iFIX 6.1

OPC UA Client Driver

Proprietary Notice

The information contained in this publication is believed to be accurate and reliable. However, General Electric Company assumes no responsibilities for any errors, omissions or inaccuracies. Information contained in the publication is subject to change without notice.

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

Trademark Notices

GE, the GE Monogram, and Predix are either registered trademarks or trademarks of General Electric Company.

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

All other trademarks are the property of their respective owners.

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

doc@ge.com

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

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

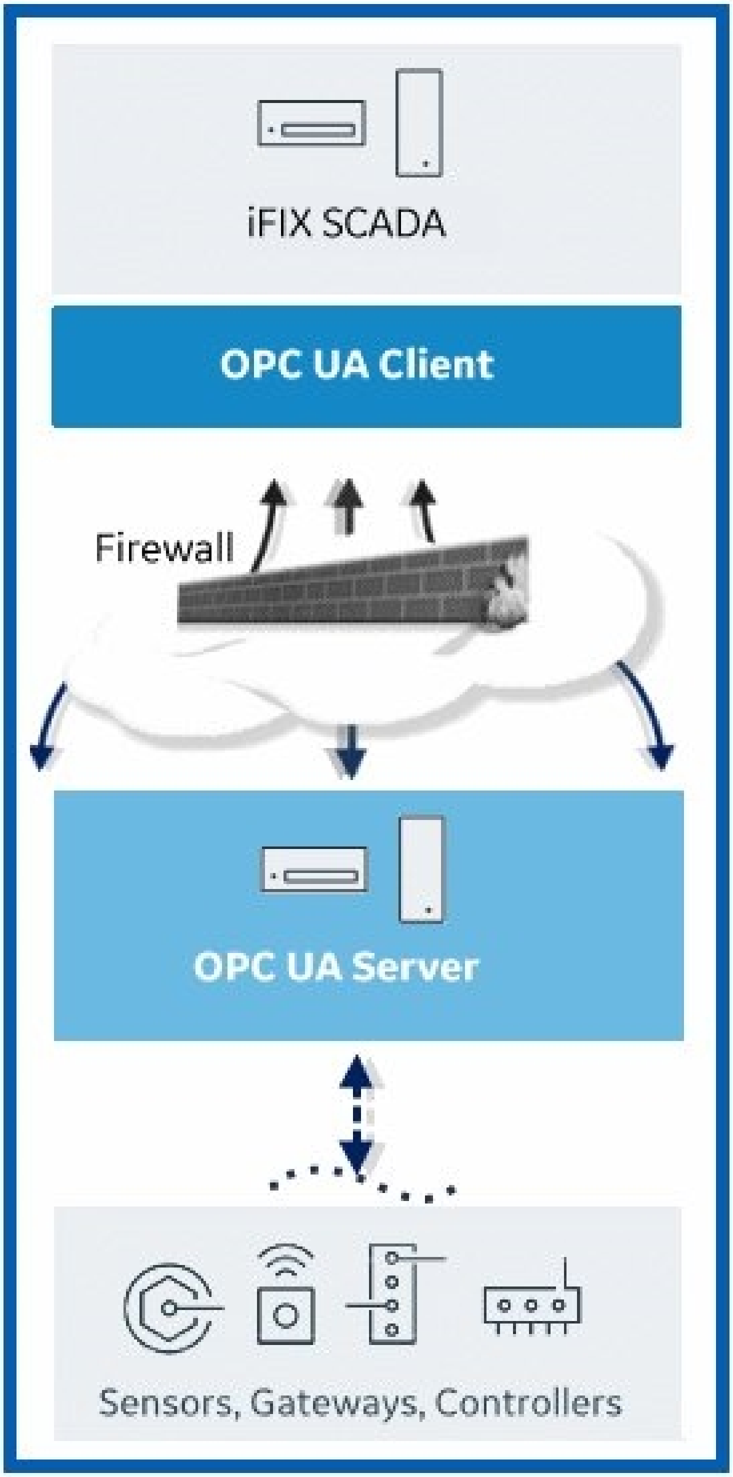
OPC UA defines a platform independent communication system that has a useful and adaptive Information Model for both industrial and business application needs. Like iFIX, OPC UA builds on the success and strength of common industrial standards. Developed by the OPC Foundation and meant to be platform 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 OPC UA Client Configuration tool to browse an OPC UA Server and automatically create driver tags in iFIX.

The OPC UA Client driver can be configured in a few simple steps. For details on these steps, refer to the "Quick Start: OPC UA Client Configuration" on page 10 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:

- A powerful HTML5 native web client that allows you to configure a connection to an OPC UA Server for iFIX, browse for data sources, and automatically populate the iFIX database with new tags.
- Web configuration tool available for use in Microsoft Edge, Google Chrome, and Mozilla Firefox.
- 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

When installing iFIX, self-signed certificates are created for the REST services and the NGINX Server that are used by this driver and its associated micro services.

Security is based on OPC UA standards. The OPC UA Client Driver provides a powerful HTML5 native web client to configure a connection to an OPC UA Server, browse for data sources, and automatically populate the iFIX database with new tags.

Use of the OPC UA Client Configuration Tool will require you to enable security in iFIX.

For more information on security, refer to the following sections:

- "Security Considerations" below
- "Certificate Management " below

Security Considerations

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

- The iFIX OPC UA Client Driver integrates with the iFIX security system for user authentication and authorization.
- The iFIX OPC UA Configuration tool must provide a valid iFIX user name and password in order to successfully connect to iFIX.
- In order to login to the iFIX OPC UA Configuration Tool, the iFIX user must have the following Application Features assigned: Database Save and Database Block Add-Delete.
- 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.
- When using Enhanced Failover, the OPC UA Client Driver will not allow you to make changes unless the primary node is in Maintenance Mode.

Certificate Management

When you install iFIX, several internal and external self-signed certificates are automatically created. Internal self-signed certificates are used in communication between iFIX applications and the OPC UA Server in run mode. External certificates are used by the OPC Client Driver Configuration tool and its associated micro services on the NGINX server when iFIX is in configure mode.

Following good security practices, both types of certificates (for internal and external communication) have expiration dates associated with them. When expired, in both instances, you will need to generate new certificates, import them to the Windows store, rebind them to a port, and re-establish the trust relationship between the server and the clients. All certificates associated with the iFIX OPC UA Client driver have an expiration period of 5 years.

For stronger security on your external certificates, you may want to use a server certificate that you purchased from a Certificate Authority (CA). The CA will require a Certificate Signing Request (CSR). For the OPC UA Client Driver Configuration tool, the custom certificate names can be entered in a configuration file, the ifix_config_service.json file. Using the iFIX Certificate Service Configuration tool (iFixConfigServiceCertTool.exe), you can import them to the Windows store and rebind them to a port.

For the NGINX, server, you need to modify the nginx.conf configuration file and restart Windows to update your certificates.

The following steps provide more details about updating certificates.

Update the Self-Signed Certificates for the OPC UA Client Driver (External Communication)

You may need to update these self-signed certificates if you want to change ports, regenerate them after an expiration period, or to assist in troubleshooting a failed connection.

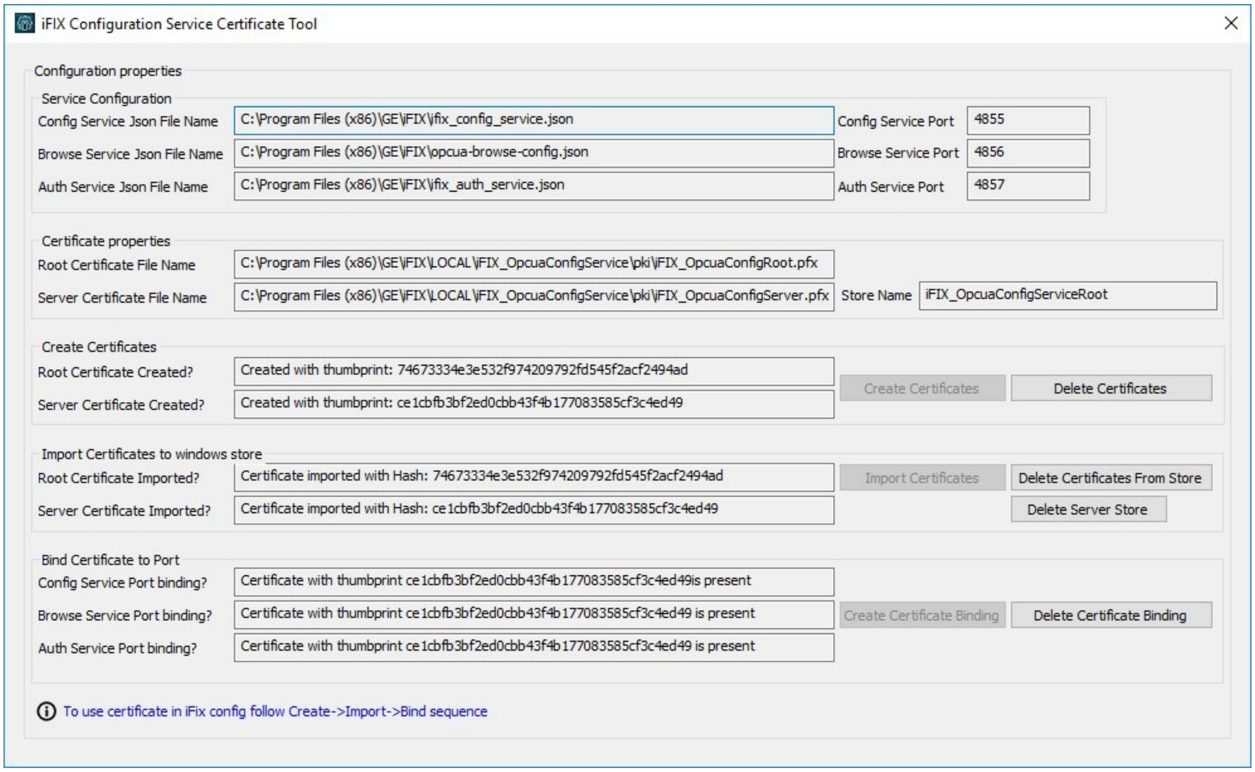
The following steps outline how to update your certificates for the OPC UA Client Configuration tool.

1. If you want to make changes to the default certificate settings, like change a port number for instance, update the ifix_config_service.json file in the iFIX base path (by default: C:\Program Files (x86)\GE\iFIX). For instance, you can change the default port of 4855 to something else.
2. Open the iFIX Configuration Service Certificate tool (iFixConfigServiceCertTool.exe) in the iFIX base path.
3. Click the Delete Certificates button to remove your existing certificates.
4. To generate the new self-signed certificate, click Create Certificates. This action creates your certificate, imports it, and then binds it.
5. Review the status in the Create Certificates, Import Certificates to Windows Store, and Bind Certificate to Port sections to ensure the certificate was created properly.
6. Close the iFIX Configuration Service Certificate Tool.
7. Restart iFIX.

Example of an Expired Certificate

When a certificate expires on the OPC UA Client Driver Configuration tool, your browser shows the "Not Secure" icon when you attempt to login:

Example of Successful Certificate Creation with Binding



iFIX Configuration Service Certificate Tool

Configuration properties

Service Configuration

Config Service Json File Name: C:\Program Files (x86)\GE\iFIX\ifix_config_service.json — Config Service Port: 4855

Browse Service Json File Name: C:\Program Files (x86)\GE\iFIX\opcua-browse-config.json — Browse Service Port: 4856

Auth Service Json File Name: C:\Program Files (x86)\GE\iFIX\ifix_auth_service.json — Auth Service Port: 4857

Certificate properties

Root Certificate File Name: C:\Program Files (x86)\GE\iFIX\LOCAL\iFIX_OpcuaConfigService\pki\iFIX_OpcuaConfigRoot.pfx

Server Certificate File Name: C:\Program Files (x86)\GE\iFIX\LOCAL\iFIX_OpcuaConfigService\pki\iFIX_OpcuaConfigServer.pfx — Store Name: iFIX_OpcuaConfigServiceRoot

Create Certificates

Root Certificate Created?: Created with thumbprint: 74673334e3e532f974209792fd545f2acf2494ad

Server Certificate Created?: Created with thumbprint: ce1cbfb3bf2ed0cbb43f4b177083585cf3c4ed49

Import Certificates to windows store

Root Certificate Imported?: Certificate imported with Hash: 74673334e3e532f974209792fd545f2acf2494ad

Server Certificate Imported?: Certificate imported with Hash: ce1cbfb3bf2ed0cbb43f4b177083585cf3c4ed49

Bind Certificate to Port

Config Service Port binding?: Certificate with thumbprint ce1cbfb3bf2ed0cbb43f4b177083585cf3c4ed49is present

Browse Service Port binding?: Certificate with thumbprint ce1cbfb3bf2ed0cbb43f4b177083585cf3c4ed49 is present

Auth Service Port binding?: Certificate with thumbprint ce1cbfb3bf2ed0cbb43f4b177083585cf3c4ed49 is present

ⓘ To use certificate in iFix config follow Create->Import->Bind sequence

Create Certificates
Delete Certificates
Import Certificates
Delete Certificates From Store
Delete Server Store
Create Certificate Binding
Delete Certificate Binding

Remote Instances of the OPC UA Client Driver Configuration Tool

If you are using the default self-signed certificates and would like to run the OPC UA Client Configuration tool from a computer other than the iFIX SCADA node, you need to copy the root certificate (iFIX_OpcuaConfigRoot.crt) into the Trusted Root Store in the Windows certificate store on the remote computer. Otherwise, the connection will be insecure.

The following steps outline how to install the root certificate for the OPC UA Client Configuration tool on anther computer.

1. Copy the iFIX_OpcuaConfigRoot.crt from the pki folder on local system (by default, it is C:\Program Files (x86)\GE\iFIX\LOCAL\iFIX_OpcuaConfigService\pki) to the destination computer.
2. Double-click the .crt file to launch the installer.
3. Click the Install Certificate button.
4. On the next screen, click Local Machine and then click Next.
5. When prompted for the certificate store, select Place All Certificates in This store.
6. Click Browse and select Trusted Root Certification Authorities and click Next. The last screen of the certificate import screen appears.
7. Click Finish.

Update the Self-Signed Certificates for the NGINX Server (External Communication)

You may need to update these self-signed certificates if you want to change ports, regenerate them after an expiration period, or to assist in troubleshooting a failed connection. The following steps outline how to do so.

1. If you want to make changes to the default certificate settings, like change a port number for instance, update the nginx.conf file (in the C:\Program Files (x86)\GE\iFIX\web\conf folder). For instance, you can change the default port of 9444 to something else here:

   ```
   server {
   listen 9444 ssl default_server;
   server_name localhost;
   ssl_certificate iFIX_OpcuaConfigServer.crt;
   ssl_certificate_key iFIX_OpcuaConfigServer.key;
   ```

2. From the Services desktop app, right-click the iFIX NGINX Server service and select Stop to shut down the service.

3. Shutdown iFIX.

4. Remove the certificate and key files from the C:\Program Files (x86)\GE\iFIX\LOCAL\iFIX_OpcuaConfigService\pki folder.

5. Remove certificate and key files from the C:\Program Files (x86)\GE\iFIX\web\conf folder.

6. Restart your computer.

7. Start iFIX.

Use a Certificates from External Certificate Authority (External Communication)

You can configure certificates received from external Certificate Authorities (CA), such as VeriSign and DigiCert, for use with the OPC UA Client Configuration tool and its supporting NGINX web server. For the OPC UA Client Configuration tool, you will need to update the ifix_config_service.json file and run the iFixConfigServiceCertTool.exe. For NGINX, you will need to update the nginx.conf file and restart your computer. The following steps outline the process for updating the certificates for both the OPC UA Client Configuration tool and NGINX server, if you want to use another certificate for external communication.

1. Remove the certificate and key files from the C:\Program Files (x86)\GE\iFIX\LOCAL\iFIX_OpcuaConfigService\pki folder.

2. Remove the certificate and key files from the C:\Program Files (x86)\GE\iFIX\web\conf folder.

3. Copy the external certificate and key files into the C:\Program Files (x86)\GE\iFIX\LOCAL\iFIX_OpcuaConfigService\pki folder.

4. Copy the external certificate and key files into the C:\Program Files (x86)\GE\iFIX\web\conf folder.

5. In Notepad or another text editor, open the ifix_config_service.json file (by default: C:\Program Files (x86)\GE\iFIX folder).

6. Update the following settings in bold and save the file:
   - "rootCertificateName": "**iFIX_OpcuaConfigRoot**" - This line contains the name of the root certificate.
   - "serverCertificateName": "**iFIX_OpcuaConfigServer**", - This line contains the name of the server certificate.
   - "serverCertificateStoreName": "**iFIX_OpcuaConfigServiceRoot**" - This line contains the name of the Windows server certificate store.
   - "serverCertificatePassPhrase": "**B08B21B12A854B7CA22F27139411DA69**" - This line contains the certificate pass phrase for both root and server certificates.
7. Open the iFIX Configuration Service Certificate tool (iFixConfigServiceCertTool.exe) in the iFIX base path.
8. Review the status in the Import Certificates to Windows Store and Bind Certificate to Port sections to ensure the certificate was created properly.
9. Close the iFIX Configuration Service Certificate Tool.
10. In Notepad or another text editor, open the nginx.conf file in the C:\Program Files (x86)\GE\iFIX\web\conf folder.
11. Update the certificate name and key with the new certificate (marked in bold with actual file names), and save the file:

    ```
    server {
    listen 9444 ssl default_server;
    server_name localhost;
    ssl_certificate iFIX_OpcuaConfigServer.crt;
    ssl_certificate_key iFIX_OpcuaConfigServer.key;
    ```
12. From the Services desktop app, right-click the iFIX NGINX Server service and select Stop to shut down the service.
13. Shutdown iFIX.
14. Restart your computer.
15. Start iFIX.

Establishing the Trust Relationship Between the Client Driver and the Server

The following steps describe how to establish the trust relationships using the OPC UA Client Configuration tool, the iFIX OPC UA Server Configuration tool, and the OPC UA Server.

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 OPC UA Client Configuration 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’ error.
3. Trust the OPC UA Server's certificate in the iFIX OPC UA Server Configuration tool:
   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 OPC UA Configuration tool, with the same server selected, click Test Connection again. The connection should now succeed.

Generating New Self-Signed Certificates (Internal Communication)

In iFIX run mode, when your internal certificate expires nothing will change until you attempt to make a configuration change in the OPC UA Client Configuration tool, you restart iFIX, or a reconnection is attempted after you lose connectivity to your OPC UA Server. At that point in time, or when the actual certificate expires, you need to create a new self-signed certificate and establish the trust relationship. You can do all this in the iFIX OPC UA Server Configuration tool.

To generate a new self-signed certificate for your internal driver communication:

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 Certificate tab, click Generate Self-Signed.
4. On the Trust tab, click the Refresh button.
5. Select the certificate and click Trust.
6. Select Save and Exit to save all your changes.
7. Restart iFIX.

Allow a Modified Port Through the Windows Firewall

If you enable a new port through your certificate settings, be sure to also allow that port the Windows firewall as well.

1. From the Start menu, open the Windows Firewall with Advanced Security.
2. Click Inbound Rules in the left frame of the window.
3. Right-click Inbound Rules, and select New Rule…
4. For the Rule Type, click Port. Click Next.
5. On the Ports and Protocols screen, select TCP and enter the port number. For example, you may have decided to use a different port than one of the defaults: 9444, 4855, 4856, and 4857.
6. Leave the defaults for the other fields.
7. On the last screen enter a name for the rule and click Finish.

Use Certificates with Enhanced Failover

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.

Configuration

Configuration for the OPC UA Client Driver includes the following:

- Quick Start: OPC UA Client Configuration
- Overview of the OPC UA Client Configuration Tool
- Server Configuration
- Group Configuration
- Driver Tag 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 the web configuration tool. The following steps outline how to quickly add and configure your driver.

1. In iFIX, add user privileges (Database Save and Database Block Add-Delete) and enable security.
2. In the iFIX System Configuration Utility, add the OPC UA Client driver.
3. Start or restart iFIX.
4. Start the OPC UA Driver Configuration tool 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 OPC UA Client Configuration Tool, click the plus sign (+) next to the Servers list to add a server.
7. On the Connection tab, click Test Connection to begin the certificate trust process:
    a. On the iFIX SCADA, in the OPC UA Server Configuration tool, trust the server.
    b. On the OPC UA Server, in its certificate management tool, trust the OPC UA Client Driver.
    c. In the OPC UA Client Configuration Tool, click Test Connection again. The connection should succeed.
8. Proceed to create your Groups and Driver Tags.

IMPORTANT: Every time you make a change in the configuration from the OPC UA Client Configuration tool, 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 OPC UA Client Configuration tool.

Steps from the quick start are expanded below with more details.

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

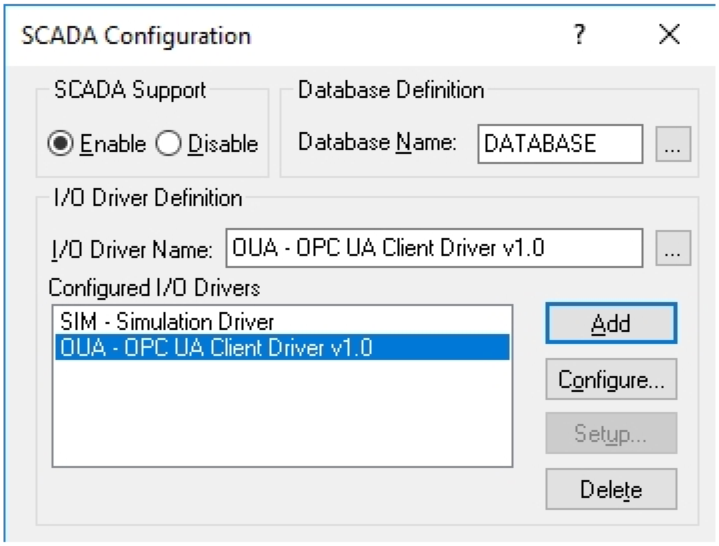
1. Start iFIX.
2. In the WorkSpace, on the Applications tab, click Security and then Security Configuration Utility.
3. On the Edit menu select User Accounts. The User Accounts dialog box appears.
4. Click Add. The User Profile dialog box appears.
5. If using Windows users, select Use Windows Security.
6. In the User Name field, enter the user that you created for use with iFIX.
7. If needed, enter the Domain.
8. Modify group and security areas as appropriate.
9. For Application Features, click Modify. The Application Features dialog box appears.
10. For User-based Security, select Enabled.
11. Scroll the Available list to find both Database Save and Database Block Add-Delete. Click Add to add the privileges.
12. Click OK, and OK again.
13. 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

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

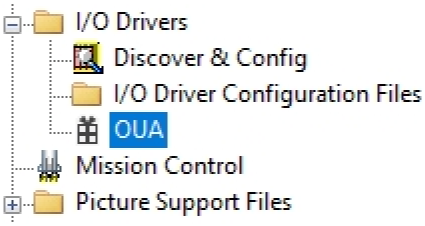
I/O Driver Definition – I/O Driver Name: OUA - OPC UA Client Driver v1.0

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 OPC UA Client Configuration tool, and then open the WorkSpace.

How to Start the OPC UA Client Configuration Tool

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



The iFIX UA Client Configuration tool appears.

3. Enter the user name and password of the account configured to use the OPC UA Client Configuration tool.

   NOTE: You can use Edge, Chrome, or Firefox to open this tool. The OPC UA Client Configuration tool is currently not supported in Internet Explorer.

How to Add a Server in the OPC UA Client Configuration Tool

The following steps describe how to add a server in the OPC UA Configuration 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 changes in the OPC UA Client Configuration Tool.
2. From the OPC UA Configuration tool, on the Connection tab, click the plus icon (+) to add a server.
3. On the Connection tab, in the SERVER NAME field, enter the logical name of the computer where

the OPC UA Server is running.

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. Click Discover Policies to view what policies are available for selection on your OPC UA Server. 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.
6. Click Enable so that you can use this driver to create groups and tags for iFIX. When disabled, the configuration exists, but it is not available for use yet.
7. 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.
8. If UserName/Password is selected, enter the user name and password to connect to the OPC UA Server.
9. Click Create to add the server configuration.

How to Trust Certificates for the OPC UA Client Configuration Tool

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 OPC UA Configuration 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 OPC UA Configuration tool, with the same server selected, click Test Connection again. The connection should now succeed.
7. You can now proceed to create Groups and Driver Tags.

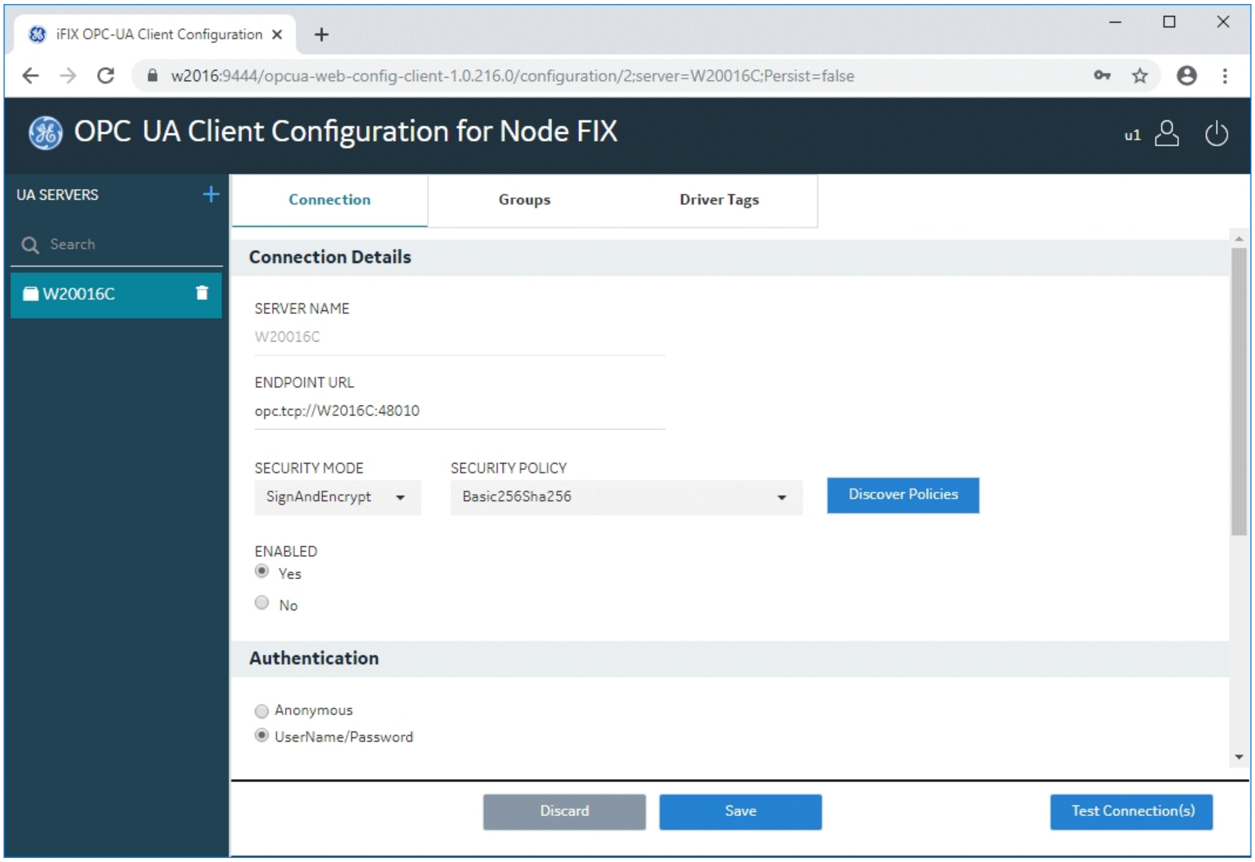
Server Configuration

Use the Connection tab in the OPC UA Client Configuration tool to configure your connection to the OPC UA Server, as shown in the following figure. On the Connection tab you 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.



iFIX OPC-UA Client Configuration

w2016:9444/opcua-web-config-client-1.0.216.0/configuration/2;server=W20016C;Persist=false

OPC UA Client Configuration for Node FIX

Connection Details

SERVER NAME
W20016C

ENDPOINT URL
opc.tcp://W2016C:48010

SECURITY MODE
SignAndEncrypt

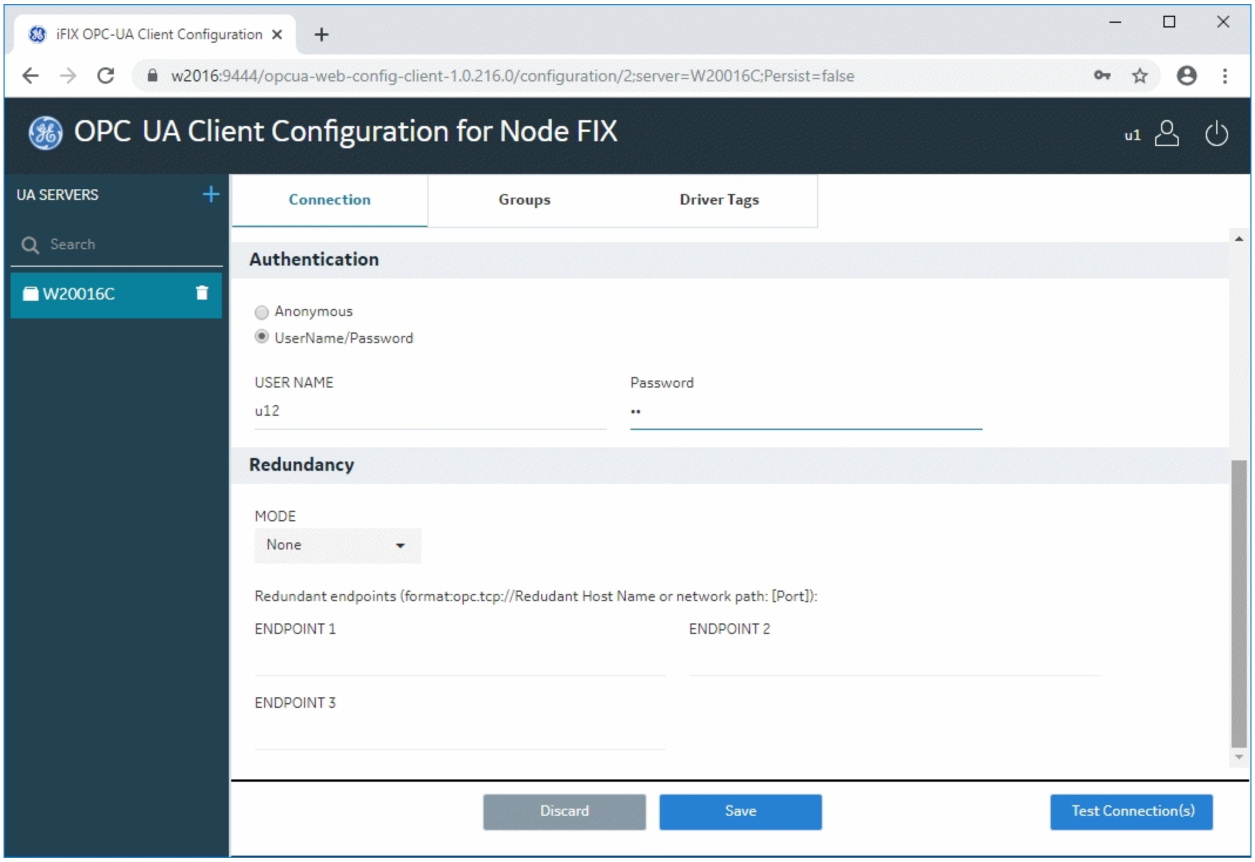
SECURITY POLICY
Basic256Sha256

ENABLED
● Yes
○ No

Authentication

○ Anonymous
● UserName/Password

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. Scroll to view the Redundancy settings on the Connection tab, as show in the following figure. You can configure up to 3 backup servers (endpoint URLs).



iFIX OPC-UA Client Configuration

w2016:9444/opcua-web-config-client-1.0.216.0/configuration/2;server=W20016C;Persist=false

OPC UA Client Configuration for Node FIX

UA SERVERS

W20016C

Connection | Groups | Driver Tags

Authentication

○ Anonymous
● UserName/Password

USER NAME: u12

Password: ••

Redundancy

MODE: None

Redundant endpoints (format:opc.tcp://Redudant Host Name or network path: [Port]):

ENDPOINT 1

ENDPOINT 2

ENDPOINT 3

For details on each of the server configurations fields on this screen, refer to the Overview of the OPC UA Client Configuration Tool topic.

Prerequisites to Add a Server in the OPC UA Client Configuration Tool

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

- Confirm that you have a license to use the OPC UA Client Driver.
- Create a user for the iFIX OPC UA Client Driver.
- In iFIX, confirm that the user is assigned the Database Save and Database Block Add-Delete application features.
- Enable security in FIX.
- Switch the primary SCADA into maintenance mode, if using Enhanced Failover. You cannot use the OPC UA Client Driver Configuration 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, and restart iFIX after you add it.

For details on these steps, refer to the "Quick Start: OPC UA Client Configuration" on page 10 topic.

Add a Server in the OPC UA Client Configuration Tool

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

1. On the computer where your OPC UA Server resides, confirm that your OPC UA 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 changes in the OPC UA Client Configuration Tool.
2. From the OPC UA Configuration tool, on the Connection tab, click the plus icon (+) to add a server.
3. On the Connection tab, in the SERVER NAME field, enter the logical name of the computer where the OPC UA Server is running.
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. Click Discover Policies to view what policies are available for selection on your OPC UA Server. 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.
6. Click Enable so that you can use this driver to create groups and tags for iFIX. When disabled, the configuration exists, but it is not available for use yet.
7. 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.
8. If UserName/Password is selected, enter the user name and password to connect to the OPC UA Server.
9. Click Create to add the server configuration.

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.

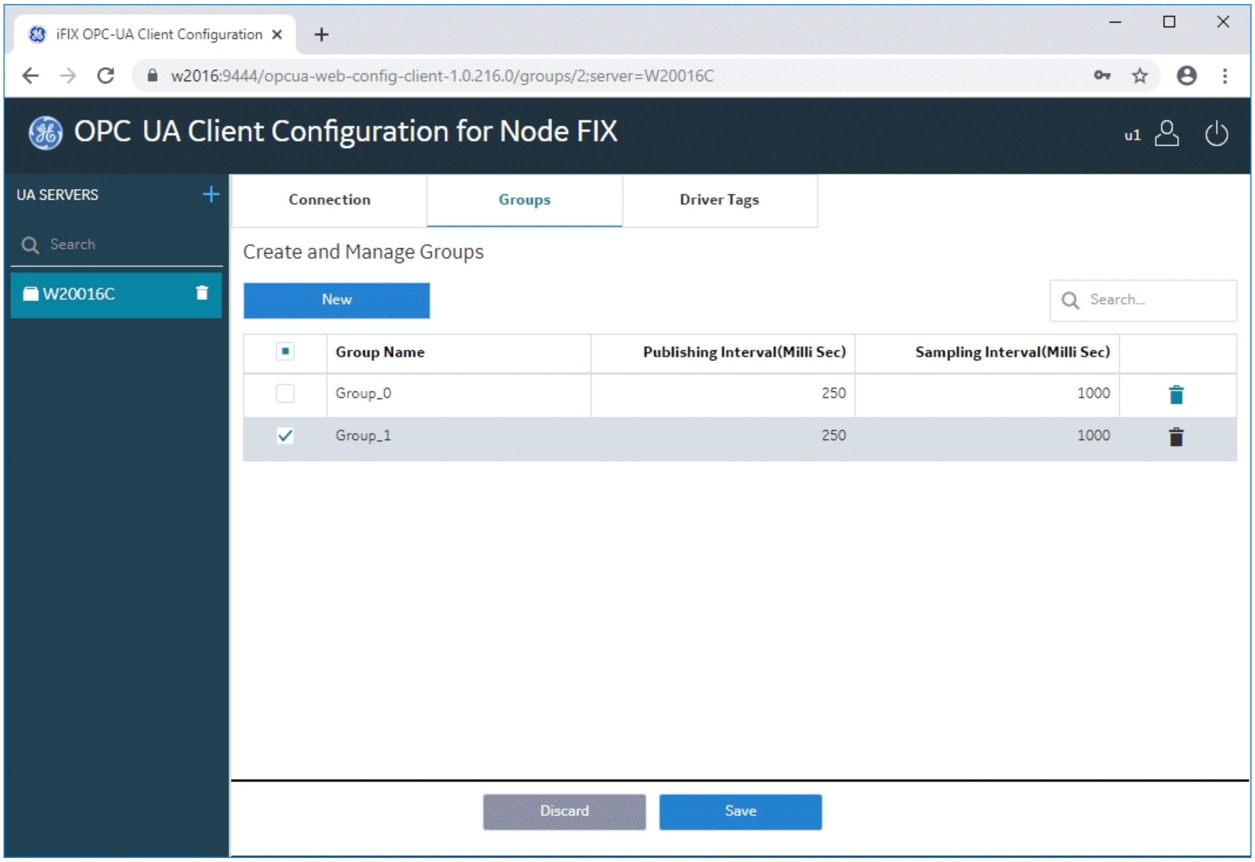
1. From the OPC UA Configuration tool, select the configured server on the Connection tab. (The server name, endpoint URL, security mode, security policy, and authentication settings should already be configured.)
2. Click Test Connection. Based on the server security policies, the connection will fail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

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 OPC UA Configuration tool, with the same server selected, click Test Connection again. The connection should now succeed.
7. You can now proceed to create Groups and Driver Tags.

Group Configuration

The Groups tab allows you to create, manage, and view groups added or associated with your OPC UA Server. It also allows you to 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 can use this tab.


iFIX OPC-UA Client Configuration
w2016:9444/opcua-web-config-client-1.0.216.0/groups/2;server=W20016C
OPC UA Client Configuration for Node FIX
u1
UA SERVERS
Search
W20016C
Connection
Groups
Driver Tags
New
Search...
Discard
Save

Create and Manage Groups

■	Group Name	Publishing Interval(Milli Sec)	Sampling Interval(Milli Sec)	
□	Group_0	250	1000	🗑
✓	Group_1	250	1000	🗑

Add a New Group

1. On the Groups tab, click New.
2. Enter the group name. Group names can be up to 19 alphanumeric characters including underscores (_) and hyphens (-).
3. Enter a Publishing Interval for the OPC UA subscription in milliseconds.
4. Enter a Sampling Interval to sample data sources in the OPC UA Server for changes, in milliseconds.
5. Click Save.

Delete a Group

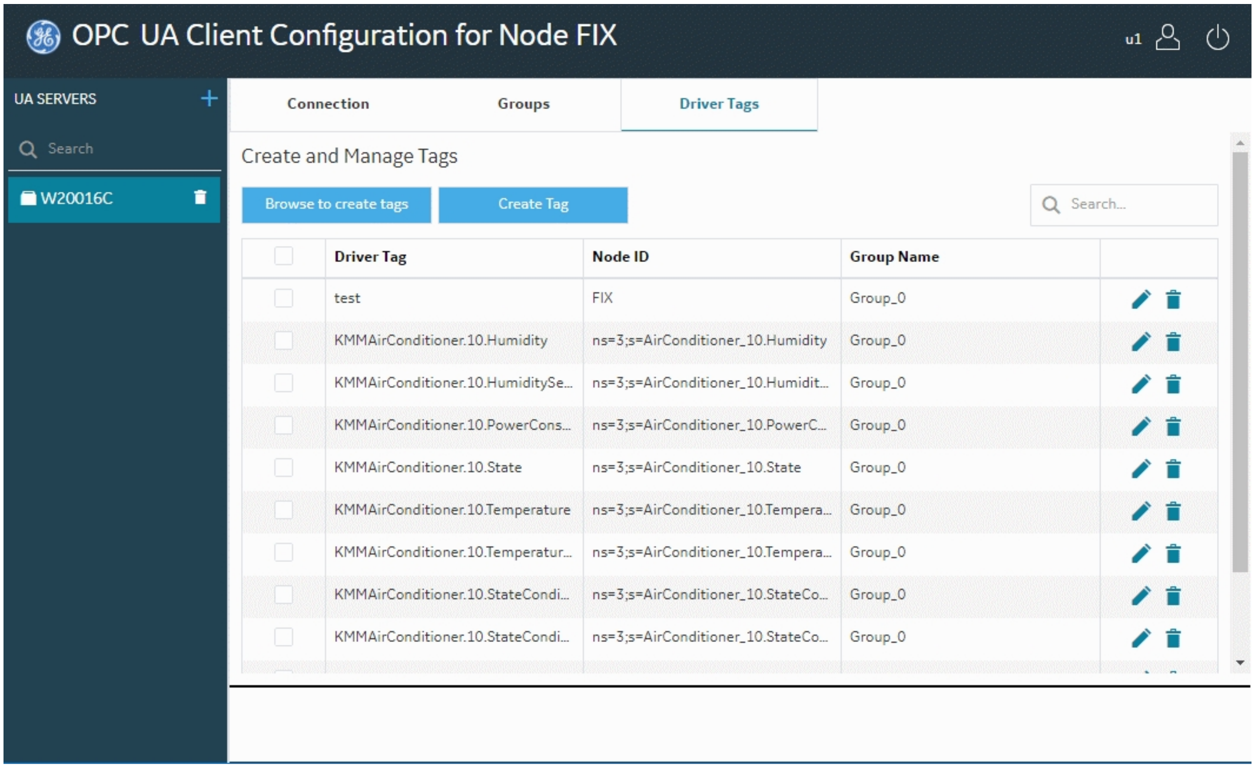
1. Select the group, by clicking the check box next to the group name or selecting the row.
2. Click the Trash Can icon.
3. Click Save to complete the deletion and update the server.

Driver Tag Configuration

The Driver Tags tab lists the data points defined for this OPC UA Server, along with the node ID and group name. You can automatically generate one or more tags at a time by browsing the OPC UA

Server, or you can manually add a single tag if you know the Node ID from the OPC UA Server. When autocreating a group of tags, it is recommended that you create no more than the maximum of 5,000 at a time.

You must have an enabled OPC UA Server configured and a connection established before you can use this tab.



□	Driver Tag	Node ID	Group Name
□	test	FIX	Group_0
□	KMMAirConditioner.10.Humidity	ns=3;s=AirConditioner_10.Humidity	Group_0
□	KMMAirConditioner.10.HumiditySe...	ns=3;s=AirConditioner_10.Humidit...	Group_0
□	KMMAirConditioner.10.PowerCons...	ns=3;s=AirConditioner_10.PowerC...	Group_0
□	KMMAirConditioner.10.State	ns=3;s=AirConditioner_10.State	Group_0
□	KMMAirConditioner.10.Temperature	ns=3;s=AirConditioner_10.Tempera...	Group_0
□	KMMAirConditioner.10.Temperatur...	ns=3;s=AirConditioner_10.Tempera...	Group_0
□	KMMAirConditioner.10.StateCondi...	ns=3;s=AirConditioner_10.StateCo...	Group_0
□	KMMAirConditioner.10.StateCondi...	ns=3;s=AirConditioner_10.StateCo...	Group_0

How to Autocreate Tags by Browsing the OPC UA Server

1. On the Driver Tags tab, click Browse Tags. The browse tag screen appears.
2. From the Server folder, place a check mark next to all the tags you want to create.
3. To include all children from a folder, right-click the folder and choose Select All Children, as shown in the following figure.
4. Click Create Tags. The tags are moved to a staging area to prepare the creation in the iFIX database.
5. If you want to add a prefix to the selected driver tag names, enter it in the Name Prefix field.
6. If you want to shorten the tag names for the selected tags, enter a value in the Number of Levels to Strip field. This number indicates the number of levels in the namespace to be stripped off from the beginning of the tag names.
7. Click Create (number) Tags. A message appears informing you that the driver tags will get created in the iFIX database, and the driver will be restarted.

8. Click Yes to continue. A message will appear when the tag is successfully created in the database.

How to Manually Create a Single Tag from the OPC UA Server

Use these steps if you want to create a tag but you are not connected to the server and know the node ID. You might also want to use these steps for full editing control over the driver tag and iFIX tag names. For example, say you want to add more details in a tag name - more than just adding a prefix and/or stripping out levels of text during the autogeneration of tags.

1. On the Driver Tags tab, click Create Tag. The tag details screen appears, as shown in the following figure.

2. Click the Browse button to select a tag from the server. The driver tag name, iFIX tag name, and Node ID are auto-populated.
3. If you are not connected to the server and cannot browse to it, you can still create the tag in iFIX. In this case, you would then need to know the node ID from the server; the driver tag name and iFIX tag name can be user-defined. Enter this information into the Driver Tag Name, iFIX Tag Name, and Node ID fields.

   Valid Entries for Driver Tag Name: Up to 79 alphanumeric characters including underscores (_), hyphens (-), and the following characters: ~!@#$%^&*()_+-={}|[]\:";'?,./`

   Valid Entries for iFIX Tag Name: Up to 256 alphanumeric characters including underscores (_), hyphens (-), exclamation marks (!), number symbols (#), percent signs (%), dollar signs ($), pipe bars (|), and brackets ([ ]).

   Valid Entries for Node ID: ~!@#$%^&*()_+-={}|[]\:";'?,./`
4. In the iFIX Block Type drop-down list, select a block type: Numeric: AI, AA, AR, and AO; Boolean: DI, DA, DR, DO; or String: TX.
5. In the Group Name field, select a group. (Groups are defined on the Group tab.)
6. If this item is an array, select the Is Array check box. When the Array check box is selected, the Start Index and End Index fields appear.
7. If this item is an array, enter values into the Start Index and End Index fields.
8. Click Create Tag. A message appears informing you that the driver tag will get created in the iFIX database, and the driver will be restarted.
9. Click Yes to continue. A message will appear when the tag is successfully created in the database.

Adding a Prefix or Stripping Levels When Autocreating Tags

You can add a prefix and remove extra levels from tags from the staging area on the Driver Tags tab. To view the staging screen, you first need to browse the OPC UA Server to select the tags you want to add. By default, all tags are selected, but you can apply the Name Prefix and Number of Levels to Strip settings to all tags or only the ones you select in the list.

Autocreating Tags Using the Database Manager

As an alternate option, you can use the tag import iFIX Database Manager to autocreate tags. Autocreating driver tags during database import will significantly slow down the import process, due to the frequent disk access to update the underlying configuration and the fact that Database Manager creates a single tag at a time during import.

If creating a database block directly in the Database Manager or via an import, you can autocreate a group, and use node id as the driver tag. The driver tag's name will be the same as the node ID in this case. An OPC UA Server cannot be autocreated in this manner. However, you can use an existing group, or autocreate a group with the default settings by specifying a new group name.

Autocreate of driver tags from the Database Manager import only works for node IDs (I/O address field in database) no longer than 80 characters.

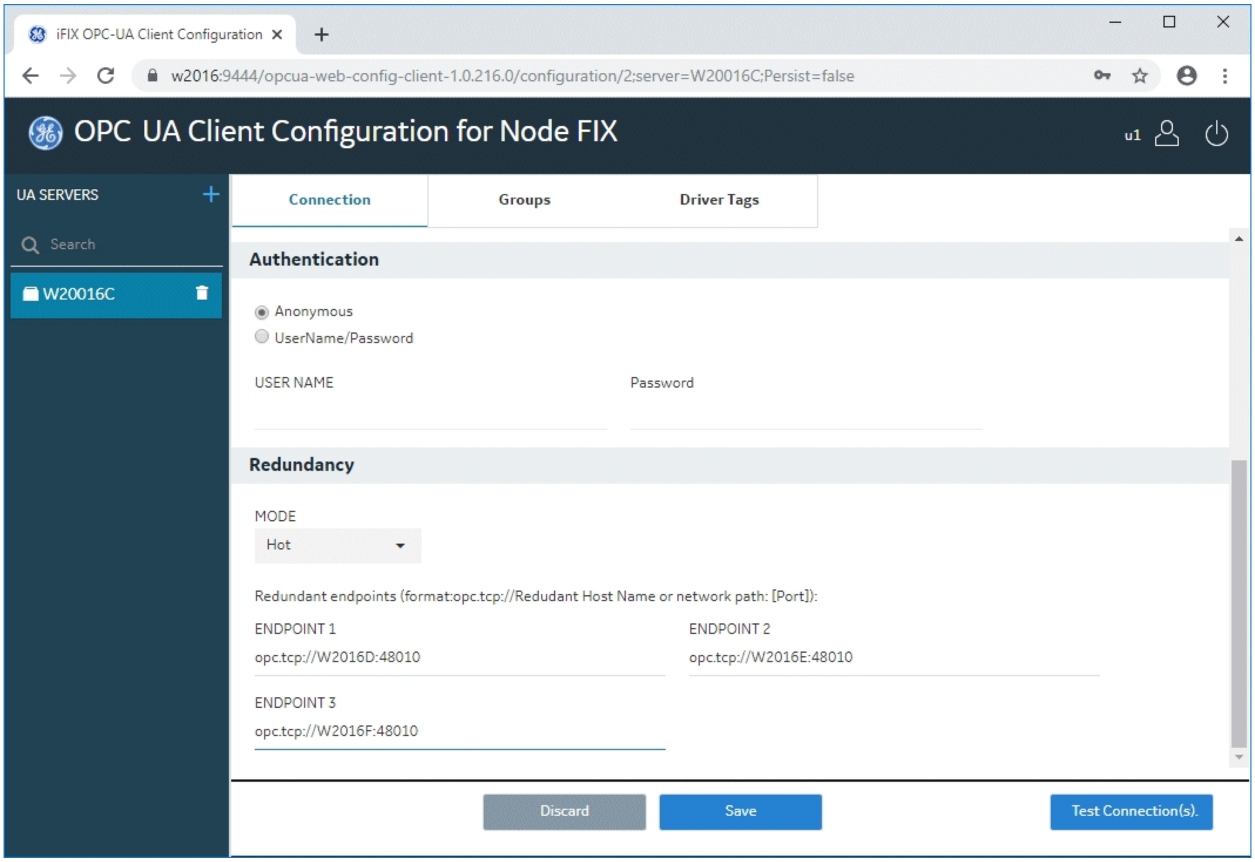
NOTE: If you create or load a database with a large numbers of tags for I/O addresses that contain node IDs, you may encounter performance issues with the Database Manager as it makes a one-time conversion of those addresses into driver tags. After the conversion takes place, the performance issues should subside and not be encountered again.

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).



iFIX OPC-UA Client Configuration
w2016:9444/opcua-web-config-client-1.0.216.0/configuration/2;server=W20016C;Persist=false
OPC UA Client Configuration for Node FIX
u1
UA SERVERS
Search
W20016C
Connection
Groups
Driver Tags
Discard
Save
Test Connection(s).

Authentication

● Anonymous
○ UserName/Password

USER NAME

Password

Redundancy

MODE: Hot

Redundant endpoints (format:opc.tcp://Redudant Host Name or network path: [Port]):

ENDPOINT 1: opc.tcp://W2016D:48010

ENDPOINT 2: opc.tcp://W2016E:48010

ENDPOINT 3: opc.tcp://W2016F:48010

Configure Redundancy

1. From the OPC UA Configuration tool, on the Connection tab, 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.

Technical Reference

The OPC UA Client Driver help provides advanced guidance on the following:

- "Troubleshooting the OPC UA Client" on the facing page
- "Diagnostics" on page 25
- "Logging" on page 27
- "iFIX Block and Data Type Support" on page 31

- "Advanced Configuration" on page 32
- "Special Considerations for Enhanced Failover" on page 37

Troubleshooting the OPC UA Client

How to Obtain Diagnostic Information on Your Connections

You can obtain diagnostic information on the OPC UA Client from the following:

- Mission Control
- Existing Database Fields
- Special I/O Addresses

Refer to the "Diagnostics" on page 25 section for more detailed information.

How to Use Logging to Troubleshoot

When troubleshooting the OPC UA Client Driver, there are several logs that you may find useful to review. These include the logs for the:

- OPC UA Client Driver Tool
- OUASPOLL driver application
- Browse Micro service
- iFIX Config Micro service
- iFIX Auth Micro service
- Certificate Management
- NGINX Web Server
- Browser Console

For each of these log files, you may want to enable and or change the logging levels to get more details to review. For more information on what each of these logs does and where they are located, refer to the Logging section.

IMPORTANT: Whenever you change a logging configuration, you need to restart iFIX to enforce your new settings. Be aware that if you enable or increase logging levels in your application or micro service, that the higher the log setting, the greater the potential to impact performance. Review your log files after any changes. Make sure that enough appropriate and consistent logging content is output in the files to troubleshoot.

How to Resolve Connection Issues

If something goes wrong with the connection, make sure you can ping instance of the server from the client machines. Next, make sure application is allowed through firewalls. If you still cannot log in, try temporarily changing the security protocol policy to None, just to see if you can connect. The steps are outlined in the following sections.

Checking the Connections

1. From the Start menu, open the Command Prompt.
2. Enter the ping command followed by the IP address. For example: ping 1.2.3.4.

NOTE: If you do not know the IP address you want to ping, from a command prompt on the other computer, run the ipconfig command. The IP should be listed next to the IPv4 Address line.

3. Watch the results. You should receive a result like this:

   ```
   Reply from 1.2.3.4: bytes=32 time<1ms TTL=128
   ```

   Instead of something like: Request Timed Our or Destination Host Unreachable. If you do not get a reply, you likely have a networking issue. See Editing the HOSTS File for a possible solution.

Manually Adding a Port to Firewall Exception List

1. From the Start menu, open the Windows Firewall with Advanced Security.
2. Click Inbound Rules in the left frame of the window.
3. Right-click Inbound Rules, and select New Rule…
4. For the Rule Type, click Port. Click Next.
5. On the Ports and Protocols screen, select TCP and enter the port number. For example, ports 9444, 4855, 4856, and 4857 are ports that may require opening (if you are using the default ports).
6. Leave the defaults for the other fields.
7. On the last screen enter a name for the rule and click Finish.

Temporarily Changing the Security Policy

1. On the computer where your OPC UA Server resides, confirm that your server is up and running.
2. From the OPC UA Configuration tool, select a server.
3. On the Connection tab, select None for the security mode.
4. For the security policy, select None.
5. Click Test Connection. If the connection goes through when you have no security policy or mode, but does not otherwise, then you know that you most likely have a certificate issue. Review the ifix_config_service_cert.log in the iFIX\LOCAL\Logs for more details.

Editing the HOSTS File

In some configurations, you may need to update the HOSTS file to assist with DNS name resolution if the network is unable to resolve the name. In this case, connection issues can occur if the HOSTS file does not include entries for all the servers you need to connect to. To fix this issue, try updating the HOSTS file on your iFIX SCADA Server with all of your server and client node names and IP addresses. Then, copy this file to each server and all client nodes. The contents of the HOSTS file should be identical on the iFIX SCADA Server, the OPC UA Server, and each iFIX Client on your network. This ensures the highest reliability for connectivity.

To Update the HOSTS file:

1. Locate the HOSTS file in the C:\WINDOWS\system32\drivers\etc folder.
2. Use a text editor such as Notepad to edit the HOSTS file, and do not add a file extension to the file.
3. Be sure to update the HOSTS file on the SCADA Server, OPC UA Server, and each iFIX Client that you install.
4. Confirm the same, identical entries should appear in the HOSTS file for the iFIX SCADA Server and each iFIX Client on your network.

An example entry in the HOSTS file is as follows:

```
198.212.170.4      SCADA01
```

If you do not know the TCP/IP address of the computer, run the IPCONFIG command in a command prompt to view it.

Replacing a Corrupted Self-Signed Certificate

To resolve issues with your self-signed certificates for the OPC UA Client connection, use the iFIX Configuration Service Certificate Tool. The following steps outline how to open the tool and regenerate the certificate, import it into the Windows store, and redo the bindings.

1. From the File Explorer, browse to the iFIX base path folder. By default, this folder is: C:\Program Files (x86)\GE\iFIX.
2. Locate and double-click the iFixConfigServiceCertTool.exe file. The iFIX Configuration Service Certificate Tool appears.
3. Click the Delete Certificates button to remove your corrupted files. Optionally, You can also click Delete Certificates from Store and then Delete Binding.
4. Click Create Certificates. This action regenerates the self-signed certificate.
5. Review the status in the Create Certificates, Import Certificates to Windows Store, and Bind Certificate to Port sections.
6. Close the iFIX Configuration Service Certificate Tool.
7. Restart iFIX.

Diagnostics

You can obtain diagnostic information on the OPC UA Client from the following:

- Existing Database Fields
- Special I/O Addresses
- Mission Control

Refer to the following sections for more detailed information.

Existing Database Fields

Currently, OPC UA status codes are not mapped to special iFIX fields. Instead, you will find OPC UA quality information mapped to existing OPC classic fields. For instance, the following database fields contain OPC UA Server information:

- **A_OPCLIMIT**: The limit status for the value from the OPC UA server.
- **A_OPCQLTY**: The quality status for the value from the OPC UA server.
- **A_OPCSUBSTAT**: The quality substatus for the value from the OPC UA server.
- **A_OPCTIME**: The time and date from the OPC UA server.

More detailed information about errors is included in the log files created by the OPC UA Client Driver. See the "Logging" on page 27 section for more details.

Special I/O Addresses

For information on your connections, there is a special I/O address to show the server connection status:

```
;OUA_DIAGNOSTICS;Server.ConnectionStatus.<UA server Name>
```

There is also one to show the current Endpoint URL:

```
;OUA_DIAGNOSTICS;Server.CurrentEndpointUrl.<UA server Name>
```

These special I/O addresses are very helpful in a Redundancy Configuration for the OPC UA Client. Between the ConnectionStatus and CurrentEndpointUrl, you can see the overall connected status of a (logical) server, and the endpoint it is currently using for data.

For example, to see the current connection status, in the iFIX Database Manager, add a TX tag with an I/O address like this:

```
;OUA_DIAGNOSTICS;Server.ConnectionStatus.<UA server Name>
```

Note the empty server name in first part of I/O Address, and that it begins with a semicolon. This was intentional. For example, for a server called TestServer1, the tag would be:

```
;OUA_DIAGNOSTICS;Server.ConnectionStatus.TestServer1
```

Similarly, for the endpoint name you would use is as follows:

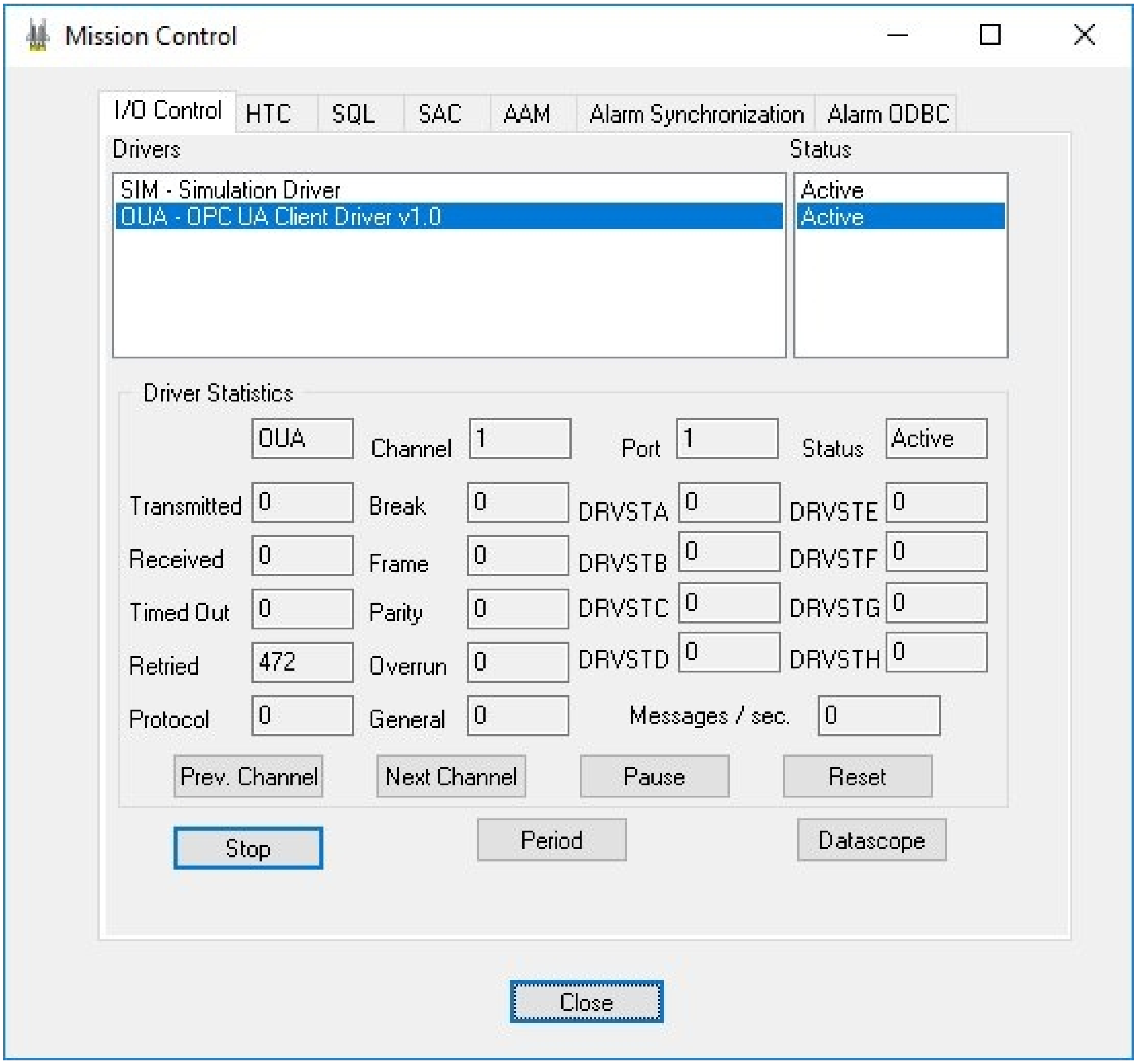
```
;OUA_DIAGNOSTICS;Server.CurrentEndpointUrl.TestServer1
```

The I/O address indicates which UA Server to retrieve the status from. The value (A_CV) of the database tag shows the current state of a given server, such as Connected or Disconnected.

Mission Control

Mission Control allows you to view the diagnostics on a per-server basis. Mission Control represents each OPC UA Server as a channel and provides buttons to switch between the previous and next channels. For example, if you have 5 OPC UA Servers, you will have 5 channels display in Mission Control.

Channel numbers are mapped to server names alphabetically. For example, if you have servers A and B configured, Mission Control shows the statistics for server A as Channel 1 and server B as Channel 2. The following figure shows the driver statistics for Channel 1.



Drivers	Status
SIM - Simulation Driver	Active
OUA - OPC UA Client Driver v1.0	Active

Driver Statistics

	OUA	Channel	1	Port	1	Status	Active
Transmitted	0	Break	0	DRVSTA	0	DRVSTE	0
Received	0	Frame	0	DRVSTB	0	DRVSTF	0
Timed Out	0	Parity	0	DRVSTC	0	DRVSTG	0
Retried	472	Overrun	0	DRVSTD	0	DRVSTH	0
Protocol	0	General	0	Messages / sec.	0		

From the I/O Control tab, the Driver Statistics you want to review for the OPC UA Client Driver (OUA) include:

- **Transmitted** - a count of messages sent by the OUA driver to an OPC UA Server, such as attempts to subscribe or write to data points.
- **Received** - a count of messages received by the OUA driver from an OPC UA Server, such as data change notifications or responses to subscribe or write messages.
- **Timed Out** - a count of the OPC UA Watchdog timeouts received while connected to the OPC UA Server
- **Retried** - the number of times a connection has been re-attempted to an OPC UA Server
- **General** - the number of errors or bad quality messages received for individual data points from an OPC UA Server

Other Driver Statistic fields on this tab, including DRVSTA through DRVSTH, are currently unused.

Logging

Logs are a powerful way to troubleshoot your connection issues. You can find more information about these logs in the following sections.

Locations of Log and Configuration Files

The following table outlines the default log file names associated with the OPC UA Client Driver. By default, the iFIX base path is: C:\Program Files (x86)\GE\iFIX.

Application	Default Log file Name	Location	Configuration File
OPC UA Client Driver	iFixUaClient_<Process_name>.log	iFIX\LOCAL\Logs	iFIX\LOCAL\ServerConfig.XML
OUASPOLL Driver Application	iFixUaClient_OUASPOLL.log	iFIX\LOCAL\Logs	iFIX\LOCAL\ServerConfig.XML
Browse Micro service	opcua-browse-config.log	iFIX\	iFIX\opcua-browse-config.json
iFIX Config Micro service	ifix_config_service.log	iFIX\LOCAL\Logs	iFIX\ifix_config_service.json
iFIX Auth Micro service	ifix_auth_service.log	iFIX\LOCAL\Logs	iFIX\ifix_auth_service.json
NGINX Web Server	access.log and error.log	iFIX\Web\logs	iFIX\web\conf\nginx.conf
Certificate Management	ifix_config_service_cert.log	iFIX\LOCAL\Logs	Not applicable.
OPC UA Client Configuration Tool (User Interface)	See Browser Console	Browser Console	iFIX\web\html\opcua-web-config-client-1.0.257.0\config.json
Web Browser	Displays on screen. Your choice to save to a file.	Your choice.	Not applicable.

IMPORTANT: Whenever you change a logging configuration, you need to restart iFIX to enforce your new settings. Be aware that if you enable or increase logging levels in your application or micro service, that the higher the log setting, the greater the potential to impact performance. After any changes, review your log files. Make sure that enough appropriate and consistent logging content is output in the files to troubleshoot.

OPC UA Client Driver Logging

For the OPC UA Client Driver, you configure the logging levels in ServerConfig.XML file. This file can be found in the iFIX LOCAL folder. The default location for this files is: C:\Program Files (x86)\GE\iFIX\LOCAL. Edit the ServerConfig.XML file in a text editor like Notepad, and scroll to the end of the file to find the <iFixUaClientSettings> section. This is where you configure your logging levels.

For the UaAppTraceLevel setting, the default value is Errors. But, when troubleshooting we recommended the Info level, like this:

```
<UaAppTraceEnabled>true</UaAppTraceEnabled>
<UaAppTraceLevel>Info</UaAppTraceLevel>
```

For the UaStackTraceLevel setting, for troubleshooting, you can also pick a logging level. The default level is ERROR. However, to get a more detailed level traces for troubleshooting, start by setting the level to INFO here as well. Be aware that both these values are case-sensitive.

```
<UaStackTraceEnabled>true</UaStackTraceEnabled>
<UaStackTraceLevel>INFO</UaStackTraceLevel>
```

You can also set the UaStackTraceLevel to DEBUG or ALL (everything is logged). However, if you do this, be aware that the higher the log setting, the greater the potential to impact performance.

You can find the generated log files in the LOCAL\LOGS folder (by default: C:\Program Files (x86)\GE\iFIX\LOCAL\Logs). In iFIX, there are various modules that load the UA Client related libraries. Each of the processes associated with these modules have a log file with a prefix assigned to it. The file names use the convention of: iFixUaClient_<Process_name>.log. For example, the log file for the Database Manager application using OPC UA Client Driver will have the name of: iFixUaClient_DatabaseManager.log for the file name.

Review your log files after the levels are set (ERROR, INFO, or DEBUG). Make sure that enough appropriate and consistent logging content is output in the files to troubleshoot.

Descriptions of UA Stack Trace Levels

NONE - No Trace.

ERROR - Critical errors (unexpected and/or requiring external actions) which require attention.

WARNING - Non-critical faults which should not go unnoticed but are handled internally.

SYSTEM - Rare major events (good cases) like initializations, shut-down, and so on.

INFO - Regular good case events like connects, renews.

DEBUG - Used for debugging purposes.

CONTENT - Used to add additional content (whole message bodies) to debug traces.

ALL - Everything is logged.

Descriptions of UA Application Trace Levels

NoTrace - No Trace.

Errors - Unexpected errors. (This is default and will log only any error conditions.)

Warning - Unexpected behavior that is not an error.

Info - Information about important activities like connection establishment.

InterfaceCall - Calls to module interfaces.

CtorDtor - Creation and destruction of objects.

ProgramFlow - Internal program flow.

Data - Complete logging.

OUASPOLL Driver Application

An important log file to inspect is the iFixUaClient_OUASPOLL.log file. This file contains any run mode logging. This log file can also be found in the iFIX\LOCAL\Logs folder.

Browse Micro service

The browse micro service log file, opcua-browse-config.log, records the interactions from OPC UA Client Configuration tool and the browse micro services. For example, this includes items such as the REST API and token expirations for authentication failures due to browse service connection errors. The default logging level is info. After a default file size of 5MB is reached, the file will be renamed. For example: from ifix_config_service.log.1 to ifix_config_service.log.2, and on, depending on the maximum-files setting. The maximum files setting can be modified in the opcua-browse-config.json.

iFIX Config Micro service

This log file, ifix_config_service.log, records the interactions between the OPC UA Client Configuration tool and the Config Micro service. For example, when Servers, Groups, and Driver Tags are added, the events are recorded in this file. You can trace the server security polices discovered here as well, while testing connections to server. By default, info level logging is configured.

iFIX Auth Micro service

This log file, ifix_auth_service.log, records the interactions between the OPC UA Client Configuration tool and other micro services with the authentication micro service. For example, this includes token requests, token timeouts, and token refreshes (timeout on the UI). By default, the info level logging is configured.

NGINX Web Server Logs

The NGINX log files are found under iFIX base path in the Web\logs folder. They are named access.log and error.log. To change the error.log levels open the nginx.conf file in the iFIX base path web\conf folder. Find the commented line and remove the "#" to enable the logging:

```
#error_log  logs/error.log  info;
```

After this change, messages from all severity levels above "Info" are logged in the error.log.

Use the access.log for NGINX to trace information about client requests. Client requests are written to this log immediately after the request is processed.

Certificate Management Log

If you have any issues during the certificate creation, binding, and trusting process, use this log file to trace them. The ifix_config_service_cert.log file is also found in the LOCAL\LOGS folder (by default: C:\Program Files (x86)\GE\iFIX\LOCAL\Logs).

OPC UA Client Configuration Tool (User Interface)

This file contains logging details for the OPC UA Client tool. Use the logLevel setting in the config.json file found in the iFIX\web\html\opcua-web-config-client-1.0.257.0 folder. By default: C:\Program Files (x86)\GE\iFIX\web\html\opcua-web-config-client-1.0.257.0.

The log messages can be set to the following levels: NONE = 0, INFO = 1, WARNING = 2, ERROR = 3, FATAL = 4, and PERF = 5. Logging modules could be from the following: NONE = 0, OPCUA_

CONFIG, LOGIN, HEADER, VIEW, CONFIG, ALIASES, GROUPS, TAGS, REDUNDANCY, PREFERENCES, SERVICE_AUTHENTICATION, SERVICE_ALIAS, SERVICE_GROUP, SERVICE_BROWSE, and SERVICE_UA.

Browser Console Log

After the OPC UA Client Driver web session is up and running, you can also capture the logs of the browse activity by launching the developer tools for each browsing session. Typically, the F12 key or the Developer Tools option (under More Tools in the browser menu) launches the debug window right in the browser. The Console tab in this window captures live logging of operations performed by user while using the OPC UA Client Configuration Tool. Right-click the menu on this screen and save the log to a text file on your computer for further inspection.

If you want to track any network requests when reproducing the issue with OPC UA Client Driver Configuration Tool and using the Developer Tools, right-click the Network tab, and save the contents by selecting "Save all HAR with content" to a file.

iFIX Block and Data Type Support

When creating iFIX tags in the OPC UA Client Driver tool, you can only create tags using the primary block; you cannot use secondary block types for iFIX tag creation. Primary blocks are usually associated with one or more pieces of process hardware. For example, a pump, a tank, a temperature sensor, a photo cell, a limit switch are all process hardware with which you might associate with a primary block.

The following table lists the primary block types supported by the OPC UA Client Driver.

All iFIX Primary Blocks Supported by the OPC UA Client Driver

Block	Description
Analog Alarm (AA)	Provides read/write access to analog data and lets you set and acknowledge alarms.
Analog Input (AI)	Provides read/write access to analog data and lets you set alarm limits.
Analog Output (AO)	Sends analog data to an I/O driver or OPC server when the upstream block, an operator, a Program block, a script, or an Easy Database Access (EDA) program supplies a value.
Analog Register (AR)	Provides read/write access to analog data only when a Data link connected to the block appears on an operator display.
Digital Alarm (DA)	Provides read/write access to digital data and lets you set and acknowledge alarms.
Digital Input (DI)	Provides read/write access to digital data and lets you set alarm limits.
Digital Output (DO)	Sends digital data to an I/O driver or OPC server when the upstream block, an operator, a Program block, a script, or an Easy Database Access (EDA) program supplies a value.

Digital Register (DR)	Provides read/write access to digital data only when a Data link connected to the block appears on an operator display.
Text (TX)	Lets you read and write a device's text information.

Data Types Not Supported

Be aware that complex data types are not supported with the OPC UA Client Driver. 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)

Advanced Configuration

You can configure the additional settings for the OPC UA Client Configuration tool and its associated micro services by using these files: config.json, ifix_config_service.json, ifix_auth_service.json, and opcua-browse-config.json. You can also configure the additional settings for the NGINX web server in the nginx.conf file. The settings exposed in these configuration files are currently not available in the UIs provided with iFIX.

Whenever you change a setting, you need to restart iFIX to enforce your new settings. Be aware that if you enable or increase logging levels in your application or micro service, that the higher the log setting, the greater the potential to impact performance. After any changes, review your log files. Make sure that enough appropriate and consistent logging content is output in the files to troubleshoot.

The default settings of these configuration files is sufficient for most scenarios. Update the configuration files only if absolutely necessary.

Locations of Configuration Files

The following table outlines the default log file names associated with the OPC UA Client Driver. By default, the iFIX base path is: C:\Program Files (x86)\GE\iFIX.

Application	Configuration File	Location
OPC UA Client Driver	ServerConfig.XML	iFIX\LOCAL
OUASPOLL Driver Application	ServerConfig.XML	iFIX\LOCAL
Browse Micro service	opcua-browse-config.json	iFIX\
iFIX Config Micro service	ifix_config_service.json	iFIX\
iFIX Auth Micro service	ifix_auth_ser-	iFIX\

Application	Configuration File	Location
	vice.json	
NGINX Web Server	nginx.conf	iFIX\web\conf
Certificate Management	Not applicable.	Not applicable.
OPC UA Client Configuration Tool (User Interface)	config.json	iFIX\web\html\opcua-web-config-client-1.0.257.0
Web Browser	Not applicable.	Not applicable.

The tables that follow outline the location of these files and the entries available for editing.

ifix_config_service.json file

The following table outlines the configurable entries in this file.

Item	Description
port	The port used by this micro service. By default, this port is 4855.
secure	Defines whether security is enabled on this port. By default, this is set to true.
log	Defines the file name, logging level, maximum log file size, number of log files to create, as well as the number of seconds to flush the log. By default, logging is enabled for the file name ifix_config_service.log, and the level is set to info. The maximum size of a log file is set to 5242880, with a maximum of 3 files, and a flush cycle of 10 seconds.
configLimits	The size limit for the server name, group name, and tag name. For the server it is 19 characters. For the group name it is 19 characters. For the driver tag name it is 79 characters. Do not to increase these values.
datatypeToBlockType	The block types allowed by the OPC UA Client Driver tool (Numeric: AI, AA, AR, and AO; Boolean: DI, DA, DR, DO; String: TX). Do not edit this setting.
generateSSLCerts	Configures whether to generate SSL certificates for the

Item	Description
	OPC UA Client Driver. By default, this is set to true.
startiFixOpcuaBrowseService	Configures whether the browse micro service is enabled on client. By default, this field is set true. Do not edit this setting.
iFixOpcuaBrowseServiceStartCommand	The command to start the ifix_auth_service.json service. Do not edit this setting.
useBasicAuth	Configures whether to use basic authentication. By default, this value is set to false. Do not edit this setting.
startiFixAuthService	Configures whether the authentication micro service is enabled on client. By default, this field is set true. Do not edit this setting.
iFixAuthServiceStartCommand	The command to start the iFIX authentication micro service. Do not edit this setting.
authenticationMicroserviceTokenUrl	The URL for the iFIX authentication micro service. By default: https://localhost:4857/ifix-auth-service/v1/oauth/token.
authenticationMicroserviceTokenKeyUrl	The key for the iFIX authentication micro service. by default: https://localhost:4857/ifix-auth-service/v1/oauth/token_key.
authenticationMicroserviceTokenIntrospectUrl	The introspect URL for the iFIX authentication micro service. By default: https://localhost:4857/ifix-auth-service/v1/oauth/introspect_token.
authenticationMicroserviceTokenRevokeUrl	The revocation URL for the iFIX authentication micro service. By default: https://localhost:4857/ifix-auth-service/v1/oauth/token/revoke.
rootCertificateName	The name of the root certificate used by the OPC Client Driver. By default: iFIX_OpcuaConfigRoot.
serverCertificateName	The name of the server cer-

Item	Description
	tificate. By default: iFIX_OpcuaConfigServer.
serverCertificateStoreName	The name of the Windows server certificate store name. By default: iFIX_OpcuaConfigServiceRoot.
serverCertificatePassPhrase	Certificate pass phrase for both root and server certificates.

ifix_auth_service.json file

The following table outlines the configurable entries in this file.

Item	Description
AccessTokenExpiryInterval	The default token expiration interval time before the OPC UA Client Configuration tool refreshes a token. If the OPC UA Client application does not refresh the token within this interval, the access token expires, and the application will be forced to make the user sign in again. By default: 1800 seconds.
RefreshTokenExpiryInterval	The OPC UA Client Configuration tool can renew the token after the interval expires. After this interval expires, the user is forced to log in again. By default: 86400 seconds.
port	The port used by this micro service. By default, this port is 4857.
secure	Describes whether security is enabled. By default, this value is set to true.
Clientid	The ID name of the Client for authentication service. By default, it is: admin.
ClientSecret	The key name known only to the application and the authorization server.
log	Describes whether the log file is enabled, the file name, and level. By default, logging is configured to be true. The file name is ifix_auth_service.log, and the default logging level is info.
max-size	The maximum size of a single log for this micro service. By default, it is: 5242880 KB.
max-files	The maximum number of files used to create log files before overwriting. By default, it's 3.
flush-seconds	The number of seconds before data from memory is flushed onto disk: 10 seconds.

opcua-browse-config.json file

The following table outlines the configurable entries in this file.

Item	Description
port	The port used by this micro service. By default, this port is 4856.
maxReadRequestObjects	The maximum read request size. By default, it is 5000 bytes. If this value is too high, the 413 Payload Too Large error may occur. If this value is too low, the browsing and tag creation performance will be affected.

Item	Description
maxBrowseRequestObjects	The maximum browse request size. By default, it is 5000 bytes. If this value is too high, the 413 Payload Too Large error may occur. If this value is too low, the browsing and tag creation performance will be affected.
maxBrowseResultObjects	The maximum browse result size. By default, it is 5000 bytes. If this value is too high, the 413 Payload Too Large error may occur. If this value is too low, the browsing and tag creation performance will be affected.
log	Defines the file name, logging level, maximum log file size, number of log files to create, as well as the number of seconds to flush the log for this micro service. By default, the log file name is opcua-browse-config.log, the level is info, the maximum size is 5242880, number of files is 3, and flush seconds is set to 10.

nginx.conf file

The following table outlines the configurable entries in this file.

Item	Description
listen	The port used by the NGINX web server. The default port number is 9444.
certificate	The .crt file used by the NGINX server for communication. By default: FIX_OpcuaConfigServer.crt.
certificate_key	The private key used by the certificate .crt file when a signing is requested. By default: FIX_OpcuaConfigServer.key.
error_log	Used for logging capabilities. To enable logging for the NGINX server, comment out this line: #error_log logs/error.log info; After this change, messages from all severity levels above "Info" are logged in the error.log. The NGINX log files are found under iFIX base path in the Web\logs folder.
client_max_body_size	The maximum size (in megabytes) of a client request that goes through the NGINX server. By default, this value is set to 5 MB. If this value is too low and the request is too big, a 413 Payload Too Large error will occur. If this value is too high, it could cause out-of-memory errors in the services and application, and could allow attackers to occupy the services for too long.
proxy_read_timeout	The maximum time that the NGINX server will wait for a proxied response to be returned. By default, this value is set at 5 minutes. If this value is too low, when you browse or create tags, a 404

Item	Description
	errors may occur. If this value is too high, it may take longer for issues with services to be discovered, and could allow attackers to occupy the services for too long.

config.json file

The following table outlines the configurable entries in this file.

Item	Description
protocol	By default this value is https. Do not change this setting.
hostName	By default this value is localhost. Do not change this setting.
configServicePortNum	The port used by this application. By default, this port is 9444.
basicAuth	When enabled (true), you allow authentication to be used when communicating with the OPC UA Server. By default this feature is set to false.
browseServicePortNum	The port used by this browsing service. By default, this port is 9444. It should match the configServicePortNum setting.
browseServiceBasePath	By default: /uabr. Do not edit this setting.
configServiceAPIBasePath	By default: /ifix-scada-config/v1. Do not edit this setting.
syncDelay	The amount of seconds to wait for a delay. By default: 1000 seconds.
inactiviyTimeOut	The amount of seconds to wait before the application times out due to inactivity. By default, 1200 seconds.
clientId	The client user name. Do not edit this field.
clientSecret	The client password. Do not edit this field.
maxNumberOfDriverStartTimePolls	Maximum number of start times a driver will be polled, By default, 100.
logLevel	The log messages can be set to the following levels: NONE = 0, INFO = 1, WARNING = 2, ERROR = 3, FATAL = 4, and PERF = 5.
tagHierarchySeparator	By default, this value is an underscore (_).It is recommended that you do not change this value.

Special Considerations for Enhanced Failover

If using Enhanced Failover, you must be in Maintenance Mode before you log in the OPC UA Client Driver Configuration tool 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.

The OPC UA Client Driver 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 OPC UA Driver 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.

Every time you make a change in the configuration, 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 OPC UA Client Driver tool. 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.

NOTE: 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 the OPC UA Driver (OUA) Configuration Tool on the Primary will not be deleted on Secondary after the maintenance mode synchronization happens. This is an issue with iFIX 6.1. 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 the OPC UA Client Driver Configuration tool 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, the certificate management to communicate to a remote OPC UA server is different. 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" on page 25 topic.

Index