Proficy* HMI/SCADA - iFIX

SETTING UP THE ENVIRONMENT

Version 5.5

January 2012

Disclaimer of Warranties and Liability

The information contained in this manual is believed to be accurate and reliable. However, GE Intelligent Platforms, Inc. assumes no responsibilities for any errors, omissions or inaccuracies whatsoever. Without limiting the foregoing, GE Intelligent Platforms, Inc. disclaims any and all warranties, expressed or implied, including the warranty of merchantability and fitness for a particular purpose, with respect to the information contained in this manual and the equipment or software described herein. The entire risk as to the quality and performance of such information, equipment and software, is upon the buyer or user. GE Intelligent Platforms, Inc. shall not be liable for any damages, including special or consequential damages, arising out of the user of such information, equipment and software, even if GE Intelligent Platforms, Inc. has been advised in advance of the possibility of such damages. The user of the information contained in the manual and the software described herein is subject to the GE Intelligent Platforms, Inc. standard license agreement, which must be executed by the buyer or user before the use of such information, equipment or software.

Notice

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

All other brands or names are property of their respective holders.

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

doc@ge.com

Table of Contents

Setting Up the Environment

Setting Up the Environment

About This Guide

Setting up the Environment is intended for system integrators, OEMs, and process control engineers responsible for setting up an iFIX® server or configuring their process environment. This manual assumes familiarity with Microsoft Windows and your network environment.

Reference Documents

For related information on the System Configuration Utility (SCU), refer to the following manuals:

- Implementing Alarms and Messages
- Configuring Security Features
- Building a SCADA System
- Mastering iFIX

Introduction

As you begin setting up your iFIX® environment, you have the following main tasks to complete:

- Setting up each node's hardware and operating system.

- Setting up the network you want to use.

- Configuring iFIX.

When setting up a node, you should be familiar with your hardware and Microsoft Windows operating system. If you are not, make sure you have all relevant documentation nearby for reference. Should you need to purchase one or more computers for use with iFIX, refer to the Getting Started chapter. A list of iFIX requirements and recommended computers is available in the Getting Started with iFIX guide.

After setting up each node's hardware and operating system, configure the network for each computer if you plan to set up a distributed processing system. Typically, this requires you to install a network interface card (also called a network adapter) and network software on each computer. Choosing these items carefully is important to the success of your total system.

Once your nodes are connected and communicating on the network, you are ready to configure iFIX. Your main tool for accomplishing this is the System Configuration Utility (SCU). With this utility, you can specify what functions your local server performs, including:

- Where to find files.

- Where to establish security provisions.

- Which nodes to establish network connections with.

- Where to send alarm and operator messages.

- Which SCADA options to use.

- Which I/O drivers to load.

- Which database to load.

- Which programs to execute.

SCU Overview

iFIX needs two things to successfully start up:

- An SCU file.

- Local startup options.

When you start iFIX, it looks for a file that tells it how to configure the local server. This file, known as the SCU file, contains specific information about programs and options unique to that particular server.

When you start the SCU, it automatically opens the SCU file specified by the local startup options.

iFIX only reads this file during startup. Any subsequent changes you make to the SCU file while iFIX is running do not take effect until you save it and restart iFIX.

For more information on the SCU file, refer to the SCU File Operations section. For more on local startup options, refer to the Configuring Local Startup Options section.

Getting Started

Before you start setting up your iFIX environment, complete the following tasks:

- Identify the computers that will function as your View clients, SCADA servers, and development workstations.

- Identify which nodes will be networked, if any.

- Decide if you want to use a file server to share alarm area databases, or SCU, security, historical, or recipe files.

- Identify the computer that will function as the file server if you decide to use one.

- Make sure that you have a Windows user account that is a member of either the Administrators group or the standard Users group. For Windows XP and Windows 2003, you must use the Power Users or the Administrators group.

  Refer to the Using Terminal Server manual for more information on using Terminal Server clients with different user accounts.

More Information

For more information on how to get started with iFIX, refer to these sections in the Getting Started with iFIX guide:

- Hardware Requirements

- Recommended Computers

- Memory Requirements

- Software Requirements

- Supported Regional Settings

- Video Drivers

- Supported Networking Protocol

- Supported File Servers

- Optional Hardware

- Online Registration

- Set-up Overview

- The Hardware Key

Networking iFIX Nodes

This chapter describes how to set up network hardware and driver software for Ethernet adapters. The chapter also describes how to set up TCP/IP protocols for iFIX nodes. For more information, refer to the following topics:

- Working with TCP/IP

- Notes on Networking with Other iFIX and FIX Nodes

In general, you can accomplish these tasks as follows:

1. Select the TCP/IP network protocol.
2. Enable TCP/IP for each computer in the network. iFIX allows up to 200 Client connections (outbound and inbound).

When you finish, make sure each computer can communicate with your network before proceeding. If it cannot, refer to the chapter Troubleshooting to resolve any difficulties you experience.

Working with TCP/IP

iFIX uses TCP/IP to provide connectivity for your nodes. Microsoft's TCP/IP is built into the operating system. For more information on using TCP/IP with iFIX, refer to the following sections:

- Before You Begin With TCP/IP

- Configuring TCP/IP

Before You Begin With TCP/IP

To use TCP/IP, make sure you have the following components:

- Microsoft Windows installation disks or CD-ROM and documentation.

- Network adapter, drivers, and cabling.

For detailed information, refer to the online Help that came with your Microsoft Windows operating system.

In addition to the components you need to get started, you need do the following:

- Map the names of each SCADA server IP addresses.

- Verify the communication ports that FIX will use.

- Configure TCP/IP.

- Enable the TCP/IP protocol in the SCU.

The following sections provide guidelines for completing these tasks. Refer to your TCP/IP manuals for additional configuration information.

Mapping IP Addresses

To use a TCP/IP network with iFIX, each SCADA server must be mapped to unique IP addresses. This process is called *name resolution*, and TCP/IP vendors handle this in many different ways. You need to decide which method of name resolution is appropriate for your site. This section provides guidelines to help you reach that decision.

TCP/IP software can handle name resolution using the following:

- A local HOSTS file.

- DNS (Domain Name System).

- DHCP/WINS (Dynamic Host Configuration Protocol and Windows Internet Naming Service).

It is recommended that you use a local HOSTS file since this method has provided the highest reliability during our testing. More information on using a local HOSTS file is included in the section Using a Local HOSTS File.

If your company currently uses DNS servers, this option can be implemented since DNS servers are based on HOSTS files.

Using a Local HOSTS File

The HOSTS file provides mapping between node names and IP addresses. This text file is stored locally on each node. The contents of the HOSTS file should be identical on each node in your TCP/IP network. All FIX SCADA servers must be in the HOSTS file.

NOTE: In Windows Vista or Windows Server 2008, you cannot save the HOSTS file unless you are an Administrator (in the built-in Administrator user group).

The syntax of the HOSTS file is as follows:

```
address       HOSTNAME
```

Address — defines the IP address of the node.

Hostname — defines the iFIX node name, as specified in the SCU. The node name must be in uppercase and is limited to eight characters.

An example of an entry in the HOSTS file is as follows:

```
198.212.170.4      SCADA01
```

You can also provide an alias name for the host name as an optional third parameter.

TIP: A common mistake made when creating the Hosts files is leaving an extension at the end on the file name. For example: HOSTS.txt or HOSTS.doc. Do not include a file extension. The name of the file used by the operating system is: HOSTS.

Using DNS Servers

A DNS server is a HOSTS file stored on a server. This configuration is easier to administer than local

HOSTS files since any changes to the HOSTS file need to be made only once. However, a single DNS server can be a single point of failure should it fail to respond. If avoiding a single point of failure is important to you, consider doing one of the following:

- Reverting back to local HOSTS files.

- Implementing redundant DNS servers.

Using DHCP/WINS

When using iFIX with DHCP, you also need to use WINS. The local host name must be the same as the iFIX node name. Refer to your Microsoft documentation for more information on setting up DHCP and WINS.

Verifying Port Assignments

By default, iFIX uses the following port:

```
FIX2010/tcp
```

You should not have to change this setting. If the number is used by another application on your node, you must edit or create a SERVICES file. The SERVICES file defines the port used by each TCP/IP application.

To define unique port numbers for iFIX, refer to your TCP/IP manuals for instructions on locating and editing the SERVICES file. Make sure, when you edit the file, you enter a unique port number for iFIX or change the port number of the conflicting application.

NOTE: The port used for iFIX Database Synchronization is port 53014.

Configuring TCP/IP

You can configure TCP/IP with the Windows Network control panel. Microsoft recommends that you use the Network control panel for all network configuration tasks rather than manually editing the registry.

NOTE: Have the Microsoft Windows disks or CD-ROM available. You may need them to configure TCP/IP.

▶ **To configure TCP/IP for Windows XP:**

1. In the Control Panel, open Windows XP Network Connections.

2. Right-click the Local Area Connection icon and select Properties. The Local Area Connection Properties dialog box appears.

3. From the General tab, verify that all the components for TCP/IP are installed: TCP/IP Protocol and a network adapter driver required for the network adapter hardware.

4. Consult your Windows XP documentation for information about installing missing components.

▶ **To configure TCP/IP for Windows Server 2003:**

1. In the Control Panel, open Windows Server 2003 Network Connections.

2. Right-click the Local Area Connection icon and select Properties. The Local Area Connection Properties dialog box appears.

3. From the General tab, verify that all the components for TCP/IP are installed: TCP/IP Protocol and a network adapter driver required for the network adapter hardware.

4. Consult your Windows Server 2003 documentation for information about installing missing components.

▶ To configure TCP/IP for Windows Vista:

1. In the Control Panel, open the Windows Vista Network and Sharing Centre.

2. In the Tasks list on the left, click the Manage network connections link.

3. Right-click the Local Area Connection icon and select Properties. The Local Area Connection Properties dialog box appears.

4. From the Networking tab, verify that all the components for TCP/IP are installed: TCP/IP Protocol and a network adapter driver required for the network adapter hardware.

5. Consult your Windows Vista documentation for information about installing missing components.

▶ To configure TCP/IP for Windows Server 2008:

1. In the Control Panel, open the Network and Sharing Centre.

2. In the Tasks list on the left, click the Manage network connections link.

3. Right-click the Local Area Connection icon and select Properties. The Local Area Connection Properties dialog box appears.

4. From the Networking tab, verify that all the components for TCP/IP are installed: TCP/IP Protocol and a network adapter driver required for the network adapter hardware.

5. Consult your Windows Server 2008 documentation for information about installing missing components.

Notes on Networking with Other iFIX and FIX Nodes

iFIX can share data and alarms with previous versions of iFIX, as well as with FIX32 6.15 and FIX 7.0. FIX32 view nodes will only receive alarms from alarm areas A-P.

NOTE: You cannot run iFIX and FIX 6.x or greater at the same time on a single computer.

Getting Started with the SCU

This chapter helps you start configuring iFIX with the System Configuration Utility (SCU). It explains how to start and exit the SCU, complete file operations, and define the iFIX paths for your computer.

- Before You Begin with the SCU
- Starting and Exiting the SCU
- SCU File Operations
- Overview Checklist

Before You Begin with the SCU

The following SCU configuration tips may help you start up and maintain your iFIX environment more efficiently.

- Configure the SCU *before* you start the Proficy iFIX WorkSpace. This way you do not have to exit the WorkSpace and restart iFIX.

- Use the local node alias feature in your computer to save development time later. Refer to the Enabling the Local Node Alias Feature section for more information.

- Run iFIX as a service under Windows to give you more flexibility and security in your process environment. Refer to the Running iFIX as a Service section for more information.

- Store your SCU files remotely on the network so that FIX Startup can access them on a file server. If you are using a file server, it may be useful to store all your SCU files in one place. In Microsoft Windows, you have another option — simply connect a networked drive to a remote server on the local network that contains the desired files or directories. This strategy increases control over configuration files and makes your routine maintenance easier.

Refer to the iFIX Startup chapter for detailed information regarding the startup program in iFIX.

Starting and Exiting the SCU

To properly start and configure the SCU, you should do so before you open the Proficy iFIX WorkSpace. You can start the SCU by clicking Start and pointing to Programs, Proficy HMI SCADA - iFIX, and then System Configuration. However, if you are in the Proficy iFIX WorkSpace and you need to make changes, you can start the SCU by clicking the SCU button on the Application toolbar (Classic view), or on the Applications tab, in the System & Security group, click SCU (Ribbon view), or by double-clicking System Configuration in the system tree. Note that, for its first startup, the SCU uses the node name you specified during installation.

The main SCU window displays graphics and icons that represent enabled options and tools. You can click many parts of the window to bring up the related dialog box. This graphical interface lets you determine at a glance what kind of node and options the open SCU file enables. You can also disable an option by selecting the graphic or icon in the main SCU window and pressing Delete.

NOTE: Deleting an icon from the main SCU window removes that service from your server's configuration. A dialog box appears warning you of this.

Using the SCU Toolbox

The bottom of the SCU window contains a toolbox that includes all the tools you need to use the SCU. These tools are accessed by clicking a button in the toolbox. The table below shows what each button does.

SCU Toolbox Buttons and Their Functions		
Clicking the button...	**Displays the...**	**Which lets you...**
	Path Configuration dialog box.	Specify the location and names of your iFIX directories.
	Alarm Configuration dialog box.	Enable and configure alarm services.
	Network Configuration dialog box.	Configure network connections.
	SCADA Configuration dialog box.	Configure SCADA servers.
	Task Configuration dialog box.	Select tasks to run automatically in various start-up modes.
	Security Configuration window.	Configure security in your process environment.

SCU Toolbox Buttons and Their Functions		
Clicking the button...	**Displays the...**	**Which lets you...**
	SQL Accounts dialog box.	Create a SQL login account and configure the SQL task.
	Edit Alarm Area Database dialog box.	Edit the Alarm Area Database.

To exit the SCU, select Exit from the File menu.

SCU File Operations

The SCU file contains all of the necessary information for iFIX to run as you have specified. You can perform several operations with SCU files, as described in the following sections.

- Opening a New File
- Adding a File Description
- Creating a Report
- Configuring Directory Paths

Opening a New File

When you start the SCU, it automatically opens the SCU file specified by the local startup options. If the SCU cannot find the specified file, it opens a new one. To create a new file while the SCU is open, select New from the File menu. A new SCU main window appears with no link to the process database and no drivers configured.

Adding a File Description

At the top of the SCU window, a short title appears under the menu bar. This is the name of your SCU file, also known as a file description. You can change the name so that each SCU file has a unique identifier. The file description is only there to help you distinguish between SCU files; the system does not use the description in any way.

To name your SCU file, select Description from the File menu, or double-click the title area. Enter a description of up to 40 characters in the Enter Configuration File Description field.

Creating a Report

SCU reports contain network information about your server's configuration, including the system path, and SCADA, alarm, task, and SQL configuration. To create a report of the open SCU file, select Report from the File menu, type a file name in the File name field, and click Save. The SCU notifies you whether it successfully wrote the file. You can view or print the report with any text editor or word processor.

SCU reports have an .RPT file extension and are stored in the directory pointed to by the local path.

Configuring Directory Paths

iFIX uses a number of directories to store program and data files. Use the Path Configuration dialog box to specify the location and names of your iFIX directories. You can display this dialog box by clicking the Path button on the SCU toolbox.

When iFIX is installed it creates a directory, called the Base directory, and all the subdirectories you see listed in the Path Configuration dialog box. If you decide to change the Base path, and the other directories are subdirectories of the Base path, click Change Base to automatically update all the listed directory names. When you change a path the SCU creates the new directory for you. However, it does not copy the files from the old directory to the new directory.

NOTE: When configuring paths for your iFIX components, it may be helpful to place some directories on the local machine and some on a network server. For example, keeping your Local and Database directories on a local path name allows you easy accessibility on your computer, whereas copying the Picture and Historical files to a network server enables anyone on the network to access these files to view a picture, historical data, and so forth.

The table below describes the use of each directory.

Path Descriptions		
The path...	**Is used for storing...**	**Default Path**
Base	All executable files. The Base path points to the main iFIX directory. Other directories are usually subdirectories of the Base directory.	C:\Program Files\Proficy\Proficy iFIX
Language	The language files used to create dialog boxes and help files. If you choose to implement a language other than English, the new language and help files replace the files found in this directory.	C:\Program Files\Proficy\Proficy iFIX\NLS
Local	Configuration files associated with the local computer, including SCU, recipe format, and system security files.	C:\Program Files\Proficy\Proficy iFIX\LOCAL

Path Descriptions		
The path...	**Is used for storing...**	**Default Path**
Project	A grouping of application files, such as pictures, databases, and tag groups, saved in a specific folder identified by the project name. You can manage your application files by naming a different path for each project.	C:\Program Files\Proficy\Proficy iFIX
Database	Process database files, Database Manager configuration files, and I/O driver configuration files.	C:\Program Files\Proficy\Proficy iFIX\PDB
Picture	The pictures of the configuration and run-time environments. *NOTE: If you are using a shared PIC directory on a drive other than the one on which iFIX is installed, you must enter the full path to the PIC directory. For example, if you want to use a shared PIC directory on the G:\ drive, you must enter G:\PIC in the SCU.*	C:\Program Files\Proficy\Proficy iFIX\PIC
Application	Data and configuration files for your iFIX applications. If you create your own applications, use this directory to store data files.	C:\Program Files\Proficy\Proficy iFIX\APP
Historical	Historical Trending configuration files.	C:\Program Files\Proficy\Proficy iFIX\HTR
Historical Data	Historical data files. Historical Trending creates a unique subdirectory to this directory for each node that data is being collected from. The subdirectory uses the name of the node the data comes from.	C:\Program Files\Proficy\Proficy iFIX\HTRDATA

Path Descriptions		
The path...	**Is used for storing...**	**Default Path**
Alarms	Alarm data files and event log. *NOTE: If you want to view an event log (.evt) in Windows Vista or Windows Server 2008, make sure that you associate an editor such as Notepad with the .evt file type so that you can open and read the file. If you do not, when you double-click the .evt file in Windows Vista or Windows Server 2008, an error may appear.*	C:\Program Files\Proficy\Proficy iFIX\ALM
Master Recipe	Master recipe, master recipe error, and master recipe report files.	C:\Program Files\Proficy\Proficy iFIX\RCM
Control Recipe	Control recipe, control recipe error, and control recipe report files.	C:\Program Files\Proficy\Proficy iFIX\RCC
Alarm Areas (AAD)	Primary Alarm Area Database files.	C:\Program Files\Proficy\Proficy iFIX\PDB

Overview Checklist

Following is a list of general tasks for implementing the SCU in iFIX.

▶ **To use the SCU in iFIX:**

1. Start the SCU before you open the Proficy iFIX WorkSpace.

2. Configure your local startup options, including the local server name, local logical name, and the local SCU file name.

3. Configure the path in which to store the program and data files.

4. Make any start-up or configuration changes using the SCU toolbox and associated dialog boxes. Refer to the appropriate chapters in this manual for more information.

5. Save any configuration changes to either a local disk or a remote file server.

Configuring iFIX Using the SCU

This chapter describes how to configure iFIX with the System Configuration Utility (SCU). This includes:

- Configuring Local Startup Options
- Configuring Security
- Configuring Network Connections
- Configuring Network Security
- Configuring Alarms
- Configuring SCADA Servers
- Configuring Startup Tasks
- Configuring iFIX for Relational Databases

Configuring Local Startup Options

Local startup options allow you to define configuration options that apply only to your server. If you try to exit the SCU without specifying local startup options, the SCU warns you that iFIX will not be able to properly configure your server. Local startup options allow you to specify:

- The local server name.
- The local logical name.
- The local SCU file name.
- Whether the local server runs as a service under Windows.
- Whether the local server uses the local node alias feature.

Specifying the Local Server, Local Logical, and SCU File Name

Before you start iFIX, you need to specify the local server name, local logical name, and local SCU file name in your Windows Registry. (The Windows Registry is a database that your operating system uses to store application information.) We strongly recommend that you use the SCU to write changes to the registry for you instead of editing the registry directly.

Logical node names are used to group partner SCADA servers (primary and secondary) to form a logical pair. This ensures that you can establish SCADA server failover in your SCADA network. For more information on configuring SCADA server failover using the SCU, refer to the Enhanced Failover electronic book.

To choose local node, local logical, and configuration file names, select Local Startup from the Configure menu and enter the names in the appropriate fields of the Local Startup Definition dialog box. The SCU stores all SCU files created on the local server in the directory defined by the local path, unless you specify otherwise when saving the file.

NOTE: If you enable security and set the security path to a folder other than the default, which is the C:\Program Files\Proficy\Proficy iFIX\Local folder, when you change the node name, security is disabled. You will need to configure iFIX security again and enable it.

Running iFIX as a Service

You can run iFIX as a service under Windows. When enabled, this option allows you to close any foreground task and log out of Windows without shutting down core iFIX tasks like networking, SAC processing, alarming, and I/O driver control. This provides a much higher level of security to your process, because operators can log in and log out of a Windows server before and after their shift without affecting the process.

To configure iFIX to run as a service, shut down iFIX, log in as an Administrator, and select the Continue Running After Logoff check box in the Local Startup Definition dialog box in the SCU. Be aware that if iFIX is running, this check box is unavailable.

After iFIX is configured to run as a service, the applications that you start in the Task Configuration dialog box also start as services. For more information, refer to the Configuring Startup Tasks section.

When you run iFIX as a service, you should be aware of the following:

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.

Disabling iFIX as a Service

After disabling the Continue Running After Logoff option in the Local Startup Definition dialog box in the SCU, you must restart iFIX.

Running iFIX with Terminal Server

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 the 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 on Proficy HMI/SCADA iFIX server, then 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.

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.

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.

Using with Environment Protection

If you plan to use environment protection when iFIX is running as a service, be sure to add TSFE.EXE to your Windows Startup program group. TSFE.exe is an iFIX application (located in your iFIX install folder) that enables task switching and keyboard filtering when a new user logs into Windows. By adding TFSE.exe to your startup group, you are ensuring that users can log into Windows with environment protection enabled and then operate iFIX in an appropriate, secured environment.

Enabling the Local Node Alias Feature

The Local Node Alias feature allows you to substitute a placeholder, THISNODE, for the node portion of a data source in order to automatically access information from the local SCADA server. This is ideal for developing pictures that can be shared among several computers that each access different SCADA servers. To use the Local Node Alias feature, you must first enable it in the Local Startup Definition dialog box.

Configuring Security

You can configure security using the Security Configuration program, which can be accessed from the SCU by clicking the Security button on the SCU toolbox.

Before starting the Security Configuration program, make sure that iFIX is running and, if security is enabled, that you have the proper account privileges.

The Configuring Security Features manual fully describes the security program.

Configuring Network Connections

You can enable network communications between any two iFIX servers by configuring each computer's network connections. To define these connections, click the Network button on the SCU toolbox.

You can use the Network Configuration dialog box to configure network protocols, configure network communications, establish dynamic connections. Refer to the following subsections for information on all of these functions.

- Configuring Protocols
- Configuring Remote Nodes
- Configuring LAN Redundancy
- Configuring Network Timers

Configuring Protocols

iFIX allows you to establish communications with the TCP/IP protocols. Enabling the TCP/IP protocol in the SCU, allows you to use that protocol for your iFIX network.

Configuring Remote Nodes

iFIX allows you to configure primary and secondary nodes for SCADA server failover. By entering a primary and secondary node in the Network Configuration dialog box, you ensure connection with that node should communication with the primary node fail. The following sections describe how you can enable, configure, and modify remote nodes in your network environment.

For more information on implementing SCADA server failover in your environment, refer to the Enhanced Failover electronic book.

Enabling Secondary SCADA Nodes

You must first add a remote node to your configuration before you can enable SCADA server failover in your network.

You can view or make changes to the configured remote nodes in the Remote Nodes area of the dialog box. To view the primary and secondary nodes currently configured, select the Show All Names check box.

Using Network Timers on a Per-node Basis

The Remote Node Configuration dialog box allows you to modify network timer values on a per-node basis.

Refer to the Advanced Topics chapter for more information on configuring network timers, including what each time-out value represents.

Dynamic Connections

Dynamic connections allow iFIX to make a network connection when it needs to retrieve data from a server. For example, if a picture references a remote server, and the remote server has not been configured in the SCU, iFIX automatically makes a dynamic connection to that server when you open the picture. The servers will remain connected, even if you close the picture or exit the run-time environment. In fact, with Dynamic Connections enabled, you do not have to enter node names in the Configured Remote Nodes list at all.

When iFIX first opens a picture that requires a dynamic connection, it may take a slightly longer time resolving the connection. This delay depends on the amount of network connections required for the specific picture and if these servers are available for a connection.

The Dynamic Connections option is disabled by default, and affects all connections from the node. All dynamic connections will inherit the network timer settings defined within the SCU. If you choose to enable dynamic connections, iFIX may attempt to establish a connection when calling the System.FindObject method in a script. This happens when a name or an object is referenced in a script but is not currently loaded. For example, consider the following script:

```
Dim shape as Object

Set shape = System.FindObject("badname.rect1")
```

badname is the name of a picture that is not currently loaded. In this script, iFIX attempts to establish this connection with *badname*. When the connection fails, the following error occurs:

```
Object not found
```

NOTE: With Dynamic Connections enabled, a new node will not receive alarms from a SCADA server until a connection is established. If you want a remote node to receive alarms from a SCADA server immediately after starting up, you should add the SCADA server name to the Configured Remote Nodes list of the View client.

Configuring LAN Redundancy

You can configure LAN redundancy simply by enabling it in the SCU. You must have a protocol enabled so that the SCU is configured for network support.

To enable LAN redundancy, click the Advanced button on the Network Configuration dialog box. A caution message box warns you not to modify these values without familiarity with the system. If you are unsure as to how to proceed, refer to the Advanced Topics chapter and your network documentation. To continue, click Yes.

Refer to the Mastering iFIX manual for more information on configuring LAN redundancy in iFIX.

Configuring Network Timers

The Advanced Configuration dialog box allows you to change your View client's network session timer values. You can also change your network timers on a per-node basis. For more information, refer to the Configuring Remote Nodes section. Refer to the Advanced Topics chapter for more information on network session timers.

Configuring Network Security

Secure communications between two or more iFIX nodes is available with authenticated server-to-client communications, as well as end-to-end data protection. The ability to configure non-listening clients also provides additional security measures.

Refer to the following topics for more detailed information about network security:

- Connection Authentication

- Site-Specific Certificates

- Encryption of Packet Data

- Non-listening Clients

There are two types of network computing: Legacy (default) and Trusted (secure).

An iFIX network can be configured to have multiple IP addresses; however, you cannot mix trusted and legacy communications on the same network. You can configure the network to be only trusted, or only legacy secure.

Legacy Network Computing

Legacy (default) network computing allows you to continue to use legacy security with iFIX 4.0. Legacy security works on non-secure IP addresses. Legacy security limits the network exposure through several methods:

- Communications through authorized incoming IP validation

- Authorized IP connections

- Authorized modification validation a the communications layer

- Basic network encryption

Communications through authorized incoming IP validation

iFIX is aware of the IPs assigned to the machine it is running on and can be set to allow communications only on the dedicated IP address. This can be used in conjunction with hardware firewalls to limit the computers that can communicate with an iFIX installation. Machines with multiple Ethernet cards can be used to bridge between trusted and un-trusted networks.

Authorized IP connections

Legacy security supports the Accept Unknown Connections feature. This feature is a list of authorized IPs that are allowed to make connections to the iFIX networking system. Machines not on this authorized list are not allowed to connect and communicate with the SCADA. For more information, refer to Disabling Connections from Unauthorized Nodes.

Authorized modification validation at the communications layer

Legacy security supports the Accept Unknown Writes feature. This feature is a list of authorized nodes that are allowed to modify the iFIX databases. The type of packet coming in is validated against the list, and nodes that are not on the list are not allowed to modify the iFIX databases. For more

information, refer to Disabling Database Write Access for Unauthorized Nodes.

Basic network encryption

Legacy security supports a number of methods to encrypt the data being sent over the network, such as simple encryption and data hiding. For more information, refer to your Windows documentation.

Trusted Network Computing

Secure networking is either enabled or disabled. Authentication and data packet encryption can only be enabled together. When enabled, the communications server (the client or SCADA the receiving incoming connections) accepting the incoming connection will require all incoming connections to be secure. All incoming connections on a secure communications network must meet the secure communications requirements.

For more information about trusted computing, refer to Connection Authentication.

Failure Modes

There are three situations that will cause a connection attempt to fail:

- A legacy machine attempting to connect to a secure only (trusted network) machine is rejected and a security message sent.

- A machine with an invalid certificate attempting to connect is rejected and a security message is sent.

- Connection is lost and the new connection reverts back to the authentication of certificate per the initial connection.

Connection Authentication

Clients connecting to a server must use an authentication requirement to validate the connection to the server. This assures that the client (sender) is authorized to communicate with the server (SCADA) within the secure network. An authentication certificate method is used to ensure that the client is authorized by having the same set of certificates as the server. This is done using a signed (encrypted) password that is validated on the server end to authenticate that the client's certificate will be used to authorize connections between iFIX 4.0 and greater nodes. Your iFIX installation provides a default network password (INETWORK) that allows a default configuration to continue to work as it currently does.

Authentication is managed by the user and is either enabled or disabled; that is, you can only turn on authentication and encryption together. This means that you can have only default computing (legacy and iFIX 4.0) or trusted computing (iFIX 4.0 to iFIX 4.0) on an iFIX network; you cannot combine legacy and trusted computing on a node . When secure networking is enabled, the communications server (the client or SCADA) accepting the incoming connection will require all incoming connections to be secure; that is, incoming connections must fulfill the requirements of a secure iFIX connection.

Secure communications allow only machines with known credentials to complete a connection within the secure network. In addition, the encryption of the data packets will allow sensitive data an additional layer of security during the transmission from client to server, and server to client. For more information about packet encryption, refer to Encryption of Packet Data.

A secure layer is used to authenticate communications. This gives iFIX networking the ability to validate end-to-end communications. The default certificate used allows all of iFIX to communicate with transmission security without site-specific authentication. An authorized user can change the default certificate for a machine to a site-specific certificate. For more information, refer to Site-Specific Certificates.

The following image graphically demonstrates how trusted networking allows or disallows connections among various types of iFIX installations.
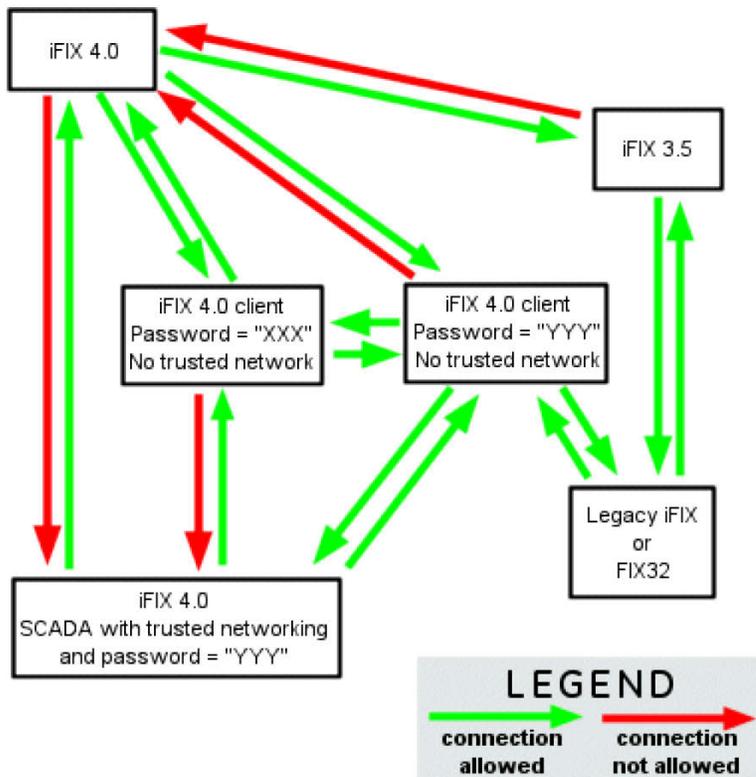
Site-Specific Certificates

iFIX 3.5 and earlier uses the same method and certificate for basic networking security features in all instances of the product. iFIX 4.0 and greater, however, gives you the ability to create site-specific certificates to provide your own security certificate for a network and prevent non-certified iFIX installations from communicating in that network.

You can change the default certificate used to validate, encrypt, and authenticate network transmissions. This allows you to set up multiple secure networks with different certificates, thus isolating iFIX networks from each other. As a result, non-configured or default installations cannot be used to intercept or initiate communications in a secure network.

Non-certified machines can communicate through legacy communications, if the network has been configured in that manner. Only by having two or more iFIX 4.0 machines properly configured will the authentication step be used; however, you can still encrypt communications for all iFIX 4.0 to iFIX 4.0 communications using default certificates.

You can use the certificate information to enable other instances of iFIX 4.0 and greater to communicate within the secure network.

Site-specific certificates are created by entering a password in the Network Password field in the Network Configuration dialog box on the System Configuration Utility (SCU), as shown in the figure below.
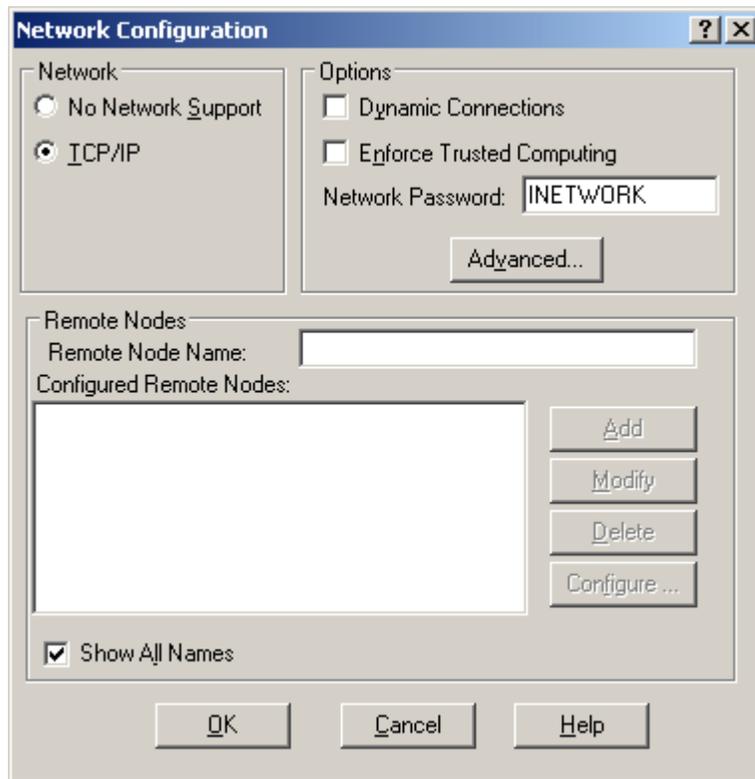
The password is not encrypted in this dialog box, but is encrypted in the SCU file. You can also use security areas to lock users out of the SCU, as well as directory security. This is the physical layer of security for the network password. For more information about SCU security areas, refer to Configuring Security.

The default password displayed in the Network Password field is provided for legacy security and connection authentication. For more information, refer to Connection Authentication.

Encryption of Packet Data

The packets generated between two secured iFIX 4.0 and greater nodes is encrypted to prevent the interception of data. Non-certified machines will not be able to access real time data and other information passed during the normal operation of secure iFIX nodes. Encryption is user configurable and site specific to allow individual instances of secure networking.

When a secure connection has been established between iFIX 4.0 and greater nodes, the packing of TCP/IP packets is encrypted prior to transmission between nodes. This packing uses the certificate the two iFIX nodes have to ensure only those nodes can use the data being transmitted.

Since each node can have only one certificate, all server to client communications the node participates in must be using the same certificate for secure communications. This allows sub-networks of iFIX nodes to exist on the same network, each with a different certificate, without the interception and use of transmitted packets.

For more information on certificates, refer to Connection Authentication and Site-Specific Certificates.

Non-listening Clients

All iFIX 3.5 and earlier SCADA and client nodes create listeners for incoming communications. For clients, this usually means that unsolicited alarm messages can be accepted from SCADA machines they have not initiated communications with.

A non-listening client is a client/SCADA that cannot accept incoming connections. Non-listening clients/SCADAs allow the machines to make connections to other servers as normal, but also allow them to not have a listener created. This means that any attempts to communicate with a non-listening client will fail, but the non-listening client can still communicate when it initiates the connection.

Creating Non-listening Clients

iFIX 4.0 and greater allow you to configure clients to be non-listening by default, securing iFIX so that non user-configured communications are denied. You can modify the clients' behavior at a later time if you want them to accept incoming connections.

▶ **To create a non-listening client:**

1. Open the FIX.INI on your SCADA server or client using a text editor. This file resides in the iFIX Local path.

2. Locate the TCPTASK under the [NETWORK] section and change:

    ```
    RUN=%TCPTASK.EXE
    ```

    to:

    ```
    RUN=%TCPTASK.EXE/s
    ```

3. Save the file. You can now start an iFIX session without opening a listening socket.

NOTE: The use of non-listening machines is independent of the secure communications requirements and is node/instance specific. For more information about secure communications, refer to Connection Authentication.

Non-listening Clients and Terminal Services

With the use of Terminal Services and secure operating systems, such as Windows XP with Service Pack 2, creating listening sockets for every machine has become a potential security risk.

On Terminal Services, only the last iFIX client session to open a socket maintains the socket; that is, any call to open a socket closes the previous socket. Therefore, on Terminal Services, only one iFIX client has a listener, and that is based on the last client to start.

Using Terminal Services, all clients, except the last one to start, are automatically non-listening. The creation of non-listening clients is not required. However, it is recommended that you make the clients non-listening, as non-listening clients are more secure than listening clients.

Non-listening Clients and Windows XP Service Pack 2 (SP2)

If you are using Windows XP SP2 or Windows Server 2003 SP1, and an iFIX client attempts to open a

socket, the firewall appears informing you of this attempt. If you choose No, the client closes the socket and becomes non-listening; if you choose Yes, you create an open socket. Closing down this socket prevents firewall notifications from being displayed; however, as outgoing communications establish the socket to the SCADA, only the ability to *receive* unsolicited messages is removed.

Denial of Service Attacks

Denial of service (DoS) attacks are a potential problem when unnecessary listening sockets are open. A DoS attack is an attempt to prevent legitimate users of a service from using that service.

Nothing done in iFIX can prevent a DoS, nor mitigate its affect on the network; however, closing down unnecessary listening sockets prevents iFIX from needlessly processing DoS messages aimed at the client nodes.

In a physically secure situation this is not a problem, as the attack would have to come from within the secure network. In a distributed network, however, where clients and SCADAs are on separate networks, the chance of one of the networks not being secure increases. Closing the listening socket prevents iFIX from processing incoming messages that are not intended for iFIX; that is, an iFIX only firewall.

Configuring Alarms

When a process value exceeds a limit that you define, iFIX issues an alarm to inform operators of this event. You can enable and configure alarm services using the Alarm Configuration functionality of the SCU.

To configure alarms, click the Alarm button on the SCU toolbox. The following sections detail how to configure alarming functions.

- Enabling Alarm Services

- Customizing Alarm Services

- Advanced Alarm Configuration

- Editing the Alarm Area Database

- Configuring the Auto Alarm Manager

- Configuring the Alarm Horn

Enabling Alarm Services

Alarm services give you the tools you need to customize your alarm configuration. They are flexible in that you can enable any one or all of them, and you can define settings for each service to help you implement your alarming scheme. The following alarm services are available on the Alarm Configuration dialog box:

- Alarm Printers 1, 2, 3, and 4

- Alarm Summary Service

- Alarm File Service

- Alarm History Service

- Alarm Network Service (active only if you are networked)

- Alarm Startup Queue (active only if you are configured as a networked SCADA server)

- Alarm ODBC Service

To enable and configure a service, simply double-click it. For more detailed information on alarm services, refer to the Implementing Alarms and Messages manual. The following sections detail how you can customize alarm services using the SCU.

Customizing Alarm Services

You can modify several settings of each alarm service to customize your configuration. Each alarm service contains its own configuration dialog box with specific options that you can modify. You can also access the Alarm Areas dialog box from this configuration dialog box.

Refer to the Implementing Alarms and Messages manual for more detail on how the dialog boxes work for each service.

Configuring Alarm Areas

The Configure Alarm Areas dialog box controls which alarms and application messages the alarm service can receive. You can access this dialog by clicking the Areas button on the configuration dialog box for the task you have selected.

NOTE: You can also perform advanced alarm area configuration functions. Refer to the Advanced Alarm Configuration section for more details.

Refer to the Implementing Alarms and Messages manual for more information on routing alarm areas.

The following section briefly describes how to use the Configure Alarm Areas dialog box when configuring alarm areas.

How to use the Configure Alarm Areas Dialog Box

The SCU allows you to access the Configure Alarm Areas dialog box from several locations in the interface, including the following:

Alarm Services. Double-click on an alarm service in the Alarm Configuration dialog box and then click Areas. A Configure Alarm Areas dialog box appears specific to the service you enabled.

Common Alarm Areas. Click Advanced on the Alarm Configuration dialog box and then click Common Areas. A Configured Alarm Areas dialog box appears for common areas. Note that the Use Areas Common to All Services option button is not available because you have already chosen to route to common areas.

Application Messages. Click Advanced on the Alarm Configuration dialog box and then click either Operator Messages or Recipe Messages for the messages you want to route to specified alarm areas. You can configure up to fifteen alarm areas.

There are several areas of the dialog box that help you configure your alarm areas. The following simple example illustrates how to configure alarm areas D and E to receive operator messages.

▶ To configure alarm areas D and E to receive operator messages:

1. Select alarm areas. The alarm area selection option buttons let you choose which alarm areas you want to configure.

   - Click the Select from Alarm Area Database option to display all areas from the alarm area database in the Available Areas list box. You can also click the Browse button to search alternate directories.

   - Click the Use "ALL" Alarm areas option to add all the alarm areas in the database to the list of configured alarm areas.

   - Click the Use areas common to all services option to add all the alarm areas common to all services to list of configured alarm areas.

2. Add alarm areas to the Configured Areas list box. Highlight areas D and E in the Available Areas list box and click the right arrow button. This adds the selected areas to the Configured Areas list box. If you need to remove an area, highlight the area to be removed and click the X button. (If you selected Use "ALL" Alarm Areas in Step 1, the alarm area ALL is added to the Configured Areas list box. This alarm area indicates the configured alarm services receives alarms from every available alarm area.)

3. When you are finished, click OK to save your configuration, and exit the Configure Alarm Areas dialog box.

Formatting Messages

You can define the length, number of characters, and the column order for alarm or event messages. To do this, click Format on the configuration dialog box for the task you have selected, and enter the appropriate formatting options in the Message Format Configuration dialog box. This dialog box shows the column content and layout fields for block information.

To use areas common to all alarms and messages across the network, click Use Common, and configure the common messages using the Advanced Alarm Configuration dialog box. Refer to the Advanced Alarm Configuration section for more information.

Selecting a Port

For each printer service, you can connect the printer to serial ports (COM) 1 or 2, to parallel ports (LPT) 1 or 2, or to a USB port.

Naming a Printer

The Printer Description area displays the printer that corresponds to the port selection. Rather than use a generic title, such as Alarm Printer 1, you can change the name of the printer task as it appears in the Printer Name text box.

Deleting Alarms

You can automatically or manually delete alarms using the Alarm Summary service. Select either the Automatic or Manual option buttons in the Alarm Deletion area to choose the method of alarm deletion.

Enabling the Startup Queue Configuration

Using the Startup Queue Configuration dialog box, you can configure the SCADA server to send all the alarms that have occurred prior to starting iFIX on the View client. The SCADA server sends these alarms to the iClient when the client starts. To enable the Startup Queue Configuration, double-click the Alarm Startup Queue service. The Startup Queue Configuration dialog box appears.

NOTE: You must be configured as a SCADA server and have the Network Alarm Service enabled in order to enable the Startup Queue Service.

By default, the Summary Alarms Only check box is selected so that the Alarm Startup Queue service delivers only the current alarms. If you want to receive additional alarms and messages, click the check box to disable this function.

NOTE: By disabling the Summary Alarms Only option, you may receive duplicate alarms at some alarm destinations. You also increase network traffic if iClients are configured to receive alarms from the local SCADA server.

You can also filter alarms according to a set time. To do this, select the Enable Time Filter check box and enter the hour and minute in the appropriate Filter Alarms Older Than fields.

Enabling the Alarm ODBC Service

Another valuable service you can enable in the SCU is Alarm ODBC. This service sends alarms and messages to an ODBC relational database. Once the relational database receives and stores the data, you can easily retrieve any information you want by querying the database.

For more information on the Alarm ODBC Service, refer to the Configuring the Alarm ODBC Service section in the Implementing Alarms and Messages manual.

Advanced Alarm Configuration

The SCU provides advanced functionality that gives you more ways to configure your alarm destinations. To access advanced configuration options, click the Advanced button in the Alarm Configuration dialog box.

The sections that follow summarize the functions that are available. For complete details on how to work with alarm areas, refer to the Implementing Alarms and Messages manual.

Configuring Common Alarm Areas

To assign alarm areas common to all services, click the Common Areas button and select the alarm areas you want.

Defining a Common Message Format

You can define a common message format for alarms and messages received by Alarm Printer, Alarm File, and Alarm History services. To do this, click the Common Format button and select or edit the properties of the messages you wish to define.

Routing Application Messages

To control which alarm areas receive application messages on other servers, configure the alarm areas for these messages. You can configure areas for either operator messages, recipe messages, or both, by clicking the Operator Messages or Recipe Messages buttons.

Modifying Alarm Queues

Sometimes a large process environment requires that you balance using system resources against handling large numbers of alarms. In order to do this, you may have to modify alarm queues so that your local SCADA server can handle the number of alarms being routed through the network. For more information on modifying alarm queues, refer to the Implementing Alarms and Messages manual.

Editing the Alarm Area Database

The SCU makes it easy for you to configure the Alarm Area Database. You can make changes to the database after you have configured any number of alarm areas.

To edit the alarm area database, start iFIX on the local SCADA server, click the Alarm Area Database button on the SCU toolbox. You can also access this dialog box by clicking Advanced on the Alarm Configuration dialog box and then clicking Alarm Area Database.

Using the Edit Alarm Area Database dialog box you can add, modify or delete an alarm area, or designate a name for an alarm area that is specific to your process environment. For example, you can replace the default alarm area, A, with a more intuitive name, *Main Oil Well*, by selecting A in the Configured Alarm Areas list, entering a new name in the Alarm Area field, and clicking Modify. The new name is added to the list in alphabetic order.

NOTE: Changing alarm area names in the alarm area database automatically changes them in your process database.

Refer to the Implementing Alarms and Messages manual for more information on editing the Alarm Area Database.

Configuring the Auto Alarm Manager

The Auto Alarm Manager lets you configure a remote server so that it automatically delivers alarms to a central location using the Microsoft Remote Access Service.

To access the Auto Alarm Manager feature in the SCU, select Auto Alarm Manager from the Configure menu. The Auto Alarm Manager Configuration dialog box appears. Click Enable to activate all the fields. By default, the Auto Alarm Manager is disabled.

Auto Alarm Manager statistics are displayed in Mission Control so that you can easily monitor the program's progress. Refer to the Viewing Auto Alarm Manager Statistics section for more information.

Refer to the Using Auto Alarm Manager section in the Implementing Alarms and Messages electronic book for more information on configuring the Auto Alarm Manager.

Configuring the Alarm Horn

When a new alarm occurs in the system, iFIX can notify you through the alarm horn. You can enable or disable the alarm horn from the SCU, and also from the WorkSpace through the Alarm Horn Expert. For example, you can disable the horn in SCU, then enable or disable it from the Alarm Horn Expert once iFIX has started.

It is important to note that these two alarm horn configurations work independently of each other. For example, if you disable the alarm horn in the SCU, then enable it using the alarm horn expert once iFIX has started, each time that you shutdown and restart iFIX, the horn will be disabled. This occurs because the SCU setting is the initial value and it takes effect each time that you start iFIX.

NOTE: Shutting down and restarting the WorkSpace has no effect on the alarm horn configuration.

For more information on running experts, refer to the Running Experts section in the Creating Pictures manual.

Configuring SCADA Servers

SCADA servers monitor process values and communicate with process hardware. To establish and configure a SCADA server, click the SCADA button on the SCU toolbox. The following subsections detail how to configure SCADA servers using the SCADA Configuration dialog box.

- Enabling SCADA Support
- Naming the Database
- Configuring Drivers

Enabling SCADA Support

To operate as a SCADA server, you must first enable SCADA support using the SCADA Configuration dialog box. When you enable SCADA support, the local node becomes a SCADA server capable of accessing your process hardware. You can then set up and configure I/O drivers and establish SCADA server failover in your network.

Naming the Database

Once you enable SCADA support, you can define the process database you want to load when iFIX starts. You can also change the database name from the main SCU window by double-clicking the database entry (located under the Node name entry).

NOTE: iFIX comes with an empty database file named EMPTY.PDB. This database is read-only. By loading and saving the database to a different name you can quickly create an empty, working database. We recommend that you create a new database with a new name to prevent overwriting your work when re-installing or upgrading software.

Configuring Drivers

iFIX provides at least two I/O drivers to provide the communications link between the process hardware and iFIX. Before your SCADA server can communicate with the process hardware, you need to define and configure at least one I/O driver. iFIX can load up to eight I/O drivers during startup.

The first step in configuring your driver is to tell iFIX which driver you want to use.

Setting up the Driver

Some drivers use an interface card to communicate with the process hardware. In this case you may have to configure the interface card to use the driver.

NOTE: Not all drivers require an interface card, so the setup field may be grayed out. Refer to your I/O driver manual for information on configuring this card.

Configuring an I/O Driver

I/O drivers are configured using the I/O Driver Configuration program.

NOTE: Not all drivers have a configuration program, so the Configure field may be grayed out. Also, the initial screen of the I/O Driver Configuration program varies depending on the type of driver you are configuring.

Configuring Startup Tasks

You can specify tasks for automatic start-up by clicking the Task button on the SCU toolbox and displaying the Task Configuration dialog box. The tasks listed in this dialog box start when you run the FIX Startup program. For example, if you always use I/O Control when you start iFIX, configure the SCU to start IOCNTRL.EXE automatically. Add the IOCNTRL.exe to the top of the configured task list.

In the Task Configuration dialog box, an asterisk (*) next to a task means that Startup minimizes the task after starting it. A percent sign (%) preceding a task means that Startup starts that task in the background. To change the state of a task, select the task, select an option from the Start Up Mode area, and click Change. iFIX executes the tasks in the same order as they appear in the Configured Tasks list. To remove a task from the list, select the task from the Configured Tasks list and click Delete.

If desired, add any specific command line parameters in the Command Line field. Refer to the Controlling SAC Startup section for available SAC command line parameters, or refer to individual application manuals for available command line parameters for each application.

Refer to the Running iFIX Tasks in the Background section for information on iFIX tasks that can be started in the background.

If you run iFIX as a service, the tasks listed in the task list also start as a service. Refer to the Running iFIX as a Service section for information on how to start iFIX as a service.

Running iFIX Tasks in the Background

When you automatically start programs, you can specify that they run in the background so that they do not interfere with your typical operation. You should only configure the following iFIX tasks as background tasks (All of these files are located in the FIX Base path):

- SAC (WSACTASK.EXE)
- Historical Collect (HTC.EXE)

- SQL Task (WSQLODC.EXE)

- I/O Control (IOCNTRL.EXE)

- Event Scheduler (FIXBACKGROUNDSERVER.EXE)

Controlling SAC Startup

iFIX lets you control the startup status of SAC using the task configuration of the SCU.

Starting SAC Automatically

When you enable the SCADA function, the SCU includes WSACTASK.EXE in the startup list within the Task Configuration dialog box. This starts SAC automatically.

If you disable SAC during development, you must enable it again. You can also modify how SAC operates by entering specific command line parameters. The following command line parameters are available:

- **S** – Synchronizes SAC to the system clock. Refer to the Building a SCADA System manual for information on scan times and synchronization.

- **Dseconds** – Delays SAC processing of the database until the I/O driver initializes and receives data from control devices. By default, SAC automatically delays processing for 8 seconds. You can use the D parameter to specify a delay of 1 to 300 seconds, for example D30, to control initial processing of database blocks.

- **Q** – Sets the number of queue entries for the Alarm Queue Status program that monitors the alarms deleted by SAC. This parameter lets you override the default (500), and prevents the queue from expanding to the maximum length of 2000.

- **R** – Suppresses Range (RANGE) alarms.

- **UN** – Suppresses Under Range (UNDER) alarms.

- **N** – Suppresses No Data (NO_DATA) alarms.

- **C** – Suppresses communication (COMM) alarms.

- **U** – Suppresses the Over Range (OVER) alarms.

  IMPORTANT: *SAC parameters do not use the slash (/) or dash (-) delimiters. Use spaces to enter optional SAC parameters. For example: S D30*

Starting I/O Drivers Automatically

I/O drivers are started by the I/O Control program through the Task Configuration dialog box. When you install an I/O driver, the I/O Control program is automatically added to the list of tasks.

If you remove the I/O Control program from the task list, you can add it back again. The table below shows you the command line parameters you can use to specify how I/O drivers start.

I/O Control Command Line Parameters	
Parameter	**Description**
/A	Starts all I/O drivers identified in the SCADA configuration.
/S*xxx*	Starts one I/O driver, where *xxx* is the three letter I/O driver acronym. For example, /SABH.
/D*xxx*	Delays the startup of a driver where *xxx* is the delay time in seconds.
/AP*xxx*	Sets the message rate for all drivers, where *xxx* is a value of 1 to 100.
/S*drv*P*xxx*	Sets a specific driver's message rate, where *xxx* is a value of 1 to 100.

NOTE: FIX I/O drivers 7.x or greater automatically start communicating with their OPC server. No command line parameter is needed.

Configuring iFIX for Relational Databases

iFIX supports relational databases, such as Microsoft SQL Server and Oracle through Microsoft's industry-standard Open Database Connectivity (ODBC). Using the SCU, you can set up your server to access multiple relational databases from a process database. The SCU's SQL functionality allows you to read and write data between a SCADA server's process database and multiple relational databases.

▶ **To access a relational database data source:**

1. Set up your relational database and ODBC driver.
2. Configure the ODBC data source.
3. Add the database to the SQL connection list.
4. Create the library and error tables.

For more information on accessing relational database data sources, refer to the Installing and Configuring Data Sources chapter in the Using SQL manual.

Configuring the SQL Service

The SQL Task Configuration dialog box lets you configure the SQL service, including enabling SQL support, specifying a backup file location, identifying a relational database, routing SQL errors and messages to alarm areas, and defining a sleep interval.

For more information on configuring the SQL service, refer to the Configuring the SQL Task chapter in the Using SQL manual.

SCU Dialog Boxes

The SCU includes the following dialog boxes (listed in alphabetical order):

- Advanced Alarm Configuration Dialog Box

- Advanced Network Configuration Dialog Box

- Advanced Send Alarm Settings Dialog Box

- Alarm Configuration Dialog Box

- Alarm File Service Configuration Dialog Box

- Alarm History Service Configuration Dialog Box

- Alarm ODBC Service Configuration Dialog Box

- Alarm Printer Configuration Dialog Box

- Alarm Queues Configuration Dialog Box

- Alarm Service Configuration Dialog Boxes

- Alarm Summary Service Configuration Dialog Box

- Auto Alarm Manager Configuration Dialog Box

- Available Phonebook Entries Dialog Box

- Configure Alarm Areas Dialog Box

- Database Definition Dialog Box

- Database IDs Available Dialog Box

- Database Types Available Dialog Box

- Drivers Available Dialog Box

- Edit Alarm Area Database Dialog Box

- File Description Dialog Box

- iFIX Alarm ODBC Service Configuration Dialog Box

- List of Alarm Clients Dialog Box

- Local Startup Definition Dialog Box

- Message Format Configuration Dialog Box

- Network Alarm Configuration Dialog Box

- Network Configuration Dialog Box

- Path Configuration Dialog Box

- Remote Alarm Areas Dialog Box

- Remote Node Configuration Dialog Box

- SCADA Configuration Dialog Box

- Select the File Name to Use Dialog Box

- Send Alarm Filters Dialog Box

- SQL Accounts Dialog Box

- SQL Login Information Dialog Box

- SQL Task Configuration Dialog Box

- Startup Queue Configuration Dialog Box

- Task Configuration Dialog Box

- Timers Dialog Box

Advanced Alarm Configuration Dialog Box

This dialog box allows you to access advanced settings for the alarm configuration. The Advanced Alarm Configuration dialog box displays the following items:

Common Format

Opens the Common Message Format Configuration dialog box.

Common Areas

Opens the Configure Alarm Areas dialog box.

Queue Configuration

Opens the Alarm Queues Configuration dialog box.

Operator Messages

Opens the Configure Alarm Areas dialog box for the Operator Messages.

Recipe Messages

Opens the Configure Alarm Areas dialog box for the Recipe Messages.

Alarm Area Database

Opens the Edit Alarm Area Database dialog box.

Advanced Network Configuration Dialog Box

This dialog box allows you to change the values of the network timers and control LAN redundancy on your node. iFIX uses your entries in this dialog box to tailor resources precisely for your configuration.

CAUTION: Modifying network resources can seriously affect the performance of a node. You should not use this dialog box unless you have a thorough understanding of iFIX networking concepts.

The Advanced Network Configuration dialog box displays the following items:

Network Timers

Field	Description
Keep Alive Field and Check Box	Allows you to specify the amount of time that, if no activity has occurred over an established connection, a View client waits before sending a heartbeat message. The default value for this field is 20 seconds.
Send Field and Check Box	Allows you to specify the amount of time that a View client waits for a request to the SCADA server to be acknowledged. If this timer expires, the session ends. The default value for this field is 30 seconds.
Receive Field and Check Box	Allows you to specify the amount of time that a View client waits for a reply from the SCADA server. When running iFIX over TCP/IP, the effective session timeout values is either the Send timer or the Receive timer, whichever is greater. If this timer expires, the session ends. The default value for this field is 60 seconds.
Inactivity Field and Check Box	Allows you to specify the amount of time that, if no data activity has occurred over an established connection, a View client waits before removing the dynamic connection from the list of outgoing connections. If this timer expires, the session ends. The default value for this field is 300 seconds.
Reset to Defaults Button	Allows you to reset the network timers to their default values.

NOTE: See the Determining Session Timer Values section in the Setting up the Environment electronic book for more information on network timers.

LAN Redundancy

Field	Description
Available Paths List	Displays a list of available network paths.
Enable Status Option Button	Allows you to enable the network path selected in the Available Paths list box for LAN redundancy.
Disable Status Option Button	Allows you to disable the network path selected in the Available Paths list box for LAN redundancy.

Field	Description
Enable LAN Redundancy Check Box	Allows you to enable the LAN redundancy feature on the node.
Reset to Defaults Button	Allows you to reset LAN redundancy to its default values.

More Network Options

Field	Description
Accept Unknown Host	Select this option to allow the SCADA node to accept connections from any computer. When the parameter is disabled, access is restricted to the iClients (View) you specify.
Accept Unauthorized Writes	Select this option to allow the SCADA node to log all unauthorized write attempts from the iClients.
Log Unauthorized Writes	Select this option to enable the logging of failed writes.
Edit Box	Allows you enter a node name to add to the Hosts or Write Nodes list.
Add Hosts Button	Click the button to add a node from the above edit box to the Hosts list.
Remove Host	Select a host in the list and then click this button to remove it from the list.
Add Write Node Button	Click the button to add a node from the above edit box to the Write Nodes list.
Remove Node	Select node that allows writes in the list and then click this button to remove it from the list.
Hosts List	Displays a list of hosts.
Write Nodes List	Displays a list of writable nodes.

Advanced Send Alarm Settings Dialog Box

This dialog box allows you to set up the Auto Alarm Manager as a service and set up the program's communication timers. The Advanced Send Alarm Settings dialog box displays the following items:

Username

Allows you to specify the user name of a Windows user account that the Auto Alarm Manager can use to report alarms when no one is logged into the sending node. The user name you specify must reside on the RAS server and must have dial-in permission.

Password

Allows you to specify the password of a Windows user account that the Auto Alarm Manager can use to report alarms when no one is logged into the sending node. Use the Confirm Password field to re-enter the password specified in this field.

Confirm Password

Allows you to confirm the password specified in the Password field.

Send Timeout

Allows you to fine tune serial communication between the sending and receiving nodes. This field controls the amount of time the Auto Alarm Manager has to send alarms to the receiving node.

Receive Timeout

Allows you to fine tune serial communication between the sending and receiving nodes. This field controls the amount of time the Auto Alarm Manager waits for a response from the receiving node that the alarms were delivered successfully.

Alarm Configuration Dialog Box

This dialog box allows you to enable or disable the following alarm services:

- Alarm Printers 1-4
- Alarm Summary Service
- Alarm File Service
- Alarm History Service
- Alarm ODBC Service
- Alarm Network Service
- Alarm Startup Queue Service

Once enabled, you can configure an alarm service by specifying alarm areas, port definitions, printer names, message formats, and other settings when appropriate.

NOTE: If you do not have the Alarm Network Service enabled, application messages are logged only

to local alarm services. Enable the Alarm Network Service to send messages out over the network.

The Alarm Configuration dialog box displays the following items:

Alarm Configuration List Box

Double-click an entry within the Alarm Configuration list box to modify an alarm service and access its configuration dialog box. You can only access configuration dialog box if the alarm service is enabled.

Enable

Allows you to enable an alarm service.

Disable

Allows you to disable an alarm service.

Modify

Allows you to access a service's configuration dialog box.

Advanced

Allows you to access advanced settings for the dialog box.

Alarm Queues Configuration Dialog Box

This dialog box displays the alarm queue resources. iFIX uses your entries in the SCU menus to tailor resources precisely for your configuration. Most users never need to modify these defaults.

CAUTION: Modifying alarm queue resources can seriously affect the performance of a node. You should not use this dialog box unless you have a thorough understanding of iFIX alarming concepts.

In the Setup areas, each enabled service displays the maximum number of alarms it can handle at any one time. This means that enough system resources are reserved to hold the number of messages listed here in memory until they can be sent to the alarm service (for example, a printer). If more messages come in after the memory queue has been filled, the older messages are discarded.

You must strike a balance between using up resources and recording all alarms. If your system can handle it, you should set these entries to the maximum number of alarms that the system will send to the alarm service at any one time.

The Alarm Queues Configuration dialog box displays the following items:

Local Setup

Field	Description
Summary Queue	Displays the size of the Summary queue.
File Queue	Displays the size of the File queue.
Printer 1 Queue	Displays the size of the Printer 1 queue.
Printer 2 Queue	Displays the size of the Printer 2 queue.
Printer 3 Queue	Displays the size of the Printer 3 queue.
Printer 4 Queue	Displays the size of the Printer 4 queue.
History Queue	Displays the size of the History queue.

Network Client Setup

Field	Description
Send Queue	Displays the size of the Send queue.
Control Queue	Displays the size of the Control queue.

Network Manager Setup

Field	Description
Receive Queue	Displays the size of the Receive queue.
Startup Queue	Displays the size of the Startup queue.
Control Queue	Displays the size of the Control queue.
Send Buffers	Displays the size of the Send Buffers.

Reset Sizes Button

Allows you to configure your alarm queues to the standard defaults, or the defaults to be calculated by the maximum alarms.

Alarm Service Configuration Dialog Boxes

The Alarm Service Configuration dialog box allows you to specify some or all of the following features for an alarm service:

- Which alarm area information and messages are sent to the printer.

- The format for the alarm information and messages.

- The port the printer is connected to.

- The name of the printer.

- Whether manual alarm deletion is enabled or disabled.

- The information for the ODBC Alarm Service.

The following sections describe the fields in each individual Alarm Service Configuration dialog box.

Alarm Printer Configuration Dialog Box

Field	Description
Port Definition Area	The Port Definition area lets you connect an alarm printer to serial ports (COM) 1 or 2, to parallel ports (LPT) 1 or 2, or to a USB port. Each printer service must be attached to a unique port. The default port is USB.
Printer Name Field	Allows you to specify the name of the alarm printer as it appears on the Alarm Configuration dialog box. The printer name can be up to 32 characters in length.
Areas Button	Allows you to access the Configure Alarm Areas dialog box. This dialog box lets you specify the alarm areas for the selected alarm service.
Format Button	Allows you to access the Alarm Service Message Configuration dialog box. This dialog box lets you specify a format for the alarm information and messages generated by this node.

Alarm Summary Service Configuration Dialog Box

Field	Description
Manual Button	Allows you to enable manual alarm deletion. Once manual alarm deletion is enabled, you can delete any alarm in the Alarm Summary OCX. To delete these alarms, use one of the following methods: Select the alarm you want to delete and then select the Delete command from the right mouse button menu. Create a script for a push button that allows you to delete selected alarms.
Automatic Button	Allows you to disable manual alarm deletion.
Horn Support Enable	Allows you to enable the alarm horn so that an alarm sounds when a new alarm appears. The horn repeats at three speeds to distinguish between low, medium, and high priority alarms. A one-second increment between beeps signifies high priority alarm, a two-second increment signifies a medium priority, and a three-second increment signifies a low priority.
Horn Support Disable	Allows you to disable the alarm horn. *NOTE: You can later enable or disable the alarm horn from the Alarm Horn Expert once iFIX has started. The SCU alarm horn settings and the the Alarm Horn Expert settings work independently of each other. For example, if you disable the alarm horn in the SCU, then enable it using the alarm horn expert once iFIX has started, each time that you shutdown and restart iFIX, the horn will be disabled. This occurs because the SCU setting is the initial value and it takes effect each time that you start iFIX.*
Areas Button	Allows you to access the Configure Alarm Areas dialog box. This dialog box lets you specify the alarm areas for the selected alarm service.

Alarm File Service Configuration Dialog Box

Field	Description
Areas Button	Click to access the Configure Alarm Areas dialog box.

Field	Description
Format Button	Click to access the Alarm File Service's Message Format Configuration dialog box.

Alarm History Service Configuration Dialog Box

Field	Description
Areas Button	Click to access the Configure Alarm Areas dialog box.
Format Button	Click to access the Alarm History Service's Message Format Configuration dialog box.

Alarm ODBC Service Configuration Dialog Box

Field	Description
Areas Button	Click to access the Configure Alarm Areas dialog box.
Configure Button	Click to access the iFIX Alarm ODBC Service Configuration dialog box.

Network Alarm Configuration Dialog Box

Field	Description
Send Startup Queue Alarms to Original Typers Check Box	Allows you to configure the Alarm Network Service to send start-up alarms to all of the client's enabled alarm destinations.

Startup Queue Configuration Dialog Box

Field	Description
Enable Time Filter Check Box	Allows you to filter the alarms received by the View node by selecting the Enable Time Filter check box and entering a time interval. When you do this, the View node receives all current SCADA node alarms upon startup in addition to all previous alarms within the time interval you specify.
Filter Alarms Older Than Hours Field	Allows you to specify the number of hours previous to startup in which you want to receive the SCADA node's alarms. Valid entries are from 0 to 23. The default is 23. *NOTE: The default setting, 23 hours and 59 minutes, displays all of the SCADA node's alarms that occurred between the time the View node started up and the previous day.*
Filter Alarms Older Than Minutes Field	Allows you to specify the number of minutes previous to startup in which you want to receive the SCADA node's alarms. Valid entries are from 0 to 59. The default is 59. *NOTE: The default setting, 23 hours and 59 minutes, displays all of the SCADA node's alarms that occurred between the time the View node started up and the previous day.*
Summary Alarms Only Check Box	Allows you to receive only summary alarms on the View node. To display summary and operator alarms on the View node, clear the Summary Alarms Only check box. *NOTE: If this check box is cleared when using the Alarm Startup Queue, duplicate alarms will be displayed on all alarm destinations except alarm summary every time the connection to a SCADA node is established.*

Auto Alarm Manager Configuration Dialog Box

This dialog box allows you to enable and configure the Auto Alarm Manager option. The specific fields you complete depends on whether you are setting up the sending node or the receiving node. On the sending node, complete the fields in the Send Alarms box. On the receiving node, complete the fields in the Receive Alarms box.

The Auto Alarm Manager Configuration dialog box displays the following items:

Send Alarms Area

Field	Description
Disable Button	Allows you to disable the Auto Alarm Manager option. On the sending node, use the Enable and Disable buttons in the Send Alarms box. On the receiving node, use the Enable and Disable buttons in the Receive Alarms box.
Enable Button	Allows you to enable the Auto Alarm Manager option. On the sending node, use the Enable and Disable buttons in the Send Alarms box. On the receiving node, use the Enable and Disable buttons in the Receive Alarms box.
Disable Tagname Field	Allows you to specify a tagname that is monitored by iFIX. When the tagname's value is 1, the Auto Alarm Manager cannot send alarms. You can specify a tagname using the format NODE:TAG (the Auto Alarm Manager automatically uses the F_CV field for the tagname).
Primary Contact Field	Allows you to specify the name of a Remote Access Service (RAS) phone book entry that the Auto Alarm Manager dials when it reports alarms. Each phone book entry defines a phone number at which the receiving node can be reached. The Auto Alarm Manager dials the Primary Contact phone book entry first. If for some reason it cannot connect to the node at this phone number (for example, if the line is busy), the Auto Alarm Manager dials the Secondary Contact phone number. If it cannot connect to this node either, the Auto Alarm Manager assumes the alarms are undeliverable. To specify the name of a phone book entry, enter the name you want or press the browse (...) button to display a list of available phone book entries from which you can select. The name of the phone book entry you specify must match the name of the receiving node that the Auto Alarm Manager is trying to reach. The phone book entry entered in the Primary Contact field can be different from the phone book entry entered in the Secondary Contact field.
Primary Contact Browse Button	Allows you to display a list of available phone book entries from which you can select.

Field	Description
Secondary Contact Field	Allows you to specify the name of a Remote Access Service (RAS) phone book entry that the Auto Alarm Manager dials when it reports alarms. Each phone book entry defines a phone number at which the receiving node can be reached.
	The Auto Alarm Manager dials the Primary Contact phone book entry first. If for some reason it cannot connect to the node at this phone number (for example, if the line is busy), the Auto Alarm Manager dials the Secondary Contact phone number. If it cannot connect to this node either, the Auto Alarm Manager assumes the alarms are undeliverable.
	To specify the name of a phone book entry, enter the name you want or press the browse (...) button to display a list of available phone book entries from which you can select. The name of the phone book entry you specify must match the name of the receiving node that the Auto Alarm Manager is trying to reach. The phone book entry entered in the Primary Contact field can be different from the phone book entry entered in the Secondary Contact field.
Secondary Contact Browse Button	Allows you to display a list of available phone book entries from which you can select.
Emergency Tagname Field	Allows you to specify a tagname on the sending node that is set to 1 when the Auto Alarm Manager cannot connect to the primary and secondary contacts or when the Auto Alarm Manager loses a connection to the receiving node during delivery and is unable to finish sending all of its alarms. The format for entering an emergency tagname is NODE:TAG. The Auto Alarm Manager automatically writes to the F_CV field.
	TIP: While you can specify any database block in Manual mode that accepts writes as the emergency tag, Intellution recommends entering the name of an output block for best results.
Max Retries Field	Allows you to specify the maximum number of times the Auto Alarm Manager re-dials either the primary or the secondary contact when reporting alarms. For example, if you set the value of this field to 2, the Auto Alarm Manager re-dials the primary contact twice before trying the secondary contact.
	If the number of retries is exceeded for both primary and secondary contacts, the emergency tag is set to 1. By default, the field is set to 3. You can enter any value from 0 to 10.

Field	Description
Pause Time Field	Allows you to specify the number of seconds the Auto Alarm Manager waits between each retry. Once the pause time expires, the Auto Alarm Manager re-dials the receiving node. For example, assume the maximum number of retries is 3 and the pause time is 30 seconds. If the Auto Alarm Manager dials a remote site and the line is busy, it waits 30 seconds and re-dials the receiving node. When the number of retries is exceeded, the Auto Alarm Manager dials the secondary contact. If you do not have a secondary contact defined, or when the number of retries for the secondary contact is exceeded, the Auto Alarm Manager assumes the alarms are undeliverable and sets the emergency tag. By default, the value in this field is set to 60 seconds. You can enter any value from 15 to 255 seconds.
Remote Alarm Areas Button	Allows you to access the Remote Alarm Areas dialog box, which lets you select one or more alarm areas. The alarm areas you select are assigned to the outgoing alarms, enabling you to reassign the alarms selectively to new alarm areas before they are sent to the receiving node.
Alarm Filters Button	Allows you to access the Send Alarm Filters dialog box, which lets you select one or more alarm area and an alarm priority. Incoming block alarms are filtered based on the alarm areas and alarm priority you select from the dialog box. Only the block alarms that meet the criteria selected are sent to the receiving node.
Yes Acknowledge Delivered Alarms Button	Allows the Auto Alarm Manager on the sending node to automatically acknowledges alarms that were delivered to the receiving node. If the Auto Alarm Manager cannot deliver the alarms, it deletes the alarms in its alarm queue. These alarms are not acknowledged; they are removed from the alarm queue because they could not be delivered.
No Acknowledge Delivered Alarms Button	Prevents the Auto Alarm Manager on the sending node from automatically acknowledging alarms that were delivered to the receiving node.
Delay After Send Field	Allows you to specify the number of seconds the sending node waits between hanging up the modem and dialing the receiving node again. This interval is intended to let an operator dial into the sending node and change the condition that generated the last set of alarms reported. By default, the value in this field is set to zero. You can enter any value from 0 to 32767 into the field.

Field	Description
Advanced Button	Allows you to access the Advanced Send Alarm Settings dialog box, which lets you set up the Auto Alarm Manager as a service and set up the program's communication timers.

Receive Alarms Area

Field	Description
Disable Button	Allows you to disable the Auto Alarm Manager option. On the sending node, use the Enable and Disable buttons in the Send Alarms box. On the receiving node, use the Enable and Disable buttons in the Receive Alarms box.
Enable Button	Allows you to enable the Auto Alarm Manager option. On the sending node, use the Enable and Disable buttons in the Send Alarms box. On the receiving node, use the Enable and Disable buttons in the Receive Alarms box.
Receiving Tagname Field	Allows you to specify a tagname on the receiving node that is set to 1 when new alarms are received. The format for entering a receiving tagname is NODE:TAG. The Auto Alarm Manager automatically writes to the F_CV field. *TIP: While you can specify any database block in Manual mode that accepts writes as the receive tag, Intellution recommends entering the name of an output block for best results.* Once new alarms are received, you must reset the tag's value to 0 manually in order to see when the next set of alarms are delivered. *NOTE: All alarms sent by the Auto Alarm Manager are received as operator messages. These alarms appear in the enabled alarm destinations of the receiving node, except the Alarm Summary link.*

Available Phonebook Entries Dialog Box

The Available Phonebook Entries dialog box displays the following item:

Available Phonebook Entries List Box

Displays a list of the Remote Access Service (RAS) phone book entries you have defined. To select an entry, click the phone book entry you want and click the OK button.

Configure Alarm Areas Dialog Box

When configuring alarm areas, you can assign:

- Every alarm area to alarm services.

- Common alarm areas to alarm services.

- Specific alarm areas to alarm services.

- Every alarm area to application messages.

- Specific alarm areas to application.

The Configure Alarm Areas dialog box displays the following items:

Use All Alarm Areas

Allows you to add all the alarm areas in the database to the list of configured alarm areas.

Select from Alarm Area Database

Displays the alarm areas available in the database that you can add to the list of configured alarm areas. You can click the browse button to select a path for the alarm areas database.

Available Areas

Displays the alarm areas available in the database that can be added to the list of configured alarm areas. This list is displayed only when the Select from Alarm Area Database option button is selected.

Arrow Button

Allows you to add the alarm area selected in the Available Areas list box to the list of configured alarm areas. This button can only be used when the Select from Alarm Area Database option button is selected.

Remove Button

Allows you to delete an alarm area from the list of configured alarm areas. You must select an alarm area in the Configured Areas list box before you can use this button.

Configured Areas

Displays a list of configured alarm areas.

Add Text Box

Allows you to specify an alarm area to add to the list of configured alarm areas. You must click the Add button to add the alarm area to the list.

Add Button

Allows you to add the alarm area specified in the Add field to the list of configured alarm areas.

Browse (...) Button

Allows you to browse to the alarm areas database. This button can only be used when the Select from Alarm Area Database option button is selected.

Database Definition Dialog Box

This dialog box allows you to edit the database information currently defined for this node. The Database Definition dialog box displays the following items:

Database Name

Enter a name in the Database Name field to specify the database used by this node. iFIX loads the database specified in this field during startup.

Browse (...) Button

Click to browse for an iFIX database name.

Database IDs Available Dialog Box

The Database IDs Available dialog box displays the following item:

Database IDs Available List Box

Displays all available ODBC data sources to which you can connect. Select an ODBC data source and click OK to place that data source name in the Database Identifier field.

Database Types Available Dialog Box

The Database Types Available dialog box displays the following item:

Database Types Available List Box

Displays all available relational database types to which you can connect. Select a relational database and click OK to place that relational database name in the Database Type field.

Drivers Available Dialog Box

This dialog box allows you to select a driver to add to the I/O Driver Name field of the SCADA Configuration dialog box. To choose a driver, select it from the list box and click OK to return to the SCADA Configuration dialog box. The driver is then available for you to add to your SCADA configuration.

The Drivers Available dialog box displays the following item:

Drivers Available List Box

Displays a list of I/O drivers configured on this node.

Edit Alarm Area Database Dialog Box

This dialog box allows you to create, edit, or remove alarm areas in the database. The Edit Alarm Area Database dialog box displays the following items:

Alarm Area

Allows you to specify a name for an alarm area.

Configured Alarms

Displays the names of all the alarm areas configured in the database. You can modify the name of an alarm area by selecting it in the list, entering a new name in the Alarm Area field, and clicking the Modify button.

Add

Allows you to add an alarm area to the database. You must enter a name in the Alarm Area field before you can add a new alarm area.

Modify

Allows you to change the name of an alarm area. You must select an alarm area from the Configured Alarm Areas list box and enter a new name in the Alarm Area field to modify an alarm area.

Delete

Allows you to delete an alarm area from the database. You must select an alarm area from the Configured Alarm Areas list box before you can delete an alarm area.

File Description Dialog Box

The File Description dialog box displays the following item:

Configuration File Description

Allows you to add or change your SCU file's unique identifier, displayed at the top of the SCU window. To change the description, enter up to 40 characters in the Configuration File Description field.

NOTE: The description is there only to help you distinguish between SCU files. The system does not use the description in any way.

iFIX ODBC Alarm Service Configuration Dialog Box

The iFIX ODBC Alarm Service Configuration dialog box displays the following items:

SQL Login Information

Field	Description
Use Login Information from SQL Configuration Check Box	Allows you to use the existing SQL setup to specify the database type, user name, password, and database identifier. This feature can be used only if you have installed and configured the iFIX SQL option.
Database Type Field	Allows you to specify a database type for the relational database. You can also click the Browse button to display a list of available database types. If you are using a Microsoft Access database, the database and the Alarm ODBC service must be on the same machine.
Database Type Browse Button	Allows you to display a list of available database types.
User Name Field	Allows you to enter the user name required to connect to the relational database.
Password Field	Allows you to enter the password required to connect to the relational database.
Database Identifier Field	Allows you to specify a database identifier for the relational database. You can also click the Browse button to display a list of available database identifiers.
Database Identifier Field Browse Button	Allows you to display a list of available database identifiers.

Options

Field	Description
Allow Operator to Pause Alarm Logging Check Box	Allows you to temporarily stop alarms from being written to the relational database.
Update Interval Text Box	Allows you to control how often data is written to the relational database. Valid entries are 1 to 300 seconds. The default is 1 second.

Field	Description
Alarm Queue Size Field	Allows you to specify the maximum number of records in the iFIX Alarm Queue. By increasing the queue size, you can prevent alarm loss. Valid entries are from 1 to 32767. The default value is 100.
Number of Records to Log from iFIX Field	The number of records to read from the user queue before writing to the relational database. Increasing this number will result in a more efficient ODBC, but will also increase the risk of losing alarms. The maximum number you can enter is 100.
Number of Records to Log from Backup File Field	The number of records to read from the Lost Connection file before writing to the relational database.

Lost Connections Options

Field	Description
File Field	Allows you to specify a temporary (TMP) file for the Alarm ODBC Service. If the service cannot access the relational database, alarms and messages are saved in this file. When the relational database re-establishes contact with the Alarm ODBC Service, iFIX automatically reads the data in the TMP file to update the relational database. Leave this field blank to disable this feature.
File Field Browse Button	Allows you to select a file.
Tag Field	Allows you to specify a tag that indicates a broken connection with the relational database. Alternatively, instead of entering a tag here, you can create an Alarm ODBC watch dog using the Scheduler. For more information, refer to the Creating an Alarm ODBC Watchdog Using the Scheduler section.
Tag Field Browse Button	Allows you to enter the node name and tag name.

User Fields

Field	Description
Field Name1	Allows you to enter any ASCII format (A_) database block field. For a complete list of available database block fields, refer to the Database Manager Help system.
Field Name2	Allows you to enter any ASCII format (A_) database block field. For a complete list of available database block fields, refer to the Database Manager Help system.
Field Name3	Allows you to enter any ASCII format (A_) database block field. For a complete list of available database block fields, refer to the Database Manager Help system.
Field Name4	Allows you to enter any ASCII format (A_) database block field. For a complete list of available database block fields, refer to the Database Manager Help system.

Database Configuration

Field	Description
Create Table at Runtime if Not Found Check Box	Allows you to have the Alarm ODBC Service create the table at run-time if it does not exist.
Table Name Field	Allows you to specify a table name. When you enter your own table name, you must select the alarm and message fields you want to archive using the Column Configuration spreadsheet. If you are creating a table, you must enter a unique name. You cannot overwrite an existing table. *NOTE: When writing to an Oracle database, be aware that the table name cannot include an embedded period (.) in the name. For instance, an entry such as SchemaName.TableName.Alarms would not be acceptable in this field, since it includes a period between SchemaName and TableName.*
Create Table Now Button	Allows you to create a table when you configure the Alarm ODBC Service.

Column Configuration

Field	Description
Select All Button	Allows you to select all the iFIX Field Names and populate the SQL Column Names automatically. When Clear All is active, allows you to disable any selected iFIX Field Names.
Restore Defaults Button	Allows you to use the default table name, FIXALARMS, to simplify the table setup. When you use the default table name, the Alarm ODBC Service completes the Column Configuration spreadsheet.
Column Configuration List Box	Allows you to specify the alarm and message fields you want to archive.

List of Alarm Clients Dialog Box

You can filter the alarms sent to each iFIX or FIX32 client by entering information into the List of Alarm Clients dialog box (this information can also be entered directly into the FilterAlm.ini file). The List of Alarm Clients dialog box displays the following items:

Clients

Lists the available iFIX Clients that you want to filter alarms on.

NOTE: If you do not want to filter alarms for a specified client, do not include it in this list.

Edit Box

Allows you to enter an iFIX Client name to add to the Clients list.

Add Client

Click to add a client in the edit box to the Clients list.

Configured Areas

Lists the configured alarm areas for the selected iFIX Client.

Add Area

Click to add an alarm area for the selected iFIX Client. When you click Add, the Configure Alarm Areas dialog box appears, which allows you to add alarm areas to the Configured Alarm Areas list.

Local Startup Definition Dialog Box

This dialog box allows you to update your operating system's Registry to specify a local node name

and SCU file name.

If you try to exit the SCU without specifying local startup options, the SCU warns you that iFIX will not be able to properly configure your node.

You can configure to run iFIX as a service by selecting the Continue Running After Logoff check box. This is a system setting, and will make changes to your registry. When you run iFIX as a service, you can also select the Start iFIX at System Boot option, which starts iFIX whenever you start Windows.

You can also use the Local Startup Definition dialog box to enable the local node alias feature and to specify whether you want iFIX to run as a service under Microsoft Windows.

The Local Startup Definition dialog box displays the following items:

Local Node Name

Allows you to specify a unique local node name to specify the name in your operating system's Registry.

Node names can be up to eight characters long. They can include alphanumeric characters, but must begin with a letter. Special characters cannot be used.

Local Logical Name

Allows you to specify a logical node name used for configuring redundancy.

Node names can be up to eight characters long. They can include alphanumeric characters, but must begin with a letter. Special characters cannot be used.

Configuration File

Allows you to specify the full path and name of the local SCU file you want to use as a default. You can also click the browse (...) button to access the File Open dialog box and search for previously defined SCU files (*.SCU).

Browse (...) Button

Allows you to access the File Open dialog box and search for previously defined SCU files (*.SCU).

Local Node Alias

Allows you to enable the local node alias feature. The local node alias feature allows you to substitute a placeholder, THISNODE, for the node portion of a tagname in order to automatically access information from the local SCADA node. This is ideal for developing pictures that can be shared among several computers that each access information from their own SCADA node.

IMPORTANT: You must be logged in as a user in the Administrators group to select or clear the Local Node Alias check box.

Continue Running After Logoff

Allows you to configure iFIX to run as a service under Microsoft Windows when you start iFIX. If you

log out of Windows, iFIX continues to run as a service for the next user who logs on. To stop the service, stop iFIX.

IMPORTANT: You must be logged in as a user in the Administrators group to select or clear the Continue Running After Logoff check box. Additionally, this check box is unavailable when iFIX is running.

Start FIX at System Boot

Allows you to automatically start iFIX when Windows starts. This option is available only if you select the Continue Running After Logoff check box, to run iFIX as a service.

IMPORTANT: You must be logged in as a user in the Administrators group to select or clear the Start FIX at System Boot check box. Additionally, this check box is unavailable when iFIX is running.

Message Format Configuration Dialog Box

This dialog box allows you to specify a format for the alarm information, event messages, and application messages (time and date only) generated by this node. This format applies to all enabled Alarm Printers and the Alarm File Service.

The following types of Message Format Configuration dialog boxes appear in the SCU – all displaying the same configuration items:

- Alarm Printer Message Format Configuration dialog box

- Alarm File Server Message Format Configuration dialog box

- Alarm History Service Message Format Configuration dialog box

- Common Message Format Configuration dialog box

Each Message Format Configuration dialog box displays the following items:

Columns

Allow you to add the column name to the Column Order list box. In the case of application messages, you can only define whether the message does or does not include a Time or Date column.

Length

Allow you to specify the length of text that appears in the alarm or event message.

Column Order

Lists the order that you want each column to appear.

Up Arrow

Allows you to move a column up in the list. Select the column name and then use this button to move it up in the list.

Down Arrow

Allows you to move a column down in the list. Select the column name and then use this button to move it down in the list.

Message Length

The Message Length field allows you to specify the maximum number of characters that the printer can support. Valid entries are from 1-132. The default is 132.

Current Length

The Current Length field displays the number of characters that the printer currently supports.

Use Common Button

Allows you to set the alarm information and message format of the printer or service to the common format.

Network Alarm Configuration Dialog Box

This dialog box allows you to configure the Alarm Network Service to send start-up alarms to all of the client's enabled alarm destinations.

The Network Alarm Configuration dialog box displays the following item:

Send Startup Queue Alarms to Original Typers

Allows you to configure the Alarm Network Service to send start-up alarms to all of the client's enabled alarm destinations.

Network Configuration Dialog Box

This dialog box allows you to control network communications and security for this node. The Network Configuration dialog box displays the following items:

Network

Field	Description
No Network Support Option	Allows you to configure iFIX to operate as a stand-alone service.
TCP/IP Option	Allows you to select TCP/IP as the network protocol.

Options

Field	Description
Dynamic Connections Check Box	Allows you to establish dynamic connections on this node. Clear this check box if you want to connect only to nodes configured in the Configured Remote Nodes list. This feature is not available if you are setting up a stand-alone node.
Enforce Trusted Computing Check Box	Allows you to establish trusted computing on this node. Clear this check box if you want to use legacy network computing. This feature is not available if you are setting up a stand-alone node.
Network Password Field	Allows you set a password to create a site-specific certificate for network security. The default password (INETWORK) allows legacy network security to continue. This field is not available if you are setting up a stand-alone node.
Advanced Button	Allows you to display the Advanced Network Configuration dialog box, which allows you to configure network timers and LAN redundancy for your node. This button is available only when you enable Network support.

Remote Nodes

Field	Description
Remote Node Name	Displays the name of a remote node on the Local Area Network (LAN) that you are adding to the network configuration or have selected from the Configured Sessions list box.
Configured Remote Nodes List Box	Displays the names of the remote nodes on the Local Area Network (LAN) that this node can communicate with. Up to 100 nodes can be added.
Add Button	Allows you to add a remote node name entered in the Remote Node Name field to the Configured Remote Nodes list box.
Modify Button	Allows you to change the name of the currently selected remote node. Enter the new name in the Remote Node Name field and click Modify to change the name.

Field	Description
Delete Button	Allows you to remove a selected node from the Configured Remote Nodes list box. Select the node name in the list and click the Delete button.
Configure Button	Allows you to specify the remote node type so that iFIX can correctly interpret alarming information.
Show All Names Check Box	Allows you to display the primary and secondary nodes that have been configured for the logical nodes. Clear this check box to display only the logical node names.

Path Configuration Dialog Box

This dialog box displays the location and names of the iFIX directories. If you change the base path or project path names to a new path, the SCU creates the new directories for you. However, it will not copy the files from the old directories to the new directories.

If you are using terminal services, although project paths may be different, all users must share the same base and language paths. The default base path is C:\Program Files\Proficy\Proficy iFIX, while the default language path is C:\Program Files\Proficy\Proficy iFIX\NLS.

The Path Configuration dialog box displays the following items:

Base

Displays the main iFIX directory. Other iFIX directories are usually subdirectories of the base path.

Language

Displays the main directory for the language files used to create dialog boxes and help files. If you to choose to implement a native language other than English, the new language and help files replace the files found in this directory.

Project

Displays the path that you want to store application files, such as pictures, databases, and tag groups. This allows you to manage application files on a project-by-project basis. The default value for the Project Path is the base path.

Local

Displays the main directory for configuration files associated with the local computer.

Database

Displays the main directory for process databases, Database Builder configuration files, and I/O driver configuration files.

Picture

Displays the main directory for the following files:

- Picture files
- Dynamo files
- Tag group files
- Macro files
- Block status picture files
- Configuration files

Application

Displays the main directory for data and configuration files used by iFIX applications.

Historical

Displays the main directory for historical configuration files.

Historical Data

Displays the main directory for historical data files.

Alarms

Displays the main directory for alarm data files and security log files.

Master Recipe

Displays the main directory for master recipe, master recipe error, and master recipe report files.

Control Recipe

Displays the main directory for control recipe, control recipe error, and control recipe report files.

Alarm Areas (AAD)

Displays the main directory for alarm area files.

Change Base

Allows you to automatically update all the other subdirectories off the base path if you decide to

change it.

NOTE: If you change either the base path or one of the path names to a new path, the SCU creates the new directory for you. It does not copy the files from the old directory to the new directory.

Change Project

Allows you to automatically update all the other subdirectories off the Project path if you decide to change it.

NOTE: The Change Base button overrides the Change Project button. The Change Project button changes all paths within the PROJPATH root with the exception of the BASEPATH and NLSPATH.

Remote Alarm Areas Dialog Box

This dialog box allows you to select one or more alarm areas. The alarm areas you select are assigned to the outgoing alarms, enabling you to reassign the alarms selectively to new alarm areas before they are sent to the receiving node.

The Remote Alarm Areas dialog box displays the following item:

Remote Alarm Areas List

Allows you to select an alarm area from areas A-P, select all areas, or select no areas.

Remote Node Configuration Dialog Box

This dialog box allows you to enable the logical node name feature and specify primary and secondary node names for the logical node. You can also access the Timers dialog box by clicking the Timers button.

The Remote Node Configuration dialog box displays the following items:

Enable Logical Node Names

Allows you to enable the logical node name feature on the node.

Primary Node

Allows you to specify the name of the primary node. The node name you enter cannot already be listed in the Configured Remote Nodes list box. You also cannot enter the name of a node that is already entered as a primary node.

Secondary Node

Allows you to specify the name of the standby node. The node name you enter cannot already be listed in the Configured Remote Nodes list box. You also cannot enter the name of a node that is already entered as a standby node.

Timers

Allows you to display the Timers dialog box, which allows you to change the values of the network timers on your node

SCADA Configuration Dialog Box

This dialog box allows you to:

- Enable or disable SCADA support.
- Specify a database name.
- Add and delete I/O drivers.
- Access the Device Image Definition dialog box to configure a selected driver.

The SCADA Configuration dialog box displays the following items:

Enable

Enable Allows you to use this node as a SCADA node.

Disable

Disable Allows you to use this node as a View node.

Database Name

Allows you to specify the database to use for this node. You can also click the browse (...) button to access the File Open dialog box where you can search for database files (*.PDB) in the database path.

Database Browse (...) Button

Allows you to access the File Open dialog box where you can search for database files (*.PDB) in the database path.

I/O Driver Name

Displays the name of the driver you are adding, configuring, setting up, or deleting.

I/O Driver Name Browse (...) Button

Allows you to access the Drivers Available dialog box where you can select from a list of I/O drivers installed on this node.

Configured I/O Drivers

Displays the three-letter acronym and type of driver configured (CFE or SERIAL) for up to four I/O drivers configured on this node.

Add

Allows you to add a new I/O driver to the Configured I/O Drivers list box. Enter the acronym for the driver in the I/O Driver Name field or click the browse (...) button to access the Drivers Available dialog box where you can select from a list of I/O drivers installed on this node. Click the Add button to add the driver.

If you have more than one version of the specified driver, the SCU prompts you to specify which version of the driver you want to use.

Configure

Allows you to access the selected driver in order to configure it, or the selected driver's help.

Setup

Allows you to setup the I/O driver interface card. To configure the interface card, click the Setup button and enter the information requested. Not all drivers require an interface card. Refer to your I/O driver reference manual for more information.

Delete

Allows you to deletes an I/O driver from the Configured I/O Drivers list box. Select the driver in the list box and click the Delete button. This action does not delete any configuration work you have done with the I/O driver DID program or the I/O driver files stored on disk.

Failover

Field	Description
Enable	Select this check box to enable Enhanced Failover on this SCADA node.
Data Sync Transport	Click this button to open the Data Sync Transport dialog box, where you configure you network preferences for data transport.
Primary	Select this option if the node is the primary SCADA.
Secondary	Select this option if the node is the secondary SCADA.
Primary/Secondary SCADA Name	Enter the name of the partner SCADA node.

Field	Description
Maintenance Mode Security Area	If using security areas in iFIX, enter the letter associated with the security area assigned to administrators of your Enhanced Failover configurations. Only one security area is supported in Maintenance Mode.

Select the File Name to Use Dialog Box

This dialog box allows you to select the database file name currently defined for this node. The Select the File Name to Use dialog box displays the following item:

File Name

Enter or browse for the database name (.PDB file) to be used by this node. iFIX loads the database specified in this field during startup.

Send Alarm Filters Dialog Box

This dialog box allows you to select one or more alarm area and an alarm priority. Incoming block alarms are filtered based on the dialog box selections you make. Each alarm must meet the following criteria before the Auto Alarm Manager sends it to the receiving node:

- The alarm must be from one of the alarm areas selected from the Send Alarm Filters dialog box.

- The alarm must have an alarm priority greater than or equal to the alarm priority selected from the Send Alarm Filters dialog box.

If an alarm meets these criteria, the Auto Alarm Manager reassigns it to the alarm areas selected from the Remote Alarm Areas dialog box. Once reassigned, the Auto Alarm Manager delivers the alarm to the receiving node.

The Send Alarm Filters dialog box displays the following items:

Send Alarms from Area

Allows you to select an alarm area from areas A-P, select all areas, or select no areas.

Send Alarms of Priority

Allows you to select an alarm priority of Low, Medium, or High.

SQL Accounts Dialog Box

This dialog box allows you to control the SQL account information for this node. The SQL Accounts dialog box displays the following items:

Configured Accounts

Displays the names of SQL accounts that this node can access.

Add

Allows you to access the SQL Login Information dialog box and add a SQL account to the Configured Accounts list box.

Delete

Allows you to remove a selected SQL account from the Configured Accounts list box.

Configure

Allows you to re-configure login information for the SQL account selected in the Configured Accounts list box.

Configure SQL Task

Allows you to access the SQL Task Configuration dialog box, which lets you define how the SQL software option executes SQL commands. Fields in this dialog box allow you to define how data is handled when the SQL software option is operating.

SQL Login Information Dialog Box

This dialog box allows you to control how the iFIX SQL option communicates with a server containing a relational database. This dialog box lets you identify the:

- Type of database to which the SQL option connects (for example, Oracle, or Access).
- User name for the account to which you log into on the relational system.
- Password for the account.
- ODBC data source name.

The SQL Login Information dialog box displays the following items:

Database Type

Allows you to specify the type of relational database to which the SQL option can connect. Click the browse (...) button to display a list of supported relational databases.

Database Type Browse (...) Button

Allows you to display a list of supported relational databases.

User Name

Allows you to specify the name of the user's account on the server. This name is usually the same one you use to log onto the server. This field can be left blank or can contain a name with up to 31

characters.

Password

Allows you to specify the password used to log onto the server. This field can be left blank or can contain a password with up to 31 characters.

If you enter a user name, then most likely you are required to enter a password. As each character is entered, an asterisk appears in the Password field. This protects your password.

Database Identifier

Allows you to specify the ODBC data source name to which the SQL option can connect. Click the browse (...) button to display a list of ODBC data sources.

Database Identifier Browse (...) Button

Allows you to display a list of ODBC data sources.

SQL Task Configuration Dialog Box

This dialog box allows you to control how the SQL software option executes SQL commands. Fields in this dialog box allow you to define how data is handled when the SQL software option is operating.

The SQL Task Configuration dialog box displays the following items:

Enable

Allows you to enable the SQL software option. You must enable the SQL software option before you can enter information in the other configuration fields. When you change the SQL support state from disabled to enabled, the SQL task is added to the Task Configuration dialog box.

NOTE: The SQL software option does not check to see if the SCADA node is running. You must make sure your SCADA node is running before you can transfer or receive data from a relational database.

Disable

Allows you to disable the SQL software option. When you change the SQL support state from enabled to disabled, the SQL task is removed from the Task Configuration dialog box.

Primary Backup

Allows you to specify the primary back-up path and file name that the SQL software option uses when it cannot write to the relational database. If the SQL software option cannot connect to the server, or loses a connection with the relational database, it backs up data to the file identified in the Primary field. If the SQL software option fails to write to this file, it backs up data to the file identified in the Secondary field.

If you set the primary path to a file server, consider setting the secondary path to a local drive. With this setup, if the application cannot connect to the server because of a bad cable connection, the secondary path can back-up data to the local drive. Once the system re-establishes a connection to the

relational database, the system first processes any backed up SQL commands and data and then deletes the back-up file once the backup operation completes.

IMPORTANT: *The SQL software option processes backed up SQL commands in the order in which they were backed up. This means that the backed up SQL commands are processed in a first in, first out (FIFO) basis.*

You can enter any valid path and back-up file name in this field. A sample path and file name are shown below:

```
C:\Program Files\Proficy\Proficy iFIX\PDB\filename.SQL
```

NOTES:

- *The path that you enter does not have to be an iFIX path. If your path entry does not exist at runtime, no paths are created. This means that the SQL software option generates an error message because it tries to send back-up data to a file that is assigned no destination path.*

- *For SQT blocks to log to the primary or secondary backup files, you must select the Enable BackUp checkbox found on the Advanced tab. You must do this for each SQT block you want to utilize backup files.*

Secondary Backup

Allows you to specify the secondary back-up path and file name that the SQL software option uses when it cannot write to the relational database. If the SQL software option cannot connect to the server, or loses a connection with the relational database, it backs up data to the file identified in the Primary field. If the SQL software option fails to write to this file, it backs up data to the file identified in the Secondary field.

If you set the primary path to a file server, consider setting the secondary path to a local drive. With this setup, if the application cannot connect to the server because of a bad cable connection, the secondary path can back-up data to the local drive. Once the system re-establishes a connection to the relational database, the system first processes any backed up SQL commands and data and then deletes the back-up file once the backup operation completes.

IMPORTANT: *The SQL software option processes backed up SQL commands in the order in which they were backed up. This means that the backed up SQL commands are processed in a first in, first out (FIFO) basis.*

You can enter any valid path and back-up file name in this field. A sample path and file name are shown below:

```
C:\Program Files\Proficy\Proficy iFIX\PDB\filename.SQL
```

NOTES:

- *The path that you enter does not have to be an iFIX path. If your path entry does not exist at runtime, no paths are created. This means that the SQL software option generates an error message because it tries to send back-up data to a file that is assigned no destination path.*

- *For SQT blocks to log to the primary or secondary backup files, you must select the Enable BackUp checkbox found on the Advanced tab. You must do this for each SQT block you want to utilize backup files.*

Error Msg Routing

Allows you to access the Configure Alarm Areas - SQL Error Messages dialog box, which lets you enable the alarm areas that will receive error messages generated by the SQL software option.

Debug Msg Routing

Allows you to access the Configure Alarm Areas - SQL Debug Messages dialog box, which lets you enable the alarm areas that will receive debug messages generated by the SQL software option.

Error Msg to Screen

Allows you to control whether error messages are sent to the SQL system task window while the SQL software option is operating (enabled).

NOTE: If you enable the Debug Message to Screen option, the system automatically enables the Error Message to Screen option even if the Error Message to Screen check box is disabled.

Debug Msg to Screen

Allows you to control whether debug messages are sent to the SQL system task window while the SQL software option is operating (enabled).

Be aware that these messages are displayed in Mission Control, on the SQL tab.

NOTE: If you enable the Debug Message to Screen option, the system automatically enables the Error Message to Screen option even if the Error Message to Screen check box is disabled.

Database ID

Displays the ODBC data source name specified during ODBC setup. Any database specific information such as the server name or the database name is configured during the ODBC setup. Once the ODBC data source has been configured, only the data source name needs to be specified to access that relational database.

Database ID Browse (...) Button

Allows you to access the Database IDs Available dialog box, which lets you select from a list of available database identifiers.

SQL Cmd Table

Allows you to specify the name of the SQL Library Table that contains the SQL commands. The default name is SQLLIB. Valid SQL Command Table names can include up to 31 characters.

Error Log Table

Allows you to specify the name of the SQL Error Log Table to which the SQL system task sends error messages. If a SQL transaction fails, an entry is made to this table. In isolating troublesome SQL transactions, a maintained table becomes a useful debugging tool. Consider maintaining this log on an ongoing basis.

The default name for the Error Log Table is SQLERR. Valid Error Log Table names can include up to 31 characters. If no table name is entered in this field, the application records no error messages to the relational database.

NOTE: Completing the ERROR LOG TABLE field is optional.

Task Sleep Interval

Allows you to specify how often the SQL system task is processed (that is, how often it checks the SQT blocks in the node's database). You should enter a time that is sufficient to monitor your application. Valid entries are 0 to 99 seconds. The default is 5 seconds.

Startup Queue Configuration Dialog Box

This dialog box allows you to control the types of alarms a View node receives upon startup. By default, the View node receives all the current SCADA node summary alarms that have occurred prior to the time the View node started.

The Startup Queue Configuration dialog box displays the following items:

Enable Time Filter

Allows you to filter the alarms received by the View node by selecting the Enable Time Filter check box and entering a time interval. When you do this, the View node receives all current SCADA node alarms upon startup in addition to all previous alarms within the time interval you specify.

Filter Alarms Older Than – Hours

Allows you to specify the number of hours previous to startup in which you want to receive the SCADA node's alarms. Valid entries are from 0 to 23. The default is 23.

NOTE: The default setting, 23 hours and 59 minutes, displays all of the SCADA node's alarms that occurred between the time the View node started up and the previous day.

Filter Alarms Older Than – Minutes

Allows you to specify the number of minutes previous to startup in which you want to receive the SCADA node's alarms. Valid entries are from 0 to 59. The default is 59.

NOTE: The default setting, 23 hours and 59 minutes, displays all of the SCADA node's alarms that occurred between the time the View node started up and the previous day.

Summary Alarms Only

Allows you to receive only summary alarms on the View node. To display summary and operator alarms on the View node, clear the Summary Alarms Only check box.

NOTE: If this check box is cleared when using the Alarm Startup Queue, duplicate alarms will be displayed on all alarm destinations except alarm summary every time the connection to a SCADA node is established.

Task Configuration Dialog Box

This dialog box allows you to specify the tasks you want to automatically start when iFIX is started. iFIX executes the tasks in the order that they are listed in the Configured Tasks list box.

The Task Configuration dialog box displays the following items:

Filename

Displays the name of the executable (.EXE) or dynamically linked library (.DLL) that you are adding to or have selected from the Configured Tasks list box.

To add a new startup task, type a name in this field and click the Add button. You can also click the browse (...) button to access the File Open dialog box and search for executable or dynamically linked library files.

Command Line

Allows you to add any command line parameters associated with an executable file specified in the Filename field. For example, you can define command line parameters for SAC (WSACTASK.EXE), I/O Control (IOCNTRL.EXE), and selected iFIX applications.

To add command line parameters to third-party executables, check the application's reference documentation for valid entries.

Configured Tasks

Displays the names of the iFIX tasks selected for automatic startup. An asterisk (*) next to a task indicates that the task minimizes once it is started. A percent sign (%) next to a task indicates that the task is started as a background task.

iFIX executes the tasks in the order that they are displayed in this list box. To change the order of a startup task, select the task and use the up and down arrow buttons to move the task to the desired place in the list.

Minimized

Allows you to start the task with its window minimized.

Normal

Allows you to start the task with its window open.

Background

Allows you to start the task as a background task.

Add

Allows you to add an executable file specified in the Filename field to the Configured Tasks list box.

Change

Allows you to change the start up mode of a task selected in the Configured Tasks list box. To change the mode, select the task in the Configured Tasks list box, click the option button in the Start Up Mode area, and click the Change button.

Delete

Allows you to delete a task from the Configured Tasks list box. To delete a task, select the task in the list box and click the Delete button. This action removes the task from the list, but does not delete the files from the disk.

Timers Dialog Box

This dialog box allows you to change the values of the network timers on the remote node. iFIX uses your entries in this dialog box to tailor resources precisely for your configuration. Most users never need to modify these defaults.

CAUTION: Modifying network resources can seriously affect the performance of a node. You should not use this dialog box unless you have a thorough understanding of iFIX networking concepts. See the Understanding iFIX Session Timers and Determining Session Timer Values sections in the Setting up the Environment electronic book for more information on network timers.

The Timers dialog box displays the following items:

Use FIX Network Timers

Allows you to enable the use of network timers on the remote node.

Keep Alive

Allows you to specify the amount of time that, if no activity has occurred over an established connection, the node waits before sending a heartbeat message. The default value for this field is 20 seconds.

Send

Allows you to specify the amount of time that the node waits for a request to the SCADA server to be acknowledged. If this timer expires, the session ends. The default value for this field is 30 seconds.

Receive

Allows you to specify the amount of time that the node waits for a reply from the SCADA server. When running iFIX over TCP/IP, the effective session timeout values is either the Send timer or the Receive timer, whichever is greater. If this timer expires, the session ends. The default value for this field is 60 seconds.

Inactivity

Allows you to specify the amount of time that, if no data activity has occurred over an established connection, the node waits before removing the dynamic connection from the list of outgoing

connections. If this timer expires, the session ends. The default value for this field is 300 seconds.

Reset to Defaults

Allows you to reset the remote node network timers to their default values.

How Do I...

The following sections explain how to use the System Configuration Utility (SCU) in iFIX:

- Working with SCU Files
- Working with SCADA Support
- Configuring Paths
- Using Alarms
- Working with Networks
- Using SQL
- Configuring Tasks
- Working with the Alarm Area Database
- Configuring the Auto Alarm Manager
- Defining Local Startup Settings

Click a section above for steps on how to use or configure this part of the SCU.

Working with SCU Files

In the SCU, you can perform the following steps with SCU Files:

- Adding a File Description to the SCU File
- Creating an SCU File Report
- Implementing the SCU in iFIX

Adding a File Description to the SCU File

▶ **To add a description to the SCU file:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. In the SCU, on the File menu, click Description, or double-click the file description area.

3. In the Enter Configuration File Description field, enter a description of up to 40 characters.

Creating a SCU File Report

▶ **To create a SCU file report:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

    -Or-

    In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the File menu, click Report.

3. In the File Name field, enter a file name and click the Save button.

Implementing the SCU in iFIX

▶ **To implement the SCU in iFIX:**

1. Before you open the iFIX WorkSpace, start the SCU from the Proficy iFIX 4.0 program folder in Windows.

2. From the Configure menu, choose Local Startup. The Local Startup Definition dialog box appears.

3. Configure your local startup options, including the local server name, local logical name, and the local SCU file name.

4. Configure the path in which to store the program and data files.

5. Make any start-up or configuration changes using the SCU toolbox and associated dialog boxes. For more information, refer to the Configuring iFIX using the SCU section in the Setting up the Environment e-book.

6. Save any configuration changes to either a local disk or a remote file server.

Working with SCADA Support

In the SCU, you can perform the following steps with SCADA Support:

*   Adding an I/O Driver to the Configured I/O Drivers List Box

*   Configuring an I/O Driver

*   Deleting an I/O Driver from the Configured I/O Drivers List Box

*   Selecting a Process Database

Adding an I/O Driver to the Configured I/O Drivers List Box

▶ **To add an I/O Driver to the Configured I/O Drivers list box:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

    -Or-

In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the SCADA button.

3. Next to the I/O Driver Name field, click the browse (...) button to display a list of I/O drivers installed on the local node. The Drivers Available dialog box appears.

4. Select the driver you want and click OK. The driver appears in the I/O Driver Name field.

5. Click the Add button. The SCU adds the I/O driver to the Configured I/O Drivers list box. Only drivers added to this list box are started during iFIX startup.

    NOTE: During installation, the Simulation (SIM) driver is automatically installed for you. This driver provides 2000 registers for simulating process data and testing your database. Refer to the Building a SCADA System e-book for more information on using the SIM driver.

Configuring an I/O Driver

▶ To configure an I/O driver:

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

    -Or-

    In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the SCADA button.

3. Select a driver in the Configured I/O Drivers list box and click the Configure button. This starts the I/O Driver Configuration program.

4. Enter the required information.

    NOTE: You do not need to set up a SIM driver; the installation program configures it for you. For more information on the configuration program, refer to your driver documentation.

Deleting an I/O Driver from the Configured I/O Drivers List Box

▶ To delete an I/O driver from the Configured I/O Drivers list box:

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

    -Or-

    In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the SCADA button.

3. From the Configured I/O Drivers list, select the I/O driver.

4. Click the Delete button.

Enabling and Disabling SCADA Support

▶ To enable and disable SCADA support:

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the SCADA button.

3. In the SCADA Support area, select the Enable option.

4. To disable SCADA support, select the Disable option.

Selecting a Process Database

▶ **To select a process database:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the SCADA button.

   - Or -

   On the SCU main screen, double-click the PDB:DATABASE row.

3. In the Database Name field, enter the desired process database. If you want to use an existing database, click the browse (...) button to search for database files for your server using the Select the File Name to Use dialog box.

Configuring Paths

In the SCU, you can perform the following steps with Paths:

- Changing the Base Path
- Changing the Project Path
- Defining the Alarm Areas Path

Changing the Base Path

▶ **To change the base path:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Paths button.

3. In the Base field, enter a new directory path or click the browse (...) button to browse for a directory.

4. Click the Change Base button to automatically update all of the directories in the Path Configuration dialog box.

   NOTE: All of the other directories must be subdirectories of the Base path in order for them to change automatically.

Changing the Project Path

▶ **To change the project path:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Paths button.

3. In the Project field, enter a new path or click Browse to browse for a project path.

4. Click the Change Project button to automatically update all of the project file directories in the Path Configuration dialog box.

   NOTE: All of the other project file directories must be subdirectories of the Project path in order for them to change automatically. The Base and Language paths are not updated when you change the project path.

Defining the Alarm Areas Path

▶ **To define the Alarm Areas path:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Paths button.

3. Enter the file server path containing the alarm area database in the Alarm Areas path.

Using Alarms

In the SCU, you can perform the following steps with Alarms:

- Assigning Common Alarm Areas to an Alarm Service
- Assigning Every Alarm Area to an Alarm Service
- Assigning Every Alarm Area to Application Messages
- Assigning Specific Alarm Areas to an Alarm Service

- Assigning Specific Alarm Areas to Application Messages

- Configuring Alarm Areas

- Configuring an Alarm Printer Service

- Configuring the Alarm File Service

- Configuring the Alarm History Service

- Configuring the Alarm ODBC Service

- Configuring the Alarm Startup Network Service

- Configuring the Alarm Startup Queue Service

- Configuring the Alarm Startup Summary Service

- Configuring the Message Format

- Configuring the Alarm Horn in the SCU

- Customizing the Common Message Format for an Alarm Service

- Defining a Common Message Format

- Disabling an Alarm Destination

- Enabling an Alarm Destination

- Entering the Retry, Pause, and Delay Intervals

- Entering the Alarm ODBC Queue Size

- Enabling an Alarm Queue's Size

- Selecting Common Alarm Areas

- Selecting Common Alarm Areas Not Listed in the Database

- Selecting the Common Message Format for and Alarm Service

- Viewing the Alarm History of the Local Node

- Selecting the Alarm Areas for Incoming and Outgoing Alarms

Assigning Common Alarm Areas to an Alarm Service

▶ **To assign the common alarm areas to an alarm service:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Alarms button.

3. Double-click the alarm service you want to set up.

4. Click the Areas button.

5. Select the Use Areas Common to All Services option.

Assigning Every Alarm to an Alarm Service

▶ **To assign every alarm area to an alarm service:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Alarms button..

3. Double-click the alarm service you want to set up.

4. Click the Areas button.

5. Select the Use ALL Alarm Areas option.

Assigning Every Alarm Area to Application Messages

▶ **To assign every alarm area to application messages:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Alarms button.

3. Click the Advanced button.

4. Click the Recipe Messages button to assign alarm areas for recipe messages, or the Operator Messages button to assign alarm areas for any other type of application message. When you click either button, the Configure Alarm Areas dialog box appears.

5. Select the Use ALL Alarm Areas option to assign the messages to every alarm area.

Assigning Specific Alarm Areas to an Alarm Service

▶ **To assign specific alarm area to an alarm service:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Alarms button.

3. Double-click the alarm service you want to set up.

4. Click the Areas button.

5. Select the "Select from the Alarm Areas Database" option.

6. From the Available Areas list, double-click the alarm areas you want to assign.

Assigning Specific Alarm Areas to Application Messages

▶ **To assign specific alarm areas to application messages:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Alarms button.

3. Click the Advanced button.

4. Click the Recipe Messages button to assign alarm areas for recipe messages, or the Operator Messages button to assign alarm areas for any other type of application message. When you click either button, the Configure Alarm Areas dialog box appears.

5. Select the "Select from the Alarm Areas Database" option.

6. From the Available Areas list, double-click the alarm areas you want.

Configuring an Alarm Printer Service

▶ **To configure an Alarm Printer Service:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Alarms button.

3. Double-click the Alarm Printer Service.

4. In the Port Definition areas, click the option button for the printer port to which your printer is connected. Each port can handle only one Alarm Printer Service. If a port selection is not selectable, it is assigned to another printer.

5. In the Printer Name field, enter a printer name.

6. Select the printer's alarm areas.

7. Select the printer's message format.

Configuring the Alarm File Service

▶ **To configure the Alarm File Service:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2.   On the SCU toolbox, click the Alarms button.

3.   Double-click the Alarm File Service.

4.   Click the Format button.

5.   Click the Area button to display the Configure Alarm Areas dialog box, and select the service's alarm areas.

6.   Click the Format button to display the Alarm File Service Message Format Configuration dialog box, and select the service's message format.

Configuring the Alarm History Service

▶ **To configure the Alarm History Service:**

1.   In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2.   On the SCU toolbox, click the Alarms button.

3.   Double-click the Alarm History Service.

4.   Click the Area button.

5.   Select the service's alarm areas and click OK.

6.   Click the Format button.

7.   Configure the desired options for the service's message format and click OK.

Configuring the Alarm ODBC Service

▶ **To configure the Alarm ODBC Service:**

1.   In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2.   On the SCU toolbox, click the Alarms button.

3.   Double-click the Alarm ODBC Service.

4.   Click the Configure button.

5.   Enter the SQL login information required to connect to your relational database. If you want to use the existing SQL configuration, select the Use Login Information from SQL Configuration check box.

6.   Configure the column and table names for the relational database. If you want to use your own column and table names, enter them instead.

7. Select the Allow Operator to Pause Alarm Logging check box to let operators temporarily stop writing to the relational database.

8. In the Update Interval field, enter the number of seconds the service should wait between writes to the relational database. At each write, the service will check the iFIX AlarmQueue and the Lost Connection File.

9. In the AlarmQueue Size field, enter the maximum number of records in the iFIX AlarmQueue.

10. In the Number of records to log from iFIX field, enter the number of records to write to the relational database at one time from the iFIX AlarmQueue.

11. In the Number of records to log from Backup File field, enter the number of records to write to the relational database at one time from the Lost Connection File.

12. In the Lost Connection Options section, enter the path where you want to save your backup file and the tag that will indicate a broken connection with the relational database. Alternatively, instead of entering a tag here, you can create an Alarm ODBC watch dog using the Scheduler. For more information, refer to the Creating an Alarm ODBC Watchdog Using the Scheduler section.

13. In the User Fields section, edit the ASCII format database blocks for any user defined iFIX field names you selected.

14. Click OK.

Configuring the Alarm Startup Network Service

▶ **To configure the Alarm Network Service:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Alarms button.

3. Double-click the Alarm Network Service.

   NOTE: *Networking must be enabled in the Network Configuration dialog box for the Alarm Network Service to appear in this list.*

4. Select the Send Startup Queue Alarms to Original Typers check box to distribute alarms from the SCADA server to all the enabled alarm destinations on the View client. Clear the check box if you want to send the alarms to the Alarm Summary and Alarm Startup Queue Services, or if the Alarm Queue Service is disabled.

5. Click OK.

Configuring the Alarm Startup Queue Service

▶ **To configure the Alarm Startup Queue Service:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

-Or-

In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Alarms button.

3. Double-click the Alarm Startup Queue Service.

NOTE: The Alarm Startup Queue Service only appears in the alarm configuration list if networking is enabled in the SCU. To enable networking from the SCU, close the Alarm Configuration dialog box, and on the Configure menu, click Network. The Network Configuration dialog box appears. In the Network area, select the network type. Once networking is enabled, you can try to configure the Alarm Startup Queue Service again.

4. In the Startup Queue Configuration dialog box, clear the Summary alarms only check box to receive alarms and messages. To receive only alarms from the Alarm Summary Service, leave the check box selected.

5. If you want to filter alarms by time, select the Enable Time Filter check box and enter the maximum age of the alarms and messages you want to receive in the Hours and Minutes fields.

6. Click OK.

Configuring the Alarm Startup Summary Service

▶ **To configure the Alarm Summary Service:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Alarms button.

3. Double-click the Alarm Summary Service.

4. If you want to manually delete alarms from the Alarm Summary Service, select the Manual option. Otherwise, select the Automatic option.

5. Select the service's alarm areas.

6. Click OK.

Configuring the Message Format

When working with message formats, you can:

- Select the common message format.
- Customize the message format.

Configuring the Alarm Horn in the SCU

▶ **To configure the Alarm Horn in the SCU:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Alarms button.

3. Double-click the Alarm Summary Service.

   NOTE: If it is disabled, select the Enable option in the upper right corner of the screen to enable the service, and then double-click Alarm Summary Service

4. In the Horn Support section, select the Enable or Disable option.

5. Click OK to close the dialog box and return to the Alarm Configuration dialog box.

6. Click OK to close the dialog box and save the changes.

Customizing the Common Message Format for an Alarm Service

▶ **To customize the message format for an alarm service:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Alarms button.

3. Double-click the alarm service you want to set up.

4. Click the Format button.

5. Select the check boxes in the Columns area to include the fields you want. To exclude a field, clear its check box.

6. In the Length fields, enter the length of each field.

7. From the Column Order list, select a field name.

8. Click one of the arrow buttons to move the field up or down in the list.

9. Repeat steps 6 and 7 until you arrange the fields in the order you require.

10. Click OK.

Defining a Common Message Format

▶ **To define a common message format:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Alarms button.

3. Click the Advanced button.

4. Click the Common Format button.

5. In the Columns area, select the check boxes of the necessary fields to include in the common format. To exclude a field, clear its check box.

6. In the Length fields, enter the length of each field.

7. From the Column Order list, select a field name.

8. Click the up or down arrow buttons to move the field in the list.

9. Repeat steps 6 and 7 to arrange the fields in the order you require.

10. Click OK.

Disabling an Alarm Destination

▶ **To disable an alarm destination:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

    -Or-

    In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Alarms button.

3. Select an alarm service and click Disable.

4. Click OK.

Enabling an Alarm Destination

▶ **To enable an alarm destination:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

    -Or-

    In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Alarms button.

3. Select an alarm service and click Enable.

4. Click OK.

Entering the Retry, Pause, and Delay Intervals on the Sender Node

▶ **To enter the retry, pause, and delay intervals on the sender node:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

-Or-

In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the Configure menu, click Auto Alarm Manager.

3. Make sure the Enable button is selected, so that you can edit the fields.

4. In the Max Retries field, enter the maximum number of times you want the Auto Alarm Manager to re-dial the primary or secondary contact.

5. In the Pause Time field, enter the number of seconds you want the Auto Alarm Manager to pause between retries.

6. In the Delay After Send field, enter the number of seconds you want the Auto Alarm Manager to wait between hanging up the modem and dialing the receiving node again.

7. Click OK.

Entering the Alarm ODBC Queue Size

▶ **To enter the Alarm ODBC queue size:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Alarms button.

3. Double-click the Alarm ODBC service.

4. Click the Configure button.

5. In the Alarm Queue Size field, enter the alarm queue size.

6. Click OK.

Modifying an Alarm Queue's Size

▶ **To modify an alarm queue's size:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

   The System Configuration Utility (SCU) window appears.

2. On the SCU toolbox, click the Alarms button. The Alarm Configuration dialog box appears.

3. Select the Advanced button. The Advanced Alarm Configuration dialog box appears.

4. Click the Queue Configuration button and click Yes when prompted to continue. The Alarm Queues Configuration dialog box appears.

5. In the Maximum field, enter the alarm queue size. If you are configuring the Alarm History queue, enter the queue size In the Initial field.

6. Click OK.

Selecting Common Alarm Areas

▶ **To select common alarm areas:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

    -Or-

    In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Alarms button.

3. Click the Advanced button.

4. Click the Common Areas button.

5. Select the Select from Alarm Area Database option.

6. In the Available Areas list, double-click the alarm areas you want to make common. This moves the alarm area to the Configured Areas list.

7. Click OK.

Selecting Common Alarm Areas Not Listed in the Database

▶ **To select a common alarm area that is not listed in the alarm area database:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

    -Or-

    In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Alarms button.

3. Double-click the alarm service you want to set up.

4. Click the Areas button.

5. Select the Select from Alarm Area Database option.

6. In the Add field, enter the area's name and click the Add button.

7. Click Yes when prompted to use the undefined name.

Selecting the Common Method Format for an Alarm Service

▶ **To select the common message format for an alarm service:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

-Or-

In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Alarms button.

3. Double-click the alarm service you want to set up.

4. Click the Format button.

5. Click the Use Common button.

Viewing the Alarm History of the Local Node

▶ **To view the alarm history of the local node:**

- From the system tree in the Proficy iFIX WorkSpace, double-click the Alarm History icon.

Selecting the Alarm Areas for Incoming and Outgoing Alarms

▶ **To select the alarm areas for incoming and outgoing alarms:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the Configure menu, click Auto Alarm Manager.

3. Make sure the Enable button is selected, so that you can edit the fields.

4. Click the Alarm Filters button.

5. Select the alarm areas and alarm priorities with which to filter the incoming alarms.

6. Click OK.

7. Click the Remote Alarms Areas button.

8. Select the alarm areas you want to assign to the outgoing alarms.

9. Click OK.

Working with Networks

In the SCU, you can perform the following steps with Networks:

- Activating Network Timers on a Per Node Basis

- Adding Remote Nodes to your Network Configuration

- Changing the Network Protocol

- Configuring iFIX Session Timers

- Adding or Removing Networking Support in iFIX

- Disabling a Network Path

- Enabling Dynamic Connections

- Enabling Trusted Computing

- Creating Site-Specific Certificates

- Modifying a Remote Node on the Network

- Re-enabling a Network Path

- Removing a Node from the Configured Remote Nodes List

- Modifying a Diagnostic Display to Reference a Local Node Name

Activating Network Timers on a Per Node Basis

▶ **To activate network timers on a per-node basis:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Network button.

3. From the Configured Remote Nodes list, select the node you want to configure.

4. Click the Configure button.

5. Click the Timers button. .

6. Click the Reset to Defaults button to use the default timer settings, or clear the Use FIX Network Timers check box and enter values in the Seconds field for the network timers you want to activate.

7. Click OK to close the Timers dialog box.

8. Click OK again to close the Remote Node Configuration dialog box.

9. Click OK.

Adding Remote Nodes to your Network Configuration

▶ **To add remote nodes to your network configuration:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Network button.

3. In the Remote Node Name field, enter the remote node name.

4. Click the Add button. The node name is added to the Configured Remote Nodes list. If there is more than one node, the last entry is placed at the bottom of the list.

Adding or Removing Networking Support in iFIX

▶ **To add or remove networking support in iFIX:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Network button.

3. In the Network area, click the TCP/IP option to allow for TCP/IP networking, or click the No Networking Support option to remove the networking option.

4. Click OK.

Configuring iFIX Session Timers

▶ **To configure the iFIX session timers:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Network button.

3. Click the Advanced button and click Yes when prompted to continue.

4. Edit the Seconds field of the session timer that you want to change.

5. Click OK.

Configuring Network Protocols

▶ **To configure the network protocol:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Network button.

3. In the Network area, click TCP/IP to configure the network protocol. If you do not want to be connected to a network, click No Network Support. This option configures iFIX to operate as a stand-alone server.

4. Click OK.

Disabling a Network Path

▶ **To disable a network path:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

    -Or-

    In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Network button.

3. Click the Advanced button and click Yes when prompted to continue.

4. From the Available Paths list, select the path that you want to disable.

5. Select the Disable option.

6. Repeat steps 4 and 5 for all network paths that you want to disable.

7. Click OK.

Enabling Dynamic Connections

▶ **To enable dynamic connections:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

    -Or-

    In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Network button.

3. In the Options area, select the Dynamic Connections check box.

4. Click OK.

Enabling Trusted Computing

▶ **To enable trusted computing:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

    -Or-

    In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Network button.

3. In the Options area, select the Enforce Trusted Computing check box to enable connection authentication security and packet encryption for the network.

4. Click OK.

Creating Site-Specific Certificates

▶ **To create a site-specific certificate:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Network button.

3. In the Network Password field, enter a password to create a site-specific certificate for secure networking.

4. Click OK.

Modifying a Remote Node on the Network

▶ **To modify a remote node on the network:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Network button.

3. From the Configured Remote Nodes list, select the node you want to modify.

4. Click the Modify button.

Re-enabling a Network Path

▶ **To re-enable a network path:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Network button.

3. In the Network area, select TCP/IP.

4. Click the Advanced button and click Yes when prompted to continue.

5. From the Available Paths list, select the path that you want to re-enable.

6. Select the Enable option.

7. Repeat steps 5 and 6 for all network paths that you want to re-enable.

8. Click OK.

Removing a Node from the Configured Remote Nodes List

▶ **To remove a node from the Configured Remote Nodes list:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Network button. The Network Configuration dialog box appears.

3. From the Configured Remote Nodes list, select the logical node name that you want to delete.

4. Click the Delete button.

5. Click OK to save your settings.

Modifying a Diagnostic Display to Reference a Local Node Name

▶ **To modify a diagnostic display to reference a local node name:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. Open the diagnostic display in the Proficy iFIX WorkSpace.

3. In the iFIX WorkSpace, on the Edit menu, click Select All.

4. In the iFIX WorkSpace, on the Edit menu, click Find and Replace. The Find and Replace dialog box appears.

5. In the Find What field, enter *.* and click the Find button.

6. Click the Replace tab and enter *local_nodename*.* in the Replace With field, where *local_nodename* is your local node name.

7. Click the Replace All button. To preview the results of Find and Replace beforehand, click the Replace Preview button.

Using SQL

In the SCU, you can perform the following steps with SQL:

- Adding Command Parameters for the SQL Task
- Configuring the SCU for an ODBC Data Source
- Configuring the SQL Task
- Displaying the Setup and Status of iFIX ODBC
- Setting the Reference to the Microsoft DAO Object Library

- Setting the Reference to the Microsoft Remote Data Object Library

- Entering Your Own Table and Column Names

Adding Command Parameters for the SQL Task

▶ **To add command parameters for the SQL task:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Tasks button.

3. In the Configured Tasks list, select the SQL task, WSQLODC.EXE. The SQL task appears in the filename field.

4. In the Command Line field, enter the command parameters.

5. Click the Change button.

Configuring the SCU for an ODBC Data Source

▶ **To configure an ODBC data source:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the SQL button.

3. Click the Add button.

4. In the Database Type field, enter the type of data source, or click the browse (...) button to display the Database Types Available dialog box. Select the database type from the list in the dialog box, and click OK.

5. In the Database Identifier field, enter a database ID, or click the browse (...) button next to the Database Identifier field to display the Database IDs Available dialog box. Select a database ID from the list in the dialog box, and click OK.

6. In the User Name and Password fields, enter a valid user name and password for the database you want to access. If you are accessing a Microsoft Access data source and security is disabled, leave the User Name and Password fields blank.

7. Click OK.

Configuring the SQL Task

▶ **To configure the SQL task:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on

the toolbar.

-Or-

In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the SQL button.

3. Click the Configure SQL Task button.

4. Complete the SQL Task Configuration dialog box, as desired.

   NOTE: When using the confirm tag for an SQT block that is triggered by an event, make sure that you define the security so that users do not have access to Mission Control to shut down the SQL task.

5. Click OK.

Displaying the Setup and Status of iFIX ODBC

▶ **To display the setup and status of iFIX ODBC:**

1. In Classic view, from the Application toolbar in the iFIX WorkSpace, click the Mission Control icon.

   -Or-

   In Ribbon view, on the Applications tab, in the Utilities group, click Mission Control.

2. Click the SQL tab.

3. Click the Status button.

Setting the Reference to the Microsoft DAO Object Library

▶ **To set the reference to the Microsoft DAO object library:**

1. In Classic view, from the iFIX WorkSpace, click the Visual Basic Editor button on the toolbar.

   -Or-

   In Ribbon view, on the Home tab, in the WorkSpace group, click Visual Basic Editor.

2. On the Tools menu, click References.

3. Select the Microsoft DAO Object 3.51 or 3.6 Library check box.

4. Click OK.

Setting the Reference to the Microsoft Remote Data Object Library

▶ **To set the reference to the Microsoft Remote Data Object library:**

1. In Classic view, from the iFIX WorkSpace, click the Visual Basic Editor button on the toolbar.

-Or-

In Ribbon view, on the Home tab, in the WorkSpace group, click Visual Basic Editor.

2. On the Tools menu, click References.

3. Select the Microsoft Remote Data Object 2.0 check box.

4. Click OK.

Entering Your Own Table and Column Names

▶ To enter your own table and column names:

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. Click the Alarm button on the SCU toolbox.

3. Select the Alarm ODBC Service and the Enabled option.

4. Click Modify.

5. Click Configure.

6. In the Database Configuration area, in the Table Name field, enter the name of the table to which you want to archive your alarms and messages.

7. Select the Create Tables at Runtime If Not Found check box to create the table automatically when it cannot be found.

8. From the Column Configuration area, select the alarm and message fields you want to archive.

   - Click Select All to select all the iFIX Field Names and populate the SQL Column Names automatically.

   - Click Clear All to deselect all the iFIX Field Names. The SQL Column Names remain populated.

   - Click Restore Defaults to use the FIXALARMS table to select the iFIX Field Names and the corresponding SQL Column Names.

   TIP: If you select any of UserField iFIX Field Names, you can edit the database blocks in the User Fields section of the dialog box.

9. In the Database Configuration area, click Create Table Now to create the table when you configure the service.

10. Optionally, enter the column name that will store each selected field's information in the second column of the spreadsheet.

    IMPORTANT: If you later change the table configuration through this dialog box, you must rename the table and press the Create Table Now to create it again. You cannot modify an existing table through this dialog box; you must create a new one to change the existing configuration.

11. Click OK.

Configuring Tasks

In the SCU, you can perform the following steps with Task Configuration:

- Configuring a Task to Run in the Background

- Configuring a Task to Start Automatically

- Configuring Drivers to Start Automatically

- Configuring SAC to Start Automatically

Configuring a Task to Run in the Background

▶ **To configure a task to run in the background:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Tasks button. .

3. Click the browse (...) button next to the Filename field.

4. Select the desired file and click the Open button. The selected file appears in the Filename field.

5. In the Startup Mode area, click the Background option button.

6. In the Command Line field, enter any command line parameters you may need.

7. Click the Add button to add the task to the Configured Tasks list box.

8. Click OK.

Configuring a Task to Start Automatically

▶ **To configure a task to start automatically:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Tasks button.

3. Click the browse (...) button next to the Filename field.

4. Select the desired file and click the Open button. The selected file appears in the Filename field.

5. In the Startup Mode area, click the Normal option button to start the task as an open window, the Minimized option button to start the task as a minimized window, or the Background option button to start the task in the background.

6. In the Command Line field, enter any command line parameters you may need.

7. Click the Add button to add the task to the Configured Tasks list box.

8. Click the up or down arrow buttons to move the task in the list.

9. Click OK.

Configuring Drivers to Start Automatically

▶ **To configure I/O drivers to start automatically:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Tasks button.

3. In the Filename field, enter the full path of the I/O control task.

4. In the Command Line field, enter the appropriate command line parameters. If you enter more than one parameter, separate each parameter with a space.

5. In the Start Up Mode area, click the Background option button.

6. Click the Add button.

7. Click OK.

Configuring SAC to Start Automatically

▶ **To configure SAC to start automatically:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Tasks button.

3. In the Filename field, enter the full path of the SAC task and click the Add button.

4. To modify how SAC operates, enter the appropriate command line parameters in the Command Line field.

5. Click OK.

Working with the Alarm Area Database

In the SCU, you can perform the following steps with the Alarm Area Database:

- Creating an Alarm Area

- Deleting an Alarm Area

- Renaming an Alarm Areas
- Sharing an Alarm Area Database with a File Server
- Editing Alarm Areas in the Database

Creating an Alarm Area

▶ **To create an alarm area:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Alarm Area Database button.

3. In the Alarm Area field, enter the name you want to use and click the Add button.

4. Click OK.

Deleting an Alarm Area

▶ **To delete an alarm area:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Alarm Area Database button.

3. From the Configured Alarm Areas list, select the alarm area you want to delete.

4. Click the Delete button.

5. Click OK.

Renaming an Alarm Area

▶ **To rename an alarm area:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the SCU toolbox, click the Alarm Area Database button.

3. From the Configured Alarm Areas list, select the alarm area you want to rename.

4. In the Alarm Area field, enter the new name and click the Modify button.

5. Click OK.

Sharing an Alarm Area Database with a File Server

▶ **To share an alarm area database with a file server:**

1. Create your own alarm areas:

   a. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

      -Or-

      In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

   b. On the SCU toolbox, click the Alarm Area Database button.

   c. In the Alarm Area field, enter the name you want to use and click the Add button.

   d. Click OK.

2. In Windows, copy the ALARMAREAS.AAD file from the Alarm Areas path to your file server.

3. In the SCU, on the Configure menu, click Paths.

4. In the Alarm Areas (AAD) field, enter the file server path containing the alarm area database.

5. Repeat steps 3-4 on each iFIX node.

Editing Alarm Areas in the Database

When editing alarm areas in the database, you can:

- Create an alarm area.

- Rename an alarm area.

- Delete an alarm area.

Configuring the Auto Alarm Manager

In the SCU, you can perform the following steps with Auto Alarm Manager:

- Defining Security Rights for the Auto Alarm Manager

- Enabling TCP/IP Networking for the Auto Alarm Manager

- Configuring the Auto Alarm Manager on the Sending Node

- Configuring the Auto Alarm Manager on the Receiving Node

- Entering the Names of the Database Tags You Want to Use

- Setting Up the Auto Alarm Manager Timers

- Configuring the Auto Alarm Manager as a Service

Defining Security Rights for the Auto Alarm Manager

▶ **To define security rights for the Auto Alarm Manager:**

1. In the iFIX Security Configuration application, create a user account with the login name AALARM.

2. Assign a password to the account.

3. Assign all security areas to the account.

4. Repeat steps 1 through 3 on all nodes running the Auto Alarm Manager.

   NOTE: For more information on creating user accounts and the iFIX Security Configuration application, refer to the Configuring Security Features e-book.

Enabling TCP/IP Networking for the Auto Alarm Manager

▶ **To enable TCP/IP networking on the Sender and Receiver nodes:**

1. Shut down iFIX if it is running.

2. On the Start menu, point to Programs, Proficy HMI SCADA - iFIX, and then System Configuration. The SCU application appears.

3. On the Configure menu, click Network. The Network Configuration dialog box appears.

4. In the Network group box, select the TCP/IP option.

5. Click OK.

   NOTE: It does not matter whether you have the Dynamic Connections check box selected or Remote Nodes added to the list box. The Auto Alarm Manager will work with any settings here.

6. On the File menu, click Save.

7. Exit the SCU.

   NOTE: Be sure to repeat steps 1-7 on both the Sender and Receiver nodes.

Configuring the Auto Alarm Manager on the Sending Node

▶ **To configure the Auto Alarm Manager on the Sending node:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the Configure menu, click Auto Alarm Manager.

3. Select the Enable option.

4. Optionally, in the Disable Tagname field, enter the name of the database tag you that you want to enable or disable the automatic sending of alarms during runtime. Typically, you would use a Digital Output (DO) block type for this tag.

5. In the Primary and Secondary Contact fields, enter the name of the primary and secondary contacts from your RAS phonebook. Use the browse (...) button to browse possible selections. The Secondary Contact field is optional.

6. In the Emergency Tagname field, enter the name of the database tag you want to use. Typically, you would use a Digital Output (DO) block type for this tag.

7. In the Max Retries field, enter the maximum number of times you want the Auto Alarm Manager to re-dial the primary or secondary contact.

8. In the Pause Time field, enter the number of seconds you want the Auto Alarm Manager to pause between retries.

9. In the Delay After Send field, enter the number of seconds you want the Auto Alarm Manager to wait between hanging up the modem and dialing the Receiving node again with new alarms.

10. Configure alarm filters:

    a. Click the Remote Alarm Areas button to specify the alarm areas assigned to the outgoing alarms, enabling you to reassign the alarms selectively to new alarm areas before they are sent to the Receiving node.

    b. Click the Alarm Areas button to select one or more alarm areas and an alarm priority for incoming alarms, for alarm filtering purposes.

11. In the Acknowledged Delivered Alarms area, click Yes to enable the Auto Alarm Manager to acknowledge alarms automatically.

12. If iFIX is running as a service, click the Advanced button to specify a Windows account and password in the Advanced Send Alarm Settings dialog box. For more information, refer to the Configuring the Auto Alarm Manager as a Service section.

13. If you want to configure more efficient communication intervals, click the Advanced button to specify a Sender and Receiver time-out in the Advanced Send Alarm Settings dialog box. For more information, refer to the Configuring Auto Alarm Manager Timers section.

    By specifying these time-out intervals, you can configure how long the Auto Alarm Manager has to send alarms to the receiving server, and whether to flush alarm queues upon successful or unsuccessful delivery.

14. Click OK.

Configuring the Auto Alarm Manager on the Receiving Node

▶ **To configure the Auto Alarm Manager on the Receiving node:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

    -Or-

    In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the Configure menu, click Auto Alarm Manager.

3. In the Receive Alarms area, select the Enable option.

4. In the Receiving Tagname field, enter the name of the receiving tag. Typically, you would use a Digital Output (DO) block type for this tag.

5. Click OK.

IMPORTANT: *The Auto Alarm Manager TCP only communicates over TCP/IP, and requires that Microsoft Remote Access Service (RAS) software be installed on each server running the Auto Alarm Manager. Refer to your Microsoft manuals for more information on setting up RAS. You also need to have the TCP/IP protocol installed and correctly set up on every Sending and Receiving node.*

NOTE: *The AAMTCP.exe can only read from or write to an iFIX Database tag on the <u>local</u> iFIX node. You cannot read or write to tags on remote nodes. This applies to the Emergency Tagname, Disable Tagname and the Receiving Tagname. You cannot acknowledge an alarm that comes from a remote node. For the alarm to be acknowledged, it has to be from the same (local) node that AAMTCP.exe is running on. If it is not, the alarm will still be sent to the Receiver node, but it will not be acknowledged by the Sender node.*

Entering the Names of the Database Tags You Want to Use

▶ **To enter the names of the database tags that you want to use:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the Configure menu, click Auto Alarm Manager.

3. Select the Enable option.

4. In the Disable Tagname field, enter the name of the disable tag.

5. In the Emergency Tagname field, enter the name of the emergency tag.

6. Click OK.

Setting Up the Auto Alarm Manager Timers

▶ **To set up the Auto Alarm Manager timers:**

1. On the Sender node, in Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the Configure menu, click Auto Alarm Manager.

3. Select the Enable option.

4. Select the Advanced button.

5. In the Send Timeout field, enter the number of seconds that the Sending node has to report alarms to the Receiving node.

6. In the Receive Timeout field, enter the number of seconds that the Sending node waits for an acknowledgement from the Receiving node that the alarms were delivered successfully.

7. Click OK.

Configuring the Auto Alarm Manager as a Service

▶ **To configure the Auto Alarm Manager as a service:**

1. On the Sender node, in Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the Configure menu, click Auto Alarm Manager.

3. Click the Advanced button.

4. In the Username and Password fields on the Sending node, enter a Windows user account name and password. The Windows user account you specify must reside on the RAS server and must have dial-in permission.

5. In the Confirm Password field, re-enter the password.

6. Click OK.

Defining Local Startup Settings

In the SCU, you can perform the following steps with Local Startup:

- Disabling the Local Node Alias Feature

- Enabling the Local Node Alias Feature

- Running iFIX as a Service under Windows

- Specifying the Local Server, Local Logical, and SCU File Names

Disabling the Local Node Alias Feature

▶ **To disable the Local Node Alias feature:**

1. Ensure that you are logged in as an Administrator.

2. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

3. On the Configure menu, click Local Startup.

4. Clear the Local Node Alias check box.

5. Click OK.

Enabling the Local Node Alias Feature

▶ **To enable the Local Node Alias feature:**

1. Ensure that you are logged in as an Administrator.

2. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

3. On the Configure menu, click Local Startup.

4. Select the Local Node Alias check box.

5. Click OK.

Running iFIX as a Service under Windows

▶ **To run iFIX as a service under Microsoft Windows:**

1. Shut down iFIX.

2. Make sure 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, Proficy HMI SCADA - iFIX, and then System Configuration. The System Configuration Utility (SCU) window appears.

4. In the SCU, on the Configure menu, click Local Startup. The Local Startup Definition dialog box appears.

5. In the Service area, select the Continue Running After Logoff check box.

   NOTE: The check boxes in the Service area of this dialog box are unavailable while iFIX is running. You need to shut down iFIX, as you did in step 1, to update them.

6. If you want iFIX to start automatically whenever the system reboots, select the Start FIX at System Boot check box.

7. Click OK.

8. On the File menu, click Save.

9. Close the SCU.

10. Restart iFIX.

Specifying the Local Server, Local Logical, and SCU File Names

▶ **To specify the local server, local logical, and SCU file names:**

1. In Classic view, from the iFIX WorkSpace, click the System Configuration Utility button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click SCU.

2. On the Configure menu, click Local Startup.

3. In the Local Node Name field, enter a unique server name of up to eight alphanumeric characters. You cannot use special characters, except for the underscore.

4. In the Local Logical Name field, enter a logical node name of up to eight alphanumeric characters. You cannot use special characters, except for the underscore.

5. In the Configuration File field, enter the path of the local SCU file. For example: C:\Program Files\Proficy\Proficy iFIX\LOCAL\SCADA01.SCU. To search for existing SCU files, click the browse (...) button, select a file, and click the Open button.

    NOTE: If you change the node name after you enable security, security will be effectively disabled. You will need to save the security files again, and then enable security again.

6. Click OK to save your settings in the Local Startup Definition dialog box.

Using the Startup Profile Manager

The Startup Profile Manager is a utility that allows you to link users to iFIX projects or configurations, as well as restrict the actions that these users can take when starting iFIX. With the Startup Profile Manager, you create unique startup profiles for individual iFIX users, as well as a default profile for all other users.

The following figure shows an example of the main window of the Startup Profile Manager that appears when you open the application.

Startup Profile Manager

Overview of the Startup Profile Manager

The Startup Profile Manager allows you to associate a Windows user with a specific iFIX Project Configuration. An iFIX Project Configuration is the SCU file and node name combination that you want the iFIX Startup dialog box to display when the specified user starts iFIX. In the iFIX Project Configuration, you can also define whether the user can modify these fields or restrict access to the iFIX sample system for this user.

Since the Startup Profile Manager allows you to manage many users, you will find this application most useful when you use terminal services. It is recommended that no more than 20 Terminal Server sessions running iFIX on one computer.

The startup profiles that you create and modify in this application are not used by iFIX until a profiled user attempts to start iFIX (by running Launch.exe).

What Exactly is a Startup Profile?

A startup profile is a group of settings that associate a Windows user name with a specific iFIX Project Configuration. The iFIX Project Configuration includes:

- SCU path and file name that you want the specified Windows user to use when starting iFIX.

- Node name that you want the specified Windows user to use when starting iFIX.

- Restrictions on whether the user can modify these settings during iFIX startup.

- Restriction on whether the user can run the iFIX Sample System.

When starting, iFIX checks the currently logged in Windows user name to determine if the user has a profile listed in the Startup Profile Manager. If a profile is identified, iFIX loads that profile. Otherwise, the default profile is used, if it is enabled. If a default profile does not exist, no profiles are loaded. In this case, iFIX loads the node and SCU file defined in the Local Startup Definition dialog box of the SCU application (which is the SCU file and node name defined in the Windows Registry), and there are no restrictions in the iFIX Startup dialog box, unless you changed the default iFIX Startup options in the Default Startup Profile dialog box of the Startup Profile Manager.

When Would You Use the Startup Profile Manager?

Use the Startup Profile Manager when you need to manage many iFIX users, such as when you use Terminal Services. For instance, with the Startup Profile Manager, you can globally define a default profile for all Windows users without profiles, and then create specific profiles for specific Windows users. Management of many user profiles is easily performed at a global level and an individual user level.

In the first iFIX release that included support for Terminal Services, iFIX 2.5, iFIX required that you generate a complete application environment for each remote user. For example, if there are 50 iFIX users, there must be 50 sets of SCU files, with each SCU file unique to that specific user. With the Startup Profile Manager, all user profiles are stored in a master list, making it easy to maintain and modify profiles for use with Terminal Services.

If you are upgrading from a previous iFIX release, the use of a default profile will help you in migrating from the multiple SCU files to the easier configuration in the Startup Profile Manager.

For more details on best practices when configuring Terminal Services with the Startup Profile Manager, refer to the Using Terminal Server manual.

Understanding Startup Profiles When Upgrading from a Previous iFIX Release

If you do not create startup profiles for your users, your existing startup configurations from previous iFIX releases run unchanged. If you later choose to create new startup profiles, the Startup Profile Manager includes an option that allows the new profile settings to override the pre-existing configurations. For more information on the override setting, refer to the Configuring the Options for the Startup Profile Manager section.

Startup Profile Manager Basics

There is certain basic information you should know before using the Startup Profile Manager. This section contains information on the following:

- Configuring the Options for the Startup Profile Manager

- Configuring the Default Profile

- Security Considerations when Using the Startup Profile Manager

- Key Combinations Available in the Startup Profile Manager

- Working with Startup Profiles

Configuring the Options for the Startup Profile Manager

Before you begin working with the Startup Profile Manager, you should configure the options that you want the Startup Profile Manager to use. The following figure shows the Options dialog box that appears in the Startup Profile Manager.
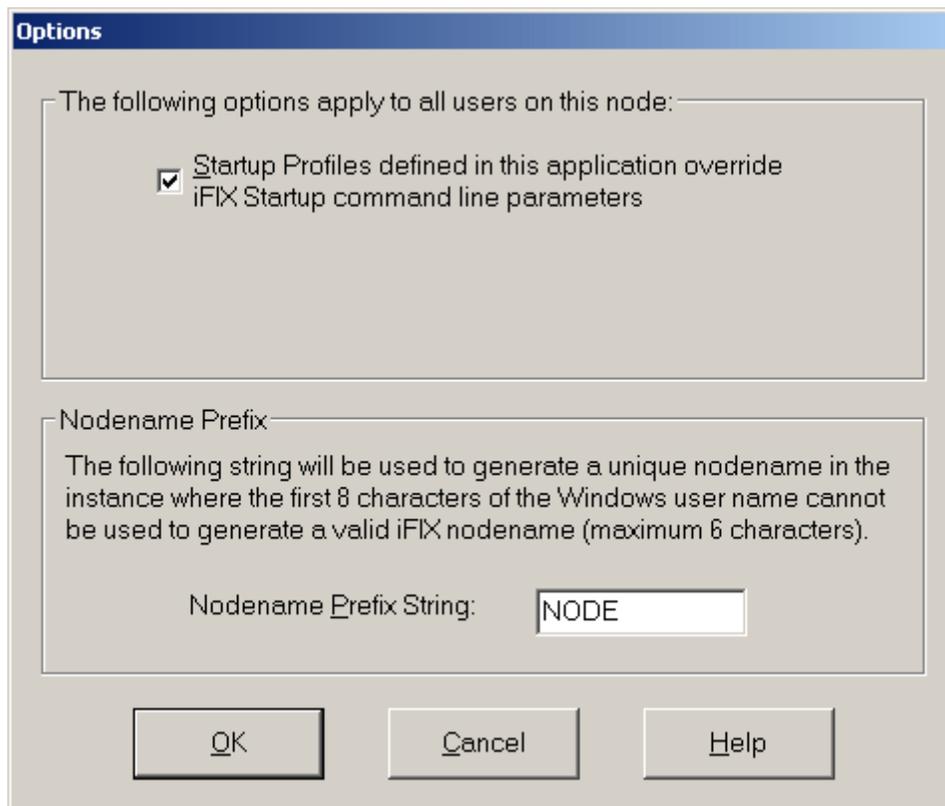
Options Dialog Box in Startup Profile Manager

▶ **To change the options for the Startup Profile Manager:**

1. On the Settings menu, click Options. The Options dialog box appears.

2. Select the *Startup Profiles defined in this application override iFIX Startup command line*

parameters check box, if you want the profiles created in this application to override the ones used when you start iFIX from the command line.

IMPORTANT: *For the override to work, the user must be defined in the Startup Profile Manager, or if the user is not defined, the default profile must be enabled. This override only applies to the /n, /s, and /l command line options.*

3. Enter a string for the default iFIX node name prefix to use if the first 8 characters of the Windows user name cannot be used to generate a valid iFIX node name.

   The Windows user name is an invalid iFIX node name, for instance, when the name starts with a number. Valid node names can be up to eight characters long. Node names can include alphanumeric characters, but must begin with a letter. Special characters, such as symbols and punctuation marks, cannot be used.

   For each startup profile using the default iFIX node name, a number is also added to the end of the default node name, starting with the number 1. For example, if you enter NODE as the prefix, the default iFIX node names used are: NODE1, NODE2, NODE3, and so on. Each default user who starts iFIX receives a different node name.

   NOTE: *When you use the Nodename Prefix field, you cannot use the iFIX automatic login feature unless you generate automatic login configurations for each of the possible node names for the defined prefix. For example: Node1, Node2, Node3, and so on. Since you will not know the name of the user logging in under that node name (since the name is generated at iFIX startup), you should also associate the auto logins with a guest or limited-access account. For more information on automatic login, refer to the iFIX Automatic Login section.*

4. Click OK.

Configuring the Default Profile

After configuring the application options for the Startup Profile Manager, you should define a default profile, if your iFIX configuration requires it. For instance, when using Terminal Services with the Startup Profile Manager, you will most likely want to configure a default profile.

If a user attempts to start iFIX and a profile does not exist for that user yet, iFIX starts with the default profile information.

To configure the SCU and iFIX Startup options for the default profile, use the Default Startup Profile dialog box, as shown in the following figure.
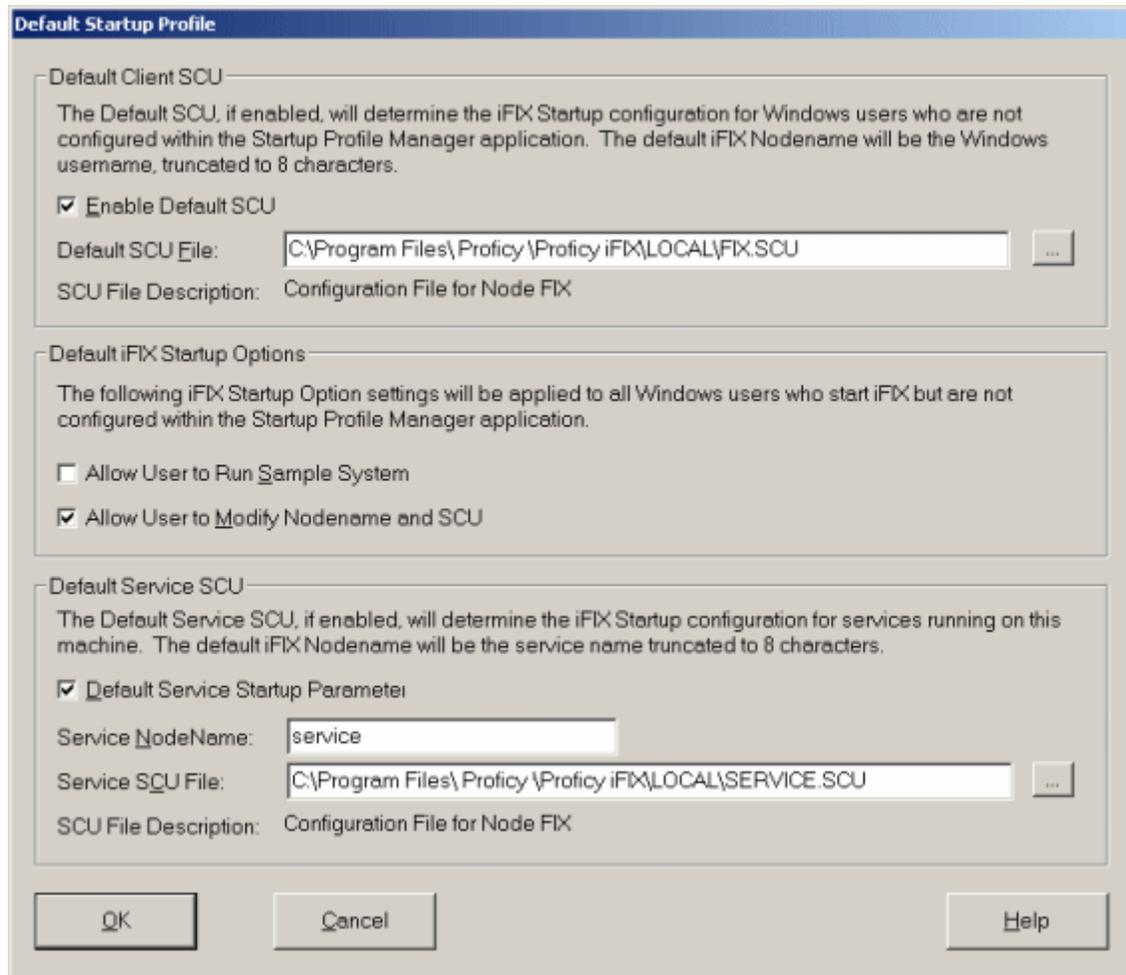
Default Startup Profile Dialog Box

Additionally, if iFIX is running as a service, you can configure the default SCU for the service, as illustrated in the previous graphic in the Default Service SCU area.

Security Considerations when Using the Startup Profile Manager

If you select the Enable the Default SCU option in the Startup Profile Manager, make sure you also enable the global security paths (Use These Paths for All Startup Profiles) option in the Configuration dialog box in the Security Configuration application. When you enable the global security paths, all iFIX user sessions on a computer share the same security configuration.

If you do not enable global security paths, you will need to individually configure security within each Terminal Services user session.

For more information on global security paths, refer to Configuring Global Security Paths in the Configuring Security Features manual.

For information on how to enable the default startup profile, refer to the Configuring the Default Profile section.

Key Combinations Available in the Startup Profile Manager

The following list summarizes the quick keys that you can enter from the keyboard and the actions that they perform.

Startup Profile Manager Key Combinations	
Enter this Key Combination...	**To...**
Ctrl+D	Open the Default Startup Profile dialog box.
Ctrl+O	Open the Options dialog box.
Ctrl+A	Open the Add Startup Profile dialog box.
Ctrl+S	Save the current startup profiles that you created.

Working with Startup Profiles

iFIX must be running in order to use the Startup Profile Manager application. After you create your startup profiles and configure the default profile (if required), you need to save your startup profiles if you want iFIX to use them. If you do not save your startup profiles during the current session, a message box reminds you to save when you exit the Startup Profile Manager.

A startup profile is not used by iFIX until the specified user attempts to start iFIX from the iFIX Startup dialog box or from the iFIX Startup command line (from a desktop shortcut or the Run dialog box, for example). If no iFIX startup profile exists for the user and you do not define any settings in the Default User Profile dialog box or provide command line settings to the iFIX Startup application, when you restart iFIX, it displays the information from the last time iFIX was run.

General Overview of Steps for Using the Startup Profile Manager

This section outlines the general steps for getting started with the Startup Profile Manager. To begin working with the Startup Profile Manager, follow these steps:

1. Configure the default profile in the Startup Profile Manager, if required.
2. Configure global security paths in the Security Configuration application, if you enable the default profile.
3. Add startup profiles in the Startup Profile Manager.
4. Save your profiles.

Disabling or Hiding Options in the iFIX Startup Dialog Box

Using the Startup Profile Manager you can disable buttons or text edit fields that appear in the iFIX

Startup dialog box on a per-user basis. To do this, you must edit the iFIX Startup Options for the user's profile. To cover users that do not have startup profiles, you should edit the Default iFIX Startup Options in the Default Startup Profile dialog box.

The following table describes the options that you disable or hide in the iFIX Startup dialog box.

Disabling or Hiding Options in the iFIX Startup Dialog Box	
To Disable or Hide the...	**Clear this check box...**
Node Name and SCU text edit fields, as well as the SCU button	Allow User to Modify Nodename and SCU
Sample System button	Allow User to Run Sample System
Entire iFIX Startup dialog box with startup options	Allow User to Run Sample System and the Allow User to Modify Nodename

For more information on the iFIX Startup dialog box, refer to iFIX Startup section in the Setting up the Environment manual.

Frequently Asked Questions About the Startup Profile Manager

The following list outlines some of the frequently asked questions about using the Startup Profile Manager.

When Does iFIX Use the Startup Profiles That You Create?

iFIX does not use the startup profiles that you create and modify in the Startup Profile Manager application until a profiled user attempts to start iFIX. When starting, iFIX checks the currently logged in Windows user name to determine if the user has a profile listed in the Startup Profile Manager.

The Override iFIX Startup Command Line Parameters Option in the Startup Profile Manager Does Not Appear to Work... Why?

The check box in the Startup Profile Manager to override the iFIX startup command line parameters (the *Startup Profiles defined in this application override iFIX Startup command line parameters* option in the Options dialog box) only applies to the /n, /s, and /l command line options. In addition, for the override to work, the user must be defined in the Startup Profile Manager, or if the user is not defined, the default profile must be enabled.

How Do I Override the /e Command Line Option?

The only way to override the /e command line option (to shut down the currently running iFIX application) is to clear the Allow User to Run Sample System check box for the specified user's startup profile or, if the user is not defined, for the default profile in the Startup Profile Manager.

How Do I Stop the iFIX Startup Dialog Box From Appearing?

If you clear both the Allow User to Run Sample System and the Allow User to Modify Nodename check boxes for the iFIX Startup Options in the Startup Profile Manager, the iFIX Startup dialog box does not appear for the specified user.

If I am Upgrading from a Previous Release, Do I Have to Use Startup Profiles?

No. Your existing startup configurations will run without changes. If you later choose to create new startup profiles, the Startup Profile Manager includes an option that allows the new profile settings that you create to override the pre-existing configurations. For more information on the override setting, refer to the Configuring the Options for the Startup Profile Manager section.

Startup Profile Manager Dialog Boxes

The Startup Profile Manager includes the following dialog boxes (listed in alphabetical order):

- Add Startup Profile Dialog Box

- Default Startup Profile Dialog Box

- Edit Startup Profile Dialog Box

- Options Dialog Box

- Startup Profile Manager Main Window

Add Startup Profile Dialog Box

The Add Startup Profile dialog box displays the following items:

Domain

Select a domain from the drop-down list. The current login domain and local computer domain, if different, for the currently logged in Windows user, appear in this list.

Click the List Domain Members button to display list of domain members in the following list box. Depending on the size of your domain and speed of your network, this action could take a few moments or several minutes.

List Domain Members

Click to list the members of the specified domain in the following list box. You may need to wait a few moments or several minutes for this list to populate, depending on the size of the domain and speed of your network.

Windows Users List

Displays a list of Windows users for the specified domain.

To display Windows user names in this box, you must select a domain from the drop-down list and then click List Domain Members button. Depending on the size of your domain and speed of your network, this action could take a few moments or several minutes.

To specify a Windows user for a startup profile, select one from the list or enter one in the Windows User field.

Windows User

Enter the name of the Windows user for which you want to create an iFIX startup profile. You do not have to be connected to the domain from which the user is a member if you enter the name manually.

Optionally, instead of entering the Windows user name in this field, select a domain and click the List of Domain Members button to list the available Windows users for you to select from.

iFIX Nodename

Leave the default name or enter another name for the iFIX node that you want to associate with this Windows user. This name can up to eight characters long.

By default, the Windows user name appears in the iFIX Node Name field. If the Windows user name is more than 8 characters, the characters after the eighth one are truncated.

If the Windows user name starts with anything other than a letter, such as a number, the Startup Profile Manager uses the default node name prefix that you specified in the Options dialog box to generate a unique, valid node name.

For each startup profile using the default iFIX node name, a number is also added to the end of the default node name, starting with the number 1. For example, if the prefix is NODE, the default iFIX node names used are: NODE1, NODE2, NODE3, and so on.

NOTE: If you manually entered a Windows user name, you must also manually enter an iFIX node name. The default name is not used in this case.

SCU File

The location and name of the SCU file that you want the specified Windows user to use when starting iFIX. Optionally, click the Browse (…) button to search for a file.

iFIX Startup Options

Item	Description
Allow user to run Sample System	Select this check box if you want to allow the specified Windows user to run the iFIX Sample System. Uncheck this option if you want to deny the use of the sample system to the specified user. By default, this check box is selected.

Item	Description
Allow user to modify Nodename and SCU	Select this check box to allow the specified Windows user to edit the SCU or node name from the iFIX Startup dialog box. Uncheck this option if you want to make these fields unavailable when the user starts iFIX. By default, this check box is selected.

Add Profile

Click to add your newly created startup profile to the list of profiles. The profile list updates when you exit the Add Startup Profile dialog box.

Default Startup Profile Dialog Box

The Default Startup Profile dialog box displays the following items:

Default Client SCU

Item	Description
Enable Default SCU	Select this check box if you want to specify a default SCU file and node name for iFIX users without a startup profile. The SCU that you specify in this dialog box appears in the iFIX Startup dialog box when you start iFIX on a computer whose Windows logged in user does not have a startup profile. The default node name that appears in this dialog box is the Windows user name. Any more than 8 characters are truncated from the name.
Default SCU File	Enter the location and name of the iFIX SCU file. Optionally, browse for an SCU file by clicking the Browse (…) button. This field is only available if you select the Enable Default SCU check box.

Default iFIX Startup Options

Item	Description
Allow User to Run Sample System	Select this check box if you want to grant users without a startup profile the ability to run the iFIX Sample System. Uncheck this option if you want to deny the use of the sample system to these users. By default, this check box is selected.

Item	Description
Allow User to Modify Nodename and SCU	Select this check box if you want to allow users without a startup profile to edit the SCU or node name from the iFIX Startup dialog box. Uncheck this option if you want to make these fields unavailable when the user starts iFIX. By default, this check box is selected.

Default Service SCU

Item	Description
Default Service Startup Parameter	Click to enable a default startup profile when iFIX runs as a service.
Service NodeName	Enter the name of the node where iFIX runs as a service.
Service SCU File	Enter the SCU name that you want to start when iFIX runs as a service.

Edit Startup Profile Dialog Box

The Edit Startup Profile dialog box displays the following items:

iFIX Nodename

Enter the iFIX node name that you want to associate with this user. This name can up to eight characters long.

SCU File

Enter the location and name of the SCU file that you want the specified Windows user to use when starting iFIX. Optionally, click the Browse (…) button to search for a file.

iFIX Startup Options

Item	Description
Allow User to Run Sample System	Select this check box if you want to allow the specified Windows user to run the iFIX Sample System. Uncheck this option if you want to deny the use of the sample system to the specified user. By default, this check box is selected.

Item	Description
Allow User to Modify Nodename and SCU	Select this check box to allow the specified Windows user to edit the SCU or node name from the iFIX Startup dialog box. Uncheck this option if you want to make these fields unavailable when the user starts iFIX. By default, this check box is selected.

Options Dialog Box

The Options dialog box displays the following items:

Startup Profiles defined in this application override iFIX Startup command line parameters

Select this check box if you want the profiles created in this application to override the ones used when you start iFIX from the command line.

For the override to work, the user must be defined in the Startup Profile Manager, or if the user is not defined, the default profile must be enabled.

NOTE: This override only applies to the /n, /s, and /l command line options.

Nodename Prefix String

Enter the default iFIX node name prefix to use if the first 8 characters of the Windows user name cannot be used to generate a valid iFIX node name.

For each startup profile using the default iFIX node name, a number is also added to the end of the default node name, starting with the number 1. For example, if the prefix is NODE, the default iFIX node names used are: NODE1, NODE2, NODE3, and so on.

Startup Profile Manager Main Window

The Startup Profile Manager main window displays the following items:

iFIX Startup Profiles (spreadsheet)

Displays a list of iFIX startup profiles. Double-click an empty row to add a profile. Or, double-click a profile in the list to modify it.

Add

Click to add a new profile.

Edit

Click to modify the selected profile.

Remove

Click to remove the selected profile.

Help

Click to display information on how to use the Startup Profile Manager.

Close

Click to close the Startup Profile Manager.

Default SCU

The location and name of the iFIX SCU file for the default profile, if enabled.

The default startup profile specifies the iFIX startup configuration to use for the Windows users who are not configured within the Startup Profile Manager application.

How Do I...

Click on any of the links below for more information on this application.

- Working with Startup Profiles
- Adding a startup profile
- Editing a startup profile
- Removing a startup profile
- Removing all startup profiles
- Key combinations available in the Startup Profile Manager
- Backing up your startup profiles
- Saving the startup profiles
- Changing the default settings for the application
- Defining the defaults for startup profiles

Working with Startup Profiles

From the Startup Profile Manager you can perform the following tasks:

- Add a startup profile
- Edit a startup profile
- Remove a startup profile

Adding a Startup Profile

▶ **To add a startup profile:**

1. In Classic view, in the Proficy iFIX WorkSpace, on the toolbar, click the Startup Profile Manager button.

   -Or-

   In Ribbon view, on the Applications tab, in the Utilities group, click Utilities, and then click Startup Profile Manager.

   NOTE: The Startup Profile Manager can also be accessed from the Start menu by pointing to Programs, Proficy HMI SCADA - iFIX, Tools, and then Startup Profile Manager.

2. Click the Add button, or double-click any empty column.

3. Select a domain from the drop-down list.

4. Optionally, click the List Domain Members button to view a list of users that you can pick from.

   NOTE: Depending on the size of your domain and speed of your network, this action could take a few moments or several minutes.

5. In the Windows User field, select a Windows user from the list, or enter one manually. You do not have to be connected to the domain if you enter the name manually.

6. Accept the default iFIX Node Name, or enter another one.

   NOTE: If you manually entered a Windows user name, you must also manually enter an iFIX node name. The default name is not used in this case.

7. Enter the location and name of the iFIX SCU file that you want to associate with this user. For example, you might enter C:\Program Files\Proficy\Proficy iFIX\LOCAL\FIX.SCU. If a default iFIX SCU name is supplied, you can use it or enter another one.

   Optionally, you can browse for an SCU file, by clicking the Browse (…) button.

8. Select the options that you want to make available for the specified user from the iFIX Startup dialog box.

   - If you select the Allow User to Run Sample System check box, the specified Windows user can start the sample system.

   - Similarly, if you select the Allow User to Modify Nodename and SCU check box, these fields are available for editing when the specified user attempts to start iFIX.

   - If you clear both the Allow User to Run Sample System and the Allow User to Modify Nodename and SCU check boxes, the iFIX Startup dialog box does not appear for the specified user.

9. Click Add Profile.

Editing a Startup Profile

▶ **To edit a startup profile:**

1. In Classic view, in the Proficy iFIX WorkSpace, on the toolbar, click the Startup Profile Manager button.

-Or-

In Ribbon view, on the Applications tab, in the Utilities group, click Utilities, and then click Startup Profile Manager.

NOTE: The Startup Profile Manager can also be accessed from the Start menu by pointing to Programs, Proficy HMI SCADA - iFIX, Tools, and then Startup Profile Manager.

2. Select the profile that you want to edit.

3. Double-click the row for that startup profile, or click the Edit button.

4. Make the applicable changes to any of the following fields:

   - **iFIX Nodename field** – the name of the iFIX node that you want to associate with this user.

   - **SCU File field** – the location and name of the iFIX SCU file that you want to associate with this user.

   - **Allow User to Run Sample System check box** – if selected, the specified Windows user can start the sample system from the iFIX Startup dialog box.

   - **Allow User to Modify Nodename and SCU check box** – if selected, the specified Windows user can edit these fields from the iFIX Startup dialog box.

NOTE: If you clear both the Allow User to Run Sample System and the Allow User to Modify Nodename and SCU check boxes, the iFIX Startup dialog box does not appear for the specified user.

5. Click OK.

Removing a Startup Profile

▶ **To remove a startup profile:**

1. In Classic view, in the Proficy iFIX WorkSpace, on the toolbar, click the Startup Profile Manager button.

   -Or-

   In Ribbon view, on the Applications tab, in the Utilities group, click Utilities, and then click Startup Profile Manager.

   NOTE: The Startup Profile Manager can also be accessed from the Start menu by pointing to Programs, Proficy HMI SCADA - iFIX, Tools, and then Startup Profile Manager.

2. Select the profile that you want to delete.

3. Click Remove.

4. Click Yes to continue.

5. On the File menu, click Save.

Removing All Startup Profiles

▶ **To remove all startup profiles:**

1. In Classic view, in the Proficy iFIX WorkSpace, on the toolbar, click the Startup Profile Manager button.

   -Or-

   In Ribbon view, on the Applications tab, in the Utilities group, click Utilities, and then click Startup Profile Manager.

   NOTE: The Startup Profile Manager can also be accessed from the Start menu by pointing to Programs, Proficy HMI SCADA - iFIX, Tools, and then Startup Profile Manager.

2. On the File menu, click Remove All Profiles.

3. Click Yes to continue. The startup profile list in the main screen appears empty after the profiles are removed.

   NOTE: The settings defined in the Default Startup Profile dialog box are not removed. Only startup profiles in the list that appears in the main window are removed.

4. On the File menu, click Save.

Key combinations in the Startup Profile Manager

The following list summarizes the quick keys that you can enter from the keyboard and the actions that they perform:

- **CTRL+D** – Opens the Default Startup Profile dialog box.
- **CTRL+O** – Opens the Options dialog box.
- **CTRL+A** – Opens the Add Startup Profile dialog box.
- **CTRL+S** – Saves the current startup profiles that you created.

Backing Up Your Startup Profiles

▶ **To manually backup the configuration file that contains your startup profiles:**

1. In Classic view, in the Proficy iFIX WorkSpace, on the toolbar, click the Startup Profile Manager button.

   -Or-

   In Ribbon view, on the Applications tab, in the Utilities group, click Utilities, and then click Startup Profile Manager.

   NOTE: The Startup Profile Manager can also be accessed from the Start menu by pointing to Programs, Proficy HMI SCADA - iFIX, Tools, and then Startup Profile Manager.

2. On the File menu, click Save to save your current startup profiles.

3. Locate the Profiles.cfg file. Usually, this file is located in the main C:\Dyanmics folder.

   NOTE: The Profiles.cfg file is an encrypted file. You cannot edit it in a text editor such as Notepad.

4. Copy this file to another location.

Saving the Startup Profiles

▶ **To save your startup profiles:**

1. In Classic view, in the Proficy iFIX WorkSpace, on the toolbar, click the Startup Profile Manager button.

   -Or-

   In Ribbon view, on the Applications tab, in the Utilities group, click Utilities, and then click Startup Profile Manager.

   NOTE: The Startup Profile Manager can also be accessed from the Start menu by pointing to Programs, Proficy HMI SCADA - iFIX, Tools, and then Startup Profile Manager.

2. Add or edit the required startup profiles.

3. On the File menu, click Save.

   NOTE: If you do not save your startup profiles during the session, a message box prompts you to when you exit the Startup Profile Manager.

The startup profile is not used by iFIX until the specified user attempts to start iFIX. If no iFIX startup profile exists for the user and you do not define any settings in the Default User Profile dialog box or provide command line settings to the Launch application, when you restart iFIX, it displays the information from the last time iFIX was run.

Changing the Default Settings

▶ **To change the default settings for the Startup Profile Manager:**

1. In Classic view, in the Proficy iFIX WorkSpace, on the toolbar, click the Startup Profile Manager button.

   -Or-

   In Ribbon view, on the Applications tab, in the Utilities group, click Utilities, and then click Startup Profile Manager.

   NOTE: The Startup Profile Manager can also be accessed from the Start menu by pointing to Programs, Proficy HMI SCADA - iFIX, Tools, and then Startup Profile Manager.

2. On the Settings menu, click Options.

3. Select the *Startup Profiles defined in this application override iFIX Startup command line parameters* check box, if you want the profiles created in this application to override the ones used when you start iFIX from the command line.

   NOTE: For the override to work, the user must be defined in the Startup Profile Manager, or if the user is not defined, the default profile must be enabled. In addition, this override only applies to the /n, /s, and /l command line options.

4. Enter the iFIX node name prefix that you want the Startup Profile Manager to use when the Windows user name is invalid as a default iFIX node name.

   The Windows user name is an invalid iFIX node name, for instance, when the name starts with a number. Valid node names can be up to eight characters long. Node names can include

alphanumeric characters, but must begin with a letter. Special characters, such as symbols and punctuation marks, cannot be used.

For each startup profile using the default iFIX node name, a number is also added to the end of the default node name, starting with the number 1. For example, if you enter NODE as the prefix, the default iFIX node names used are: NODE1, NODE2, NODE3, and so on.

5. Click OK.

Defining the Default Startup Profile

▶ **To define the default startup profile:**

1. In Classic view, in the Proficy iFIX WorkSpace, on the toolbar, click the Startup Profile Manager button.

    -Or-

    In Ribbon view, on the Applications tab, in the Utilities group, click Utilities, and then click Startup Profile Manager.

    NOTE: The Startup Profile Manager can also be accessed from the Start menu by pointing to Programs, Proficy HMI SCADA - iFIX, Tools, and then Startup Profile Manager.

2. On the Settings menu, click Default Startup Profile.

3. In the Default Client SCU area, select the Enable Default SCU check box and enter an SCU file name.

4. In the Default iFIX Startup Options area, select the check boxes that you want to apply to all iFIX users without a startup profile.

5. If you plan to run iFIX as a service, in the Default Service SCU area, enter or select the Default Service Startup Parameter, and enter the node name and SCU file name of the service. This enables you configure the startup profile that iFIX uses when it runs as a service.

6. Click OK.

    NOTE: If you select the Enable the Default SCU option, make sure you also enable the global security paths (Use These Paths for All Startup Profiles) option in the Configuration dialog box in the Security Configuration application.

iFIX Startup

The iFIX Startup program reads the SCU file and runs the tasks that support your configuration. Except for the SCU, individual iFIX applications cannot be run unless you start iFIX.

Before you start iFIX, you must make sure that you have set up the hardware, software, and network components necessary to operate iFIX in your process environment. Refer to the appropriate chapters in this manual to help you configure your environment.

When you start iFIX, the iFIX Startup dialog box appears, if you configured it to do so. From this dialog box, you can launch the iFIX Sample System, or change the iFIX node or SCU file used when iFIX starts, if you have privileges to do so. The following figure shows an example of the iFIX Startup dialog box with all options enabled.
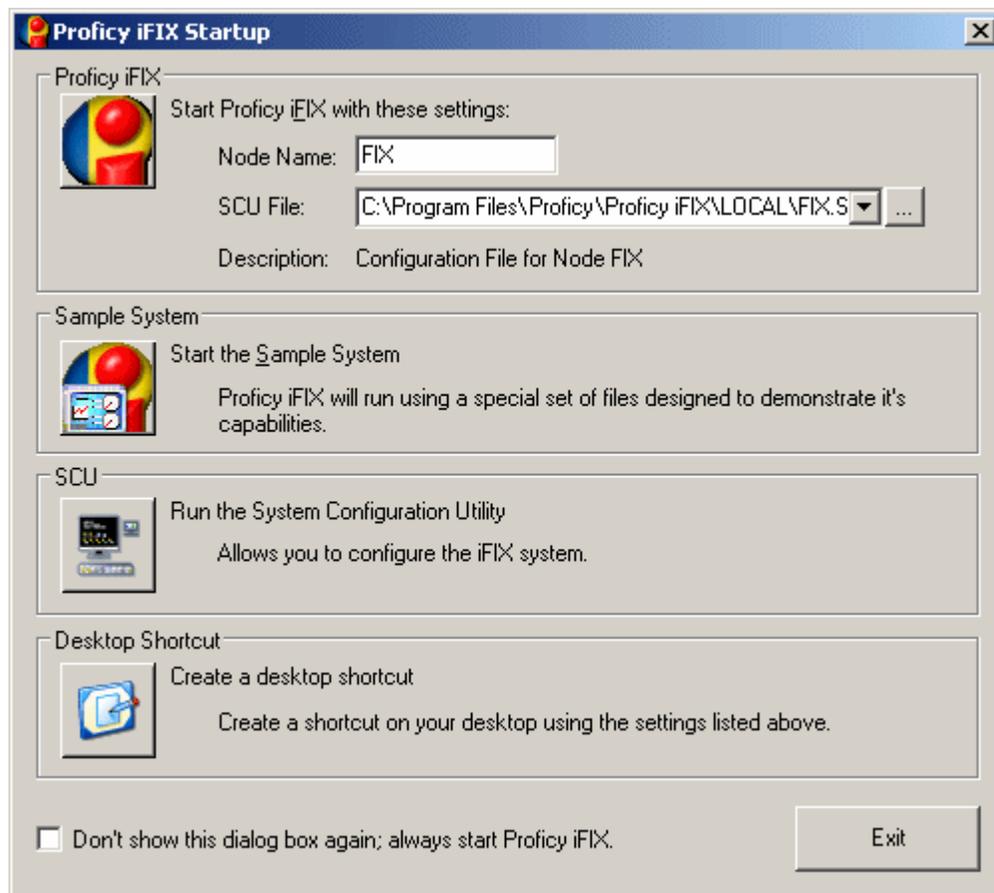
iFIX Startup Dialog Box

The privileges for your startup profile are defined in the Startup Profile Manager. For more information on how to configure startup options in the Startup Profile Manager, refer to the Using the Startup Profile Manager chapter in this manual. If you do not use the Startup Profile Manager, iFIX starts with the node name and SCU file last specified in the SCU.

Once iFIX loads, a dialog box appears with a message such as: "iFIX Software is currently running!" or "iFIX Demo System is currently running!"

Proficy iFIX Startup Dialog Box

The Proficy iFIX Startup dialog box displays the following items:

Start Proficy iFIX

Click to start iFIX with the specified SCU and node name. If you do not have privileges to start iFIX, this button launches the Sample System.

Item	Description
Node Name	Enter the iFIX node name that you want to start with. This name can up to eight characters long.
	If you do not have privileges to edit this field, the field is unavailable.
SCU File Name	Select an SCU from the drop-down list, or enter the location and name of the SCU file that you want to use when starting iFIX. Optionally, click the Browse (…) button to search for a file.
	If you do not have privileges to edit this field, the field is unavailable.
SCU File Browse	Click to browse for an iFIX SCU file. A dialog box opens from which you can browse for a file.
	By default, this dialog box lists the iFIX SCU files in the C:\Program Files\Proficy\Proficy iFIX\Local folder, but you also can browse to another folder.

Start Sample System

Click to start the iFIX Sample System. If you do not have privileges to start the Sample System, this button is unavailable.

NOTE: The Sample System runs on a special demo version of iFIX; therefore, you cannot run the Sample System and iFIX simultaneously.

SCU

Click to open the SCU. If you do not have privileges to start the SCU, this button is unavailable.

Desktop Shortcut

Click to create a shortcut to the iFIX Startup dialog box (Launch.exe) using the settings listed above.

A dialog box opens for you to enter a name for the desktop shortcut.

Hide Dialog Box

Select this check box if you want to hide this dialog box the next time the specified user starts iFIX.

iFIX Startup Options

Once iFIX starts, the Startup dialog box displays a message and the Options menu is available from this dialog box. The following figure shows the iFIX Startup dialog box after you start iFIX in normal mode.
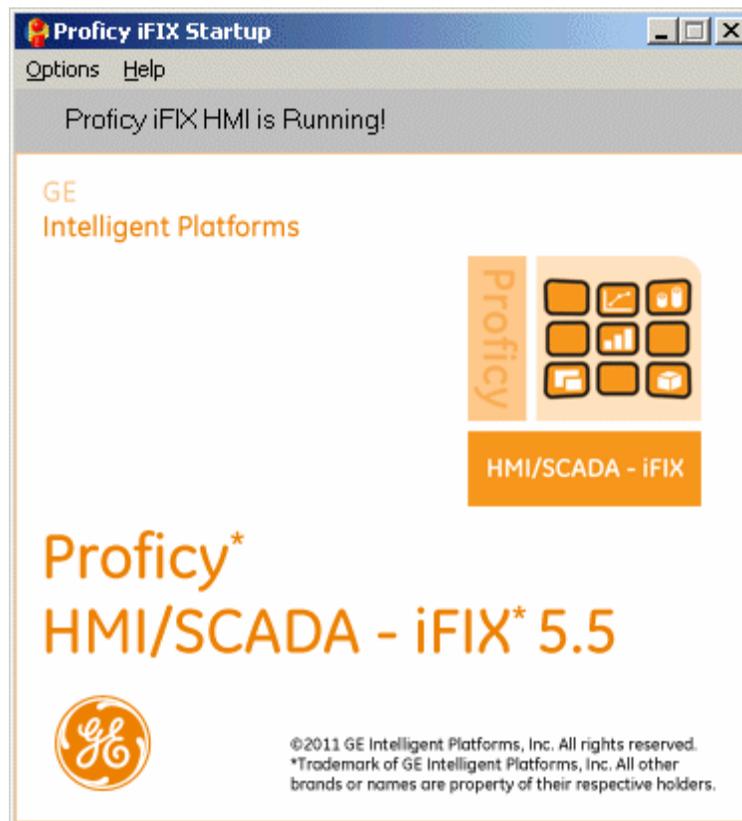
iFIX Startup Dialog Box with Options Menu

NOTE: *If you start iFIX with the Sample System, the title bar of this dialog box reads "iFIX Startup - DEMO MODE." If you start the iFIX as a service, the title bar of this dialog box reads "iFIX Startup - SERVICE MODE." If you start iFIX from a teminal server session on the iClientTS node, the title bar to this dialog box read "iFIX Startup - iClentTS."*

The Options menu on the iFIX Startup window lets you define startup window properties and view general conditions. The sections below explain the commands available from the Options and Help menus.

Minimize After Startup

By default, the iFIX Startup window minimizes on your screen after iFIX loads the startup tasks. To choose not to minimize the window at future startups, deselect Minimize after Startup from the Options menu.

Show History

To view a history of startup messages, select Show History from the Options menu. The Startup History dialog box appears.

Registered Tasks

To see a list of iFIX tasks currently running on this node, select Registered Tasks from the Options menu. The Task List dialog box appears.

Shutdown iFIX

To exit iFIX select Shutdown iFIX from the Options menu. iFIX automatically closes any remaining open tasks before shutting itself down. If you have any open files, you are prompted to save changes before exiting.

Version

To determine the version of iFIX you are running, on the Help menu, click About.

Running iFIX From the Command Line

You can run iFIX from the command line with the Launch.exe command. Launch.exe resides in your iFIX base path. The following table describes the command line options available for the Launch.exe program.

Launch Command Line Options	
Option	**Description**
/s *SCUfile*	Starts iFIX with the specified SCU file, if you have privileges to change the SCU. This option prevents the Startup dialog box from displaying, unless the /g is also on the command line.
	If the SCU file path has spaces, you should use quotes around the path. For instance:
	Launch /NSCUName /S"e:\Program Files\Proficy\Proficy iFIX\LOCAL\SCUName.SCU"

Launch Command Line Options	
Option	**Description**
/n *NodeName*	Starts iFIX with the specified node name, if you have privileges to change the node name. This option prevents the Startup dialog box from displaying, unless the /g is also on the command line.
/r	Restarts iFIX, if you have privileges to do so. If the iFIX Startup dialog box displays, continue by clicking the start iFIX button. If there are other command line options that prevent the Startup dialog box from displaying, then it is prevented and iFIX automatically restarts.
/l *LogicalNodeName*	Starts iFIX with the specified logical node name.
/e	Shuts down the currently running iFIX application, if the user has privileges to do so. iFIX does not display the iFIX Startup dialog box, nor does it try to restart iFIX. All other command line options are ignored. *NOTE: The only way to prevent a user from shutting down iFIX with the /e command line option is to uncheck the Allow User to Run Sample System check box for the user's startup profile (or, if the user is not defined, for the default profile in the Startup Profile Manager).*
/t	Starts iFIX in Demo mode.
/g	Always displays the iFIX Startup dialog box, if the user has the privileges to do so. This option overrides the Don't Show This Dialog Box Again check box settings in the iFIX Startup dialog box.
/d	Automatically starts the iFIX Sample System. Prevents the Startup dialog box from displaying, unless you include the /g option on the command line.
/w *NumSeconds*	Indicates the maximum amount of time that iFIX waits for a Terminal Server session to start. If the Terminal Server session does not start, the connection times out.
/x	Starts the DBASRV.exe program.

NOTE: The check box in the Startup Profile Manager to override the iFIX startup command line parameters (the Startup Profiles defined in this application override iFIX Startup command line parameters option in the Options dialog box) only applies to the /n, /s, and /l command line options. In addition, for the override to work, the user must be defined in the Startup Profile Manager, or if the user is not defined, the default profile must be enabled. For more information on the Startup Profile

Manager, refer to the Using the Startup Profile Manager chapter in this manual.

iFIX Background Tasks

iFIX starts and stops background tasks based on the configuration information in the SCU file. The table below describes the function of each iFIX background task. *Automatic* tasks are started by iFIX if required by your configuration. Tasks listed as *optional* require that you start them manually by adding them to the configured task list in the Task Configuration dialog box in the SCU.

NOTE: If you want, you can configure certain tasks to start up automatically. Refer to the Configuring Startup Tasks section for more information.

System Tasks		
Program	**Executable File**	**Function**
Alarm File Task (Automatic)	ALMFILE.EXE	Receives alarm messages and stores them in files.
Alarm Printer Task (Automatic)	ALMPRIN.EXE	Receives alarm messages and sends them to printers.
Alarm Summary Task (Automatic)	ALMSUM.EXE	Receives alarms for display in the Proficy iFIX WorkSpace through the Alarm Summary object.
Alarm Manager (Automatic)	NAM.EXE	Distributes alarm messages over the network. Alarm managers run on SCADA servers.
Alarm Client (Automatic)	NAC.EXE	Receives alarm messages over the network.
Historical Collect (Optional)	HTC.EXE	Collects data according to the Historical Assign configuration file.
I/O Control (Automatic, SCADA)	IOCNTRL.EXE	Starts the I/O drivers, and displays the status of the installed I/O drivers running on the SCADA server.
Summary Queue Delete (Automatic, SCADA)	SUMQDEL.EXE	Removes the acknowledged, returned to normal, alarms from the Alarm Summary queue.

System Tasks		
Program	**Executable File**	**Function**
Scan Alarm and Control (Automatic, SCADA)	WSACTASK.EXE	Updates the database with data from the I/O driver, makes requested writes to the I/O Driver, generates alarms, and executes the logic of the database chains.
Network Diagnostics (Optional)	NETDIAG.EXE	Displays the status of sessions on the local node.
TCP/IP Task (Automatic)	TCPTASK.EXE	Supports node-to-node communication over TCP/IP.
Node Name Table (Automatic)	NNTABLE.EXE	Stores network information about the local and remote nodes.
Connection Manager (Automatic)	CONMGR.EXE	During startup, establishes the sessions listed in the configuration file. Monitors the status of sessions on the local node and generates alarm messages if sessions go down. It also attempts to re-establish sessions that have gone down.
Alarm ODBC Service (Automatic)	AlmODBC.EXE	Reads alarms and messages generated by iFIX and logs them to an ODBC-compliant database.
Event Scheduler (Optional)	FixBackgroundServer.EXE	Runs time and event-based scripts, allowing you to schedule reports and monitor events.
Workspace (Optional)	Workspace.EXE	Opens the Proficy iFIX WorkSpace where you can open, edit, or view pictures. For information on command line parameters available for starting the WorkSpace in run mode, refer to the Command Line Parameters for Starting the iFIX WorkSpace section.

Monitoring the Environment with Mission Control

Mission Control provides an easy-to-use interface for monitoring iFIX programs that run in the background. It provides you with a *window* into your system, helping you diagnose potential problems with your iFIX system, and helping you improve performance on your server.

Mission Control monitors the following iFIX background tasks:

- I/O Control

- Historical Collect

- SQL task

- SAC processing

- Auto Alarm Manager

- Alarm ODBC services

NOTE: To run a iFIX task in the background you need to configure the program's startup task configuration in the SCU. For more information, refer to the Configuring Startup Tasks section.

To start Mission Control, click the Mission Control button on the Application toolbar, or select Mission Control from the Proficy iFIX WorkSpace system tree. To access a particular background task, select its tab.

Each tabbed page is summarized below:

I/O Control — allows you to monitor I/O driver communications statistics and errors. For a description of these fields, refer to your I/O driver manual.

HTC — allows you to start and stop the Historical Collect background task, and provides you with an Overrun Counter. The Overrun counter increments by one every time a historical collection fails. By examining the number of HTC overruns, you can find out if there is a problem in your collection scheme. See the Trending Historical Data manual for more information.

SQL — allows you to start and stop the SQL task, and also provides information to help you monitor your SQL connections to ODBC relational databases. For more information on the SQL task, see the Using SQL manual.

SAC — allows you to start and stop the SAC (Scan, Alarm, and Control) task, and also provides SAC statistics that may help you troubleshoot your system. For example, the Blocks/Sec field can be used to monitor the amount of blocks that are scanned per second. If the number fluctuates drastically, the blocks in your iFIX database may not be properly phased. See the Building a SCADA System manual for more information on SAC and phasing.

AAM — allows you to monitor the Auto Alarm Manager during setup and operation, and lets you view messages pertinent to its operation. For more information, refer to the Configuring the

Auto Alarm Manager section. Also refer to the Troubleshooting chapter for common messages displayed in Mission Control and their meaning.

Alarm Synchronization — allows you to monitor alarm acknowledgments synchronized by iFIX in previous versions. This tab does not apply to iFIX 5.1.

Alarm ODBC — allows you to send alarms and messages to an ODBC relational database. Once the relational database receives and stores the data, you can easily retrieve any information you want by querying the database. For more information on the Alarm ODBC Service, refer to the Configuring the Alarm ODBC Service section of the Implementing Alarms and Messages manual.

To close Mission Control, click the Close button at the bottom of the dialog box.

NOTE: Closing Mission Control does not terminate the tasks that it monitors; it only closes the dialog box itself.

Starting I/O Drivers Manually

Even if you have configured an I/O driver to automatically start, you may still want to manually start or stop the I/O driver. For example, when troubleshooting, you may need to stop the driver temporarily and then restart it.

To start I/O drivers manually in Mission Control, click the I/O Control tab. You can select a driver name from the Drivers list box. To start the selected driver, click Start. To stop the driver, click Stop.

For a description of the fields on the I/O Control tabbed page, refer to the I/O Control Tabbed Page Fields section.

Tuning the Driver's Message Rate

You can set an I/O driver's message rate to fine-tine your driver's configuration. To do this, click the Period button and enter a driver period. Follow these guidelines for setting the driver period:

- Enter a value from 1 through 100 in the field. The timer cycle ranges from 1/100 to 100/100 of a second. The default is 5.
- Enter 1 to get the fastest message time (100 messages per second).
- Enter 5 to get a slower message time (20 messages per second).

The driver period can also be specified in the Command Line of the Task Configuration dialog box. Refer to the Configuring Startup Tasks section for more information.

CAUTION: Speeding up the message rate can adversely affect the overall performance of your system, including SAC.

The Datascope Program

The Datascope program displays data that the I/O driver is reading. Refer to your specific I/O driver manual, as well as your process hardware manuals, for more information about the data shown on the Datascope screen.

Starting and Stopping Historical Collect

To start Historical Collect (HTC), click Start. To stop HTC, click Stop. The HTC tabbed page also displays the number of overruns that have occurred while collecting data. For more information on how HTC works, refer to the Trending Historical Data manual.

Viewing SQL Statistics

Mission Control allows you to view SQL statistics while you are connected to an ODBC-supported relational database. Click Start on the SQL tabbed page to load and display SQL data. The statistics displayed correspond to the SQL account and database information you have configured in the SCU. The buttons on the bottom of the tabbed page let you view specific configuration information relating to your ODBC connection. For a description of the fields on the SQL tabbed page, refer to the SQL Tabbed Page Fields section.

Refer to the Configuring iFIX for Relational Databases section for more information on SQL setup. For additional information on SQL, refer to the Using SQL manual.

Viewing SAC Information

You can use the SAC tabbed page of Mission Control to display real-time information on SAC performance.

For more information on SAC, refer to the Scan, Alarm, and Control Program section of the Understanding iFIX manual.

Viewing Auto Alarm Manager Statistics

Using the AAM tabbed page in Mission Control, you can view run-time messages and troubleshooting statistics in a scrollable window.

The lower portion of the tabbed page contains fields that the Auto Alarm Manager uses to display alarm statistics. As alarms are received from the user queue, the number of the alarms is displayed, and errors relating to the alarms are displayed in the remaining fields from top to bottom. These statistics can help you troubleshoot the sending and receiving of alarms. To reset the displayed values, click Reset Statistics.

For a description of the fields on the AAM tabbed page, refer to the Auto Alarm Manager Tabbed Page Fields section.

Refer to the Troubleshooting the Auto Alarm Manager section Implementing Alarming and Messages electronic book for an explanation of the messages that are displayed in the Auto Alarm Manager.

Viewing Alarm ODBC Information

When enabled in the SCU, the Alarm ODBC service sends alarms and messages to an ODBC relational database. The Alarm ODBC tabbed page allows you to view these alarms and messages by

querying the statistics using pre-defined fields.

To save and apply the performance tuning parameters to the local path, click Save. To change the logging state, click Pause.

For a description of the fields on the Alarm ODBC tabbed page, refer to the Alarm ODBC Tabbed Page Fields section.

For more information on the Alarm ODBC service, refer to the Configuring the Alarm ODBC Service section in the Implementing Alarms and Messages manual.

Advanced Topics

This chapter provides you with additional information you can use to configure and tune the network for iFIX. Refer to the following topics:

- Understanding Network Load

- Working with Configurable Session Timers

- Working with Wide Area Networks

- Providing Remote Access

- Network Paths

- Integrating iFIX into Your Network

- Disabling Connections from Unauthorized Nodes

- Disabling Database Write Access for Unauthorized Nodes

Understanding Network Load

You should consider optimizing iFIX to reduce network traffic when your network configuration contains slow links. Slow links are communication links with speeds between 2400bps to 128Kbps. In networks where the slowest link is greater than 256Kbps, the iFIX network load is generally low enough that it does not need to be optimized.

Understanding network messaging is important when planning for network load over a wide area network or other network configurations that contain slow links. To understand network messaging, let's review iFIX architecture.

iFIX uses a client-server model for peer-to-peer communication to share data and alarms in real-time between nodes on a network. For data access, you can consider a iClient node to be a client and a SCADA node to be a server.

All iFIX network conversations are based on transactions. The iClient sends a request to a SCADA server. After the SCADA server acts on the request, it sends a response to the iClient. Network messages are either requests or responses.

The maximum length for a message sent by iFIX to the network interface is 16 kilobytes. One 16 kilobyte message sent by iFIX may be represented on the wire by multiple network packets. The network transport itself also sends network packets for managing the communications between the two nodes and to ensure network messages arrive without errors.

Understanding Network Sessions

All iFIX network traffic is session-oriented. Transactions between two nodes occur over a session. Before a View client can initiate a request, a session must be established with the SCADA server.

Only one socket is created when using iFIX on a TCP/IP network. However, two logical sessions are maintained. The session initiated by the iClient is used to retrieve data from the SCADA servers.

Another session is established from a SCADA server to an iClient to send alarms to the client. In this case, the request portion of the transaction consists of the alarm data and is acknowledged by a response. These two logical sessions are maintained over one physical connection.

To establish a connection, the address of the remote node must be obtained. The method of finding this address, address resolution, is especially important for Wide Area Network (WAN) environments.

Understanding Data Transfer

iFIX applications retrieve real-time data from an OPC server through requests. The most important iFIX application is the Proficy iFIX WorkSpace since it puts the most load on the network.

Objects in an operator display update by polling the OPC server. Each animated object has a configurable refresh rate. This rate determines how often each link requests the current value from the OPC server. When the OPC server is an iFIX SCADA server, object update rates are grouped together and sent as one transaction, up to 16 kilobytes at a time. If the request or response for that group exceeds 16 kilobytes, it is broken up into 16-kilobyte packets.

If more than one picture is open at the same time that has objects to the same SCADA server, there is a separate group for each picture.

When animated objects communicate with a third-party OPC server, data is sent and received according the server's requirements. Refer to your OPC documentation for more information.

Alternative Way of Changing the Refresh Rate

If you find that network traffic is too high with the existing refresh rates and changing them all individually is too time consuming, it is possible to affect them all with one .INI setting. In the FixUserPreferences.ini file in the iFIX Local folder, add the following lines to control the actual refresh times:

```
[OPCEDARefresh]

SetRefreshtoActual=TRUE
```

When set to TRUE, the OPC groups refresh the data at the specified refresh rate. Anything other than TRUE will maintain the normal behavior which is to update the data at 2 times the refresh rate. Normally, the update rate is twice the object refresh rate because under certain timing conditions, the refresh would not reflect the updated data.

WARNING: Be aware that alarms could be lost if you configure the OPCEDA refresh rate to equal the objects' refresh rate.

Understanding Message Sizes

The actual message sizes transmitted by iFIX are dependent upon the type of objects in each picture.

Data links provide you with the option of requesting numeric or text data. Numeric data, the F_ fields, is always transmitted as floating point data and is four bytes in length. Text data, the A_ fields, is transmitted as the ASCII representation of the floating point value and is 12 bytes in length. One method to reduce the iFIX network load is to use only numeric data links.

Some special link types use data that is much larger than 12 bytes. For example, for each chart object,

iFIX transmits approximately 180 bytes.

Alarm Summary objects have their own refresh rate which control how often they are updated. By increasing the values for the alarm refresh and data refresh rates you can fine-tune when iFIX reads data from its alarm queue and displays it.

Understanding Alarm Transfer

Alarm conditions are detected by the Scan Alarm and Control (SAC) program that runs on each SCADA server. The SCADA server sends an alarm message to each node in the network when an alarm is detected. Each alarm is over 1024 bytes in length. The actual message size transmitted by the SCADA server is slightly larger. If several alarms are detected in the same scan cycle, the SCADA server groups as many alarms as possible into a 16 kilobyte message before distributing the alarms to each node.

Optimizing iFIX to Reduce Network Traffic

You can optimize iFIX and reduce network traffic by using the following techniques:

- Use only the objects you really need. If you need more information, create a hierarchy of pictures. Put the objects that give conditional information in a separate picture and only open that picture when those conditions occur.

- Use numeric values (F_) instead of text values (A_). In addition to putting more information on the network, requests for ASCII values also increase the work that the SCADA server must do since the floating point to ASCII conversion is done on the server.

- Minimize the number of different object refresh rates.

- Increase the object refresh rates to decrease the update frequency. For more information on changing the refresh rate, refer to the section Increasing the Refresh Rate.

- Minimize the use of chart objects.

Working with Configurable Session Timers

The following conditions can cause iFIX to temporarily lose a session:

- Running iFIX over a network that contains slow communication links (less than 256Kbps).

- Opening a picture containing many objects on the SCADA server while other iFIX nodes are requesting data from the SCADA server. In this case, the iFIX network task does not get the CPU time that it needs because other programs are competing for CPU resources.

Both of these cases can be solved by increasing the timer values that iFIX uses. These timer values are referred to as configurable session timers.

For more information on session timers, refer to the following topics.

- Understanding iFIX Session Timers

- Determining Session Timer Values

- Configuring Session Timers

Understanding iFIX Session Timers

iFIX uses network session timers to determine that another node is no longer running. Time-out values for every session-oriented message transfer are defined by iFIX when the session is established.

The four time-out values are described below:

Send — defines the amount of time that an iClient waits for a request to the SCADA server to be acknowledged. If this timer expires, the session ends.

Receive — defines the amount of time that an iClient waits for a reply from the SCADA server. When running iFIX over TCP/IP, the effective session time-out value is either the Send timer or the Receive timer, whichever is greater. If this timer expires, the session ends.

Keep Alive — defines the amount of time that, if no activity has occurred over an established connection, an iClient waits before sending a heartbeat message.

Inactivity — defines the amount of time that, if no data activity has occurred over an established dynamic connection, an iClient waits before removing the dynamic connection from the list of outgoing connections. If this timer expires, the session ends.

Determining Session Timer Values

It is important to choose your session time-out values correctly for your application. Values that are too low may cause sessions to be lost even though the remote node is running. Values that are too high may delay session problem notification. When considering what timer values to use, note that the Proficy iFIX WorkSpace may appear to be hung for up to the entire time-out period when sessions are lost. In production facilities, this delay may not give operators sufficient time to react to emergency situations.

For most applications, the default session time-out values are adequate. If you must modify the values to correct transient session losses, use this section to determine the correct values for your application.

iFIX uses the same session time-out values for every session. Changing the session timers affects sessions with every node in your iFIX network. In order to change the session timers, the changes must be made to every iFIX node.

You can also define remote node connection timers for each remote node defined in the SCU. The connection timers are identical to the session timers except that they affect communication with a particular remote node. Typically, the connection timers are used in place of the system-wide session timers when the connection to a remote node differs from the rest of the network. If you need to change these timers, make sure that the computers on both sides of the connection use the same timers.

Configurable session timers can be increased to solve the problems described at the beginning of this section. If you decide to change the values, it is recommended that you increase the Send and Receive values by 10 seconds and test to see if the problem is solved. If the problem persists, repeat the process until the problem is solved.

Configuring Session Timers

Session timers are configured in the SCU. You should only change session time-out values if you absolutely must, and only when you have a complete understanding of the implications.

For more information using the SCU, refer to chapter Configuring iFIX Using the SCU.

Working with Wide Area Networks

iFIX works equally well in a wide area network environment as it does in a local area network. TCP/IP, the iFIX supported network protocol, is especially suited to wide area networks.

Providing Remote Access

You have several choices for enabling computers at separate geographic locations to communicate with each other. Among these choices are remote control and remote access programs.

Understanding Remote Control Programs

Remote control programs take total control of a remote computer and send the remote computer's entire screen over a modem, which can result in slow performance. Note that the screen on both computers is the same. Keystrokes and mouse movements that you make locally are mirrored at the remote computer.

Understanding Remote Access Programs

Remote access programs, like Microsoft's Remote Access Service (RAS), treat a node that is located at a different geographic site as if it were on the local network. Only real-time process data is transferred over the modem. Remote access is usually more appropriate for remote monitoring of iFIX systems.

Microsoft's RAS does not require a dedicated computer to act as a gateway. Many other remote access products require some kind of dedicated computer to perform the gateway function between the LAN and the asynchronous line.

For more information about Remote Access, refer to the following topics:

- Understanding Remote Access Service
- Increasing the Refresh Rate

NOTE: The iFIX SCADA allows all configured network paths to accept connections unless the paths are explicitly disabled in the SCU. This was changed so that an existing RAS connection would still be recognized by an iClient.

Understanding Remote Access Service

Microsoft's Remote Access Service (RAS) provides TCP/IP over phone lines by treating your modem as a network adapter. TCP/IP applications that run over a network can run over a serial connection. iFIX can use the TCP/IP interface provided by RAS to communicate with other iFIX nodes over asynchronous lines.

RAS client and server software are standard with Windows. In general, a RAS client node dials into a RAS server node. A RAS client can dial in and access resources on a Windows RAS server's network. The Windows software allows multiple RAS clients to be connected simultaneously.

Although RAS allows up to 256 clients to dial into a server simultaneously, the practical limit when RAS is used with the iFIX is significantly less. This is due to the additional resources that iFIX requires to communicate. Each simultaneous connection requires a separate modem on the server. Before you incorporate RAS into your production environment, it is strongly recommended that you test the configuration using multiple connections.

Using iFIX in conjunction with a RAS server provides the following capabilities:

- Alarm Summary objects are available.

- Data and alarms are available with one pair of modems.

- Access to the Alarm Startup Queue is available.

- File transfer using Microsoft networking over RAS is available.

- Multiple remote nodes can dial into a server simultaneously.

Use the following guidelines when incorporating RAS into your iFIX network:

- Only use modems with a minimum speed of 9600 baud. Verify that when the RAS connection is made that the modems are connected at a high speed. The faster the baud rate, the better performance you can expect.

- Use the Port Status on both the RAS client and server to troubleshoot connection problems and monitor ongoing communication. Refer to the RAS documentation for more information on using Port Status to troubleshoot communication.

- When browsing on the RAS client to access a remote SCADA server, you can improve performance by copying the file, *nodename*.TAG, from the SCADA server's PDB path to the View client's PDB path.

Increasing the Refresh Rate

The steps that follow explain how to increate the refresh rate of an object.

▶ To increase refresh rate of an object:

1. Double-click the object you want to modify.

2. Click the Browse button to the right of the Data Source field.

3. In the Refresh Rate field, click the drop down menu and choose a rate number that is smaller than your current refresh rate.

4. Switch to the run-time environment, to make sure sessions are not lost and that alarms are received in a timely manner.

   If sessions are being lost or alarms are not received in a reasonable amount of time, increase the refresh rate in 1 second increments until sessions are not lost and alarms are received without delay.

Network Paths

As described in the chapter Getting Started, iFIX supports the TCP/IP network protocol. If an iClient should lose its connection to another node, the local computer attempts to re-establish its connection over all available network paths in parallel.

The computer's network protocol determines the specific network paths. When the computer's protocol is TCP/IP, each IP address is a valid path. IP addresses bound to RAS are also valid but will not start a RAS connection. If there is no RAS connection at the time the computer tries to connect, the attempt for that address fails.

The first successful connection is the one that the iClient uses. Although you cannot specify which network path to use, you can exclude network paths in the SCU. For more information about using network paths, refer to the section Understanding LAN Redundancy in the Mastering iFIX manual.

By default, iFIX enables all available network paths. You can disable any network path you do not want to use. If you subsequently discover you need the path, you can re-enable it later.

Integrating iFIX into Your Network

You may have communication requirements in addition to iFIX communications that must be considered. These network and communication requirements fall into the following categories:

- Additional network software required by the I/O driver you are using.

- File server communication software to allow central storage of data files.

- Relational database communication software.

Integrating solutions to each of these requirements can be a difficult task. It is recommended that you ensure that all the software required to address these requirements works together.

Disabling Connections from Unauthorized Nodes

By default, iFIX nodes accept connections from any remote node over TCP/IP, given adequate resources. However, you may want to prevent unknown or unauthorized nodes from obtaining a connection to a SCADA server by entering specific settings into a network initialization file called NETWORK.INI. This file contains a parameter, accept_unknown_host, which controls whether the SCADA server accepts connections from other computers.

When the parameter is set to ON, the SCADA node accepts connections from any computer. However, when the parameter is set to OFF, access is restricted to the View clients you specify. The exact nodes that can access the SCADA server are defined by listing them in the NETWORK.INI file using the following syntax:

```
hostn=nodename
```

For example, to provide access for the iClients, View01 and View05, to a remote SCADA server, your NETWORK.INI file on the SCADA server should be:

```
[TCPIP]
accept_unknown_host=OFF
host1=VIEW01
host2=VIEW05
```

Later, if you want to restrict access to only View01, you can remove the View05 line from the file. Likewise if you want to provide View04 access to the SCADA server, you can add the following line to the file:

```
host2=VIEW04
```

Notice that View04 is given the same host number that View05 had. This is necessary because all host numbers must be consecutive. For example, you cannot define host1 as View01 and host3 as View04 unless host2 is already defined in the file.

▶ **To restrict access to a SCADA server:**

1. In a text editor, type the following:

   ```
   [TCPIP]
   ```

   ```
   accept_unknown_host=OFF
   ```

2. Add the View clients that can access the local SCADA node.

3. Save the file as NETWORK.INI. Make sure you save the file to the FIX Local path on the SCADA server.

Disabling Database Write Access for Unauthorized Nodes

By default, iFIX SCADA servers accept database write requests from any remote node. However, you may want to prevent unknown or unauthorized nodes from writing to a SCADA server by entering specific settings into the server's network initialization file, NETWORK.INI. This file contains the parameter accept_unauthorized_writes, which controls whether the SCADA server accepts database writes from iClients.

When the accept_unauthorized_writes parameter is not present in the NETWORK.INI file or set to ON, the SCADA server accepts write requests from any computer. When the parameter is set to OFF, access is restricted to the View clients you specify regardless of who is logged into the remote nodes. The exact nodes that can access a SCADA server's database are defined by listing them in the NETWORK.INI file using the following syntax:

```
writenode#=nodename
```

For example, to provide access for the View clients, VIEW01 and VIEW05, to a remote server, configure your server's NETWORK.INI file as follows:

```
[WRITEACCESS]
```

```
accept_unauthorized_writes=OFF
```

```
writenode1=VIEW01
```

```
writenode2=VIEW05
```

If you subsequently want to restrict database access to VIEW01 only, you can remove VIEW05 from the file. Likewise, if you want to provide VIEW10 access to the SCADA server's database, you can add the following line to the file:

```
writenode2=VIEW10
```

Notice that VIEW10 is assigned the same number that VIEW05 had. This is necessary because all node numbers must be consecutive. You cannot define writenode1 and writenode3 without also defining writenode2.

Disabling the Logging of Unauthorized Writes

When the accept_unauthorized_writes parameter is OFF, the SCADA server treats all failed (unauthorized) write attempts as operator alarms and records these write attempts to all the alarm destinations enabled on the SCADA server. Using the parameter log_unauthorized_writes, you can disable the logging of failed writes by setting the parameter to OFF. When the parameter is not present in the NETWORK.INI file or set to ON, the SCADA logs all unauthorized write attempts.

To disable logging of unauthorized writes, configure your NETWORK.INI file as follows:

```
[WRITEACCESS]

accept_unauthorized_writes=OFF

log_unauthorized_writes=OFF

writenode1=VIEW01

writenode2=VIEW10
```

Once you create or modify the NETWORK.INI file, you changes take effect immediately.

You can also restrict database write access by assigning security areas to specific groups and users. For more information about security areas and how to use them with the accept_unauthorized_writes parameters, refer to the Configuring Security Features manual.

▶ **To restrict database write access to a SCADA server:**

1. Open the NETWORK.INI on your SCADA server using a text editor. If available, this file resides in the iFIX Local path. If the file does not exist, create it in the iFIX Local path with your text editor.

2. Enter the following text:

    ```
    [WRITEACCESS]

    accept_unauthorized_writes=OFF
    ```

3. Add the following text if you want to disable the logging of unauthorized writes:

    ```
    log_unauthorized_writes=OFF
    ```

4. Add the View clients that can access the local SCADA server. Use the format:

    ```
    writenode#=nodename
    ```

5. Save the file and make sure the file resides in the iFIX Local path.

Troubleshooting

iFIX provides an extremely secure software interface for controlling your process. Certain conditions, however, such as insufficient memory and computer failure, can cause problems when your system operates. This chapter provides descriptions of these and other typical problems operators may experience. It also lists potential courses of action that you can take to quickly resume normal operation.

- Overview
- Computer Failures
- Problems with Establishing or Losing Sessions
- Troubleshooting Networks
- Troubleshooting Microsoft Networking
- Troubleshooting TCP/IP
- Network Error Codes

Overview

Two key characteristics of your operating system that you must consider if problems occur while iFIX is running include:

Multi-tasking — allowing the operating system to run several applications simultaneously.

Memory management — handling the usage of RAM and, in the case of virtual memory, hard disk space.

Your operating system provides the Control Panel to configure these characteristics. If components within the Control Panel are not configured correctly, your computer may behave strangely or stop working. For more information, refer to the following topics:

- Understanding the Control Panel
- Avoiding Problems

Understanding the Control Panel

Your operating system's Control Panel lets you set up the following computer components:

- Video driver
- Network card
- Mouse
- Keyboard
- System (used to set up virtual memory)

- Drivers (used to set up sound boards and the timer driver)

- Services

These configuration components are critical to troubleshooting insufficient memory and computer failure problems. Instructions for accessing and implementing changes to these components are provided in your operating system's documentation.

Avoiding Problems

You can avoid problems by configuring your system properly before operation. When troubleshooting, always try to simplify your system and remove any unnecessary hardware or software.

The following list is the minimum recommended configuration you should adhere to while troubleshooting problems:

- Use recommended computers, as described in the section Recommended Computers.

- Use recommended network hardware and software, as described in the chapter Networking iFIX Nodes.

- Use standard video adapters and drivers.

- Avoid using the power-saving feature that can be configured on some computers.

Make sure that all iFIX nodes comply with these recommendations.

Computer Failures

Computers can sometimes stop working without warning. In these cases, the computer may or may not display error messages to help you determine what happened. These failures can be caused by:

- Memory conflicts between two or more drivers.

- Wrong network driver versions.

- Incorrect operating system setup information.

- Old 3COM network cards.

Troubleshooting Computer Failures

If you experience computer failures, try to resolve them using the tips below:

- If you are using a 3COM network card, verify that the card is a 3C905 or 3C509.

- See what other boards may be in the machine, such as a video board or a memory-resident interface card. Find out the memory addresses and interrupts that these boards are using and resolve any conflicts.

- If you have a network card installed, make sure that it is listed in the Control Panel.

Problems with Establishing or Losing Sessions

You can lose communication sessions because your network times out. These time-outs usually occur on the client side of a session. The primary reason for time-outs is that iFIX network tasks on the SCADA server or iClient did not get enough CPU time to service a request.

NOTE: Network sessions may be lost when you open large pictures. iFIX re-establishes the session after the picture finishes opening. To eliminate this problem, use the information in the section Working with Configurable Session Timers.

The following factors prevent the network task on the SCADA server or iClient from getting enough CPU time:

- Heavy disk activity.

- Large picture calculation time.

- SAC running to completion when database overruns occur.

- Database Manager sorting.

- Historical Collect closing and starting a new file.

- Other applications, such as iFIX WorkSpace, Historical Collect, and Database Manager, taking time-slices before data can be processed.

Troubleshooting Networks

If you are experiencing network problems while trying to run iFIX, use the following steps to identify the problem area.

▶ **To troubleshoot network problems:**

1. Refer to the Networking iFIX Nodes section to ensure that the network hardware and software are properly configured. Unless otherwise indicated, it is recommended that you use the latest version of your chosen network software.

2. Verify that the network software itself is working properly prior to running any iFIX program using:

    - the steps in the Troubleshooting Microsoft Networking section to test communications between nodes,

    - the PING program described in the Using PING section to verify a physical connection to a remote computer, and

    - the TCPTEST diagnostics tool described in the Working with TCPTEST section to verify that the TCP socket layer works and that iFIX can communicate to it successfully.

3. Use the error codes in the Network Error Codes section to modify iFIX configuration if you continue to have problems keeping iFIX sessions active.

4. Use the Network Diagnostics program, NETDIAG, by clicking the Start button, Run, and then typing the following on the command line:

    ```
    NETDIAG<Enter>
    ```

The NETDIAG program creates the file, NETDIAG.DAT, in the Application path. This file can be sent to Technical Support for further assistance.

Troubleshooting Microsoft Networking

If you experience network problems with iFIX, verify that the network software is loaded and working properly. The test described in this section must work in order for iFIX networking to function properly. This test uses the file sharing capabilities inherent in Microsoft networking to test the network. You do not need to start iFIX in order to run this test.

▶ **To test communications between two nodes:**

1. Start both computers.

2. Enable file sharing on each computer. See your operating system's documentation for more information on how to configure file sharing.

3. Define a shared directory on each computer. See your operating system's documentation for information on sharing a directory.

4. Configure a network drive, for example D:, on each node that points to the shared directory on the other computer. Click the Map Network Drive button (available on the toolbar of any window) to select the shared directory configured in step 3.

This test must run successfully. If it does not, refer to the chapter Networking iFIX Nodes and ensure that the network is configured properly.

Troubleshooting TCP/IP

If you experience difficulty establishing network communications, your TCP/IP software and the iFIX TCP/IP network software provide some utilities to help locate the cause of the problem. These utilities are described in the following sections.

- Using PING

- Working with TCPTEST

- Working with NETDIAG

Using PING

PING is a TCP/IP diagnostic utility that helps to isolate network hardware problems and incompatible configurations by allowing you to verify a physical connection to a remote computer. PING must run successfully before iFIX can run properly. To run PING, type the following from the command line:

        PING *SCU_nodename*<Enter>

For example, to test a connection from a View node to the local SCADA node, SCADA01, type the following:

        PING SCADA01<Enter>

See your TCP/IP manuals for additional information on using PING.

Working with TCPTEST

Another utility, provided by GE Intelligent Platforms, is the TCPTEST diagnostic program. To run TCPTEST, click the Start button, click Run, and then type the following into the command line:

```
TCPTEST parameters <Enter>
```

where *parameters* are one or more of the following command parameters in the table. To display a list of parameters on the screen, type the following:

```
TCPTEST <Enter>
```

The program requires two nodes to run, one as a client and one as a server. Set up the server node first, as follows:

```
TCPTEST /S <Enter>
```

The client node must use as a minimum the following TCPTEST parameters:

```
TCPTEST /C /Rnodename <Enter>
```

where *nodename* is the SCU node name of the server node. For example, to make VIEW01 a server, run TCPTEST with the /S parameter, as shown above. To communicate with VIEW01, go to another node and type the following:

```
TCPTEST /C /RVIEW01 <Enter>
```

<table>
<tr><th colspan="2">TCPTEST Parameters</th></tr>
<tr><th>The parameter...</th><th>Lets you...</th></tr>
<tr><td>/B<i>x</i></td><td>Set the receive and send buffer size to <i>x</i>. The default size is 1400 messages. If you specify this parameter, make sure that both nodes have the same buffer size.</td></tr>
<tr><td>/C</td><td>Set up a node as a client. This parameter requires you to provide the remote server node name (see the /R parameter below).</td></tr>
<tr><td>/D</td><td>Display run-time information (such as the data received).</td></tr>
<tr><td>/F<i>x</i></td><td>Set to <i>x</i> milliseconds, how often to send messages. By default, messages are sent as fast as possible.</td></tr>
<tr><td>/P<i>portnumber</i></td><td>Use <i>portnumber</i> in place of the default ports for both the server node and the client node.</td></tr>
<tr><td>/R<i>server</i></td><td>Specify the name of the remote server node.</td></tr>
</table>

TCPTEST Parameters	
The parameter...	**Lets you...**
/S	Set up this node as a server.
/T*x*	Set the TCP time-out value for sending and receiving data to *x*. This parameter is supported only if your WINSOCK implementation supports changing the TCP time-out value. Most implementations do not.
/W	Test the WINSOCK interface and display WSAData (for example, vendor information).

It is recommended that you run TCPTEST without iFIX running. If you need to run both at the same time, be sure to change the port number (/P) that TCPTEST uses. Otherwise, a conflict may occur with the data being passed because, by default, TCPTEST uses the same port number as iFIX. Note that the client and server must use identical port numbers when using TCPTEST.

Working with NETDIAG

NETDIAG provides comprehensive network diagnostic information and stores its information in the file NETDIAG.DAT. This file resides in the Application path.

To run NETDIAG, click the Start button, click Run, and then type the following on the command line:

```
NETDIAG<Enter>
```

Network Error Codes

The following sections list the error codes, messages, and explanations for the network errors you can encounter if you experience problems with your network.

- Startup Error Codes
- Run-time Error Codes

Startup Error Codes

If a network problem occurs during startup, one of the error codes or messages listed in the following table may appear.

Startup Error Messages		
Error Code	**Error Message**	**Description**
1613	Duplicate name in local name table.	iFIX did not shut down properly prior to starting back up. Restart the computer and iFIX.
1622	Name in use on remote node.	The node name assigned to the node is currently in use on another node. Rename one of the nodes to correct this conflict.
8501	Underlying network subsystem not ready.	TCP/IP is not installed properly or is missing. Use PING or TCPTASK to verify that the underlying TCP/IP is set up before attempting to run iFIX.
8502	TCPTASK: Failed to initialize network subsystem.	
8503	Windows Sockets API version mismatch.	When attempting to initialize the Winsock TCP/IP interface, TCPTASK detected that the Winsock version is less than 1.1.

Run-time Error Codes

If a network problem exists that prevents sessions from establishing or causes sessions to be terminated, one of the error codes listed in the following table may appear in the NETDIAG program.

Run-time Error Codes		
Error Code	**Error Message**	**Description**
1605	Command timed out.	These errors occur when the remote node is down. When the remote node is brought back up, the Connection Manager re-establishes the session.
1608	Invalid Local Session Number.	
1610	Session Closed.	
1624	Session Ended Abnormally.	

Run-time Error Codes		
Error Code	**Error Message**	**Description**
1620	Can't find name called.	The session cannot be established because either a remote node is not operating, a cabling problem exists between the nodes, or the remote node name is not registered on the network. Verify both nodes are running compatible network software.
1914	Connection NOT established with node.	The Connection Manager has not yet established a connection with the remote node. Wait for Connection Manager to establish the session.
1960	FIX dynamic connection in progress.	Connection Manager is in the process of establishing a dynamic connection with the remote node. Wait for Connection Manager to establish the session.
1964	FIX has been shut down on remote node.	Connection Manager has detected that iFIX has been shutdown on the remote node. This error code shows up temporarily and then changes to 1914.
8517	Node not found in TCP hosts database.	The node name that you are trying to connect to be resolved to an IP address. The name is probably not in the local hosts file or on the WINS server. Obtain the remote node's IP address and add it to the HOSTS file.

Mission Control Field Descriptions

The following sections describe the functions of dialog fields, diagnostics, and statistics found in the tabbed pages of Mission Control. Refer to the Monitoring the Environment with Mission Control chapter for detailed information on how Mission Control works.

- I/O Control Tabbed Page Fields

- HTC Tabbed Page Fields

- SQL Tabbed Page Fields

- SAC Tabbed Page Fields

- Auto Alarm Manager Tabbed Page Fields

- Alarm Synchronization Tabbed Page Fields

- Alarm ODBC Tabbed Page Fields

I/O Control Tabbed Page Fields

The table below lists the available options on the I/O Control tabbed page.

I/O Control Tabbed Page Options	
Select this button...	**To...**
Datascope	Run the Datascope program for the selected I/O driver.
Stop/Start	Stops or Starts the selected I/O driver, depending on the I/O driver's current status.
Next Chan and Prev Chan	Select the COM port from which to display messages.
Pause/Update	Temporarily stop and restart the Datascope program.
Close	Close the dialog box.
Period	Configure the driver's message rate.

HTC Tabbed Page Fields

The following fields are used on the HTC (Historical Collect) tab:

Collector Status – displays the status of the Proficy Historian collector running on the local machine, if any. The options are stopped, started, or paused. The collection status changes when you use the Stop and Start buttons. This field is visible only if you have Proficy Historian running.

Overruns – displays the number of overruns that occurred while collecting data. The overrun counter increments by one each time an historical collection is unable to collect data at the rate you configured. You can determine if there is a problem in your collection scheme by examining the number of HTC overruns. When Historical Collect cannot collect all of the data at the rate specified, a historical collect overrun can occur. When an overrun occurs, values for some tagnames in the group are not collected at the configured rate. Temporary conditions, such as heavy network traffic, network upsets or off-line nodes, can cause overruns. However, a repeated number of overruns may indicate that the phase value for the group needs adjustment. You can prevent overruns by phasing the data collection rate. Refer to the Defining a Collection Group section of the Trending Historical Data manual for information on phasing to prevent overruns.

NOTE: Preventing overruns by phasing applies only to Classic Historian; it does not apply to Proficy Historian.

Start – starts the historical collection.

Stop – terminates the historical collection.

For more information on how HTC works, refer to the Trending Historical Data manual.

For specific information on using data collection with Proficy Historian, refer to the Proficy Historian Administration Manual.

SQL Tabbed Page Fields

There are several buttons on the SQL tabbed page. These buttons are described as follows:

Status – displays the status of your SQL configuration. The statistics correspond to the SQL setup information you configured in the SCU.

Acct. Status – re-queries your SQL account and displays the status of that account as configured in the SCU. Lists how many SQL accounts are currently connected.

Cache – displays whether caching is enabled or disabled.

Login – displays your SQL login information.

Stop – terminates the current SQL query.

SAC Tabbed Page Fields

You can start and stop SAC from running using the Stop and Start toggle buttons on the SAC tab of Mission Control. The Status field indicates if SAC is running or stopped. All other fields are used internally by Technical Support for debugging purposes.

Auto Alarm Manager Tabbed Page Fields

The following fields on the AAM tab in Mission Control allow you to monitor and troubleshoot the Auto Alarm Manager:

Send Alarm Statistics

Alarms from User Queue – the number of alarms retrieved from the Auto Alarm Manager's alarm queue.

Alarms failed Block Alarm Filter – the number of non-block alarms (for example, event messages and operator messages) retrieved from the Auto Alarm Manager's alarm queue. The Auto Alarm Manager only sends block alarms to the Receiving node.

Alarms failed Alarm Area Filter – the number of alarms that have been filtered out based on their alarm area. You can control the alarm areas to filter on by selecting them from the Send Alarm Filters dialog box.

Alarms failed Alarm Priority Filter – the number of alarms that have been filtered out based on their alarm priority. You can control the alarm priority to filter on by selecting one from the Send Alarm Filters dialog box.

Alarms Packaged – the number of alarms the Auto Alarm Manager has prepared for delivery to the Receiving node.

Primary Delivery Attempts – the number of transmissions the Sending node has attempted to deliver to the primary contact.

Secondary Delivery Attempts – the number of transmissions the Sending node has attempted to deliver to the secondary contact.

Retries – the number of times the Sending node has redialed the primary or secondary contact.

Successful Deliveries – the number of transmissions the Sending node delivered to the Receiving node.

Failed Deliveries – the number of transmissions the Sending node failed to deliver to the Receiving node. When a failure occurs, the Auto Alarm Manager sets the emergency tag.

Receive Alarm Statistics

Mgmt Pkt Received – the number of management packets that have been delivered to the Receiving node. A management packet contains the protocol information to start and stop a

transmission from the Sending node to the Receiving node.

Alarm Pkt Received – the number of alarm packets that have been delivered to the Receiving node. An alarm packet contains up to six alarms.

Alarms Received – the number of alarms the local node has received.

Alarm Synchronization Tabbed Page Fields

The fields on the Alarm Synchronization tabbed page are described below.

Alarm Packets From Sync Queue – the number of alarm packets that were presented to the alarm acknowledgement synchronization task for processing.

Num Alarms Processed – the number of alarms that were processed by the alarm acknowledgement synchronization task. An alarm packet contains more than one alarm.

Num Alarms Failed Tag Resolution – the number of times the alarm acknowledgement synchronization task could not determine the tagname for an alarm.

Num Alarms Failed Local Status Read – the number of times the alarm acknowledgement synchronization task could not determine whether the local tag was already acknowledged.

Num Not In Alarm – the number of times the alarm acknowledgement synchronization task detected that the tag did not need to be acknowledged.

Num Alarms Failed Local Ack – the number of times the alarm acknowledgement synchronization task failed to acknowledge an alarm.

Num Alarms Acknowledged – the number of alarms acknowledged by the alarm acknowledgement synchronization task.

Alarm ODBC Tabbed Page Fields

The fields on the Alarm ODBC tabbed page are described below:

Database Id – the database ID as entered in the SCU.

Connection State – displays either CONNECTED to indicate a successful ODBC connection to the database, or LOST CONNECTION to indicate that the connection was not successful or was lost.

Table Name – the table name in the database as entered in the SCU.

Logging State – Displays either Active, indicating that alarms are taken from the queue and logged to the ODBC database, or Paused, indicating that alarms are taken from the queue and dropped (and thus are not logged to the ODBC database).

Reconnections – the number of times you needed to reconnect to the database.

Alarms Pending – the number of alarms in the user queue waiting to be processed.

Alarms Logged – the number of alarms successfully logged to the ODBC database.

Index