GE VERNOVA

PROFICY®SOFTWARE & SERVICES

# PROFICY iFIX HMI/SCADA

## OPC UA Server for iFIX

GE VERNOVA

**Proprietary Notice**
The information contained in this publication is believed to be accurate and reliable. However, GE Vernova assumes no responsibilities for any errors, omissions or inaccuracies. Information contained in the publication is subject to change without notice.

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

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

**Trademark Notices**
"GE VERNOVA" is a registered trademark of GE Vernova. The terms "GE" and the GE Monogram are trademarks of the General Electric Company, and are used with permission.

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

All other trademarks are the property of their respective owners.

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

# Table of Contents


**OPC UA Server for iFIX** ..... **1**

**Overview of the OPC UA Server** ..... **2**

Features of the OPC UA Server ..... 2

Limitations of the OPC UA Server ..... 2

Architecture Overview ..... 3

How the iFIX OPC UA Works ..... 3

**iFIX OPC UA Server Configuration** ..... **3**

iFIX OPC UA Configuration Workflow ..... 4

Quick Start ..... 6

OPC UA Server Configuration Tool ..... 6

Server ..... 7

Logging ..... 7

Security ..... 8

Alarms ..... 8

Certificate ..... 9

Trust List ..... 9

Browsing and Availability of the Address Space ..... 10

Subscribing to Alarms ..... 10

Subscribing to Tags ..... 10

Examples of Node IDs: ..... 10

Namespace URIs ..... 10

**Security Settings for the OPC UA Server** ..... **11**

Certificate Management and the OPC UA Server ..... 12

Use a Self-Signed Certificate for the OPC UA Server ..... 12

Use a GDS-Signed Certificate for the OPC UA Server ..... 13

About the Trust List ..... 13

Workflow for Self-Signed Certificate ..... 14

More on the Global Discovery Server ..... 14

iFIX Security and the OPC UA Server ..... 15


© 2018 General Electric Company. All rights reserved.

**Alarms and the iFIX OPC UA Server** ..... **15**
About Alarm Settings for the OPC UA Server ..... 16
Mapping of iFIX Alarm Types to OPC UA Alarm Types ..... 16
**Tag Types and Attributes** ..... **17**
Default Representation of iFIX Tag Types in the OPC UA Server ..... 17
Renaming Tag Types in the OPC UA Server's Address Space ..... 25
**Advanced** ..... **26**
Configure Logging for the OPC UA Server ..... 26
More on the Log Files ..... 27
Troubleshooting the OPC UA Server ..... 27
**Index** ..... **29**


© 2018 General Electric Company. All rights reserved.

# OPC UA Server for iFIX

This help system describes the OPC Unified Architecture (UA) Server for the iFIX product. It includes the following sections:


- Overview of the OPC UA Server
- OPC UA Server Configuration Tool
- Security Settings for the OPC UA Server
- Alarms and the iFIX OPC UA Server
- Tag Types and Attributes
- Advanced


© 2018 General Electric Company. All rights reserved.

# Overview of the OPC UA Server

The iFIX OPC UA Server implements OPC Unified Architecture (UA), which is a secure, scalable, multi-platform communication protocol. The iFIX OPC UA Server allows OPC UA Clients to access data and alarms in the iFIX database.

For example, you can use the OPC UA Server to share data in the iFIX Database with applications on your plant floor, with analytic tools, or with Enterprise Resource Planning (ERP) systems via OPC UA client interfaces.

As an add-on component to iFIX, the iFIX OPC UA Server only runs when enabled, and when a valid certificate has been issued to the server (OPC UA applications need certificates to communicate if communication, privacy, and authentication are enabled). iFIX requires a restart after any change to OPC UA Server configuration.

For more detailed information on the OPC UA Server, refer to the following sections:


- Features of the OPC UA Server
- Limitations of the OPC UA Server
- Architecture Overview


## Features of the OPC UA Server

The main features provided by the iFIX OPC UA Server include:

- OPC UA clients can read, write, and subscribe to changes in iFIX runtime database tags.
- OPC UA clients can subscribe to, view, and acknowledge alarms from the iFIX OPC UA Server.
- OPC UA clients can browse the iFIX tag database and alarm areas.
- OPC UA clients can subscribe to iFIX alarms by alarm area, or subscribe for all available alarms.
- A graphical user interface for OPC UA Server configuration.
- Privacy and integrity for information sent over the network ensured by the OPC UA protocol.
- Support for the OPC UA 1.04 specification for iFIX data and alarms.
- Support for centralized certificate management via the OPC UA GDS (Global Discovery Server) API.

## Limitations of the OPC UA Server

In general, limitations for the iFIX OPC UA Server include:

- The OPC UA Server and the OPC UA Configuration tool is only supported on the SCADA Server. Neither are supported on an iClient (View node) or Remote Desktop (Terminal Server) session.
- The OPC UA Server provides data and alarms only from the SCADA Server on which it is running. It does not provide access to data and alarms from other iFIX SCADAs.
- The Enhanced Failover feature is not supported for iFIX OPC UA Server. The OPC UA server


© 2018 General Electric Company. All rights reserved.

will provide data and alarms for the local SCADA only, regardless of its Active/Inactive failover state.

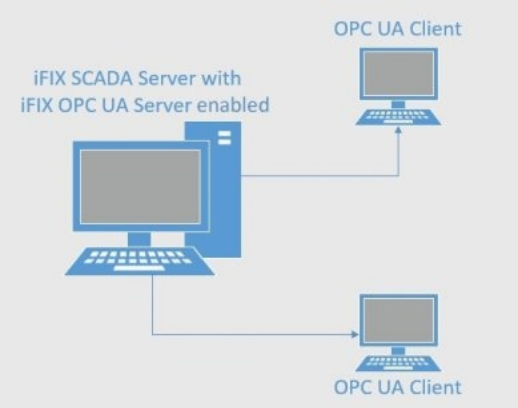
- The Electronic Signature feature is not supported for OPC UA Server access.
- Historical OPC UA data sources are not supported.
- OPC UA clients will not be able to perform alarm shelving; they will only be able to view the shelved state and changes to the state.
- The OPC UA Server cannot monitor more than 32,000 tag fields at a time.

## Architecture Overview

OPC Unified Architecture (UA) is a robust, scalable, flexible, and secure protocol used for exchanging information between industrial automation and control systems, and is well suited for IoT (Internet of Things) applications. OPC UA replaces the widely used OPC DCOM based standard (also called OPC Classic) and is designed to interoperate with existing OPC Classic installations. OPC UA is a true industrial interoperability standard for the Internet age.

Both OPC and OPC UA were developed by the not-for-profit OPC Foundation, which makes specifications for OPC UA available. For more detailed information on OPC UA, refer to the OPC Foundation web site: https://opcfoundation.org/

### How the iFIX OPC UA Works




Applications that use the OPC UA protocol have a client/server relationship. You can think of the iFIX OPC Servers as being producers of information, and OPC clients as being consumers:

- The *iFIX OPC UA Server* has data and alarms which are made available to other computers.
- The *OPC UA client* connects to the iFIX OPC UA Server to gain access to the data and alarms.

Since the OPC UA Server and OPC UA client are simply programs or applications, they can run on the same computer or different computers.

# iFIX OPC UA Server Configuration

© 2018 General Electric Company. All rights reserved.

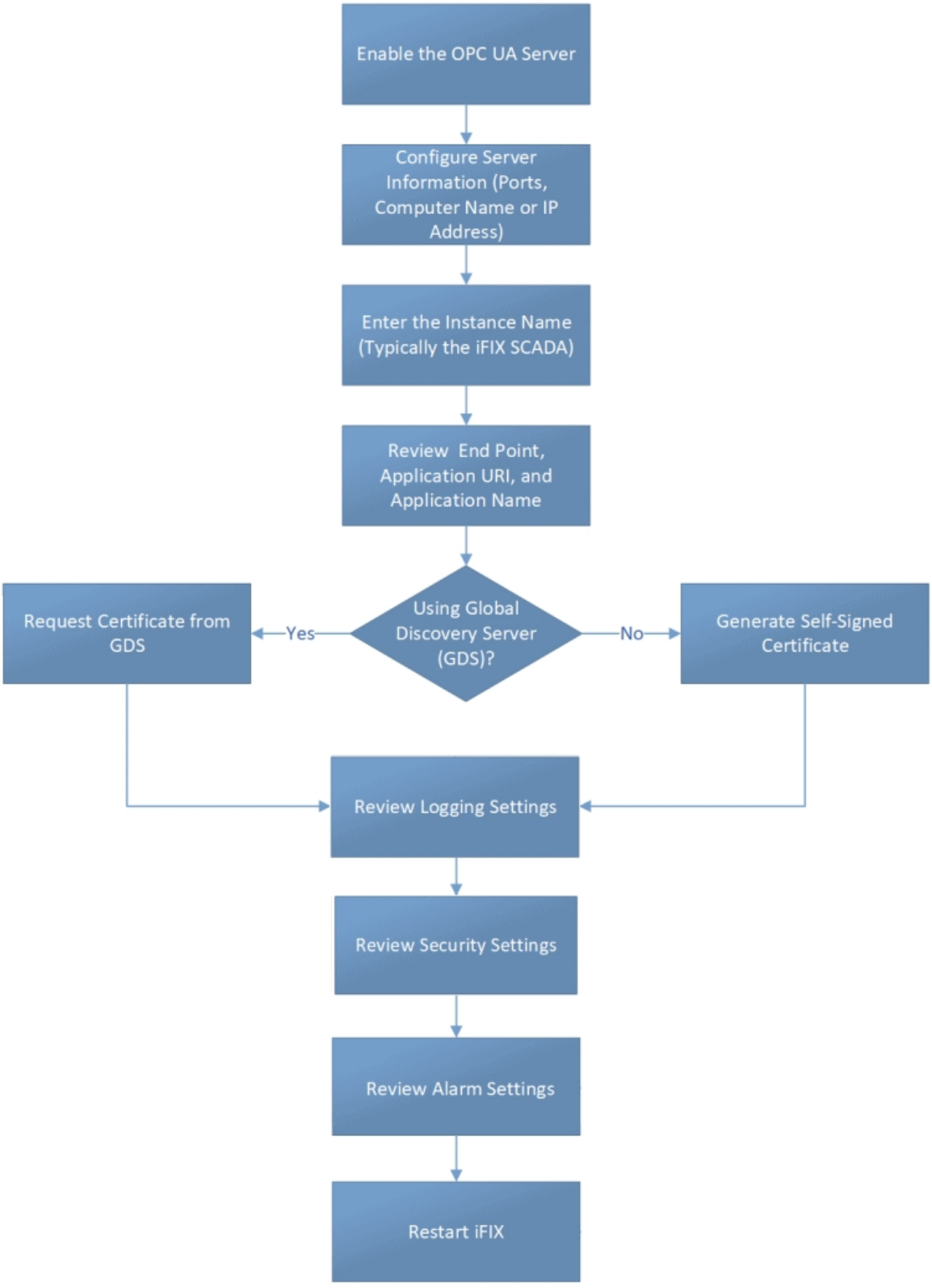
Configuration of the server includes server identification, logging setup, alarm setup, security setup, certificate configuration (self-signed or through a Global Discover Server (GDS)), and trust list management. When configuring the iFIX OPC UA Server you should review these sections:

- Quick Start
- OPC UA Server Configuration Tool

## iFIX OPC UA Configuration Workflow

The following figure illustrates the workflow for configuring your OPC UA Server. For detailed steps, refer to the Quick Start.


© 2018 General Electric Company. All rights reserved.




© 2018 General Electric Company. All rights reserved.

## Quick Start

To configure the OPC UA Server in iFIX:

1. From the ribbon bar on iFIX WorkSpace, select the Applications tab.
2. Select OPC UA Configuration. The Server Configuration Tool appears.
3. On the Server tab, select the Server Enabled option.
4. Review the default settings for port, network address, logical host name, instance name and other associated application information. Make changes as needed. The network address must be the computer name or an IP address, as this represents how clients will locate the OPC UA server. It is suggested to use the iFIX SCADA node name as the Instance name, but is not necessary.
5. On the Certificate tab, select Generate Self-Signed.
6. Optionally, on the Logging tab, review the logging settings. If the default level of logging is not detailed enough, you can change this value, but use caution in doing so. Using the highest levels of logging results in very verbose logging, and may impact performance and client connectivity. If you do select the highest level of logging, be sure to also enable the Optimize Log Output option to reduce disk access.
7. Optionally, on the Security tab, review the security settings.
8. Optionally, on the Alarms tab, select the Alarms Enabled option. Leave the defaults.
9. Select Save and Exit to save all your changes.
10. Restart iFIX. You must restart iFIX for your changes to take effect, as the OPC UA Server will start when iFIX starts.
11. After iFIX starts, using the Windows Task Manager, confirm that iFixUaServer.exe is a running process. If it is not there, check the iFixUaServer.log file in LOCAL\Logs folder.
12. Attempt to connect using an OPC UA Client with the server's URL. The first time you connect, a message will appear to trust the server certificate (depending upon the OPC UA client you are using, this message and how you trust the server can differ).
13. Trust the server certificate.
14. Try to connect the client again. The connection should be rejected with a BadSecurityChecksFailed error because the server still needs to trust the client.
15. On the iFIX Server, in the OPC UA Server Configuration Tool, click the Trust List tab.
16. Select the client's certificate and then select Trust.
17. Test the connection again.

**NOTE:** The iFixUaServer.exe application does not need to be in the iFIX task list. It runs with iFIX on startup automatically (and shuts itself down immediately if it is not enabled or if it does not have a self-signed or GDS-signed certificate generated).

## OPC UA Server Configuration Tool

The Server Configuration tool contains the following tabs:

- Server
- Logging
- Security
- Alarms
- Certificate
- Trust List


© 2018 General Electric Company. All rights reserved.

**IMPORTANT:** Be aware that if you make changes to the Server, Logging, Security, or Alarms tabs, you need to restart iFIX before your changes are applied. The Certificate and the Trust Lists tabs do not require a restart and take effect immediately.

## Server

| Item | Description |
|---|---|
| Server Enabled | If selected, the OPC UA server starts when iFIX starts. |
| Port | The TCP port that the OPC UA server uses. The default port is 51400. |
| Network Address | The DNS name or IP address for the machine where the OPC UA application is running. The network address must be the computer name or an IP address, as this represents how clients will locate the OPC UA server. |
| Logical Host Name | The logical name for the machine where the OPC UA application is running. |
| Organization Name | The name of the organization that is deploying the OPC UA application. |
| Instance Name | A unique name for the larger application instance which the OPC UA application belongs to. It is suggested to use the iFIX SCADA node name as the Instance name, but not necessary. |
| Endpoint URL | The network endpoint which OPC UA clients use to communicate with the OPC UA server. For example: opc.tcp://mycomputer:51400/.<br><br>This field is read-only. The four fields at the top of this screen control what displays here. |
| Application URI | A unique identifier for the OPC UA application. For example: urn:-mycomputer:MyCompany:iFix:FIX.<br><br>This field is read-only. The four fields at the top of this screen control what displays here. |
| Application Name | The name of the OPC UA application. This name appears when OPC UA clients browse for OPC UA servers on a network. For example: FIX@-mycomputer.<br><br>This field is read-only. The four fields at the top of this screen control what displays here. |

## Logging

| Item | Description |
|---|---|
| Logging Enabled | If selected, then the OPC UA Server will write events to the log. |
| Number of Log Files | The maximum number of log file backups that are retained. |
| Max Entries Per | The maximum number of lines written to the log file before it is backed up and a new log is created. |

© 2018 General Electric Company. All rights reserved.

| | |
|---|---|
| File | |
| Optimize Log Output | If selected, the log output is buffered before it is saved to disk. |
| Application Trace Level | The level of trace information logged by the OPC UA server. |
| Stack Trace Level | The level of trace information logged by the OPC UA stack used by the OPC UA server. |
| Log File Path | The file path for the flog file. Select the directory to use for log files produced by the server. Click the browse button to open a dialog to select the location of the log file.<br><br>By default, this path is: C:\Program Files (x86)\Proficy\iFIX\LOCAL\Logs\iFixUaServer.log |

## Security

| Item | Description |
|---|---|
| Allow secure communication with data privacy (SignAndEncrypt) | If selected, ensures all traffic is kept private and that clients are authenticated. |
| Allow secure communication without data privacy (SignOnly) | If enabled, all network traffic is visible to eavesdroppers. However, clients can be authenticated. |
| Allow communication with no security (None) | Not recommended as it does not use a certificate to secure communications between client and server. For use only in a non-production environment. |
| Basic256Sha256 (Recommended) | This policy is acceptable and more likely to be supported by older applications. |
| Aes128-Sha256-RsaOaep (Recommended - Fastest) | This policy offers good security and is faster than the most secure policies; however, older applications will not support it. |
| Aes128-Sha256-RsaPss (Recommended - Most Secure) | This policy is the most secure available; however, older applications will not support it. |
| Basic256 (Not Recommended) | This policy has theoretical problems and is not recommended. |
| Basic 128Rsa15 (Not Recommended) | This policy has known vulnerabilities and should not be used unless absolutely necessary. |

## Alarms

| Item | Description |
|---|---|
| Alarms Enabled | If selected, the OPC UA server will report alarms raised by iFIX.<br><br>**NOTE:** In order to see alarm counters via OPC UA you must have alarms enabled in the iFIX OPC UA Server. If you do not enable alarms, the Alarm |


© 2018 General Electric Company. All rights reserved.

| | |
|---|---|
| | Counter "folder" will be empty when browsed. |
| Alarm Refresh Rate | The number seconds the OPC UA server waits before checking for new alarms. |
| Data Refresh Rate | The number seconds the OPC UA server waits before checking for changes to data associated with alarms. |
| Alarm Queue Size | The number of alarms that can be buffered before they are processed by the OPC UA server on the alarm refresh cycle. If more alarms occur in this time frame before they can be processed, queue overruns will occur and alarms may be lost. |
| iFIX Priority Rank | The mapping between iFIX alarm priority ranks and OPC UA alarm severities. |
| OPC UA Severity | The OPC UA severity to be used. |

### Certificate

| Item | Description |
|---|---|
| Application Certificate | Displays the certificate assigned to the OPC UA application. A red error icon appears to the left if the certificate is not useable. |
| Generate Self-Signed | Generates a new self-signed certificate for the OPC UA application. Replaces any existing certificate. |
| Request from GDS | Requests a new certificate signed by a Certificate Authority (CA) from the Global Discovery Service (GDS). |
| Update Trust List | Reads the trust list from the GDS and updates the trust list used by the OPC UA application. |
| Configure GDS | Configures the endpoint and user credentials for the Global Discovery Service (GDS) to use. |

### Trust List

| Item | Description |
|---|---|
| Filter | All - Displays all certificates in the trust list.<br>Trusted - Displays the trusted certificates.<br>Issuers - Displays the CA certificates needed to verify trusted certificates.<br>Rejected - Displays the rejected certificates. |
| Refresh button | Reloads the certificates in the trust list from the file system. |
| View | Show certificate details. |
| Add | Select a file containing a certificate to add to the trust list. |
| Delete | Deletes the selected certificate from the trust list. |
| Trust | Trusts the selected certificate. |
| Make Issuer | Adds the CA certificate to the list of certificates needed to verify trusted certificates. |
| Reject | Stops trusting the selected certificate. |

© 2018 General Electric Company. All rights reserved.

## Browsing and Availability of the Address Space

An OPC UA client can discover iFIX tags and alarm areas that exist on the iFIX SCADA by browsing the iFIX OPC UA server's Address Space. The Address Space is made up of OPC UA nodes, each of which has a unique NodeID.

The Address Space exposes an Alarms folder which contains each of the configured iFIX alarm areas on that SCADA. Clients can subscribe to one or more individual alarm area nodes, or all of them (ALL) by subscribing to the parent Alarms folder.

The Address Space exposes iFIX tags under the Tags folder. Tags are organized into folders based on tag type (for example: Analog Input). Each tag has a Value node which represents the current value of the tag, which has a data type based on the tag type's definition in OpcUaDefinitions.csv file. Under the Value node you can browse other fields of the tag to subscribe to, read or write. Register tags (AR, DR) are exposed as arrays in the OPC UA Server and can be accessed by clients using indexes (offsets) into the Value array. Access is read-only in this case. If you want to write to these tags, you need to go to the Offsets folder and browse to the specific offset you want to write to.

### Subscribing to Alarms

From your OPC client, from the Alarms Folder, you can subscribe to all alarm areas or to individual alarms areas. There is an Alarms folder under Root > Objects that provides access to the alarm areas.

### Subscribing to Tags

From your OPC client, from the Tags folder, you can browse tags and subscribe to specific fields under each tag. There is a Tags folder under Root > Objects that provides access to the tag types and fields. the address space shows a flat list of all tags under the Tags folder.

### Examples of Node IDs:

ns=2;s=13$MIXERSPEED.CV (for a tag's Value node)

ns=2;s=11$MIXERSPEED.F_HI (for a specific field of a tag)

Node IDs are defined by the server and are internal to the OPC UA Server. OPC UA clients retrieve them by browsing the address space, and use them for reading, writing, or forming subscriptions.

The default iFIX OPC UA Server endpoint is opc.tcp//<iFIX SERVER Machine Name>:51800. For example: opc.tcp://CC-AUTO-TEST10:51400, where CC-AUTO-TEST10 is the machine name running the iFIX project.

By default, the iFIX OPC UA Server is disabled at iFIX Project startup. However, the OPC UA server can be enabled in OPC UA Server Configuration tool.

### Namespace URIs

0 - standard namespace, URI: http://opcfoundation.org/UA/ (Defined by the OPC Foundation)

1 -the same as server, URI: urn:[MyComputerName]:MyCompany:iFIXNodeName:[ProjectName]

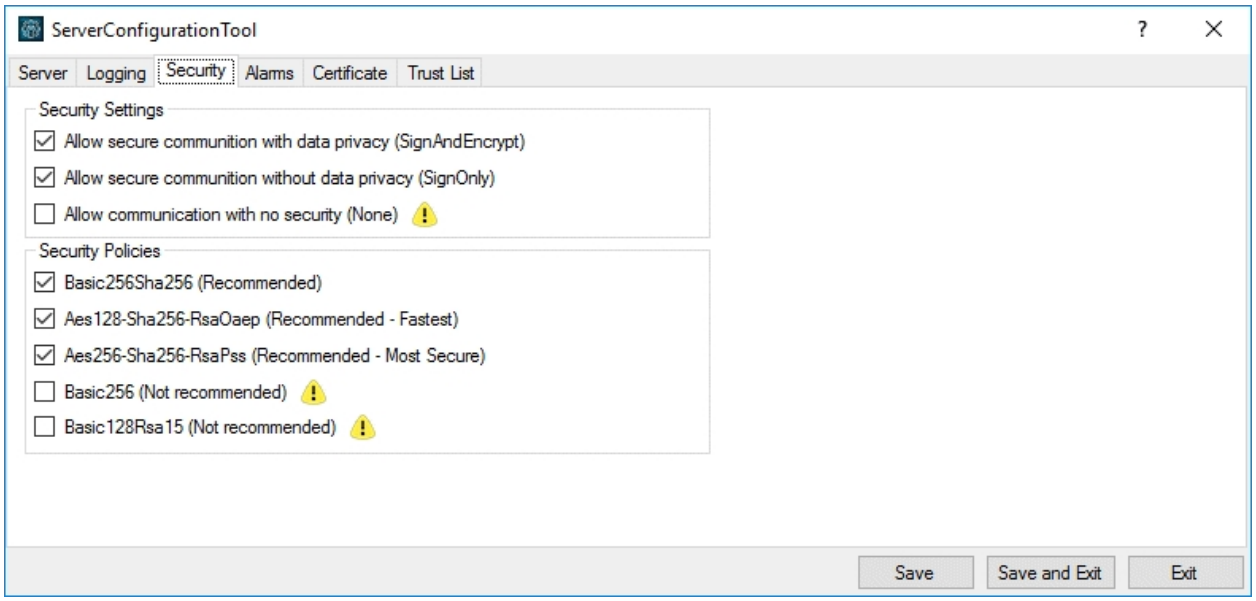
2 - common iFIX specific type definitions, URI: urn:Proficy:iFIX:UAServer


© 2018 General Electric Company. All rights reserved.

# Security Settings for the OPC UA Server

The security of your iFIX OPC UA Server is configured in the OPC UA Configuration tool on the Security, Certificate, and Trust List tabs.

Your main security settings and policies include those illustrated in the following figure. Be aware to use caution on changing any setting with an exclamation point following it.




Explanations of the security settings and recommendations are outlined in the following table.

| Item | Description |
|---|---|
| Allow secure communication with data privacy (SignAndEncrypt) | If this ensures all traffic is kept private and that clients are authenticated. This option is enabled by default. |
| Allow secure communication without data privacy (SignOnly) | If this is enabled all network traffic is visible to eavesdroppers However, clients can be authenticated. This option is enabled by default. |
| Allow communication with no security (None) | Not recommended as it does not use a certificate to secure communications between client and server. For use only in a non-production environment. |
| Basic256Sha256 (Recommended) | This policy is acceptable and more likely to be supported by older applications. This option is enabled by default. |
| Aes128-Sha256-RsaOaep (Recommended - Fastest) | This policy offers good security and is faster than the most secure policies; however, older applications will not support it. This option is enabled by default. |
| Aes128-Sha256-RsaPss (Recommended - Most Secure) | This policy is the most secure available; however, older applications will not support it. This option is enabled by default. |
| Basic256 (Not Recommended) | This policy has theoretical problems and is not recommended. |

© 2018 General Electric Company. All rights reserved.

| | |
|---|---|
| Basic 128Rsa15 (Not Recommended) | This policy has known vulnerabilities and should not be used unless absolutely necessary. |

The following sections describe how certificates and trust lists are set up, as well as more on the Global Discovery Server (GDS) if that is used as your certificate authority (CA):

- Certificate Management and the OPC UA Server
- About the Trust List
- More on the Global Discovery Server

## Certificate Management and the OPC UA Server

The iFIX OPC UA Server provides two ways to configure your certificates:

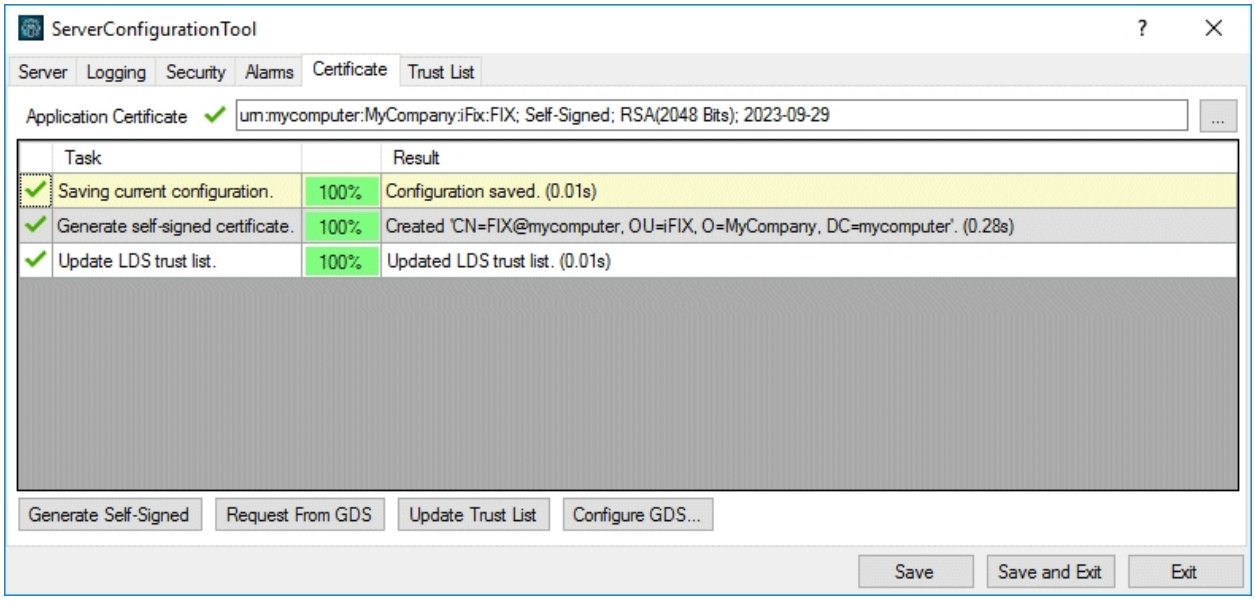
- Use a Self-Signed Certificate for the iFIX OPC UA Server
- Use a GDS-Signed Certificate for the iFIX OPC UA Server

### Use a Self-Signed Certificate for the OPC UA Server

To generate a self-signed certificate for your OPC UA Server, select the Generate Self-Signed option on the Certificate tab of the OPC UA Server Configuration tool.

**NOTE:** Generating a self-signed certificate automatically saves the current settings from the OPC UA Configuration tool. If you made any other changes, be aware that those changes will also get saved.

The following example shows a self-signed certificate.




**NOTE:** Self-signed certificates are stored in your iFIX LOCAL folder. For example: C:\Program Files (x86)\Proficy\iFIX\LOCAL\UA\pkiserver\own\certs


© 2018 General Electric Company. All rights reserved.

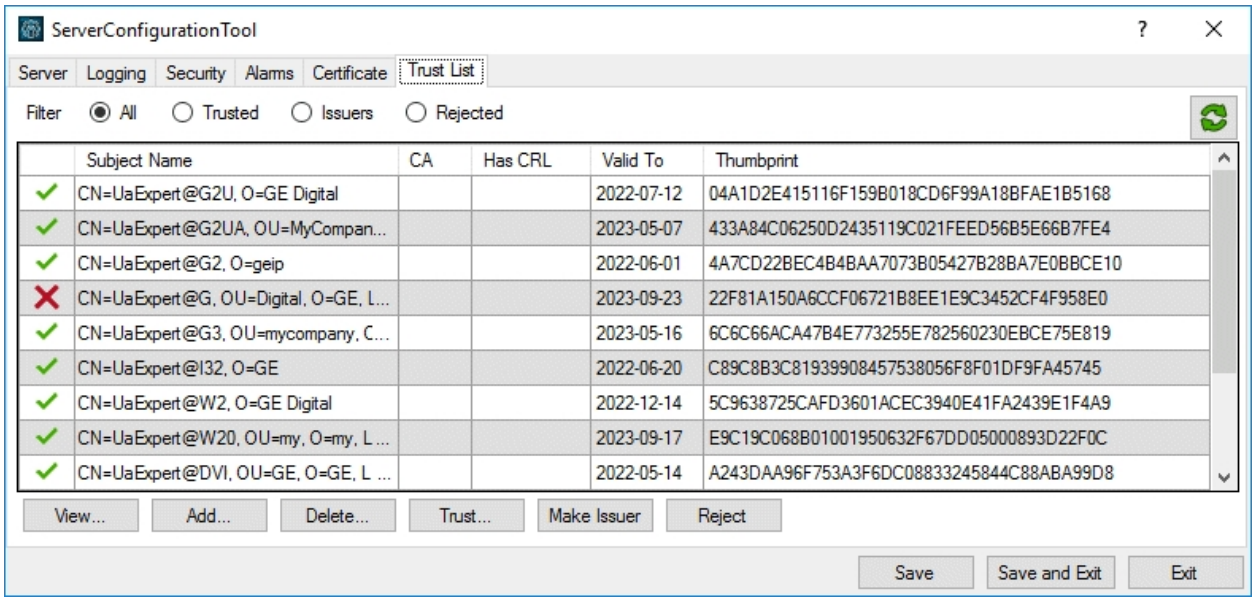
### Use a GDS-Signed Certificate for the OPC UA Server

To request a certificate for your OPC UA Server from a Global Discover Server (GDS), select the Request from GDS option on the Certificate tab of the OPC UA Server Configuration tool.

When you select the Configure GDS option, you enter the Endpoint URI, and user name and password to connect to your GDS Server.

## About the Trust List

Use the OPC UA Server Configuration tool to add an OPC UA Client to the Trust List for your iFIX OPC UA Server. From the Trust List tab, select the client's certificate and then select Trust. You can manage all trusted connections from this tab.



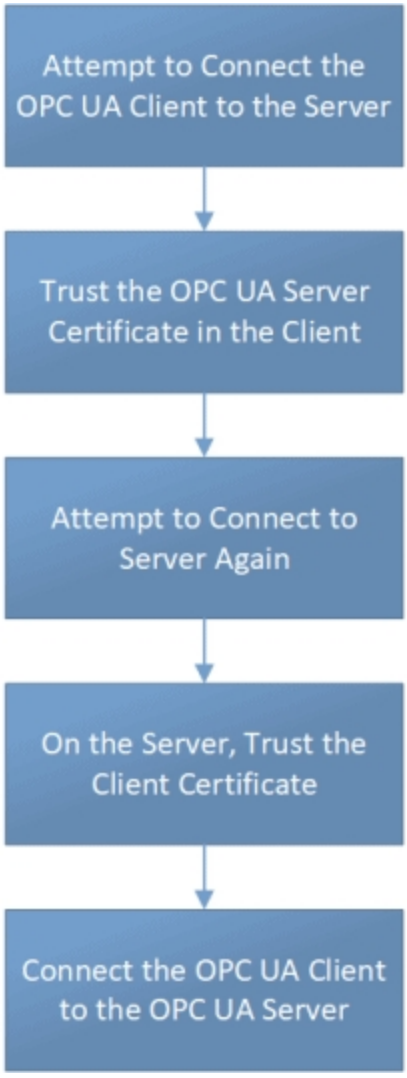

When setting up the trusts relationships, the client must first trust the server. Then, the server trusts the client. After that relationship is setup, you can then test the connection between the iFIX OPC UA Server and your OPC UA client. For an overview of setup steps, refer to the "Quick Start" on page 6.

If you are using the Global Discover Server to manage your certificates, the GDS automatically sets up your trusts between clients and servers.

If you are not using the GDS and instead have a self-signed certificate, the following diagram describes the workflow a self-signed certificate. This workflow assumes the iFIX OPC UA Server is already running.

© 2018 General Electric Company. All rights reserved.

### Workflow for Self-Signed Certificate

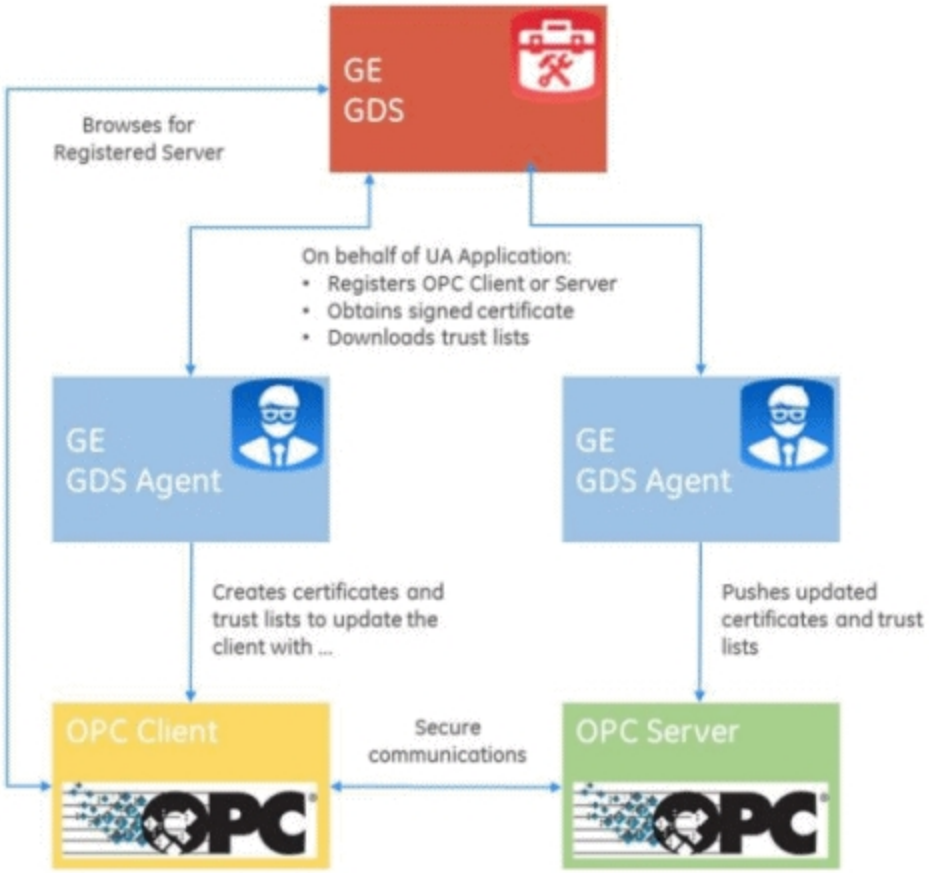



## More on the Global Discovery Server

The GE Global Discovery Server (GDS) can be used to manage application certificates for all OPC UA applications at a site. The GDS is a database of applications. It enables all applications in the GE GDS to communicate with each other securely. It also performs like a search engine and can find all the applications that are running in your factory or environment.

The following figure describes how the GE GDS interacts with OPC UA Servers and Clients.


© 2018 General Electric Company. All rights reserved.




If you want to create a GDS-signed certificate, the GE Global Discovery Server is available to make communication between OPC UA applications and iFIX easier and more secure.

Applications with certificates that are signed by the GE Global Discovery Server can communicate with any other client or server that also has its certificate signed by the GE Global Discovery Server.

### iFIX Security and the OPC UA Server

Be aware of the following when using iFIX Security and the OPC UA Server:

- The OPC UA Server integrates with the iFIX security system for user authentication and authorization.
- OPC UA clients cannot use Anonymous mode for authentication if iFIX security is enabled.
- OPC UA clients must provide a valid iFIX user name and password in order to successfully connect to the OPC UA Server.
- Once a session has been established with the OPC UA Server, the user's permissions and privileges are enforced by the iFIX security system. If the logged-in user does not have permission to write to a given tag or acknowledge its alarms (based on the tag's security areas configuration), then the operation will fail.

## Alarms and the iFIX OPC UA Server

© 2018 General Electric Company. All rights reserved.

For information on how iFIX alarms work with the OPC UA Server, see the following sections:

- About Alarm Settings for the OPC UA Server
- Mapping of iFIX Alarm Types to OPC UA Alarm Types

## About Alarm Settings for the OPC UA Server

When Alarms are enabled for the iFIX OPC UA Server, the OPC UA server will report alarms raised by iFIX.

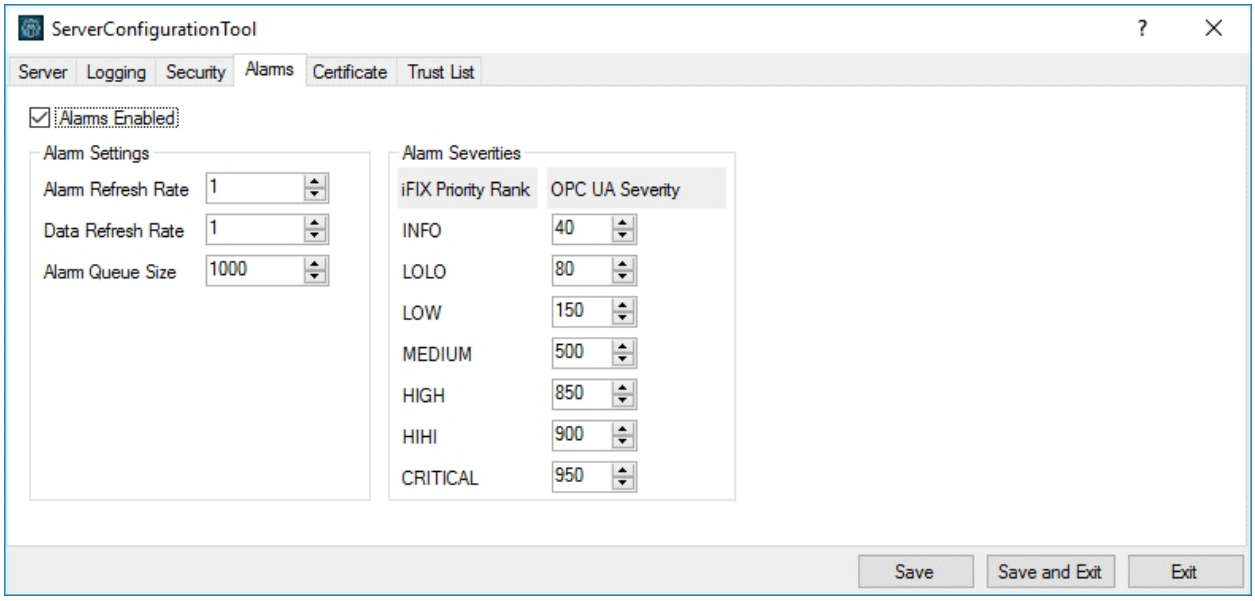
In order to see alarm counters via OPC UA you must have alarms enabled in the iFIX OPC UA Server. If you do not enable alarms, the Alarm Counter "folder" will be empty when browsed.

OPC UA alarm notifications are sent to subscribers as a result of certain changes to the alarm's state. Each OPC UA alarm type's notification to clients has its own set of event data associated with it. For example, the ExclusiveLevelAlarmType has LimitState, which represents a limit is being exceeded by the tag's value: HighHigh, High, Low, or LowLow.

In addition, all alarm notifications share data members that derive from parent OPC UA types, such as ConditonType, AcknowledgeableConditionType, and AlarmConditionType.

The OPC UA specification (mostly in Part 9) defines the data associated with the different types of event notifications, including whether that data is required or optional for a given event type. It also defines the behaviors that define or are required by each event type. For more information, refer to the OPC Foundation web site.

Alarms are not enabled by default for the iFIX OPC UA Server. You must enable and configure alarming from the Alarms tab of the OPC UA Server Configuration tool.




The mapping between iFIX alarm priority ranks and OPC UA alarm severities are used to translate iFIX alarm priorities into OPC UA numeric severity values. For details, refer to the Mapping of iFIX Alarm Types to OPC UA Alarm Types section.

## Mapping of iFIX Alarm Types to OPC UA Alarm Types


© 2018 General Electric Company. All rights reserved.

iFIX tags can generate several different alarm types, based on the type of tag (AI, DI, PID, and so on). Some tags can generate multiple types of alarms, although a tag is either in alarm or not in alarm. This means that an alarm cannot be in two alarm states at once even with the concept of a current alarm state and possibly a latched alarm state. Acknowledgment of a tag's alarm acknowledges all current and prior alarm states since the tag was last acknowledged or went into alarm.

iFIX alarm types are mapped to certain OPC UA defined types. The following table describes how the iFIX alarm types map to OPC UA alarm types.

| iFIX Tag Type | iFIX Alarm Type | OPC UA Alarm Type |
|---|---|---|
| AI/AA | HIHI, HI, LO, LOLO | ExclusiveLevelAlarmType |
| | RATE (Rate of Change) | ExclusiveRateOfChangeAlarmType |
| AA/PID | DEV (Deviation) | ExclusiveDeviationAlarmType |
| CA | URNG, ORNG (Under/Over range) | ExclusiveLevelAlarmType |
| DI/DA | CFN (Change Form Normal)CFN (Change Form Normal) | OffNormalAlarmType |
| | COS (Change of State) | OffNormalAlarmType |
| TM (Timer) | TIME | OffNormalAlarmType |
| MDI (Multi-state Digital Input) | CFN | OffNormalAlarmType |
| Any with I/O Address | COMM | SystemOffNormalAlarmType |

# Tag Types and Attributes

The following sections will help you with understanding the iFIX tag type mappings and how they apply to the OPC UA Server:

- Default Representation of iFIX Tag Types in the OPC UA Server
- Renaming Tag Types in the OPC UA Server's Address Space

## Default Representation of iFIX Tag Types in the OPC UA Server

The following table describes how each iFIX tag type is represented in the iFIX OPC UA Server.

**NOTE:** The 'TopLevelFields' column is a list, for each tag type, of the fields that appear directly below a tag's Value node in the address space. All other tag fields appear in an 'All Fields' folder that also exists under Value.

| iFIX Type Name | Display Name | Variable Type | Data-type | Value Rank | Array Dimensions | Access Level | Top Level Fields |
|---|---|---|---|---|---|---|---|

© 2018 General Electric Company. All rights reserved.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AA | Analog Alarm | AnalogValue | Double | Scalar | 0 | ReadWrite | A_AUTO;A_CUALM;A_DESC;A_ENAB;A_LAALM;E_HIHI;E_HI;E_LO;E_LOLO;A_NALM;A_SCAN |
| AI | Analog Input | AnalogValue | Double | Scalar | 0 | ReadWrite | A_AUTO;A_CUALM;A_DESC;A_ENAB;A_LAALM;E_HIHI;E_HI;E_LO;E_LOLO;A_NALM;A_SCAN |
| AIS | Scaled Analog Input | AnalogValue | Double | Scalar | 0 | ReadWrite | A_AUTO;A_CUALM;A_DESC;A_LAALM;E_HIHI;E_HI;E_LO;E_LOLO;A_NALM;A_SCAN |
| AO | Analog Output | AnalogValue | Double | Scalar | 0 | ReadWrite | A_AUTO;A_COLD;A_DESC;E_HILIM;E_LOLIM;E_RATE;A_ROUT |
| AR | Analog Register | AnalogValue | Double | OneDimension | 1024 | ReadWrite | A_AUTO;A_DESC;A_EOUT |
| AR2 | Analog | AnalogValue | Double | OneDi- | 1024 | | A_ |


© 2018 General Electric Company. All rights reserved.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Register 2 | | | mension | | ReadWr-ite | AUTO;A_ DESC;A_ EOUT |
| BB | On-Off Control | TextOrNoValue | String | Scalar | 0 | ReadOn-ly | A_ AUTO;A_ C1ENA;A_ C2ENA;A_ DESC;A_ HI1;A_ HI2;A_ LO1;A_ LO2;A_ ONCE |
| BL | Boolean | TwoStateDis-creteValue | Boolea-n | Scalar | 0 | ReadOn-ly | A_ DESC;A_ GETF1;A_ GETF2;A_ GETF3;A_ GETF4;A_ GETF5;A_ GETF6;A_ GETF7;A_ GETF8 |
| BPL | Lin-earization | AnalogValue | Float | Scalar | 0 | ReadOn-ly | A_DESC |
| CA | Cal-culation | AnalogValue | Double | Scalar | 0 | ReadOn-ly | A_ CUALM;A_ DESC |
| CTR | Counter | TextOrNoValue | String | Scalar | 0 | ReadOn-ly | A_CLR;A_ DESC;A_ GATEVAL;-A_ GET1;A_ INPUT;A_ MODE;A_ PASS |
| D16 | 16-bit Digital Alarm | AnalogValue | Float | Scalar | 0 | ReadOn-ly | A_ COUNT;-A_ DESC;A_ MODE;A_ REALM;A_ SCAN |
| DA | Digital Alarm | TwoStateDis-creteValue | Boolea-n | Scalar | 0 | ReadWr-ite | A_ ALMCK;A_ ASUSP;A_ AUTO;A_ CUALM;A_ |

© 2018 General Electric Company. All rights reserved.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | DESC;A_ ENAB;A_ EOUT;A_ LAALM;A_ NALM;A_ SCAN |
| DC | Device Control | TextOrNoValue | String | Scalar | 0 | ReadOnly | A_ AUTO;A_ BSTAT;A_ CUALM;A_ DESC;A_ LAALM;A_ NALM;A_ SCAN |
| DI | Digital Input | TwoStateDiscreteValue | Boolean | Scalar | 0 | ReadWrite | A_ ALMCK;A_ AUTO;A_ CUALM;A_ DESC;A_ ENAB;A_ EOUT;A_ LAALM;A_ NALM;A_ SCAN |
| DO | Digital Output | TwoStateDiscreteValue | Boolean | Scalar | 0 | ReadWrite | A_ AUTO;A_ DESC;A_ INV;A_ SCAN |
| DR | Digital Register | TwoStateDiscreteValue | Boolean | OneDimension | 1024 | ReadWrite | A_ AUTO;A_ DESC;A_ EOUT |
| DR2 | Digital Register 2 | TwoStateDiscreteValue | Boolean | OneDimension | 1024 | ReadWrite | A_ AUTO;A_ DESC;A_ EOUT |
| DT | Dead Time | AnalogValue | Double | Scalar | 0 | ReadOnly | A_ AUTO;A_ DESC;A_ TIME |
| ETR | Extended Trend Block | AnalogValue | Float | Scalar | 0 | ReadOnly | A_ AUTO;A_ BC;A_ DESC;A_ GET1;A_ TIME |


© 2018 General Electric Company. All rights reserved.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| EV | Event Action | TextOrNoValue | Boolean | Scalar | 0 | NoAccess | A_COND0;A_COND1;A_DESC;A_FAL0;A_FAL1;A_TRU0;A_TRU1 |
| FN | Fanout | TextOrNoValue | Boolean | Scalar | 0 | NoAccess | A_DESC;A_PUT1;A_PUT2;A_PUT3;A_PUT4 |
| GAB | Group Alarm Block | TextOrNoValue | Double | Scalar | 0 | NoAccess | A_DESC;A_ENAB;A_NALM;A_CUALM;A_LAALM;A_PRI |
| GEN | Signal Generator | AnalogValue | Double | Scalar | 0 | ReadOnly | A_CENT;A_DESC;A_NOISE;A_SCALE;A_SCAN;A_PER;A_WAVE |
| HS | Histogram | TextOrNoValue | Boolean | Scalar | 0 | NoAccess | A_AUTOC;A_DESC;A_GROUP |
| ITM | Interval Timer-Totalizer | TextOrNoValue | String | Scalar | 0 | ReadOnly | A_DESC;A_CUALM;A_LAALM;A_RANGE;F_GATE;F_RESET;F_STATE;A_PASS;F_AVG;A_HMSINT;-A_HMSTOTAL |
| LL | Lead Lag | AnalogValue | Double | Scalar | 0 | ReadOn- | A_ |

© 2018 General Electric Company. All rights reserved.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | ly | DESC;A_K;A_LAG;A_LEAD |
| MDI | Multistate Digital Alarm | MultiStateDiscreteValue | Byte | Scalar | 0 | ReadOnly | A_CUALM;A_DESC;A_ENAB;A_LAALM;A_NALM;A_REALM;A_RV;A_SCAN;F_CV0;F_CV1;F_CV2 |
| MDO | Momentary Output | TwoStateDiscreteValue | Boolean | Scalar | 0 | ReadOnly | A_COLD;A_DESC;A_DUTY;A_INVRT;A_RETRY;A_RMAX;A_SCAN |
| ODO | Pulse Digital Output | AnalogValue | Float | Scalar | 0 | ReadOnly | A_DESC;A_INVQ;A_INVRT;A_SCAN |
| PA | Pareto | TextOrNoValue | Boolean | Scalar | 0 | NoAccess | A_AUTO;A_DESC;A_SCAN;A_SORT |
| PAR | Persistent Array | AnalogValue | Float | Scalar | 0 | ReadWrite | A_DESC |
| PG | Program Block | TextOrNoValue | String | Scalar | 0 | ReadOnly | A_AUTO;A_DESC;A_SCAN;A_TV1 |
| PI2 | Improved PID | AnalogValue | FLoat | Scalar | 0 | ReadOnly | A_AUTO;A_CUALM;A_DFILT;A_FRC;A_LAALM;A_NALM;F_ |


© 2018 General Electric Company. All rights reserved.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | DGLIM;F_ PBAND;F_ RESET;F_ RATE;F_ TV1 |
| PID | PID | AnalogValue | Double | Scalar | 0 | ReadOn-ly | A_ AUTO;A_ BUMP;A_ CUALM;A_ DESC;A_ ENAB;A_ LAALM;A_ NALM;A_ SPHI;A_ SPLO;F_ TV1 |
| RB | Ratio Bias | AnalogValue | Double | Scalar | 0 | ReadOn-ly | A_ CUALM;A_ DESC;A_ ENAB;A_ RATIO;F_ TV1;F_TV2 |
| RM | Ramp | AnalogValue | Double | Scalar | 0 | ReadOn-ly | A_ AUTO;A_ DESC;A_ ENAB;A_ HOLD1;A_ HOLD2;A_ RATE1;A_ RATE2;A_ RATE3;F_ TV1;F_ TV2;F_TV3 |
| SC | Statistical Control | AnalogValue | Double | Scalar | 0 | ReadOn-ly | A_ALM;A_ AUTO;A_ DESC;A_ DEV;A_ RCALC;A_ SENT;A_ SHOW;A_ SLOPE |
| SD | Statistical Data | AnalogValue | Double | Scalar | 0 | ReadOn-ly | A_ AUTO;A_ AUTOX;A_ CUALM;A_ DESC;A_ |

© 2018 General Electric Company. All rights reserved.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | ENAB;A_LCALC;A_NGRP;A_NOBS;A_SCAN |
| SQD | SQL Data | TextOrNoValue | Boolean | Scalar | 0 | NoAccess | A_DESC;A_TF01;A_TF02;A_TF03;A_TF04;A_TF05 |
| SQT | SQL Trigger | AnalogValue | Double | Scalar | 0 | ReadOnly | A_CUALM;A_DBERR;-A_DESC;A_ENAB;A_EVPD;A_NALM;A_PDTMR;-A_SCAN;A_SQL;A_SQLST |
| SS | Signal Select | AnalogValue | Double | Scalar | 0 | ReadOnly | A_DESC;A_GET1;A_GET2;A_GET3;A_GET4;A_GET5;A_SEL |
| TDS | Time-Date Stamp | TextOrNoValue | String | Scalar | 0 | ReadOnly | A_DESC;A_FMT;A_MODE;A_SEP |
| TM | Timer | AnalogValue | Double | Scalar | 0 | ReadOnly | A_COND;A_CUALM;A_DESC;A_DIRN;A_ENAB;A_MODE;A_NALM;A_PV;A_TV |
| TR | Trend | AnalogValue | Double | Scalar | 0 | | A_BC;A_ |


© 2018 General Electric Company. All rights reserved.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | ReadOnly | DESC;A_GET1;A_TIME;F_INP |
| TT | Totalizer | AnalogValue | Double | Scalar | 0 | ReadOnly | A_DESC;A_EF;A_TIME |
| TX | Text | TextOrNoValue | String | Scalar | 0 | ReadWrite | A_AUTO;A_DESC;A_NTFY;A_SCAN |
| TXR | Text Register | TextOrNoValue | String | Scalar | 0 | ReadWrite | A_DESC;A_OUT |
| TXT | Text Lookup | TextOrNoValue | String | Scalar | 0 | ReadOnly | A_AUTO;A_CASE;A_DESC;A_OUT;F_RV |

## Renaming Tag Types in the OPC UA Server's Address Space

Tag Type metadata such as the definition and datatype of the tag type's value, the display name of the tag type, and anything else needed by the iFIX OPC UA Server is stored in a .csv file, OpcUaDefinitions.csv, on the SCADA Server. The OpcUaDefinitions.csv file found in the iFIX LOCAL folder. By default, this folder is typically located here: C:\Program Files (x86)\Proficy\iFIX\LOCAL.

The OpcUaDefinitions.csv file is initially populated with the iFIX defined tag type information. However, it can be edited to change the representation of existing tag types in the OPC UA server's address space, or to add information about custom block toolkit (BTK) tag types that customers or 3rd parties create.

Use extreme caution in editing this file, however. A third-party .csv parser should be incorporated to manage the file contents. Be aware that the file also needs to be consumed (at startup), so that the metadata can be provided to the OPC UA Server to form the SCADA's address space. Also, changes to the configuration of tag types will change how the Value of tags of that type is represented, and if the configuration is invalid it may result in the inability to access the tag’s value, or an incorrect representation of the tag’s value.

If you make change to the OpcUaDefinitions.csv file, you will need to restart iFIX after you save your changes. Changes to the config (tag type data types) are reflected when iFIX is restarted.

For a description of the iFIX tag types and OPC UA mapping, refer to the "Default Representation of iFIX Tag Types in the OPC UA Server" on page 17 section.

© 2018 General Electric Company. All rights reserved.

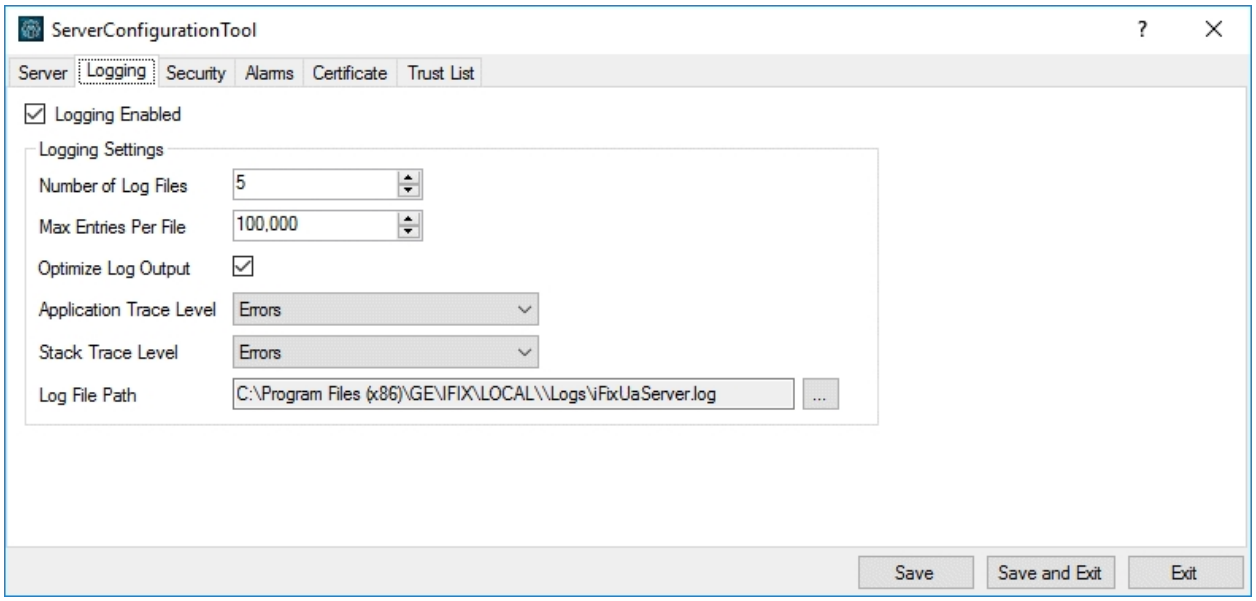
# Advanced

The following sections provide assistance with understanding and troubleshooting your iFIX OPC UA Server:

- Configure Logging for the OPC UA Server
- Troubleshooting the OPC UA Server

## Configure Logging for the OPC UA Server

The level of trace information logged by the OPC UA stack used by the OPC UA server is specified in the OPC UA Configuration tool on the Logging tab.




From the Logging tab, you can change the level of logging, if the default value is not detailed enough. To specify the level of data logged in the trace log file, select an option from the Trace Level field. The following table describes the types of communication information you can choose from in this field. Be aware that logging configured higher than the default level can be a CPU-intensive operation. It is recommended that you use detailed logging only when setting up your OPC Server or to diagnose problems, and turning it off when the system is functioning correctly.

| Stack Trace Level | Description |
|---|---|
| None | Turns off all logging. |
| Errors | Logs only errors from the iFIX OPC UA server. Errors is the default setting. |
| Errors and Warnings | Logs error and warning messages from the iFIX OPC UA Server. |


© 2018 General Electric Company. All rights reserved.

| | |
|---|---|
| Errors, Warnings, and Information | Logs errors, warnings, and information level messages from the OPC UA Server. Be aware that logging configured higher than the default level can be a CPU and disk intensive operation. Using the highest levels of logging results in very verbose logging, and may likely impact performance and client connectivity. Be sure to enable the Optimize Log Output option if using this level of logging. |
| Detailed (Impacts Performance | Logs detailed errors, warnings, and information on iFIX data and alarms read by the iFIX OPC UA Server. Be aware that logging configured higher than the default level can be a CPU and disk intensive operation. Using the highest levels of logging results in very verbose logging, and may likely impact performance and client connectivity. Be sure to enable the Optimize Log Output option if using this level of logging. |

### More on the Log Files

By default, the iFIX OPC UA Server stores the log files to the following folder: C:\Program Files (x86)\Proficy\iFIX\LOCAL\Logs. You also can change this path from the Logging tab in the OPC UA Server Configuration tool. The following logs are created by the iFIX OPC UA Server:

- **OpcUaEdaApi.log:** contains messages and errors related to iFIX interaction, including browsing of alarms and data as well as security checks and reading and writing data.
- **iFixUaServer.log:** contains more of the server-related messages, messages related to OPC UA, and, if stack-level tracing is enabled, messages from the UA stack which involve low-level communications and events.

If something is going wrong with interaction with the underlying iFIX system, the OpcUaEdaApi.log file should provide some useful errors, including the iFIX error codes.

**NOTE:** In some cases, errors will be logged due to the OPC UA Server trying to access a field that does not exist for a given tag type. This is usually a normal occurrence and does not indicate a problem unless OPC UA clients are actually trying to access that field of the tag and are receiving errors.

An example of a log message in the iFixUaserver.log file would be a message regarding a client connection rejection. For instance, if the license limit of 2 clients was exceeded, you would find that message in the iFixUaserver.log file.

## Troubleshooting the OPC UA Server

Some issues you may encounter when using the iFIX OPC UA Server include those outlined in the following table:

| Issue | Description |
|---|---|
| Client Rejects the Server Certificate Immediately After Generation | If a client rejects the server's certificate almost immediately after you generate it, check that the client's date and time is not before the time the self-signed certificate was generated. Even if it is only a few minutes off, an error can occur. In a client it should show up as a "BadCer- |

© 2018 General Electric Company. All rights reserved.

| | |
|---|---|
| | tificateIssuerTimeInvalid" error: An issuer certificate has expired or is not yet valid. This error can also happen if the server's certificate has expired. |
| Client Can Not Connect | If an OPC UA client cannot connect to the iFIX OPC UA Server, check:<br>• If client connection rejection was a result of a license limitation. You may have exceeded the default limit of 2 clients.<br>• If the server is trusted. There could be an issue with your certificate.<br>• If the OPC UA Server is enabled and that the OPC UA Client is using the correct port number. Confirm that you following all the setup steps outlined in the Quick Start.<br>• If there is an unexpected error in the log files. The OpcUaEdaApi.log contains messages and errors related to iFIX interaction, including browsing of alarms and data as well as security checks and reading and writing data. The iFixUaServer.log contains more of the server-related messages, messages related to OPC UA, and, if stack-level tracing is enabled, messages from the UA stack which involve low-level communications and events. For more information on log files, refer to the Configure Logging for the OPC UA Server topic. |
| iFIX Error | If something is going wrong with interaction with the underlying iFIX system, the OpcUaEdaApi.log file should provide some useful errors, including the iFIX error codes if calls to iFIX fail for some reason. For more information on log files, refer to the Configure Logging for the OPC UA Server topic. |
| OPC UA Client Certificate Not Trusted | Could be an issue with your certificate. Confirm that you following all the setup steps. Refer to the Quick Start. |
| Error When Subscribing to a Tag in the OPC UA Client | An iFIX tag is represented as an Object. If you want the current value of the tag, you must select the Value Variable which is a component of the Tag Object or one of its fields. |
| OPC UA Server Does Not Start After You Enable It and Restart iFIX | Check that the FIX.INI file contains an entry for the iFIX OPC UA Server. If not, manually update the FIX.INI to include this entry at the bottom of the [SCADA] section:<br>`RUN=%IFIXUASERVER.EXE`<br>Restart iFIX after you save your changes. |


© 2018 General Electric Company. All rights reserved.

# Index


**C**

certificate management 12

configuration mode, OPC UA Server 27

**F**

features 2

**G**

getting started, iFIX OPC UA Server 1

**O**

OPC UA Server 1

**P**

passed attributes 17

**S**

service, running as 5


© 2018 General Electric Company. All rights reserved.