter the location in the process hardware where data for this tag is saved and where output is sent.
	Valid Entries

Field	Description
	Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations. ⚠️ **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. ⚠️ **CAUTION:** TestConfiguration 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.
H/W Options	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range. 📝 **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. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.

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	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. **Valid Entries** A label of up to 16 characters. **Examples** Open, Off
Close Tag	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. **Valid Entries** A label of up to 16 characters. **Examples** Close, On.

Alarm Options

Field	Description
Alarm Areas	Displays the alarm areas that receive alarms and messages generated by this tag. Double-click an

Field	Description
	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 to show alarm conditions, and enabling other tags to detect alarms from the tag. **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.
Priority	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. **Valid Entries** INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL

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).

Advanced Options

Field	Description
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. **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.
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 down-

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	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

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.

Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($).

Invalid Entries

You cannot use the following special characters in a tag name: |

Field	Description
	~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries** 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.

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	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. 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.

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
	Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples** 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. 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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector. Select either Milliseconds or Seconds.
Collector Compression	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. Select Disabled to prevent the tag from being compressed.
Collector Deadband	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. Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.

Field	Description
	Select Absolute to set the Collector Deadband value to an absolute value. 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)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver. After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred. The Collector Compression Timeout value should be in increments of your collection interval, and not less. **Valid Entries** Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature: - 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	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.
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. 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.

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
	Valid Entries Any number from 0 to 6 digits of precision. > ✎ **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 .
Sort Order	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. **Valid Entries** Descending, Ascending, or No Sorting. By default, the sort order is Descending. Database Manager sorts the data as follows: • 1 Special characters (such as punctuation marks) by ASCII value. • 2 Numbers by numeric value. • 3 Letters in alphabetic order.
Initial Scan	Lets you select whether the tag is initially placed on or off scan. 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.

Field	Description
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. > ✎ **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.
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 Imple-

Field	Description
	menting 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.
Scan Time	Lets you specify how often the Scan, Alarm, and Control (SAC) program processes the tag and any tags (blocks) chained to it. **Valid Entries** • 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 **Example** 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	Lets you specify how long the Scan, Alarm, and Control (SAC) program delays in scanning the tag.

Field	Description
	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. **Valid Entries** 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-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.

PAR Tag

This tag contains the following details:

General

Field	Description
Tag Name	Lets you enter the tag's name. The tag name is ref-erenced by other tags, display links, and other pro-grams. 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** Tag names must begin with a letter or number and can be up to 256 characters, including certain spe-cial characters. Tag names must also contain at least one non-numeric character. For iFIX internal

Field	Description
	databases, single quotes are not supported in tag names.
	Tag names can also include dashes (-), under-scores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($).
	Invalid Entries
	You cannot use the following special characters in a tag name:
	~ ` + ^ : ? " * = { } . , ; ? @
	Examples
	AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag.
	Valid Entries
	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	Lets you enter the block's minimum value.

Field	Description
	Valid Entries You can enter a low limit in one of three formats: • 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. > ✏️ **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.
High Limit	Lets you enter the block's maximum value. **Valid Entries** You can enter a low limit in one of three formats: • 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. > ✏️ **Note:** > If you are using scientific notation, up to six decimal places may be configured with

Field	Description
	📝 precision, and the range may be positive or negative.
Units	Lets you enter text describing the engineering units range. **Valid Entries** Up to 33 characters. **Example** Kilograms per square meter; liters per minute; degrees Celsius. 📝 **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.

Array Values

Field	Description
Value 01-60	Lets you read values from or write values to each of the 60 fields. **Valid Entries** You can enter a value in one of three formats: Stan • 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
	• Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38. ✎ **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.
Text 01-60	Lets you read descriptions from or write descriptions to each of the 60 fields. **Valid Entries** Up to 40 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.

Advanced Options

Field	Description
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 Man-

Field	Description
	ager or the iFIX WorkSpace, the operator must have access to that tag's security area. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. > ✎ **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.
Previous Block	Displays the name of the previous (upstream) tag. **Valid Entries** None. This is a read-only field.
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**

Field	Description
	Text, up to 80 characters.

PG 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** 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. Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name: ~ ` + ^ : ? " * = { } . , ; ? @

Field	Description
	Examples
	AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag.
	Valid Entries
	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
PGM Statement 0 -19	Lets you enter the commands and arguments for the Program tag. Use the Browse (...) button to select from a list of valid commands.
	Valid Entries
	The list box can include up to 20 programming statements, each containing up to 44 alphanumeric characters in length.

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
	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 to show alarm conditions, and enabling other tags to detect alarms from the tag. **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.
Priority	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. **Valid Entries** INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL

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	Used with the collection interval to schedule collection of data from a tag. **Valid Entries** Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples** 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. 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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector. Select either Milliseconds or Seconds.
Collector Compression	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. Select Disabled to prevent the tag from being compressed.
Collector Deadband	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.

Field	Description
	Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.

Select Absolute to set the Collector Deadband value to an absolute value.

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) | Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.

After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.

The Collector Compression Timeout value should be in increments of your collection interval, and not less.

Valid Entries

Any numeric value. |

E-Signature

Field	Description
Type	The Type of Electronic Signature:

- 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
	• 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.
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. 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.

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	Lets you select whether the tag is initially placed on or off scan. 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.
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. > **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.
Previous Block	Displays the name of the previous (upstream) tag.

Field	Description
	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 down-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.
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 chained to it. **Valid Entries**

Field	Description
	• 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 **Example** 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	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. **Valid Entries** 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.

PI2 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** 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. Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name: ~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries**

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 * 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	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 to show alarm conditions, and enabling other tags to detect alarms from the tag. ✎ **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.

Field	Description
Priority	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. **Valid Entries** INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL ✎ **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.
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	The Type of Electronic Signature: • 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. 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes.

Field	Description
	Unsigned writes can originate from scripts, recipe downloads, and other data sources. 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
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.
Feedback Tag	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.
Reverse Output	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.
No Initial Clamp	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

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	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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. **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.
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 down-

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.

PID 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
	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.
	Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($).
	Invalid Entries
	You cannot use the following special characters in a tag name:
	~ ` + ^ : ? " * = { } . , ; ? @
	Examples
	AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag.
	Valid Entries
	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	Lets you enter the tag's minimum value. **Valid Entries** • 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 (un-signed integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). **Note:** The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. 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. 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. If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
High Limit	Lets you enter the tag's maximum value. **Valid Entries**

Field	Description
	You can enter a high limit in one of three formats: • 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 (un-signed integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). **Note:** The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. 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. 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. If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
EGU Tag	Lets you enter text describing the engineering units range. **Valid Entries** Up to 33 characters.

Field	Description
	Example Kilograms per square meter, Liters per minute, degrees Celsius. > ✏️ **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.
Low Output Limit	Displays the low limit for the output of the PID block. **Valid Entries** The lowest value the controlled variable (the Analog Output or another PID block) can have should be specified in the Low Limit field. 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.
High Output Limit	Displays the high limit for the output of the PID block. **Valid Entries** The highest value the controlled variable (the Analog Output or another PID block) can have should be specified in the High Limit field. 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-

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	Lets you enter a tuning constant, equal to the inverse of the proportional gain multiplied by 100%. **Valid Entries** 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.
Integral Time	Lets you enter an integral time constant. **Valid Entries** A value from 0.000 to 99.000 minutes per repeat. 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.

Field	Description
	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.
Derivative Time	Lets you enter a derivative time constant measured in minutes per repeat. **Valid Entries** A value from 0 to 20 minutes. Enter values smaller than a minute in decimals. **Example** 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. **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.
Alpha-rate Factor	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. **Valid Entries**

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	Lets you specify a proportional action constant for algorithm tuning. This value serves as a multiplier for the proportional term. **Valid Entries** 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.
Gamma-reset Factor	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. **Valid Entries** 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.

Setpoint Limits and Options

Field	Description
Dead band value	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. **Valid Entries** Numeric value within the EGU range.

Field	Description
	Example 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.
Deviation value	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: DEVIATION = SET POINT VALUE - PROCESS VARIABLE **Valid Entries** The appropriate value, in engineering units. Use 0 to disable the deviation alarm.
Gap Action	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. **Valid Entries** Enter a value that represents the dead band range. If the change is within this range, the deviation is set to 0 (zero).
Low Setpoint Clamp	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.

Field	Description
	Valid Entries The minimum value for the set point.
High Setpoint Clamp	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. **Valid Entries** The maximum value for the set point.
Setpoint Tag	Lets you specify the desired value of a controlled variable. **Valid Entries** 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. 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. 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.

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 to show alarm conditions, and enabling other tags to detect alarms from the tag. **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.
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	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** Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples** 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. 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.

Field	Description
Time Resolution	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector. Select either Milliseconds or Seconds.
Collector Compression	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. Select Disabled to prevent the tag from being compressed.
Collector Deadband	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. Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage. Select Absolute to set the Collector Deadband value to an absolute value. 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)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.

Field	Description
	After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred. The Collector Compression Timeout value should be in increments of your collection interval, and not less. **Valid Entries** Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature: • 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.

Field	Description
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.
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. 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.

Advanced Options

Field	Description
Reverse Output	Inverts the output of the tag.
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.
Transfer Status	Lets you control how the PID tag reacts during a transition between automatic and manual modes. **Valid Entries**

Field	Description
	• 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	Lets you control how the PID tag reacts during a transition between automatic and manual modes. **Valid Entries** • 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	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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. > ✎ **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.
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 Imple-

Field	Description
	menting 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.

RB 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** 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.

Field	Description
	Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name: ~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries** 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	Lets you enter the tag's minimum value. **Valid Entries**

Field	Description
	• 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).
	Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information.
	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.
	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.
	If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
High Limit	Lets you enter the tag's maximum value. **Valid Entries** You can enter a high limit in one of three formats: • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999.

Field	Description
	• 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). **Note:** The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. 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. 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. If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
Units	Lets you enter text describing the engineering units range. **Valid Entries** Up to 33 characters. **Example** Kilograms per square meter, Liters per minute, degrees Celsius,

Field	Description
	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.
Ratio Value	Multiplies the value from the upstream block by a constant. **Valid Entries** The constant by which you want to multiply the incoming signal. The default value is 1.
Bias Value	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. **Valid Entries** 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. **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.
Offest Value	Lets you specify the value you want to subtract from the upstream tag's incoming signal. **Valid Entries**

Field	Description
	A numeric constant or a tag and field name pair in the format tag.field.

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 to show alarm conditions, and enabling other tags to detect alarms from the tag. **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.

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
	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** Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples** 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. 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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector. Select either Milliseconds or Seconds.

Field	Description
Collector Compression	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. Select Disabled to prevent the tag from being compressed.
Collector Deadband	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. Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage. Select Absolute to set the Collector Deadband value to an absolute value. 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)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver. After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred. The Collector Compression Timeout value should be in increments of your collection interval, and not less.

Field	Description
	Valid Entries Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature: • 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.

Field	Description
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. 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.

Advanced Options

Field	Description
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. 📝 **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.
Previous Block	Displays the name of the previous (upstream) tag. **Valid Entries**

Field	Description
	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 down-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.

RM 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** 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. Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name: ~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries**

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	Lets you enter the tag's minimum value.

Valid Entries

- 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).

> **Note:**
> The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information.

In a Calculation or Signal Select tag, if the output of the tag is 10 and the Low Limit is 15, the tag

Field	Description
	clamps the value at 15. You must enter a Low Limit of 10 or less to output a value of 10.
	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.
	If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
High Limit	Lets you enter the tag's maximum value.
	Valid Entries
	You can enter a high limit in one of three formats:
	• 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).
	Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information.
	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.

Field	Description
	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. If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
Units	Lets you enter text describing the engineering units range. **Valid Entries** Up to 33 characters. **Example** Kilograms per square meter, Liters per minute, degrees Celsius, > ✎ **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.
Low Operator Limit	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. **Valid Entries** A value between the Low and High EGU fields. If appropriate, you can use the Low EGU for this value.
High Operator Limit	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.

Field	Description
	Valid Entries A value between the Low and High EGU fields. If appropriate, you can use the High EGU for this value.
Scan Time	Lets you specify how often the Scan, Alarm, and Control (SAC) program processes the tag and any tags chained to it. **Valid Entries** • 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 **Example** 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	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. **Valid Entries** 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-

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	Lets you specify the value you want the tag to reach. **Valid Entries** A value or a tag and field name (uses the current value of another block). 📝 **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.
Ramp Rate 1	Lets you specify the increments at which the current value is modified until reaching the target value for each stage. **Valid Entries** A value based on hours. Use 0.00 to prevent the execution of the ramp stage. **Example**

Field	Description
	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.
Hold Time 1	Lets you specify how long the Ramp tag waits after reaching the target value and before continuing on to the next stage. **Valid Entries** A value based on hours. The default hold time is 0.000. The maximum hold time is 1000 hours. **Example** To hold for one hour, enter 1.000. > **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 SETTIME2 sets the ramp time for the second stage.
Target Value 2	Lets you specify the value you want the tag to reach. **Valid Entries** A value or a tag and field name (uses the current value of another block). > **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

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	Lets you specify the increments at which the current value is modified until reaching the target value for each stage. **Valid Entries** A value based on hours. Use 0.00 to prevent the execution of the ramp stage. **Example** 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.
Hold Time 2	Lets you specify how long the Ramp tag waits after reaching the target value and before continuing on to the next stage. **Valid Entries** A value based on hours. The default hold time is 0.000. The maximum hold time is 1000 hours. **Example** To hold for one hour, enter 1.000. 📝 **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-

Field	Description
	📝 TIME2 sets the ramp time for the second stage.
Target Value 3	Lets you specify the value you want the tag to reach. **Valid Entries** A value or a block and field name (uses the current value of another tag). 📝 **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.
Ramp Rate 3	Lets you specify the increments at which the current value is modified until reaching the target value for each stage. **Valid Entries** A value based on hours. Use 0.00 to prevent the execution of the ramp stage. **Example** 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.

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.

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.

Field	Description
	Valid Entries Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples** 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. 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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector. Select either Milliseconds or Seconds.
Collector Compression	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. Select Disabled to prevent the tag from being compressed.
Collector Deadband	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. Select Disabled to prevent the tag from being compressed.

Field	Description
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage. Select Absolute to set the Collector Deadband value to an absolute value. 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)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver. After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred. The Collector Compression Timeout value should be in increments of your collection interval, and not less. **Valid Entries** Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature: • 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
	• 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.
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. 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.

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.
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. 📝 **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.
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.

Field	Description
	✎ **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.

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
	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** 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. Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name: ~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries** 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.

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	Lets you pass the adjustment value of the Statistical Control block to the specified tag. The tag can add this adjustment to: • The current value of the Analog Output block. • The target value of the PID block. • The target value of the Ramp block. **Valid Entries** The tag and field name pair in tag.field format.
Recalculate Status	Re-computes the upstream Statistical Data tag's upper and lower control limits after adjusting a value and the delay time expires. **Valid Entries** Select the check box to recalculate the limits. Clear the check box to maintain previously set control limits.
Alarm Suppression	Suppresses the generation of alarms until the Statistical Data tag processes a new set of groups. **Valid Entries** Select the check box to suppress alarms. Clear the check box to generate alarms.

Field	Description
Track Messages	Sends a message to the Statistical Control block's active alarm destinations each time the tag adjusts a value. **Valid Entries** Select the check box to send messages. Clear the check box to suppress messages.
Show Calc Adjustment	Lets you display the latest calculated adjustment in the iFIX WorkSpace. **Valid Entries** 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. > **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.
Slope Constant	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. **Valid Entries** A value between -99,999.0 and 900,000.0
Deviation Constant	Multiplies the average deviation of XBAR values from XBARBAR by the specified value. The deviation constant is a floating-point scaling factor.

Field	Description
	Valid Entries
	The appropriate floating point value.
Delay Time	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.
	Valid Entries
	A time in seconds between 1 and 32767.
	🛈 **Tip:** Allow time for the upstream block to read at least one full set of data groups.

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 to show alarm conditions, and enabling other tags to detect alarms from the tag.

Field	Description
	📝 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.

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
	Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples** 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. 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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector. Select either Milliseconds or Seconds.
Collector Compression	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. Select Disabled to prevent the tag from being compressed.
Collector Deadband	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. Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.

Field	Description
	Select Absolute to set the Collector Deadband value to an absolute value. 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)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver. After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred. The Collector Compression Timeout value should be in increments of your collection interval, and not less. **Valid Entries** Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature: • 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	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.
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. 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.

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
	mode, the tag receives data from the operator, scripts, recipes, or Program blocks.
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. > ✏️ **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.
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**

Field	Description
	Text, up to 80 characters.

SD 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
	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.
	Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($).
	Invalid Entries
	You cannot use the following special characters in a tag name:
	~ ` + ^ : ? " * = { } . , ; ? @

Field	Description
	Examples
	AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag.
	Valid Entries
	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	Lets you enter the tag's minimum value.
	Valid Entries
	• 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
	Note: The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. 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. 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. If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
High Limit	Lets you enter the tag's maximum value. **Valid Entries** You can enter a high limit in one of three formats: • 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). **Note:** The I/O driver can set certain limitations on the engineering units range. Consult

Field	Description
	📝 your I/O driver manual for more information.
	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. 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. If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
Units	Lets you enter text describing the engineering units range. **Valid Entries** Up to 33 characters. **Example** Kilograms per square meter, Liters per minute, degrees Celsius, 📝 **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.
Scan Qualifier	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.

Field	Description
	Valid Entries The name of a block with an F_CV field that returns a 1 or 0.
Input Score	Lets you specify the input source of the Statistical Data tag. **Valid Entries** • 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	Lets you specify the input source of the Statistical Data tag. **Valid Entries** 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.
Observations/group	Lets you specify the number of observations that the Statistical Data tag makes per group. **Valid Entries** A value from 1 to 25. **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.

Field	Description
Wait time	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. **Valid Entries** A value from 0 to 32767 seconds. > ✏ **Note:** > The wait time is valid only when the tag is in Automatic mode.
CTL limit calc mode	Lets you specify the calculation mode of control, warning, and specification limits for XBAR, S, and R charts. **Valid Entries** • Startup – Instructs the tag not to recalculate limits for XBAR, R, and S charts after startup. 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. > ✏ **Note:** > If you choose to manually input limit values, verify that the values are very close to

Field	Description
	📝 the ones the block would calculate. Otherwise, the validity of statistical alarms and control charts is questionable.
XBB calc mode	Specifies the calculation mode of XBARBAR, SBAR, and RBAR values. **Valid Entries** • 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. 📝 **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.
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
	Valid Entries • 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 **Example** 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	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. **Valid Entries** 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.

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 to show alarm conditions, and enabling other tags to detect alarms from the tag. **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.
Priority	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. **Valid Entries**

Field	Description
	INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL 📝 **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.
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	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** Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples** 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.

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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector. Select either Milliseconds or Seconds.
Collector Compression	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. Select Disabled to prevent the tag from being compressed.
Collector Deadband	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. Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage. Select Absolute to set the Collector Deadband value to an absolute value. Select Percentage to set the Collector Deadband value to a percentage of the Engineering Units, which are specified on the Basic tab.

Field	Description
Compression Time-out (ms)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver. After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred. The Collector Compression Timeout value should be in increments of your collection interval, and not less. **Valid Entries** Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature: • 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.
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. 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.

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	Lets you select whether the tag is initially placed on or off scan. Click On Scan to place the tag on scan as soon as the Scan, Alarm, and Control (SAC) program starts

Field	Description
	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.
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. > ✏️ **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.
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 down-

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.

SQD 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
	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.
	Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($).
	Invalid Entries
	You cannot use the following special characters in a tag name:
	~ ` + ^ : ? " * = { } . , ; ? @
	Examples
	AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag.
	Valid Entries
	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.

Data Definitions

Field	Description
Tag 1 - 20	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. 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.
Direction 1 - 20	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: • 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. **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

Field	Description
	📝 sets the value of each data point's Direction field to Out.
Reset Status Tag 1 - 20	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: • 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	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.

Historian

Field	Description
Tag Description	Lets you enter the tag description that is used by Historian when the tag is collected.

Field	Description
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** Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples** 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. 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.

Field	Description
Time Resolution	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector. Select either Milliseconds or Seconds.
Collector Compression	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. Select Disabled to prevent the tag from being compressed.
Collector Deadband	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. Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage. Select Absolute to set the Collector Deadband value to an absolute value. 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)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.

Field	Description
	After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.
	The Collector Compression Timeout value should be in increments of your collection interval, and not less.
	Valid Entries
	Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature: • 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.

Field	Description
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.
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. 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.

Advanced Options

Field	Description
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.

Field	Description
	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.
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 down-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.

Field	Description
	Valid Entries Text, up to 80 characters.

SQT 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** 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. Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name:

Field	Description
	~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries** 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.

SQL Definitions and Date Filters

Field	Description
SQL Command Name	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. **Valid Entries** An alias up to eight characters. Lowercase letters are automatically capitalized.

Field	Description
Database ID	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.
Event Start Date	Lets you specify when the SQL Trigger tag executes. **Valid Entries** • 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. **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.
Event End Date	Lets you specify when the SQL Trigger tag stops. Use the following guidelines when defining the End Date:

Field	Description
	• 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). **Valid Entries** • 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	Lets you specify how often the Scan, Alarm, and Control (SAC) program processes the tag and any tags chained to it. **Valid Entries** • 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	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

Field	Description
	or longer, SAC offsets the initial scan starting at midnight. **Valid Entries** 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.

Time and Block Events

Field	Description
Event Start Time	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: - 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	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:

Field	Description
	• 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	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: • 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	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. **Valid Entries**

Field	Description
	• 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	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. ⚠️ **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. **Example** 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

Field	Description
	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. 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.
Event Type	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: • 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
	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 to show alarm conditions, and enabling other tags to detect alarms from the tag. > **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.
Priority	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. **Valid Entries** INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL

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	Used with the collection interval to schedule collection of data from a tag. **Valid Entries** Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples** 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. 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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector. Select either Milliseconds or Seconds.
Collector Compression	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. Select Disabled to prevent the tag from being compressed.
Collector Deadband	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.

Field	Description
	Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage. Select Absolute to set the Collector Deadband value to an absolute value. 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)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver. After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred. The Collector Compression Timeout value should be in increments of your collection interval, and not less. **Valid Entries** Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature: • 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
	• 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.
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. 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.

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	Lets you select whether the tag is initially placed on or off scan. 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.
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. > **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.
Previous Block	Displays the name of the previous (upstream) tag.

Field	Description
	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 down-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.
Table Mode	Lets you specify the SELECT mode of the SQL Data tag. Select one of the following options:

Field	Description
	• 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	Choose one of the following: • 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	Lets you enable the SQL Trigger tag to back up process data if it detects a problem with the relational database. **📝 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-

Field	Description
	✎ sis, not whenever the connection is re-established.
Rows	Lets you specify the starting row, depending on the Select Parameters mode: • 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. 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** 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

Field	Description
	databases, single quotes are not supported in tag names. Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name: ~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries** 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	Lets you select an I/O driver, OPC server, or OPC UA server for the tag. The selected driver or serv-

Field	Description
	er enables the tag to communicate with process hardware on the plant floor. 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.
I/O Address	Lets you enter the location in the process hardware where data for this tag is saved and where output is sent. **Valid Entries** Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations. ⚠️ **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. ⚠️ **CAUTION:** TestConfiguration 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.
Signal Conditioning	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range.

Field	Description
	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. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.
H/W Options	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range. **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. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.
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. **Valid Entries** • 0 (one shot processing) • 0.05 to .95 in .05 increments (subsecond scan times) • 1 to 60 in 1 second increments

Field	Description
	• 1M to 60M in 1 minute increments • 1H to 24H in 1 hour increments **Example** 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	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. **Valid Entries** 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 Inputs

Field	Description
Low Limit	Lets you enter the tag's minimum value. **Valid Entries** • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999.

Field	Description
	• 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). **Note:** The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. 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. 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. If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
High Limit	Lets you enter the tag's maximum value. **Valid Entries** You can enter a high limit in one of three formats: • Standard Integer. • Expanded Decimal Notation, ranging from -9999999 to 9999999. • Scientific Notation, ranging from +/-3.4E-38 to +/-3.4E+38.

Field	Description
	• Standard integers range from -32768 to 32767 (signed integers), 0 to 65535 (unsigned integers), 0 to 999 (3BCD), or 0 to 4095 (12 Binary). 📝 **Note:** The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. 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. 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. If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
Units	Lets you enter text describing the engineering units range. **Valid Entries** Up to 33 characters. **Example** Kilograms per square meter, Liters per minute, degrees Celsius, 📝 **Note:** This entry does not affect the calculation or function of any variables in iFIX. It is

Field	Description
	📝 used strictly as a display label to identify the engineering units.
Scale Enabled	Lets you enable or disable scaling for this tag. Enabling scaling allows the system to convert the data received from input sensors to designated data ranges. 📝 **Note:** Linear scaling and signal conditioning cannot be applied simultaneously. If you select Linear Scaling, verify that Signal Conditioning is set to NONE. **Example** Scaling allows conversion of temperature data received in Fahrenheit to an output which uses Celsius values.
Input 1-6	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. **Valid Entries** 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.

Field	Description
	📝 Note: Input 1 is always the upstream tag, tied to the Signal Select tag through the upstream block's Next Block field.
Selection Mode	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: • 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. **Notes** • 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	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.

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**

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	Used with the collection interval to schedule collection of data from a tag. **Valid Entries** Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples** 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. 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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector. Select either Milliseconds or Seconds.
Collector Compression	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. Select Disabled to prevent the tag from being compressed.
Collector Deadband	Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values

Field	Description
	that fall within a deadband centered around the last reported value. Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage. Select Absolute to set the Collector Deadband value to an absolute value. 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)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver. After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred. The Collector Compression Timeout value should be in increments of your collection interval, and not less. **Valid Entries** Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature:

Field	Description
	• 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.
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. The Perform by Comments Required check box appears in every tag configuration where Electron-

Field	Description
	ic Signature settings are available. By default, this check box is disabled.

Advanced Options

Field	Description
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. ⏹ **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.
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 down-

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
	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. Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name: ~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries** 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.

Advanced Options

Field	Description
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.
Mode	Trigger on OPEN, CLOSE or COS. > ✎ **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 bewteen 0 and any non-zero value will trigger on COS. A change between two non-zero values will not trigger COS. As mentioned elsewhere this block is generally used with Digital Inputs.
Format	Allows a variety of date formats to allow for different country and/or relational database needs.
Separator	Allows a variety of date separators to allow for different country and/or relational database needs.

TM 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
	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.
	Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($).
	Invalid Entries
	You cannot use the following special characters in a tag name:
	~ ` + ^ : ? " * = { } . , ; ? @
	Examples
	AI1, CA_10, DI#, 4PID, 'TEST'

Field	Description
Description	Lets you enter optional descriptive text about the tag. **Valid Entries** 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.

Timer and Setup Options

Field	Description
Timing Direction	Lets you increment or decrement the Timer tag value. Up is the default direction.
Target Value	Lets you specify the value that triggers the following events when alarms are enabled: • Generates an alarm. • Closes the specified digital block, if the Alarm Tag field contains an entry. • Continues counting. **Note:** If alarms are disabled, the block continues counting when it reaches this value. **Valid Entries** The tag and field pair in tag.field format or a numeric value in the format ddd:hh:mm:ss, up

Field	Description
	to 365:23:59:59. The default target value is 365:00:00:00. 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.
Preset Value	Lets you specify an initial value for the tag. This field also controls the value of the tag when it resets. **Valid Entries** 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. > **Note:** > If you use a tag name (tag.field) in the Preset Value field, you must check the Clear on Startup check box.
Clear on Startup	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).

Field	Description
	• 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	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. **Valid Entries** Any of the following tag types: • Digital Alarm • Digital Input • Digital Output • Boolean ✏️ **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.
Hold Tag	Lets you specify an optional digital tag that temporarily suspends Timer tag counting when the

Field	Description
	hold tag's value changes from zero to one. When the value changes from one to zero, the tag resumes counting. **Valid Entries** A tag name with the F_CV field.

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 to show alarm conditions, and enabling other tags to detect alarms from the tag. **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.
Priority	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

Field	Description
	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. **Valid Entries** INFO, LOLO, LOW, MEDIUM, HIGH, HIHI, or CRITICAL 📝 **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.
Alarm Contact Mode	Lets you specify when to open the digital tag specified in the Alarm Contact field. Select one of the following options: • **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
	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. **Valid Entries** The name of a: - Digital Output tag - Digital Input tag - Digital Alarm tag (in manual mode) **Note:** Disabling alarms prevents this field from generating alarms.

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**

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	Used with the collection interval to schedule collection of data from a tag. **Valid Entries** Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples** 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. 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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector. Select either Milliseconds or Seconds.
Collector Compression	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. Select Disabled to prevent the tag from being compressed.
Collector Deadband	Lets you select if the tag is set for compression. Compression applies a smoothing filter to incoming data by ignoring incremental changes in values

Field	Description
	that fall within a deadband centered around the last reported value. Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage. Select Absolute to set the Collector Deadband value to an absolute value. 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)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver. After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred. The Collector Compression Timeout value should be in increments of your collection interval, and not less. **Valid Entries** Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature:

Field	Description
	• 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.
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. The Perform by Comments Required check box appears in every tag configuration where Electron-

Field	Description
	ic Signature settings are available. By default, this check box is disabled.

Advanced Options

Field	Description
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. > 📝 **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.
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 down-

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.
Next Blk Processing	Lets you specify when the Scan, Alarm, and Control (SAC) program processes the next tag in the chain. Select one of the following options: • **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	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** 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. Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name: ~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries**

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	Lets you enter the tag's minimum value. **Valid Entries** • 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). > **Note:** > The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information. In a Calculation or Signal Select tag, if the output of the tag is 10 and the Low Limit is 15, the block

Field	Description
	clamps the value at 15. You must enter a Low Limit of 10 or less to output a value of 10.
	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.
	If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
High Limit	Lets you enter the tag's maximum value.
	Valid Entries
	You can enter a high limit in one of three formats:
	• 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).
	📝 **Note:** The I/O driver can set certain limitations on the engineering units range. Consult your I/O driver manual for more information.
	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.

Field	Description
	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. If you are using scientific notation, up to six decimal places may be configured with precision, and the range may be positive or negative.
Units	Lets you enter text describing the engineering units range. **Valid Entries** Up to 33 characters. **Example** Kilograms per square meter, Liters per minute, degrees Celsius, > **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.
Buffer Clear Status	Lets you clear the block's data buffers every time the block is put on scan.
Input	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. **Valid Entries** A tag and field name pair in the tag.field (F_CV) format.

Field	Description
	Note: To chain Trend tag, enter a Trend block's name followed by the F_INP field.
Compression Factor	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. **Valid Entries** A value from 1 - 255. **Example** 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). **Note:** Using this field does not affect or delay the value passed by the Next Block field to the downstream block.

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
	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** Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples** 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. 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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector. Select either Milliseconds or Seconds.

Field	Description
Collector Compression	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. Select Disabled to prevent the tag from being compressed.
Collector Deadband	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. Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage. Select Absolute to set the Collector Deadband value to an absolute value. 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)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver. After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred. The Collector Compression Timeout value should be in increments of your collection interval, and not less.

Field	Description
	Valid Entries Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature: • 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.

Field	Description
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.
	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.

Advanced Options

Field	Description
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.
	Valid Entries
	One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default.
	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.
Previous Block	Displays the name of the previous (upstream) tag.
	Valid Entries

Field	Description
	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 down-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.

TT 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** 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. Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name: ~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries**

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	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.

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.

Field	Description
	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** Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples** 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. 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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector. Select either Milliseconds or Seconds.
Collector Compression	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.

Field	Description
	Select Disabled to prevent the tag from being compressed.
Collector Deadband	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.
	Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.
	Select Absolute to set the Collector Deadband value to an absolute value.
	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)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.
	After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.
	The Collector Compression Timeout value should be in increments of your collection interval, and not less.
	Valid Entries
	Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature: • 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.
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

Field	Description
	run mode. Comments in the Verify Comment section are optional. 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.

Advanced Options

Field	Description
Display Format	Lets you specify the number of decimal digits that appear to the right of the decimal point in an operator display. **Valid Entries** A value from 0 to 15, to indicate the digits of precision. > **Note:** > From a picture, the Display field can contain 15 characters total, consisting of numbers to the left and right of a decimal point.
Units	Lets you enter text describing the engineering units range. **Valid Entries** Up to 33 characters. **Example** Kilograms per square meter, Liters per minute, degrees Celsius,

Field	Description
	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.
Period	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. **Valid Entries** A time in the format HH:MM:SS. **Example** 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. 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): • #inputs/period = period/scan time • corrected total/period = raw total/# inputs

Field	Description
	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.
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. > ✏️ **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.
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 down-

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.

TX 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
	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. Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name: ~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries** 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	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. 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.
I/O Address	Lets you enter the location in the process hardware where data for this tag is saved and where output is sent. **Valid Entries** Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations. ⚠ **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. ⚠ **CAUTION:** TestConfiguration 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.

Field	Description
Signal Conditioning	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range. ✎ **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. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.
H/W Options	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range. ✎ **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. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.
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. **Valid Entries**

Field	Description
	• 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 **Example** 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	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. **Valid Entries** 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.

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
	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 to show alarm conditions, and enabling other tags to detect alarms from the tag. **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.
Enable Event	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. Analog Output, Analog Register, Digital Output, Digital Register, Digital Input, and Text tags have event messaging capabilities. **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

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	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
	Any numeric value that does not exceed the collection interval. The value is in seconds. **Examples** 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. 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	Lets you select the Time Resolution, or the level of precision for the timestamps for the GE Historian collector. Select either Milliseconds or Seconds.
Collector Compression	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. Select Disabled to prevent the tag from being compressed.
Collector Deadband	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. Select Disabled to prevent the tag from being compressed.
Compression Type	Lets you select if the deadband value entered in the Collector Deadband field is an absolute value or a percentage.

Field	Description
	Select Absolute to set the Collector Deadband value to an absolute value.
	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)	Indicates the maximum amount of time the collector will wait between sending samples for a tag to the archiver.
	After the timeout value is exceeded, the tag stores a value at the next scheduled collection interval, and not when the timeout occurred.
	The Collector Compression Timeout value should be in increments of your collection interval, and not less.
	Valid Entries
	Any numeric value.

E-Signature

Field	Description
Type	The Type of Electronic Signature: • 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	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. When an unsigned write is rejected, a message is sent indicating that the tag rejected an unsigned write. This is the default selection.
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. 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.

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
	mode, the tag receives data from the operator, scripts, recipes, or Program blocks.
Initial Scan	Lets you select whether the tag is initially placed on or off scan. 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.
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. > 📝 **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.
Message Length	Lets you specify the length of text that the tag reads and writes. **Valid Entries** 1 to 80 characters.

Field	Description
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.

TXR 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** Tag names must begin with a letter or number and can be up to 256 characters, including certain spe-

Field	Description
	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. Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($). **Invalid Entries** You cannot use the following special characters in a tag name: ~ ` + ^ : ? " * = { } . , ; ? @ **Examples** AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag. **Valid Entries** 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	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. 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.
I/O Address	Lets you enter the location in the process hardware where data for this tag is saved and where output is sent. **Valid Entries** Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations. ⚠️ **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. ⚠️ **CAUTION:** TestConfiguration 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.

Field	Description
H/W Options	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range. **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. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.
Signal Conditioning	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range. **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. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.
Message Length	Indicates the number of bytes to read from the poll table. Maximum value is 80. **Note:** Most GE drivers will only read or write an EVEN number of bytes and will round

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: • 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. The Perform by Comments Required check box appears in every tag configuration where Electron-

Field	Description
	ic Signature settings are available. By default, this check box is disabled.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources. 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.
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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. > 📝 **Note:** > Read access for database tags is available to all users regardless of security area. This allows users to retrieve data from a

Field	Description
	📝 specific security area even if they cannot write to that area.
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.

TXT 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
	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.
	Tag names can also include dashes (-), underscores (_), forward slashes (/), exclamation points (!), pipes (|), number signs (#), open brackets ([), close brackets (]), percent signs (%), and dollar signs ($).
	Invalid Entries
	You cannot use the following special characters in a tag name:
	~ ` + ^ : ? " * = { } . , ; ? @
	Examples
	AI1, CA_10, DI#, 4PID, 'TEST'
Description	Lets you enter optional descriptive text about the tag.
	Valid Entries
	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	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. 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.
I/O Address	Lets you enter the location in the process hardware where data for this tag is saved and where output is sent. **Valid Entries** Depends on your driver. Consult your I/O driver or server manual for details on the proper input/output addresses and configurations. ⚠️ **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. ⚠️ **CAUTION:** TestConfiguration 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.

Field	Description
Signal Conditioning	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range. **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. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.
H/W Options	Lets you select how to map the range of values coming from your process hardware into the tag's EGU range. **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. **Valid Entries** Depends on your driver or server. Refer to your driver or server manual for more information.

Limits and Scaling

Field	Description
Low 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 ta-

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
	• 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. 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.
Unsigned Writes	Select to allow this tag to accept or reject unsigned writes. Unsigned writes can originate from scripts, recipe downloads, and other data sources.

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	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. **Valid Entries** One security area name per field, ALL, or NONE (disables tag security). iFIX names security areas A-P by default. > ✏️ **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.

Field	Description
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.

Save and Publish

When configuring an iFIX node in TestConfiguration Hub, the common toolbar will contain two buttons at the top left named Publish and Save.
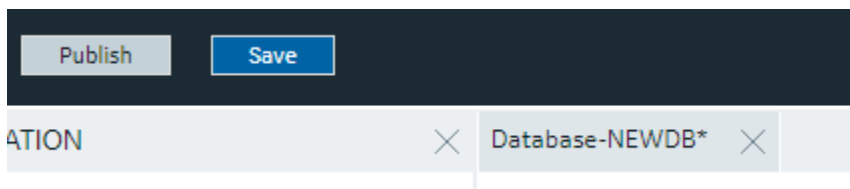
The Save button responds to certain panel actions that can queue up and will not be applied to the unpublished list until the Save is clicked. For example, any changes in the Database panel must be saved before they are applied. If you do not want to save changes you have made, close the panel and choose not to save. An asterisks (*) 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 TestConfiguration 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.
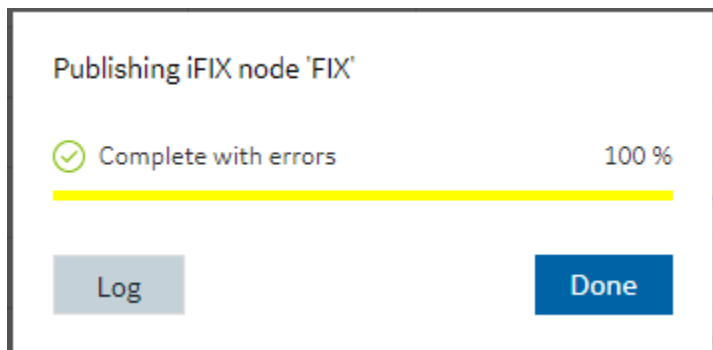
> **Note:**
>
> When Publishing, the Progress Bar does not update quickly and may take a while to complete. The Publish operation may take a while depending on the number of tags being published to the active iFIX node. Please wait for the Done indication.

You can discover unpublished changes in each panel via the status column in the panels 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.

Publish happens in three parts corresponding to the three panels you can open from the Navigation panel. Connectivity changes are published first, followed by Model changes, and finally Database changes. The log file reports the results in this order 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 in Configuration Hub

Overview

About Historian in Configuration Hub

The Configuration Hub application allows you to manage the Historian models, Historian systems, and their components.
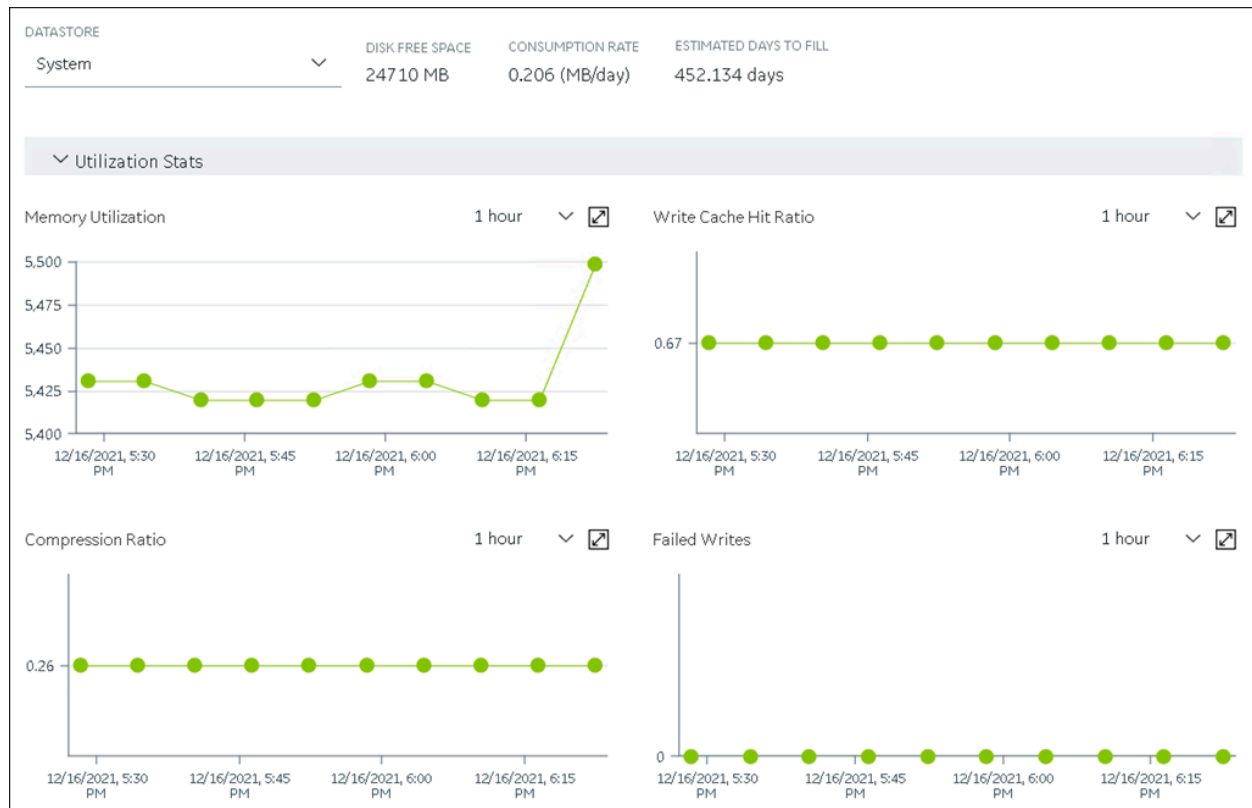
Advantages of Using Configuration Hub:

- **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 773)*.
- **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 for Historian *(on page 777)*.

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.
- Using Configuration Hub, you cannot create enumerated sets and user-defined types (UDT) for tags. You can, however, use the ones created in Historian Administrator.

- Using Configuration Hub, you cannot define a calculation formula for a tag for a Calculation collector. You can, however, define a calculation formula using Historian Administrator or other Web-based Clients.
- Using Configuration Hub, you cannot configure an iFIX Alarms and Events collector and an OPC Classic Alarms and Events collector. However, you can configure them using Historian Administrator.
- Using Configuration Hub, you cannot configure a HAB collector. You can, however, configure it using XML files.
- When browsing for tags hierarchically, if a folder contains subfolders, the tags in the parent folder do not appear. You can, however, access these tags using Historian Administrator.

Configuration Hub Workflow

This topic provides the high-level steps in using Configuration Hub.

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 773)* or a horizontally scalable system *(on page 777)*. 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 783)*.
5. As needed, create an object model *(on page 787)*.
6. Specify the tags for data collection *(on page 775)*.

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 for Historian

To set up Configuration Hub, you must perform the following steps:

1. Install the Historian server *(on page 742)*.
   - 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 747)*.
3. Install collectors *(on page 760)*.
4. Perform the post-installation tasks *(on page 763)*.

If you want to upgrade Configuration Hub, refer to Upgrade Configuration Hub for Historian *(on page 765)*.

After you install or upgrade the required components, you can access Configuration Hub *(on page 765)*.

Install the Historian Server Using the Installer

- Set up the Historian environment and login using an account with administrator rights.
- 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.
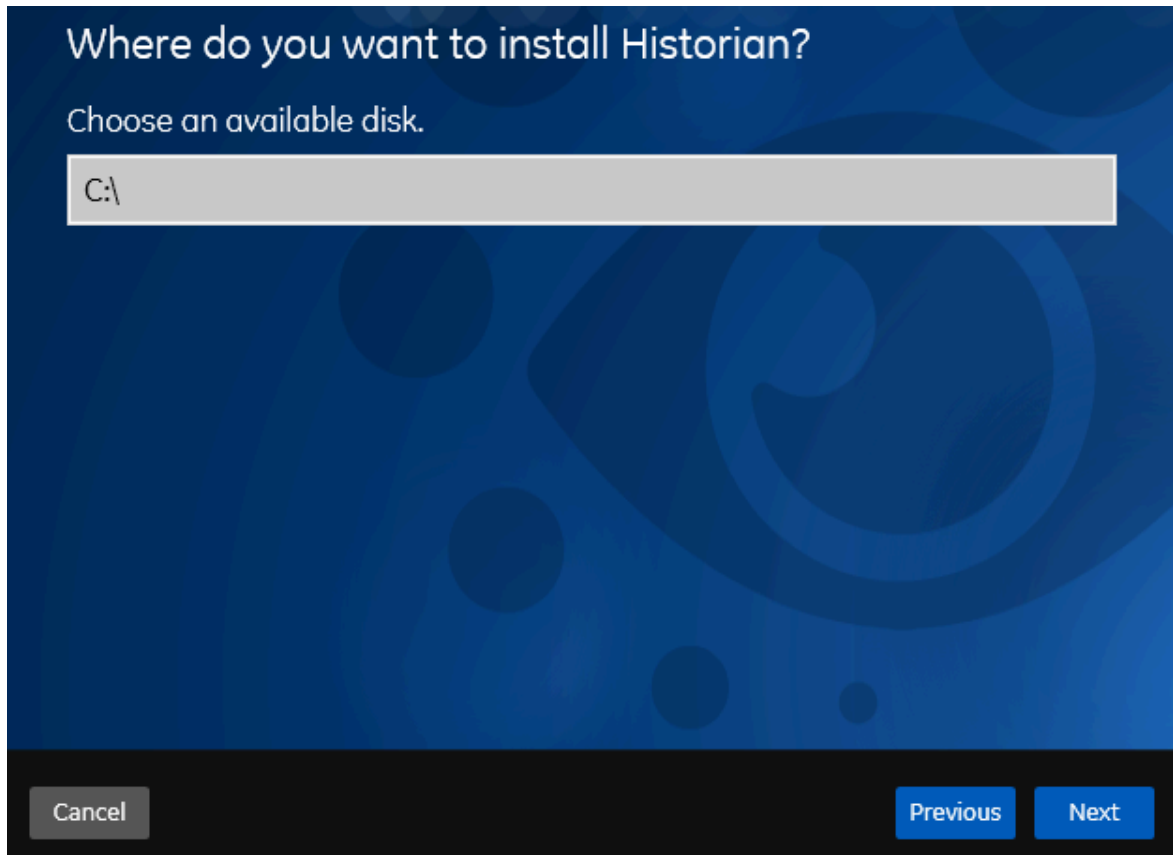
6. If needed, change the default installation drive of the Historian server, and then select **Next**.

The **Override the default Historian data Path?** page appears.
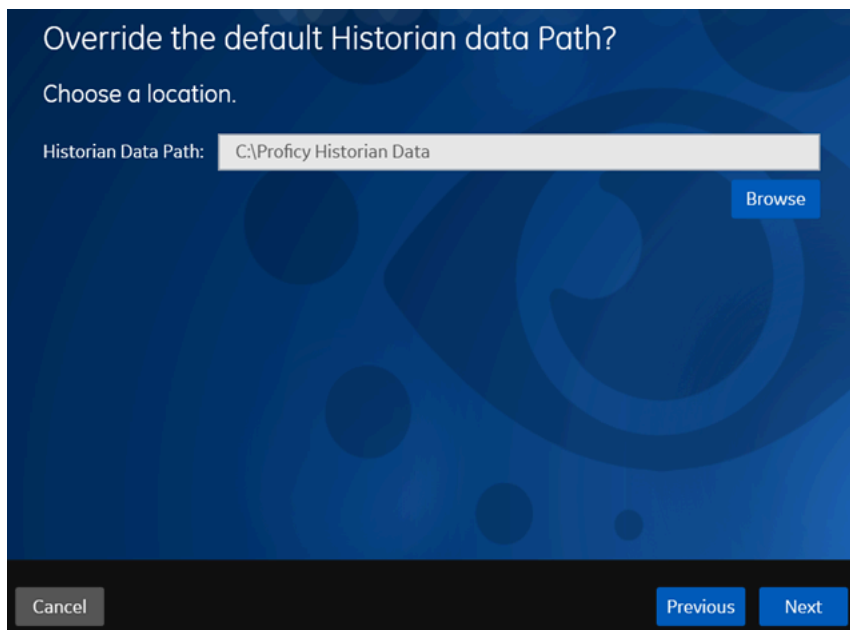
7. If needed, change the default folder of the log files, and then select **Next**. If you want to include the Historian server in a cluster, enter the path to the shared folder of the cluster.
   The **Proficy Authentication Service** page appears.

   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.
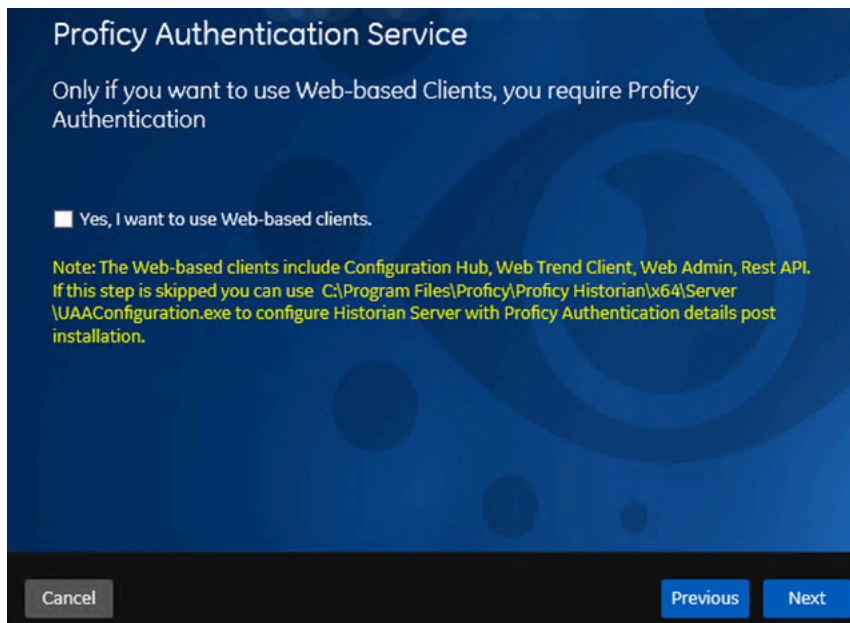
8. If you want to use Web-based Clients, select the **Yes, I want to use Web-based Clients** check box, and provide values as described in the following table.

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.
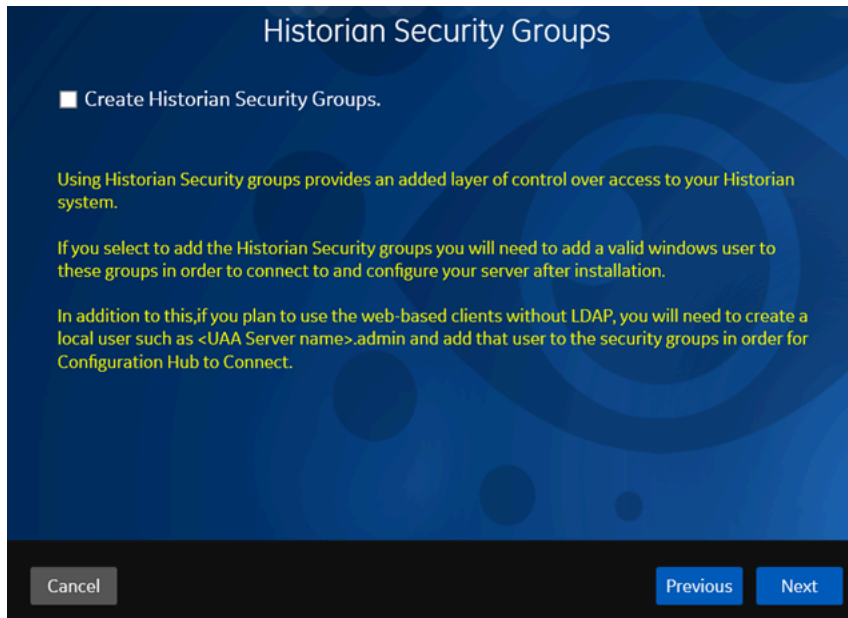
10. If you want the installer to create Historian security groups, select the corresponding check box, and then select **Next**.

The **Choose the type of install you want to perform** page appears.
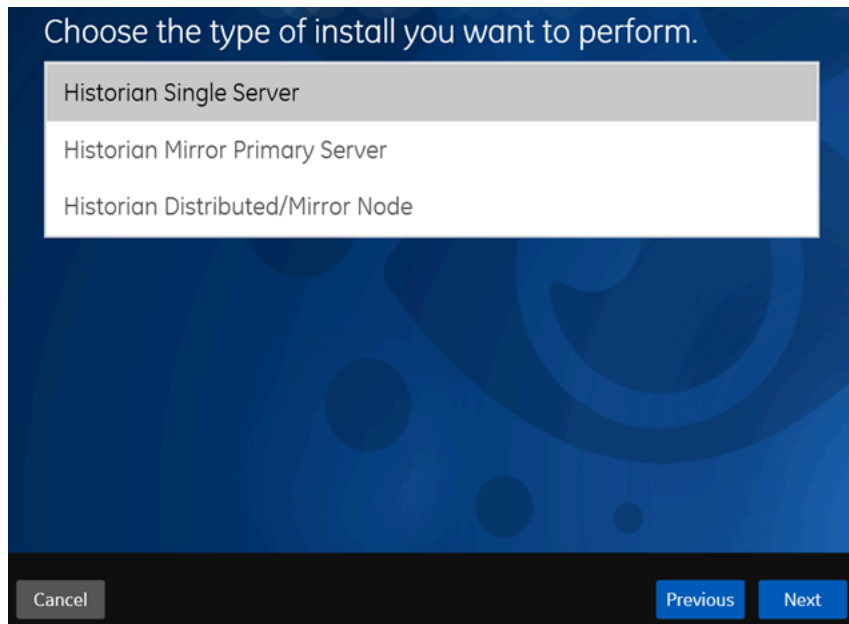
11. Select the type of the Historian server that you want to install, and then select **Next**.
    - **Historian Single Server**: This is for a stand-alone Historian system, which contains only one Historian server. This type of system is suitable for a small-scale Historian setup.
    - **Historian 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.

◦ **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.

Install Web-Based Clients Using the Installer

1. Install the Historian server *(on page 742)*. 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.
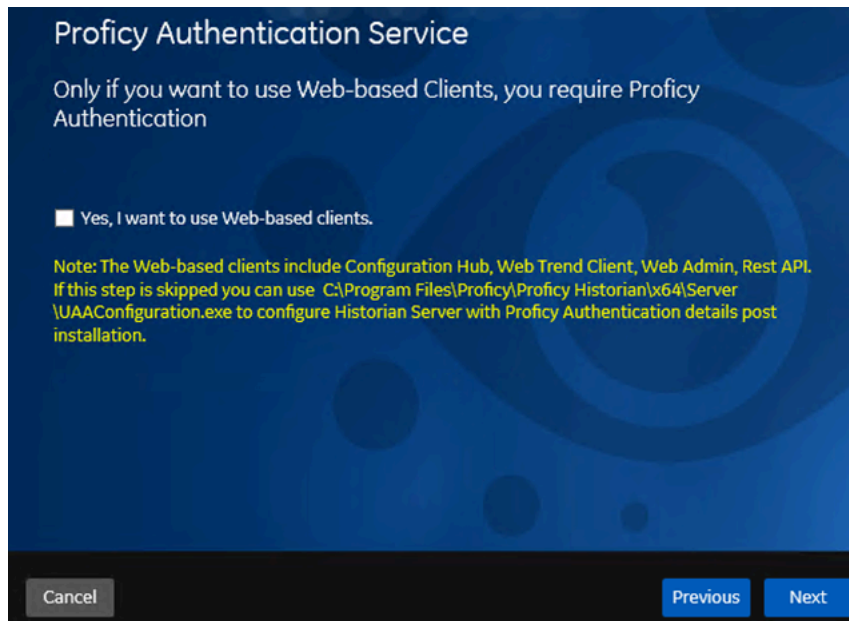
2. If you want to use Web-based Clients in a cluster environment, ensure that your network is enabled for multicast traffic, and set up high availability on each node in the cluster.

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.
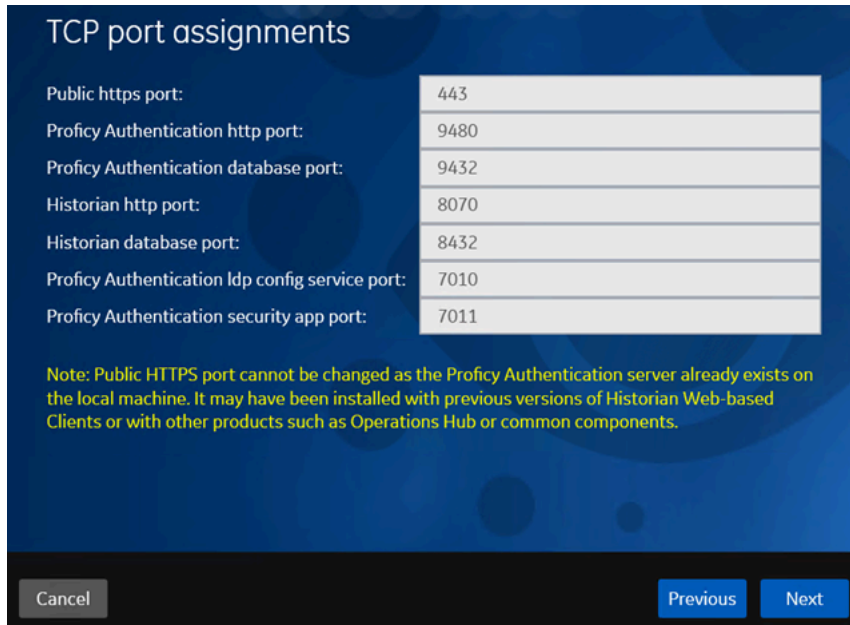
5. As needed, change the values for TCP port assignments as described in the following table, and then select **Next**.

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: ◦ 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.

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:// 127.0.0.1 /historian-visualization/hwa
   - https:// aliasName /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.
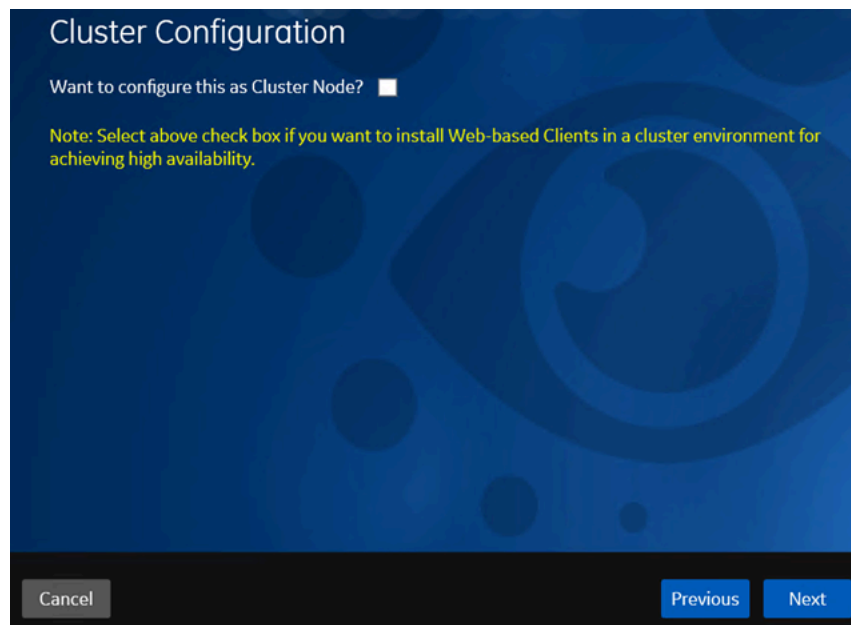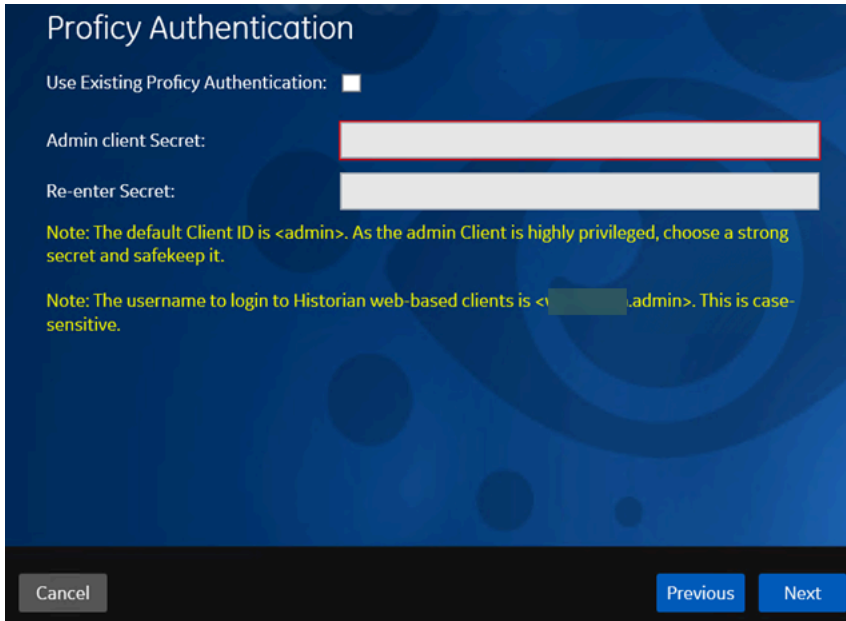
If, however, you are upgrading Web-based Clients, this page does not appear. In that case, skip the next step.

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 *must* 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	Enter the URL of the external Proficy Authentication server in the following format: https://*<Proficy Authentication server name>*:*<port number>*, where *<Proficy Authentication server name>* is the FQDN or hostname of the machine on which Proficy Authentication is installed. By default, the port number is 443. > **Note:** > Do not enter a trailing slash character.
Admin Client ID	Enter the client name that you provided while installing the external Proficy Authentication. The default value is admin.

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 739)*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. > **⚠ Important:** > You can install Configuration Hub only in the C drive. If, however, you want to install it in a different drive: > a. Create Configuration Hub server certificates. > b. Start the ConfigHubNGINXService service. > c. Using the Web Based Clients Configuration tool *(on page 772)*the Web Based Clients Configuration tool, provide the Proficy Authentication and Configuration Hub details, test the connection, and select **Register** to re-register the Historian plugin with Configuration Hub.
Plugin Name	If needed, modify the name of the Configuration Hub plugin for Historian. The default value is in

Field	Description
	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: ◦ All English alphanumeric characters (ABCDEFGHIJKLMNOPQRSTUVXYZ abcdefghijklmnopqrstuvwxyz_-0123456789) ◦ The following special characters: ><:~!@#$%^&*?|
Client Secret	Enter the password to connect to Configuration Hub. The value that you enter can contain: ◦ Must contain at least eight characters. ◦ All English alphanumeric characters (ABCDEFGHIJKLMNOPQRSTUVXYZ abcdefghijklmnopqrstuvwxyz_-0123456789) ◦ The following special characters: ><:~!@#$%^&*?|
Re-enter Secret	Re-enter the password to connect to Configuration Hub.

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.

   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.

Field	Description
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.
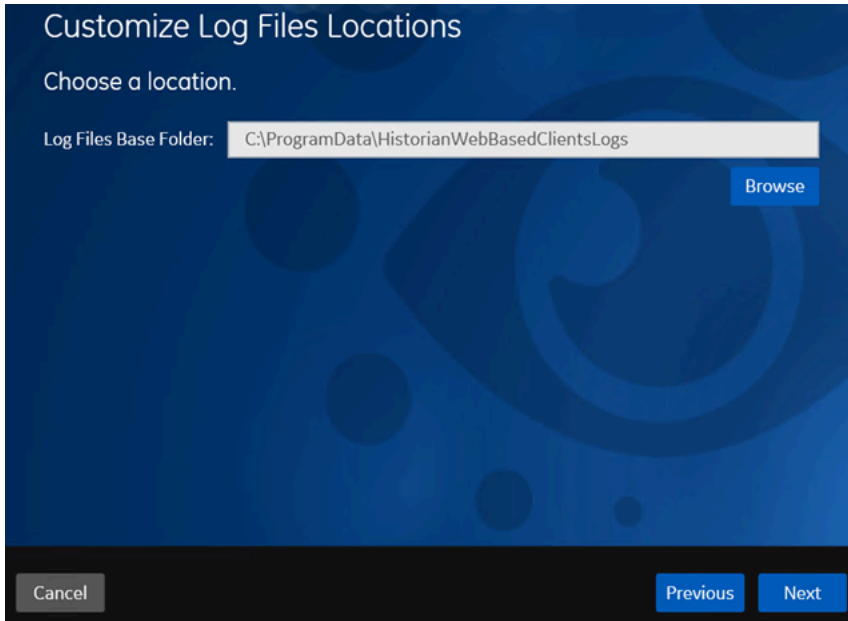
14. Select **Next**.

    The default installation drive appears.
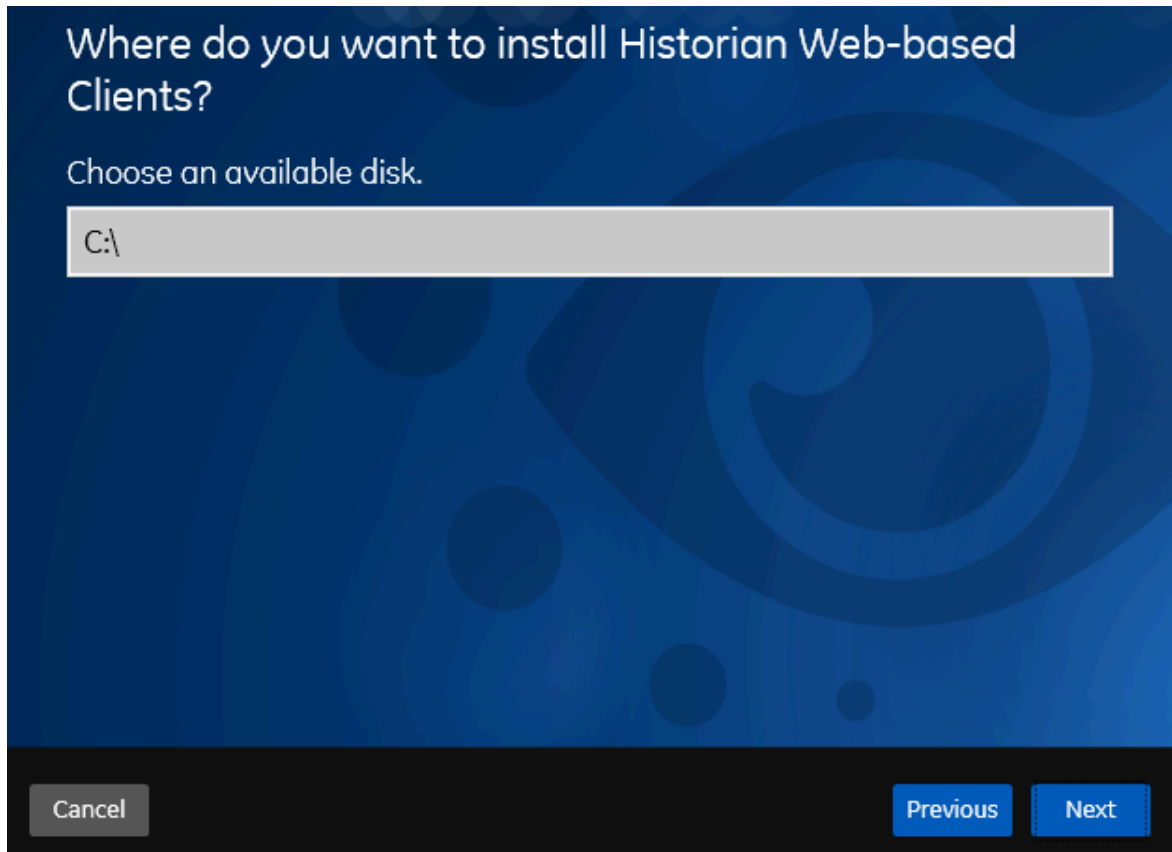
15. If needed, change the installation drive for Web-based Clients, and then select **Next**.

    The log files location page appears.
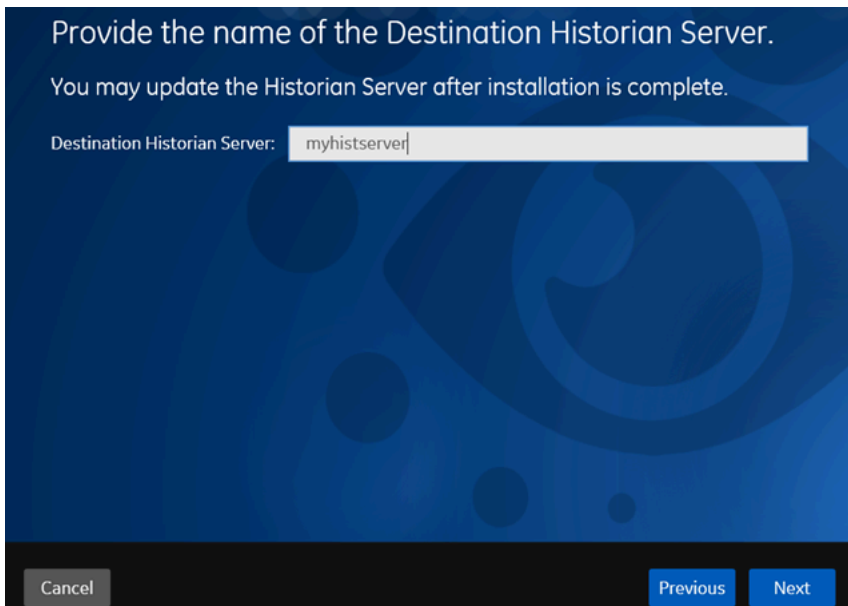
16. If needed, change the location for log files, and then select **Next**.

    The destination Historian server page appears.

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
  remotelymanage collectors remotely.

This topic describes how to install collectors using an installer. 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.
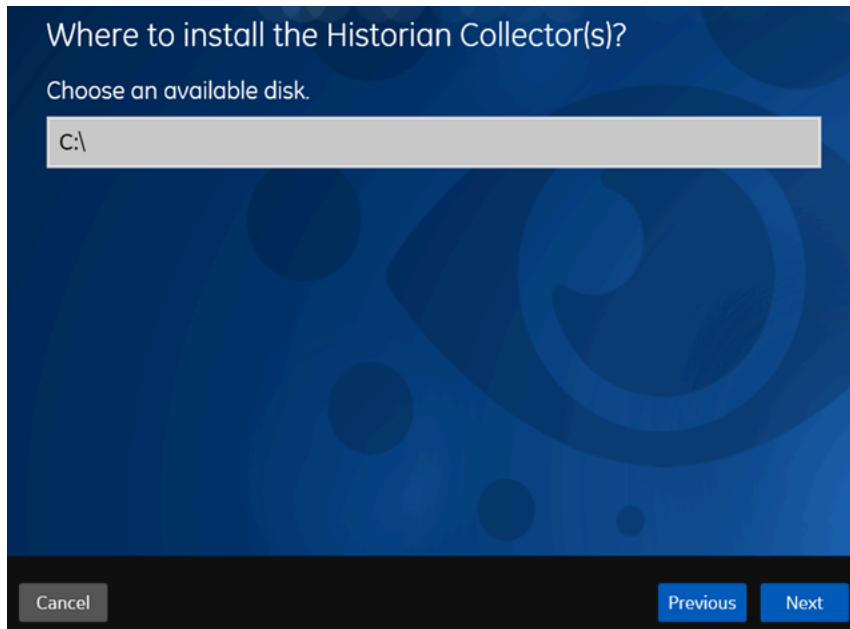
5. If needed, modify the installation drive, and then select **Next**.

   The data directory page appears.
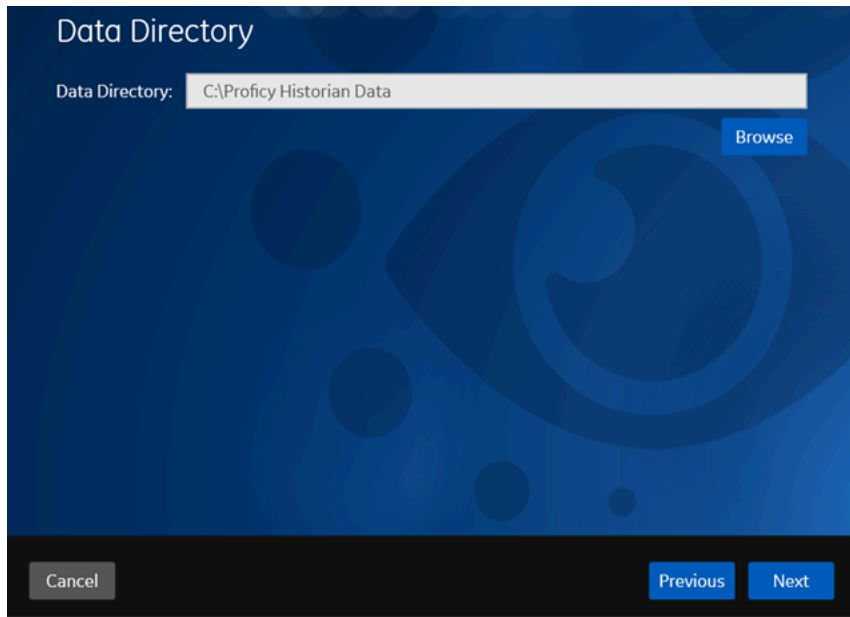
6. If needed, change the folder for storing the collector log files, and then select **Next**.

   The destination Historian server page appears.
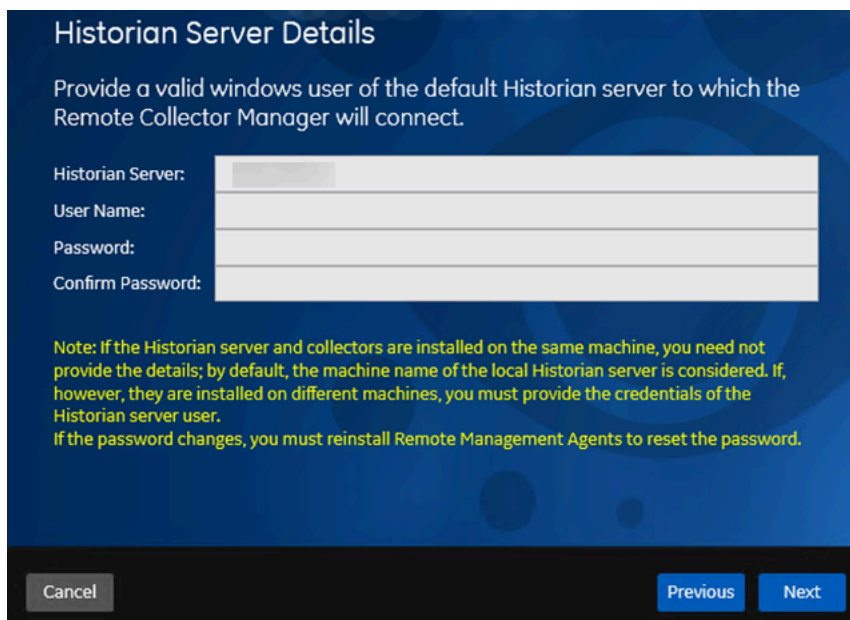
7. Provide the credentials of the Windows user account of the destination Historian server to which you want Remote Management Agent to connect.

   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 name>`
- `HKEY_LOCAL_MACHINE\SOFTWARE\GE Digital\iHistorian\Services\<collector name>`

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 Install Tasks

Overview of 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 *(on page 764)*. 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.

Depending on whether the Historian server will use local or domain security groups, select the appropriate option in the 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 *(on page 772)*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 765)*.

Adding Users to Windows Security Group

Add your users to the Windows system.

1. Open the **Control Panel**.
2. Double-click the **Administrative Tools**.
3. Double-click the **Computer Management** icon.
   The **Computer Management** console opens.
4. Select **Groups** from the **Local Users and Groups** folder in the system tree.
5. Select the group to which you want to add users.
6. From the **Action** menu, select **Properties**.
   The **Users Properties** window appears.
7. Select **Add**.
8. Select the users or groups to add from the listed users or enter the names of the users or groups you want to add in the bottom field.
9. Select **Add**.

> ✎ **Note:**
> To validate the user or group names that you are adding, select **Check Names**.

10. When you have added all users to the group, select **OK**.

About Proficy Authentication Groups

A Proficy Authentication group is created for a specific type of users who will likely perform the same type of activities.

If you have groups in a remote Proficy Authentication service, you can use them with Historian using the Proficy Authentication LDAP Integration tool. This section describes how to map the groups in the remote Proficy Authentication service with Historian counterparts. By default, Historian contains the following Proficy Authentication groups:

- **historian_visualization.admin:** Provides access to Trend Client and the Web Admin console.
- **historian_visualization.user:** Allows access to Trend Client.
- **historian_rest_api.read:** Provides read access to public REST API.
- **historian_rest_api.write:** Provides write access to public REST API.
- **historian_rest_api.admin:** Provides read/write access to public REST API.
- **historian_enterprise.admin:** Provides read/write access to Configuration Hub APIs.

> **Note:**
> Instead of mapping the groups, you can choose to map individual users with Historian users.

Workflow

1. Provide the details of the remote Proficy Authentication service while installing Web-based Clients.
2. Connect to the remote Proficy Authentication service.
3. Map the Proficy Authentication groups with that of the Historian Proficy Authentication instance. You can map the groups in LDAP and LDAPS (LDAP via SSL) as well.

Upgrade Configuration Hub for Historian

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 741)*.

Access Historian in Configuration Hub

Perform the tasks outlined in About Setting up Configuration Hub for Historian *(on page 741)*.

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/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.
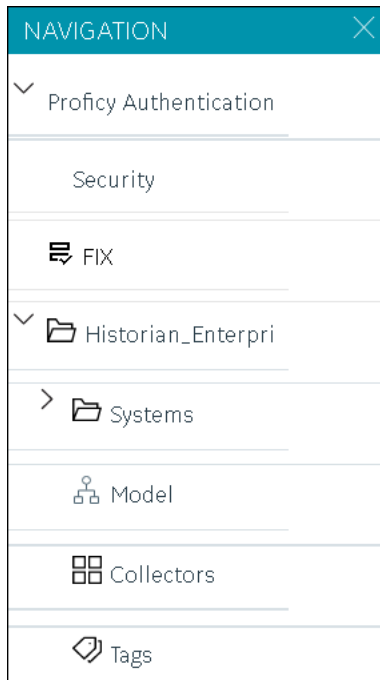
◦ **The main section:** Displays content based on your selection in the **NAVIGATION** section. For example,if you select a Historian system, you can access a list of servers in the system. You can also navigate to the system statistics as shown in the following image.
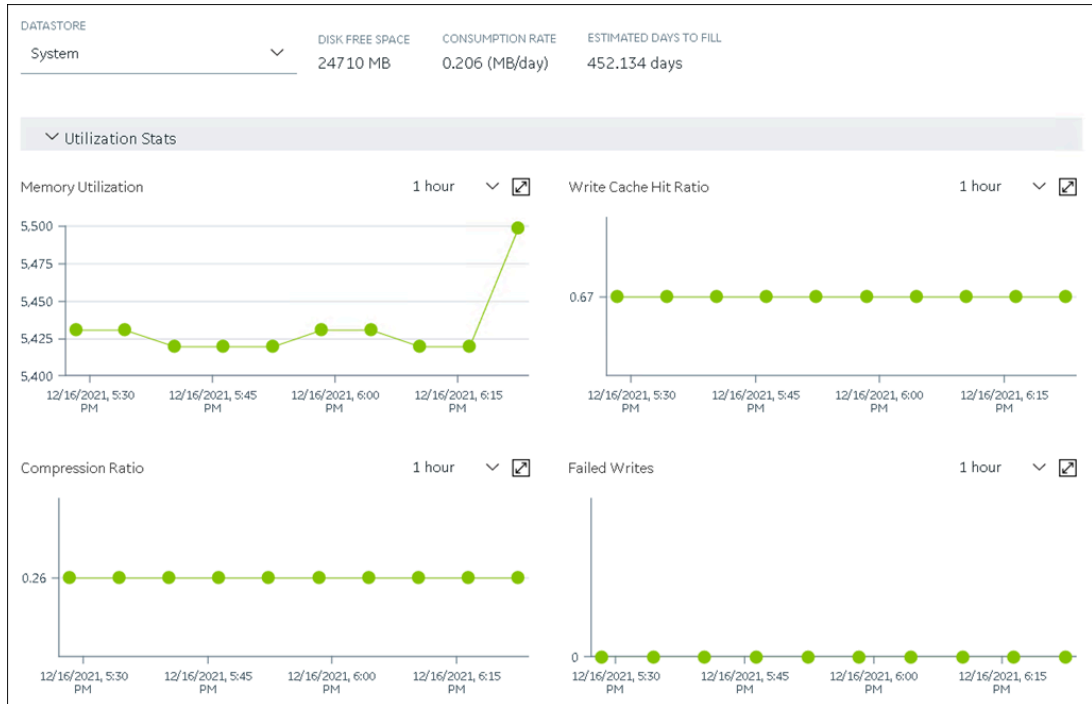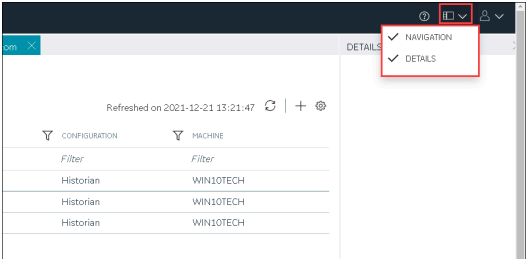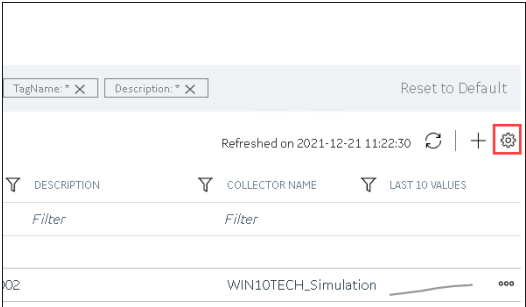
Similarly, if you select **Model** in the **NAVIGATION** section, you can access the Historian model.
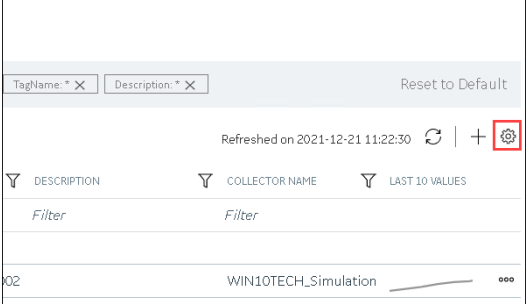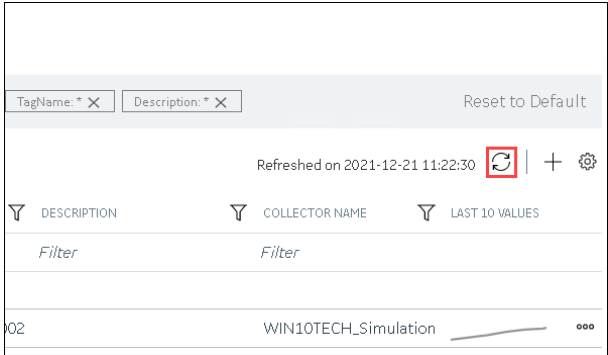
◦ **The Details section:** Contains the details of the item selected in the main section. For example, If you select a system, you can view the description of the system, and add data stores and mirror locations using the **Details** section.

Depending on your requirements, set up a stand-alone system or a horizontally scalable system.

Common Tasks in Configuration Hub

Task	Procedure
Show or hide the **Navigation** or the **Details** section.	1. In the upper-right corner of the page, select ![icon]. 2. Select the check boxes for the sections that you want to show.
Show or hide columns in a table. ✏️ **Note:** You cannot hide some of the columns (for example, the **COLLECTOR NAME** column).	1. In the upper-right corner of the table, select ⚙.

Task	Procedure
	The **Table Settings** window appears. 2. Select the check boxes in the **SHOW COL-UMN** column, and then select **Apply**.
Reorder columns in a table. **Note:** You cannot reorder some of the columns.	1. In the upper-right corner of the table, select . The **Table Settings** window appears. 2. Use the arrow buttons in the **RE-ORDER** column, and then select **Apply**.
Refresh a page/table.	In the upper-right corner of the main section or a table, select .

Work with Certificates

Enable Trust for Proficy Historian for a Self-signed Certificate

During Historian installation, a self-signed certificate is generated that you 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. This topic describes how to ensure that Google Chrome trusts the self-signed certificate.

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 **Certification Path**, select the root certificate, and then select **View Certificate**.
   The **Certificate** window appears, displaying the **General**, **Details**, and **Certification Path** sections.
4. 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 **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.
8. Restart the browser, and connect to the server.
9. Open the URL authenticated by the certificate.
   If error messages do not appear, the certificate is successfully imported.

Configure Web-based Clients

You can configure the following settings for Web-based Clients:

- Reconfigure Proficy Authentication to point to a different Proficy Authentication server.
- Reconfigure the same Proficy Authentication instance to resolve any issues with login.

- Re-register Configuration Hub to resolve any issues.
- Unregister Configuration Hub, and register another one.

To perform these tasks, Historian provides a utility called Web Based Clients Configuration. It is installed during Web-based Clients installation.

To run this utility, run the `Web_Clients_Configuration_Tool.exe` file. By default, it is located in the following folder: `C:\Program Files\GE Digital\Historian Config`

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 741)*.

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 the Historian documentation.

- **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 774)* 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 775)* 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 845)*
- The CygNet collector *(on page 848)*
- The File collector *(on page 852)*

Specify Tags for Data Collection

- Add the collector instance *(on page 774)* 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 786)*.

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 983)*.

1. Access Historian in Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, select **Tags**.
3. In the upper-right corner of the main section, select ╋.

The **<system name> - Add Tag** section 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.

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 in the Historian documentation.

Setting up a Horizontally Scalable System

About Setting up a Horizontally Scalable System for Historian

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 741)*.

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 the Historian documentation.

- **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 783)*.

        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 783)*.

- **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 774)* 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 775)* 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 742)* on the machine that you want to add as a distributed server.
2. Add a system *(on page 832)*. 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 Historian in Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, 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 ＋.

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 784)*, and then add the data stores *(on page 786)*. If not, add the data store *(on page 786)* 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 845)*
- The CygNet collector *(on page 848)*
- The File collector *(on page 852)*
- The HAB collector *(on page 855)*
- The iFIX collector *(on page 862)*
- The MQTT collector *(on page 866)*
- The ODBC collector *(on page 869)*
- The OPC Classic Alarms and Events collector *(on page 873)*
- The OPC Classic DA collector *(on page 876)*
- The OPC Classic HDA collector *(on page 881)*
- The OPC UA DA collector *(on page 885)*
- The OSI PI collector *(on page 888)*

- The OSI PI distributor *(on page 892)*
- The Server-to-Server collector *(on page 896)*
- The Server-to-Server distributor *(on page 899)*
- The Simulation collector *(on page 903)*
- The Windows Performance collector *(on page 905)*
- The Wonderware collector *(on page 908)*

Specify Tags for Data Collection

- Add the collector instance *(on page 774)* 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 786)*.

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 983)*.

1. Access Historian in Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, select **Tags**.
3. In the upper-right corner of the main section, select ╬ .

The **<system name> - Add Tag** section 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.

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 in the Historian documentation.

Setting up High Availability for Historian

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

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 765)*.
2. In the **NAVIGATION** section, 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 can 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 786)*.

Add a Data Store

If you want to add a data store to a distributed server, add the distributed server *(on page 779)* to the system. If you want high availability of the data store, add a mirror location *(on page 786)* to the system.

1. Access Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, select **Systems**.

   The **Systems** section appears, displaying a list of systems.
3. Right-click the system to which you want to add a data store (or select [⠿]), and then select **Browse Locations**.

A list of distributed locations in the system appears.

4. Right-click the location in which you want to add a data store (or select), and then select **Add Data Store**.

   The **Add Data Store: <location name>** window appears.

5. Provide values as described in the following table.

Field	Description
DATA STORE NAME	Enter a name for the data store. A value is required and must be unique for the system.
Description	Enter a description for the data store.
Set as default data store for the System	Select the check box if you want to set the data store as default. When you do so, while creating a tag, this data store will be used by default.

6. Select **Add**.

   The data store is added to the location.

Specify the tags whose data you want to store in the data store.

Creating a Model with Historian

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).
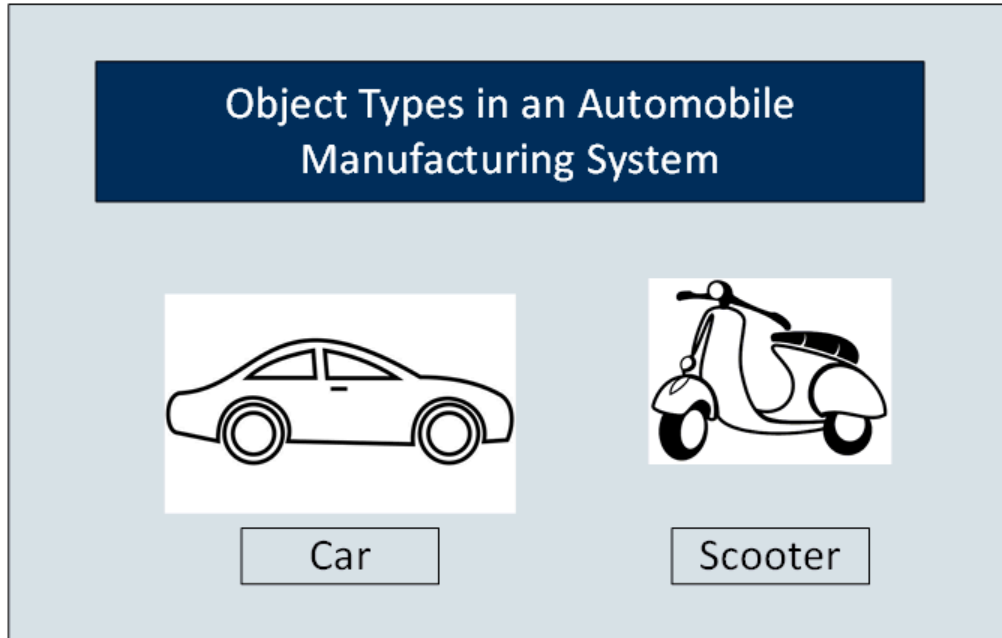
Contained Types: A contained type is an object type that you can include in another object type. For example, suppose you manufacture cars with the following types of engines:

- 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.
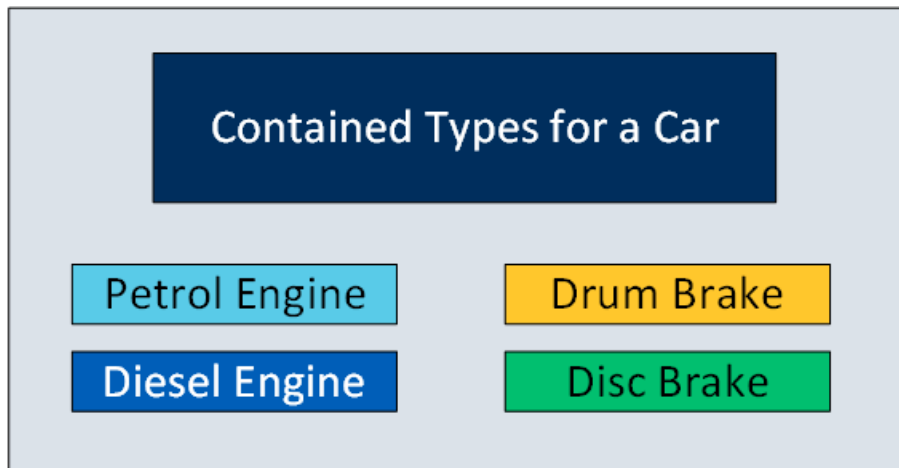
When you create an object type for a car, you can include any of these contained types.
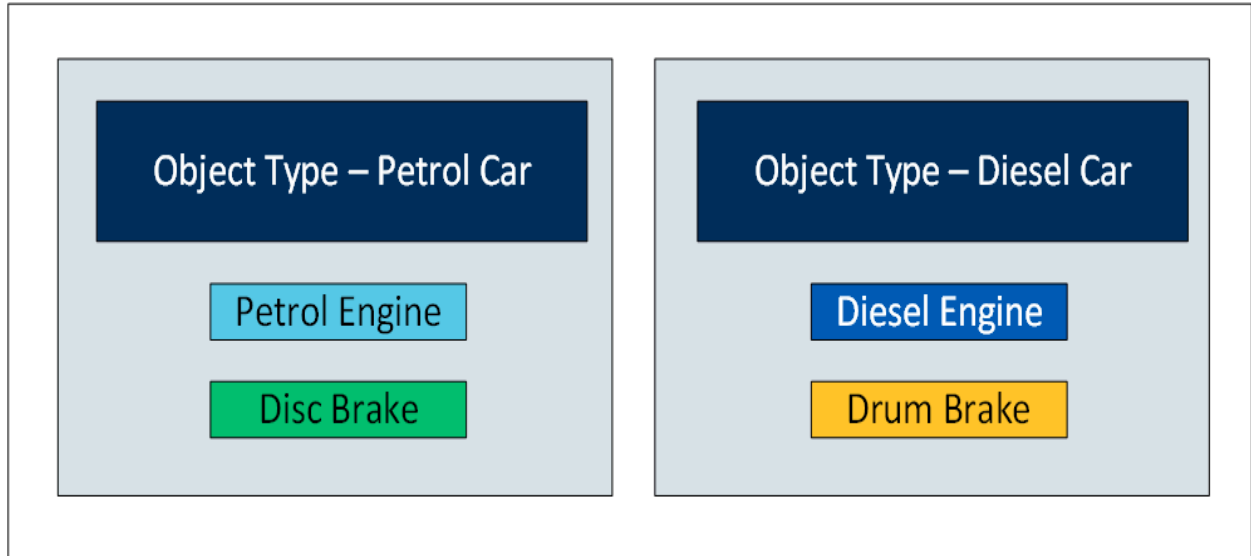
You can include multiple contained types in a single object instance. In addition, you can include a single contained type in multiple object instances.

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.
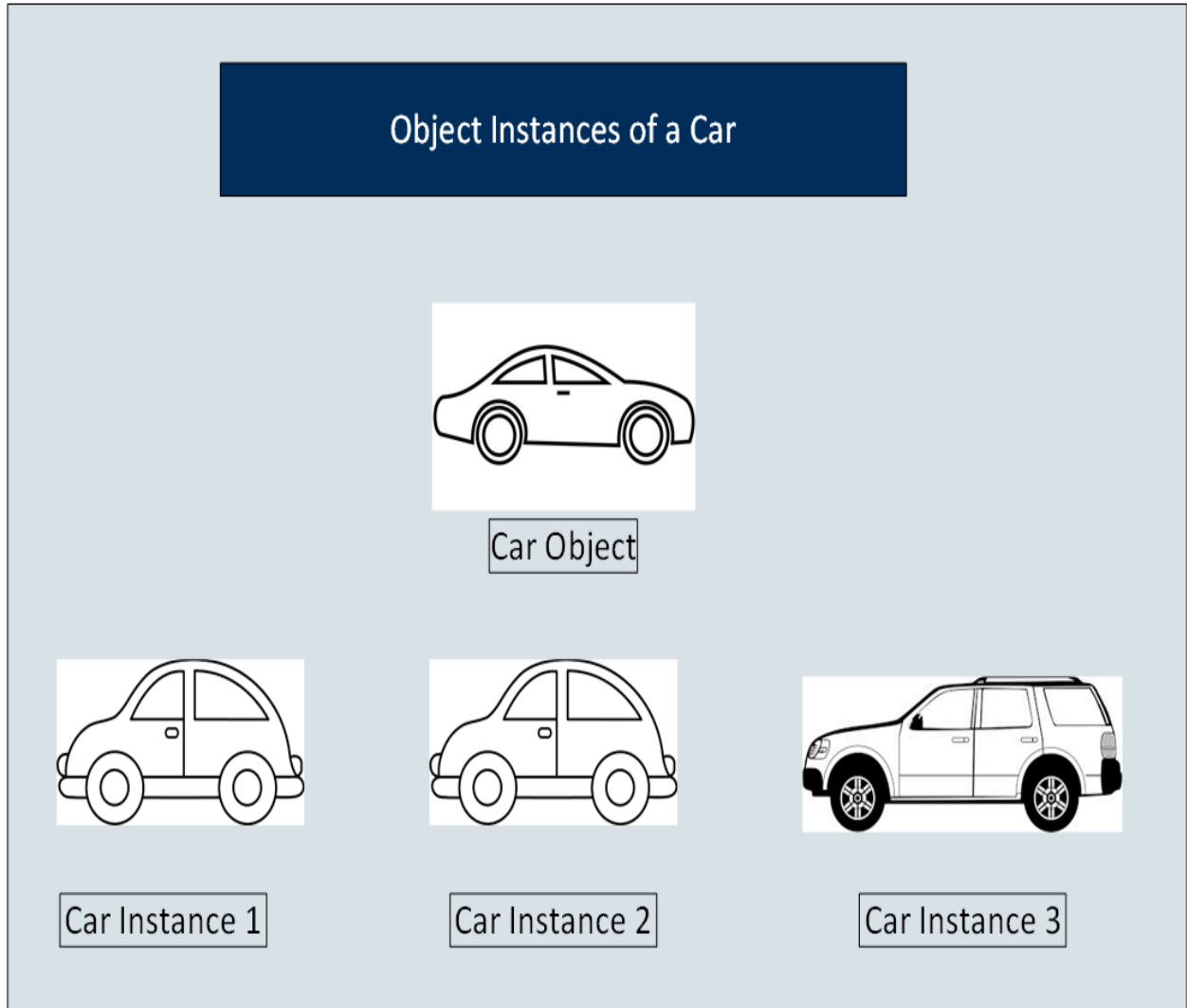
An object instance is specific to a Historian system. An object type, however, is not associated with a system.

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.
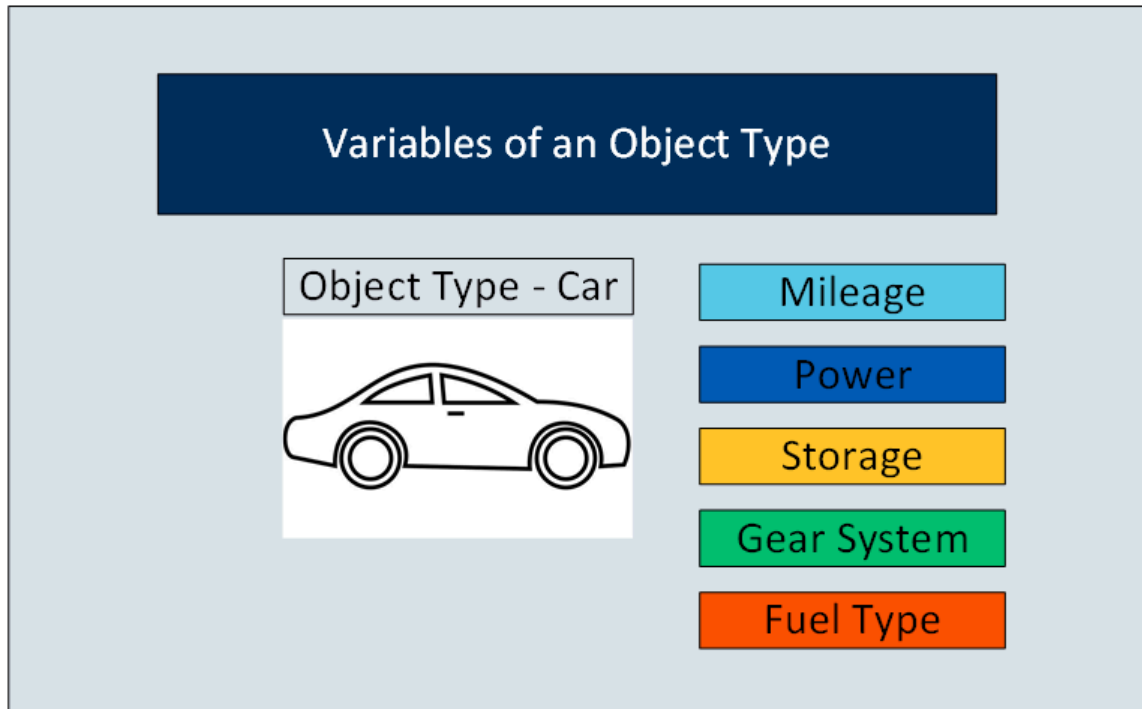
When you create instances of an object type, by default, the variables in the object type are inherited to all the instance as well. You can choose to include or exclude one or more of these variables for each instance.

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.
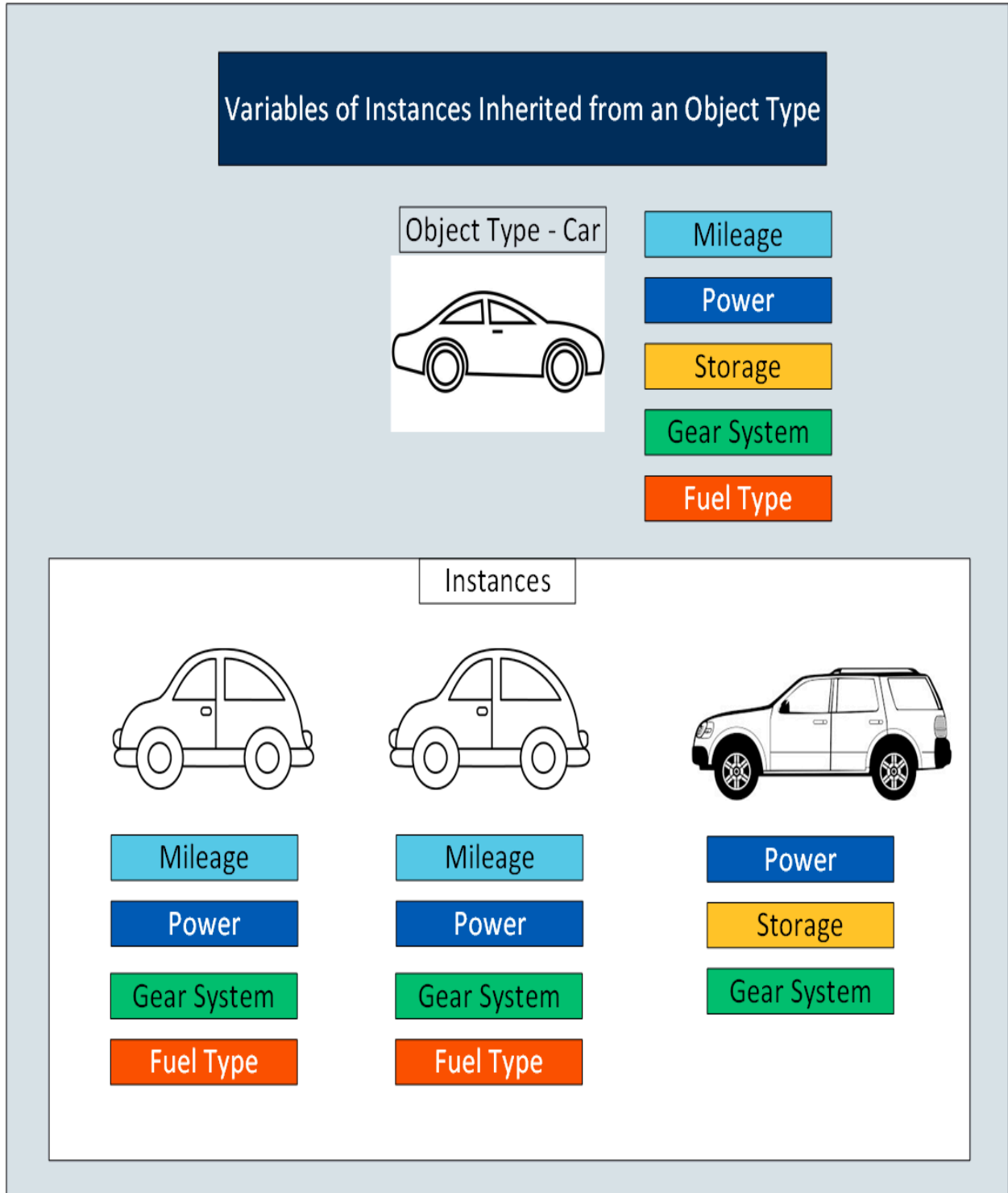
If an object type contains contained types, the variables in the contained types are inherited as well.

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 809)*.
- **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 812)*.
- **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 807)*.

Limitations:

- An OPC UA model is not supported.
- If using an iFIX model on the same machine, you cannot use a Historian model.
- 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.
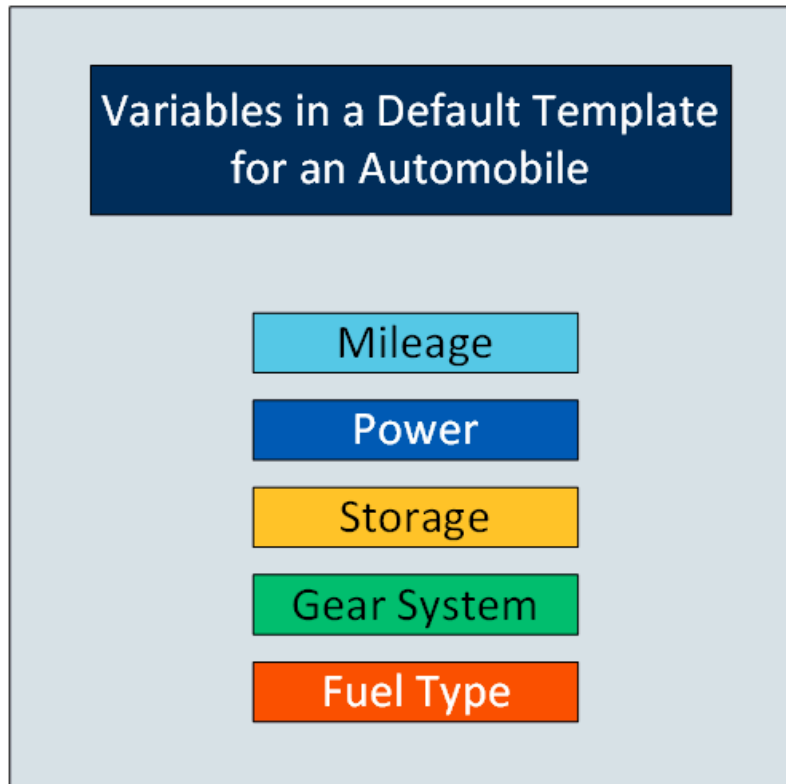
In addition to the default template, you can create custom templates for the object type, and add variables to it. For example, in the automobile object type, you can create a template for a car and another one for a scooter. Some of the variables in the default template (such as storage and gear system) may not be applicable to a scooter. Therefore, you can exclude them.
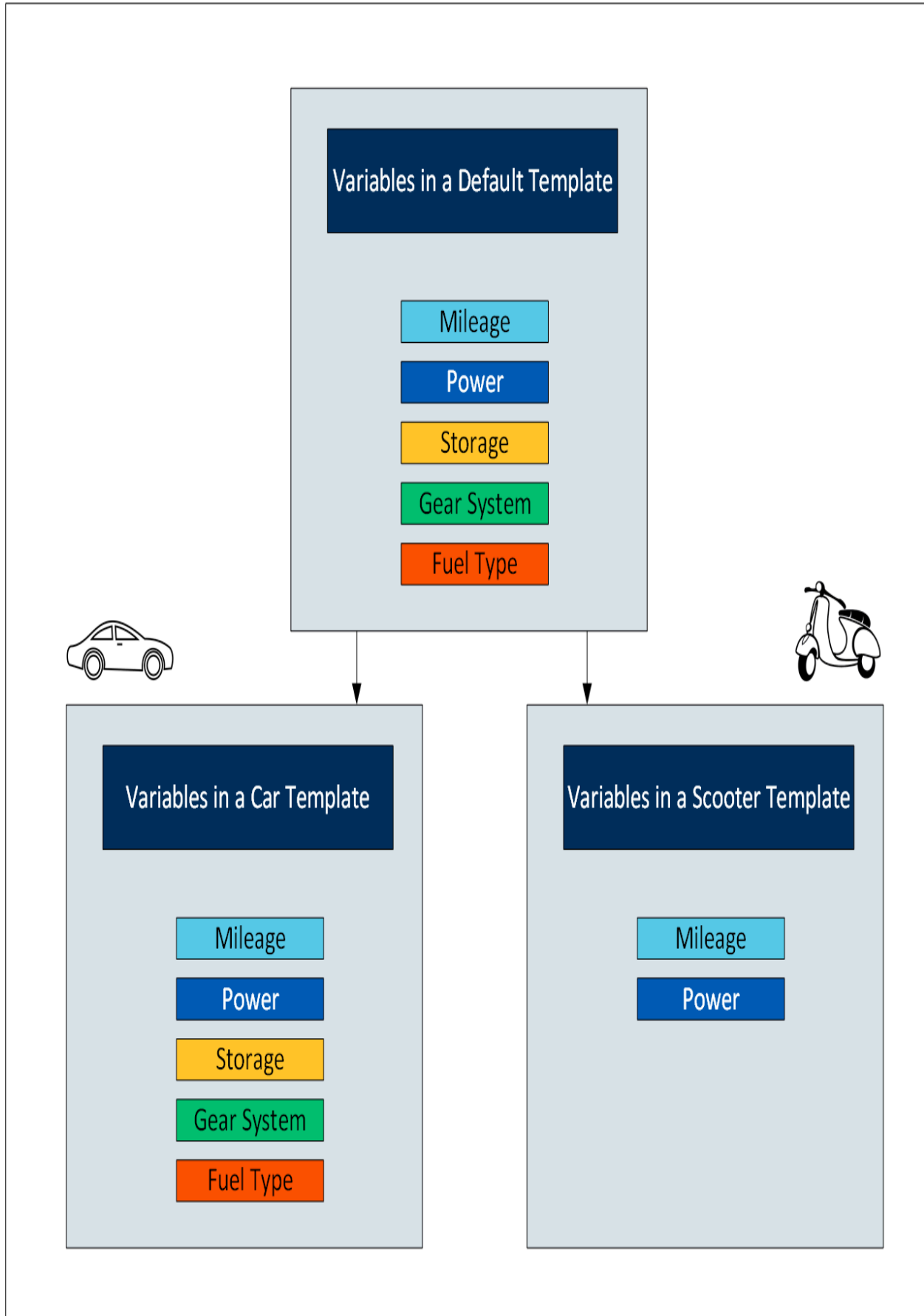
When you later create instances of the object type, you can choose any of the three templates. When you do so, all the variables in the template are included in the object instance. You will then capture values of these variables in Historian.

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 741)*.	This step is required. It involves installing the required components to get started with Configuration Hub.
2	Create a collector instance *(on page 774)*.	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 775)*.	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 797)*.	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 805)*.	This step is required. It involves creating an object instance and applying the required

Step Number	Description	Notes
		template from the object type. The object instance then inherits the variables from the object type.
6	Provide/collect data for static *(on page 807)*, direct *(on page 809)*, and indirect *(on page 812)* variables.	This step is required. You can provide data for the following types of variables: • **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 *existing* Historian tag. The values for the variable are then collected by the collector instance and stored in Historian. For more information on the types of variables, refer to About a Historian Model *(on page 787)*.

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 793)* and About a Historian Model *(on page 787)*.

This topic describes how to create an object type. You can also copy one *(on page 817)*.

1. Access Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, 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 $+$.
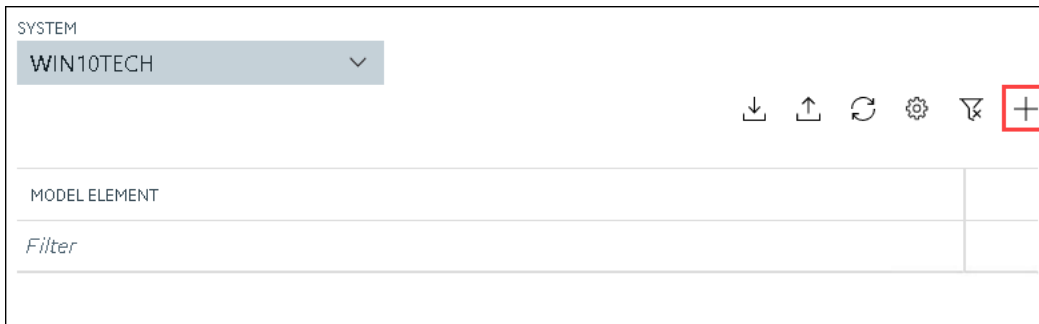
   The **New Object Type** window appears.
4. Enter values as described in the following table.

Field	Description
NAME	Enter a name for the object type. A value is required and must be unique.
	The value that you enter:
	◦ 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**.
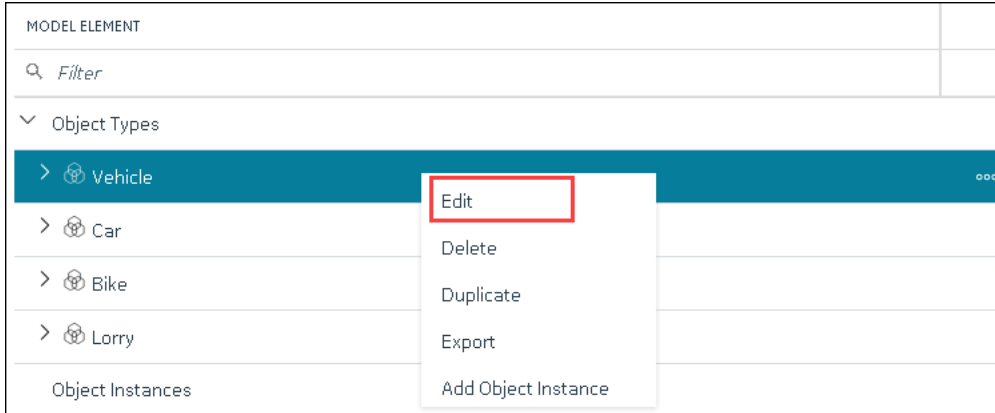
The **<object type name>** section appears. The **OBJECT TYPE TEMPLATE** field contains the default template.

7. To add variables to the default template:

    a. In the **Variables** table, select **New**.
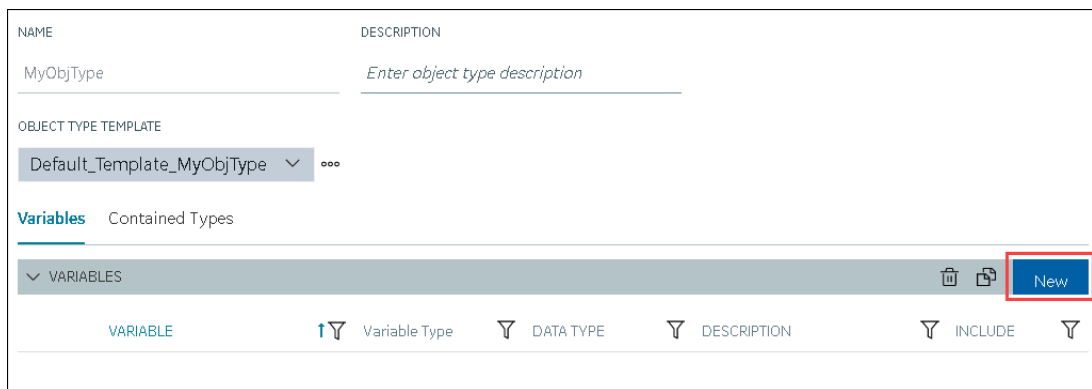
    A blank row appears in the table.

    b. Enter values as described in the following table.

Column	Description
VARIABLES	Enter the name of the variable. A value is required and must be unique for the object type. The value that you enter: ▪ Must begin with a letter or a number. ▪ Can contain up to 256 characters.

Column	Description
	▪ Can include any of the following special characters: /!|#{}%$-_ ▪ Must not include a space or any of the following characters: ~` +^:;.,?"*={}@
VARIABLE TYPE	Choose one of the following types of variables: ▪ **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 817)*, 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**.
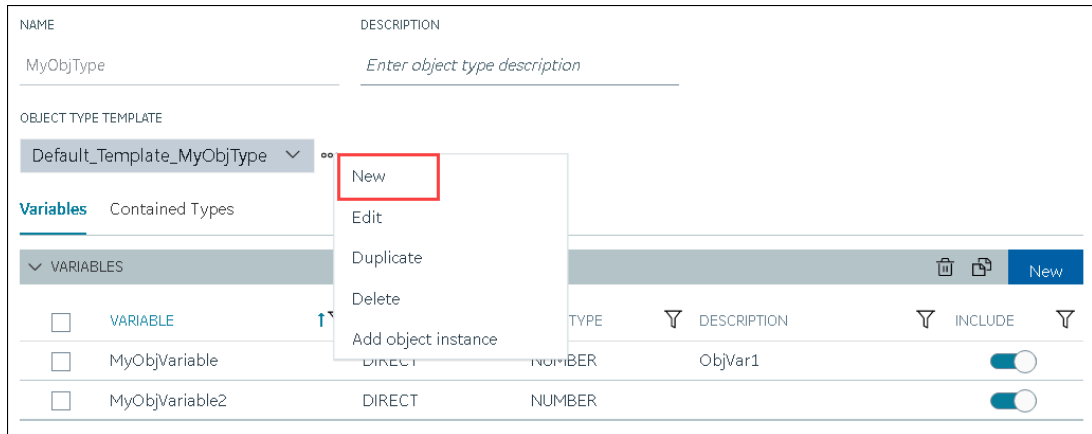
    The **New Object Template** window appears.
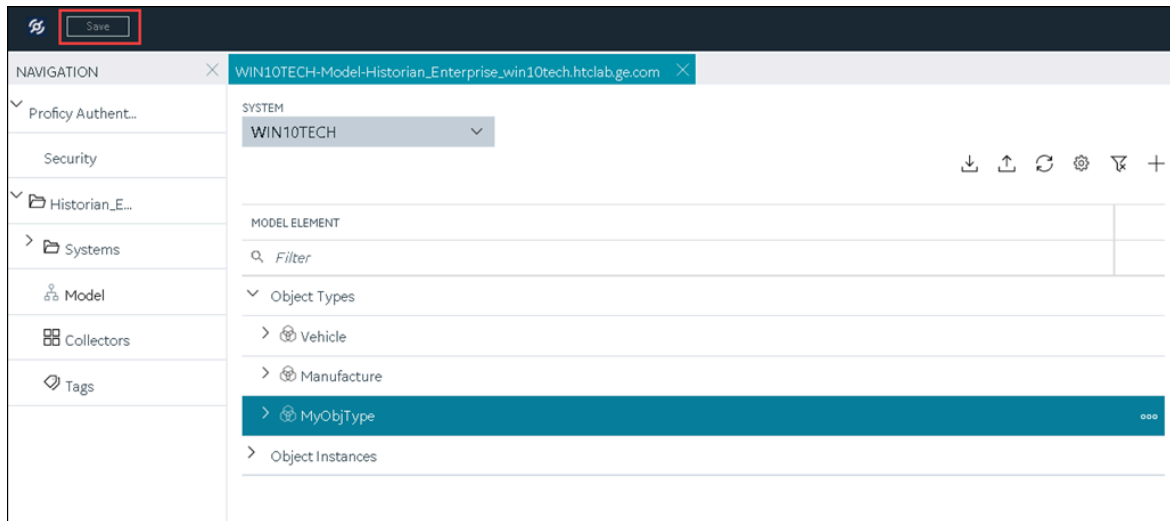
    b. Enter values as described in the following table.

Field	Description
NAME	Enter a name for the template. A value is required and must be unique. The value that you enter: ▪ 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 805)*.

Include a Contained Type in an Object Type

Create an object type *(on page 797)* 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 787)*.

1. Access Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, 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**.
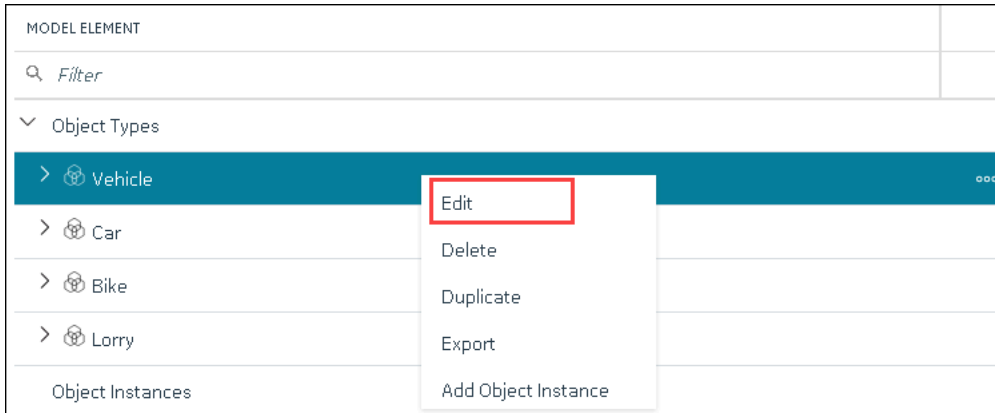
The **<object type name>** section appears, displaying a list of variables in the object type.

4. Select **Contained Types**.
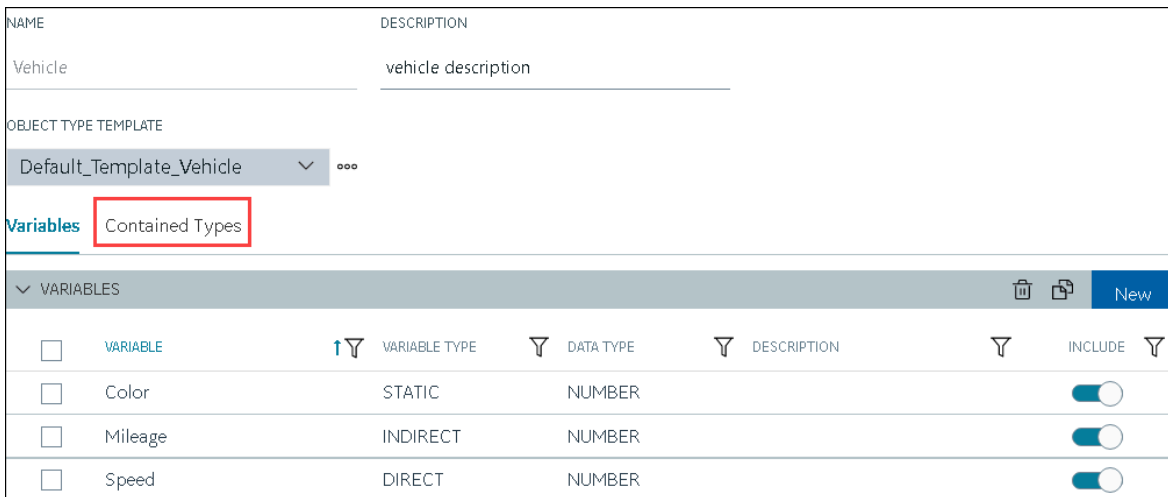
A list of contained types in the object type appears.

5. In the **CONTAINED TYPES** table, select **New**.
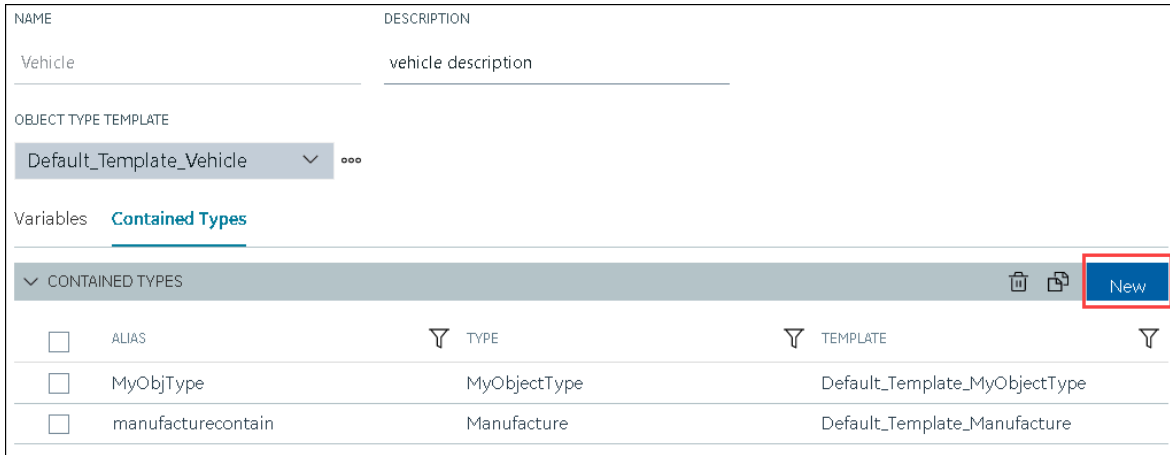
A blank row appears in the table.

6. Enter values as described in the following table, and press ENTER.

Field	Description
ALIAS	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. The value that you enter: ◦ 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	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.
TEMPLATE	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.

The contained type is included in the object instance.

7. In the upper-left corner of the page, select **Save**.
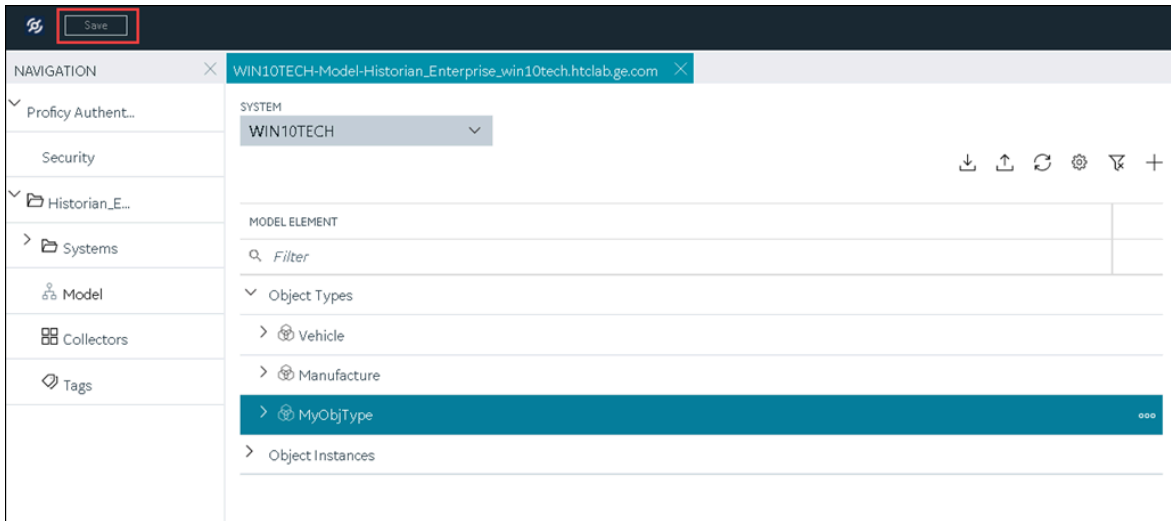
The changes to the object type are saved.

Create an object instance *(on page 805)*. 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 797)*.

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 765)*.
2. In the **NAVIGATION** section, 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 [icon]), and then select **Add Object Instance**.
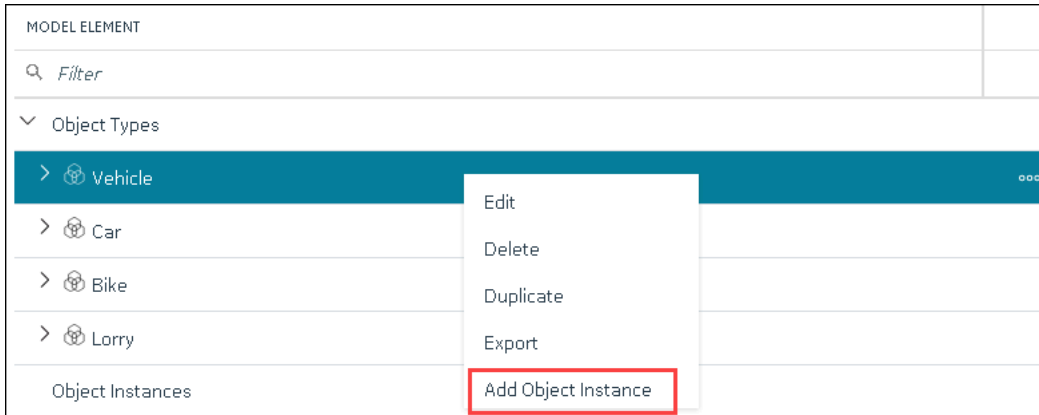
The **New Object Instance** window appears.

5. Enter values as described in the following table.

Field	Description
NAME	Enter a name for the object instance. A value is required and must be unique for the object type. The value that you enter: ◦ 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 instance.
OBJECT TYPE	This field is disabled and populated with the object type that you have selected.
OBJECT TYPE TEMPLATE	Select the template that you want to apply to the object instance.

Field	Description
	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.

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 ![icon], and then select **DETAILS**.

- Provide data for static variables *(on page 807)*.
- Collect data for direct *(on page 809)* and indirect *(on page 812)* 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 765)*.
2. In the **NAVIGATION** section, select **Model**. Alternatively, you can select **Systems**, and then in the row containing the system in which you want to create a model, select ![icon], 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.
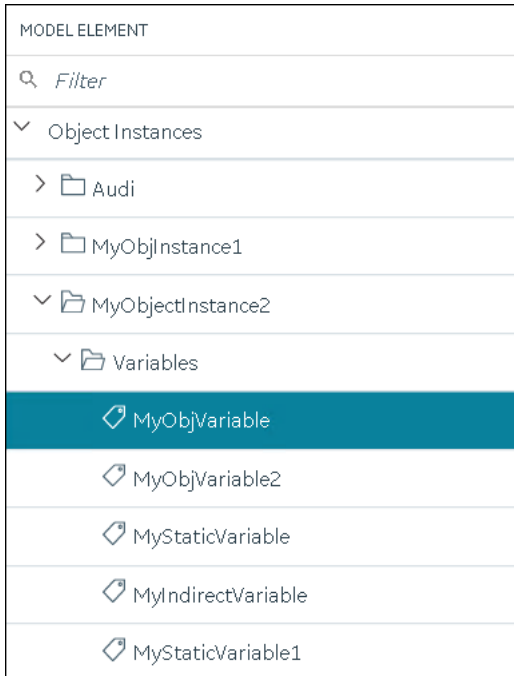
The details of the variable appear in the **DETAILS** section.

> **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.
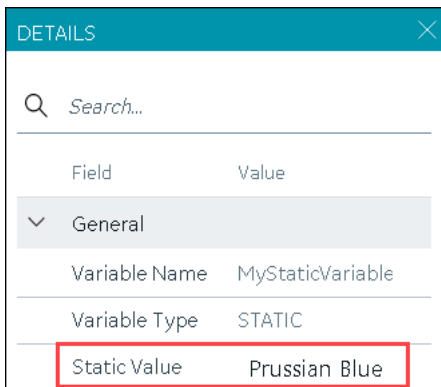
5. In the upper-left corner of the page, select **Save**.
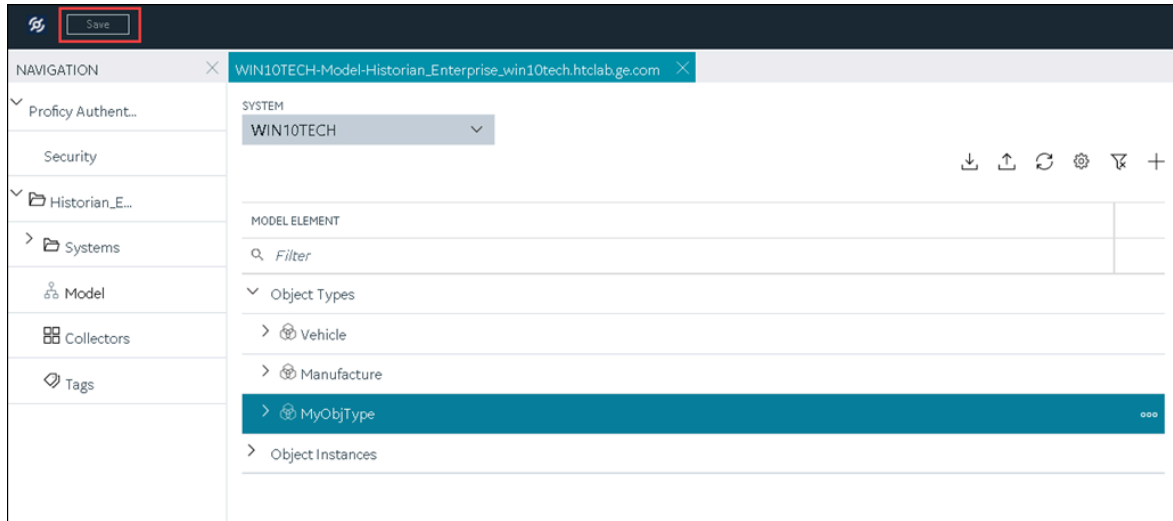
The value for the variable is saved.

Collect Data for a Direct Variable

1. using which you want to collect data for the variable.
2. 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. .
2. In the **NAVIGATION** section, 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 **Source Address** field, select .
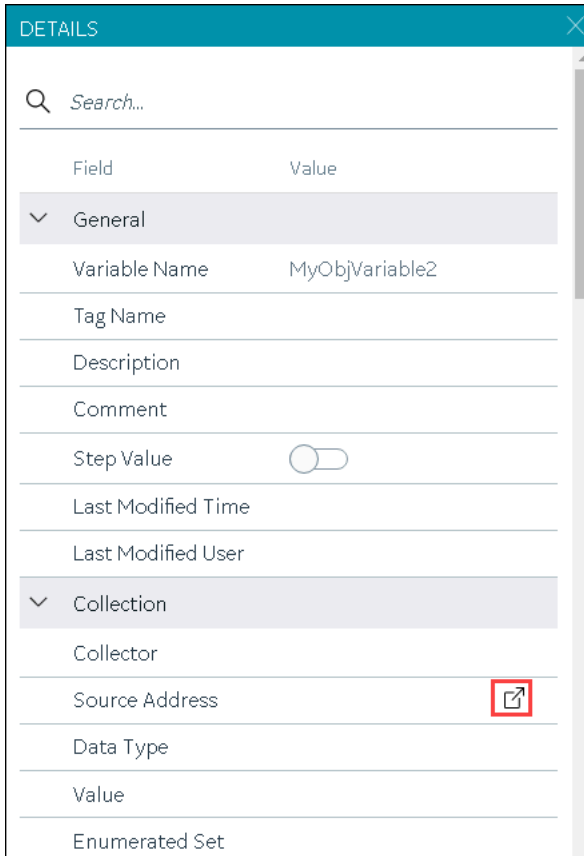
The **Browse Source Tag** window appears.

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 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**.
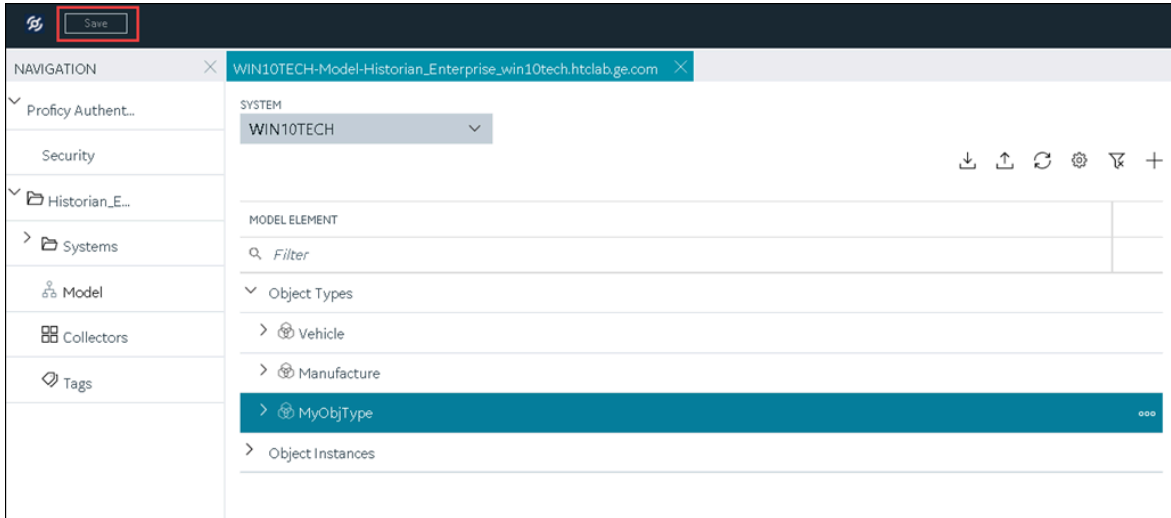
The tag is mapped with the variable. A corresponding tag is created in Historian. The details of the tag and the collector instance are disabled and populated in the **DETAILS** section. All the data that is collected for the tag is now stored in Historian (or in a cloud destination as configured in the collector instance).

Collect Data for an Indirect Variable

1. Create a collector instance using which you want to collect data for the variable.
2. Add the tag that you want to map with the variable.

To collect data of a direct 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.
2. In the **NAVIGATION** section, select **Model**. Alternatively, you can select **Systems**, and then in the row containing the system in which you want to create a model, select [ooo], 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 **DETAILS** section, in the **Tag Name** field, select ⬀.
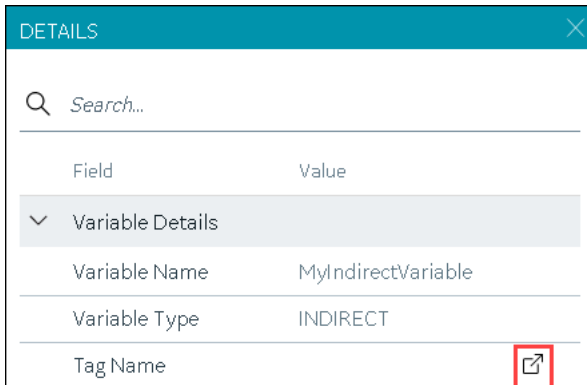
The **Tag Selection: <variable name>** window appears.

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**.
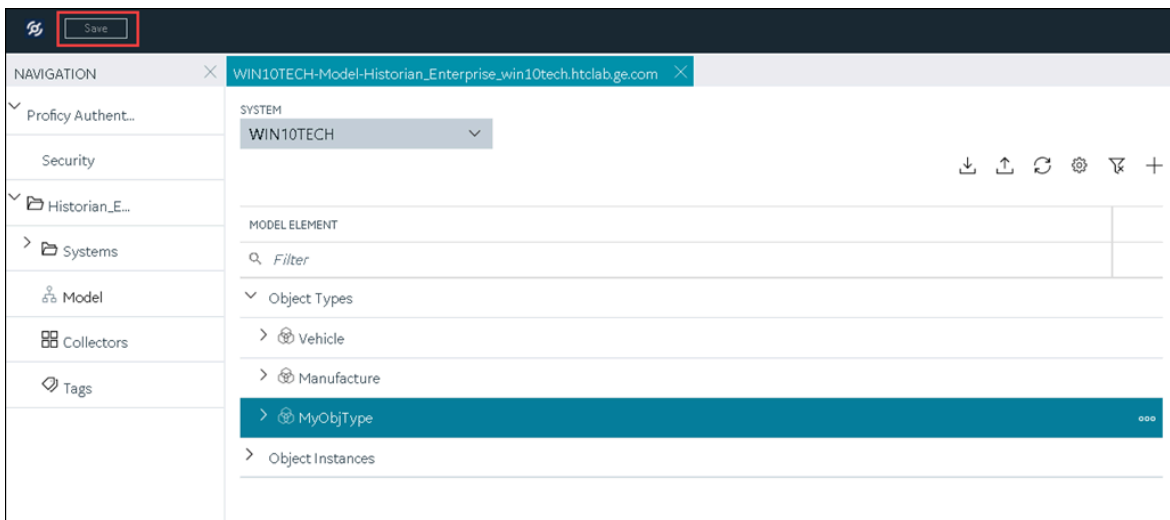
The tag is mapped with the variable. All the data that is collected for the tag is now stored in Historian (or in a cloud destination as configured in the collector instance).

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 .
2. In the **NAVIGATION** section, 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 ⬆.

MODEL ELEMENT	
🔍 *Filter*	
⟩ Object Types	
⟩ Object Instances	
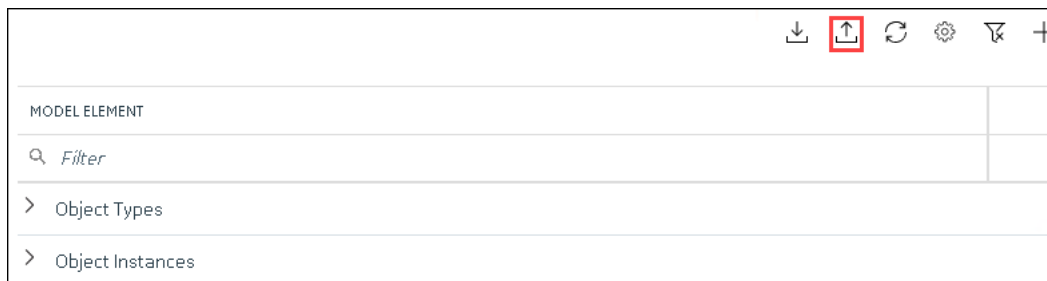
If you want to export a single object type/instance, under **Object Types** or **Object Instances**, right-click the object type/instance that you want to export (or select ⬛), and then select **Export**.
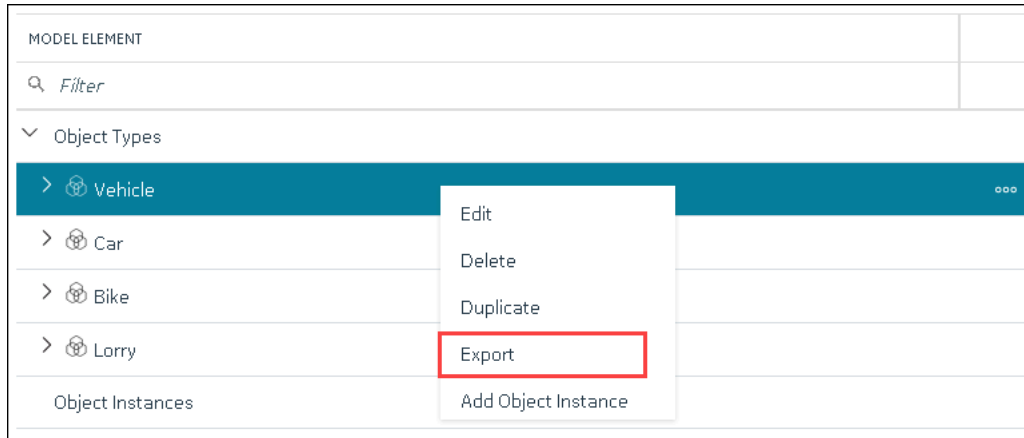
The **Export Model** window appears. Depending on whether you are exporting all the object types/instances in the system or just a single one, the **File name** field contains a value in the following format: *<host name>*.csv or *<object type>*.csv or *<object instance.*csv.

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. 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.

7. 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 765)*.
2. In the **NAVIGATION** section, 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 ⤓.
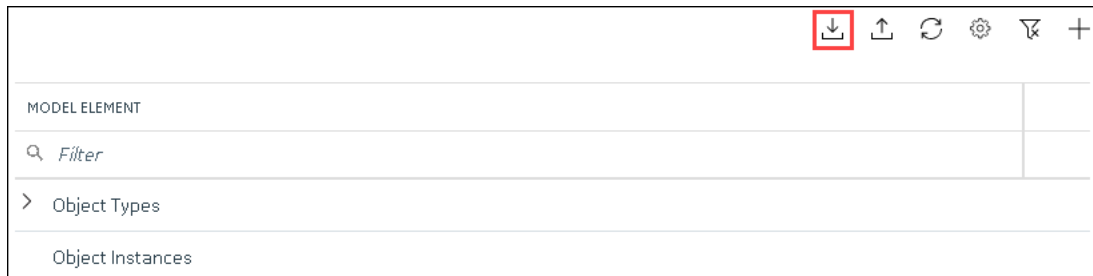
   The **Import Model** window appears.
4. Select **Choose File**, and then select the .csv file that contains the object types/instances that you want to import.
5. Depending on whether you want to import the templates, the object instances, or both, ensure that the corresponding check boxes are selected.
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 787)* and About Object Templates *(on page 793)*.

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 797)*.

1. Access Configuration Hub *(on page 765)*.
2. In the **Navigation** section, 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**.
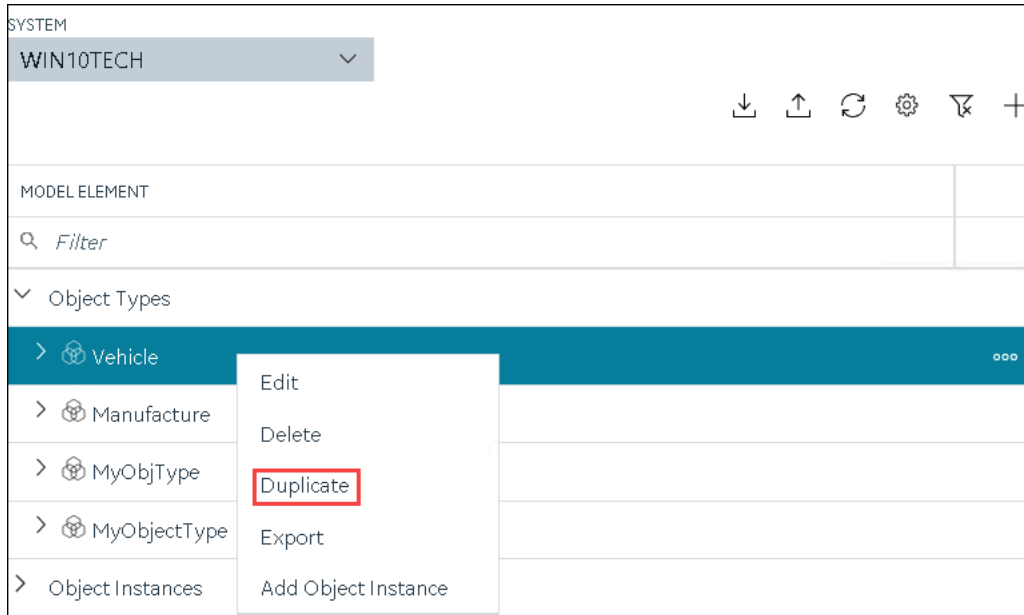
The **Duplicate Object Type** window appears.

4. Enter values as described in the following table.

Field	Description
NAME	Enter a name for the object type. A value is required and must be unique.
	The value that you enter:
	◦ 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**.
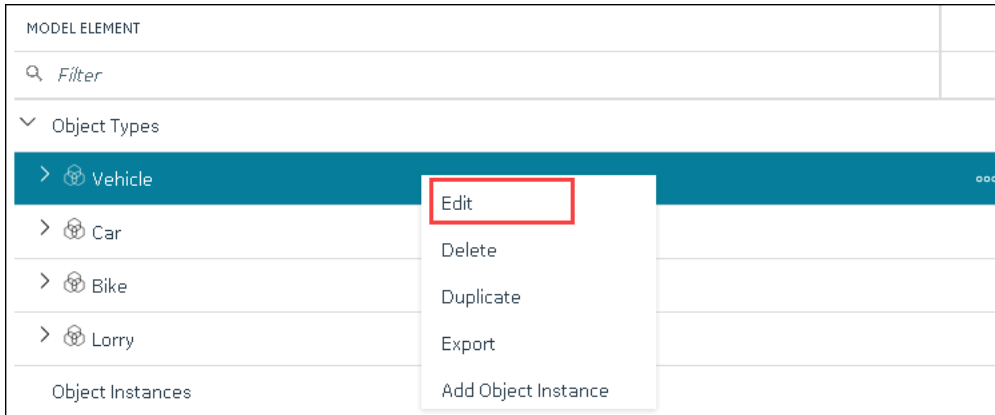
The **<object type name>** section appears. The **OBJECT TYPE TEMPLATE** field contains all the templates in the original object type. In addition, each template contains all the variables as defined in the original object type.

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**.
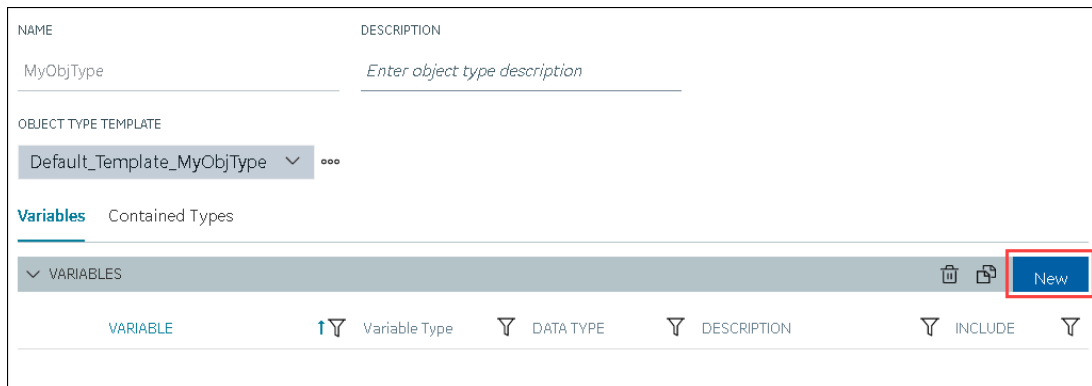
   A blank row appears in the table.

   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.

Column	Description
VARIABLE TYPE	Choose one of the following types of variables: ▪ **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**.
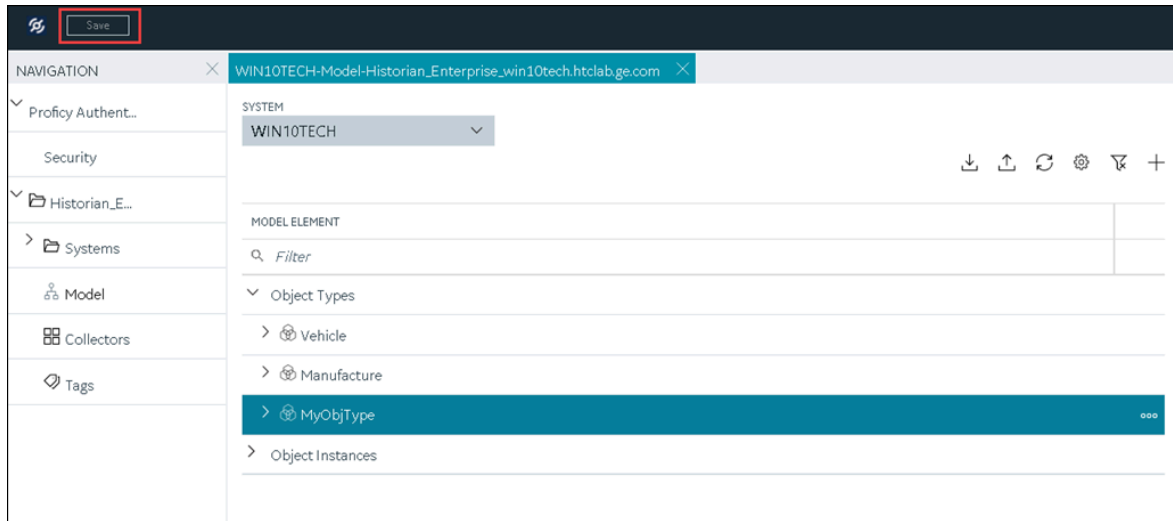
The object type, along with the default template, custom templates, and variables, is created.

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.
2. In the **NAVIGATION** section, select **Model**. Alternatively, you can select **Systems**, and then in the row containing the system in which you want to create a model, select ooo , 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 ooo), and then select **Edit**.
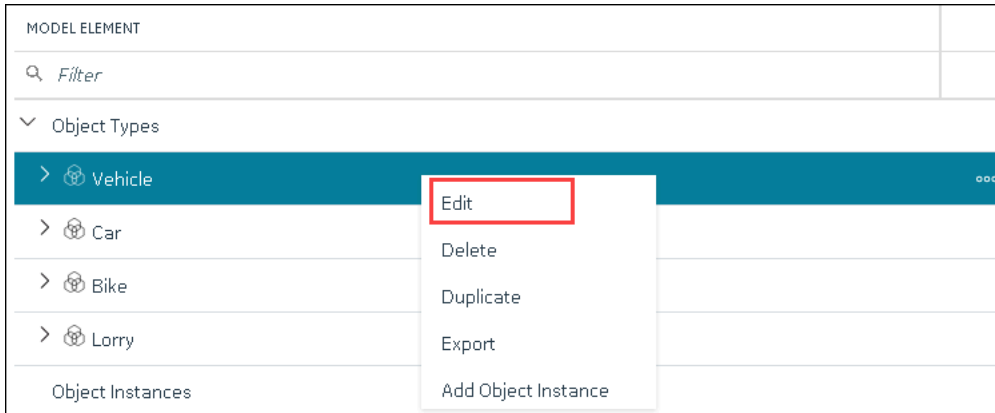
The **<object type name>** section appears. The **OBJECT TYPE TEMPLATE** field contains the default template.

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**.
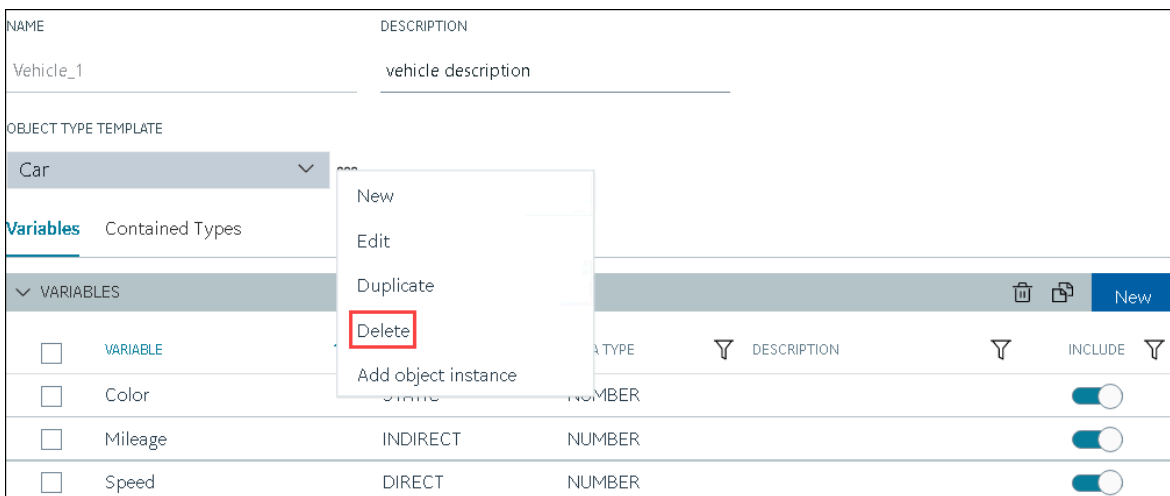
A message appears, asking you to confirm that you want to delete the template.

6. Select **Yes**.

The template is deleted.

7. In the upper-left corner of the page, select **Save**.
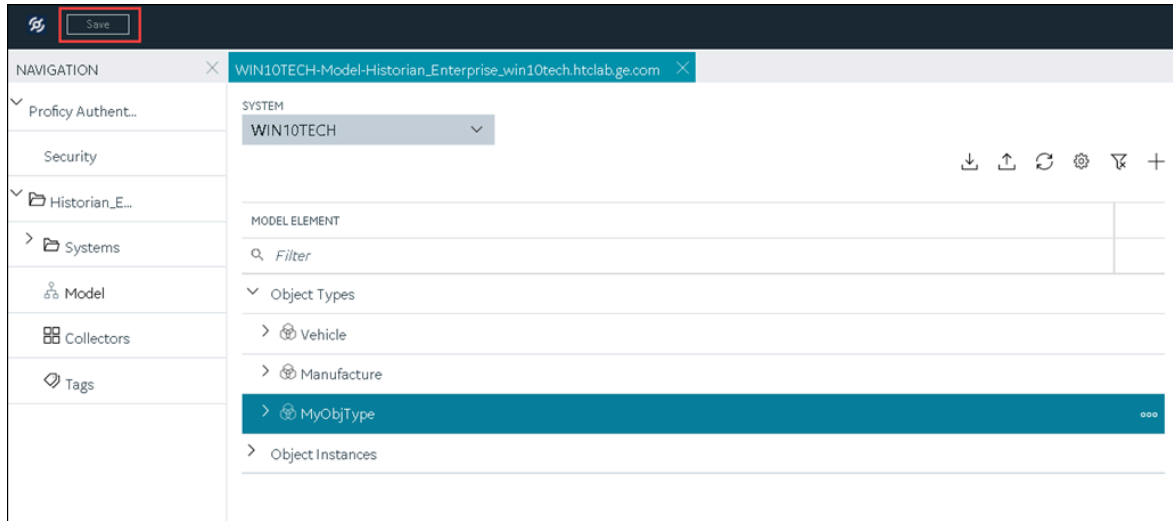
The changes to the object type are saved.

Delete an Object Instance

1.
2. In the **NAVIGATION** section, 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**.
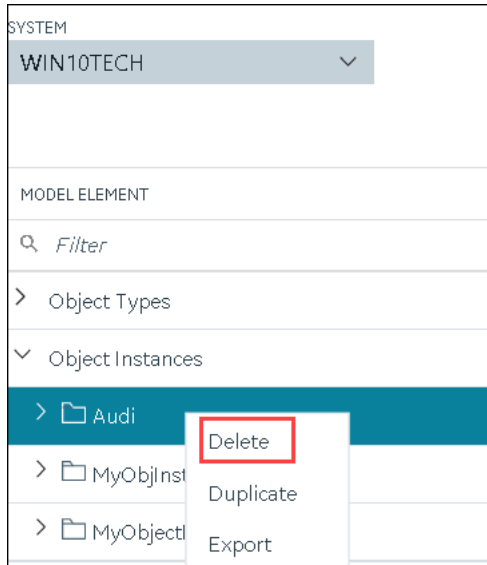
A message appears, asking you to confirm that you want to delete the object instance. If there are direct variables in the object type, you can also choose to delete the tags associated with these variables (along with their data).

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 823)*.

1. Access Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, 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**.
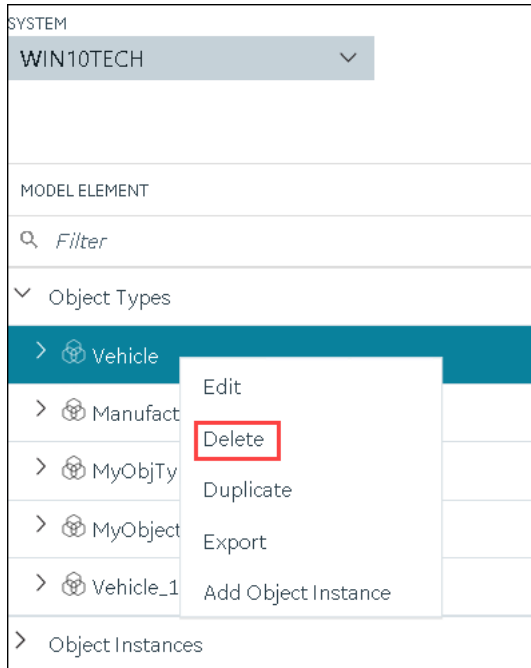
A message appears, asking you to confirm that you want to delete the object type.

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. .
2. In the **NAVIGATION** section, expand **Systems**, and then select the system that you want to access.

The system appears in the main section.
3. Expand the system in the main section.

A list of servers in the system appears, displaying the following information.

Field	Description
MACHINE NAME	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.

Field	Description
STATUS	The current status of the Historian system.
ARCHIVE COMPRESSION	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.
	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.
	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.
WRITE CACHE HIT RATIO	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.
	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 percent-

Field	Description
	age. Out-of-order data also reduces the hit ratio.
CONSUMPTION RATE	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. 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).
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)	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.

Field	Description
	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. 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.
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.
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.

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.
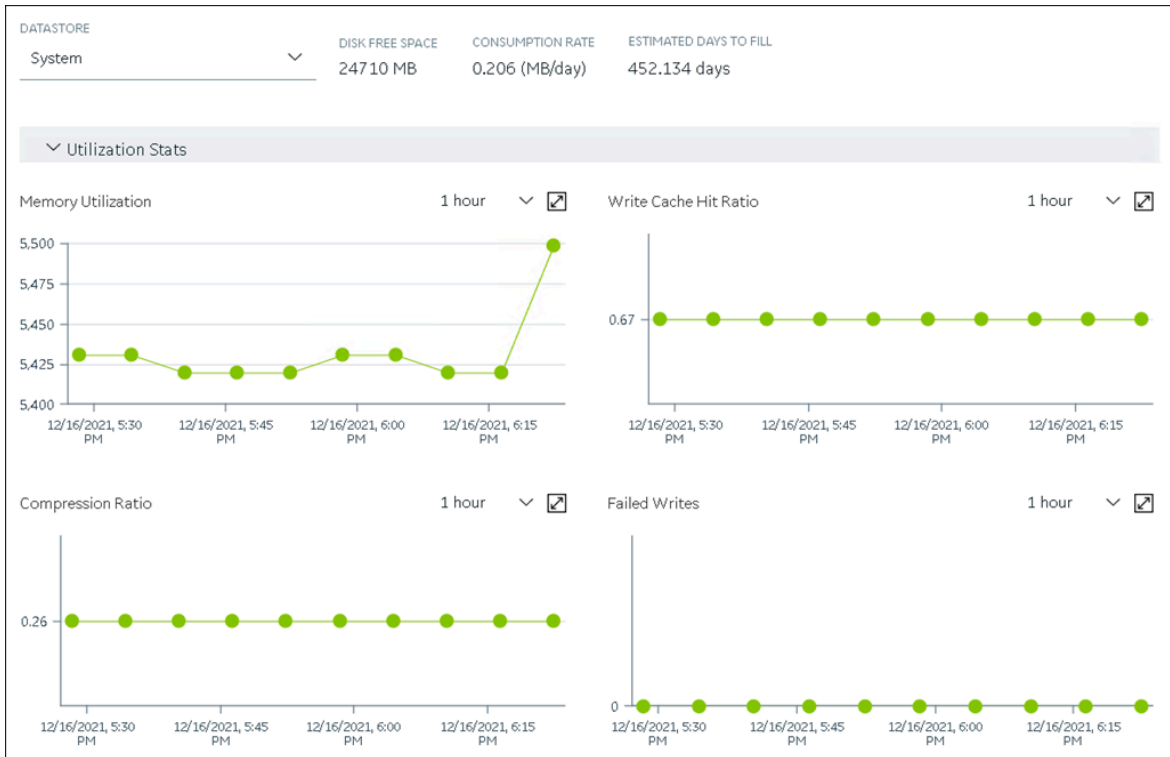
Access the Collectors in a System

1.
2. In the **NAVIGATION** section, 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 `000`), and then select **Browse Collectors**.
   The collector instances added to the system appears, 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: ◦ **Started** ◦ **Stopped** ◦ **Running** ◦ **Paused** ◦ **Unknown**
CONFIGURATION	The source of the tag configuration for the collector. Contains one of the following values: ◦ **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.
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.

Column	Description
REDUNDANCY	Indicates whether collector redundancy is enabled, which decreases the likelihood of lost data due to soft- ware or hardware failures.
TAG COUNT	The number of tags for which the collector collects data.
COMMENTS	The comments that you have entered for the collector.

> **ⓘ Tip:**
> To access the details of a collector, select the row containing the collector instance. The details appear in the **DETAILS** section.

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 960)*.

1. Access Historian in Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, 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 000), 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.

Column	Description
TAG ALIAS	Indicates whether the tag contains aliases, which are created when you rename the tag using an alias *(on page 993)*.

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 742)*. If you want to create a horizontally scalable system, install Historian primary server *(on page 742)*.

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 Historian in Configuration Hub *(on page 765)*
2. In the **NAVIGATION** section, 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.
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 786)*.
   • 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 742)* and then add them to the system *(on page 779)*.

Add a Distributed/Mirror Server

1. Install Historian server *(on page 742)* on the machine that you want to add as a distributed server.
2. Add a system *(on page 832)*. 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 Historian in Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, 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 ╋.

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 784)*, and then add the data stores *(on page 786)*. If not, add the data store *(on page 786)* to the distributed location.

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 *(on page 841)*.

You cannot delete the default server in a system.

1. Access Historian in Configuration Hub *(on page 765)*.

2. In the **NAVIGATION** section, 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 786)*. 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 Historian in Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, 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 Historian in Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, 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.

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.
2. In the **NAVIGATION** section, 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 Historian in Configuration Hub .
2. In the **NAVIGATION** section, 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 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.
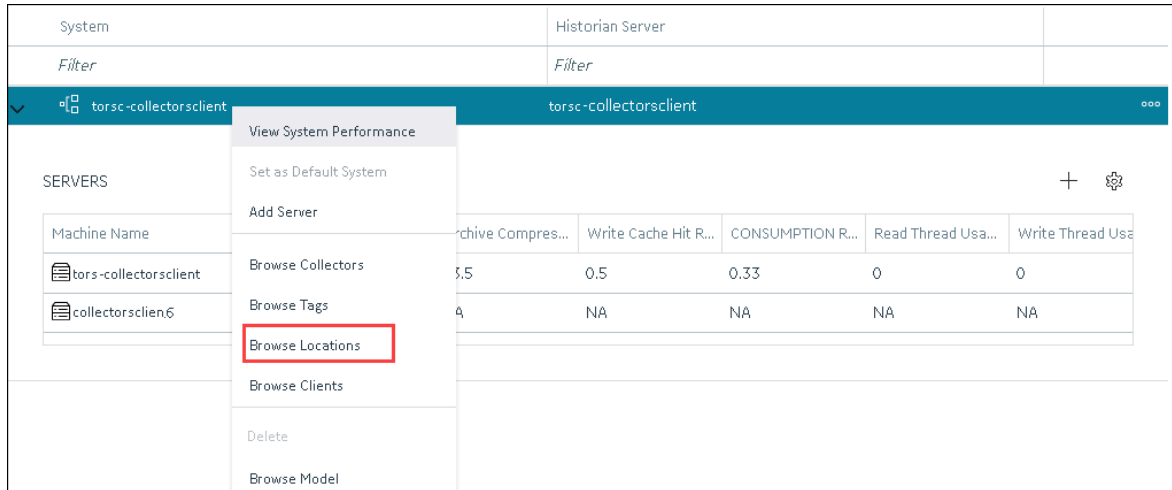
1. Access Configuration Hub .
2. In the **NAVIGATION** section, select **Systems**.

   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 can 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 786)*.

Rename a Mirror Location

1. Access Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, select **Systems**.

The **Systems** section appears, displaying a list of systems.

3. Right-click the system in which you want to rename 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. Select the location that you want to rename.

   The details of the mirror location appear in the **Details** section.

6. In the **Name** field, enter the new name of the mirror location.

7. In the upper-left corner of the page, select **Save**.
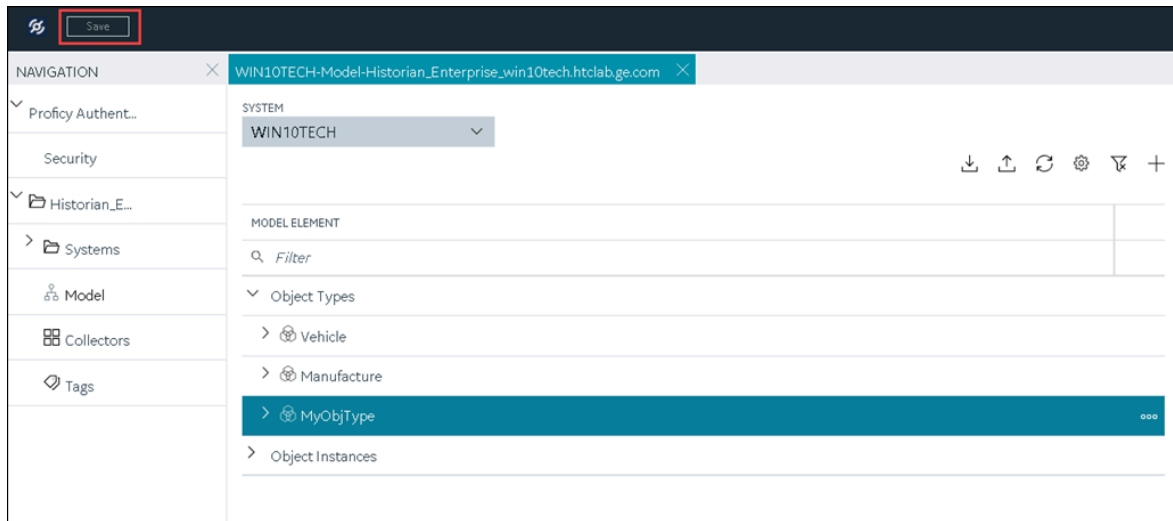
The mirror location is renamed.

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.
2. In the **NAVIGATION** section, select **Systems**.
   The **Systems** section appears, displaying a list of systems.
3. Right-click the system to which you want to add a machine (or select ![000]), and then select **Browse Locations**.
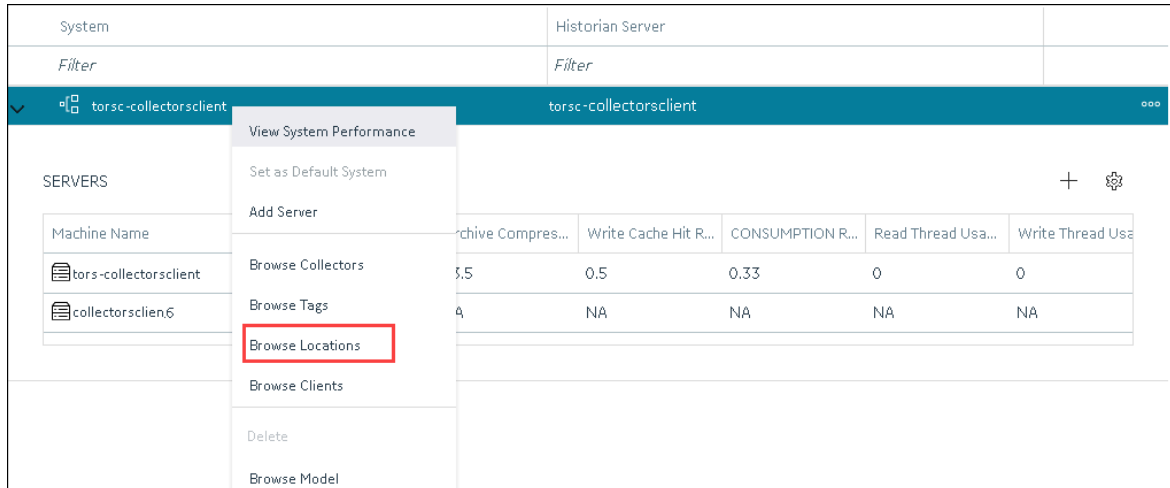
A list of distributed locations in the system appears.

4. Select **Mirror Locations**.

   A list of mirror locations in the system appears.

5. Right-click the mirror location 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.

6. 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.

1. Access Configuration Hub *(on page 765)*.

2. In the **NAVIGATION** section, select **Systems**.

   The **Systems** section appears, displaying a list of systems.

3. Right-click the system from which you want to remove a machine (or select ⬚), and then select **Browse Locations**.
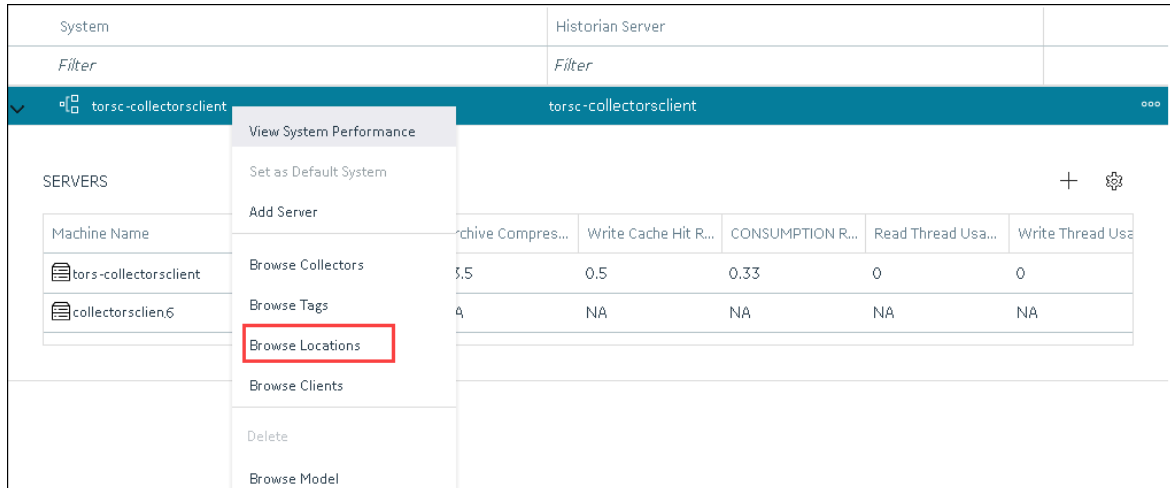
A list of distributed locations in the system appears.

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 ![icon]), 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 765)*.
2. In the **NAVIGATION** section, 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 ![icon]), and then select **Browse Locations**.
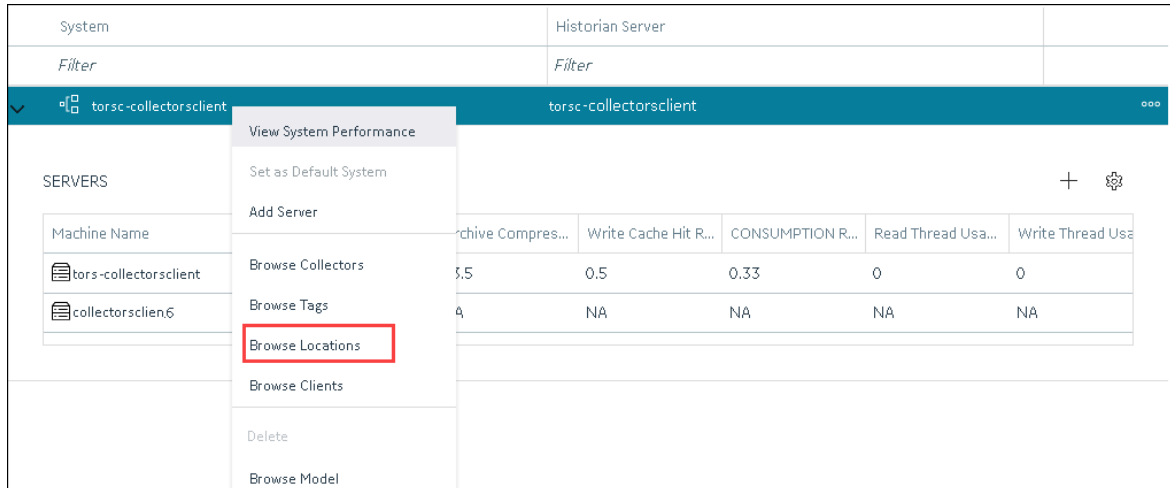
A list of distributed locations in the system appears.

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 ![icon]), 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

Add a Data Store

If you want to add a data store to a distributed server, add the distributed server *(on page 779)* to the system. If you want high availability of the data store, add a mirror location *(on page 786)* to the system.

1. Access Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, select **Systems**.

   The **Systems** section appears, displaying a list of systems.

3. Right-click the system to which you want to add a data store (or select ![icon]), and then select **Browse Locations**.

A list of distributed locations in the system appears.

4. Right-click the location in which you want to add a data store (or select 000), and then select **Add Data Store**.

   The **Add Data Store: <location name>** window appears.

5. Provide values as described in the following table.

Field	Description
DATA STORE NAME	Enter a name for the data store. A value is required and must be unique for the system.
Description	Enter a description for the data store.
Set as default data store for the System	Select the check box if you want to set the data store as default. When you do so, while creating a tag, this data store will be used by default.

6. Select **Add**.

   The data store is added to the location.

Specify the tags whose data you want to store in the data store.

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.
2. In the **NAVIGATION** section, select **Systems**.
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: <system name>** window appears.
5. Select the data store that you want to set as default, and then select **Set as Default**.

   The default data store of the system is changed.

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.

> ✏️ **Note:**
>
> Using Configuration Hub, you cannot define a calculation formula for a tag for a Calculation collector. You can, however, define a calculation formula using Historian Administrator or other Web-based Clients.

1.
2. In the **NAVIGATION** section, 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.

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 must be unique.

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 canceled, 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 912)*.

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.

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.

> **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. .
2. In the **NAVIGATION** section, 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.

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 **Cygnet 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 must be unique.

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	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.
	Continuous data collection is resumed only after the previous data has been recovered.
	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).
Thread Count	The maximum number of threads that you want to collector to use to query data from the CygNet server.

Field	Description
CygNet Debug Mode	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). **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.
General Optimized	Indicates whether you want to apply optimization on the tag data reads.
Service-Site	Identifies the CygNet site or data source from which the CygNet collector collects data. A value is required.

16. If needed, enter values in .

17. In the upper-left corner of the page, select **Save**.
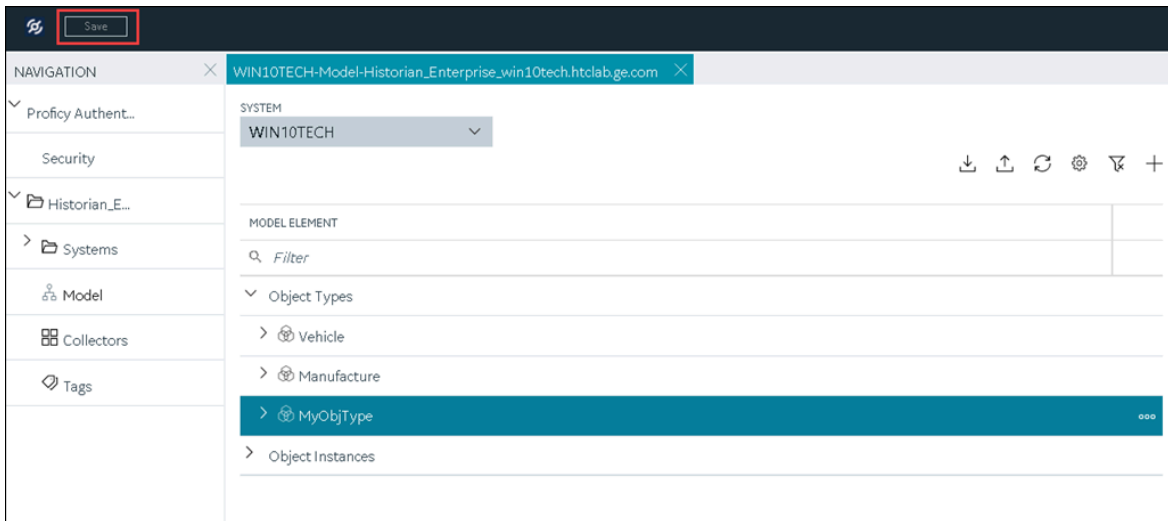
The changes to the collector instance are saved.

18. If needed, restart the collector.

Specify the tags *(on page 775)* 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.

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 Historian in Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, 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 ▽
Filter	*Filter*	*Filter*	*Filter*
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. 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 must be unique.

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 `Processed Files` folder to be automatically purged.
Purge Error (days)	The number of days after which you want the contents of the `Error Files` folder to be automatically purged.

14. If needed, enter values in .
15. In the upper-left corner of the page, select **Save**.
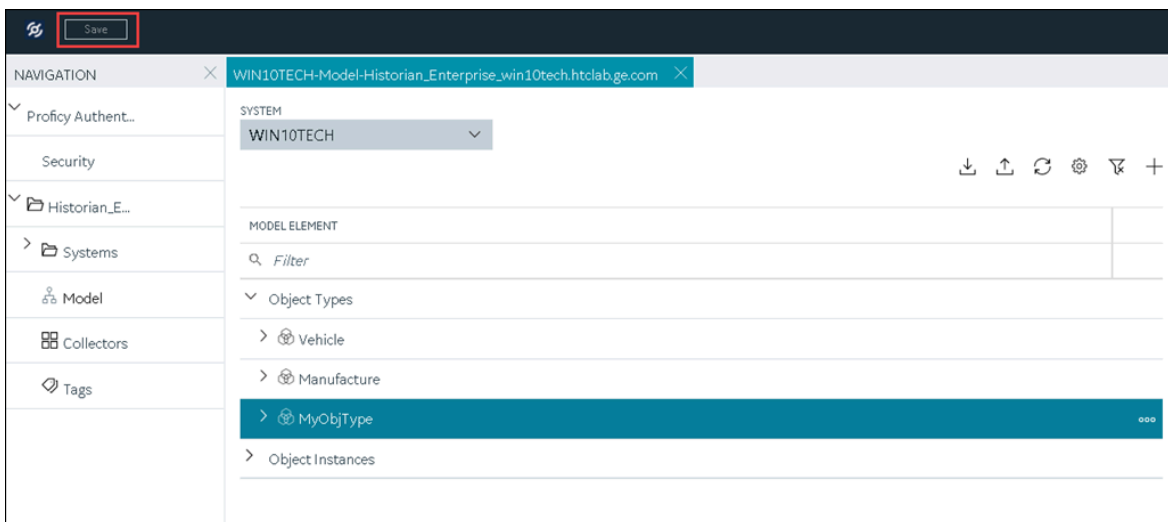
The changes to the collector instance are saved.

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.

This topic describes how to create a HAB collector using Configuration Hub. You can also create it at a command prompt.

1. Access Historian in Configuration Hub .
2. In the **NAVIGATION** section, 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.

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 **Hab 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
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: `<Historian server name>Hab`
SERVER 1 (under NODE 1)	Enter the host name or IP address of the Habitat server in the 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.
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. For example, if you want to connect to Machine-A, MachineB, MachineC, and MachineD, enter MachineA and MachineB in the SERVER 1 and SERVER 2 fields under NODE 1, and then enter MachineC and MachineD in the corresponding fields under NODE 2.
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.

Field	Description
RETRY	The duration, in seconds, after which the collector tries to communicate with the site. The default value is 5 seconds.

9. 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.

10. If you want to connect to a remote Historian server, enter values in the **USERNAME** and **PASSWORD** fields.

11. 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`

12. If needed, modify the value in the **COLLECTOR NAME** field. The value must be unique and must not exceed 15 characters.

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. In addition, the following files are created:

    ◦ `<collector name>_Config.xml`
    ◦ `<collector name>_Tag.xml`

    By default, these files are located in the following folder: `C:\Program Files\GE Digital \Historian HAB Collector\Server`

15. Access the `<collector name>_Config.xml` file, and provide values for the parameters.

16. In Configuration Hub, in the **Collectors** section, select the collector instance, and provide values in the available fields .

17. In the upper-left corner of the page, select **Save**.
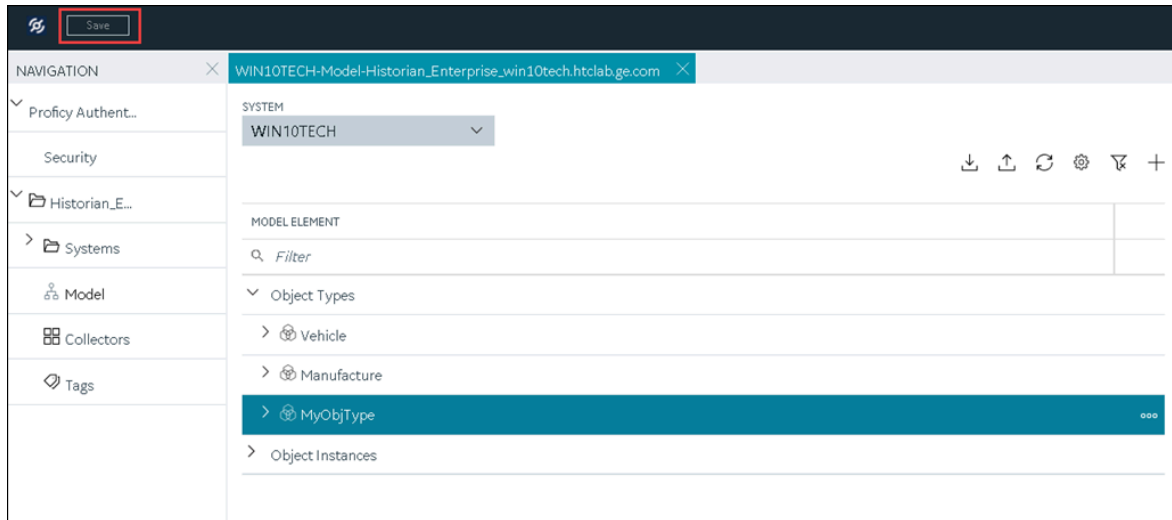
The changes to the collector instance are saved.

18. Start the collector .

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_Unconfirmed.xml` file. Approve the changes so that they are reflected in Historian.

> **Note:**
> If you have enabled the automatic tag sync option, tag changes are automatically reflected in Historian; no manual steps are needed.

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
iFIX is running in service mode and is secured. The iFIX Alarms and Events and the OPC Alarms and Events Servers are running as service.	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**.	• 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.
iFIX is running as a service and is not secured. The iFIX Alarms and Events and the OPC Alarms and Events servers are running as service.	You can configure the iFIX collector service using a local system account or a specific user account.	• 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**.	• 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
iFIX is not running as a service mode, and is not secured.	You can configure the iFIX collector service using a local system account or a specific user account.	• 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.
iFIX is not running.	You can configure the iFIX collector service using a local system account or a specific user account, as per the security configuration of iFIX.	• 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
		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. • 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 About Adding an iFIX Collector Instance *(on page 858)*.

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 Historian in Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, 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.

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 **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 *(on page 920)*, AWS Cloud *(on page 925)*, Azure Cloud *(on page 931)*, Google Cloud *(on page 944)*, or Predix Cloud *(on page 949)*. 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 must be unique.

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.
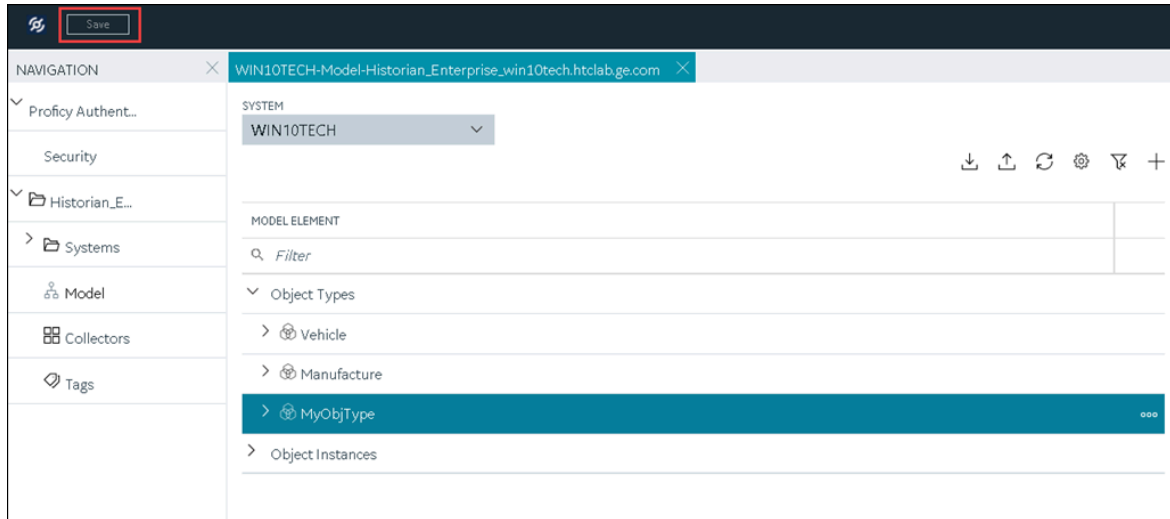
14. Select **Add**.

    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 *(on page 858)*.

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 775)*.

    > **Note:**
    >
    > If you want to add block or field types to the list, edit the `FixTag.dat` file for Historian Administrator you are using.

17. If needed, enter values in the other sections *(on page 912)*.

18. In the upper-left corner of the page, select **Save**.

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 775)*.
- 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>`. 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

The MQTT collector collects data published to a topic using an MQTT broker.

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 Historian in Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, 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.

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 **MQTT 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
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.

Field	Description
TOPIC	Enter the MQTT topic from which you want to collect data. 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 with the value you selected in the **MACHINE NAME** field in the **Collector Selection** section.

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 920)*, AWS Cloud *(on page 925)*, Azure Cloud *(on page 931)*, Google Cloud *(on page 944)*, or Predix Cloud *(on page 949)*.

11. Select **Next**.

    The **Collector Initiation** section appears.

12. If needed, modify the value in the **COLLECTOR NAME** field. The value must be unique.

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

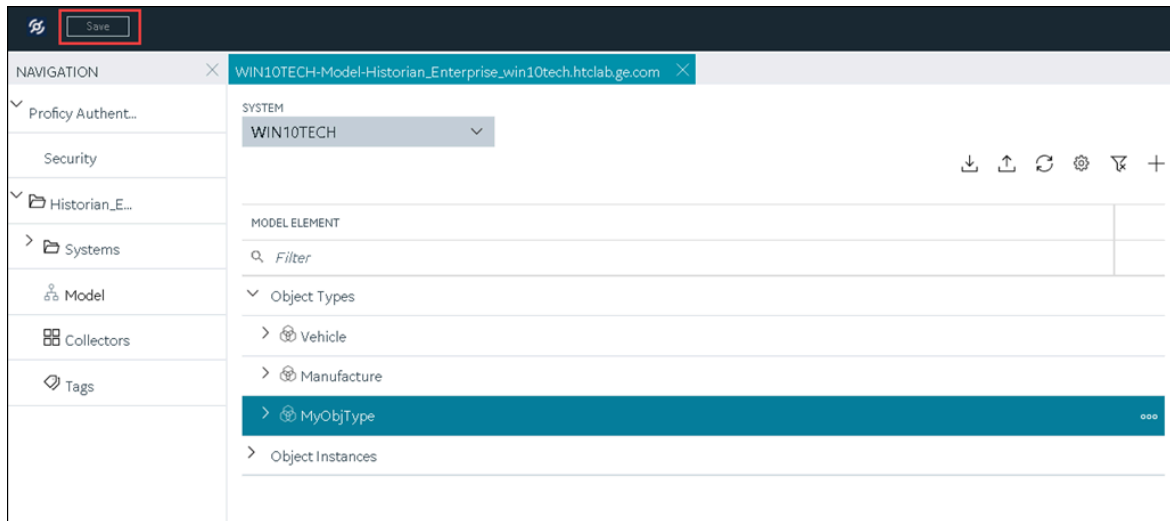   ▪ iH Collector Admins

    ▪ 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 available fields *(on page 912)*.

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 775)*.
- 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>`. This option is applicable only if you have selected a cloud destination.

Add and Configure an ODBC Collector

The ODBC collector collects data from an application based on an ODBC driver.

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 Historian in Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, 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.

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.

Field	Description
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 920)*, AWS Cloud *(on page 925)*, Azure Cloud *(on page 931)*, Google Cloud *(on page 944)*, or Predix Cloud *(on page 949)*.

11. Select **Next**.

   The **Collector Initiation** section appears.

12. If needed, modify the value in the **COLLECTOR NAME** field. The value must be unique.

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
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 ODBC 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. 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).
Throttle (Milliseconds)	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. 📝 **Note:** If this field is blank, enter the required minimum value of 100 milliseconds.

16. If needed, enter values in the other sections *(on page 912)*.
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 775)*.

- 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>`. 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.
2. In the **NAVIGATION** section, 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.

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 must be unique.

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 912)*.

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 775)* 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.

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 Historian in Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, 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.

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 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.

Field	Description
MACHINE NAME	Enter the host name or IP address of the OPC server. This field appears only if you have se-lected 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 920)*, AWS Cloud *(on page 925)*, Azure Cloud *(on page 931)*, Google Cloud *(on page 944)*, or Predix Cloud *(on page 949)*.

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 must be unique.

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**.

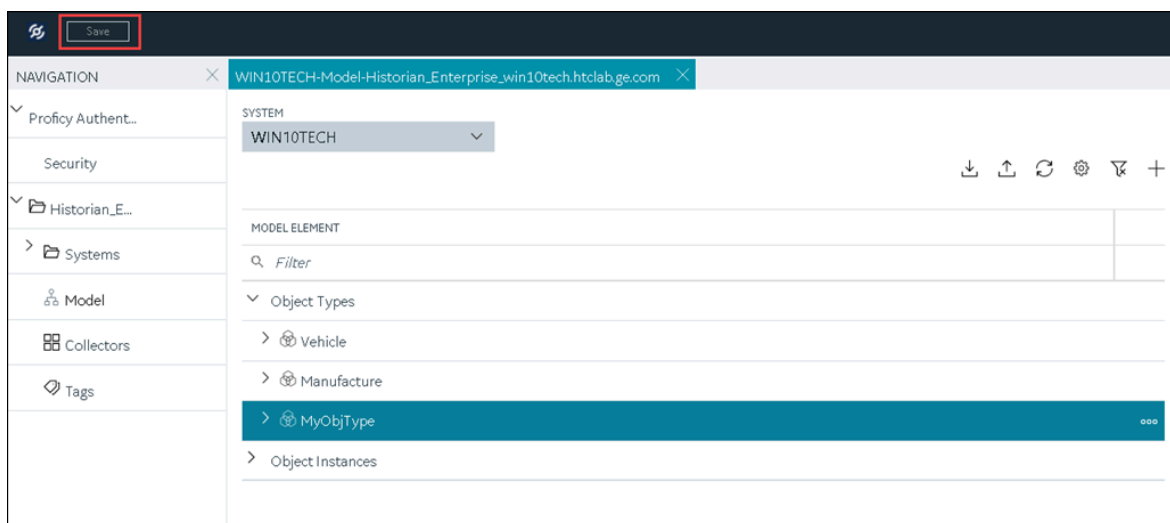The collector instance is added. The fields specific to the collector section appear in the **DETAILS** section.

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	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. For example, if you enter `USGB014` in the **First Browse Criteria** field and `F_CV, B_CUALM` in the **Second Browse Criteria** field, it returns all the tags that contain: ◦ 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.
Threading Model	The type of the threading model selected for the collector. The model selected must match the threading model of the OPC server. ◦ **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 mul-

Field	Description
	ti-threading. If you experience problems running your collector with multi-threading, use the apartment model. The default setting is multi-threaded. For information, refer to the documentation of the OPC server you are using.

Configuration Changes	Indicates whether the collector configuration changes are processed in real time or after restarting the collector.
	
	◦ **Made On-Line**: Select this option to process any configuration changes immediately (after 30 seconds) after you select the **Update** button.
	
	    📝 **Note:**
	    ▪ Some OPC servers cannot handle processing configuration changes online. If you experience any instability with changes made online, use the next option.
	
	◦ **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 912)*.

17. In the upper-left corner of the page, select **Save**.
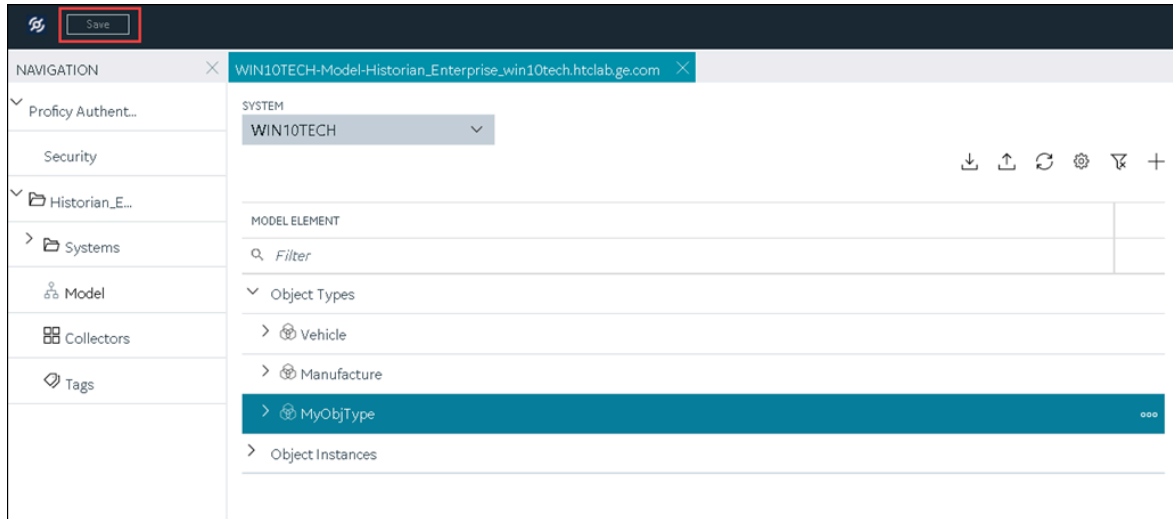
The changes to the collector instance are saved.

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 775)*.
- 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>`. 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.

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 Historian in Configuration Hub *(on page 765)*.
2. If needed, select the system in which you want to add a collector instance.

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 **OPC HDA 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
OPC HDA SERVER	Select the machine on which you have installed the OPC Classic HDA server from which you want to collect data.

Field	Description
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.

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 *(on page 920)*, AWS Cloud *(on page 925)*, Azure Cloud *(on page 931)*, Google Cloud *(on page 944)*, or Predix Cloud *(on page 949)*.

10. Select **Next**.

    The **Collector Initiation** section appears.

11. If needed, modify the value in the **COLLECTOR NAME** field. The value must be unique.

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.
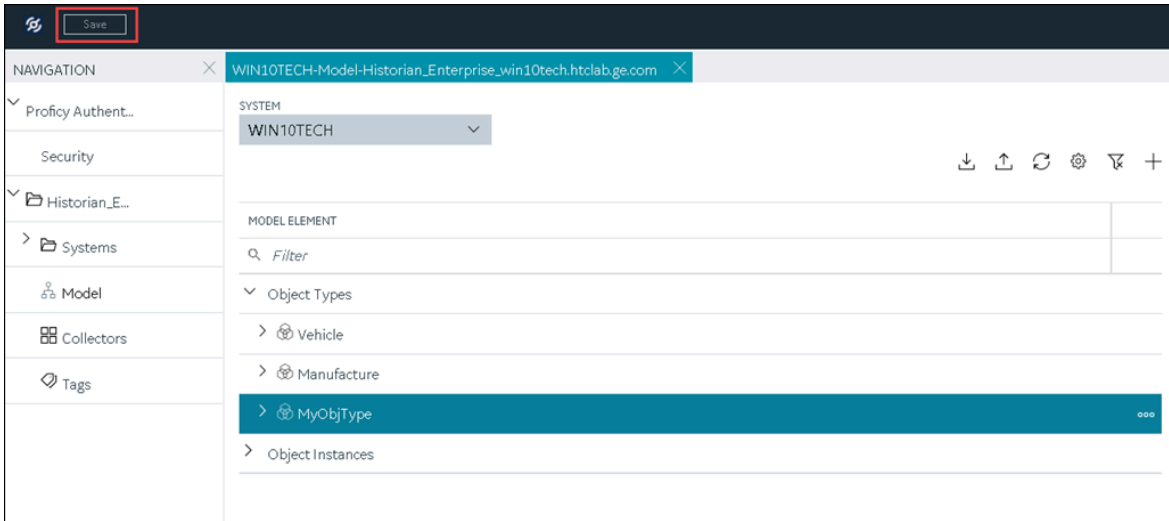
13. Select **Add**.

    The collector instance is added. The fields specific to the collector section appear in the **DETAILS** section.

14. 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.

15. If needed, enter values in the other sections (on page 912).
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 775).
- 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>`. 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.

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 Historian in Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, 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.

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 920)*, AWS Cloud *(on page 925)*, Azure Cloud *(on page 931)*, Google Cloud *(on page 944)*, or Predix Cloud *(on page 949)*.

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 must be unique.

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: `opc.tcp://<host name or IP address of the OPC UA server>:<port number>`
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: ◦ **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	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 `ClientConfig.ini` file.
Username	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 `ClientConfig.ini` file is considered.
Password	This field id 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 `ClientConfig.ini` file is considered.

16. If needed, enter values in the other sections *(on page 912)*.
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.

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 Historian in Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, 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.

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 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.

Field	Description
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 *(on page 920)*, AWS Cloud *(on page 925)*, Azure Cloud *(on page 931)*, Google Cloud *(on page 944)*, or Predix Cloud *(on page 949)*.

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 must be unique.

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:
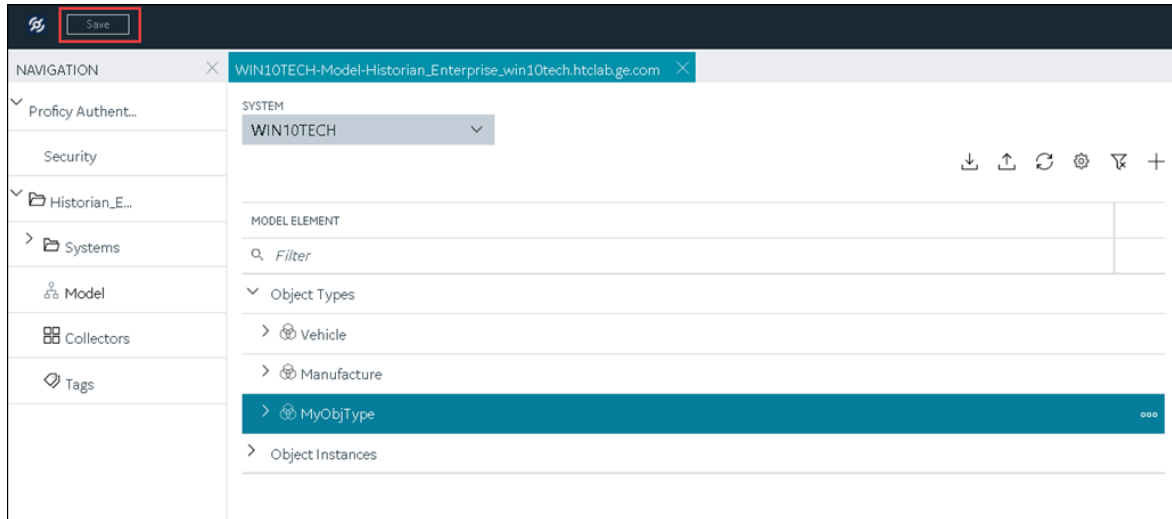
    ▪ iH Security Admins

    ▪ 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)	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. Continuous data collection is resumed only after the previous data has been recovered. The default value is 4 hours.
Data Source	Specify whether you want to collect data from PI archive or PI snapshot: ◦ **Archive**: Stores timeseries-based data. ◦ **Snapshot**: Stores the most recent values of tags.

16. If needed, enter values in available fields .

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 775)*.
- 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>`. 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.

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 Historian in Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, 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.

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 must be unique.

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.
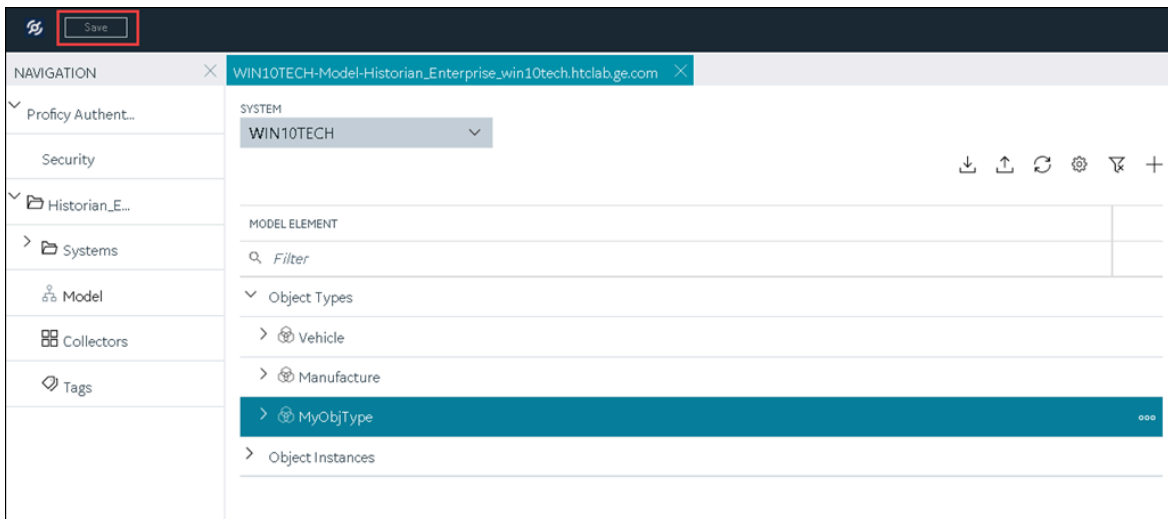
14. Select **Add**.

    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)	Enter the maximum time, in hours, for which the collector will attempt to recover data after

Field	Description
	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. Continuous data collection is resumed only after the previous data has been recovered. The default value is 4 hours.

Data Source	Specify whether you want to collect data from PI archive or PI snapshot:
	  ◦ **Archive**: Stores timeseries-based data.
	  ◦ **Snapshot**: Stores the most recent values of tags.

16. If needed, enter values in available fields (on page 912).

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 775) 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.

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 Historian in Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, 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.

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 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 *(on page 920)*, AWS Cloud *(on page 925)*, Azure Cloud *(on page 931)*, Google Cloud *(on page 944)*, or Predix Cloud *(on page 949)*.

11. Select **Next**.

    The **Collector Initiation** section appears.

12. If needed, modify the value in the **COLLECTOR NAME** field. The value must be unique.

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.
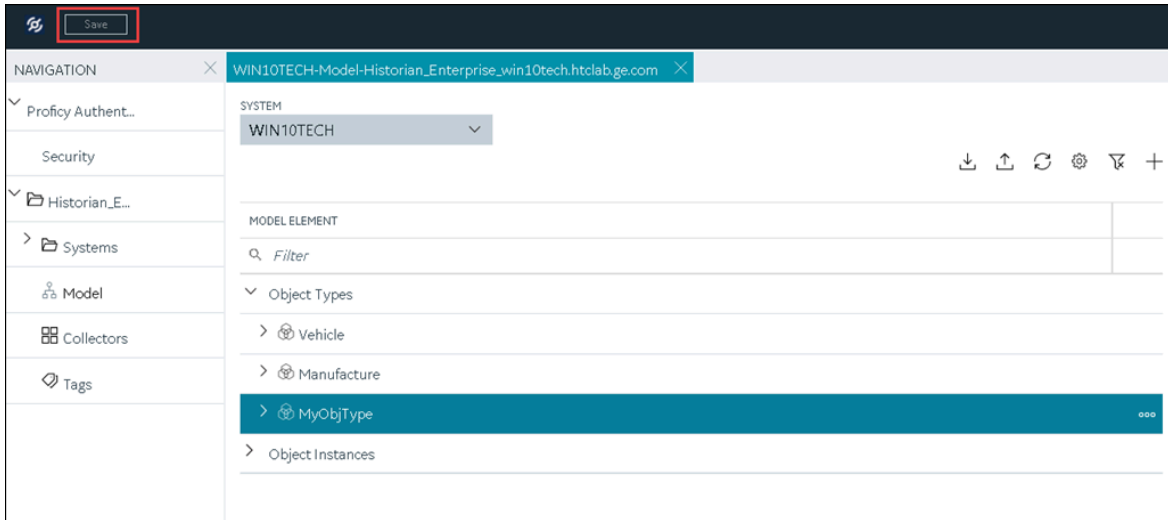
14. Select **Add**.

    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	The prefix to identify replicated messages on the destination. Alarms and events data will automatically have a prefix added to it with the following syntax: `MachineName_Datasource` For example, if your alarm is forwarded from the server `Almserver12` with a data source named `OPCAE`, the prefix will be `Almserver12_OPCAE`.

16. If needed, enter values in .
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 775)*.
- 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>`. 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.

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 896)* 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 Historian in Configuration Hub *(on page 765)*.

2. In the **NAVIGATION** section, 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.

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 must be unique.

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**.
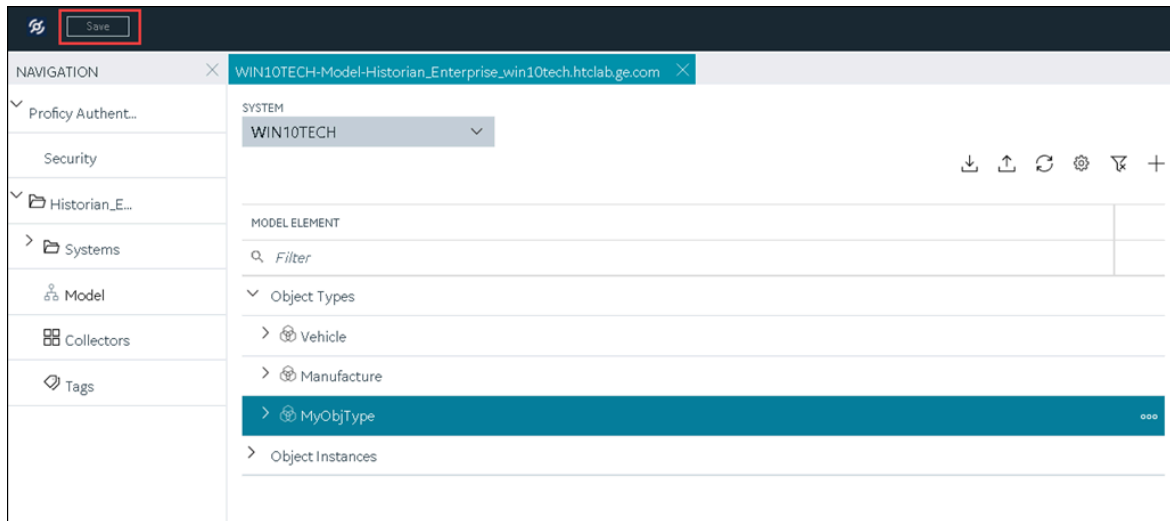
    The collector instance is added. The fields specific to the collector section appear in the **DETAILS** section.

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.

Field	Description
	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	The prefix to identify replicated messages on the destination. Alarms and events data will automatically have a prefix added to it with the following syntax: `MachineName_Datasource` For example, if your alarm is forwarded from the server `Almserver12` with a data source named `OPCAE`, the prefix will be `Almserver12_OPCAE`.

16. If needed, enter values in .

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.

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.

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 Historian in Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, 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.

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 **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 *(on page 920)*, AWS Cloud *(on page 925)*, Azure Cloud *(on page 931)*, Google Cloud *(on page 944)*, or Predix Cloud *(on page 949)*.

10. Select **Next**.

    The **Collector Initiation** section appears.

11. If needed, modify the value in the **COLLECTOR NAME** field. The value must be unique.

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

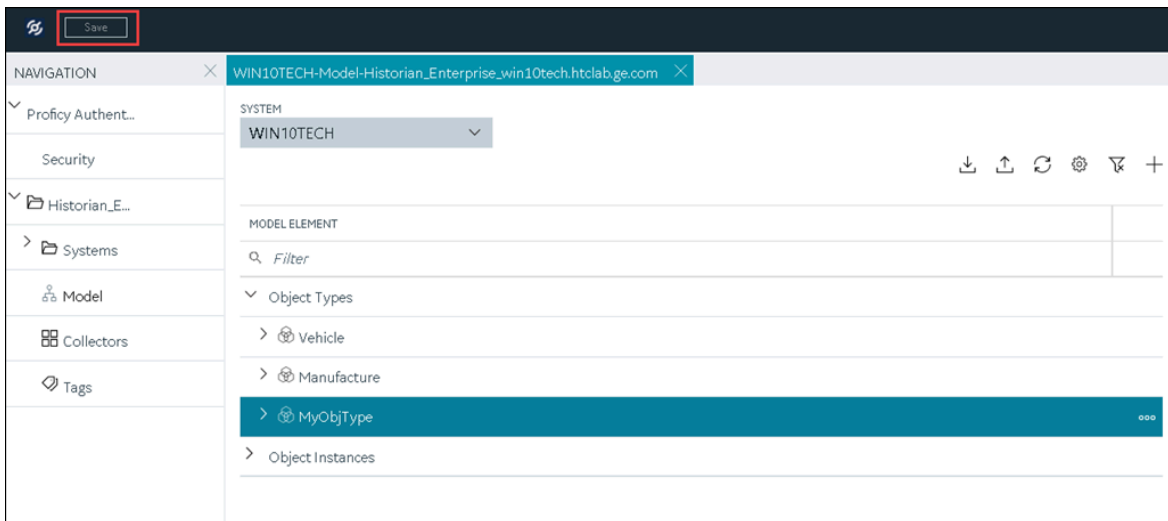   You can also configure the collector to start automatically when you start the computer.

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 `SIN`, `STEP`, and `RAMP` functions implemented in the collector.

15. If needed, enter values in the other sections .
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 .
- 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>`. 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.

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 Historian in Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, 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.

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 *(on page 920)*, AWS Cloud *(on page 925)*, Azure Cloud *(on page 931)*, Google Cloud *(on page 944)*, or Predix Cloud *(on page 949)*.

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 must be unique.

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 912)*.

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 775)*.
- 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>`. 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.

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 Historian in Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, 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.

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 *(on page 920)*, AWS Cloud *(on page 925)*, Azure Cloud *(on page 931)*, Google Cloud *(on page 944)*, or Predix Cloud *(on page 949)*.

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 must be unique.

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
	Continuous data collection is resumed only after the previous data has been recovered.
	The default value is 0 hours.
Throttle (Milliseconds)	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.

18. If needed, enter values in the available sections .

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 775)*.
- 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>`. 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 *(on page 920)*, AWS Cloud *(on page 925)*, Azure Cloud *(on page 931)*, Google Could *(on page 944)*, and Predix Cloud *(on page 949)*. 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 1. 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 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.

Table 1. The General Section (continued)

Field	Description
	The default value is 20.
Minimum Free Space (MB)	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.
Total Events Collected	This field is disabled.
Total Events Reported	This field is disabled.

Table 2. The Tags section

Field	Description
Tag Prefix	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.
	This field applies to all collectors except File and Calculation collectors.
Collection Interval Value	The interval at which the collector collects data for all the tags configured in the collector instance.
	• 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.
	You can set this value for each tag as well.

Table 2. The Tags section (continued)

Field	Description
	⚠ **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.
Collection Interval	The units of measure for the collection interval value.

Collection Type	The type of the data collection:
	
	• **Polled:** Data is collected based on a scheduled time interval. This type of data collection is supported only for:
	  ◦ 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:
	  ◦ 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 2. The Tags section (continued)

Field	Description
	◦ The Server-to-Server distributor
	◦ The Wonderware collector
Time Assigned By	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.

Table 3. The Collector Compression Section

Field	Description
Collector Compression	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.
Deadband	Indicates whether you want to apply a deadband based on the percentage of values or on absolute values.
	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.
	Note: If the data quality changes from good to bad or vice versa, the values are stored in

Table 3. The Collector Compression Section (continued)

Field	Description
	Historian regardless of the deadband value.
Deadband Value	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.
	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.
Compression Timeout	The time for one poll cycle for which collector compression is not used, thus sending all the samples to Historian.
	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.
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

Table 3. The Collector Compression Section (continued)

Field	Description
	spike, and retains a more accurate picture of the data leading up to it.
Multiplier	Specifies how much larger a spike value must be than the deadband range before the spike logic is invoked.
	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.
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 4. 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.
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	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

Table 4. The Collector Options Section (continued)

Field	Description
	and the collector machine, independent of time zone or daylight saving differences.
	Note: • 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.
Delay Collection at Startup (sec)	The duration, in seconds, after which you want the data collection to begin post tag configuration.

Table 5. The Advanced Section

Field	Description
Debug Mode	The debug mode for collector logs. 0 indicates normal log level, whereas 255 indicates that debugging is enabled. **Note:** Leaving the debug mode enabled for a long time consumes disk space.
Message Compression	Indicates whether you want to apply message compression.

Table 6. The Collector Status Output Section

Field	Description
Rate Output Address	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.
	You must enter the address of a writable analog field.
	For example, for an iFIX collector, enter the address of an iFIX tag in the following format: `<node name>.<tag name>.<field name>` (for example, `MyNode.MySIM_AO.F_CV`).
Status Output Address	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.
	You must enter the address of a writable text field of at least eight characters.
	For an iFIX collector, use TX tag for the output address. Enter the address in the following format: `<node name>.<tag name>.<field name>` (for example, `MyNode.MyCollector_TX.A_CV`).
Heartbeat Output Address	The address in the source database into which the collector writes the heartbeat signal output. Values are captured once a minute.
	You must enter the address of a writable analog field.
	For an iFIX data collector, use an iFIX tag for the output address. Enter the address in the following

Table 6. The Collector Status Output Section (continued)

Field	Description
	format: `<node name>.<tag name>.<field name>` (for example, `MyNode.MyCollector_TX.A_CV`). You can program the iFIX database to generate an alarm if values are not written every minute, notifying you that the collector has stopped.

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**.

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 Historian in Configuration Hub *(on page 765)*.

7. 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.

9. 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.

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. 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: `<product name>.iot-as-mqtt.<region ID>.aliyuncs.com`. A value is required. For example: `a23dr53dwrt.iot-as-mqtt.cn-shanghai.aliyuncs.com`
PORT	Enter `1883`. A value is required.

CLIENT ID	Enter a value in the following format: `<device name>|securemode=<value>,signmethod=<algorithm name>`. A value is required.
	
	  ◦ 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: `MyDevice|securemode=3,signmethod=hmacsha1`

TOPIC	Enter a value in the following format: `/sys/<product name>/<device name>/thing/event/property/post`. A value is required. For example: `/sys/a23dr53dwrt/MyDevice/thing/event/property/post`
USERNAME	Enter a value in the following format: `<device name><product name>`. A value is required. For example: `MyDevicea23dr53dwrt`
PASSWORD	Enter the password that you have generated. A value is required.

Field	Description
CHOOSE CONFIGURATION	Select the type of the configuration to specify the tags whose data you want to collect. Select one of the following options: ◦ **Historian Configuration**: Select this option if you want to add the tags manually using Historian Administrator. 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: `<installation folder of Historian>\GE Digital\<collector name>`

14. Select **Next**.

    The **Collector Initiation** section appears.

15. Enter a unique collector name.
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 775)*.

    - 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.
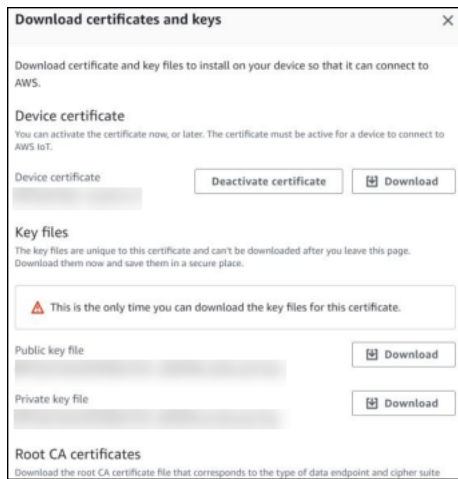
> ⚠ **Important:**
>
>   This is mandatory, and it is the only time you can download the certificates.

6. In the left navigation pane, select **Settings**.
7. Make a note of the endpoint that appears.
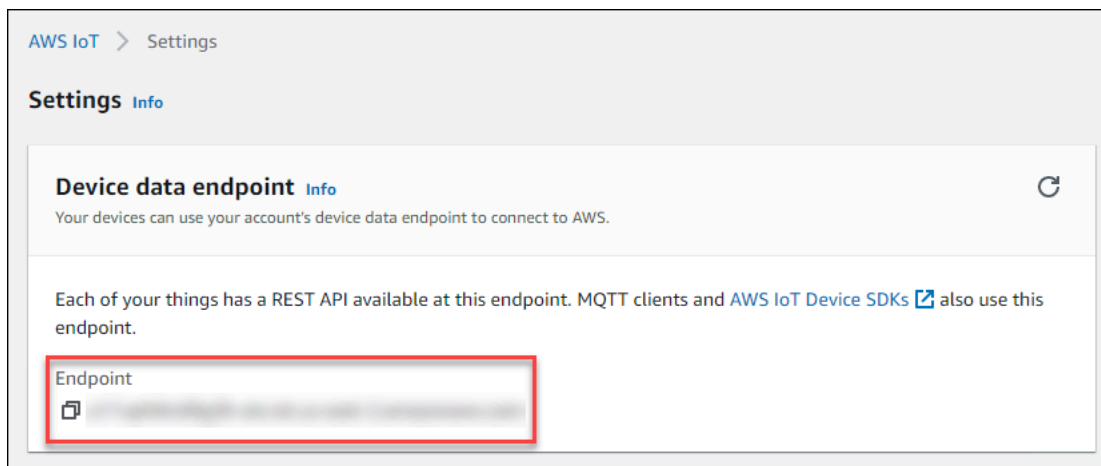
8. Access Historian in Configuration Hub *(on page 765)*.

9. 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

WIN10TECH

Refreshed on 2021-12-21 16:10:40

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
Filter	Filter	Filter	Filter
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 ╋.

SYSTEM

WIN10TECH

Refreshed on 2021-12-21 16:10:40

COLLECTOR NAME	STATUS	CONFIGURATION	MACHINE
Filter	Filter	Filter	Filter
WIN10TECH_Distributor	● Unknown	Historian	WIN10TECH
WIN10TECH_Simulation ⚑	● Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	● Unknown	Historian	WIN10TECH

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.

12. 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.

13. Select **Next**.

The **Source Configuration** section appears, populating the hostname of the collector machine.

14. 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	Select the type of the configuration to specify the tags whose data you want to collect. Select one of the following options: ◦ **Historian Configuration**: Select this option if you want to add the tags manually using Historian Administrator. 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: `<installation folder of Historian>\GE Digital\<collector name>`

16. Select **Next**.

The **Collector Initiation** section appears.

17. Enter a unique collector name.

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 775)*.

    ◦ 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.

> ℹ️ **Tip:**
>
> To find out the message size, modify the collector instance *(on page 962)* 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}] ,"messa`

You can also send data in the KairosDB format *(on page 939)*.

> **✎ 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:
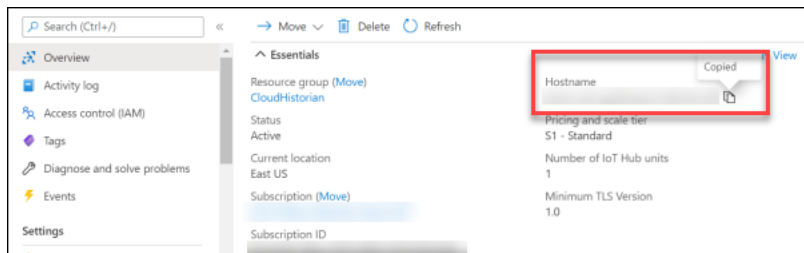
3. Create devices in Azure IoT Hub to group related tag information; thus mapping a collector instance to a device. We recommend that you create one device per collector instance. Ensure that the device is running.

    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 Historian in Configuration Hub *(on page 765)*.

6. In the **NAVIGATION** section, 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.

9. 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.

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.

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

Field	Description
	and must be in the following format: `<Azure IoT Hub name>.azure-devices.net`
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 `devices/<device ID>/messages/events`.

AUTO REFRESH	Indicates whether you want to automatically create/refresh the SAS authentication token when it expires.
	
	   ◦ 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.
	
	This is applicable only if you have selected **Symmetric Key** in step 3.

USERNAME	Enter a value in the following format: `<host name or IP address>/<device ID>/?api-version=2018-06-30`
PASSWORD	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. 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.
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**

Field	Description
	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/IoTMQTTSample/blob/master/IoTHubRootCA_Baltimore.pem.
CLIENT CERTIFICATE	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: ○ **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.
PRIVATE KEY FILE	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: ○ **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	Enter the path to the public key file. This is applicable only if you have selected one of these options in step 3: ○ **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.

Field	Description
CHOOSE CONFIGURATION	The type of the configuration to specify the tags whose data you want to collect. Select one of the following options: ○ **Historian Configuration**: Select this option if you want to add the tags manually (on page 775). 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: `<installation folder of Historian>\GE Digital\<collector name>`
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 unique collector name.

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 775)*.

    ◦ 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 931)*.

> 📝 **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.

   > ℹ️ **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.
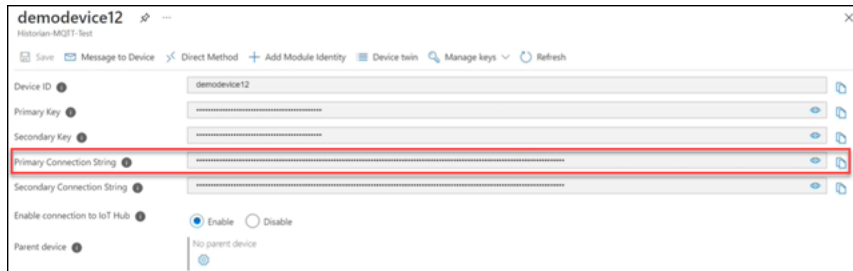
4. Access Historian in Configuration Hub *(on page 765)*.

5. In the **NAVIGATION** section, 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.

8. 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.

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.

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: ◦ HTTP ◦ MQTT ◦ AMQP

Field	Description
	◦ MQTT_OVER_WEBSOCKETS ◦ AMQP_OVER_WEBSOCKETS For information on which protocol to use, re-fer to Protocols and Port Numbers *(on page 955)*.
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 ac-cess web resources outside of the network, then you must provide the proxy server set-tings. However, it does not affect the proxy server used by Windows when establishing se-cure 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	The type of the configuration to specify the tags whose data you want to collect. Select one of the following options: ◦ **Historian Configuration**: Select this op-tion if you want to add the tags manually *(on page 775)*. If you select this option, the **CONFIGURATION HISTORIAN SERV-ER** field appears. ◦ **Offline Configuration**: Select this option if you want to provide the tag names us-ing the offline configuration file instead of adding tags manually. By default, this file is located in the following location:

Field	Description
	`<installation folder of His-torian>\GE Digital\<collector name>`
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 unique collector name.
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 775)*.
   ◦ 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 Historian in Configuration Hub *(on page 765)*.

6. In the **NAVIGATION** section, 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 ▽
Filter	*Filter*	*Filter*	*Filter*
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 ＋.

SYSTEM WIN10TECH ⌄			
Refreshed on 2021-12-21 16:10:40 ↻ │ + ⚙			
COLLECTOR NAME ▽	STATUS ▽	CONFIGURATION ▽	MACHINE ▽
Filter	*Filter*	*Filter*	*Filter*
WIN10TECH_Distributor	● Unknown	Historian	WIN10TECH
WIN10TECH_Simulation ⚑	● Running	Historian	WIN10TECH
WIN10TECH_To_WIN10TECH	● Unknown	Historian	WIN10TECH

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.

14. Select **MQTT**, and provide values as described in the following table.

Field	Description
HOST ADDRESS	Enter `mqtt.googleapis.com`. A value is required.
PORT	Enter `8883` or `443`.
CLIENT ID	Enter the ID of the device that you created in the following format: `projects/<project ID>/locations/<cloud region>/reg-istries/<registry ID>/devices/<device ID>`. For example: `projects/mygcpproject/loca-tions/asia-east1/registries/testmqttgcpi-ot/devices/gcptesting` A value is required and must be unique for an MQTT broker.
TOPIC	Enter `devices/<device ID>/events`.

Field	Description
AUTO REFRESH	Indicates whether you want to automatically re-fresh the authentication token when it expires. 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	The type of the configuration to specify the tags whose data you want to collect. Select one of the following options: ◦ **Historian Configuration**: Select this option if you want to add the tags manually (on page 775). 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
	`<installation folder of Historian>\GE Digital\<collector name>`
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 unique collector name.
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**.
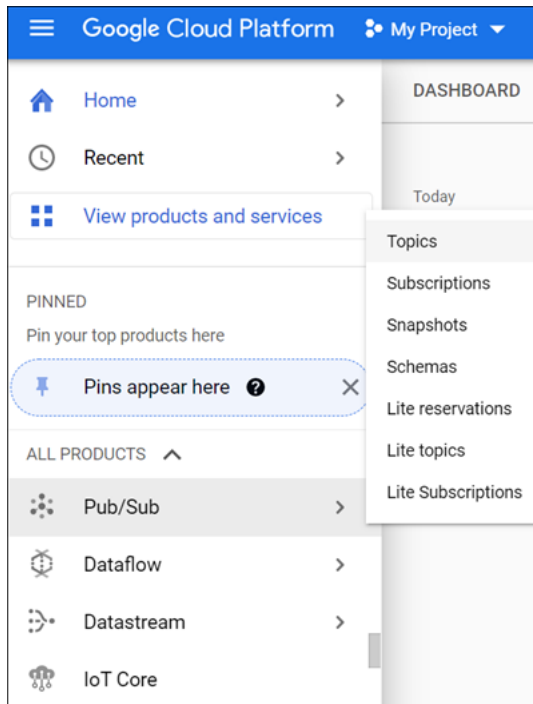
20. Select **Messages > PULL**.

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 Historian in Configuration Hub *(on page 765)*.
3. 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.

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.

6. 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.

7. Select **Next**.

   The **Source Configuration** section appears, populating the hostname of the collector machine.

8. 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.

Field	Description
	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 `time-series.zones. {ZoneId}.ingest` and `time-series.zones.{ZoneId}.query` authorities are granted access to the client for the Predix Zone ID specified. Your Predix Time Series administrator can provide this information.
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.

Field	Description
DATAPOINT 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	The type of the configuration to specify the tags whose data you want to collect. Select one of the following options: ◦ **Historian Configuration**: Select this option if you want to add the tags manually (on page 775). 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: `<installation folder of Historian>\GE Digital\<collector name>`
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.

10. Select **Next**.

    The **Collector Initiation** section appears.

11. Enter a unique collector name.

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 775)*.

     ◦ 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
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.

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.

You can then add a collector instance. This section describes how to add a collector instance using Configuration Hub *(on page 774)*. 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 Historian in Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, 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.

Column	Description
STATUS	The status of the collector. Contains one of the following values: ◦ **Started** ◦ **Stopped** ◦ **Running** ◦ **Paused**
CONFIGURATION	The source of the tag configuration for the collector. Contains one of the following values: ◦ **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.
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.

Column	Description
REDUNDANCY	Indicates whether collector redundancy is enabled, which decreases the likelihood of lost data due to soft- ware or hardware failures.
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 filter the collectors by the system name.
>
>
>
> You can also add, reorder, and remove columns from the table. For instructions, refer to
> Common Tasks in Configuration Hub *(on page 770)*.

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**.

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 Historian in Configuration Hub .
2. In the **NAVIGATION** section, select **Collectors**.

   A list of collectors appears.

   > **ⓘ Tip:**
   >
   > You can filter the collectors by the system name.
   >
   > | SYSTEM |
   > | WIN10TECH ⌄ |
   >
   > Refreshed on 2021-12-20 14:29:16 ↻ | + ⚙
   >
   > | COLLECTOR NAME | STATUS | CONFIGURATION | MACHINE |
   > | --- | --- | --- | --- |
   > | *Filter* | *Filter* | *Filter* | *Filter* |
   > | WIN10TECH_Distributor | ● Unknown | Historian | WIN10TECH |
   > | WIN10TECH_Simulation ⚑ | ● Running | Historian | WIN10TECH |
   > | WIN10TECH_To_WIN10TECH | ● Unknown | Historian | WIN10TECH |

3. Right-click the collector instance whose tags you want to access (or select ⠿), and then select **Browse Tags**.

A list of tags for which the 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.

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 845)*
- The CygNet collector *(on page 848)*
- The File collector *(on page 852)*
- The HAB collector *(on page 855)*

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 in unknown, you cannot modify it.
> - You cannot modify the instance of an offline collector.

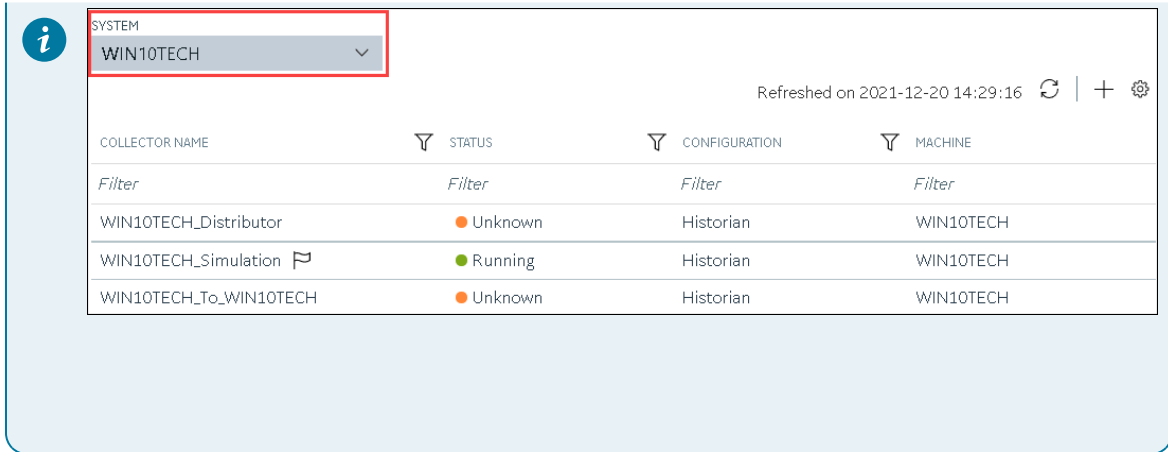1. Access Historian in Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, select **Collectors**.
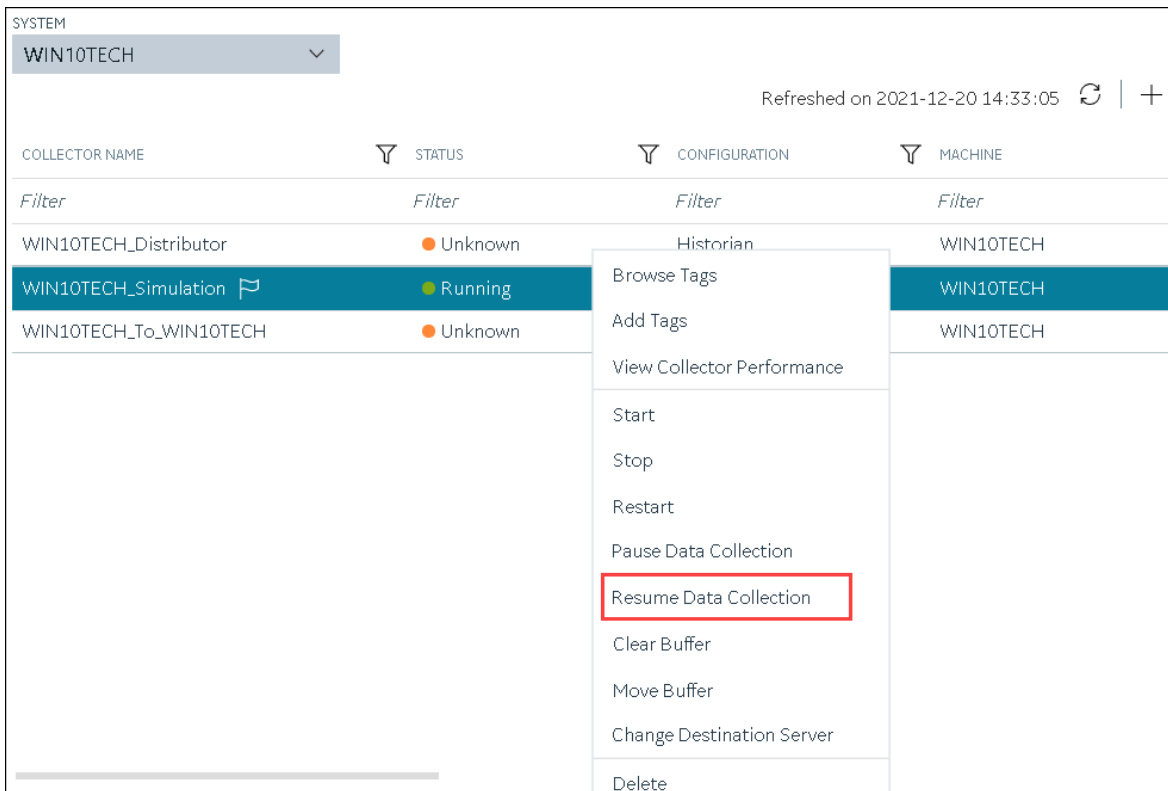
   A list of collectors appears.

   > **Tip:**
   > You can filter the collectors by the system name.

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 912)*.

   > **Note:**
   >
   > You cannot modify the destination of a collector.

5. In the upper-left corner of the page, select **Save**.
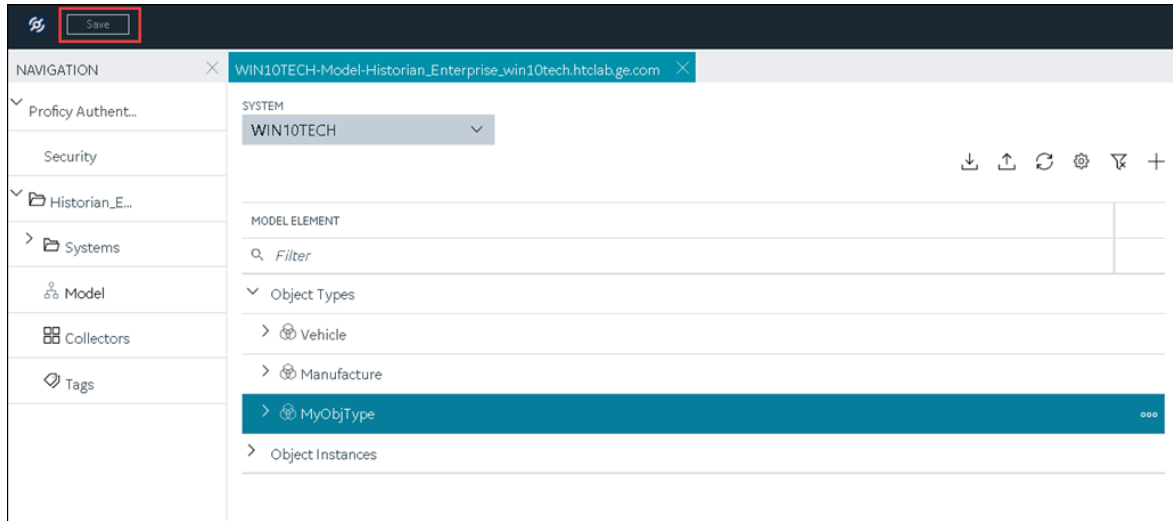
The changes to the collector instance are saved.

> **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.
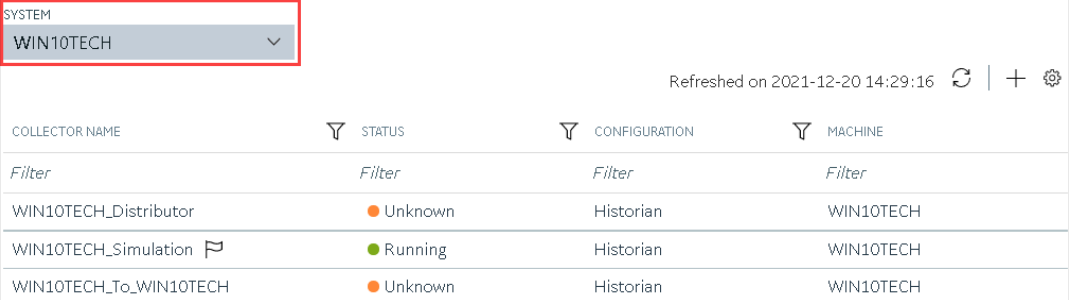
> **Note:**
>
> - You cannot modify or delete comments.
> - You cannot add comments to offline collectors.

1. Access Historian in Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, select **Collectors**.

A list of collectors appears.

> **i** **Tip:**
>
> You can filter the collectors by the system name.
>
> | SYSTEM | | | |
> |---|---|---|---|
> | WIN10TECH ∨ | | | |
> | | | Refreshed on 2021-12-20 14:29:16 ⟳ \| + ⚙ | |
> | COLLECTOR NAME ▽ | STATUS ▽ | CONFIGURATION ▽ | MACHINE ▽ |
> | *Filter* | *Filter* | *Filter* | *Filter* |
> | 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.

   > **i** **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 Historian in Configuration Hub .
2. In the **NAVIGATION** section, select **Collectors**.

   A list of collectors appears.

   > **i** **Tip:**
   >
   > You can filter the collectors by the system name.

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.

   > **ⓘ 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 Historian in Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, select **Collectors**.

   A list of collectors appears.

> **i** **Tip:**
>
> You can filter the collectors by the system name.
>
>

3. Right-click the collector instance that you want to start (or select ![dots]), and then select **Start**.

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 971)*.

1. Access Historian in Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, select **Collectors**.

    A list of collectors appears.

> **Tip:**
>
> You can filter the collectors by the system name.
>
> | SYSTEM | | | |
> | --- | --- | --- | --- |
> | WIN10TECH ⌄ | | | |
> | | | | Refreshed on 2021-12-20 14:29:16   ⟳ \| + ⚙ |
> | COLLECTOR NAME | ▽ STATUS | ▽ CONFIGURATION | ▽ MACHINE |
> | *Filter* | *Filter* | *Filter* | *Filter* |
> | 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**.

The **Stop: <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 **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.

1. Access Historian in Configuration Hub *(on page 765)*.

2. In the **NAVIGATION** section, select **Collectors**.

   A list of collectors appears.

   > **ⓘ Tip:**
   >
   > You can filter the collectors by the system name.
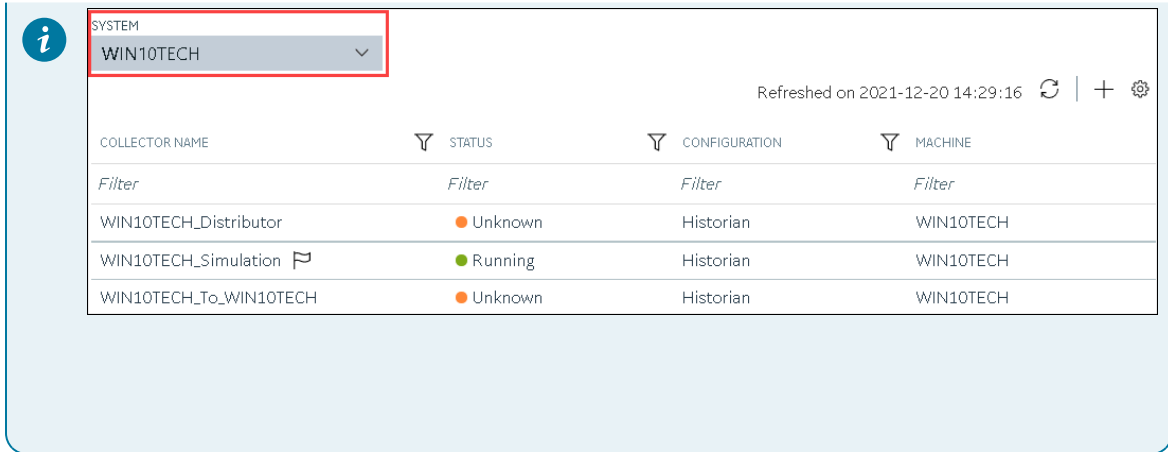
3. Right-click the collector instance that you want to restart (or select), and then select **Restart**.
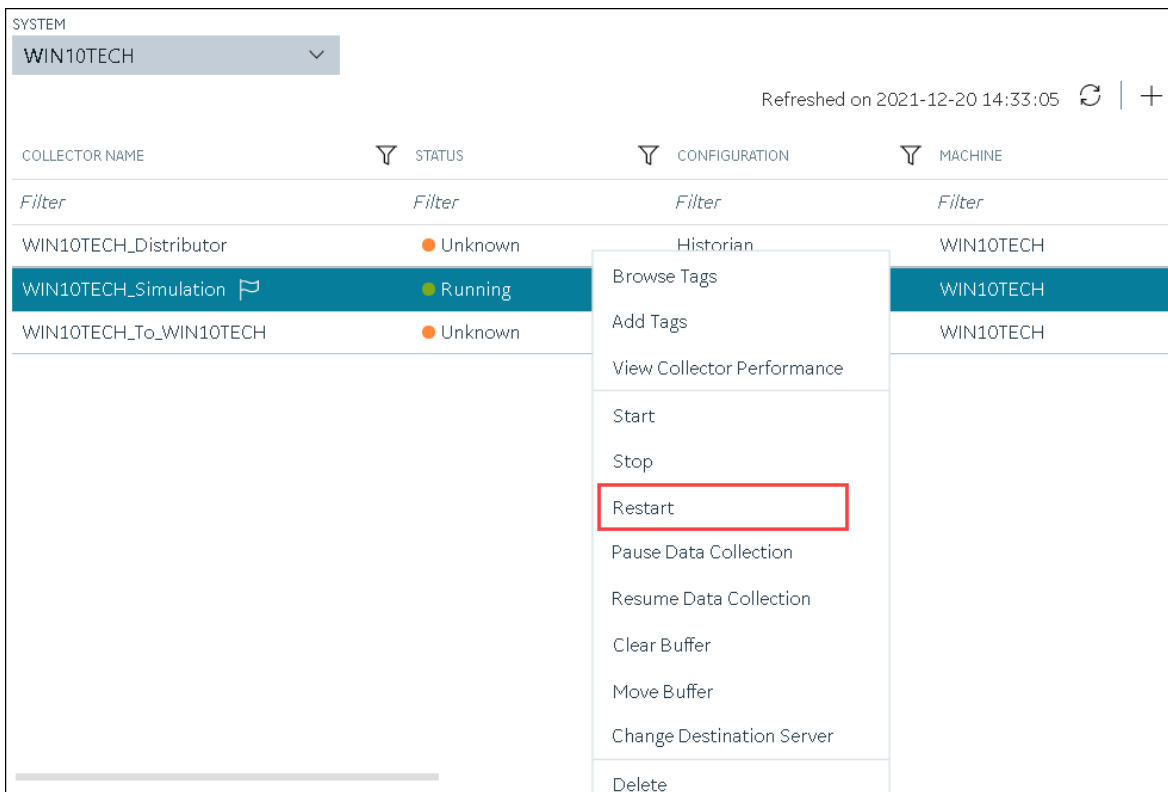
The **Restart: <collector name>** window appears. The **COLLECTOR MACHINE** and **CURRENT RUNNING MODE** fields are populated and disabled.

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 968)*.

> **Note:**
>
> You cannot pause the data collection of an offline collector.

1. Access Historian in Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, select **Collectors**.

   A list of collectors appears.

   > **Tip:**
   >
   > You can filter the collectors by the system name.
   >
   >

3. Right-click the collector instance for which you want to pause data collection (or select), and then select **Pause Data Collection**.

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 Historian in Configuration Hub .
2. In the **NAVIGATION** section, select **Collectors**.

A list of collectors appears.

> ℹ️ **Tip:**
> You can filter the collectors by the system name.

3. Right-click the collector instance for which you want to resume data collection (or select), and then select **Resume Data Collection**.

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 Historian in Configuration Hub .
2. In the **NAVIGATION** section, select **Collectors**.

    A list of collectors appears.

    > **ⓘ Tip:**
    >
    > You can filter the collectors by the system name.
    >
    > | SYSTEM | | | |
    > | --- | --- | --- | --- |
    > | WIN10TECH ⌄ | | | |
    > | | | Refreshed on 2021-12-20 14:29:16 ↻ \| + ⚙ | |
    > | COLLECTOR NAME ▽ | STATUS ▽ | CONFIGURATION ▽ | MACHINE ▽ |
    > | *Filter* | *Filter* | *Filter* | *Filter* |
    > | 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**.

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 Historian in Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, select **Collectors**.

A list of collectors appears.

> **ⓘ Tip:**
>
> You can filter the collectors by the system name.
>
> | SYSTEM | | | |
> | --- | --- | --- | --- |
> | WIN10TECH ⌄ | | | |
> | | | Refreshed on 2021-12-20 14:29:16 ↻ \| + ⚙ | |
> | COLLECTOR NAME | ▽ STATUS | ▽ CONFIGURATION | ▽ MACHINE |
> | *Filter* | *Filter* | *Filter* | *Filter* |
> | 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.

2. In the **NAVIGATION** section, select **Collectors**.

   A list of collectors appears.

3. Right-click the collector instance whose destination server you want to change (or select), and then select **Change Destination Server**.

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 969)*.

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 Historian in Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, select **Collectors**.
   A list of collectors appears.

> **Tip:**
> You can filter the collectors by the system name.
>
> | SYSTEM | | | |
> |---|---|---|---|
> | WIN10TECH ⌄ | | | |
> | | | | Refreshed on 2021-12-20 14:29:16 ⟳ ︙ + ⚙ |
> | COLLECTOR NAME ▽ | STATUS ▽ | CONFIGURATION ▽ | MACHINE ▽ |
> | *Filter* | *Filter* | *Filter* | *Filter* |
> | 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**.

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 Tags for Data Collection

Specify Tags for Data Collection

- Add the collector instance *(on page 774)* 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 786)*.

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 983)*.

1. Access Historian in Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, select **Tags**.
3. In the upper-right corner of the main section, select $+$.

The **<system name> - Add Tag** section 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.

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 in the Historian documentation.

Add a Tag Manually

- Add the collector instance *(on page 774)* 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 786)*.

After you create a collector instance, you specify which tags from the source must be used for data collection *(on page 775)*. 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 Historian in Configuration Hub *(on page 765)*.
2. In the **NAVIGATION** section, select **Tags**.
3. In the upper-right corner of the main section, select ╋.
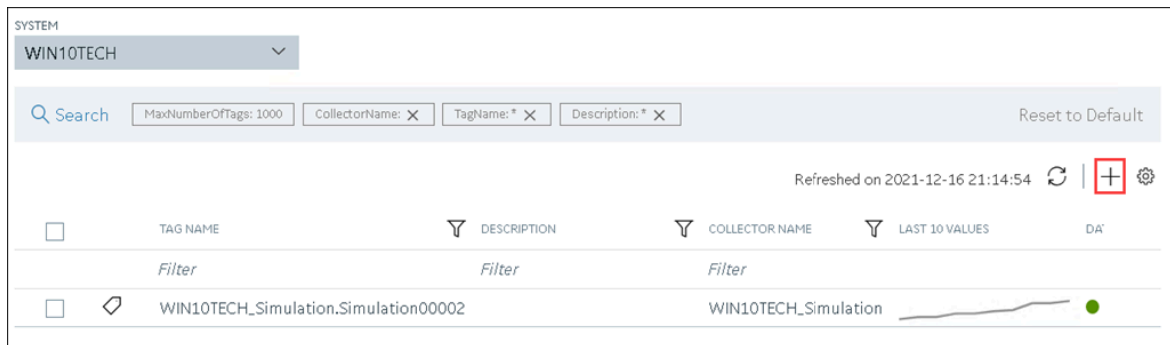
The **<system name> - Add Tag** page appears. The **Add Tags from Collector** option is selected by default.
4. Select **Add Manually**.

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.

Field	Description
	The value that you enter: ◦ 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: ~`+^:;,.?"*={}@
DATA TYPE	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. ⚠ **Important:** If you select an unsupported data type, you may receive incorrect data or even lose data. If you select **Multi-Field**, the **USER-DEFINED TYPE NAME** field appears, and the **ENUMERATED SET** and **ARRAY TAG** fields are disabled. If you select **Fixed String**, the **STRING LENGTH** field appears.
STRING LENGTH	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. You can enter a value between 1 and 255. The default value is 8.
USER-DEFINED TYPE NAME	Select the user-defined data type that you want to use for the tag. This field appears only if the value in the **DATA TYPE** field is **Multi-Field**. A value is required.

Field	Description
ENUMERATED SET	Select the enumerated set that you want to use for the tag. This field is not applicable for string and multi-field data types.
ARRAY TAG	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**.
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 that 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. For information on the delta query modes, refer to Counter Delta Queries in the Historian documentation.

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 Historian in Configuration Hub *(on page 765)*.
2. If you want to access all tags, in the **NAVIGATION** section, select **Tags**.

   A list of all the tags 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.
TAG ALIAS	Indicates whether the tag contains aliases, which are created when you rename the tag using an alias *(on page 993)*.

3. 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.

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.

4. 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.

5. Select the row containing the tag that you want to access.

The tag details appear in the **DETAILS** section.

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.

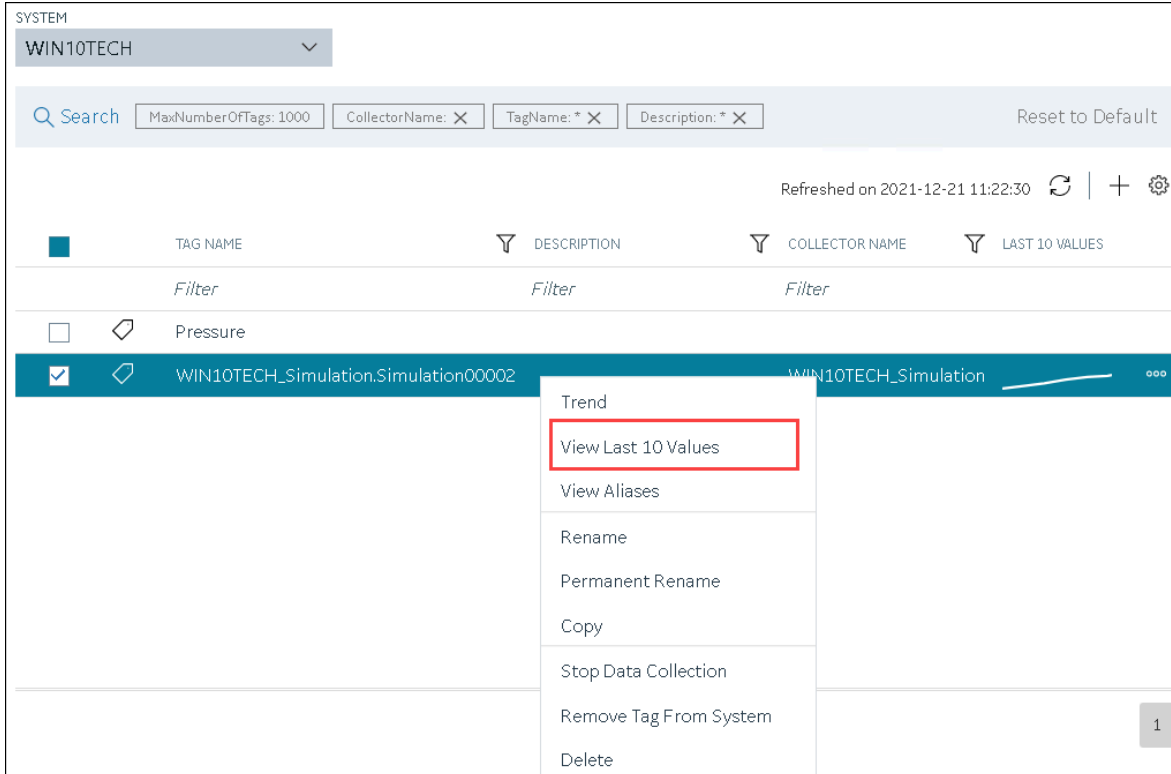1. Access Historian in Configuration Hub .
2. If you want to access all tags, in the **NAVIGATION** section, select **Tags**.

   A list of all the tags appears.
3. If you want to narrow down the search results, select **Search**.
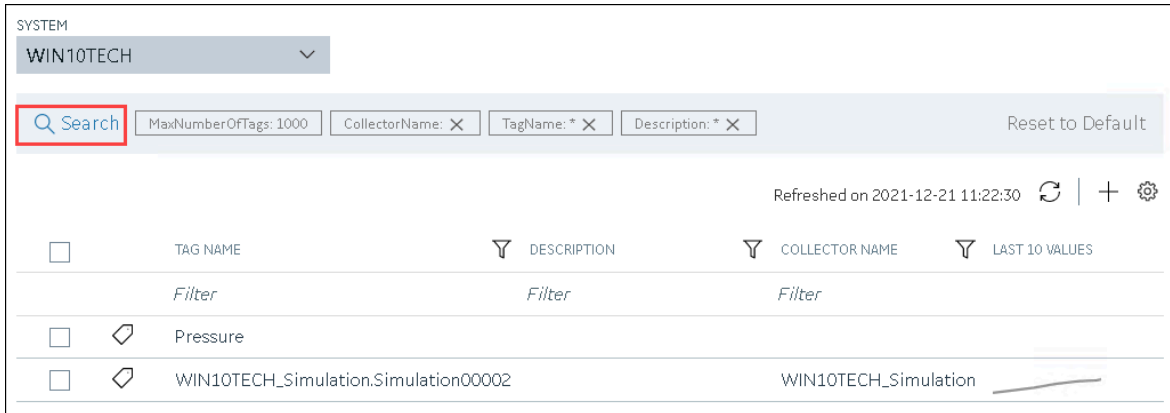
Enter the search criteria, and then select **Search**. You can add more attributes by selecting **Add Attribute**. You can enter a name or a value partially or use the wildcard character asterisk (*). The list of tags are filtered based on the search criteria.

4. If you want to access the trend chart of a single tag, right-click the tag (or select), and then select **Trend**.
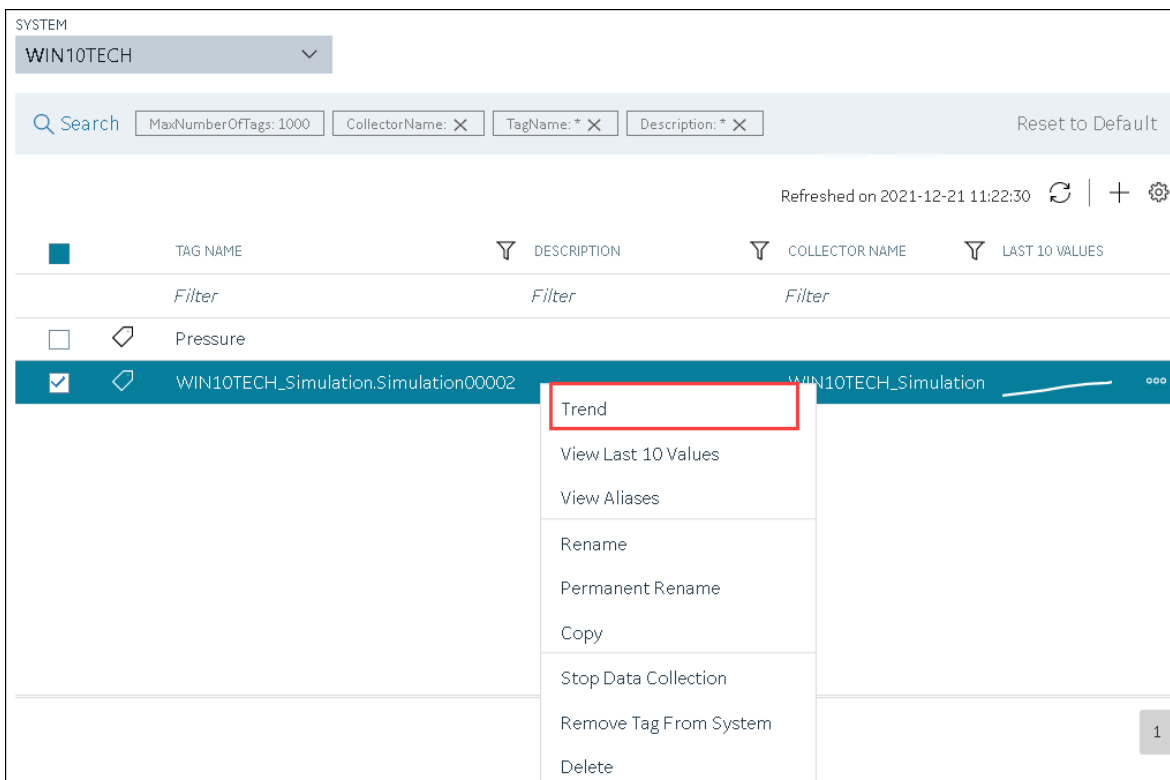
If you want to access the trend chart for multiple tags, select the check boxes corresponding to the tags, right-click (or select ⬚⬚⬚), and then select **Trend**. You can select up to 10 tags.

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 Historian in Configuration Hub *(on page 765)*.
2. If you want to access all tags, in the **NAVIGATION** section, select **Tags**.

   A list of all the tags appears.
3. If you want to narrow down the search results, select **Search**.
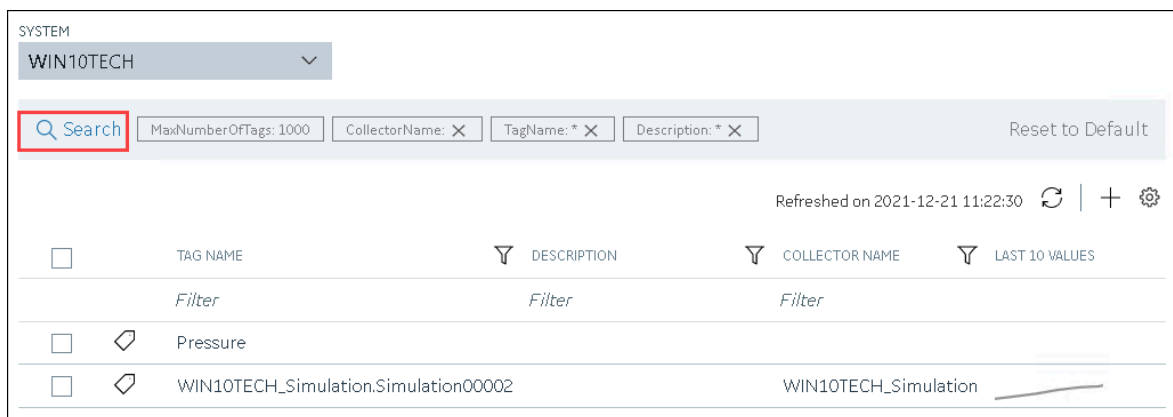
Enter the search criteria, and then select **Search**. You can add more attributes by selecting **Add Attribute**. You can enter a name or a value partially or use the wildcard character asterisk (*).

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 ⚬⚬⚬), and then select **View Last 10 Values**.

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 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 ▽.

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 Historian in Configuration Hub *(on page 765)*.
2. If you want to access all tags, in the **NAVIGATION** section, 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 Historian in Configuration Hub *(on page 765)*.
2. If you want to access all tags, in the **NAVIGATION** section, 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 rename (or select ⚆⚆⚆).
5. If you want to rename the tag using an alias, select **Rename**.

If you want to rename the tag permanently, select **Permanent Rename**.
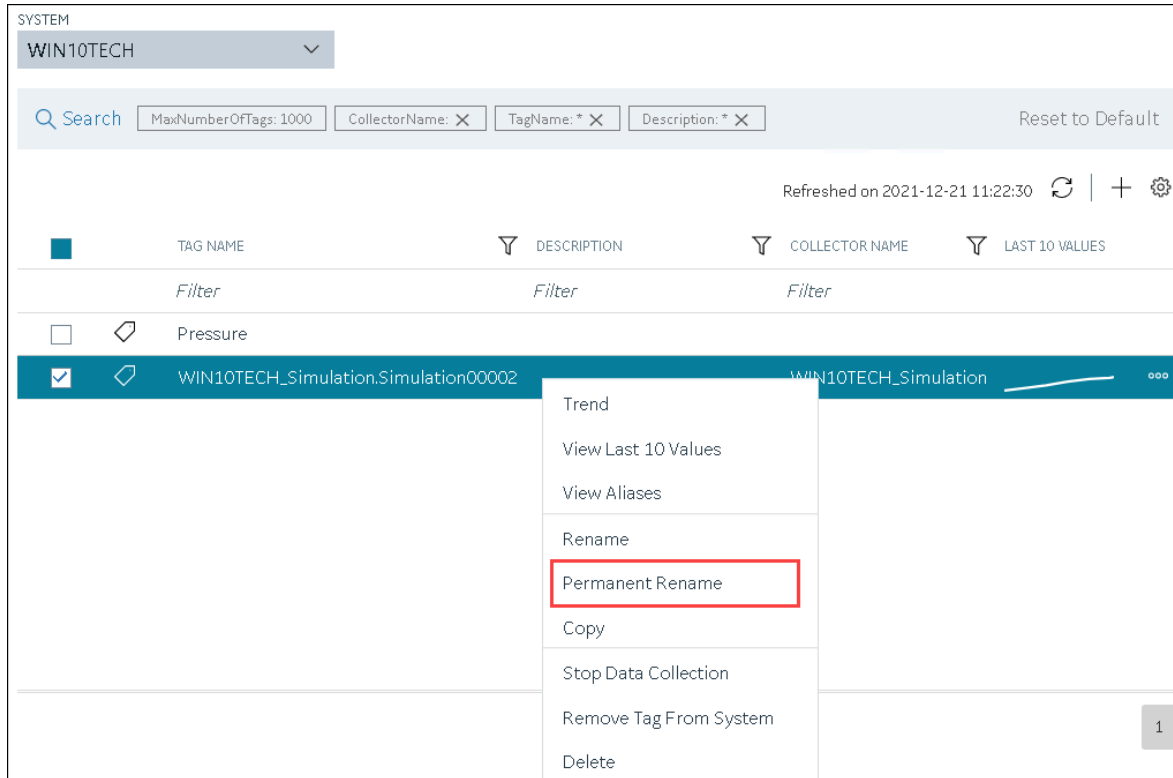
The **Rename Tag: <tag name>** window or the **Permanent Rename Tag: <tag name>** window appears.

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 969)*.

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 Historian in Configuration Hub *(on page 765)*.
2. If you want to access all tags, in the **NAVIGATION** section, 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 copy (or select), and then select **Copy**.
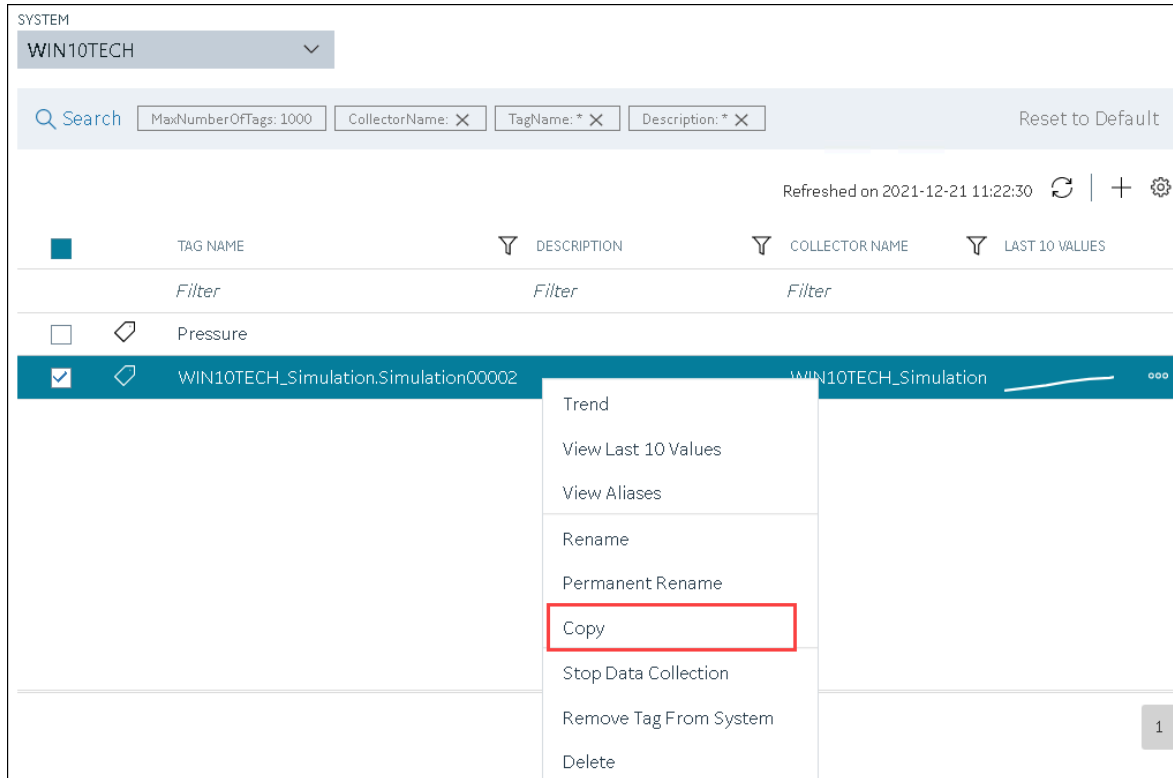
The **Copy Tag: <tag name>** window appears.

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 1000)* or delete it *(on page 1002)*.

1. Access Historian in Configuration Hub *(on page 765)*.

2. If you want to access all tags, in the **NAVIGATION** section, select **Tags**.

A list of all the tags appears.

3. If you want to narrow down the search results, select **Search**.
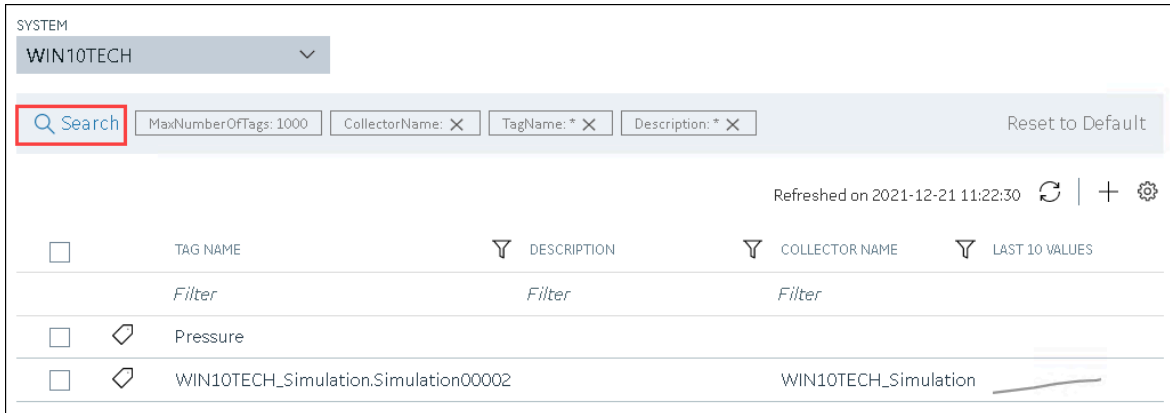
Enter the search criteria, and then select **Search**. You can add more attributes by selecting **Add Attribute**. You can enter a name or a value partially or use the wildcard character asterisk (*). The list of tags are filtered based on the search criteria.

4. Right-click the tag for which you want to stop data collection (or select ⦿⦿⦿), and then select **Stop Data Collection**.
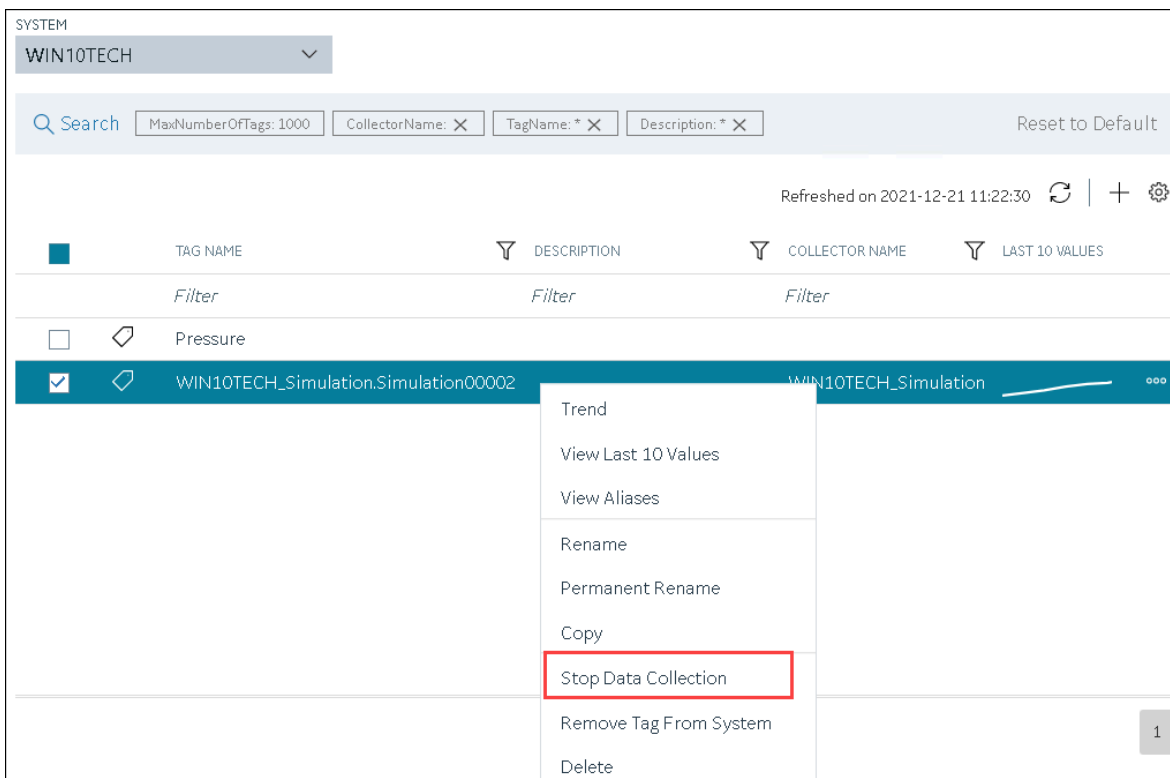
A message appears, asking you to confirm that you want to stop the data collection for the tag.

5. Select **Stop**.

Data collection is stopped for the tag.

Resume the Data Collection of a Tag

1. Access Historian in Configuration Hub *(on page 765)*.
2. If you want to access all tags, in the **NAVIGATION** section, 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 resume data collection (or select ⬤⬤⬤), and then select **Resume Data Collection**.

   A message appears, asking you to confirm that you want to resume the data collection for the tag.
5. Select **Resume**.

   Data collection is resumed 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 1002)*. Or, you can choose to stop the data collection *(on page 998)* for the tag, which allows you to resume the data collection *(on page 1000)* later.

1. Access Historian in Configuration Hub *(on page 765)*.

2. If you want to access all tags, in the **NAVIGATION** section, 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 remove (or select), and then select **Remove Tag From System**.
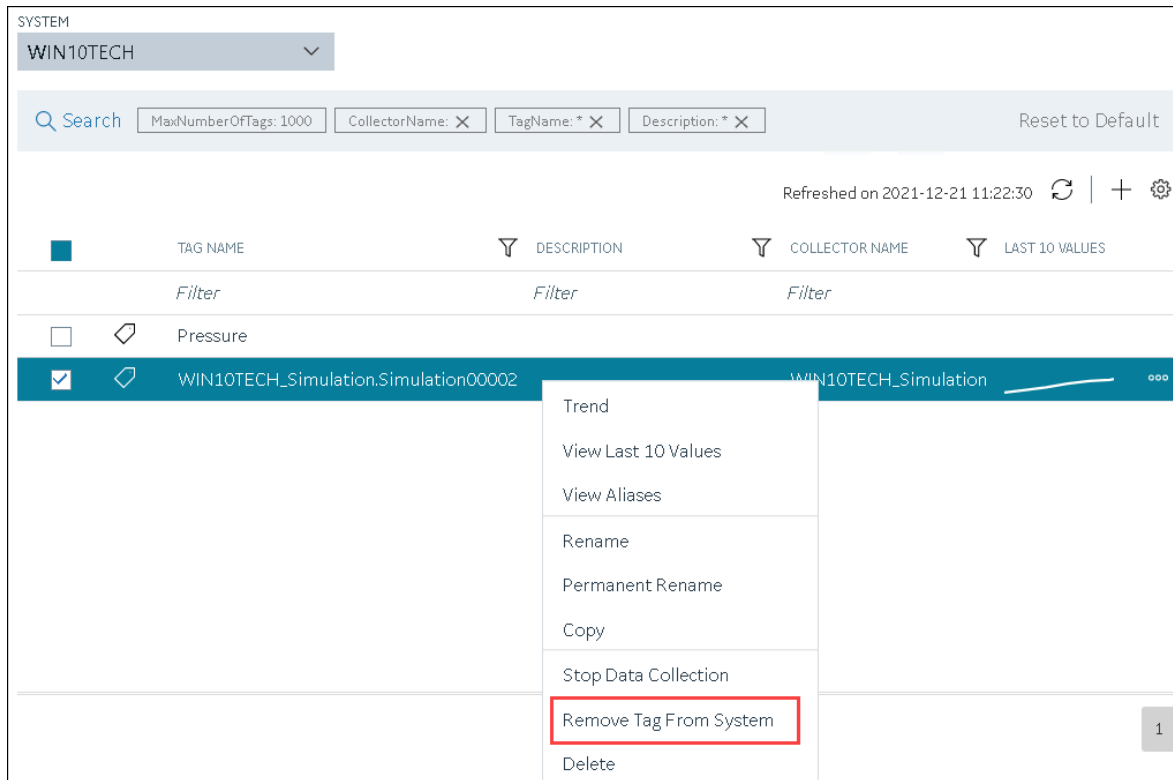
A message appears, asking you to confirm that you want to remove the tag from the system.

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 1000)*. Or, you can choose to stop the data collection *(on page 998)* for the tag, which allows you to resume the data collection *(on page 1000)* later.

1. Access Historian in Configuration Hub *(on page 765)*.
2. If you want to access all tags, in the **NAVIGATION** section, 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.

Troubleshooting Historian and Configuration Hub

This topic contains solutions/workarounds to some of the common issues encountered with Historian in Configuration Hub. This list is not comprehensive. If the issue you are facing is not listed on this page, refer to the Historian documentation.

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\confighub`
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

You can install Configuration Hub only in the C drive

Workaround:

1. Create Configuration Hub server certificates.
2. Start the ConfigHubNGINXService service.
3. Using the Web Based Clients Configuration tool *(on page 772)*, provide the Proficy Authentication and Configuration Hub details, test the connection, and select **Register** to re-register the Historian plugin with Configuration Hub.

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 page 772)* on the machine on which you have installed Web-based Clients, install the Proficy Authentication certificate *(on page 772)*, 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: While installing collectors and the Historian server on the same machine, if strict collector authentication is enabled, providing the user credentials is mandatory. Otherwise, an error occurs when you access the list of collectors or add a collector instance using Configuration Hub or the RemoteCollectorConfigurator utility.

To fix this issue, disable the strict collector authentication using Historian Administrator, and then restart the Historian Remote Collector Management Agent service.

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.

Chapter 5. 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 TestConfiguration 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 TestConfiguration Hub server or the iFIX server (or both when the TestConfiguration Hub server is local to the iFIX server). Be aware that the iFIX plugin will only be accessible in TestConfiguration Hub if the certificates are valid. If the host name is changed (in either TestConfiguration Hub or iFIX) and you did not update the certificates, then iFIX plugin may not be accessible in TestConfiguration Hub, as the certificates are not valid anymore. Use the following steps to update your certificates.

Steps for Self-Signed Certificate Creation Due to TestConfiguration Hub Server Host Name Change

During the TestConfiguration Hub install, self-signed certificates are created and stored in the C:\Program Files (x86)\GE\ConfigurationHub\ConfigHubPki folder. The TestConfiguration Hub nginx server certificates are stored in the C:\Program Files (x86)\GE\ConfigurationHub\Web\conf directory. If you want to change the web server name after the TestConfiguration Hub install, you need to update the self-signed certificates.

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

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

```
restart_confighub.bat "C:\Program Files (x86)\GE\ConfigurationHub" "C:\Program Files

 (x86)\GE\ConfigurationHub\Web" 5678 4890 htclab.ge.com
```

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

4. Copy the server_cert.crt and server_cert.key files the from C:\Program Files (x86)\GE\ConfigurationHub\ConfigHubPki folder to the C:\Program Files (x86)\GE\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)\GE\iFIX\LOCAL\iFIX_OpcuaConfigService\pki folder. The iFIX nginx server certificates are stored in the C:\Program Files (x86)\GE\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)\GE\iFIX\ folder. The iFIX Configuration Service Certificate Tool appears, similar to the following figure.
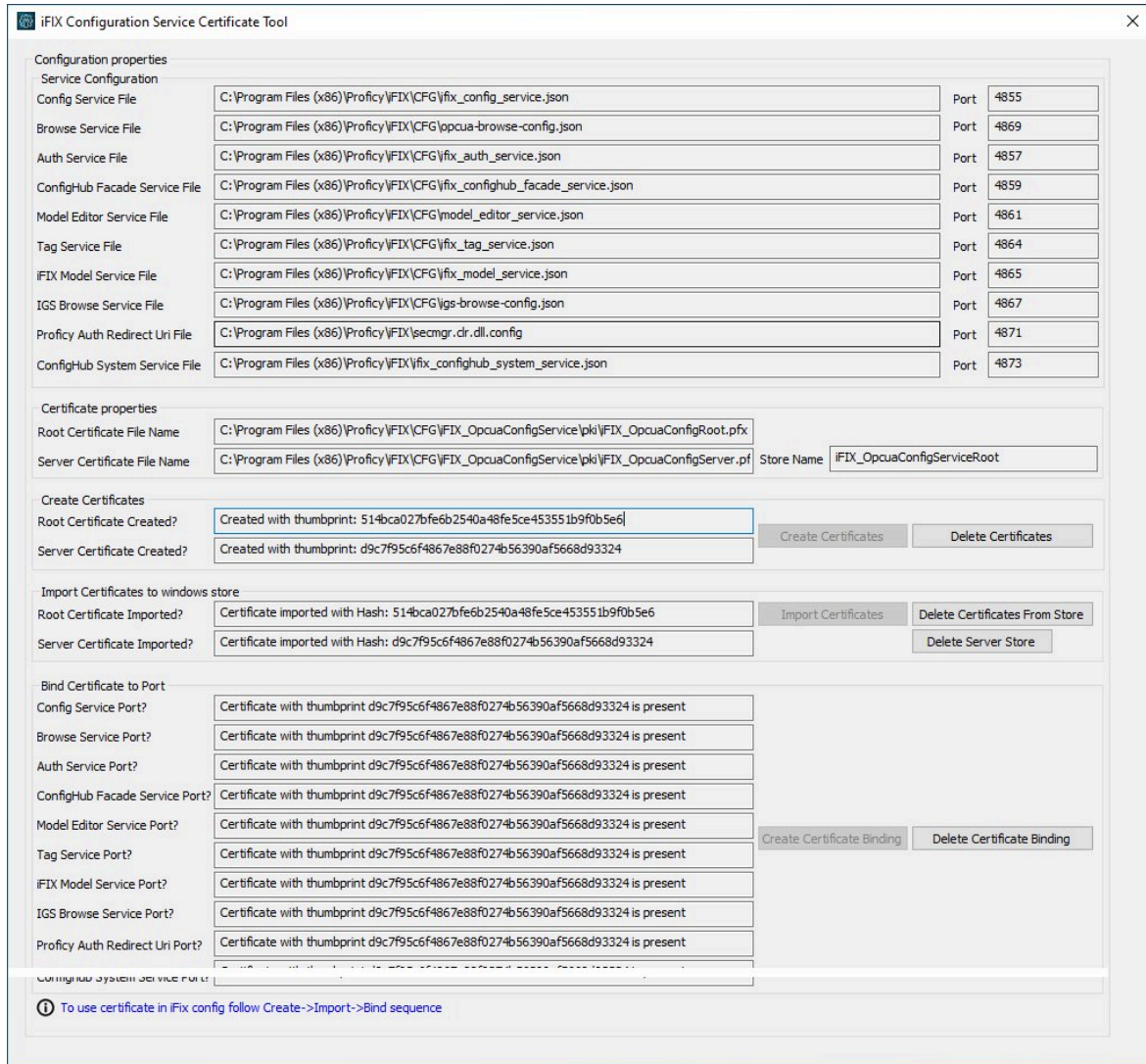
2. Click Delete Certificates, and then click Delete Certificate Binding.
3. From the Windows File Explorer, remove or backup the certificate files in C:\Program Files (x86)\GE\iFIX\LOCAL\iFIX_OpcuaConfigService\pki directory.
4. From iFIX Configuration Service Certificate Tool, create the new certificates 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:

After the new certificate creation, the thumbprint is:

6. Copy the iFIX_OpcuaConfigServer.crt and iFIX_OpcuaConfigServer.key files from C:\Program Files (x86)\GE\iFIX\LOCAL\iFIX_OpcuaConfigService\pki into the C:\Program Files (x86)\GE\iFIX\web \conf directory.

7. Restart the computer.

Port Changes for Configuration Hub

If you need to change the ports used by TestConfiguration Hub web server after install, use the ConfigHubSettingsUtility.exe utility found in the TestConfiguration Hub folder (by default this folder is: C: \Program Files (x86)\GE\ConfigurationHub) to reset them.

> ✎ **Note:**
> If you are planning to update the ConfigHub Server port number which is the TestConfiguration Hub web server, then you must update all plugins to update ConfigHub Server port change. Otherwise, the plugins cannot communicate with the TestConfiguration Hub. To update your iFIX plugin post install, use the Registration tool available in the iFIX WorkSpace; see iFIX Plugin Registration *(on page 88)* 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 6. 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.

Configuration Hub Log Files

By default, the logs for TestConfiguration Hub are saved to the following locations: C:\Program Files\GE\ConfigurationHub\Web\logs, and C:\Program Files\GE\ConfigurationHub\Logs.

IGS Log File

For IGS, the log file named igs-browse-config.log is located in the C:\Program Files (x86)\GE\iFIX\LOCAL folder, by default.

Historian Log Files

For Historian, the logs are stored in the default install path. This path can be the default: C:\Proficy Historian Data, or another custom path as specified during the Historian installation.

iFIX Log Files

For iFIX, the associated logs are in C:\Program Files (x86)\GE]iFIX\LOCAL\Logs folder, by default. The names of these files are:

Log Name	Description
ifix_auth_service.log	iFIX authentication service log file.
ifix_config_service.log	iFIX OPCUA Config Service log file.
ifix_confighub_facade_service.log	iFIX ConfigHub Facade service log file.
ifix_model_editor_service.log	Model editor service log file.
ifix_model_service.log	iFIX model service which is used for publishing model information to iFIX.
ifix_tag_service.log	iFIX tag service log file.

Log Name	Description
ifix_tag_validators.log	iFIX tag validator log file.
igs-browse-config.log	IGS browsing log file.

The following list are the .json files located in the iFIX LOCAL directory that are associated with the log files in the previous table:

- ifix_auth_service.json
- ifix_config.service.json
- ifix_confighub_facade_service.json
- ifix_model_service.json
- ifix_tag_service.json
- ifix_tag_validators.json
- igs-browse-config.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_auth_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.

```
{

        "AccessTokenExpiryInterval": 1800,

        "RefreshTokenExpiryInterval": 86400,

        "port": "4857",

        "secure" : true,

        "Clientid" : "admin",

        "ClientSecret" : "admin",

        "log" :
```

```
            {
         "enable": true,

         "name" : "ifix_auth_service.log",

         "level": "info",

         "max-size": 5242880,

         "max-files": 3,

         "flush-seconds": 10

            }

        }
```

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\Logs 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.