GE VERNOVA

PROFICY® SOFTWARE & SERVICES

iFIX

Getting Started Guide

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.

Trademark Notices

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

Getting Started with iFIX

Welcome to iFIX®! Thank you for taking the time to install and use iFIX.

Before you begin installing our product, please take some time to review this Getting Started guide. The guide includes information about the following:

- Installing iFIX
- Upgrading from earlier versions of iFIX
- Supported networking components

Reference Documents

For more information on the System Configuration Utility, troubleshooting your set-up, working with the iFIX WorkSpace, or setting up a process database or SCADA system after you install iFIX, please refer to the following electronic books:

- Setting Up the Environment
- Understanding iFIX
- Building a SCADA System

General Installation Information

This chapter provides general information you need to install iFIX including:

- Hardware requirements, including required computer hardware, recommended computers, required memory, and required hard disk space.
- Installing the license and replacing defective ones.
- Installing iFIX.
- iFIX software requirements, including operating systems, supported regional settings, optimizing virtual memory, and running iFIX as a service.
- Optional installation features, including online registration, and installing optional hardware.
- Installing iFIX with other applications including Microsoft® Office and GE Change Management.

Set-up Overview

When you are ready to begin setting up your iFIX environment, use the following steps to set up your nodes.

To set up your nodes:

1. Set up each computer you require. Use the section Hardware Requirements as a guide and refer to the user manual that accompanies each computer for detailed setup information.
2. Install and optimize Microsoft Windows on each computer as needed. Also make sure you create a login account with administrator rights so you can install iFIX later. For instructions on optimizing Windows, refer to the Optimizing Virtual Memory section.
3. Set up the network adapters and network software required for each computer. Refer to the Networking iFIX Nodes and Advanced Topics chapters of the Setting Up the Environment manual for more information.
4. Install iFIX and any other hardware you may have purchased. Refer to the Installing the iFIX Software section for instructions. For information on installing other hardware, refer to that product's documentation.
5. Configure iFIX on each computer. Make sure that the user installing iFIX is a member of the Administrators Windows group. Refer to the Configuring iFIX Using the SCU chapter of the Setting Up the Environment manual for more information on configuring iFIX.

Language Support

When working with iFIX, be aware that:

- The iFIX English product is supported on the English Windows operating system (OS), with English (United States) or non-English regional settings.
- The iFIX English product is supported on non-English Windows operating systems only when the system locale and region format match the OS language. Our language and locale testing is focused on a set of representative environments.
- The non-English iFIX product is supported on an operating system with a matching language, region format, and system locale.
- The System Locale must match the language of the Region Settings.
- All keyboard inputs must also match the system locale of the SCADA.
- Configuration Hub will display the number formats and strings as they appear on SCADA node. Changing the browser language will not have an impact on the appearance of this data.
- For the English Proficy installer, when entering the Client ID or Client Secret fields for Configuration Hub and Proficy Authentication during the install, you can only use English alphanumeric characters and the following symbols: ~`!@#$*()-_={}[]\'",.?/
- For the Proficy installer, when installing iFIX English with non-English Regional Settings, non-English characters are not supported for the Client ID or Client Secret fields in the installer.
- For a translated Proficy installer, when installing on a non-English operating system, you can enter characters from that specific language in the Client ID and Client Secret fields displayed in the installer.
- Running iFIX on a computer with a machine name that contain non-English characters such as æ, ø, å in the name is not supported.
- If there is a new iFIX product language release, it typically comes after the release of the English version of the software. For more information on the available iFIX versions for each language, contact your regional Sales Representative.

The following tables provide examples of supported combinations of the product language, OS language, region, and system locale.

English Product Support

iFIX Product Language	Operating System	Regional Settings Format	System Locale
English iFIX	English	English (United States).	English (United States).
English iFIX	English	Non-English regional settings. For example: Chinese (Simplified, China).	Matching Non-English system locale. For example: Chinese (Simplified, China).
English iFIX	Non-English	Non-English matching regional settings.	Non-English matching system locale.

Non-English Product Support

iFIX Product Language	Operating System	Regional Settings Format	System Locale
Chinese	Chinese	Chinese regional settings. For example: Chinese (Simplified, China).	Chinese system locale. For example: Chinese (Simplified, China).
French	French	French regional settings. For example: French (France).	French system locale. For example: French (France).
German	German	German regional settings. For example: German (Germany).	German system locale. For example: German (Germany).
Japanese	Japanese	Japanese regional settings. For example: Japanese (Japan).	Japanese system locale. For example: Japanese (Japan)
Polish	Polish	Polish regional settings.	Polish system locale. For example: Polish (Poland)

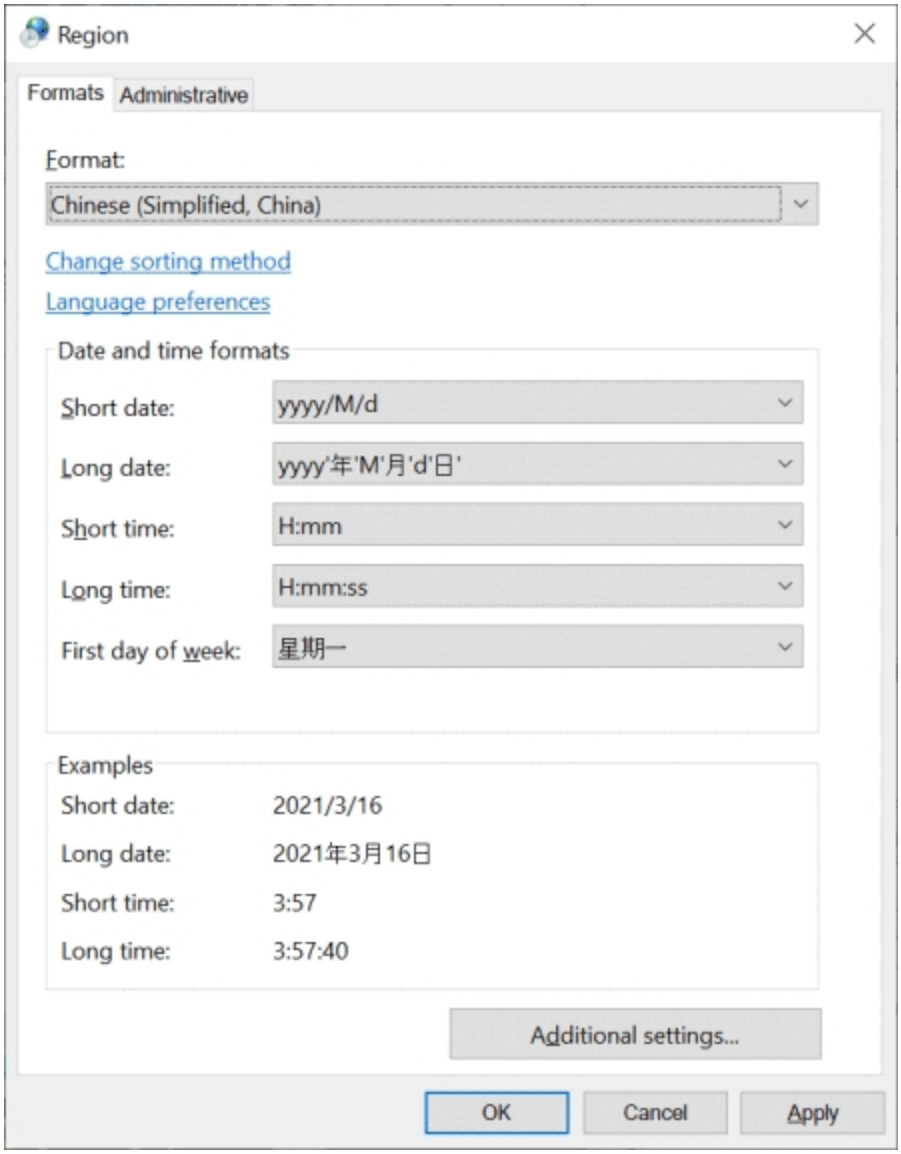
Russian	Russian	For example: Polish (Poland). Russian regional settings. For example: Russian (Russia).	Russian system locale. For example: Russian (Russia)

Unsupported Items

- GE does NOT support running the localized version of the product on an English operating system.
- Multilingual User Interface versions of the Windows Operating Systems are not supported by the iFIX product.
- iFIX client/server configurations with different OS languages are not supported. For instance, connecting an English SCADA Server (on an English OS) with a German View node or iClient (on a German OS) is not supported.
- Importing CSV configurations that were created on a different locale than the SCADA is not supported.
- Double-byte characters are not supported on single-byte operating systems.
- Right-to-left languages are not supported .
- The Productivity Tools are supported in English OS, with English regional settings.
- The following special characters are not supported when using the Romanian language in iFIX: ș, ț, Ș, Ț .
- Non-English Node Names are not supported.
- Non-English Tag Group Symbols are not supported in the Tag Group Editor.

How to Change the Regional Setting Format

1. From the Windows Control Panel, select Clock and Region. The Clock and Region settings appear.
2. Select the Change date, time, or number formats link. The Region dialog box appears.
3. In the Format field, view or select the region you want specify. For instance, the following dialog box shows Chinese (Simplied, China) as the region.



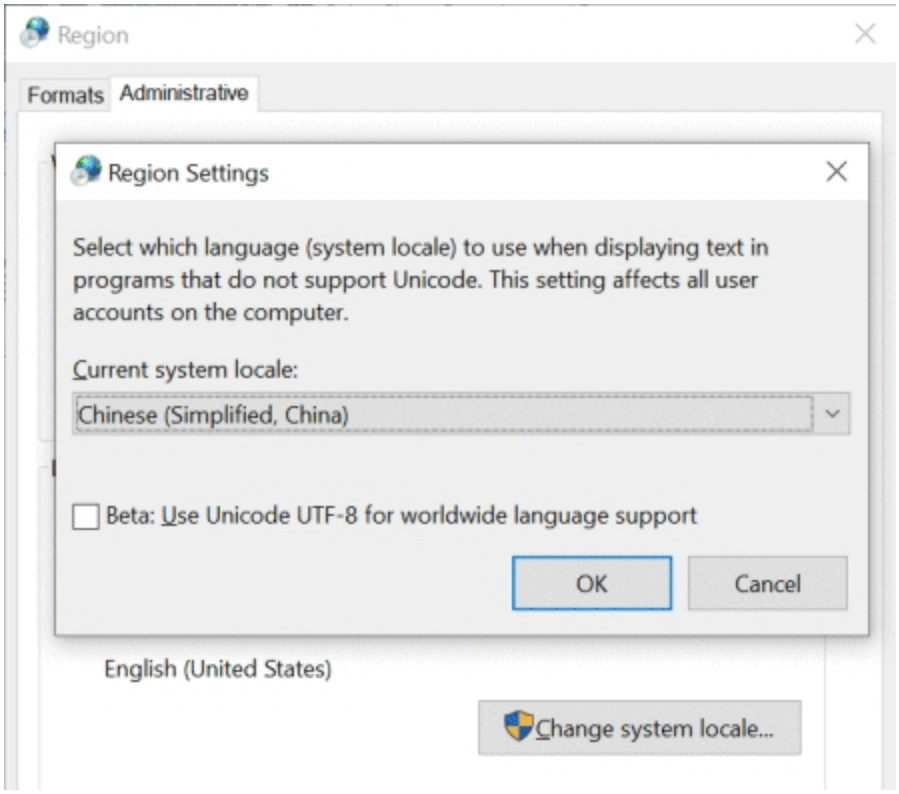
How to Set the System Locale

1. From the Windows Control Panel, select Clock and Region. The Clock and Region settings appear.
2. Select the Change date, time, or number formats link. The Region dialog box appears.
3. In the Format field, confirm that the format is correct. If not, change it now and leave the dialog box open.
4. Click the Administrative tab.
5. Click Change System Locale.
6. If there are changes that need to get applied, click Apply to proceed. The Region Settings dialog

box appears.

7. Enter a matching system locale for the region identified or configured in step 3. For example, the following screen capture shows the matching Chinese locale for the regional setting defined above.
8. Click OK and then restart your system to apply the change.

IMPORTANT: Be sure that you do not select the “Beta – Use Unicode UTF-8 for World-wide support” option in the Region Settings dialog box. Otherwise, you will experience issues with the iFIX Database Manager.



How to Match the Regional Settings Format in Configuration Hub and iFIX

On the iFIX system, if you notice that the Regional Settings for the logged in user are changed or different from the default System Regional Settings, you will need to make this update.

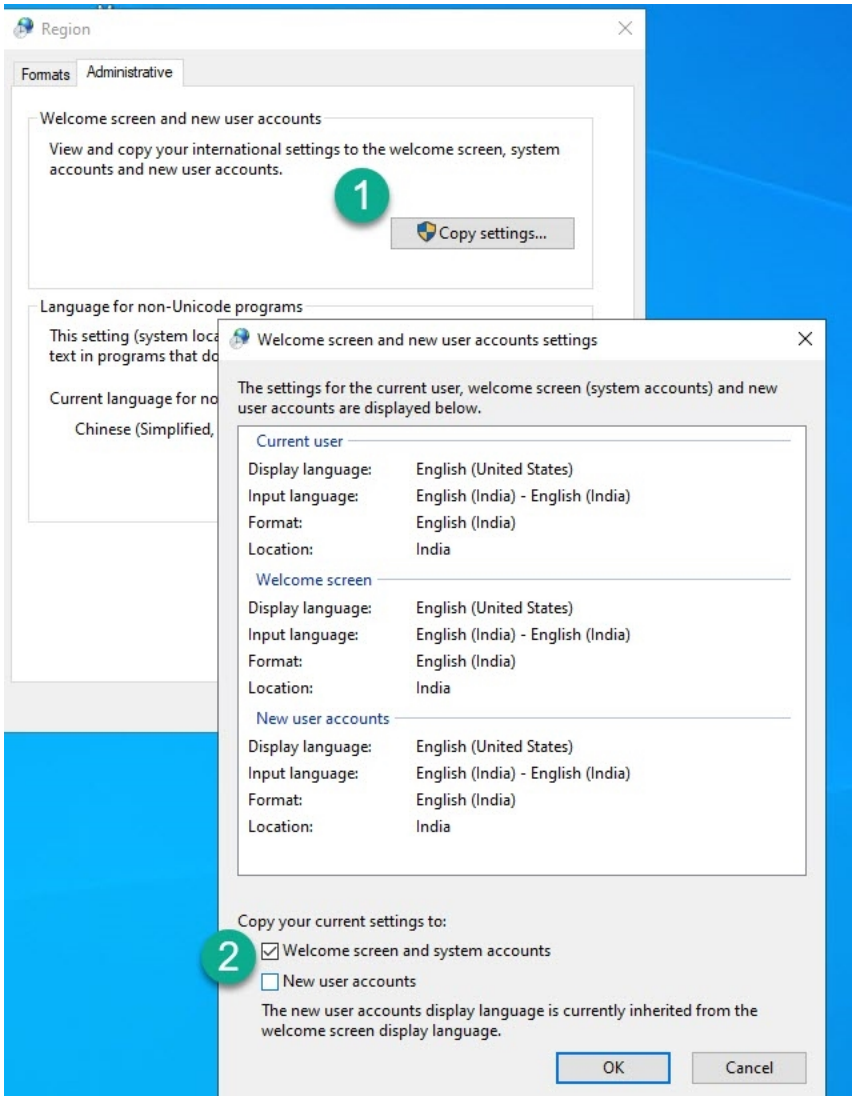
This update will ensure that Configuration Hub gets the correct Regional Format information from the iFIX system.

NOTE: The Browser Language settings where Configuration Hub is opened should be kept same language as system where iFIX is installed.

On the iFIX system, perform the following steps to make this update:

1. From the Windows Control Panel, select Clock and Region. The Clock and Region settings appear.
2. Select the Change date, time, or number formats link. The Region dialog box appears.

3. Click the Administrative tab.
4. Click Copy Settings.
5. From the Windows Screen and New User Accounts Settings dialog box, select the Welcome Screen and System Accounts check box and then click OK to save your changes.



Supported Regional Settings

iFIX supports the following regional settings available in the Windows Control Panel:

- Decimal symbol - one character
- Digit grouping symbol
- List separator - one character
- Time style

- Time separator
- Short date style
- Date separator

NOTE: The decimal symbol and the digit grouping symbol cannot be the same character. Also, the time separator and the date separator cannot be the same character.

Formatting the Time and Date

Avoid changing the time style or short date style in regional settings to values that are outside of the standard styles provided. Changing these values to non-standard styles may result in improperly formatting times and dates in some parts of iFIX.

iFIX supports the following short date formats, some of which may not be available in certain language versions of Windows:

- dd/mm/yy, or dd/mm/yyyy
- dd/yy/mm, or dd/yyyy/mm
- mm/dd/yy, or mm/dd/yyyy
- mm/yy/dd, or mm/yyyy/dd
- yy/dd/mm, or yyyy/dd/mm
- yy/mm/dd, or yyyy/mm/dd

Formatting the Regional Language Setting

Avoid changing the language setting once a timer has been used in a schedule. If changed, the date always reverts to 30/12/99, regardless of what you set the start time to be.

Setting the System Default Locale

The selected locale must be set as the system default.

Installing the iFIX Software

The Proficy product installer streamlines the deployment experience for iFIX, along with the other products iFIX is often used with. The Proficy installer supplies the default settings for you, based on the type of install you select, making it easier and faster to get your product installed. Any of the default settings configured with the Proficy installer can be updated after the install through the iFIX SCU.

The Proficy installer is the preferred way to install iFIX. In order to use iFIX with Configuration Hub, Configuration Hub needs to be installed only once. It does not need to be installed on all nodes. You can also install other components as required.

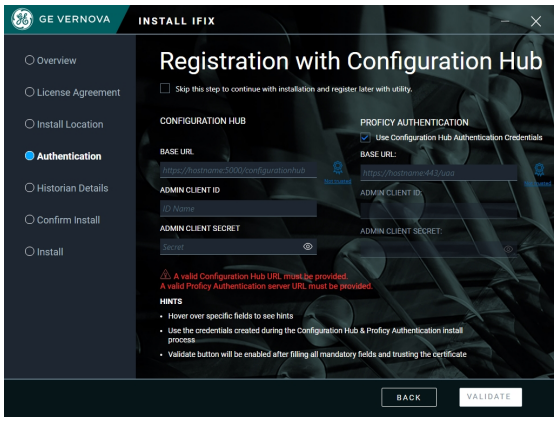
The log file for the iFIX install is named iFIX 2024_SETUP.LOG. The log appears in your Windows folder. This log file can be used to troubleshoot any issues that occur during the iFIX install.

See the steps below, or this Quick Start for help on getting started.

Steps to Install iFIX with the Proficy Installer

To install iFIX from the Proficy installer:

1. From the install folder, double-click Setup.bat to run the installer. The Installation screen appears.
2. Select the option to install:
   - SCADA Standalone Server
   - SCADA Client
   - SCADA with Remote Historian
3. Click Start.
4. When the License Agreement appears, read through the terms and click Accept to continue. The Install Location screen appears.
5. Leave the defaults, or specify another location.
6. Click Next to Continue. The Registration with Configuration Hub screen appears.



On this page you can register iFIX with Configuration Hub only if Configuration Hub and Proficy Authentication have been installed.

IMPORTANT: Be aware that any time you install a Proficy software product without registering that software with Configuration Hub during the installation process, you will need to run the Node Manager utility on the desktop before you can see that software show up centrally in the Configuration Hub > Administration > Node Manager panel.

7. If you have installed Configuration Hub and Proficy Authentication, enter the Base URL, Admin Client ID and Admin Client Secret for each. (Later, when you reboot your machine and log into Configuration Hub, the iFIX plug-in will appear in the Navigation pane, ready for use.) Click Validate.

   NOTE: If you used the same credentials for both Configuration Hub and Proficy Authentication during installation, select the Use Configuration Hub Authentication Credentials check box in the Proficy Authentication section.

8. If you have not installed Configuration Hub and Proficy Authentication, click the check box to skip this step and continue the installation. You will have to use the Node Manager Configuration utility to register iFIX with Configuration Hub later, after installing both Configuration Hub and Proficy Authentication. See Registration with Configuration Hub. Click Next.

   The Historian Details screen appears. For other install options, the Credentials screen appears.

9. Enter the data requested. If installing Historian with iFIX, you are presented with Historian options. Leave the defaults. If you want to enable security for Historian, select the Enable Historian Services Security check box; this will require additional steps (you can also perform these same steps later. If the Historian Data Path is different from what appears in this screen, enter it now.
10. Click Next. The Confirm Install screen appears.
11. Click Start. When the install completes a message appears.
12. Click Close. Another message appears. You can choose to install more products, reboot now or later.

Steps to Install Configuration Hub with the Proficy Installer

NOTE: Configuration Hub only needs to be installed only once. It does not need to be installed on remote nodes.

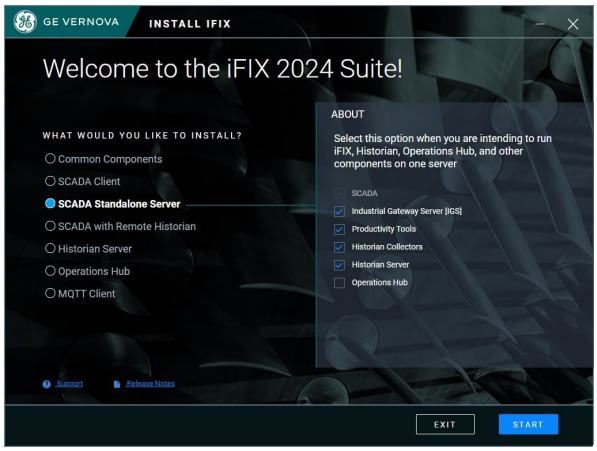
To install Configuration Hub from the Proficy installer:

1. From the install folder, double-click Setup.bat to run the installer. The Installation screen appears.
2. Select the Common Components option to install.
3. Leave the defaults and install both Configuration Hub and Proficy Authentication.
4. When the License Agreement appears, read through the terms and click Accept to continue. The Install Location screen appears.
5. Leave the defaults, or specify another location.
6. Click Next to Continue. The Credentials screen appears.
7. Enter the required credentials. Be sure to retain these credentials for future use, as they cannot be reset without reinstalling.

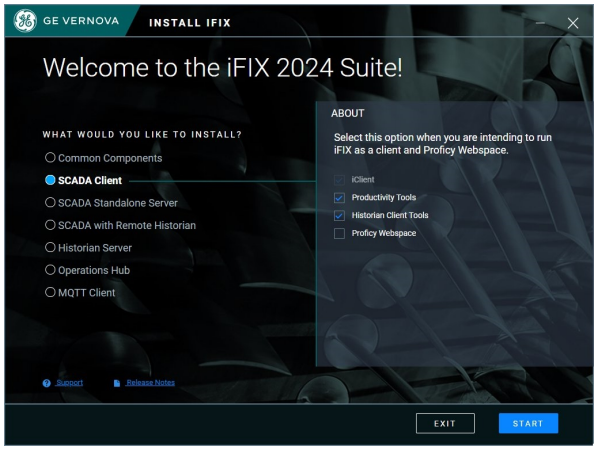
   IMPORTANT:

   - For the English Proficy installer, when entering the Client ID or Client Secret for Configuration Hub and Proficy Authentication during the install, be aware that you can only include English alphanumeric characters and the following symbols: ~`!@#$*()-_={}[]\'",.?/
   - For the English Proficy installer, even when installing on a non-English operating system, the non-English characters are not supported for the Client ID or Client Secret fields displayed in the installer.
   - For the translated Proficy installers, when installing on a non-English operating system, you can enter characters from that specific language in the Client ID and Client Secret fields displayed in the installer.
8. Click Next. The Confirm Install screen appears.
9. Click Start. When the install completes a message appears.
10. Click Close. Another message appears. You can choose to install more products, reboot now or later.
11. Register Configuration Hub with iFIX. See "Configuration Hub Registration" on page 18.

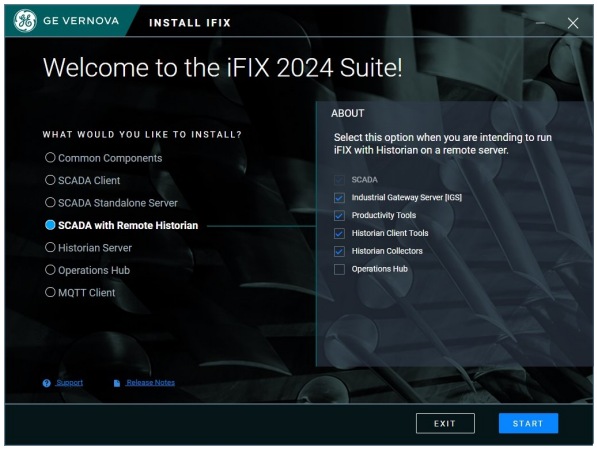
SCADA Standalone Server Option from the Proficy Installer



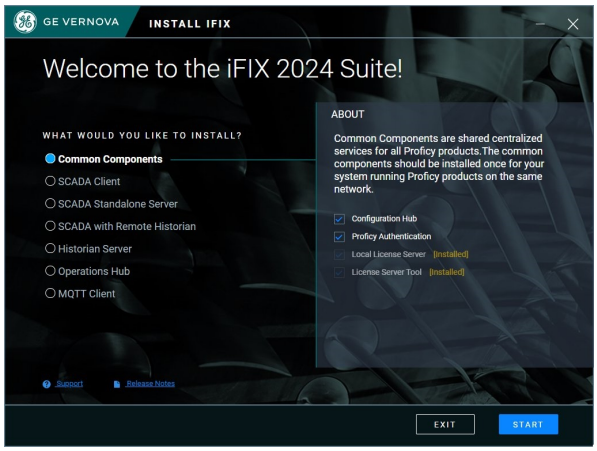
SCADA Client Option from the Proficy Installer



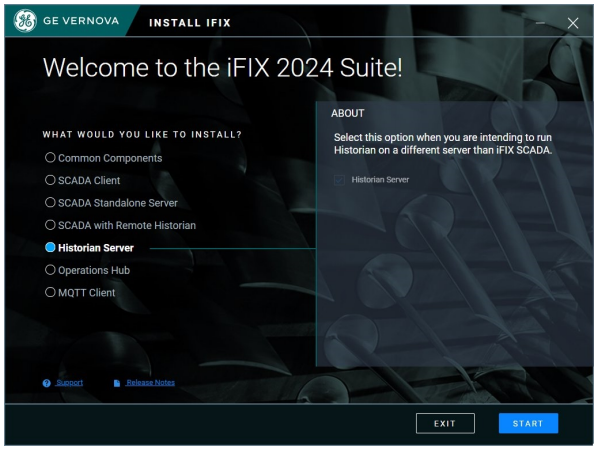
SCADA with Remote Historian Option from the Proficy Installer



Common Components Option from the Proficy Installer

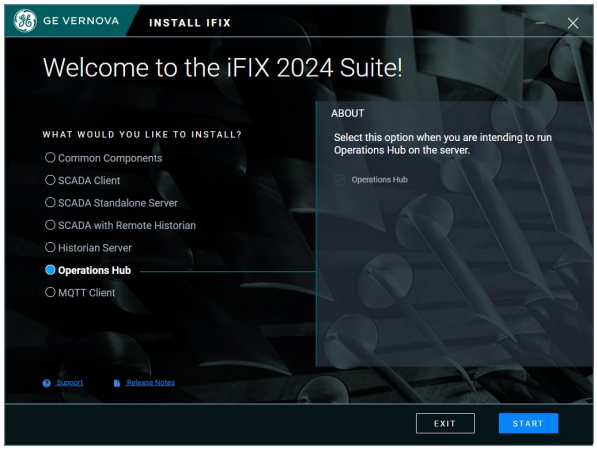


Historian Server Option from the Proficy Installer

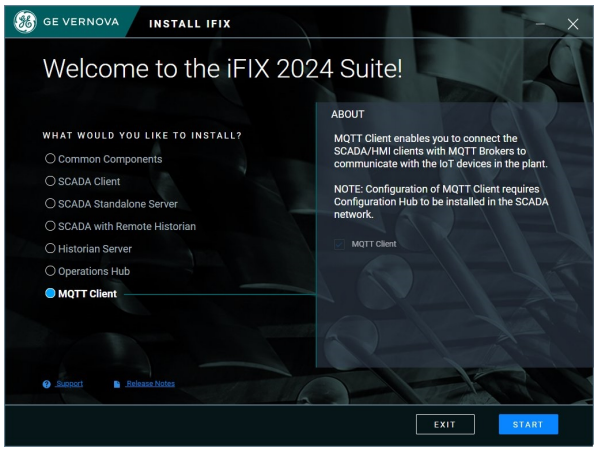


Operations Hub Option from the Proficy Installer

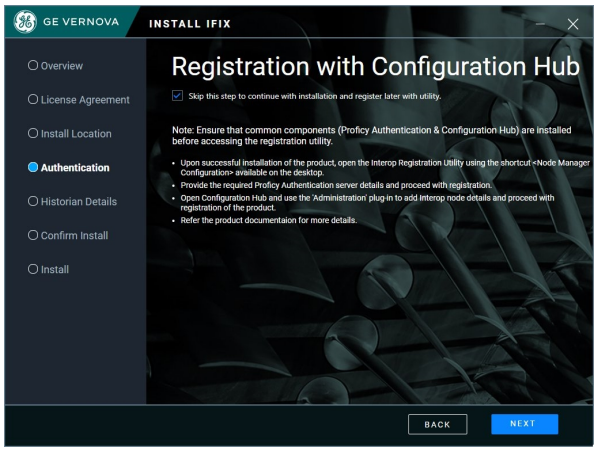
NOTE: For steps on how to run the Interactive Installer from Operations Hub from the Proficy installer.



MQTT Option from the Proficy Installer



Skipping Plug-in Registration During Installation



Running the Proficy Install from a Command Line

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

NOTE: As of iFIX 2024, you must use a file created by the latest installed version. For example, if you have installed iFIX 2024, you cannot use a SilentInstallResponseFile.json file created by any earlier iFIX version.

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

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

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

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

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

To further customize the iFIX install:

1. In Windows Explorer, create a folder on your local drive named isoimage. For example: C:\isoimage.
2. Copy all of the files and folders from the Proficy installer, and paste them in your isoimage folder.
3. Navigate to the iFIX\Setup folder to locate the scadaconfig.ini or installconfig.ini.
4. Make your changes, and save the file. Your customized settings are saved for the next time you run the install from the command line, using this install image.

Common Components

```
{
"packageSelected": "CommonComponents",
"installLocation": "C:\\Program Files (x86)\\Proficy",
"configHubClientId": "admin",
"configHubClientSecret": "******",
"uaaClientId": "admin",
"uaaClientSecret": "******",
"selectedPackageProducts": [
{
"productName": "Configuration Hub",
"installType": "installText"
},
{
"productName": "Proficy Authentication",
"installType": "installText",
"uaaInstallType": "Silent Install"
},
{
"productName": "License Server Tool",
"installType": "upgrade",
"installedLocation": "C:\\Program Files (x86)\\Proficy\\Proficy Common\\Proficy Common Licensing"
}
],
"isAuthCredsProvided": false,
"rebootFlag": false
```

```
}
```

SCADA Client

```
{
"packageSelected": "ScadaClient",
"installLocation": "C:\\Program Files (x86)\\Proficy",
"selectedPackageProducts": [
{
"productName": "iClient",
"installType": "installText"
},
{
"productName": "Productivity Tools",
"installType": "installText"
},
{
"productName": "Historian Client Tools",
"installType": "installText"
},
{
"productName": "Proficy Webspace",
"installType": "installText"
}
],
"nodeName": "FIXVIEW"
"historianServerLocation": "10.10.01.10",
}
```

SCADA Standalone Server

```
{
"packageSelected": "ScadaStandAloneServer",
"installLocation": "C:\\Program Files (x86)\\Proficy",
"nodeName": "FIX",
"selectedPackageProducts": [
{
"productName": "SCADA",
"installType": "installText"
},
{
"productName": "Industrial Gateway Server [IGS]",
"installType": "installText"
},
{
"productName": "Productivity Tools",
"installType": "installText"
},
{
"productName": "Historian Collectors",
"installType": "installText"
},
{
"productName": "Historian Server",
"installType": "installText"
}
],
"dataPathFolder": "C:\\Proficy Historian Data",
"enableCertificateSecurity": false,
"serverCertPassPhrase": "",
"isAuthCredsProvided": false,
"rebootFlag": false
}
```

SCADA with Remote Historian

```
{
"packageSelected": "ScadaWithRemoteHistorian",
"installLocation": "C:\\Program Files (x86)\\Proficy",
"selectedPackageProducts": [
{
"productName": "Interop Service",
"installType": "installText"
},
{
"productName": "SCADA",
"installType": "installText"
},
{
"productName": "Industrial Gateway Server [IGS]",
"installType": "installText"
},
{
"productName": "Productivity Tools",
"installType": "installText"
},
{
"productName": "Historian Client Tools",
"installType": "installText"
},
{
"productName": "Historian Collectors",
"installType": "installText"
}
],
"nodeName": "FIX",
"dataPathFolder": "C:\\Proficy Historian Data",
"historianServerLocation": "MYSERVER",
"historianUserName": "admin",
"historianPassword": "******",
"isAuthCredsProvided": false
}
```

Historian Server

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

Operations Hub

```
{
"packageSelected": "productOpsHub",
"installLocation": "C:\\Program Files (x86)\\Proficy",
"opshubusername": "ch_admin",
```

```
"opshubpassword": "******",
"ophub": {
"configHubRegClientId": "admin",
"configHubRegClientSecret": "******",
"uaaBaseUrl": "",
"adminClientId": "admin",
"adminClientSecret": "******",
"configHubBaseUrl": "",
"deferConfigHubRegistration": true,
"useLocalUaa": true
},
"opshubdrivelocation": "C:",
"selectedPackageProducts": [
{
"productName": "Operations Hub",
"installType": "installText",
"opshubinstalltype": "Silent Install"
}
],
"isAuthCredsProvided": false
}
```


Configuration Hub Registration

If you did not register iFIX with Configuration Hub during product installation, you must take additional steps (after you have installed both Configuration Hub and Proficy Authentication) to register iFIX with Configuration Hub.

- If you installed Configuration Hub locally on the same machine as iFIX, you need to register iFIX and Proficy Authentication. You will need to provide the Client ID and Client Secret information you entered when you installed the Common Components from the Proficy Installer.
- If you want to use a Configuration Hub server on a computer that is not on the local machine, you will need to register with the Configuration Hub server on the remote computer.
- If you configured Configuration Hub with iFIX and now you want to change to a remote Configuration Hub server, you will need to unregister Configuration Hub on the local machine first, and then register with the remote Configuration Hub server. See "Unregistering iFIX Plug-in" on page 22.
- Any time that you install Proficy software without registering that software with Configuration Hub during install, you will need to run the Node Manager utility on the desktop before you can see that software show up centrally in the Configuration Hub > Administration > Node Manager panel.

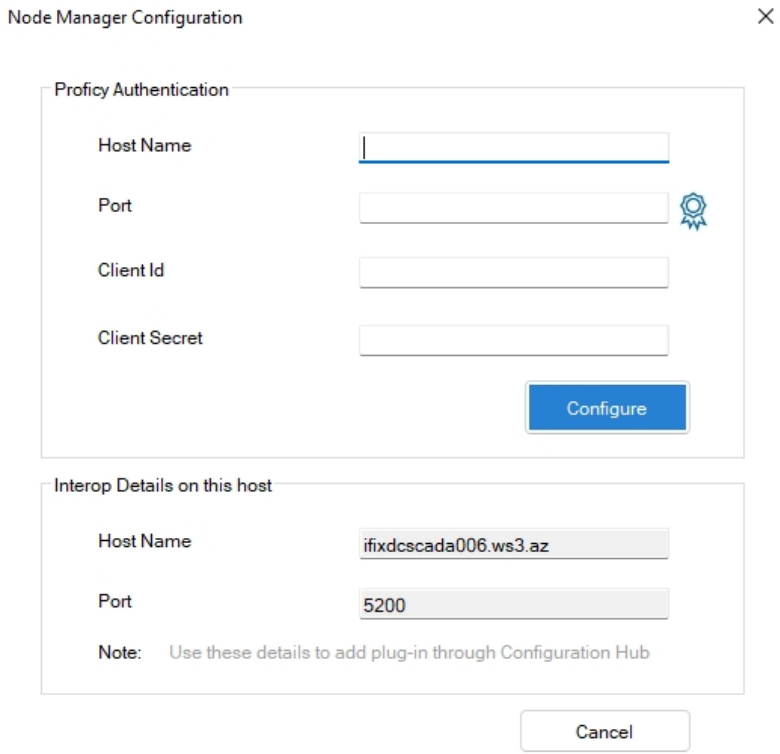
Before Registering iFIX with Configuration Hub

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

- If your computers are in a workgroup environment, follow all steps in Registering iFIX with Configuration Hub for Workgroups.

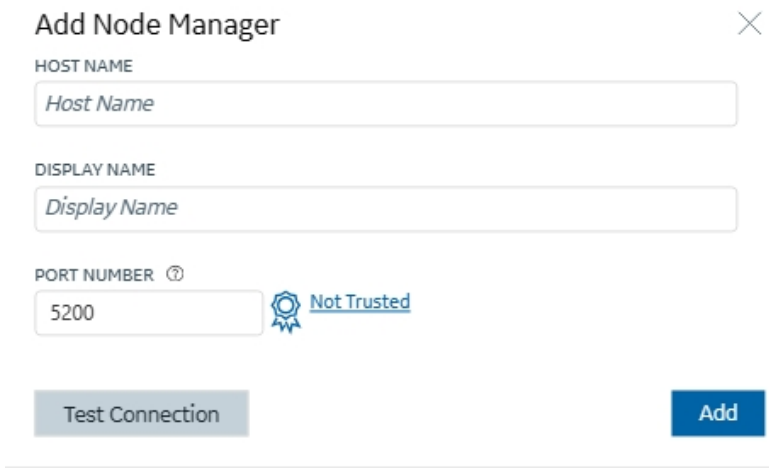
iFIX Plug-in Registration

1. Use the desktop icon to run the Node Manager Configuration utility with Administrator privileges.

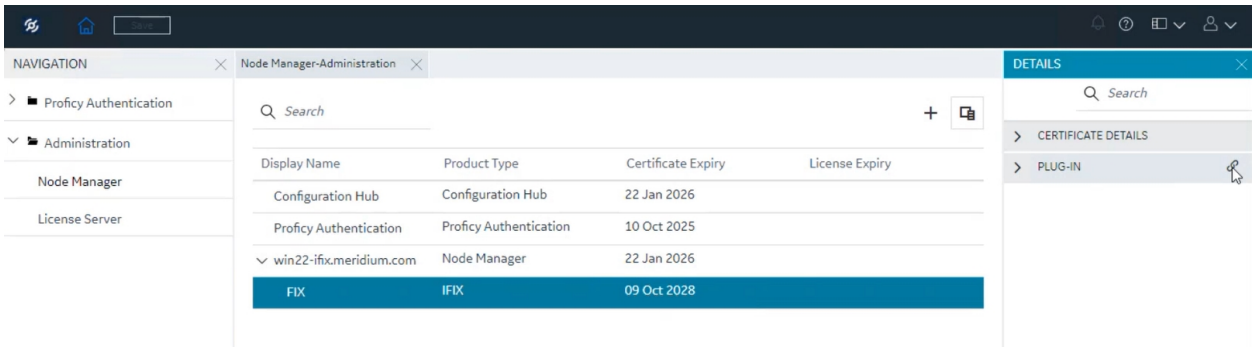


2. In the Proficy Authentication field, enter the Host Name of the Proficy Authentication server. Edit the value in the Port field if necessary. Enter the Client ID and Client Secret.
3. Click the certificate icon to trust the certificate.
4. Click Configure.
5. Log into Configuration Hub to add the Node Manager.
6. Expand the Administration menu in the Navigation panel.
7. Click Node Manager. The Node Manager-Administration panel will open.
8. Click the Add Node Manager button in the Node Manager-Administration panel. The Add

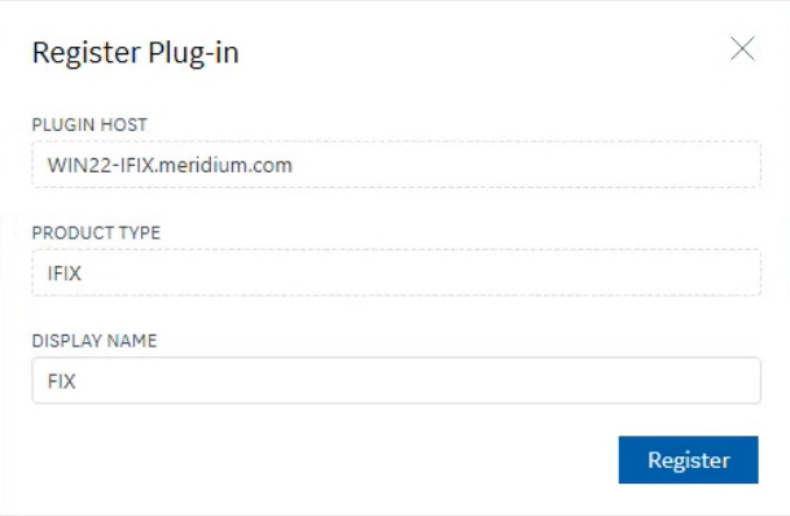
Node Manager dialog box will appear.



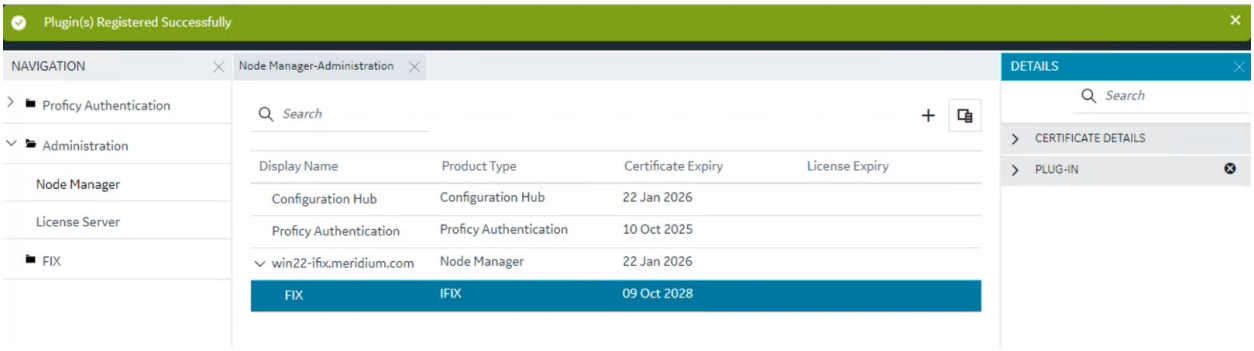
9. Enter the Host Name, Display Name and Port.
10. Click the Not Trusted link beside the certificate icon. The Certificate Details dialog will appear.
11. Click Trust.
12. Click Add.
13. The iFIX plug-in will appear under the node manager, but not in the navigation panel.



14. Click to open the Register Plug-in dialog.



15. Click Register. The iFIX plug-in will now appear in the navigation panel. Refresh the browser.



Registering with the Remote Configuration Hub

The remote Configuration Hub server root certificate (C:\Program Files (x86)\GE\ConfigurationHub\ConfigHubPki\ ConfigHubRootCA.crt) must be installed into the iFIX server windows certificate store trusted roots folder. To do that, copy the root certificate file from the remote Configuration Hub server (C:\Program Files (x86)\GE\ConfigurationHub\ConfigHubPki\ ConfigHubRootCA.crt) on to the iFIX server computer and then double-click on it to import it into the Local Machine Trusted Root Certificate Authorities.

Upgrade/Migration Considerations

Upgrade

- From iFIX 2022/iFIX 2023: If the common components have already been installed and upgraded to the latest version, the old/existing iFIX plug-in will be unregistered and replaced by the new plug-in during the install process.

- From iFIX 2024: If the common components have already been installed and upgraded, the old/existing iFIX plug-in will be retained.
- If you skip plug-in registration during install, or upgrade/install the common components after installing/upgrading iFIX, follow steps 1 to 7 above.

Migration of Common Components (v2024 or later) Post-Registration

If a new Proficy Authentication Server has been installed on the same network:

1. Unregister the iFIX plug-in. See "Unregistering iFIX Plug-in" below.
2. Unregister Configuration Hub with the old Proficy Authentication server and register with the new Proficy Authentication server.
3. Follow steps 1 to 7 above to provide the credentials for the new Proficy Authentication server.
4. Register iFIX using the Configuration Hub Administrator plug-in.

If a new Configuration Hub server has been installed on the same network:

1. Unregister the iFIX plug-in from the old Configuration Hub server. See "Unregistering iFIX Plug-in" below.
2. Register the new Configuration Hub server with the existing Proficy Authentication server.
3. Register iFIX using the Configuration Hub Administrator plug-in.

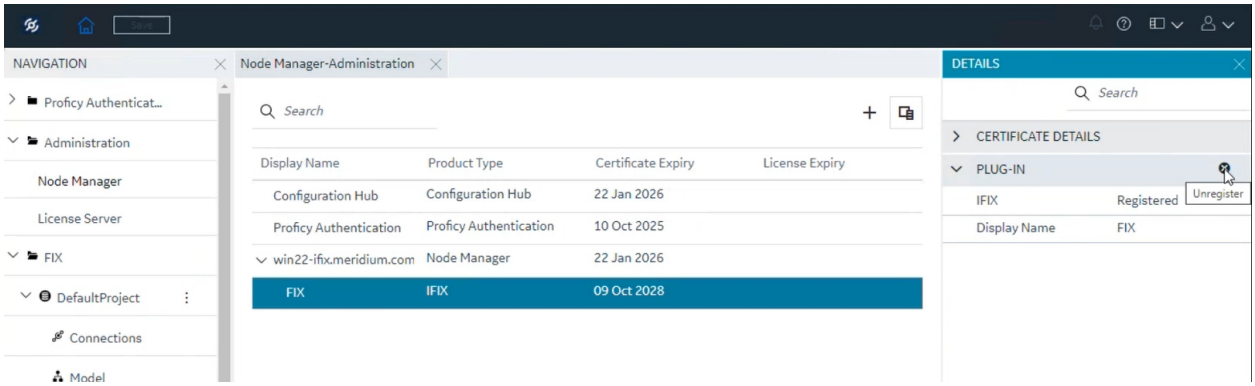
If both a new Configuration Hub server and Proficy Authentication server have been installed on the same network:

1. Unregister the iFIX plug-in from the old Configuration Hub server. See "Unregistering iFIX Plug-in" below.
2. Register the new Configuration Hub server with the existing Proficy Authentication server.
3. Follow steps 1 to 7 above to provide the credentials for the new Proficy Authentication server.
4. Register iFIX using the new Configuration Hub's Administrator plug-in.

Unregistering iFIX Plug-in

To un-register the iFIX plug-in in Configuration Hub:

1. Log in to Configuration Hub.
2. In the Navigation panel, expand the Administration section. Click Node Manager.
3. Click + in the Node Manager section to bring up the Add Node Manager dialog. Enter the host name of your SCADA device to trust the certificate. Click Add.
4. Expand the Node Manager to display your iFIX plug-in.
5. Select the iFIX plug-in in the main (center) pane, click ⊗ beside the PLUG-IN heading on the Details panel.
6. The Unregister Plug-in dialog will appear. Click Continue.

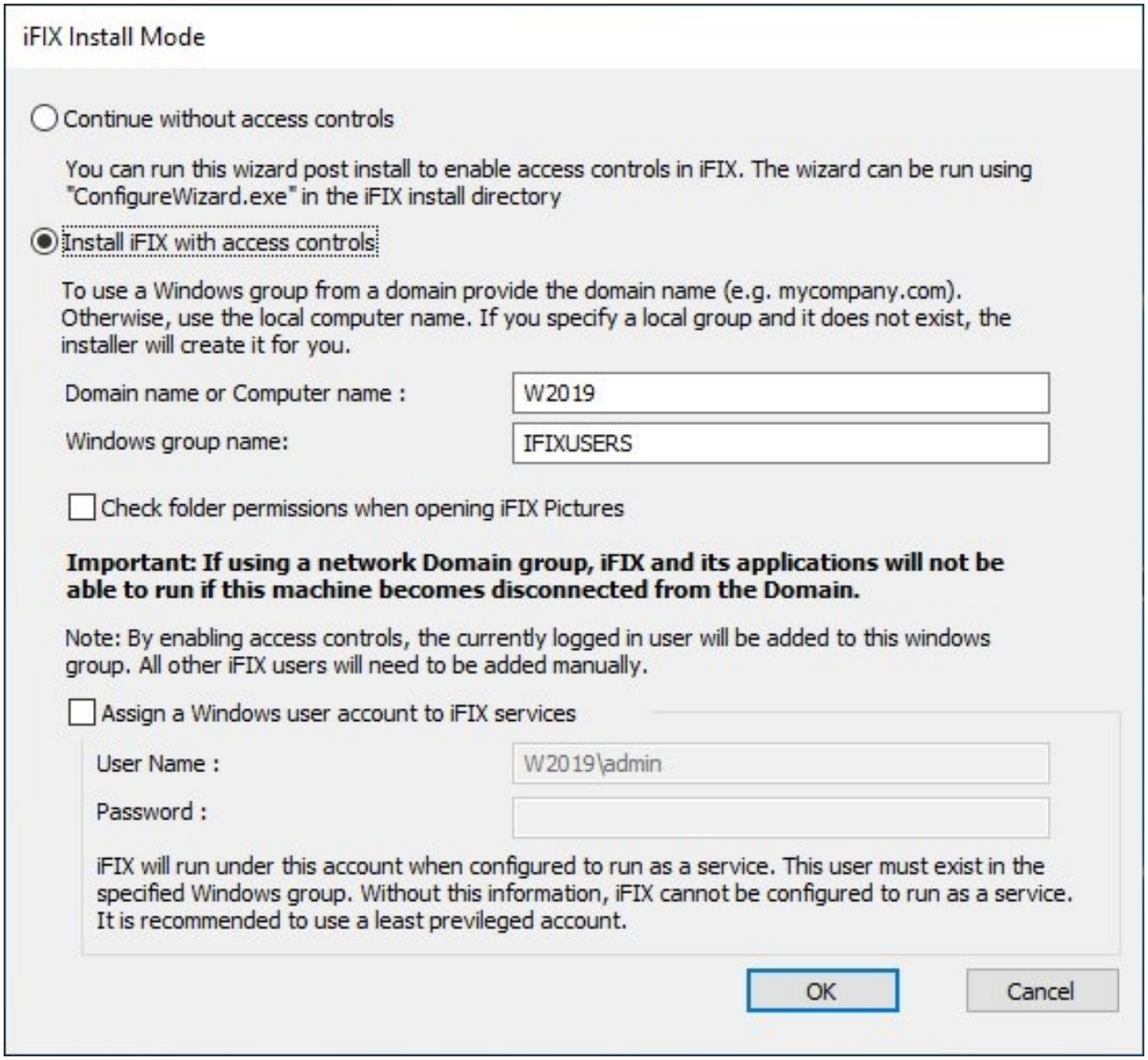


Access Controls in iFIX

The Access Controls feature in iFIX (formerly known as "secure mode") assists you in reducing security risks on your SCADA system. By applying Access Control Lists (ACLs) to iFIX, access rights to shared memory used by your iFIX processes, files, and Registry entries are regulated by Windows.

By default, Access Controls are disabled when you install iFIX to allow you to quickly configure your system. If you later want to enable Access Controls or change your current settings, you can do so by using the ConfigureWizard.exe. Click the Start menu, iFIX, and then select the Setup Access Controls option. You can also access ConfigureWizard.exe from the iFIX install folder; by default, this location is: C:\Program Files (x86)\Proficy\iFIX\ConfigureWizard.exe

With Access Controls enabled, you can also restrict the opening of pictures to folders that have restrictions based on Access Controls. For example, if a user has pictures in a non-default folder, such as C:\Temp\iFIXPictures, and the "Check folder permissions when opening iFIX Pictures" option is enabled, that folder will need to be secured with the group name configured in this Configure Wizard utility in order for the picture to be opened.



To configure access controls in iFIX:

1. From Start menu, select iFIX and then Setup Access Controls. Or, from the iFIX install folder, double-click ConfigureWizard.exe. By default this folder location is: C:\Program Files (x86)\Proficy\iFIX\ConfigureWizard.exe. The iFIX Install Mode dialog box appears.
2. Select the **Install iFIX with Access Controls** option.
3. If using a domain network group as the scope for validation, in the Domain or Computer Name field, enter a domain name (for example mycompany.com). Otherwise, specify the local computer name (the default).
   - When using the network domain group, iFIX and its applications will not be able to run if this machine becomes disconnected from the domain.

- If you specify a local group and it does not exist, the installer will create it for you. By choosing secure mode, the currently logged in user will be added to this Windows group. All other iFIX users will need to be manually added.

3. Optionally, if you want to secure your picture viewing, select the "Check folder permissions when opening iFIX Pictures" option.
4. Optionally, if you want to run iFIX as a service along with Access Controls, select the "Assign a Windows user account to iFIX services" option, and enter and user name and password. iFIX will run under this account when configured to run as a service. For more information, see "Windows and Security" on page 49.
   - This user must exist in the specified Windows group name.
   - If you choose not to provide this information, then iFIX cannot be configured to run as a service.
   - It is recommended to use a least privilege account, and not an administrative account.
5. Click OK to save your settings.
6. Restart your computer.
7. Start iFIX.

Running iFIX as a Service

If you are running iFIX as a service, please take note of the following information. For more information on Windows security and running iFIX as a service, see "Windows and Security" on page 49.

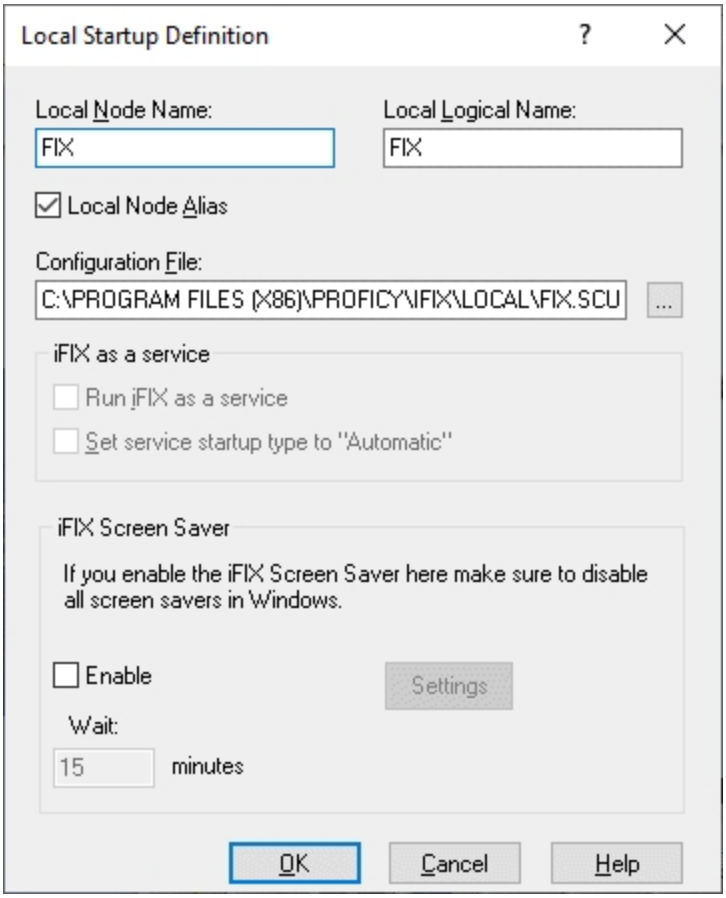
Windows Services

In the Windows Services control panel, do not stop the iFIX service or make changes to the iFIX configuration. This applies to iFIX running on any operating system.

Enabling iFIX to Run as a Service

To enable iFIX to run as a service:

1. Shut down iFIX.
2. Ensure that you are logged in as a user in the iFIX Administrators group. If not, log in as an Administrator now.
3. On the Start menu, point to Programs, iFIX, and then System Configuration. The System Configuration Utility (SCU) window appears.
4. On the Configure menu, click Local Startup. The Local Startup Definition dialog box appears.
5. In the Service area, select the "Run iFIX as a Service" check box, as illustrated in the following figure.This dialog box allows you to configures iFIX to run as a service when you start iFIX.



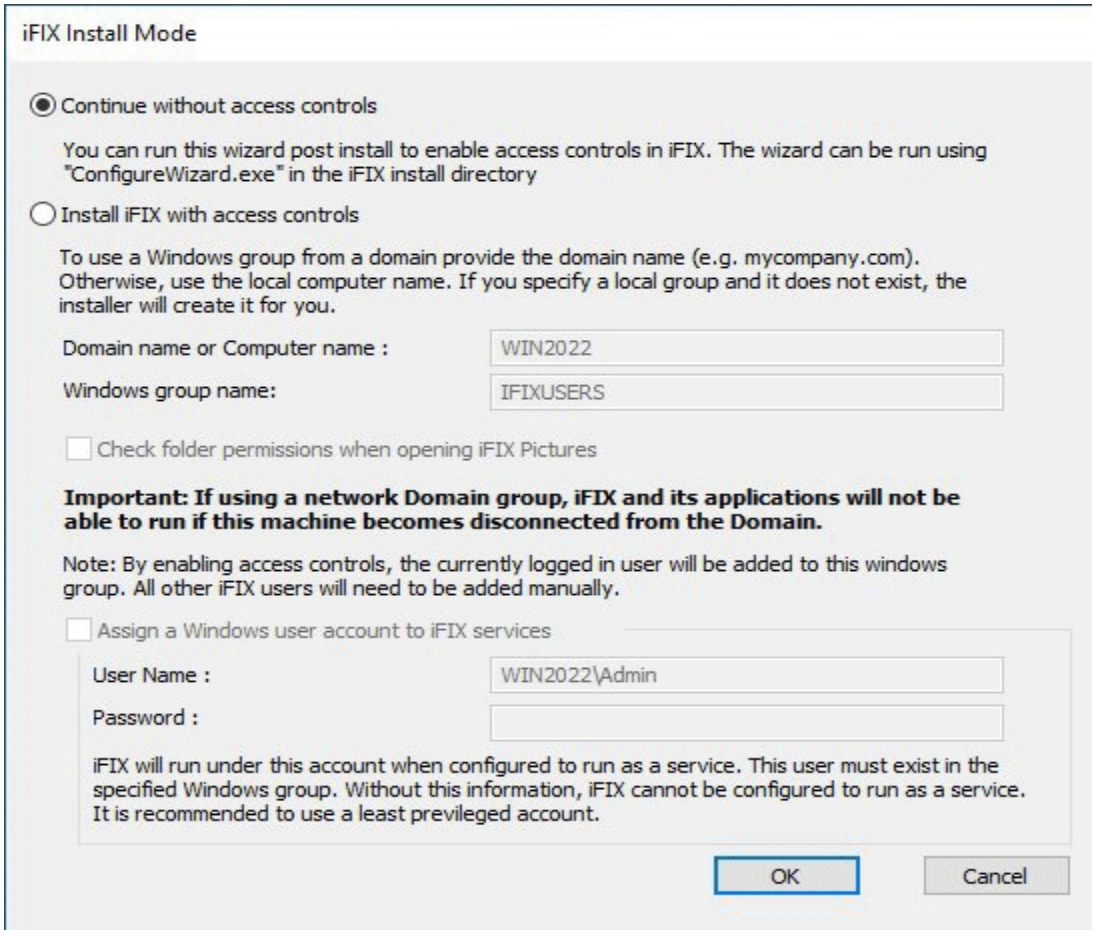
NOTE: The check boxes in the iFIX as a Service area of Local Startup Definition dialog box are unavailable while iFIX is running. You need to shut down iFIX, as you did in step 1, in order to configure the service. If a message appears that access controls are enabled (instead of greyed out fields), iFIX is running with access controls and the service account is not set up for this node. Run ConfigureWizard.exe in the iFIX install folder to add a Windows user to the iFIX service account. See steps below.

7. To start iFIX as a service when Windows starts, click the "*Set Service Startup type to Automatic*" option.
8. Click OK.
9. Save and exit the SCU.
10. Start iFIX, or restart Windows with a user allowed to run iFIX as a service.

Adding a Windows User to the iFIX Service Account

If you want to add a Windows user to the service account, follow these steps:

1. Log in as an iFIX Administrator.
2. Locate and run configure wizard (ConfigureWizard.exe) in the iFIX install folder. By default this path is: C:\Program Files (x86)\Proficy\iFIX\ConfigureWizard.exe. The Install Mode wizard appears.



3. Select the Install iFIX with Access Controls option.
4. Select the "Assign a Windows User Account to iFIX services" option.
5. Enter a user name. If on a domain, enter the fully qualified domain name with the user account. For example, the previous illustration specified W2022\Admin as the user account.-

   NOTE: When installing iFIX with access controls, the Windows Group name used from the domain or computer name provided (**IFIXUSERS**) must be different than any local group name configured on the machine with iFIX installed.
6. Enter the password for this account.
7. Click OK.
8. Restart your computer.
9. Start iFIX

Disabling iFIX as a Service

To disable iFIX from running as a service:

1. Shut down iFIX.
2. Ensure that you are logged in as a user in the Administrators group. If not, log in as an Administrator now.
3. On the Start menu, point to Programs, iFIX, and then System Configuration. The System Configuration Utility (SCU) window appears.
4. On the Configure menu, click Local Startup. The Local Startup Definition dialog box appears.
5. In the Service area of dialog box, clear the *Run iFIX as Service* check box.
6. lick OK.
7. On the File menu, click Save to save the SCU file.
8. Exit the SCU.
9. Restart iFIX.

iFIX Paths

Windows does not map network drives until a user logs in. Therefore, if you are running iFIX as a service under Windows, all iFIX paths must be set to a local drive.

Required Application Feature

You must assign the Enable Ctrl+Alt+Del application feature to the user that is logged in when iFIX is running as a service. Otherwise if a user logs out of the operating system while iFIX is running as a service, no one will be able to log back in to the operating system.

Running iFIX with Terminal Services

You must configure the Default Service SCU in the Startup Profile Manager if you want to run iFIX as a service on the Terminal Server. For more information, refer to the Configuring the Default Profile section in the Using Terminal Server electronic book.

Running iFIX with Other Programs

By default, iFIX uses the local System account when running as a service. However, you cannot use the System account with certain applications, such as Proficy Historian.

To configure a different user account for iFIX running as a service:

1. From Control Panel, open the Administrative Tools, then Services.
2. In the Services folder, right-click iFIX server and select Properties.
3. In the Log On tab, set the user name and password for This Account to the user account you want to log in when iFIX is running as a service.

Fast User Switching Not Supported

Fast user switching is not supported with iFIX, even if you are running iFIX as a service.

Running the OPC Client Driver and iFIX as a Service

If you want to run the OPC Client driver as a service, iFIX must also run as a service. Likewise, if you want to run iFIX as a service, the OPC Client driver must run as a service. You cannot run one as a

service, without the other also running as a service.

Running Workspace.exe from the SCU Task List Not Supported

It is not recommended that you run Workspace.exe in the SCU task list when iFIX is running as a service.

Using iFIX with Proficy Historian

With Proficy Historian, you can perform the following tasks in iFIX:

- Set Historian tags for collection for the iFIX database.
- Insert a Historical Data Link into your picture in the iFIX WorkSpace.
- Use a Historical HP Dynamo with Historian tags.
- Use Time Lapse Playback to replay an event.
- Use VisiconX data and grid objects to access Historian data from the iFIX WorkSpace.

When making your decision on how you want to use GE Historian with iFIX, keep the following considerations in mind.

Configuration Considerations

Although many of the features of GE Historian can be configured in iFIX, some cannot. They must be configured directly in GE Historian. These features include:

- Security
- Alarms, if you are using them
- Collection on any field other than F_CV.
- Archive compression
- Archive back-up
- Other tag properties not configurable in iFIX
- GE Historian parameters for Database Dynamos, or loadable blocks
- Redundancy

Other Considerations

Multiple Databases

Only a single, local database is supported with Proficy Historian. If you want to use multiple databases, you may want to use Proficy Historian separately from iFIX. When used together, Proficy Historian does not recognize tags from the iFIX database with the same name as different tags, even though the source is different. So, tags that exist in your iFIX database are ignored. The data that is populated comes from Proficy Historian, not from the iFIX database. To avoid this problem, verify that each tag has a unique name.

When using multiple iFIX databases that have the same node name and the same tag name, Proficy Historian will be unable to discriminate a tag coming from one node with a tag coming from another node, and these tags will be subsequently be ignored. It is best practice to not use the same iFIX node name on multiple nodes.

For example, you have a tag called AI1 in both Process Database 1 (PDB1) and Process Database 2 (PDB2). Both tags are added to Proficy Historian as FIX.AI1.F_CV. If you reload PDB1 and then PDB2, the AI1 tag is overwritten in Proficy Historian.

Collection Delay

When iFIX and Proficy Historian are used as an integrated application, rather than as separate applications, it takes longer for tags to update if the Collector is running. Additions, deletions and modifications of tags may take twice as long to display – approximately two minutes, instead of one – than if each application was used separately.

Collectors

If you choose to use Proficy Historian, not all installed collectors will be available for selection as the default Collector. Because this feature only supports collectors that read data from iFIX, the collectors available for selection are limited to the following:

- iFIX Native Collector

Electronic Signatures

If you use electronic signatures, then you should probably not use the integrated Proficy Historian feature. If a tag requires an electronic signature in Proficy Historian and does not in iFIX, and a user makes a change in iFIX, the user is not prompted for a password. Instead, the change is made, bypassing Proficy Historian's electronic signature requirement.

Spare1 Fields

When used with iFIX, the Proficy Historian Spare1 fields are used to keep track of tags that were added or modified by iFIX. When you enable Collection for a tag in the iFIX Database Manager (on the Proficy Historian tab, in the Collection Options area), the Spare1 field is assigned to iFIX. iFIX controls the creation or modification of this tag in Proficy Historian. In other words, iFIX becomes the owner of the Spare1 field. The Spare1 fields are written to when an iFIX tag is added for the first time from iFIX to the Proficy Historian Server. The Spare1 field contains the iFIX database name.

If you want to use the Spare1 field in Proficy Historian to allow data to be written to Proficy Historian from a third party application separate from iFIX, you need to Disable Collection on the tag from within iFIX (which is the default setting for any new tags you add in iFIX Database Manager). When disabled, Proficy Historian collection is not enabled for the tag and the tag is handled exclusively by Proficy Historian. When the tag is being handled by Proficy Historian, it cannot be modified or deleted from iFIX.

Choosing Not to Install Integrated Proficy Historian

If you do not want to install integrated Proficy Historian, and continue using Proficy Historian as you did before, then never do the following:

- Select the Automatically Configure Tags for Collection in Proficy Historian on the Proficy Historian tab of the User Preferences dialog box.

- Use Proficy Historian fields in iFIX Database Manager to configure anything in Proficy Historian.

Post-Installation Steps for Proficy Historian

If you choose to install Proficy Historian, there are post-installation steps you will need to perform. For more information, see Configuring iFIX to Use Proficy Historian and Configuring Security When Using iFIX with GE Historian.

Configuring Security When Using iFIX with Proficy Historian

Beginning with iFIX 5.0, iFIX configures Proficy Historian by adding and deleting tags and changing tag properties. Therefore, applicable security measures must be configured. However, tag level security and Proficy Historian domain security cannot be configured in the iFIX application; it must be done in Proficy Historian.

For Proficy Historian domain security, see "User Privileges for Starting a Collector" in the Proficy Historian e-book.

For all other security considerations for Proficy Historian, see the chapter "Implementing Historian Security" in the Proficy Historian e-book.

Configuring iFIX to Use Proficy Historian

The following tables describe the process for configuring iFIX to run with Proficy Historian:

Configuration Process - New Install of Historian

Stage	Description
1	Install iFIX.
2	Install Proficy Historian.
3	Install the Historian Client Tools and the iFIX Collector on the iFIX computer. **NOTE:** When configuring the iFIX collector from the Historian 9.0 media, see the additional steps below.
4	Define your security strategy for Historian and iFIX. Be sure to review the Historian security considerations in the "Implementing Historian Security" chapter of the Proficy Historian Getting Started guide before getting started. You may need to temporarily enable or disable these options during the installation process. Additionally, plan your iFIX security by reviewing the "Configuring Security Features" e-book in the iFIX e-books. If iFIX is not running as an Administrator, be sure to review the "User Privileges for Starting a Collector" topic in the Historian e-books as well.
5	Start iFIX and the WorkSpace.
6	On the iFIX computer, configure the iFIX Collector: • From the iFIX startup dialog box, open the SCU (System Configuration Utility) option.

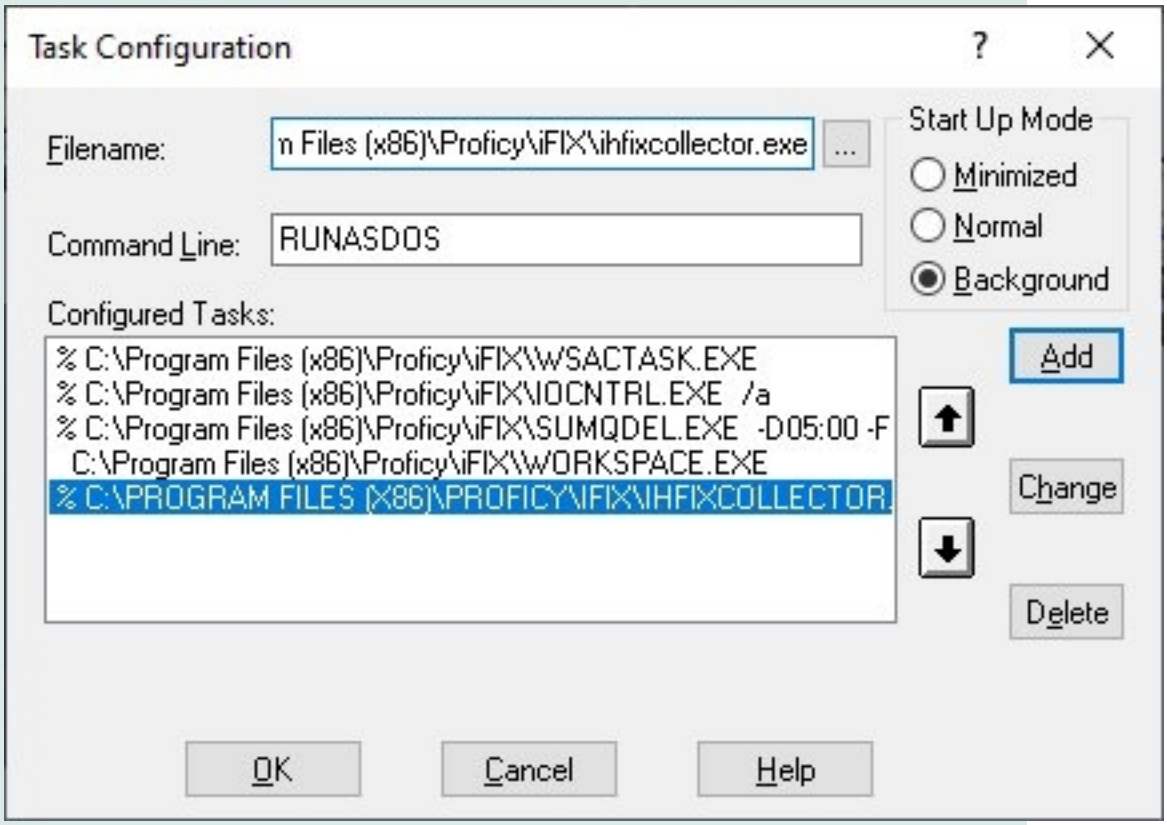
- On the Configure menu, select Tasks.
- Next to the Filename field, click the browse (…) button to select the ihfixcollector.exe file from the iFIX install folder (by default: C:\Program Files (x86)\Proficy\iFIX).
- In the Command Line field, enter one of the following command and click Add, and then OK and save the SCU file.

  IMPORTANT: When you add the iFIX Collector to the iFIX SCU Task list with the RUNASDOS command line, then the iFIX Collector will automatically start when iFIX starts, and you will not need to start the iFIX Collector manually.

Command Line 1: RUNASDOS

Use the RUNASDOS command to start default iFIX Collectors (applies to all versions of Historian except Historian 9.0 Collectors).

For example:



Command Line 2: SERVICENAME=COLLECTORSERVICENAME

Use this command to start the iFIX Collector to run as a Service.

For example, in the SCU task list, enter the command SERVICENAME=ihFixCollector with the startup mode as Background for the ihFIXCollector.exe. This example assumes that a service called ihFixCollector corresponding to the ihFIXCollector.exe application exists in the Windows Services list. The service name might be different in your Windows Services list. For default IFIX collector it is ihFixCollector.

Command Line 3: NOSERVICE

	Use this command line to start the default installed iFIX collector. You can also double-click the Start iFix Collector.bat file available in iFIX install folder to start the default Installed iFIX collector with the NOSERVICE command. For other instances of collectors use: `NOSERVICE REG=iFixCollector1` where *iFixCollector1* is the collector instance name provided in the Historian settings in Configuration Hub. After you make this change, launch iFIX and confirm your Collector starts. For Historian 9.0 and later versions , after you install the Historian Client Tools and iFIX Collector on the iFIX Server computer, you can register the iFIX Collector and create other instances of it from Configuration Hub. Refer to the Historian documentation for detailed steps on working with collectors. Use Configuration Hub with Historian to manage the collector. For Historian 9.0, you must add the instance of the iFIX Collector with Configuration Hub, as the default iFIX Collector is not created by install. The RUNASDOS command is not supported for Historian 9.0.

7	If using multiple Historian servers that are not mirror nodes, perform the following steps to add iFIX data:
	
	Add iFIX Data to Two Different Historian Servers which are Not Mirror Nodes (Historian 9.0 and Greater)
	
	Starting with Historian 9.0, you can use Configuration Hub to create multiple server instances and it will create the necessary registry entry and multiple instances of the ihFIXCollector.exe that can be run.
	
	-OR-
	
	Add iFIX Data to Two Different Historian Servers which are Not Mirror Nodes (Earlier Than Historian 9.0)
	
	If you need to send iFIX Data to two different Historian Servers which are not Mirror nodes:
	
	• Copy the “ihFIXCollector.exe" file from the iFIX install folder, paste it to a new location, and rename the new exe file as “ihFIXCollector2.exe”.
	• Go to the Windows Registry, and locate the following key: “Hkey_local_machine > Software > Wow6432Node > Intellution, Inc.”
	• Add a key under “iFixCollector.” Name this key as “FIX2nd”.
	• Add the following values for “FIX2nd”: General1 - General5, HistorianNodeName, and InterfaceName. The other values will be auto-created when the collector first starts up. Only three of the seven values need to be set:
	  ◦ General3 = iFix node name
	  ◦ HistorianNodeName = Computer name of Historian server
	  ◦ InterfaceName = Name for this iFIX collector displayed in Historian Administrator; must be different from the 1st iFix collector
	• For more information, see KB article 000034196 on digitalsupport.ge.com

8	Restart iFIX to start the Collector.
9	Configure iFIX to automatically add tag data to a single Historian server (the FIXTOHIST process is used in the background to do this). This only works if only one iFIX Collector is being used.

	In the iFIX WorkSpace, on the Administration tab: 1. Click **Configure Historian** and then Configure the Historian Server. The Configure the Proficy Historian Server(s) dialog box appears. 2. Click **Get Collectors.** (The name of iFIX Collector that is already started will be populated in the Collector Name box.) 3. Select the Collector name from the box, and then click **Set Default**. Review the Using iFIX with Proficy Historian section first before enabling a default collector. 4. To enable Historian data collection for an iFIX tag, enable Historian Collect in **Configuration Hub** or in the **iFIX Database Manager** for the tag. (When configured in this manner through iFIX, only iFIX tags with Historian options enabled will be automatically added to the Historian Administrator.)

Historian Upgrade Process

The following steps outline the process to upgrade Historian.

Configuration Process - Upgrade to GE Historian

Stage	Description
1	If upgrading from a previous release of iFIX and you have GE Historian installed on the PC, shut down all services and licensing prior to installing iFIX and then GE Historian.
2	Install iFIX.
3	Back up all the Proficy Historian archive data files (*.iha), configuration files (*.ihc), and any other backup files you maintained. By default, you can find these files in the c:\Program Files\Proficy\Historian Data\Archives folder. Make a copy of those backup files.
4	From the Add or Remove Programs feature in the Control Panel, manually uninstall Historian. Do Not Delete Archives when prompted.
5	Restart your computer.
6	Install Historian as described in the Historian Getting Started guide.
7	After the install completes, restart your computer. It is very important not to forget this step, and to restart your computer. Make sure the Historian Archiver is running.
8	Restore your Proficy Historian archive using the Historian Administrator.
9	Copy your configuration files (*.ihc) to the Archive folder.
10	Install the Historian Client Tools and the iFIX Collector on your iFIX SCADA Server. **IMPORTANT:** When upgrading from a previous version of Historian, Enforce Strict Client Authentication and Enforce Strict Collector Authentication should be disabled on the Historian Server to allow for compatibility with older clients or collectors that cannot be upgraded concurrently. It is recommended that all clients and collectors receive a timely upgrade to the latest version of Historian, which permits enabling both strict client and collector authentication on the server for the highest security configuration. By treating clients and collectors separately, it is possible to accommodate new and legacy authentication during the upgrade process. However, upgrading all clients and collectors to the latest version immediately will achieve a higher level of security. The two options, Enforce Strict Client Authentication and Enforce Strict Collector Authentication, permit flexibility during the upgrade process by selectively accommodating legacy clients and collectors.
11	Configure iFIX and your Proficy Historian Server.

Limiting the Number of Historian Servers at Workspace Startup

By default, on startup, the iFIX WorkSpace connects to all the Historian servers that have been configured, including those configured outside of iFIX such as with the Historian Administrator. If you have a large number of Historian servers, you may notice that the WorkSpace takes a long time to start. You can limit the number of Historian servers that iFIX connects to when it starts by configuring a setting in the FixUserPreferences.ini file. The FixUserPreferences.ini file is found in the iFIX\Local folder.

The WorkspaceStartupConnectHistDataSourceOnly option in the FixUserPreferences.INI file allows you to limit the number of Historian servers that WorkSpace connects to when it starts up. When enabled, the WorkSpace will connect only to the Historian servers that have been configured as historical data sources in iFIX. Typically, an iFIX historical data source is created when you use the Configure Historian Server menu item or toolbar in the iFIX WorkSpace.

To activate this feature, in the FixUserPreferences.ini file, in the [Historian] section, add the "WorkspaceStartupConnectHistDataSourcesOnly " parameter and set the value to 1. For example, here is the setting enabled:

```
[Historian]
WorkspaceStartupConnectHistDataSourcesOnly=1
```

To disable the option, set WorkspaceStartupConnectHistDataSourcesOnly to 0. For example:

```
WorkspaceStartupConnectHistDataSourcesOnly=0
```

The WorkSpace must be restarted for any changes to the WorkspaceStartupConnectHistDataSourcesOnly parameter to take effect.

Using iFIX with Microsoft Office

You can use the Microsoft Office family of products and iFIX on the same computer. However, to ensure that VBA works correctly, install Microsoft Office products before installing iFIX.

Use the following table as a guide for installing and removing either product.

If you have...	And you want to...	Then...
Installed iFIX	Install Microsoft Office Products	Remove iFIX, install Microsoft Office products, and re-install iFIX.
Installed Microsoft Office Products	Remove Microsoft Office Products	Remove iFIX, remove Microsoft Office products, and re-install iFIX.
Started the iFIX WorkSpace for the first time, and this message appears: Run time error "48": Error in loading dll.	Use iFIX and Microsoft Office harmoniously	Uninstall iFIX, uninstall Microsoft Office, re-install Microsoft Office, and re-install iFIX.

Backup Files

When you save one of the following files, iFIX creates a backup file:

- ***.PDB** – backed up as *.^DB
- ***.SCU** – backed up as *.^CU
- **Profiles.cfg** – backed up as Profiles.cfg.^AK

- **DISPLAY.DOV** – backed up as DISPLAY.^OV
- **NODENAME.DOV** – backed up as NODENAME.^OV

iFIX also creates these backup files after you start iFIX for the first time after an upgrade. These backup files are helpful in disaster recovery of the individual files.

For new iFIX installs, be aware that you can also use the Factory Default Backup for disaster recovery – performing a clean restore of your entire iFIX system. A clean restore includes the files listed above along with other Factory Default files. For more information, refer to the Using and Creating Factory Default Files section in the Understanding iFIX electronic book.

For upgrades, be aware that you can perform a backup to backup the files listed above before the upgrade. After the upgrade, you can restore these files with the Backup and Restore wizard. Refer to the Overview of the Backup Process section in the Understanding iFIX electronic book for more information.

Optionally, after you upgrade your system with the Custom Backup, you can create a new Factory Default Backup, that you can use for disaster recovery in replace of the original Factory Default Backup file. This information is described in the Using and Creating Factory Default Files and Sample BackupRestore.ini sections.

Optimizing Virtual Memory

Through the use of paging files, Windows allocates space on your hard drive for use as if it were actually memory. This space is known as virtual memory. The following steps describe how to optimize virtual memory in Windows to achieve maximum performance from iFIX.

To optimize the virtual memory paging file for iFIX in Windows:

1. From the Windows Control Panel, select System, and click on Advanced Systems. Next, click the Advanced tab and then in the Performance section click Settings. The Performance Options dialog box appears. Click the Advanced tab.
2. In the Virtual Memory group box, select Change.
3. In the Initial Size field, enter a value equal to three times your physical memory, or enter 4 GB; the value should not to exceed the Maximum Size value.
4. In the Maximum Size field, enter a value equal to three times your physical memory, or enter 4 GB – whichever is the larger of the two values.

   NOTE: For more information on the 4 GB paging file limit, refer to article 237740 on the Microsoft Knowledgebase: http://support.microsoft.com/kb/237740/en-us.

6. Select Set.
7. Click OK to save the changes and exit the dialog box.

   NOTE: If the paging file is set to grow dynamically, your system may experience severe performance problems during runtime. To ensure optimal performance, be sure that the Initial Size and Maximum Size of the paging file are the same so that the paging file does not grow dynamically.

OPC Certification

Based on Microsoft's OLE (Object Linking and Embedding) technology, OPC (OLE for Process Control) provides greater interoperability between control applications, field systems and devices, and front office/backoffice applications. OPC servers, such as DCSs, PLCs, smart field devices, and analyzers provide real-time information and can communicate directly with the iFIX product.

The iFIX product is an OPC 2.05a DA enabled client, which lets iFIX retrieve data from any OPC 1.x or 2.x (up to version 2.05a) compliant data server. To access local or remote data from a third party OPC Server, use the iFIX OPC Client version 7.4x, which is also in included with iFIX.

iFIX also has an iFIX OPC Server (OPC20iFIX.exe) that serves out data via OPC from the iFIX Database.

Be aware that iFIX currently includes two OPC servers:

- OPC20iFIX.exe (Intellution.OPCiFIX) – an OPC 2.05a (out of process) Data Server
- iFixOPCAESrv.exe – an OPC 1.10 Alarm and Events (A&E) Server

Both OPC Servers included with iFIX are in compliance with the OPC Foundation's "Self Tested" specifications. GE ran a series of OPC tests to verify compliance for the versions listed above.

You can find more information about OPC on the Support web site at: https://digitalsupport.ge.com.

Optional Hardware

iFIX supports the following optional hardware. You may want to purchase one or more of these items to enhance your iFIX system.

- A Microsoft-supported touch screen or other pointing device.
- A DigiBoard™ to provide your computer with up to 9 serial ports. If you are using multiple I/O drivers or multiple ports for one I/O driver, you may require the use of a DigiBoard. GE has tested and supports the Digichannel PC/8E.

Insufficient Disk Space

The iFIX WorkSpace checks to make sure you have at least 10 MB of disk space when you save a picture or a schedule. If there is insufficient disk space, the WorkSpace may react unpredictably and you may lose your work.

To help minimize this problem, the WorkSpace warns you if you have less than 10 MB of disk space available. Although you can continue loading the software, we recommend that you stop iFIX, free some disk space, then restart. Otherwise, the WorkSpace may become unstable.

The WorkSpace examines the iFIX Picture path and the Windows TEMP path when it starts. If you change either path so that they reference different drives, for example, D:\Program Files (x86)\Proficy\iFIX\iFIX and C:\Temp, the WorkSpace requires 10 MB on each drive.

You may find that 10MB is not enough space to protect against instability during file save operations. You can increase this threshold by changing the FreeDiskSpace parameter in the FixUserPreferences.ini file. This parameter sets the minimum amount of space that the WorkSpace requires in bytes. By default, the parameter is set as follows:

```
[AppRunPreferences]
FreeDiskSpace=10000000
```

To change FreeDiskSpace parameter:

1. Shut down the WorkSpace.
2. Locate the FixUserPreferences.ini file in the Local path.
3. Open the file with a text editor, and change the FreeDiskSpace parameter to the amount you want.
4. Save the .INI file and restart the WorkSpace.

Uninstalling iFIX

IMPORTANT: Do not to delete the user group that was created/used by the iFIX installer (to apply ACLs) before you uninstall the iFIX product. Instead, uninstall iFIX first, and then you can optionally remove this Windows group.

To uninstall iFIX, from the Control Panel, in the Add or Remove Programs dialog box, click the Remove button next to the iFIX entry. This action launches the install program allowing you to remove the iFIX product.

If you want to uninstall other items that install along with iFIX, such as the iFIX OPC Client, Common Licensing, and Discover and Auto Configure application, you need to uninstall these items separately.

Sleep or Hibernate Mode

If your SCADA computer has been sleeping overnight, or in hibernate mode, be aware that you will need to acknowledge all of the queued "License Warning" messages.

Setting Up for Remote OPC Server Access

Before you can access remote OPC servers in iFIX, you must make sure your firewall settings are correct and that the Distributed Component Object Model (DCOM) settings for your operating system are correct. These settings can be different for each operating system and also for different product revisions. If the settings are not correctly set, you may not be able to access remote OPC servers. Changes to these settings should be reviewed and approved by your system/security administrator.

For more information on configuring these settings, refer to the following:

- For DCOM information, refer to the Setting Up DCOM for Use with Remote OPC Servers section.
- For Firewall information, refer to the Setting Up the Firewall for Use with Remote OPC Server section.

Setting Up DCOM for Use with Remote OPC Servers

iFIX supports DCOM (Distributed Component Object Model) to browse remote OPC Servers. If you want to grant only certain users permission to launch or access the remote OPC servers, you can use the Windows utility, DCOMCNFG.EXE for configuring DCOM applications. DCOMCNFG.EXE is usually located in your operating system's \system32 folder.

When OPC Servers register, they set up initial custom DCOM security settings to enable users on the network to access and launch the Server. On large networks, it is recommended that you modify these settings to avoid confusion and inadvertent changes to a running OPC Server.

If Firewall security is enabled on Windows, you must also modify or add items to the Exceptions list. Refer to Setting Up the Firewall for Use with Remote OPC Servers section for more information.

IMPORTANT NOTES:

- It is recommended that all users that need to access remote OPC Servers be members of the Administrators group. To facilitate this, it is recommended that you create a users group to contain individual users that need to access remote OPC servers.
- To make any OPC Client / OPC Server application work via DCOM, changes need to be made on both sides, especially if you intend to use Asynchronous I/O communications.
- OPCENUM must reside on the remote machine with the OPC server. While most OPC Server applications install and register this file, some do not. You can download this file from www.opcfoundation.org. Currently it is contained within the OPC Core Components 2.00 Redistributable 2.30.msi file. After you download OPCENUM, run the .msi file.
- This section applies to OPC servers that need to use DCOM communications, regardless of whether the OPC server uses Serial or Ethernet devices.
- If OPC communications is confined to a single machine (that is, using COM, but not DCOM), it continues to work properly without making changes to DCOM settings.
- If you do not plan to use iFIX to connect remotely to OPC servers, then you may not need to change your DCOM settings.
- If this is the first time you are connecting to (or allowing connections from) other machines on the network, you must run the Windows Network Wizard (from Start > Control Panel) to set up your computer to run on your network. This allows you to share resources on your computer with other computers on your network. It is recommended that you run the Network Setup Wizard before modifying the DCOM settings.

DCOM Settings

The following procedures provide general guidelines for configuring DCOM settings.

To launch the DCOM configurator:

1. From the Start menu, select or type Run. The Run dialog box appears.
2. Type dcomcnfg and click OK. The Component Services dialog box appears.

System-wide COM/DCOM Limits Settings

This procedure modifies the system-wide DCOM settings for the computer on Windows operating systems. When these steps are implemented, they apply to all programs that use COM/DCOM communications on the computer.

IMPORTANT: Be careful when making any system-wide security changes. Any inadvertent changes may affect the entire system and may cause some or all programs to stop working.

To update system-wide COM/DCOM limits settings:

1. On the Component Services dialog box, expand Component Services, then expand the Computers item.
2. Right-click My Computer and choose Properties. The My Computer Properties dialog box appears.
3. Click the COM Security tab. There are four permissions on this dialog box.

   You may need to make changes to the Edit Limits… for Access Permissions and Launch and Activation Permissions.

   Do not change the Edit Default… settings, since this will change the default settings for all programs and applications running on the computer.
4. Click Access Permissions > Edit Limits… The Access Permission dialog box appears.
   i. Select the user labeled ANONYMOUS LOGON, and then select the Allow check box for Remote Access.

      NOTE: This setting is necessary for applications that use OPCenum.exe to function and also for some OPC Servers and OPC Clients that set their DCOM 'Authentication Level' to 'None' to allow anonymous connections. If you do not use such applications, you may not need to enable remote access for anonymous logon users.

   ii. Select the user labeled Everyone, and then select the Allow check box for Remote Access.

      IMPORTANT: Since “Everyone” includes all authenticated users, it is recommended to add these permissions to a smaller subset of users. One way of doing this is to create a Group named “OPC” and add all user accounts to this Group that will access any OPC server. Then substitute “OPC” everywhere that “Everyone” appears in the entire DCOM configuration dialogs.

   iii. Click OK to close the Access Permissions dialog box and return to the My Computer Properties dialog box.
5. Click Launch and Activation Permissions > Edit Limits… The Launch Permission dialog box appears.

   For each user or group (preferably add the “OPC” group) that needs to launch or activate the OPC server, or participates in OPC / DCOM communications, make sure that the Local Launch, Remote Launch, Local Activation, and Remote Activation check boxes are selected.

6. Click OK to save your changes, then click OK again to save and close the My Computer Properties dialog box.

OPC Server-specific DCOM Settings

The following procedures detail the OPC server-specific COM/DCOM settings on all supported Windows operating systems. You must change the OPC server settings so remote users can access the OPC server as an OPC Data Access Server. This procedure is also necessary for the GE OPC Client driver to connect to, launch, configure, and start the remote OPC servers.

It is recommended that all users requiring access to remote OPC servers be members of the Administrators group.

IMPORTANT: Since the “Everyone” group includes all authenticated users, it is recommended to add these permissions to a smaller subset of users.

It is recommended that you create a group to contain individual users that need to access remote OPC servers. It is also recommended that all users who require access to see OPC Servers be members of the Administrators group.

To modify driver-specific DCOM settings in Windows:

1. Access the DCOM configurator (dcomcnfg.exe). The Component Services dialog box appears.
2. Expand the Component Services item, then expand the Computers item, and then expand the My Computer item.
3. Select the DCOM Config object. A list of applications displays.
4. Right-click the OPC server you want to modify and choose Properties. The <Selected OPC Server> Properties dialog box appears.
5. Click the General tab. The Authentication Level should be set to “Default,” if it is not already. This uses the default authentication rules that are set in the system-wide DCOM settings.
6. Click the Location tab and make sure that the "Run Application on this computer" check box is selected.
7. Click the Security tab and select the Customize option for each of the permissions in this dialog box and edit them as described in the following steps.
8. In the Launch and Activation Permissions area, click Edit. The Launch and Activation Permission dialog box appears.
9. Click the Add button. The Select Users or Groups dialog box appears.
10. Click the Advanced Button. Another Select Users or Groups dialog box appears.
11. Click the Find Now button. In the search results, select the OPC group and click OK. The Select Users or Groups dialog box displays the OPC group.
12. Click OK to return to the Launch Permission dialog box. The OPC group is displayed in the Group or user names list.
13. Select the OPC group and then select the Allow check boxes for Local Launch, Remote Launch, Local Activation, and Remote Activation permissions.
14. Click OK to return to the <Selected OPC Server> Properties dialog box.
15. In the Access Permissions area, click Edit. The Access Permission dialog box appears.

16. Click the Add button. The Select Users or Groups dialog box appears.
17. Click the Advanced Button. Another Select Users or Groups dialog box appears.
18. Click the Find Now button. In the search results, select the OPC group and click OK. The Select Users or Groups dialog box displays the OPC group.
19. Click OK to return to the Access Permission dialog box. The OPC group is displayed in the Group or user names list.
20. Select the OPC group and then select the Allow check boxes for Local Access and Remote Access permissions.
21. Click OK to return to the <Selected OPC Server> Properties dialog box.
22. In the Configuration Permissions area, click Edit. The Change Configuration Permission dialog box appears.
23. Click the Add button. The Select Users or Groups dialog box appears.
24. Click the Advanced Button. Another Select Users or Groups dialog box appears.
25. Click the Find Now button. In the search results, select the OPC group and click OK. The Select Users or Groups dialog box displays the OPC group.
26. Click OK to return to the Change Configuration Permission dialog box. The OPC group is displayed in the Group or user names list.
27. Select the OPC group and then select the Allow check boxes for Full Control and Read permissions.
28. Click OK to return to the <Selected OPC Server> Properties dialog box.
29. Click OK.
30. Repeat steps 2 through 29 for each OPC server you need to access remotely.
31. When you are done, close the Component Services dialog box.

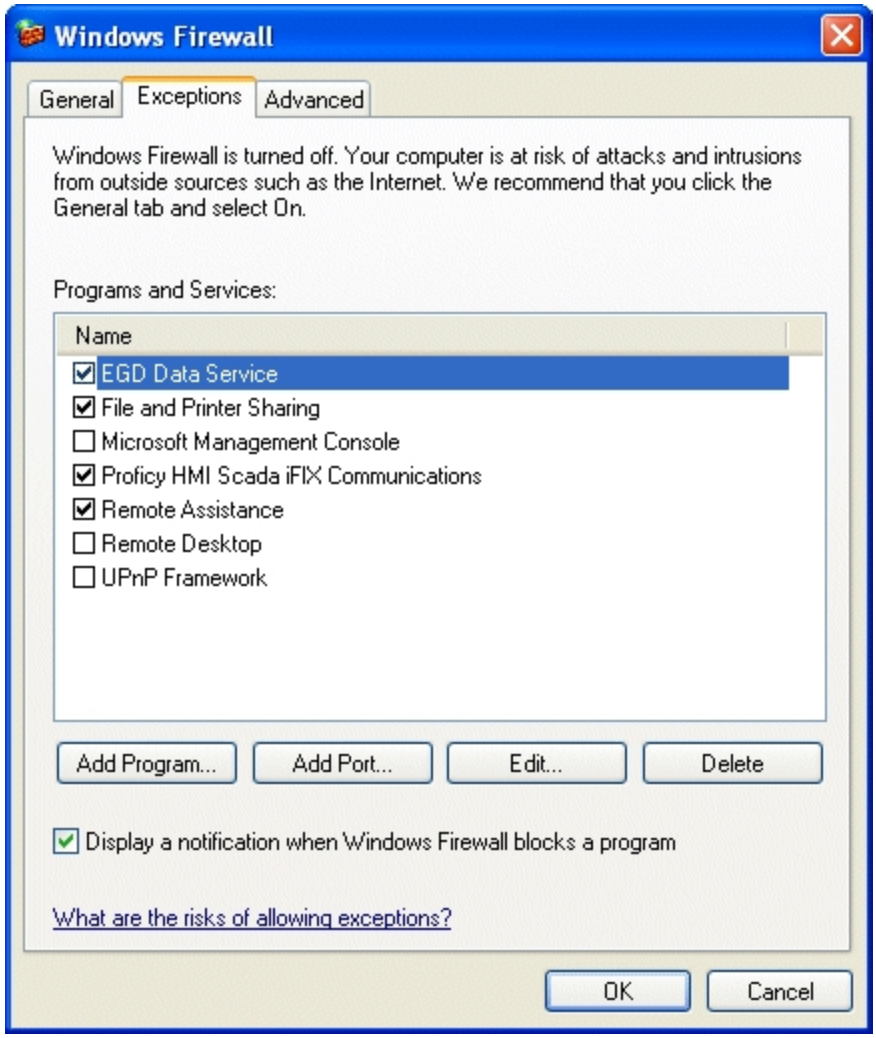
Setting Up the Firewall for Use with Remote OPC Servers

If Firewall security is enabled you may need to modify or add items to the Exceptions list.

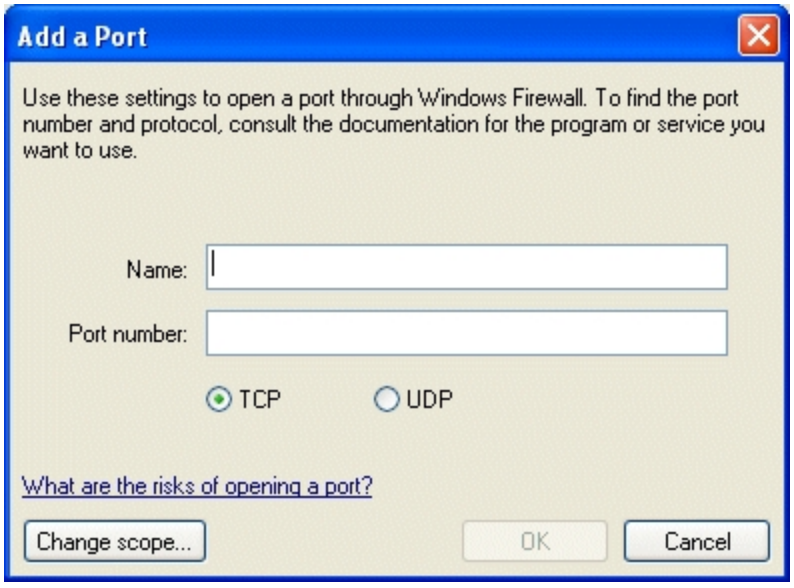
It is recommended that you enter these settings on the local machine running iFIX, as well as on the remote machine that has the OPC server you want to use.

To modify Windows Firewall settings:

1. Log into the Windows operating system with an Administrator account.
2. Open the Control Panel and double-click Windows Firewall. The Windows Firewall dialog box appears. For the Windows Vista operating system, you also need to click the "Allow a program through Windows firewall" option.
3. Click the Exceptions tab and make sure that the File and Printer Sharing check box is selected. The following figure shows an example of this dialog box in Microsoft Windows XP.

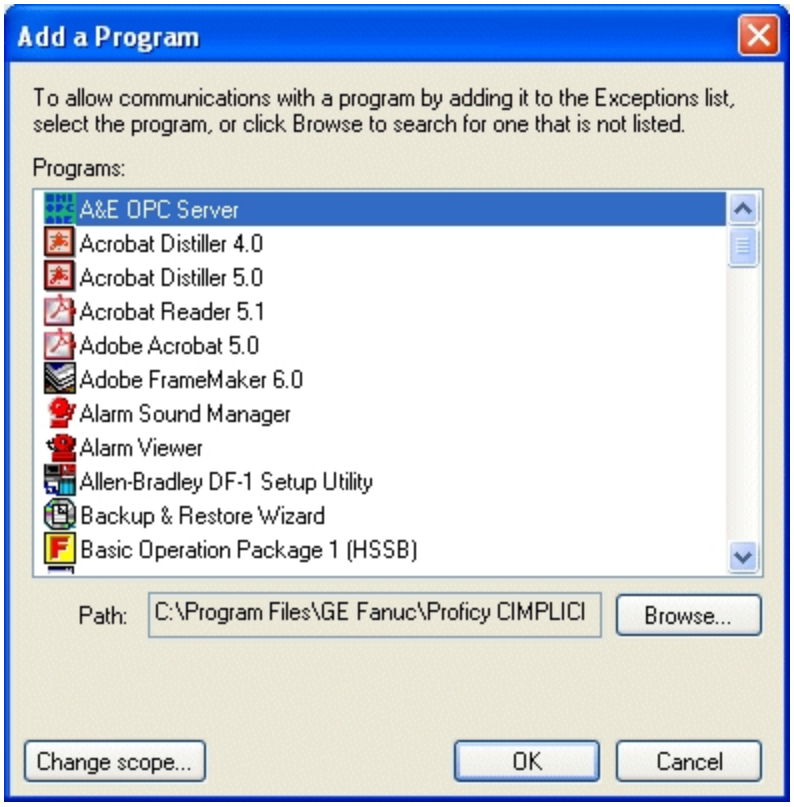


4. Click the Add Port button. The Add a Port dialog box appears. The following figure shows an example of this dialog box in Microsoft Windows XP.

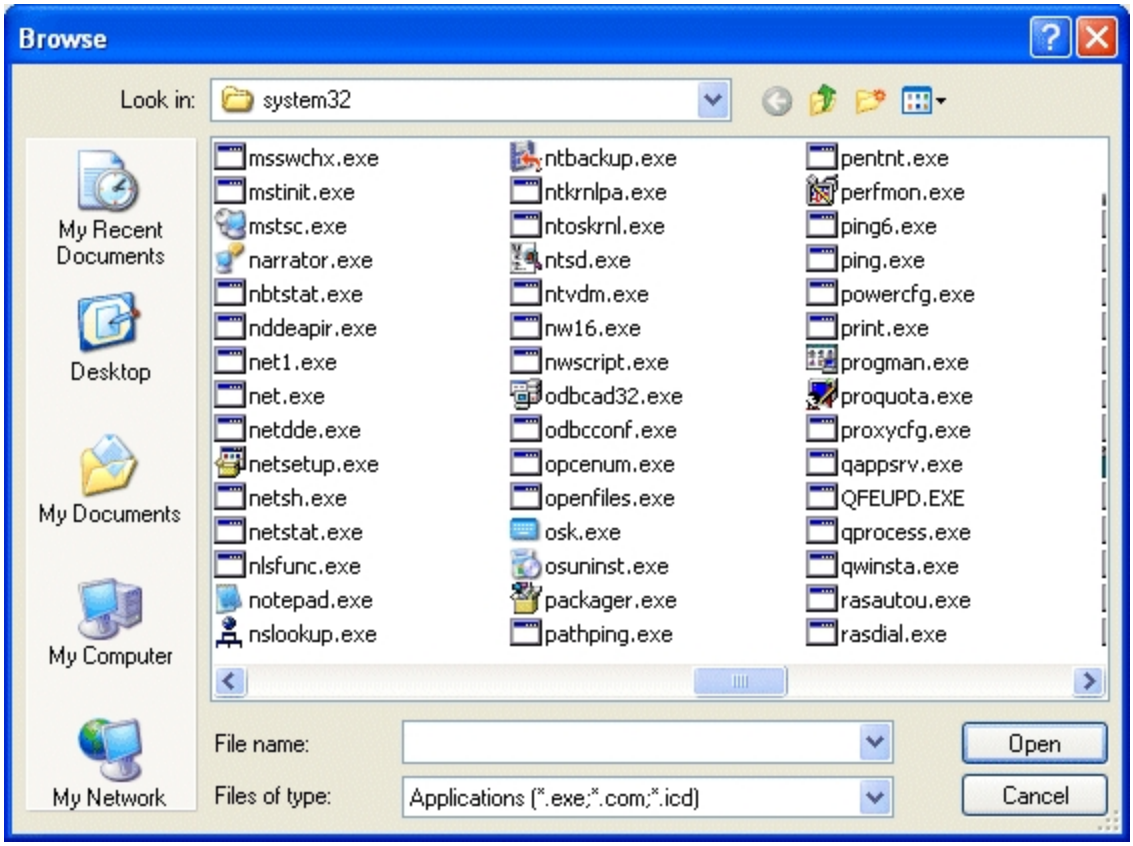


5. In the Name field, enter a name for the port.
6. In the Port Number field enter 135.
7. Select the TCP option.
8. Click OK to save your changes.

   The port name you entered is now listed with its check box selected.
9. Select the Add Program button. The Add a Program dialog box appears. The following figure shows an example of this dialog box in Microsoft Windows XP.

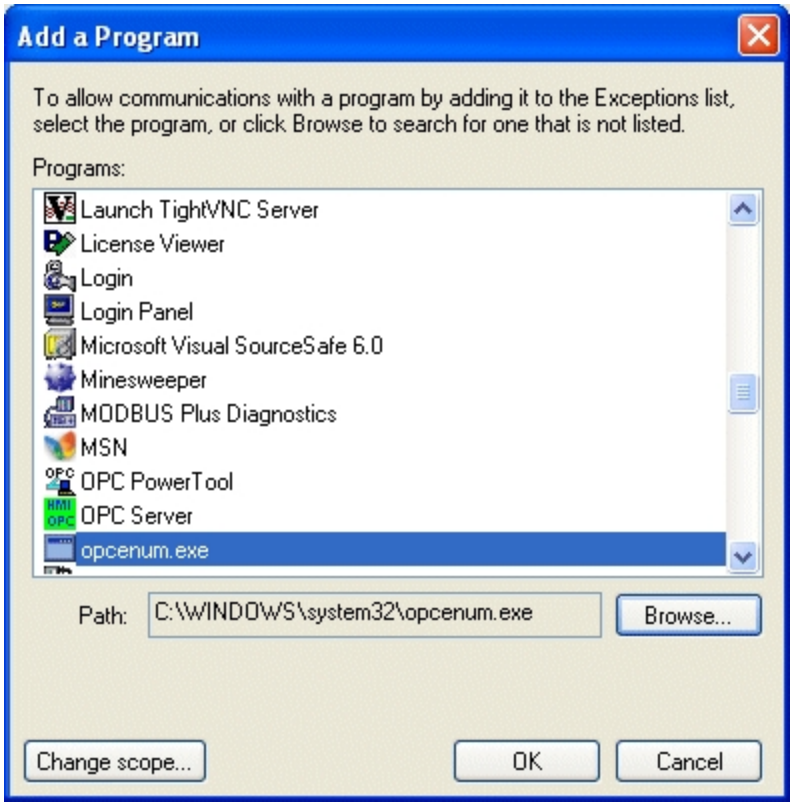


10. Click the Browse button. A Browse dialog box appears.



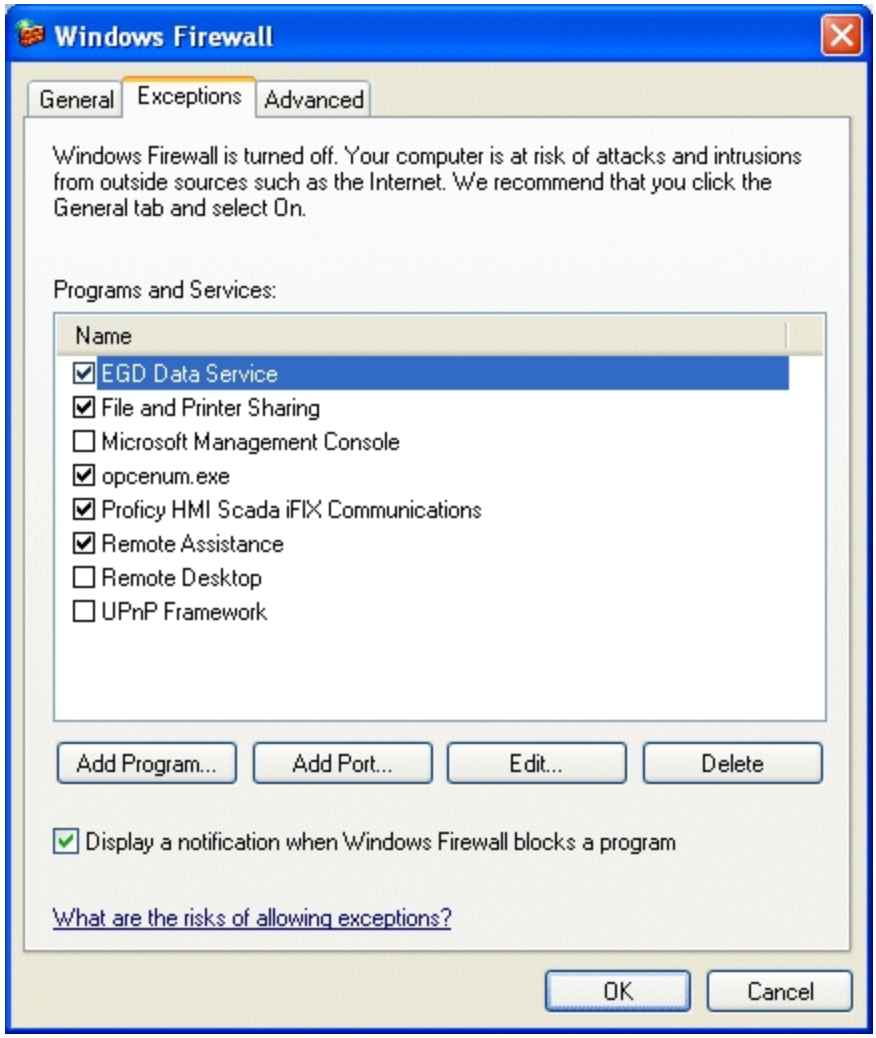
11. Navigate to the System32 folder. This folder is found under the operating system folder (usually Windows or WINNT).
12. In the System32 folder, select the OPCENUM.exe file, and then click the Open button.

    In the Add a Program dialog box the path field displays the full path to, and including, the OPCENUM.exe file.



13. Click OK.

    OPCENUM.exe should now be listed in the Exceptions list with its check box selected.



14. Complete steps 9-13 for each OPC server that you want to access.

NOTES:

- If any OPC server that you want to use is a dll surrogate (an in-process dll and not an .exe), you must add \system32\dllhost.exe into the Exceptions list.
- You must also add the GE OPC Client driver by adding the file OPCDrv.exe into the Exceptions list.
- OPCENUM must reside on the remote machine with the OPC server. While most OPC Server applications install and register this file, some do not. You can download this file from www.opcfoundation.org. Currently it is contained within the OPC Core Components 2.00 Redistributable 2.30.msi file. After you download OPCENUM, run the .msi file.

Windows Operating System Considerations

When using iFIX in newer versions of Windows, be aware of the following limitations when working with these products:

- **GE OPC Client Driver** – If you want to run the OPC Client driver as a service, iFIX must also run as a service. Likewise, if you want to run iFIX as a service, the OPC Client driver must run as a service. You cannot run one as a service, without the other also running as a service.

  If you want to run the OPC Client driver, be sure to check with the vendor of your OPC Server software to see if your OPC Server supports the operating system that you want to use.
- **Third-Party OPC Servers** – Be aware that at the time of the iFIX release there were a limited number of OPC Servers supported on newer versions of Windows. iFIX was tested with the OPC20iFIX.exe (Intellution.OPCiFIX) Server – an OPC 2.05a (out of process) Data Server.
- **Drivers** – If you want to run a driver on a newer operating system, be sure to check with the vendor of your driver software to see if your driver supports the operating system. Your driver must support your operating system.
- **VisiconX –** Make sure that your data sources use UNC pathing, rather than mapped network drives. For example, use a path like this: \\myserver\users\\mydb.mdb, instead of this: d:\myserver\users\mydb.mdb for your data source. Otherwise, you may experience connection errors.
- **PMON –** The GE diagnostic utility PMON.exe does not work when iFIX is running as a service in versions of Windows after XP.

Additionally, be aware of the following differences when working with iFIX in Microsoft Windows:

- **Security –** Microsoft Windows includes many new security enhancements in the newer operating systems. Due to these enhancements, there may be changes you need to make for the users who run iFIX. For more information, refer to the Windows and Security section.
- **Drive Mapping –** Security and data protection enhancements may require you to use data sources with UNC pathing, as opposed to mapped network drives. For more information, refer to the Windows and Mapped Network Drives section.
- **Sleep Mode –** Be aware that an iFIX View node running on a version of Windows will lose its connection to the iFIX network when going into "Sleep" mode.

Windows and Security

Running iFIX

As a built-in Windows administrator, you have the rights you need to operate an iFIX SCADA node (start and stop iFIX).

To allow a non-administrator (standard user) to operate an iFIX SCADA node **without access control**, you need to add the "Create Global Objects" policy to the individual user or group to provide access. For Domain users, the Domain user account needs to be added to this policy on the local computer also.

If you enable **access control**, you need to make sure that all iFIX users are part of the iFIX secure group (the secure group was specified during install or with the ConfigureWizard.exe).

NOTE: When installing iFIX with access controls, the Windows Group name used from the domain or computer name provided (IFIXUSERS for example) must be different than any local group name configured on the machine with iFIX installed.

IMPORTANT: WorkSpace and other iFIX applications may become unstable when running with access controls in a Domain environment if the connection to the Active Directory server is lost.

Running iFIX as a Service

If iFIX was installed **with access control,** to run iFIX as a service, make sure the user is part of the secure group specified during install (by default, this is the IFIXUSERS group). If you are not sure what this group is, run the ConfigureWizard.exe tool which is found in the iFIX install folder (by default: C:\Program Files (x86)\Proficy\iFIX) to identify it.

If installed **without access control**, to allow a user to run iFIX as a service, you need to run the GrantUserFixServiceRights utility from the command line to grant access to the service for this user. You also need to add the "Create Global Objects" policy to the individual user or group, unless they are a member of the Administrators group.

For more information on access controls, see "Access Controls in iFIX" on page 23.

To add the Create Global Objects policy to a user:

1. Log in as an Administrator.
2. Click the Start button, and in the Search box, type secpol.msc and press Enter. The Local Security Policy window appears.
3. In the tree, double-click Security Settings, and then Local Policies, to view the contents of the Local Policies folder.
4. Click the User Rights Assignment item to view the policies.
5. Double-click the Create Global Objects policy. The Create Global Object Properties dialog box appears.
6. Click Add User or Group. The Select Users or Groups dialog box appears.
7. Enter an individual user name, or group name, such as "iFIXUsers."
8. Click OK to add the user.

To run the GrantUserFixServiceRights command for a user or group:

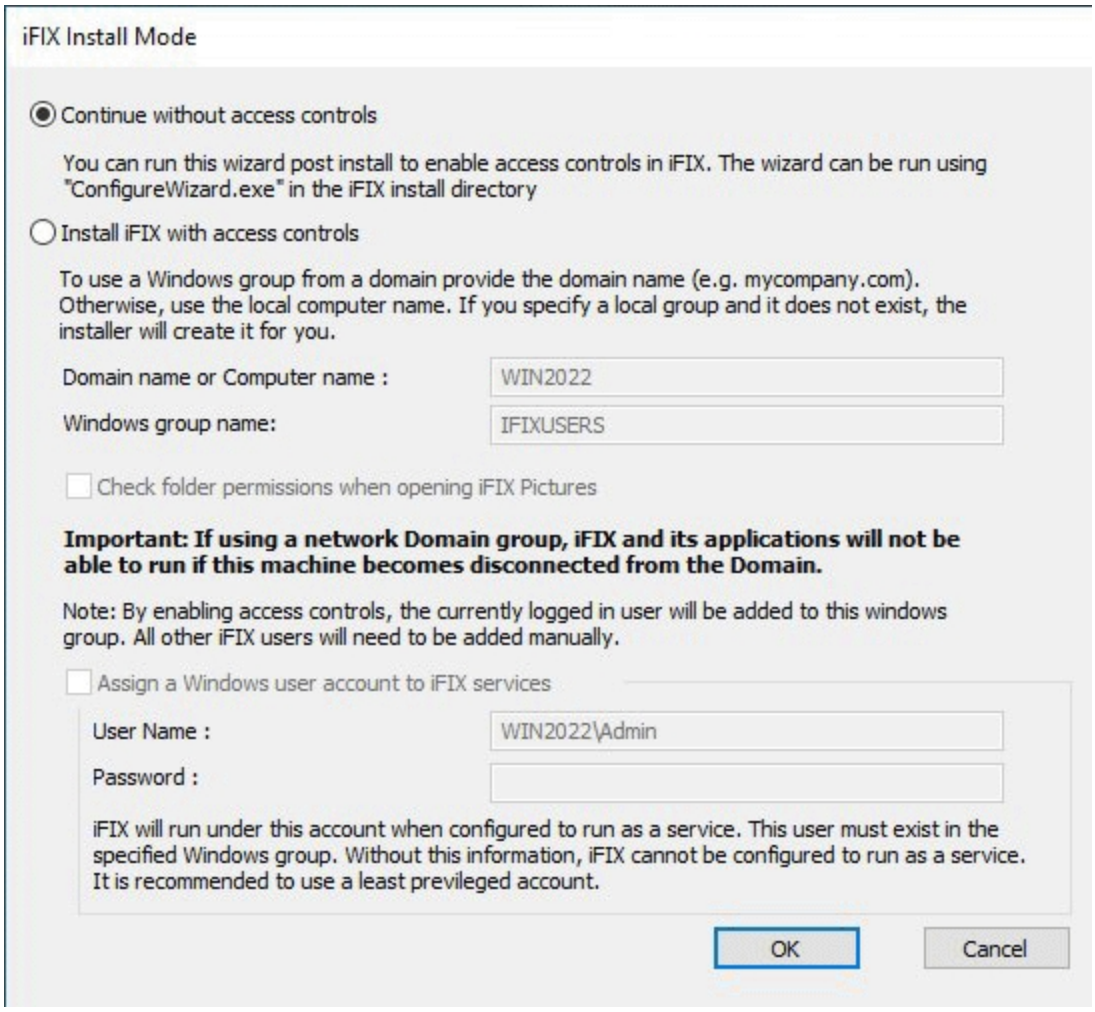
1. Log in as an Administrator.
2. Click the Start button, and in the Search box, type Command Prompt and press Enter. If the Command Prompt does not appear immediately, double-click the Command Prompt from the list of results.
3. In the Command Prompt window, type:

   GrantUserFixServiceRights GRANT FIX *USERNAME*

where *FIX* is the name of the service (iFIX) that you want to grant rights to, and *USERNAME* is the name of the user or group that you want to grant rights to.

To provide privileges to a Windows user with the ConfigureWizard.exe when access controls (secure mode) are enabled:

1. Log in as an iFIX Administrator.
2. Locate and run configure wizard (ConfigureWizard.exe) in the iFIX install folder. By default this path is: C:\Program Files (x86)\Proficy\iFIX\ConfigureWizard.exe. The Install Mode wizard appears.



3. Select the "Assign a Windows User Account to iFIX services" option.
4. Enter a user name. If on a domain, enter the fully qualified domain name along with the user account. For example, the previous illustration specified W2022\USER1 as the user account.

   NOTE: When installing iFIX with access controls, the Windows Group name used from the domain or computer name provided (**IFIXUSERS** in the previous illustration) must be different than any local group name configured on the machine with iFIX installed.
5. Enter the password for this account.

6. Click OK.
7. Restart your computer.
8. Start iFIX
9. Configure the service option in the SCU, if you have not already done so. (From the SCU and select Configure > Local Startup and the select Set iFIX as a Service option, and (if applicable) the Set Service Type to Automatic option. See the "" on page 25 topic for details.)

Running iFIX as a Service with Other Services

If you plan to run iFIX as a service along with other services such as the iFIX scheduler, the OPC A&E Server, and the OPC DA Server, make sure that your user has the rights to start/stop/pause all of those services. A user who is a member of the Administrators group usually has all these privileges. (This can be verified by opening the Windows service control panel and checking if the Start/Stop setting is enabled.) To grant a user who is a standard user rights to start/stop/pause these services, log in to Windows as an Administrator and run the following commands:

```
GrantUserFixServiceRights GRANT IFIXSCHEDULER username
GrantUserFixServiceRights GRANT IFIXOPCAESRV username
GrantUserFixServiceRights GRANT IFIXOPCDA username
```

Examples: Using GrantUserFixServiceRights

If you want to allow a user named QA1 to run iFIX as a service, type:

```
GrantUserFixServiceRights GRANT FIX QA1
```

If you want to allow all members of the group “iFIXUsers” to run iFIX as a service, type:

```
GrantUserFixServiceRights GRANT FIX "iFIXUsers"
```

If you later need to revoke the right to run iFIX as a service, use the following command:

```
GrantUserFixServiceRights REVOKE FIX USERNAME
```

where *FIX* is the name of the service that you want to revoke rights from, and *USERNAME* is the name of the user or group that you want to revoke rights from.

Windows and Mapped Network Drives

In newer versions of Windows, when you elevate an application and it runs under a different context, the application may or may not be related to the user who is logged in. As a result, drive mappings are not available in an elevated session unless you specifically map them while it is elevated.

To resolve this issue, make sure that your system data sources use UNC pathing, rather than mapped network drives. For example, use a path like this: \\myserver\users\\mydb.mdb, instead of this: d:\myserver\users\mydb.mdb for your data source. Otherwise, you may experience connection errors. Be sure to select the "Remember my password" check box in the Connection dialog box when setting up your UNC pathing. By doing this, the next time you log in, your connection will succeed without failing.

For example, you add a system data source (ODBC) with a mapped network drive for use with VisiconX. When you configure a VisiconX data control and select a data source on the Database tab, an error appears (error number -2147467259 indicates that you do have a valid path). To resolve this issue, configure your data source with UNC pathing instead.

EDA Applications and Windows

When running an iFIX Easy Database Access (EDA) application on newer versions of Windows, you may experience errors due to inadequate permissions. For instance, the logged in user may not have enough permissions to create the necessary global memory that the application requires, or the user may not be running an application with the fullest permissions (running elevated).

The "Allocation of Shareable Memory Failed" message is one of the messages that can appear in this scenario. To resolve these types of issues, elevate the application to the fullest privileges.

To mark an application for elevation using an external manifest:

1. Create a text file named yourappname.exe.manifest, where yourappname is the name of the application you want to elevate.
2. In a text editor such as Notepad, open yourappname.exe.manifest.
3. Paste the following lines of code into the text file:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
  <assemblyIdentity version="1.0.0.0"
     processorArchitecture="X86"
     name="yourappname"
     type="win32"/>
  <description>Description of your application</description>
  <!-- Identify the application security requirements. -->
  <trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">
    <security>
      <requestedPrivileges>
        <requestedExecutionLevel
          level="highestAvailable"
          uiAccess="false"/>
       </requestedPrivileges>
      </security>
  </trustInfo>
</assembly>
```

4. Save the file in the same folder as the yourappname.exe, where yourappname is the name of the application you want to elevate.

   TIP: If yourappname.exe was built with an internal manifest, yourappname.exe will ignore the external manifest created in the above manner. Instead, you need rebuild the application with the new elevation information.

   IMPORTANT: If you have run the executable before performing the above steps and it failed to work, see this link for information on adding a manifest after the fact: http://blogs.msdn.com/vistacompatteam/archive/2006/11/13/manifest-and-the-fusion-cache.aspx.

To mark an application for elevation with an internal manifest:

- Build your application's executable (.exe) file with the elevation information built into it. Be aware of issues with fusion cache when you use an external manifest file. For more information, refer to the MSDN web site: http://blogs.msdn.com/vistacompatteam/archive/2006/11/13/manifest-and-the-fusion-cache.aspx.

  For more information on User Account Control (UAC), refer to the Microsoft web site: https://-docs.microsoft.com/en-us/windows/desktop/uxguide/winenv-uac

To elevate a third party application that you do not own the source code for:

Microsoft recommends writing a wrapper to invoke the application's executable (.exe) file in an elevated manner. If this is not feasible, the following is suggested:

- Create a shortcut (.lnk) to the yourappname.exe, where yourappname is the name of the application you want to elevate.
- Right-click the shortcut and select Properties. Configure the shortcut to run as an Administrator.

Deployment Considerations for Running iFIX on a Virtual Machine

As part of our development testing and qualification, we make extensive use of virtualized environments. GE Digital products do not target any specific hardware or virtualized platform. GE Digital will support the functional operation of the product that is running on a supported operating system in a virtualized environment and will address any functional issues related to the software.

Each virtual machine (VM) instance that uses our software is required to have a valid license. Licensing in a virtualized environment will depend on access to a hardware key or a license server, depending on the selected license type.

GE Digital cannot guarantee performance of its software in a virtualized environment due to the wide range of parameters associated to the hardware, configuration, memory settings, third-party software, and the number of virtual sessions running on the same hardware, all of which can affect performance.

It is the responsibility of you, the customer, to ensure that the performance of the GE HMI/SCADA software and application are adequate to meet the needs of your runtime environment. GE does not support issues related to functionality that is not available as a result of running in a virtual machine. Examples include the functionality of card level drivers such as Genius, RMX, SA85 and functions requiring direct video access, or functionality of other software running in the same environment. It is your responsibility to check with the vendor of those applications for their ability to run in a virtualized environment.

Virtual Machine Guidelines for iFIX

The following are the recommended VM settings.

NOTE: GE Digital cannot guarantee software performance in a virtualized environment due to the wide range of parameters associated with the hardware, configuration, memory settings, third-party software, and number of virtual sessions running on the same hardware, all of which can affect performance.

Setting	SCADA Server	iClient
Processors/CPUs	Intel® Core™ i5 3.0 GHz or equivalent	Intel® Core™ i5 3.0 GHz or equivalent
RAM	8 GB	4 GB
Hard disk/disk space	40 GB **NOTE:** iFIX alarm and historical data files grow dynamically. If you plan to perform extensive alarm or data collection on a node, you may need more disk space on that particular node. It is strongly recommended there be additional free space on the hard drive to avoid performance issues.	20 GB

For additional information on iFIX System Requirements, please see System Requirements for iFIX in the IPI.

Troubleshooting VM Setups for iFIX

To help with virtual machine (VM) troubleshooting, be prepared to provide the following VM settings to GE Digital support staff:

- CPU resources assigned
- Memory resources assigned
- Disk size and configuration
- Current disk space utilized on the VM

The above should be checked against recommended specifications for the product. If the current disk space utilized on the VM is approaching 90%, consider increasing the amount of available disk space.

After verifying that the VM is properly configured, check the performance of the VM. To do this select (using VMWare for example): **VM** > **Monitor Tab** > **Performance** > **Overview** and examine the resulting graphs.

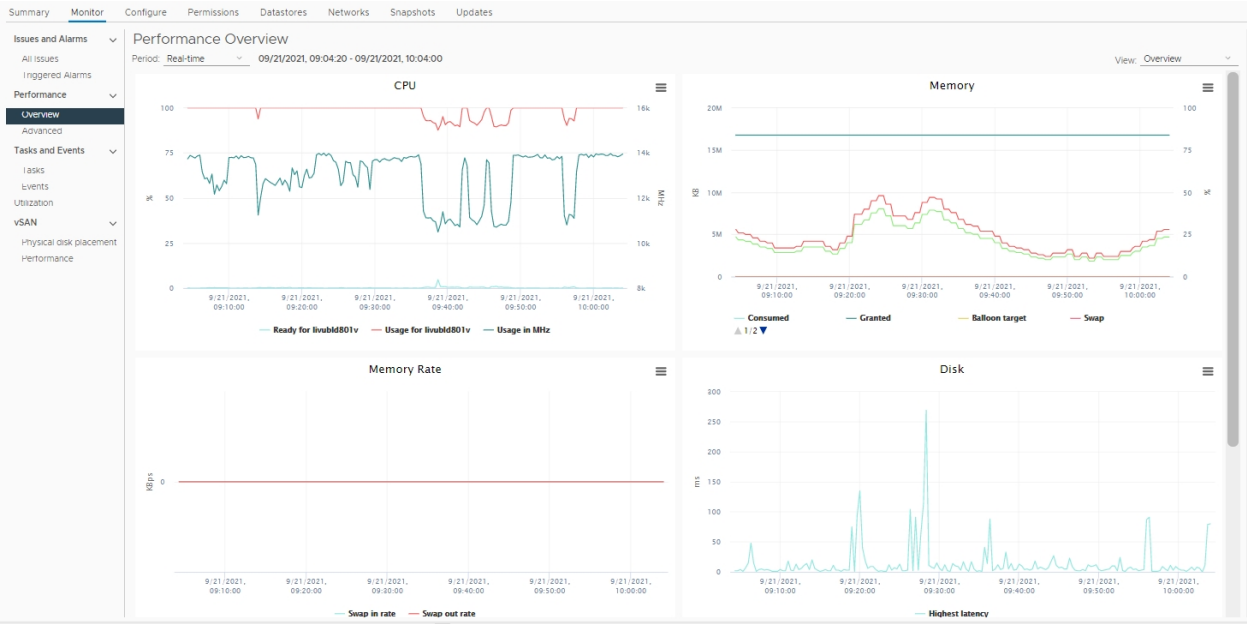


Figure 1: VM Performance Overview Graph (from VMWare)

Pay particular attention to:

- CPU usage (red line in the example) being consistently at 100%. This indicates that the VM may be undersized for the workload or that another process is consuming resources.
- Memory usage (green line) being at 100%.
- Disk highest latency (teal line) being very high for long durations. “Very high” will depend on your infrastructure and may require your infrastructure team to verify.

The final step in checking performance is to check the “CPU Ready Time” by selecting (using VMWare for example): **VM** > **Monitor Tab** > **Performance** > **Advanced** > **Select View “CPU Ready”**. This is a measurement of how long the VM must wait before it can execute the work it needs to. High CPU Ready time, when compared to other VMs on the same host, would suggest the host is overloaded. There is no “cutoff” value for poor performance, but it can be used to baseline against a known good system.

Below is an example of CPU ready where there is a spike in CPU ready, but it is not consistently high.

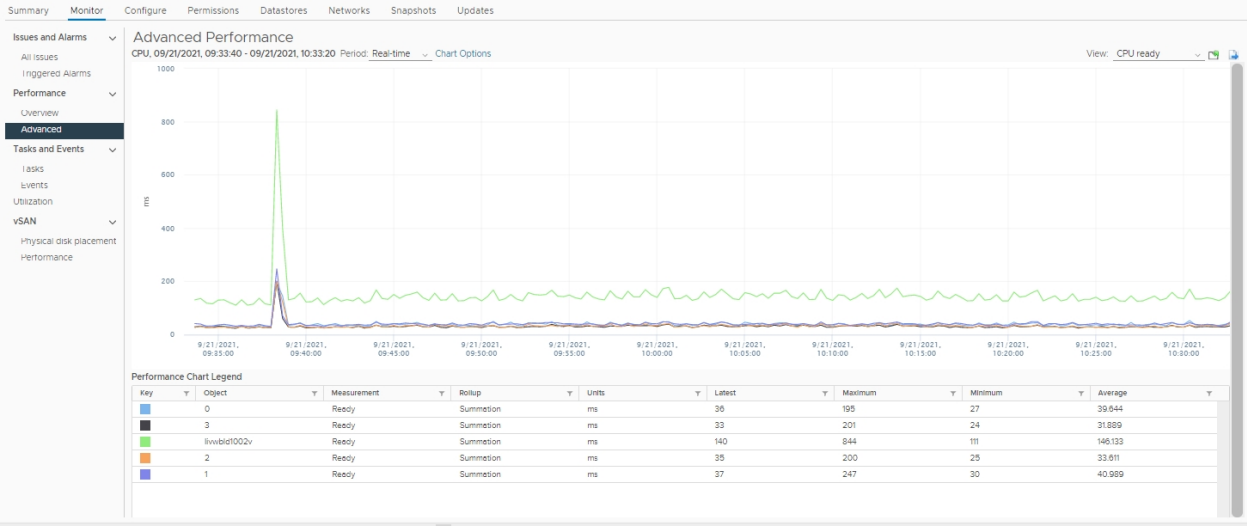


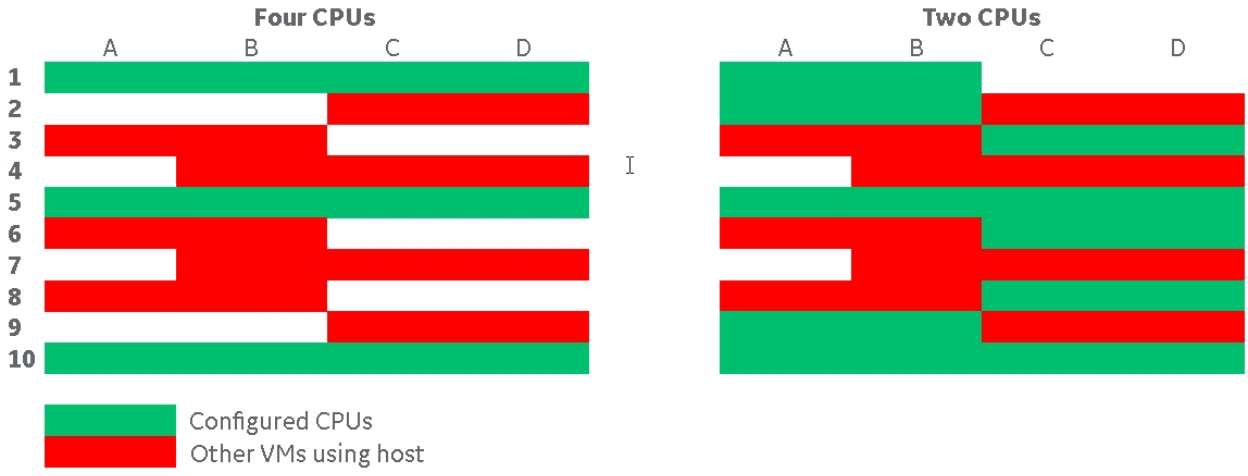
Figure 2: CPU Ready with intermittent spike

VM Processor Scheduling for iFIX

Using VMWare as the example, the virtualization layer schedules the virtual processors in the image against physical processors. All processors need to run at the same time.

For example, if four processors are required (based on the setting) and there are only two available, it will wait until four are available.

As illustrated below, a VM requiring four CPUs would get only three time slices (shown in green) on the CPUs. The VM requiring two CPUs would get eight time slices. This shows how configuring fewer CPUs (e.g., two) can be more efficient than having more CPUs (e.g., four).



Enhancing VMWare Performance with iFIX

Additional considerations when investigating your virtual environment.

• **Shares:** VMware has the concept of “shares” to help prioritize workloads. For occasional use, these can be helpful to make sure a workload runs correctly, however these should not be used, as running everything

with high priority makes them all equal. The same applies if you have a large number of VMs with high shares and a VM is normal; it will be last to be scheduled, which could impact performance.

• **Reservation:** VMware can “reserve” CPU time for a VM. As with “shares”, a VM could be slow if too many other VMs have shares on the same host as the VM with the product on it.

• **CPU Limits:** VMware can limit the amount of CPU time for a VM. If a limit is set, it could mean the VM needs more resources, but cannot get them.

• **Compatibility:** Ensure your virtualization software is up to date on all systems. Images with different compatibility may behave differently on other host systems (depending on the VM application installed on that host).

Other iFIX Installation Considerations

This chapter provides information you need to consider when using databases or drivers and iFIX. This information includes:

- Supported Drivers
- Special Keyboard Buttons

Supported Drivers

Be certain that before you purchase an I/O driver, that the driver is compatible with the hardware and operating system that you intend to run it on. For example, if the driver is not supported on a specific operating system, then you cannot use that driver with iFIX running on that operating system. For more information on iFIX supported drivers and their respective operating systems, refer to the GE Digital support web site at:

https://digitalsupport.ge.com

Special Keyboard Buttons

Some computer keyboards have special buttons for e-mail launch, internet launch, search, and other functions. These keyboard buttons may disable certain key macros or allow users to circumvent iFIX security measures.

It is recommended that you reprogram or disable the software that operates such special buttons. Refer to your computer's documentation for instructions on disabling these buttons.

Environment Protection and iFIX

Environment Protection is a feature within iFIX that allows you to restrict operator access in run mode. This feature helps to provide a secure operating environment. For instance, while in run mode, you may want to restrict an operator from:

- Starting other applications.
- Switching to other applications.
- Exiting from the WorkSpace.
- Restarting the computer using Ctrl+Alt+Del.
- Opening unauthorized pictures.
- Closing the current picture.
- Using the WorkSpace menu.
- Switching to the configuration environment.
- Accessing the system tree.
- Accessing the pull down menus.
- Viewing the title bar.

For more detailed information about Environment Protection, refer to the Configuring Security Features e-book. The Restricting Access in the Run-time Environment topic in the Defining and Assigning Security Privileges chapter, in particular, has detailed information with links to more steps.

Important Information

Be aware that when using Environment Protection:

- Environment Protection is NOT supported with the My-T-Soft® virtual keyboard.
- Environment Protection is NOT supported with remote desktop applications such as those using Remote Desktop Protocol (RDP), Virtual Network Computing (VNC), and WebEx™.

Important Task Switching Information

Task switching is disabled when security is enabled and either the logged-in user does not have task switching rights or there is no user logged-in. The task switching right can be assigned by adding the Enable Task Switching application feature to the user profile in the iFIX Security Configuration application.

Working with Touch Screens

Be aware that:

- When iFIX is configured to run as a service and to start automatically, Fix.exe should always be started before launching WorkSpace.exe to enable the on-screen keyboard functionality. If WorkSpace.exe is launched without starting iFIX in the user session on a system without a physical keyboard, the on-screen keyboard will not automatically display when the cursor is in an edit control or in edit mode.

- For Microsoft Windows 8.1 and Windows Server 2012 R2, the only supported on-screen keyboard for use with iFIX and touch screens is the tabtip keyboard (tabtip.exe).
- To launch the keyboard automatically from iFIX on Windows Server 2012 R2 systems, there is additional configuration. In the Server Manager, you must install the Desktop Experience feature included in the User Interface and Infrastructure features. (By default, this feature is already enabled in Windows 8.1). After enabling the feature and restarting Windows, the on-screen keyboard, tiptap.exe, will be available and will display automatically when focus is on an edit field in iFIX.
- To automatically display the on-screen keyboard when the focus is set to WorkSpace objects that have the ability to accept user inputs, enable PROFICYENABLEFOCUSTRACKING.EXE by adding the following lines to your FIX.INI file (located in the LOCAL folder) in the [OTHERS] section:

```
[OTHERS]
[SESSION INSTANCE]
INSTANCE0=%PROFICYENABLEFOCUSTRACKING.EXE
```

NOTE: If these lines are present in the FIX.INI, but are preceded by a semi-colon, remove the semi-colon to enable the lines.

Networking

This chapter provides general information about the iFIX supported network protocol, supported network software, supported file servers, and installing network cards with Windows. Refer to the following sections for more information:

- Supported Networking Protocol
- Supported File Servers

Supported Networking Protocol

If you decide to implement a networked iFIX system, make sure that all nodes are using compatible network configurations. iFIX supports TCP/IP interfaces for peer-to-peer communication. NetBIOS is no longer supported.

If you have difficulty networking your computer, refer to the Troubleshooting chapter of the Setting Up the Environment manual to pinpoint and resolve your problems.

Supported File Servers

GE supports using a file server to store System Configuration Utility, alarm area database, security, historical, and recipe data files and file server-based iClients. iFIX does not require a file server.

Refer to your file server documentation for installation and configuration instructions.

If a file server becomes unavailable and an iFIX node attempts to access a file, you may experience no response, slow response, or time-outs. These conditions are a result of continuously polling all available drives while it waits for a response from the file server. It is recommended that you store a backup copy of the files you need on the local node. It is not recommended that you use the file server for files if it is susceptible to failure.

Index

S

T

U

V

W