GE VERNOVA

PROFICY®SOFTWARE & SERVICES

PROFICY iFIX HMI/SCADA

OPC UA Client Driver

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.

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 Client Driver

The iFIX OPC UA (OPC Unified Architecture) Client is a device communications module that can connect to OPC UA Servers and collect data from UA variables. This help provides information on how to configure and use this client.

The OPC UA Client Driver help contains the following sections:

- Introduction
- Security
- Configuration

Introduction

For a brief introduction on the iFIX OPC UA Client, refer to the sections below.

- "Overview of the OPC UA Client Driver" below
- "How the OPC UA Driver Works" below
- "Features of the OPC UA Client Driver" on the next page
- "Limitations" on page 3

Overview of the OPC UA Client Driver

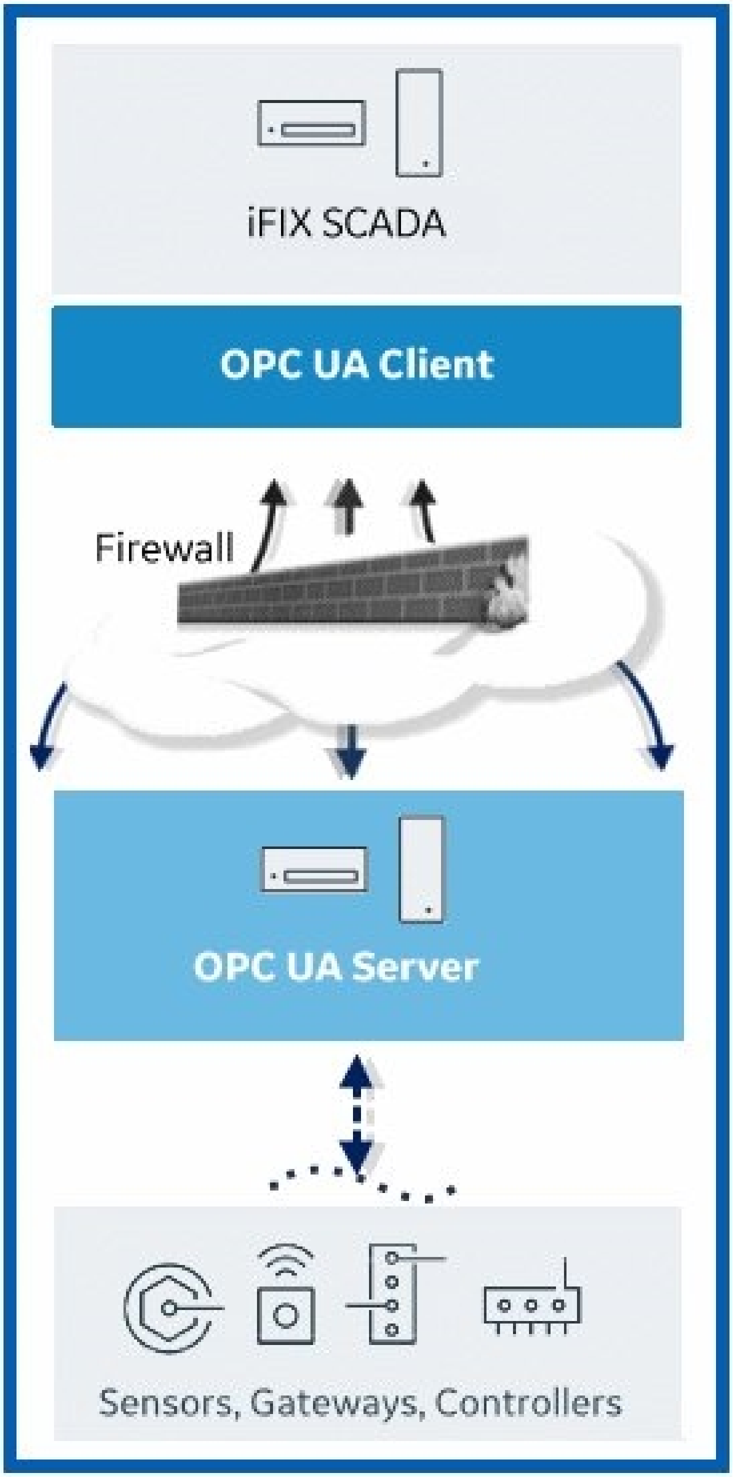
OPC UA defines a platform independent communication system that has a useful and adaptive Information Model for both industrial and business application needs. Like iFIX, OPC UA builds on the success and strength of common industrial standards. Developed by the OPC Foundation and meant to be platform independent, OPC UA can provide lower costs and increased productivity for end-users, systems integrators, and process control vendors alike by focusing communications issues on a single technology and strategy.

The iFIX OPC UA (OPC Unified Architecture) Client is a device communications module that can connect to OPC UA Servers to browse and collect data from items in the OPC UA address space. Use the Configuration Hub tool to browse an OPC UA Server and automatically create driver tags in iFIX.

The OPC UA Client can be configured in a few simple steps. For details on these steps, refer to the "Quick Start: OPC UA Client Configuration" on page 4 topic.

How the OPC UA Driver Works

Basic components for iFIX OPC UA Client communication and the general connectivity hierarchy is outlined in the following figure.



Features of the OPC UA Client Driver

The OPC UA Client Driver provides the following features:

- Web configuration provided using Configuration Hub.
- Support for the main OPC Unified Architecture (UA) information model for Data Access (DA).
- An OPC UA implementation that allows for secure and reliable communication and authentication of clients, servers, and users.
- Use of Windows Authentication for standard security protocols.
- Support for connections to the iFIX OPC UA Server or other OPC UA Servers.
- Ability to auto create iFIX tags in bulk from the Database Manager import, for node IDs no longer than 80 characters (in the I/O address field in the database) and primary blocks.
- Provides similar interactions to iFIX as other I/O drivers. The OPC UA Client Driver is loaded, configured, and accessed in the same or similar manner to existing I/O drivers.
- Support for OPC UA Client redundancy.

Limitations

When using the OPC UA Client (OUA) Driver with iFIX, be aware of the following limitations:

- While the OPC Driver supports Suppression of COMM alarms and Data Latching, the OPC UA Client driver does not.
- Array indexes greater than 65535 are not supported.
- Autocreating a driver tag in the Database Manager with an index into an array is not supported.
- Matrices are not supported. While OPC UA supports scalar values, arrays, and matrices, Matrices are not supported in the OPC UA Client Driver.
- Writing values greater than 256 bytes is not supported. This could be as few as 128 characters.
- The OPC UA Client Driver has been tested with up to 50 configured servers, and 250 groups. Performance or connectivity issues may be encountered when exceeding those limits.
- The OPC UA Client Driver can only write to individual elements (1 array index at a time). You cannot write to the whole array at the same time. Servers that do not support writing to individual array elements will reject the individual index write and may return an error such as BadWriteNotSupported.
- Servers that do not support subscriptions are unsupported. We require the server to support subscriptions.
- Autocreate of tags in the Database Manager only works for node IDs no longer than 80 characters (the I/O address field in database).
- Complex data types are not supported. Arrays of complex data types will report BadOutOfRange errors in the iFixUaClient_OUASPOLL.log file. Examples of complex types include:
  - DataValue
  - DiagnosticInfo
  - Enumeration
  - Structure
  - XmlElement (can read a single element as a string, but arrays are unreadable)

Security

Security is based on OPC UA standards. The OPC UA Client Driver uses the Configuration Hub tool for configuration. From this powerful web client you can configure a connection to an OPC UA Server, browse for data sources, and automatically populate the iFIX database with new tags.

Use of the Configuration Hub tool will require you to enable security in iFIX.

For more information on security, refer to the Security Considerations section.

Security Considerations

Be aware of the following when using the OPC UA Client Driver:

- Configuration Hub is provided for driver configuration. This tool integrates with the iFIX security for user authentication and authorization.
- The user must provide a valid iFIX user name and password in order to successfully connect to iFIX from Configuration Hub.
- In order to login to Configuration Hub, the iFIX user must belong to the Application Designer security group in iFIX.
- After 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.
- When using Enhanced Failover, the OPC UA Client will not allow you to make changes unless the primary node is in Maintenance Mode.

Configuration

Configuration for the OPC UA Client Driver includes the following:

- Quick Start: OPC UA Client Configuration
- Server Configuration
- Group Configuration
- Redundancy Configuration

Quick Start: OPC UA Client Configuration

The OPC UA Client Driver is added to iFIX the same way you would add other drivers, using the System Configuration (SCU) tool. After you add the driver and restart iFIX, you can then configure the driver using Configuration Hub. The following steps outline how to quickly add and configure your driver.

1. In iFIX, add user privileges (add user to Application Designer group) and enable security.
2. In the iFIX System Configuration Utility, add the OPC UA Client driver, if it is not already added.
3. Start or restart iFIX.
4. Start Configuration Hub from the iFIX WorkSpace (in the system tree, select the OUA entry in the I/O Drivers folder). Use the iFIX user name and password that you created in the previous steps to log in.
5. Confirm that your OPC UA Server is up and running.
6. In the Configuration Hub tool, click Connections, and on the OPC UA tab, click the New button to add a server. In the Details panel, specify user credentials, and a security policy.
7. On the Connection tab, click Test Connection to begin the certificate trust process:
    a. On the iFIX SCADA for Configuration Hub, trust the server..
    b. On the OPC UA Server, in its certificate management tool, trust the OPC UA Client.
    c. In the Configuration Hub tool, click Test Connection again. The connection should succeed.

8. Proceed to create your Groups.

IMPORTANT: Every time you make a change in the configuration from Configuration Hub, 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 Configuration Hub.

How to Add User Privileges for the OPC UA Client Driver in iFIX

1. Start iFIX.
2. In the WorkSpace, on the Applications tab, click Security and then Security Configuration Utility.
3. On the Edit menu select User Accounts. The User Accounts dialog box appears.
4. Click Add. The User Profile dialog box appears.
5. If using Windows users, select Use Windows Security.
6. In the User Name field, enter the user that you created for use with iFIX.
7. If needed, enter the Domain.
8. Add the Application Designer group to the user in order to use Configuration Hub.
9. Modify other groups, security areas, and application features as appropriate. Do not delete Database Save and Database Block Add-Delete application features as those are needed to add tags.
10. Click OK, and OK again.
11. On the File menu, click Save.

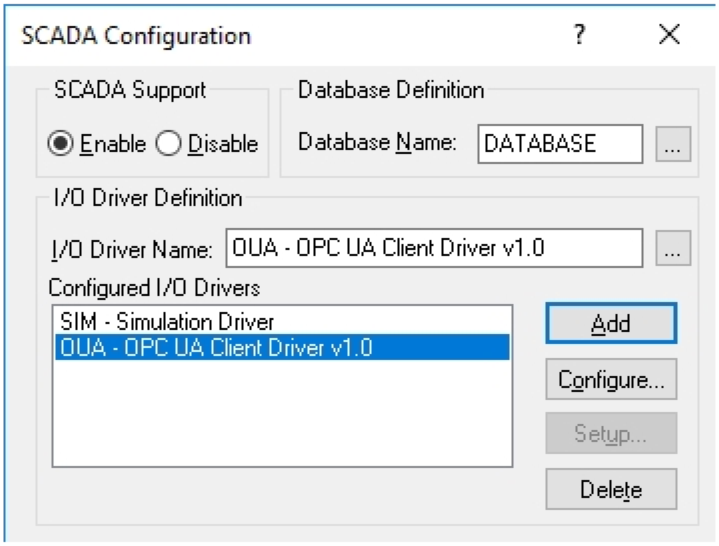
How to Enable Security in iFIX

1. From the Security Configuration Utility, on the Edit menu, select Configuration. The Configuration dialog box appears.
2. Under User-based Security, select Enabled.
3. On the File menu, click Save. You will now be requested to enter the user name and password to login.
4. Enter the user name and password for your user.

How to Add the OPC UA Driver in iFIX

NOTE: In iFIX 6.5 and greater, this driver is added by default. Follow these steps if you lost the defaults and need to add it again.

1. Shut down iFIX, and confirm that iFIX is not running.
2. On the Start menu, go to iFIX, and then click System Configuration.
3. On the Configure menu, select SCADA Configuration.
4. In the I/O Driver Name field, click the browse button to open the available driver list.
5. Select OUA - OPC Client and click OK.
6. Click Add to move the driver into the Configured Drivers list, as shown in the following figure.



SCADA Configuration

SCADA Support

● Enable ○ Disable

Database Definition

Database Name: DATABASE

I/O Driver Definition

I/O Driver Name: OUA - OPC UA Client Driver v1.0

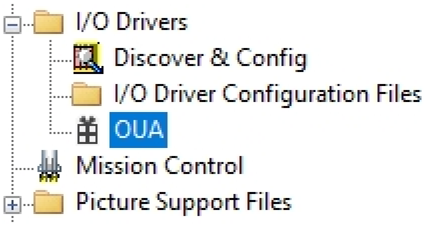
Configured I/O Drivers

SIM - Simulation Driver
OUA - OPC UA Client Driver v1.0

7. Save the configuration, and close the System Configuration utility.
8. Start or restart iFIX. Login with the user name and password configured to use the Configuration Hub tool, and then open the WorkSpace.

How to Start the Configuration Hub tool

1. From the iFIX WorkSpace, in the System tree, open the I/O Drivers folder.
2. Double-click the OUA entry to open Configuration Hub.



The server selection screen for Configuration Hub appears in a web browser.

3. Select the iFIX Server you want to connect to. The login screen appears for that selected server.
4. Enter the user name and password of the account configured to use the Configuration Hub tool.

   NOTE: Configuration Hub is currently not supported in Internet Explorer.

How to Add a Server in the Configuration Hub tool

The following steps describe how to add a server in the Configuration Hub tool.

1. On the computer where your OPC UA Server resides, confirm that your server is up and running. This step is important to ensure that you can retrieve the policies when configuring your server. You must do this before making any configuration additions or changes in the Configuration Hub tool.
2. From the Configuration Hub tool, on the Connection tab, click OPC UA, and then click the New button to add a server. The New OPC UA Server Connection dialog box appears.

3. In the Server Name field, enter the logical name of the computer where the OPC UA Server is running (include the fully qualified domain name if on a domain).
4. In the Endpoint URL field, enter 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 your OPC UA Server.
5. On the Details panel, select the Security Mode (None, Sign, or Sign and Encrypt).
6. In the Security Policy Uri field, select a 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.
7. Also on the Details panel, confirm that Disable is set to False so that you can use this driver to create groups and tags for iFIX. When the Disabled field is set to True, the configuration exists, but it is not available for use yet.
8. Select an authentication type: Anonymous or UserName/Password. It is recommended that you select UserName/Password to provide the highest level of encryption. Anonymous does not provide any protection for accessing data or logging.
9. If UserName/Password is selected, enter the user name and password to connect to the OPC UA Server.
10. Click Test Connection near the top of the Details panel to test the server configuration.
11. Click Save.

How to Trust Certificates for the OPC UA Client

The following steps describe how to configure the certificate for the server after you add it. A certificate must be configured before any connection with the server can be established. These steps are mandatory before you can use the driver in iFIX run mode.

IMPORTANT: iFIX must be running with security enabled in order to perform these steps. The OPC UA Server also must be running.

1. From Configuration Hub, select the configured server on the Connection tab. (The server name, endpoint URL, security mode, security policy, and authentication settings should already be configured.)
2. Click Test Connection. Based on the server security policies, the connection will fail with a ‘Server Not trusted’ message.
3. On the SCADA Server, trust the OPC UA Server's certificate:
   a. From the iFIX WorkSpace, on the Application tab, click OPC UA Configuration. The OPC UA Server Configuration Tool appears.
   b. Click the Trust List.
   c. Select the server name and click Trust. A message appears.
   d. Click Yes to continue.
4. Click Test Connection again. The test will fail again, this time with a ‘Server doesn’t trust this client’ message.

5. On the OPC UA Server, use the OPC UA Server's certificate management tool to trust the iFIX OPC UA Client Driver certificate.
6. Go back to the Configuration Hub tool, with the same server selected, click Test Connection again. The connection should now succeed.
7. You can now proceed to create Groups.

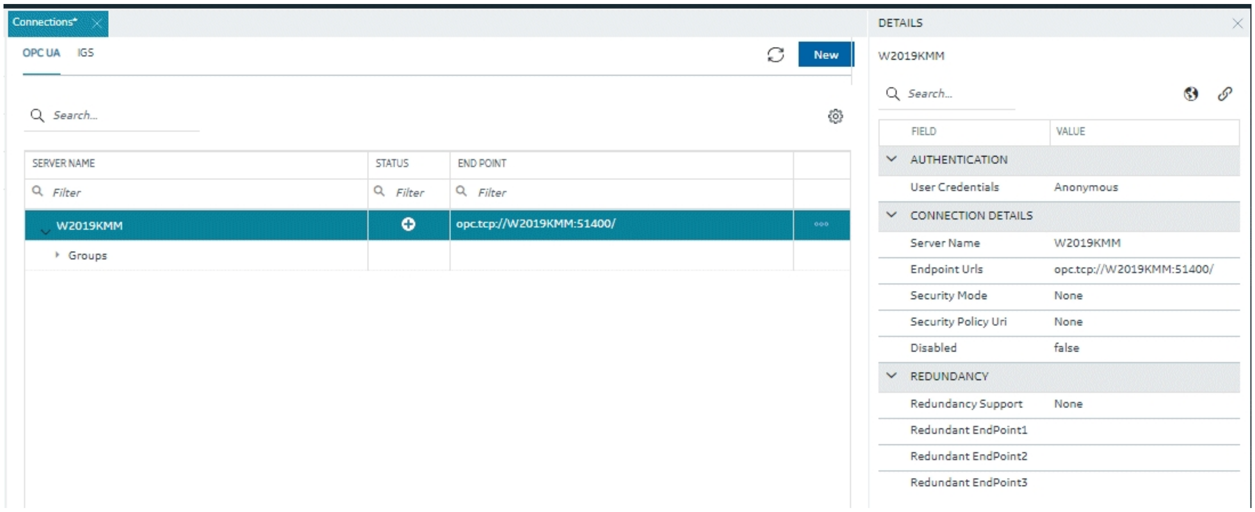
Server Configuration

Use the Connection screen in the Configuration Hub tool to add your OPC UA server, and configure your connection to the OPC UA Server, as shown in the following figure. From the Details panel, you can specify the OPC UA Server name, endpoint URL, security mode (signing options), security policy (encryption type), and authentication settings (anonymous or a specified user). Typically, the OPC UA Server is remote to the iFIX SCADA install.

After you add the connection, you must trust the server and client certificates before you can establish a connection with the server. A server must be enabled before you can add groups or driver tags.

The following text explains how to add a server and make a connection to it, so that you can subsequently add groups and tags.

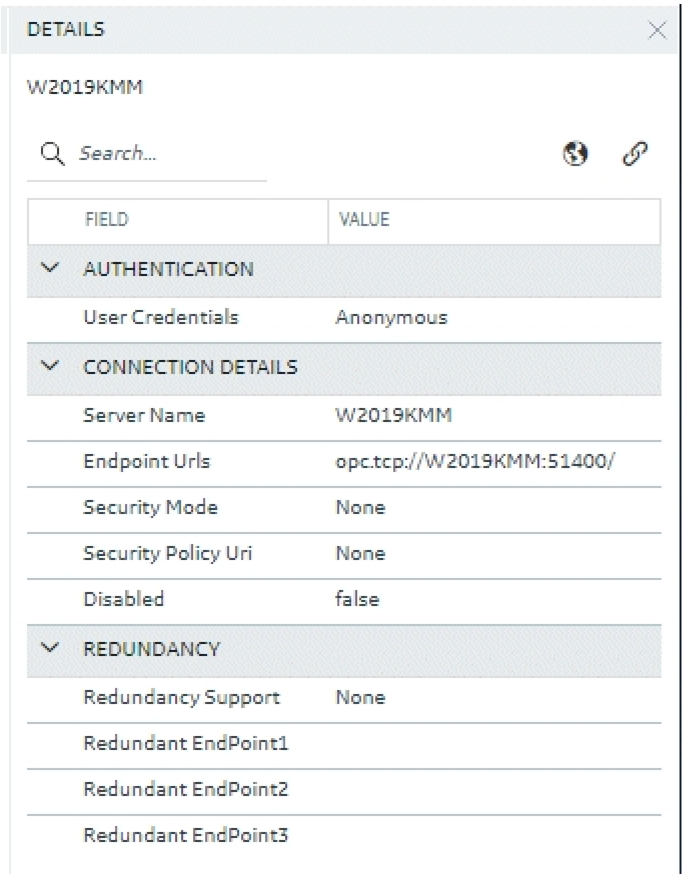
IMPORTANT: After you have successfully connected to an OPC UA Server and created Driver Tags, you should not change the configured Endpoint URL of the server unless the server instance has been moved or its endpoint has changed (such as if it now uses a different port). Changing the Endpoint URL to point to a different server can result in no data being available for some or all Driver Tags from that server. It is recommended to always create new server connections if connecting to a different server.



SERVER NAME	STATUS	END POINT
Filter	Filter	Filter
W2019KMM	⊕	opc.tcp://W2019KMM:51400/
Groups		

FIELD	VALUE
AUTHENTICATION	
User Credentials	Anonymous
CONNECTION DETAILS	
Server Name	W2019KMM
Endpoint Urls	opc.tcp://W2019KMM:51400/
Security Mode	None
Security Policy Uri	None
Disabled	false
REDUNDANCY	
Redundancy Support	None
Redundant EndPoint1	
Redundant EndPoint2	
Redundant EndPoint3	

Additionally, on the Connection tab, you can also specify the redundancy settings for your OPC UA Server connection, if you have this feature enabled on your OPC UA Server. On the Details panel, scroll to the end of the details to view the Redundancy settings, as show in the following figure. You can configure up to 3 backup servers (endpoint URLs).



DETAILS

W2019KMM

FIELD	VALUE
AUTHENTICATION	
User Credentials	Anonymous
CONNECTION DETAILS	
Server Name	W2019KMM
Endpoint Urls	opc.tcp://W2019KMM:51400/
Security Mode	None
Security Policy Uri	None
Disabled	false
REDUNDANCY	
Redundancy Support	None
Redundant EndPoint1	
Redundant EndPoint2	
Redundant EndPoint3	

Prerequisites to Add a Server in the Configuration Hub Tool

Before you can add a server on the Connection tab you must:

- Confirm that you have a license to use the OUA Driver.
- Create a user for Configuration Hub.
- In iFIX, add that user to the Application Designer group.
- Enable security in FIX.
- Switch the primary SCADA into maintenance mode, if using Enhanced Failover. You cannot use the Configuration Hub tool without doing so.
- In the iFIX System Configuration Utility (SCU), add the OPC UA Client Driver (OUA - OPC Client) to the I/O driver list (by default, on new installs this driver is added), and restart iFIX after you add it.

For details on these steps, refer to the "Quick Start: OPC UA Client Configuration" on page 4 topic.

Add a Server in Configuration Hub

The following steps describe how to add a server in Configuration Hub.

1. On the computer where your OPC UA Server resides, confirm that your server is up and running. This step is important to ensure that you can retrieve the policies when configuring your server. You must do this before making any configuration additions or changes in the Configuration Hub

tool.

2. From the Configuration Hub tool, on the Connection tab, click OPC UA, and then click the New button to add a server. The New OPC UA Server Connection dialog box appears.
3. In the Server Name field, enter the logical name of the computer where the OPC UA Server is running (include the fully qualified domain name if on a domain).
4. In the Endpoint URL field, enter 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 your OPC UA Server.
5. On the Details panel, select the Security Mode (None, Sign, or Sign and Encrypt).
6. In the Security Policy Uri field, select a 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.
7. Also on the Details panel, confirm that Disable is set to False so that you can use this driver to create groups and tags for iFIX. When the Disabled field is set to True, the configuration exists, but it is not available for use yet.
8. Select an authentication type: Anonymous or UserName/Password. It is recommended that you select UserName/Password to provide the highest level of encryption. Anonymous does not provide any protection for accessing data or logging.
9. If UserName/Password is selected, enter the user name and password to connect to the OPC UA Server.
10. Click Test Connection near the top of the Details panel to test the server configuration.
11. Click Save.

Manage Certificate Trust Lists

The following steps describe how to configure the certificate for the server after you add it. A certificate must be configured before any connection with the server can be established. These steps are mandatory before you can use the driver in iFIX run mode.

IMPORTANT: iFIX must be running with security enabled in order to perform these steps. The OPC UA Server also must be running.

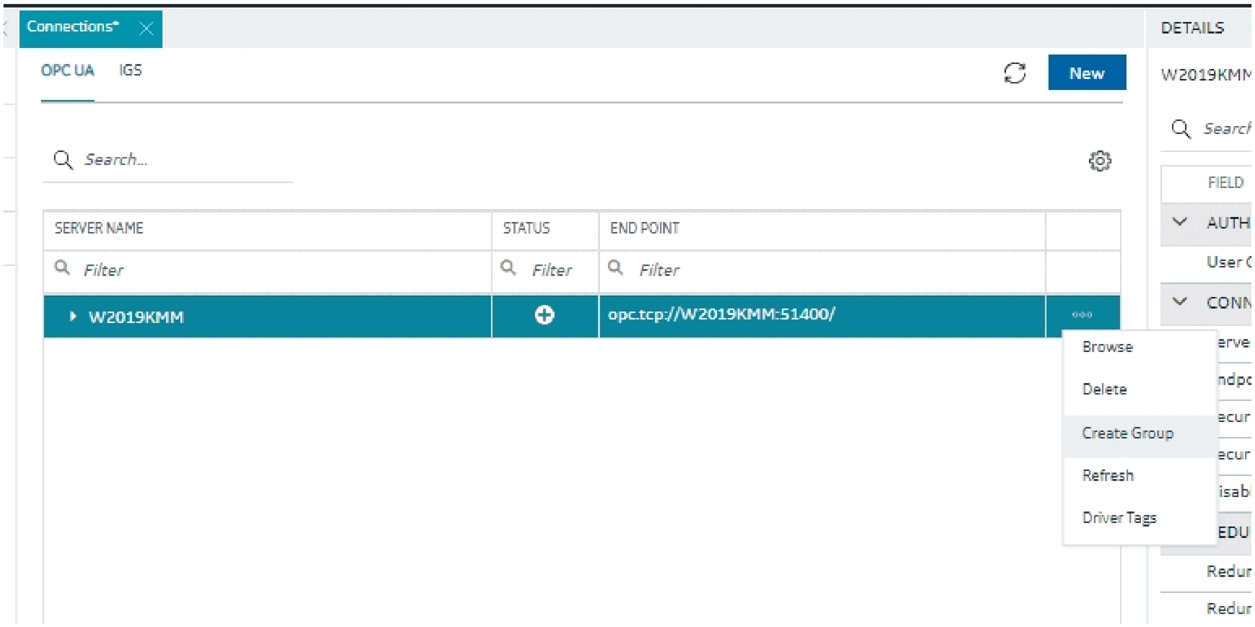
1. From the Configuration Hub tool, select the configured server on the Connection tab. (The server name, endpoint URL, security mode, security policy, and authentication settings should already be configured.)
2. Click Test Connection. Based on the server security policies, the connection will fail with a ‘Server Not trusted’ message.

3. On the SCADA Server, trust the OPC UA Server's certificate:
    a. From the iFIX WorkSpace, on the Application tab, click OPC UA Configuration. The OPC UA Server Configuration Tool appears.
    b. Click the Trust List.
    c. Select the server name and click Trust. A message appears.
    d. Click Yes to continue.
4. Click Test Connection again. The test will fail again, this time with a ‘Server doesn’t trust this client’ message.
5. On the OPC UA Server, use the OPC UA Server's certificate management tool to trust the iFIX OPC UA Client Driver certificate.
6. Go back to the Configuration Hub tool, with the same server selected, click Test Connection again. The connection should now succeed.
7. You can now proceed to create Groups.

Group Configuration

The Connections tab allows you to create, manage, and view groups added or associated with your OPC UA Server. In the New OPC UA Group Creation dialog box or in the Details panel for the specified group, you can configure the publishing interval and sampling interval for each group. 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 (-).

You must have an enabled OPC UA Server configured and a connection established before you add a group.



SERVER NAME	STATUS	END POINT
W2019KMM	⊕	opc.tcp://W2019KMM:51400/

Add a New Group

1. On the Connections tab, select OPC UA, and the click on the server.
2. Next to the server name click the ellipses (...) button and select Create Group. The New OPC UA Group Creation dialog box appears.
3. Enter the group name. Group names can be up to 19 alphanumeric characters including underscores (_) and hyphens (-).
4. Enter a Publishing Interval for the OPC UA subscription in milliseconds.
5. Enter a Sampling Interval to sample data sources in the OPC UA Server for changes, in milliseconds.
6. Click Create.
7. Click Save.

Delete a Group

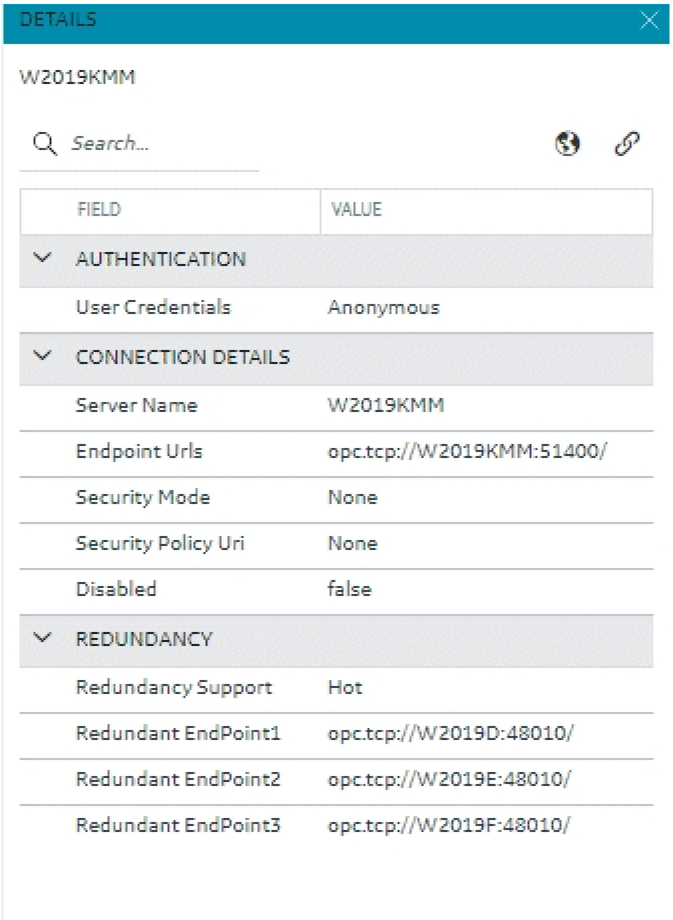
1. Select the row of the group name you want to delete.
2. Click the ellipses (...) button next to group name you want to delete.
3. Click Delete.
4. Click Save to complete the deletion and update the server.

Redundancy Configuration

On the Connection tab, you can also 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 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, 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).



W2019KMM

FIELD	VALUE
AUTHENTICATION	
User Credentials	Anonymous
CONNECTION DETAILS	
Server Name	W2019KMM
Endpoint Urls	opc.tcp://W2019KMM:51400/
Security Mode	None
Security Policy Uri	None
Disabled	false
REDUNDANCY	
Redundancy Support	Hot
Redundant EndPoint1	opc.tcp://W2019D:48010/
Redundant EndPoint2	opc.tcp://W2019E:48010/
Redundant EndPoint3	opc.tcp://W2019F:48010/

Configure Redundancy

1. From the Configuration Hub tool, on the Connection tab, select OPC UA, select the server, and then scroll down to the Redundancy section.
2. In the Mode drop-down lost, select the mode that you want to use for failover (when the active server becomes unavailable) in the OPC UA Client: Cold, Warm, or Hot. The mode defines how to perform the switch to a backup server if a failure is detected. If you are not sure what to select here, select Cold.
3. Enter the endpoint for each backup server you want to enable. You can enter up to three endpoint URLs below. The format is: opc.tcp://HostName:port/.
4. Click Save.

Special Considerations for Enhanced Failover

If using Enhanced Failover, you must be in Maintenance Mode before you log in the Configuration Hub UI. 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.

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

NOTE: If you are manually copying configuration files into the PDB\iFixUaClient subfolders on your Primary SCADA, you must do the same on your Secondary SCADA.

IMPORTANT: Be aware that if you add a server to the primary, you will need to deal with certificate management on the secondary as well.

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 Configuration Hub on the Primary will not be deleted on Secondary after the maintenance mode synchronization happens. The Secondary SCADA continues to retrieve data since the server and/or group still exist on the Secondary. As a workaround, manually delete the server and group files from the secondary SCADA, since you cannot run Configuration Hub on the secondary SCADA.

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. Do not delete the Group file for the group named OUA_DIAGNOSTICS. This is an internal group used by the OPC UA Client Driver. The file may be named differently on the Secondary than it is on the Primary node, but that is expected, and it should not be deleted.

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 servers 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. For more information on how these work, refer to the Diagnostics topic.

Index