GE VERNOVA

PROFICY® SOFTWARE & SERVICES

# PROFICY iFIX HMI/SCADA

## Configuring Security Features

GE VERNOVA

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



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

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

All other trademarks are the property of their respective owners.

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

# Table of Contents

# Configuring Security Features

Configuring Security Features is intended for system administrators who must configure and maintain security for iFIX® systems. The manual explains the concepts of iFIX security and steps you through the process of configuring iFIX security.

## Reference Documents

For related information about iFIX, refer to the following manuals:

- Understanding iFIX
- Writing Scripts
- Creating Recipes
- Using Electronic Signatures
- Setting Up the Environment

# Introduction

As iFIX monitors your process, it creates data files, such as alarm files; iFIX also modifies and updates other data, such as the process database. In some companies, access to iFIX applications and data files is available to everyone. In such an environment, changes to the data files and access to iFIX files and applications are not critical to the process. However, in other companies these applications and data are only available to authorized personnel because they are critical to the process.

iFIX provides an integrated security program to assist you in protecting your process. Refer to the following sections for more details:

- Protecting Your Process
- iFIX Security Concepts
- Understanding Security Status

## Protecting Your Process

There are different levels of security that you can implement to protect your process. On one level, you can control the physical security of your machines and buildings. On another level, you can implement security for your operating system and your network using firewalls, passwords, and filters.

You can also restrict access to your iFIX applications and files, and protect your data files from unauthorized changes, by enabling iFIX security. This manual focuses on iFIX security. iFIX security is optional and is disabled by default. When you enable iFIX security, you can restrict:

- Access to iFIX programs, operator displays, schedules, and recipes.
- Access to critical program functions (for example, reloading the process database).
- Write access to the process database.
- Data entry and alarm acknowledgement, by requiring electronic signatures and verification. This can assist you in becoming compliant with the 21 CFR Part 11 regulation.

Enabling security also allows you to track all the changes to the process database and forces operators to log in to iFIX. Logging in requires a login name and an optional password. Depending on your configuration, this data can be the same or separate from your Windows® login name and password. Refer to the Using iFIX with Windows Security chapter for more information.

iFIX security is user-based, meaning operators cannot access iFIX applications, files, or database blocks unless you assign access to them. Assigning program, file, or database access to an operator is commonly referred to as assigning a privilege to that operator.

You can enable security using the Security Configuration program. This program is a flexible and easy-to-use application that lets you assign operator rights, login names, and passwords. Refer to the Defining and Assigning Security Privileges chapter for more information

## iFIX Security Concepts

Before you restrict access to iFIX applications and files, you need to understand how security works. The security concepts described in the following list are described in more detail in the Understanding iFIX Security chapter. For information on using the concepts, see the Defining and Assigning Security Privileges chapter.

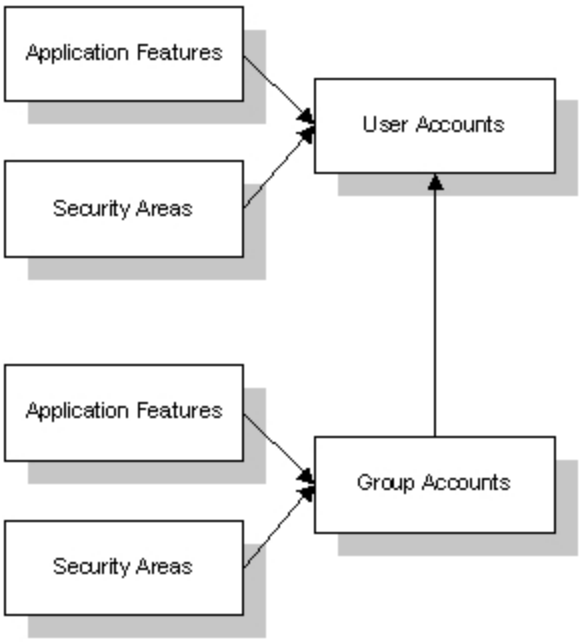
**User Account** – defines the privileges assigned to one person. iFIX identifies each user account with a login name and an optional password. User accounts can belong to one or more groups. When a user account belongs to a group, it inherits all the privileges associated with the group. The user account can have privileges in addition to the group privileges.

**Group Account** – assigns access to the most commonly-used privileges that two or more people must share. Allows you to bundle a set of privileges and assign them in one step to a user account.

**Application Feature** – a privilege that allows an operator to access specific application functions. For example, the WorkSpace Runtime application feature provides access to the WorkSpace run-time environment. To help simplify explanations, this manual collectively refers to applications and specific application functions as application features.

**Security Area** – a physical or functional division of a plant. For example, security areas can be process hardware (such as pumps or ovens), utilities (such as fuel, water, or steam), or maintenance functions.

The following figure shows how user accounts, group accounts, application features, and security areas interrelate. Each user account has privileges that are directly assigned and inherits any privileges assigned to the groups to which the user account belongs.




*Security Concepts*

**Electronic Signature** – uniquely identifies operators performing or verifying changes to your process. You can require operators to enter a user name and password before acknowledging an alarm or entering data. This functionality can assist you in becoming compliant with the 21 CFR Part 11 United States FDA government regulation.

**Run-time Environment Protection** – restricts the things that operators can do during iFIX WorkSpace Run Mode. For example, you can prevent operators from switching to other applications or exiting the WorkSpace when you have Run-Time Environment Protection enabled.

## Understanding Security Status

When you initially start the iFIX Security Configuration program, iFIX security is disabled. The Security Configuration program indicates this status by displaying an open lock on the screen. While security is disabled, anyone can use iFIX programs or modify iFIX configuration files without restriction. Electronic signature capability is also disabled when security is disabled.

When you enable security, the lock closes and operators must log into iFIX with their user accounts to gain access. For instructions on enabling and disabling security, refer to the section Enabling and Disabling Security.

# Understanding iFIX Security

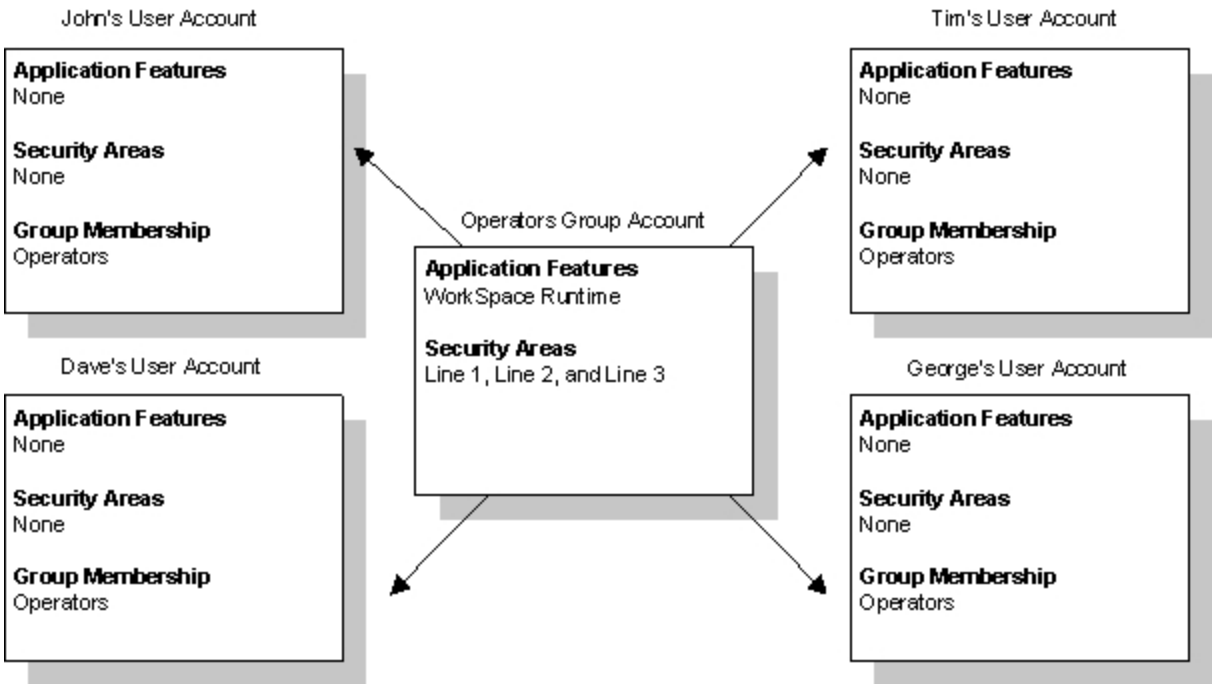
Your main design goal when developing an iFIX security strategy is to create group and user accounts. Using groups minimizes the amount of work needed to create the accounts while providing you with flexibility and power. For example, instead of creating five operator accounts that all assign the same security areas and application features, you can create one group account with these privileges and then assign the group account to the five operators.

To achieve this goal, assess your operators' needs and identify the common privileges they require. Once you identify these common privileges, you can create group accounts that provide them.

For example, John, Dave, Tim, and George are all iFIX operators. Their needs are summarized in the following table:

| User name | Application features | Security areas |
|---|---|---|
| John | WorkSpace Runtime | Line 1, Line 2, and Line 3 |
| Dave | WorkSpace Runtime | Line 1, Line 2, and Line 3 |
| Tim | WorkSpace Runtime | Line 1, Line 2, and Line 3 |
| George | WorkSpace Runtime | Line 1, Line 2, and Line 3 |

Since each operator requires access to the same application features and security areas, it is possible to create a group account called *Operators* that provides these privileges. Once you create the group account, you can assign it to each operator's user account, as the following figure shows.




*Assigning Account Privileges with a Group Account*

## Security Files

You can share iFIX security files among all your iFIX nodes. However, you cannot share these files with FIX32 nodes. If you have a network with nodes of both types, use one set of security files for your iFIX and another set for your FIX32 nodes.

| When you... | You... |
|---|---|
| Do not share security files. | Must copy the security files to each iFIX node. |
| Share security files. | Can make system-wide changes quickly and avoid the need for copying files. |

### Using Security with a File Server

Using a file server, you can eliminate the need to copy security files to multiple computers. The simplest way to share your security files is to enter your file server path as the security path. To learn how to change the security path, refer to the section, Defining the Security Path.

### Using Security Without a File Server

You can set up security without a file server by storing all the security files and the Security Configuration program on each local computer. The security files reside in a path called the security path, which the Security Configuration program defines.

Security also keeps another copy of the security files in a path called the backup path. Security uses this path when it cannot find the security path, for example, if the security path becomes unavailable.

Once you set up security and enable it on one computer, you must duplicate the security configuration on every node. The simplest way to do this is to copy your security files to every computer on your network. For a list of files to copy, refer to the Troubleshooting chapter.

Also, make sure you enable security on every node. Otherwise, security may not function properly.

## User Accounts

A user account defines the privileges assigned to one person. iFIX identifies each user account with a login name and an optional password. User accounts can belong to one or more groups. When a user account belongs to a group, it inherits all the privileges associated with the group. The user account can have privileges in addition to the group privileges

When designing a user account, always include the user's full name, login name, and password in your security plan. If you plan to use Windows security, you should also include the domain name if you plan to store the user accounts on a domain controller.

Including the user's full name is especially important when you are using electronic signatures, because the full name is recorded in messages sent to the audit trail for electronic signatures.

Including the password is particularly important because iFIX security does not display user account passwords. Consequently, including user passwords ensures that you provide the correct password to your operators.

**NOTE:** iFIX user passwords are case insensitive when not using Windows security.

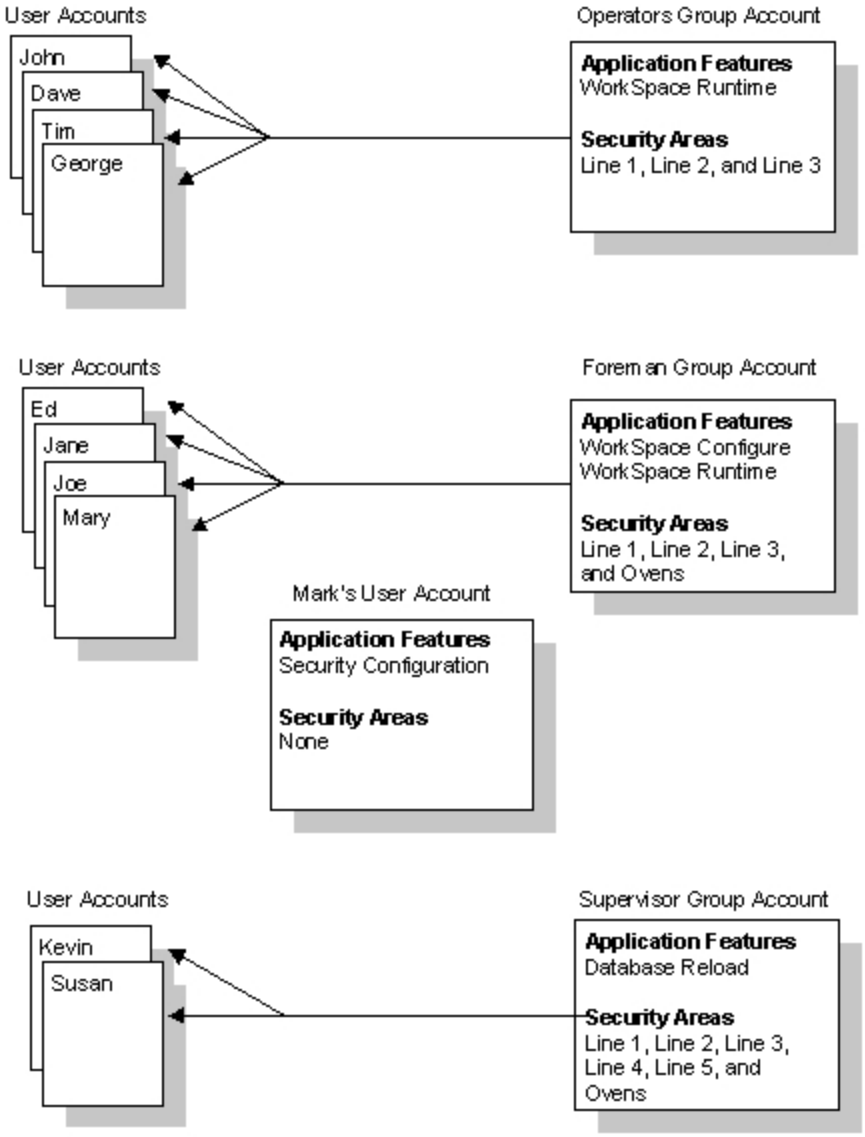
## Group Accounts

Whenever possible, use group accounts to assign the majority of account privileges. You greatly simplify creating a security configuration if you take the time and effort to assess your operators' needs. If the security requirements at your site do not warrant such an effort, use the sample group accounts provided. These accounts provide you with a simpler approach to Configuring Security Features. For example, the sample group accounts define functional roles in a manufacturing facility. You could easily create other group accounts, such as those listed in the following table.

| To create a group account for... | Assign the following application features... |
|---|---|
| Database Designers | Database Block Add-Delete, Database Manager, Database Reload, and Database Save. |
| Operator | WorkSpace Configure, WorkSpace Runtime, WorkSpace Runtime Exit, Enable Task Switching, Runtime Visual Basic Editor Access, Database Manager, Database Save, Database Reload, and Database Block Add/Delete. |
| Display Designers | |
| Recipe Developers | Recipe Builder Development Window, Recipe Download from the Recipe Builder, Recipe Save from the Recipe Builder, Recipe Upload from the Recipe Builder, and Recipe Text Output from the Recipe Builder. |
| Supervisors | WorkSpace Runtime, WorkSpace Runtime Exit, and Enable Task Switching. |

Typically, when assigning privileges to an operator, you select the necessary group accounts first. This assigns common privileges needed by two or more operators doing similar tasks. Then, you can add any specific privileges an operator may require. Configuring your group and user accounts in this way provides a modular approach that is easy to maintain.

For example, in the following figure, the group account **Operators** defines access to the iFIX WorkSpace run-time environment and specific security areas. These privileges define the common security rights shared by all operators. If an individual operator needs additional rights, for example, to enter electronic signatures, you can assign those rights in his or her own user account.

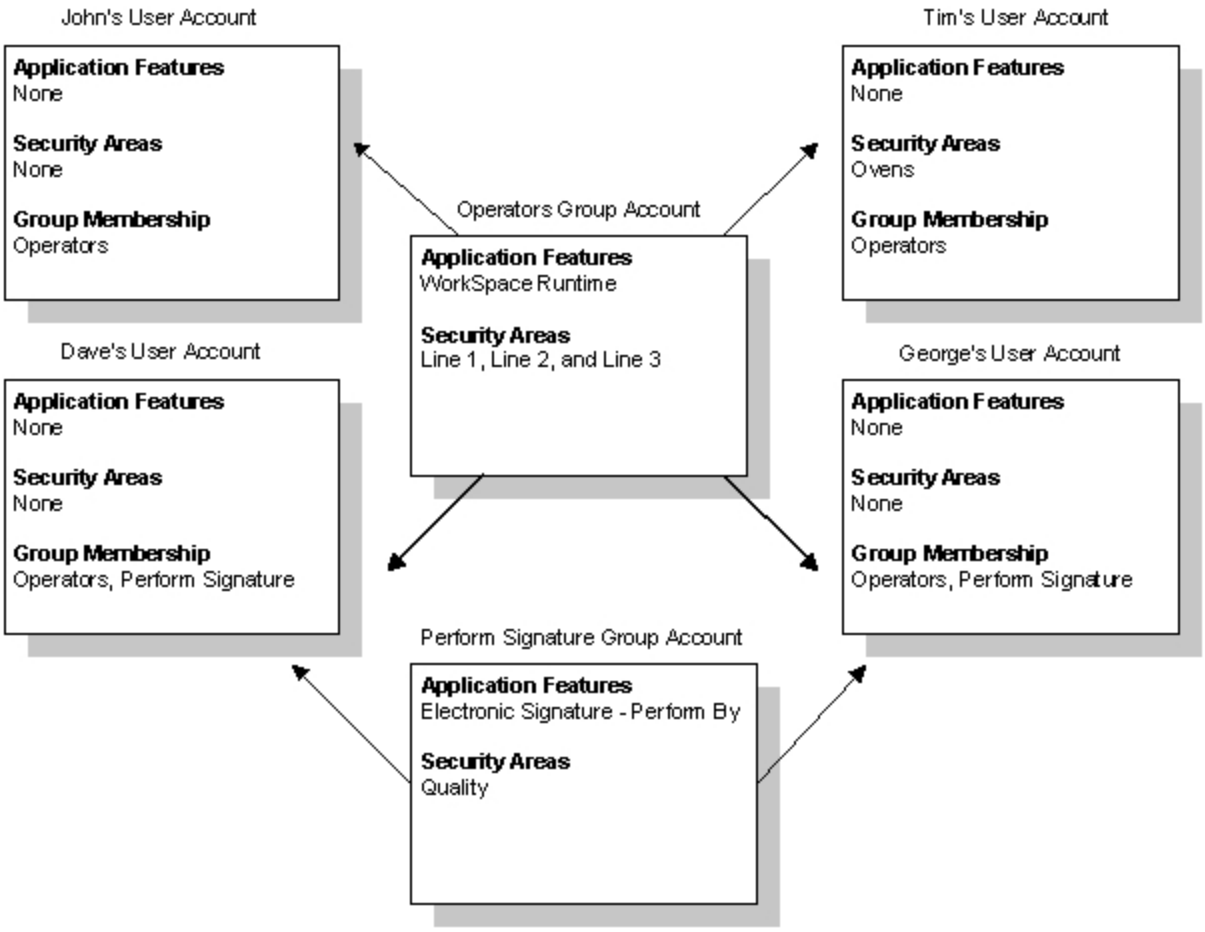



*Sample Accounts*

## Assigning Privileges

After you create your group accounts, you can assign any remaining privileges to individual user accounts. These remaining rights should be unique privileges assigned to one person. If, however, you find that two or more operators require the same privileges, consider creating additional group accounts.

For example, consider the operator accounts for John, Dave, Tim, and George. Assume that George and Dave need additional privileges to perform electronic signatures and access another security area, while Tim needs access to the functional security area Ovens. Since Tim is the only operator who requires access to this security area, you can assign it directly to his user account. However, because both George and Dave require an extra application feature and security area, you might want to create a second group account to provide these privileges. This is illustrated in the following figure.




*Assigning Extra Rights with Group Accounts*

## Identical User Accounts

While the best way to maintain flexibility in your security strategy is to define common privileges with group accounts, you may find it easier not to use them. In general, this happens when you only have to create a small number of identical user accounts. If you decide not to include group accounts in your security plan, you can save time creating identical user accounts as described in the following steps.

**To create identical user accounts:**

1. Create one user account.
2. Export your security configuration.
3. Open the export file in a text editor.
4. Copy and paste the user account as many times as needed.
5. Change the user name, login name, and password of each user account.
6. Save the file and import it back into the Security Configuration program.

For more information on using this method, refer to the section Importing and Exporting the Security Configuration.

## Security Areas

You should keep a separate list of security areas as you plan each group and user account. When you finish, the resulting list contains the names of the security areas you require, allowing you to define your security areas in one session instead of multiple sessions.

Security areas restrict access to database blocks, operator displays, schedules, and recipes. The following table summarizes the access restrictions provided by security areas.

| When you assign a security area to a... | You restrict... |
|---|---|
| Database block | Write access. Read access to blocks is available from any operator display. |
| Operator display, schedule, or recipe | Read access to the file. |

If someone attempts to change a block's value illegally, security generates a message containing the login name of the person who attempted the change. iFIX sends this message to the security audit trail and every enabled alarm destination except the Alarm Summary. To learn more about these messages, refer to the Implementing Alarms and Messages manual. To learn about the security audit trail, refer to the Understanding the Security Log File section.

### Creating a Recipe User Account

Using the GE recipe package, you can download recipes to a process database. Typically, when security is enabled, you can protect the blocks in each process database by assigning them to security areas. As a result, recipe downloads can fail because the current operator may not have rights to change the blocks to which the recipe writes.

You can eliminate this problem by creating a recipe user account. This account defines the security areas to which your recipes can download. When a download begins, iFIX examines the security areas assigned to the Recipe user account instead of the currently logged in operator.

You can create a Recipe user account by:

- Naming it **RECIPE**.
- Defining the required security areas.

Once you create the account, copy it to the security path of every SCADA server.

**IMPORTANT:** Security loads the Recipe user account into memory the first time a recipe downloads. If you modify this account, the local computer continues to use the version in memory. To force the computer to reread the new version, log out the current user, log in with the Recipe user account, and log out again.

**Do Not Use "RECIPE" as a Domain User Account**

Be aware that using "RECIPE" as a domain user account is not supported in the iFIX product. If you do attempt to use RECIPE as a domain user name, you will be able to download a recipe on a SCADA node, but not on a View node.

## Application Features

You should familiarize yourself with the available application features before you design any group or user account. Very often it is possible to assign an application feature for a specific application function, such as the iFIX WorkSpace run-time environment, without providing access to the entire application. The following table lists the available application features.

**Application Feature Descriptions**

| Application Feature | Allows the user to... |
|---|---|
| Alarm Shelving | Shelve alarms in run mode. If the Alarm Shelving feature is not enabled for a user, the user will not be able to shelve an alarm even if the alarm shelving is enabled on that block. |
| Application Validator - Creation of Baselines | Generate baseline files in the Application Validator. |
| Application Validator - Run-time Access | Run the Application Validator and generate reports. |
| Background Task Exit | Stop any background task such as SAC, or Session Monitor. |
| Batch Execution - [Action Name] | Perform a specified action in the Batch Execution product. |
| Change Management | Use Change Management version control features in iFIX. |
| Data Provider Service | Use the Data Provider Service feature in iFIX. |
| Database Block Add-Delete | Add a block to, delete a block from, or modify a block in a database.<br>**NOTE:** In FIX32, this application feature only allows add and delete functionality. |
| Database Manager | Configure individual blocks in a database and import, export, save, print, query, sort, and summarize the contents of a database. |
| Database Reload | Reload the database in memory or load a different database. |
| Database Save | Save the database in memory to disk. |
| EDA Feature 1-55 | Access an Easy Database Access (EDA) application feature. You can provide access for up to 55 EDA application features. |
| Electronic Signature - Bypass | Bypass the Electronic Signature option, and test an application without the need to repeatedly enter signatures.<br>**NOTE:** Selecting Add All when you are adding application features to a user or group |

| | |
|---|---|
| | account will not add this application feature. You must select it explicitly. |
| Electronic Signature - Perform By | Perform signed actions. |
| Electronic Signature - Verify By | Verify signed actions. |
| Enable Ctrl-Alt-Del | Log off, shut down the computer, access the Windows Task Manager, or change the computer's password by pressing Ctrl+Alt+Del.<br><br>The logged-in user needs this if iFIX is running as a service and they log off the machine. |
| Enable Task Switching | Switch between tasks. |
| FIX32 - [Action] | Perform a specified action in a FIX Desktop application. Be aware that FIX Desktop is no longer supported, as of iFIX 5.8. |
| GE OEM Reserved 1-12 | Access an application feature defined by an OEM (Original Equipment Manufacturer). You can provide access for up to 12 OEM application features. |
| Historical Trend Assign | Configure the Classic Historical Assign program. |
| Historical Trend Collection | Stop the Classic Historian HTC program. |
| Historical Trend Export | Legacy application feature that is not used in iFIX. |
| iFIX - System Shutdown | Shut down iFIX. |
| Manual Failover | Allows you to manually initiate a connection or SCADA failover. |
| OPC UA Configuration Tool | Run the OPC UA Configuration tool on a SCADA Server, or change and save OPC UA configuration information. |
| Project Backup-Restore | Back up and restore the iFIX files on the local node. |
| Recipe Builder Development Window | Create master and control recipes, enable and disable the audit trail, assign tag groups to recipes, and scale a batch. |
| Recipe Builder Operations Window | Modify control recipes and override recipe items within specific limits. |
| Recipe Download from Recipe Builder | Download recipes from the Recipe Builder. |
| Recipe Load | Legacy application feature that is not used in iFIX. |
| Recipe Save | Legacy application feature that is not used in iFIX. |
| Recipe Save from Recipe Builder | Save recipes. |

| | |
|---|---|
| Recipe Text Output from Recipe Builder | Create recipe reports, master text recipes, and control text recipes. |
| Recipe Upload from Recipe Builder | Upload recipes from the Recipe Builder. |
| Runtime Visual Basic Editor Access | Open the Visual Basic Editor from the run-time environment. |
| Security Configuration | Configure the security system, create and delete user and group accounts, and name security areas. |
| Security Synchronizer | Run the Security Synchronizer. |
| Startup Profile Manager | Run the Startup Profile Manager application. |
| System Configuration | Configure node connections, system paths, alarm services, and the SCADA configuration for a node. |
| System User Login | Log in as the system user. |
| System User Logout | Log out as the system user. |
| Tag Group Editor | Create, edit, and save tag groups.<br>**NOTE:** When you assign the Tag Group Editor application feature to a user, you must also assign the WorkSpace Configure application feature to that same user. If both these application features are not assigned, the user is considered unauthorized for the Tag Group Editor application. |
| Tag Status | View tag staus information. |
| VisiconX Writes | Allow VisconX to do writes. |
| WorkSpace Configure | Switch to the iFIX WorkSpace configuration environment. |
| WorkSpace Runtime | Switch to the iFIX WorkSpace run-time environment. |
| WorkSpace Runtime Exit | Quit the iFIX WorkSpace from the run-time environment. |

**NOTE:** Refer to the Batch Execution documentation for more information about the application features specific to Batch Execution.

## Assigning Special Application Features

Regardless of how you set up your group accounts, you should provide the following application features on an individual basis:

- Security Configuration
- iFIX - System Shutdown

- Background Task Exit
- Enable Ctrl-Alt-Del
- Enable Task Switching

The Security Configuration application feature should be assigned to your system administrator or the person in your organization responsible for creating and maintaining iFIX security. In fact, iFIX security requires you to assign the application feature to at least one user account; providing access to the program with a group account does not fulfill this requirement.

The iFIX - System Shutdown and Background Task Exit application features should be assigned to anyone responsible for shutting down iFIX. If no one is assigned these features, it will be impossible to shut down iFIX programs in an orderly fashion.

The Enable Ctrl-Alt-Del application feature should be assigned to at least one user if you are planning to enable Environment Protection. Also, it should be assigned to the user that is logged in when iFIX is configured to run as a service under Windows.

The Enable Task Switching application feature is required for the system administrator.

## Run-time Environment Protection

The iFIX WorkSpace provides a run-time environment. While an operator is in this environment, you may not want them to:

- Start other applications.
- Switch to other applications.
- Exit from the WorkSpace.
- Restart the computer using Ctrl+Alt+Del.
- Open unauthorized pictures.
- Close the current picture.
- Use the WorkSpace menu.
- Switch to the configuration environment.
- Access the system tree.
- Access the pull down menus.
- View the titlebar.

By enabling environment protection, you restrict operators from performing these actions and provide a secure run-time environment. For more information on setting up a secured environment, refer to the section Restricting Access in the Run-time Environment.

After you configure a secure environment, the iFIX WorkSpace uses your settings as defaults for the run-time environment. You can set up a user account to override one or more of these settings by assigning certain security features to it.

In general, the rights of the logged-in user will override the Environment Protection settings in the iFIX WorkSpace User Preferences. An exception to that rule is the Enable ALT+F4 option. If the Disable

Title Bar and Menu option is checked and the Allow ALT+F4 option is unchecked, no user will be able to shut the Workspace down using the ALT+F4 key combination.

**IMPORTANT:** If you plan to use environment protection when iFIX is running as a service, and you are running on an operating system earlier than Microsoft Windows 8 or Windows Server 2012, 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. Operating systems such as Microsoft Windows 8 or Windows Server 2012 do not require TFSE.exe in your startup group, since they work differently.

**TIP:** Be aware that you if you disable the WorkSpace title bar and do not allow ALT+F4, it may not be obvious how to shut down the WorkSpace in run mode. This is a security feature. If the shut down ability is desired, you can add a VBA script to shut down the WorkSpace. Refer to the section for more details on how to add this script to your picture.

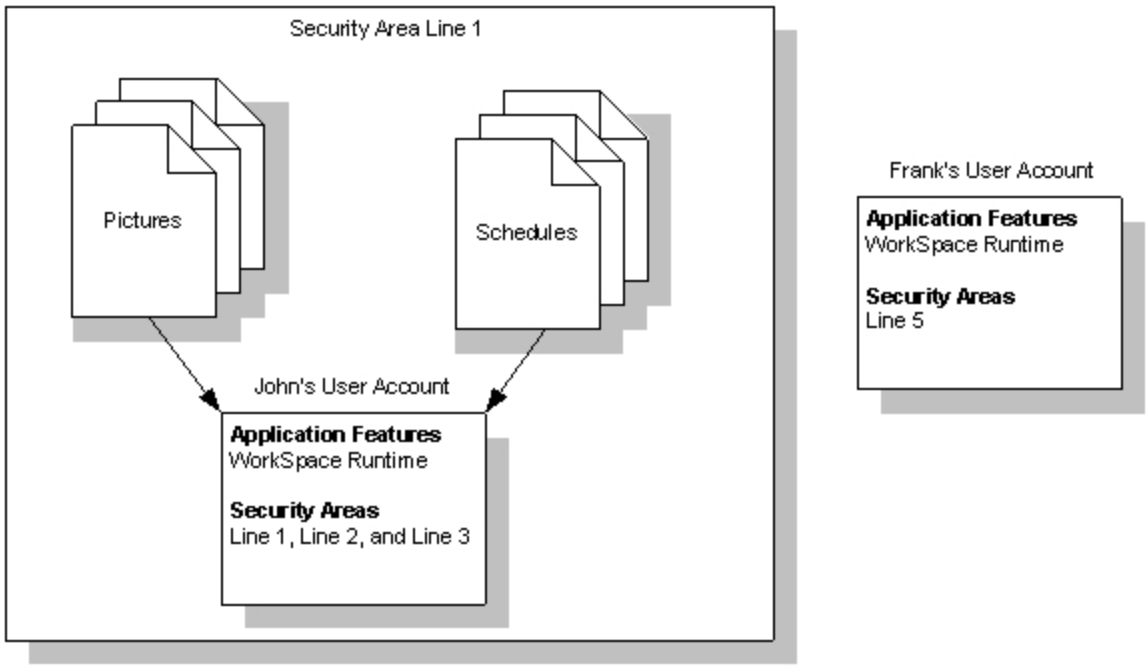
## Securing Scripts and the Visual Basic Editor

One of the options you have when you enable environment protection is to restrict access to the Visual Basic Editor. If access is not restricted, the editor appears when a compilation error or a run-time error occurs, allowing you to correct the error.

However, when you restrict access, the iFIX WorkSpace suppresses the Visual Basic Editor even if an error occurs. Consequently, if you plan to enable this option, your scripts must have error-handling routines. Otherwise, an error message appears and the script terminates.

## Securing Pictures and Schedules

In addition to securing scripts, you can also secure pictures and schedules by using the Security Area property. You can set this property on a picture or schedule using the Property window. For more information on properties, refer to the Controlling Object Properties chapter in the Creating Pictures manual. This property restricts access to a picture or schedule at run-time so that only users with rights to the specified area can access the pictures and schedules assigned to the security area, as the following figure shows.




*Securing Pictures and Schedules*

In the Securing Pictures and Schedules figure, notice that John can access the pictures and schedules in the security area Line 1 because he has rights to it. However, Frank cannot access the area Line 1 because Frank has rights to Line 5 only. If Frank attempts to open a picture or schedule in Line 1, a message box appears alerting him of the security violation. The violation is also recorded in the security audit trail and every enabled alarm destination except the Alarm Summary.

Pictures and schedules that you configure to preload at run-time are also restricted by the security area. Consequently, if you assign the operator display OVERVIEW.GRF to the security area Line 4 and configure the WorkSpace to load the picture automatically on startup, the picture will not load when John logs in because he does not have rights to Line 4. Preloading schedules works the same way: the logged-in user must have rights to the security area of the schedule, or the schedule does not run.

## Electronic Signatures

Use electronic signatures to create a more secure environment by requiring that operators electronically sign for all process changes and alarm acknowledgements. Electronic signatures uniquely identify the operator making the change, and can require the electronic signature of another person to verify the change.

Detailed permanent records of operator actions are written to and stored in a relational database. You can query and report on these records, and then use this data to provide a comprehensive audit trail detailing the history of your process.

The following application features give user or group accounts electronic signature privileges:

- Electronic Signature – Perform By
- Electronic Signature – Verify By

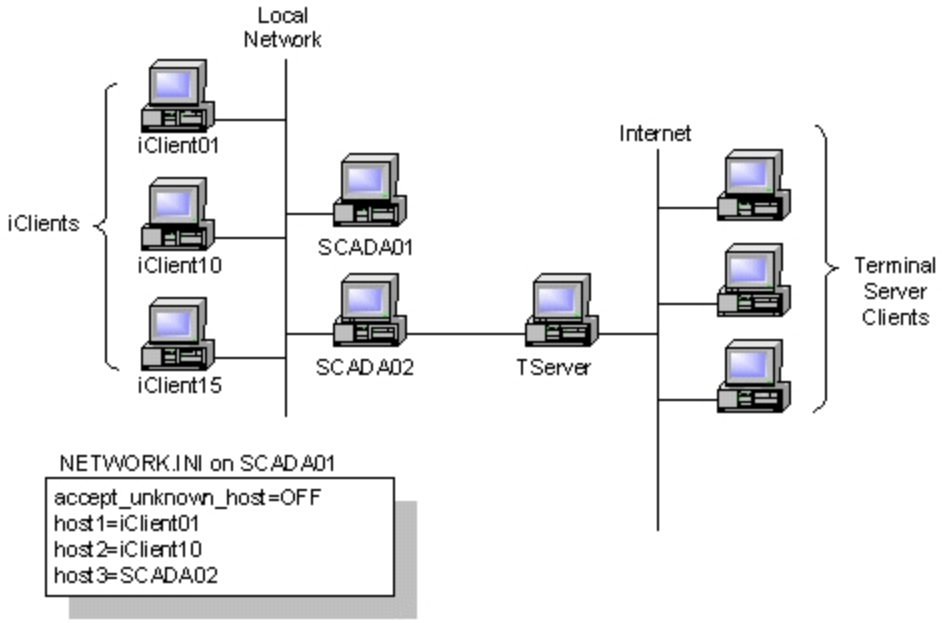
Refer to the Using Electronic Signatures manual for detailed information on using electronic signatures.

## Protecting SCADA Nodes

Application developers can allow certain operators the ability to write to specific SCADA nodes only. This prevents the possibility of access from unknown or unauthorized nodes. This is an important feature to ensure that operators are positioned physically close to the equipment they are manipulating.

By default, iFIX nodes accept connections from any remote node over TCP/IP. You can restrict access from unknown or unauthorized nodes using the accept_unknown_host parameter in the NETWORK.INI file. The configuration shown in the following figure illustrates one method to restrict access to a SCADA server.

In this example, the accept_unknown_host parameter restricts access to the main SCADA server, SCADA01. Access is restricted to iClients iClient01 and iClient10, and to a second SCADA server, SCADA02. SCADA02 duplicates the information on SCADA01 so that the Terminal Server, TServer, can provide the data to remote nodes. However, direct access from the Internet to SCADA01 is not provided. This feature keeps SCADA01 secure from unauthorized nodes.




*Restricting Access from Unauthorized Nodes*

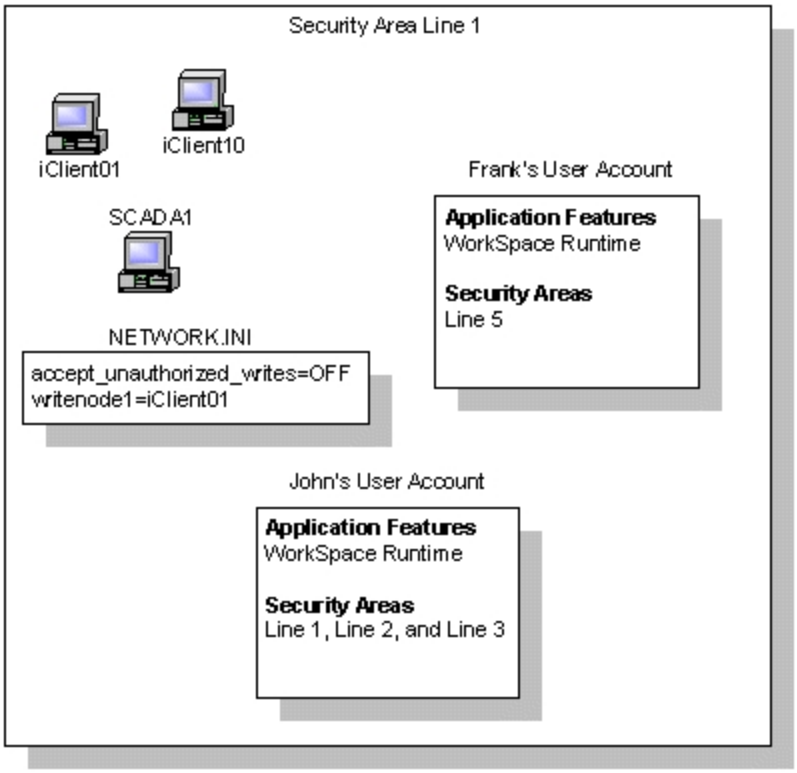
For more information about restricting access from remote nodes, refer to the section Disabling Connections from Unauthorized Nodes in the Setting up the Environment manual.

## Restricting Database Write Access on a Node-by-Node Basis

You can also restrict database write access on a node-by-node basis using the accept_unauthorized_writes parameter in the NETWORK.INI file. When you use this parameter with security areas, database writes are first restricted by security area and then by node. The following figure illustrates how security areas interact with the accept_unauthorized_writes parameter.

In this example, John and Frank cannot modify SCADA01's database from iClient10. John cannot modify the database because the NETWORK.INI file authorizes writes from iClient01 only. Frank cannot change the database because he does not have rights to Line 1.

However, when John logs into iClient01, he can modify the database because the NETWORK.INI file grants access. Conversely, when Frank logs into iClient01, he cannot modify the database because he does not have rights to Line 1. Consequently, the SCADA server rejects his request even though he is logged into an authorized node.




*Restricting Database Write Access*

For more information about restricting database write access on a node-by-node basis, refer to the section Disabling Database Write Access for Unauthorized Nodes in the Setting up the Environment manual.

## Working with Visual Basic for Applications

Using Visual Basic for Applications (VBA), you can write scripts that provide security access and information. For example, you can use a script to determine the currently logged in operator and his or her security rights. You can also write scripts that let operators log into and out of iFIX. Such scripts let you customize the login process to your needs.

To learn how to write a script with iFIX security, refer to the Writing Scripts e-book. To learn about specific VBA methods that access the security system, refer to the iFIX Automation Reference file.

## The iFIX Screen Saver

A customized screen saver is integrated into the iFIX software. You can use the iFIX Screen Saver as part of your strategy to secure inactive computers. This screen saver activates in the same way that other Windows screen savers do, but it also has some features specific to iFIX.

The moment when a screen saver appears is typically referred to as the activation of the screen saver. A screen saver deactivates once the operator moves the mouse or presses a key on the keyboard. When the iFIX Screen Saver activates, it may display a bitmap image. You can substitute your own bitmap image, such as one containing a company logo, for the default bitmap image. In the iFIX LOCAL folder, rename the iFIXScreenSaver.bmp file. Copy your .bmp file into the iFIX LOCAL folder and then rename it to iFIXScreenSaver.bmp.

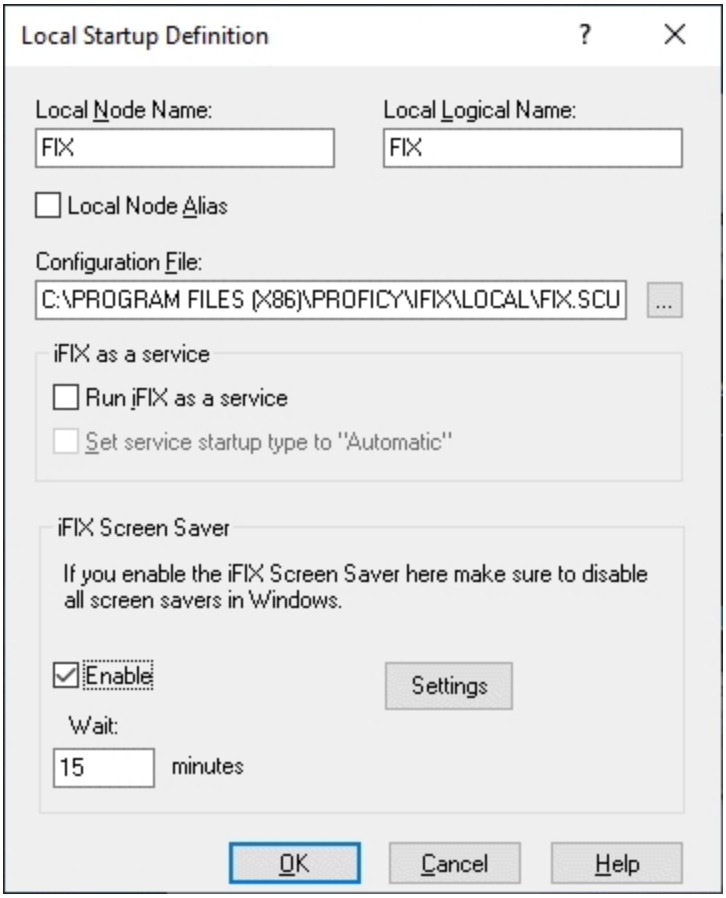
You can configure the iFIX Screen Saver to perform these tasks when it activates:

- Terminate the continuous use period. Refer to Allow Continuous Use in the Using Electronic Signatures manual for more details on continuous use.
- Blank out the screen.
- Log out the current iFIX user.
- Prompt for login.
- Log in a specified user.
- Open a specified picture.

**NOTE:** The screen saver sends all errors to the Windows Event Log. For example, if you have the screen saver configured to open a specific picture and that picture is unavailable, this error is sent to the Event Log. To see these errors, start the Window Event Viewer and open the Application log. Screen saver errors have VB Runtime as their source.

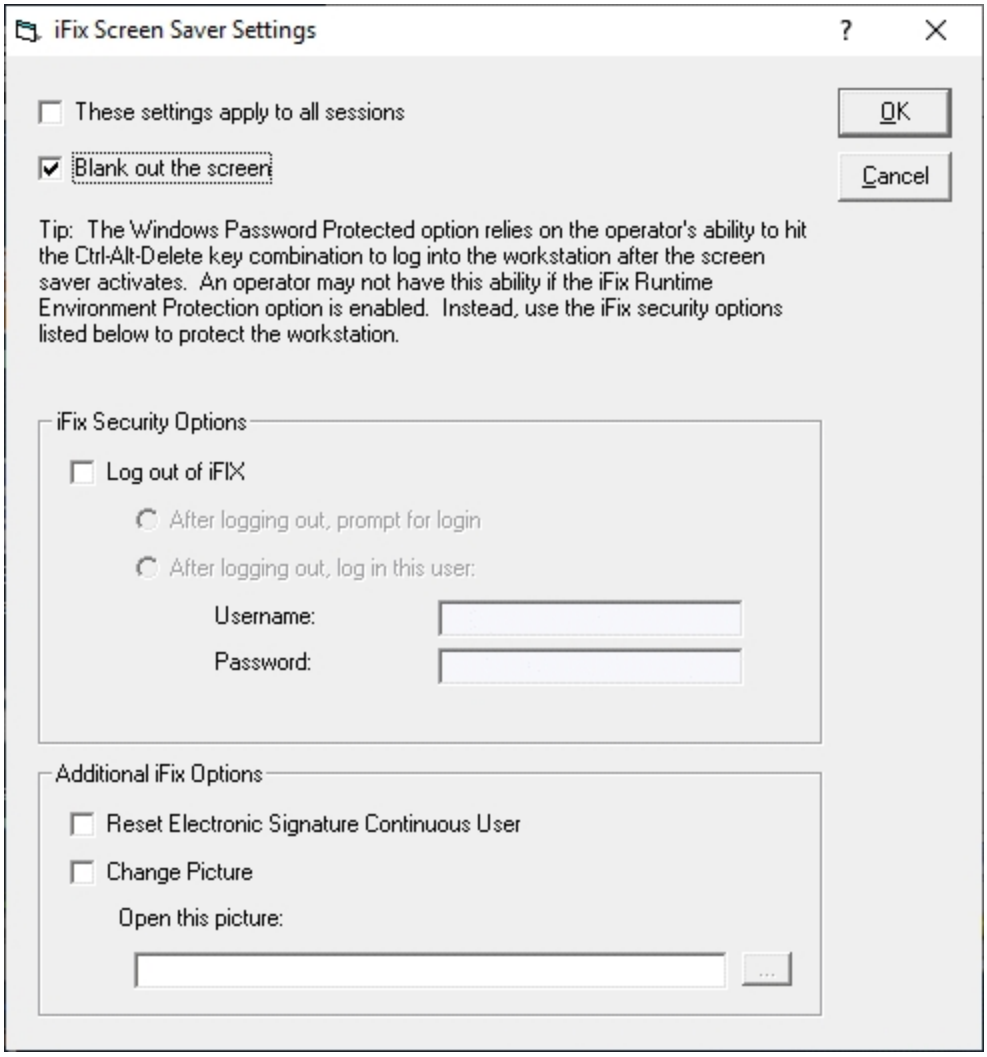
### Overview of Configuration

You enable the iFIX Screen Saver in the iFIX SCU in the Local Startup Definition dialog box, as shown in the following figure.




Although configured here, the iFIX Screen Saver settings are not saved in the SCU file. The Enable/Disable screen saver option and the Wait time apply to all sessions.

To configure the iFIX Screen Saver, click the Settings button in the Local Startup Definition dialog box. This displays the iFIX Screen Saver Settings dialog box, shown in the following figure. Here is where you configure the majority of your screen saver settings.




*iFIX Screen Saver Settings*

## Steps to Configure the iFIX Screen Saver

Use the following steps to configure the iFIX Screen Saver.

**To configure the iFIX Screen Saver:**

1. Open the iFIX SCU.
2. On the Configure menu, click Local Startup. The Local Startup Definition dialog box appears.
3. In the iFIX Screen Saver area, select Enable. The Enable/Disable screen applies to all sessions.
4. In the Wait field, leave the default of 15 minutes, or change it. You can enter a wait time of 1 to 9999 minutes. The wait time is how long the user session that FIX.EXE runs in is idle before the screen saver is activated. The Wait Time setting applies to all sessions.

5. Click Settings. The iFIX Screen Saver Settings dialog box appears.
6. Enter your settings as defined in the following table.

| Field | Description |
|---|---|
| These settings apply to all sessions | Click this option to apply the same screen saver settings to all sessions.<br>If the "These Settings Apply to All Sessions" is cleared, then entries entered in the iFIX Screen Saver Settings dialog box will only apply to the user currently logged into the operating system at the time those settings are saved.<br>The iFIX Screen Saver settings are not saved in the SCU file so are applied regardless of the SCU configuration being used to run iFIX by a Windows user. |
| Blank out the screen | Select this option to make the screen go empty when the screen saver activates. |
| Log out of iFIX | Select this option if you want the user to be logged out of iFIX when the iFIX Screen Saver activates. Additionally, you can configure whether the operator is prompted to log in or a new user is automatically logged in. |
| After Logging out, Prompt for Login | This option is selectable when the Log out of iFIX option is selected. Select this option to cause a login dialog box to appear after the screen saver activates. The operator must supply a user name and password.<br>When the "Log out of iFIX" option is enabled, the screen saver logs a new user into iFIX only and the Windows session continues to run under the user it was started with. |
| After Logging out, Login this user | This option is selectable when the Log out of iFIX option is selected. Select this option to log in a user automatically after the screen saver activates. To specify that user, you must supply the user's name and password in the Username and Password fields below this option. The screen saver logs a new user into iFIX only, and the Windows session continues to run under the user it was started with. |
| Reset Electronic Signature Continuous User | This option resets the continuous user when the screen saver activates. This option only applies if iFIX is running. |
| Change this Picture | This option enables you to specify the iFIX picture to open when the screen saver activates. |
| Open this Picture | When you select the Change this Picture option, use this field to specify the new picture in the Open this picture text box field. This option works only if the WorkSpace is started and is in Run mode . |

7. Click OK to save your settings.
8. Restart iFIX.

**IMPORTANT**:

- Be sure that no other screen savers are enabled in the Windows Screen Saver Settings (from the Start menu > Settings, search for "Screen saver settings").
- You can enable the iFIX Screen Saver via the Windows settings instead of via the iFIX SCU, but there are limitations. For instance, one limitation is that the iFIX Screen Saver will not work for Remote Desktop sessions.

- If you choose to enable the iFIX Screen Saver via the Windows settings, do not enable the password protected option in the Windows Screen Saver options. The Windows Password Protected option relies on the operator's ability to press Ctrl+Alt+Del to log into the workstation after the screen saver activates. If you configure your Environment Protection settings so that operators cannot use the Ctrl+Alt+Del key combination, they will not be able to dismiss the iFIX Screen Saver if the Password Protection option is enabled. To require a password for dismissing the iFIX Screen Saver, use the options in the iFIX Screen Saver Settings dialog box.
- Also, take care to disable the iFIX Screen Saver in the SCU if you choose to enable it in the Windows settings.

# Defining and Assigning Security Privileges

Before you enable the security system, you should create all required group and user accounts. Group accounts define the security areas and application features available to group members. Likewise, user accounts define the security areas, application features, and group accounts available to individuals.

By default, iFIX provides sample group and user accounts that you can examine to learn how to create your own accounts. You can also use the sample accounts to log into iFIX. The following table lists the login name and password for the sample user accounts. For instructions on logging into iFIX, refer to the Logging in to iFIX Manually section.

**Sample User Accounts**

| Account | Login Name | Password |
|---|---|---|
| Guest | Guest | Guest |
| System Administrator | Admin | Admin |

**NOTE:** Do not enable Windows security for the sample user accounts. If you have the Guest account enabled on an iFIX machine, login validation for iFIX security will not work properly.

### To implement an iFIX security strategy:

1. Name your security areas. See Defining Security Areas.
2. Create group and user accounts. See Creating Group and User Accounts.
3. If you plan to automatically log any operator into iFIX, define each automatic login configuration. See iFIX Automatic Login.
4. Specify a local security and backup path on each node. If you are using a file server, enter the path to the file server as the security path and enter a local path as the backup path. See Defining the Security Path.
5. Enable security on all nodes and save the security configuration. See Importing and Exporting the Security Configuration.
6. If you plan to enable environment protection, start the iFIX WorkSpace and set the run-time environment preferences you want to use on each iClient.
7. If you plan to use electronic signatures to protect and track data entry and alarm acknowledgement actions, set them up as recommended in Using Electronic Signatures. See the Overview: Using Electronic Signatures section in that book.

When you finish, you can verify your security configuration by logging into iFIX and accessing the application features and security areas available to each user account. Also, try to access application features and security areas that are unavailable to ensure that security denies access.

## The Security Configuration Program

In Classic view, start the Security Configuration program by clicking the Security Configuration button on the Application toolbar, as shown in the following figure.

In Ribbon view, to start the Security Configuration program, on the Applications tab, in the System & Security group, click Security Configuration Utility.

Once the program starts, the Security Configuration window appears.


*The Security Configuration Window*

## Exiting from the Security Configuration Program

You can close the Security Configuration program by selecting Exit from the File menu in the Security Configuration window.

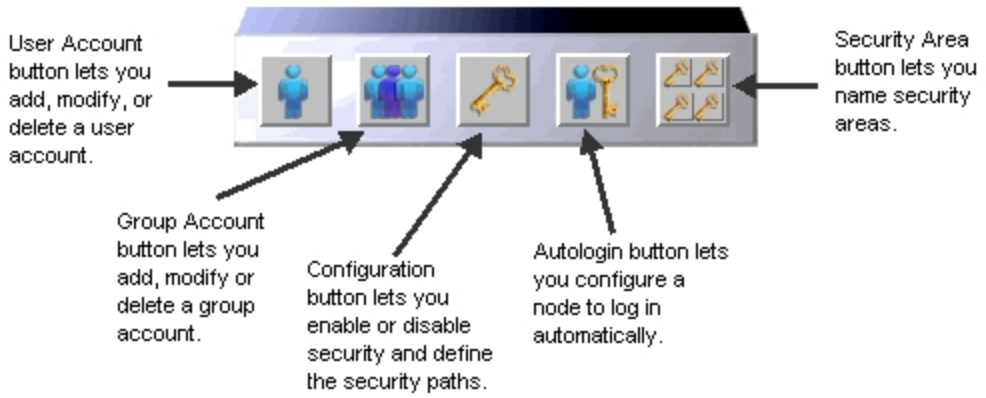
## Working with the Security Toolbox

The Security Configuration program provides a set of tools for:

- Creating group and user accounts.
- Naming security areas.

- Setting up a node to log in automatically.
- Enabling and disabling security.
- Setting security paths.

These tools are available from the Security toolbox, as the following figure shows:




*Security Toolbox*

## Enabling and Disabling Security

After you have configured your security areas, group accounts, and user accounts, you can restrict access to applications and files on a node and force operators to log into iFIX by enabling security. Once you enable security, the lock displayed by the Security Configuration program closes to indicate the computer is protected.

**NOTE:** If you enable security and set the security path to a folder other than the default, which is the C:\Program Files (x86)\Proficy\iFIX\Local folder, when you change the node name, security is disabled. You will need to configure iFIX security again and enable it.

If you want to provide complete access to the files on a computer, you can disable security. Typically, you disable security when you want to create a public node. Once security is disabled, the lock displayed by the Security Configuration program opens to indicate the computer is unprotected.

## Defining Security Areas

Once you complete your security strategy, the next step is to define your security areas and specify a name for each area. You can define up to 254 security areas, and each name can be up to 20 characters. iFIX names the first 16 security areas A through P by default. However, you can rename these areas or create a new area by clicking the Security Area button on the Security toolbox. After you define a security area, you can assign it to a group or user account.

Use the Tag Security Areas drop-down in the Security Area Naming dialog to specify how security areas assigned to a tag are evaluated when a user writes to a tag or acknowledges a tag's alarm. There are two evaluation options:

- **Require At Least One (OR)** - Users require access to at least one specified security area.
- **Require All (AND)** - Users require access to all specified security areas.

**NOTE**: You must re-start iFIX on the SCADA(s) using that Security Path (as in the case of shared security files) for this setting to take effect.

### Assigning Security Areas

Once you define the security areas you need, you can use one of the following methods to assign a security area to a database block, picture, schedule, or recipe:

- To assign a security area to a database block, open the Database Manager and double-click the block you want to modify. When the block's dialog box appears, locate the Security Areas list box. Typically, the list box resides on the Advanced tab. Once you locate the list box, select a line of text from it and enter the security area you want to assign.
- To assign a security area to a picture or a schedule, open the picture or schedule in the iFIX WorkSpace and select Property Window from the View menu (Classic view) or click Property Window in the Window group on the View tab (Ribbon view). When the Properties window appears, enter the security area you want to assign to the Security Area property.
- To assign a security area to a recipe, refer to the Creating Recipes manual.

Use the Tag Security Areas drop-down in the Security Area Naming dialog to specify how security areas assigned to a tag are evaluated when a user writes to a tag or acknowledges a tag's alarm. There are two evaluation options:

- **Require At Least One (OR)** - Users require access to at least one specified security area.
- **Require All (AND)** - Users require access to all specified security areas.

**NOTE**: You must re-start iFIX on the SCADA(s) using that Security Path (as in the case of shared security files) for this setting to take effect.

## Creating Group and User Accounts

You can create group and user accounts by clicking the Group Accounts button or the User Accounts button on the Security toolbox and clicking Add, then completing either the Group Profile dialog box or the User Profile dialog box. In these dialog boxes, you can modify the security areas and application features assigned to this account. In the User Profile dialog box, you can also modify the group accounts assigned to this user account, and set the password for this user account.

For a list of application features refer to the Application Features section. For a description of security areas, refer to the Security Areas section.

### Limiting Login Time

The Security Configuration program allows you to enter a login time-out interval when creating a user account. This interval limits the length of time an operator can remain logged into iFIX. When an operator attempts to access a restricted application feature or security area after the time interval expires, iFIX logs out the operator.

With this feature, you can configure iFIX to automatically log out operators who forget to do so at the end of their shift. For example, assume you want operators logged in for up to eight hours. By entering a time-out interval of 8:00:00, you instruct iFIX to log out your operators eight hours after they log in. If an operator exits from all iFIX applications a few minutes early, but does not log out, iFIX logs out the operator when someone from the next shift runs a program. This forces the current operator to log in with their own account, and prevents unauthorized access to applications and security areas that were available on the previous shift.

This feature does not eliminate the need to manually log out when an operator finishes using iFIX, particularly if you have strict security requirements. If you decide to use this feature, consider it as a safety mechanism that prevents operators from remaining logged in indefinitely.

### Modifying Group and User Accounts

As group and user responsibilities change, you may find it necessary to modify accounts.

**NOTE:** Once operators log in, their group and user accounts reside in memory. As a result, changes to group or user accounts do not take effect until users log out and log in again. By logging in again, the operator forces iFIX to re-read the account information.

### Deleting Group and User Accounts

You can delete group and user accounts that you no longer need. Deleting a user account that automatically logs into iFIX also removes the associated autologin configuration file as well. Refer to the section iFIX Automatic Login to learn more about setting up a user account to automatically log in.

You can delete every currently-defined account by selecting the Clear command from the File menu. When you select this command, the security system:

- Disables itself.
- Deletes all group and user accounts.
- Deletes all automatic login configurations.
- Renames the first 16 security areas A through P and deletes any other named security areas.
- Prompts you to create sample accounts. This prevents you from accidentally locking yourself out of the Security Configuration program. To be safe, you should always create sample accounts.

  If you do not create sample accounts and re-enable security, you cannot exit from the Security Configuration program until you create at least one user account. This feature also helps to prevent you from accidentally locking yourself out of the Security Configuration program.

**NOTE:** iFIX does not modify the security and backup paths when you select the Clear command.

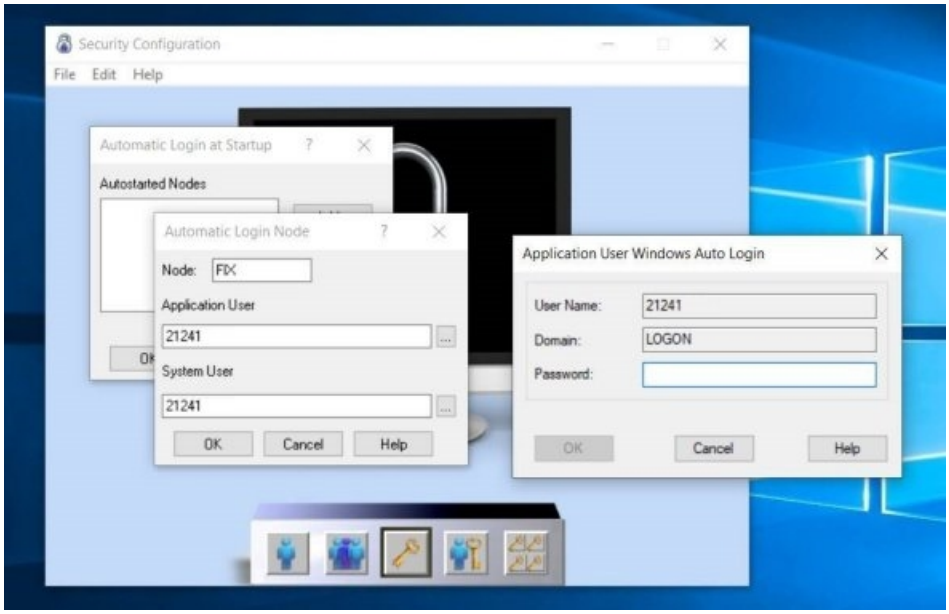
## iFIX Automatic Login

Using the Security Configuration program, you can set up iFIX to log in an operator automatically when it starts up by creating an automatic login configuration. You can create this configuration by specifying the name of the:

- Node you want to automatically log in.
- User you want logged in.

### Windows Users and Automatic Login

When a Windows user is defined as an automatic login user, you will be prompted to enter a password as shown in the following graphic.




### Automatic Login and the Security Path

You can create automatic login configurations for multiple computers. When the security path is local, you can specify an automatic login configuration for each node by configuring it locally. However, by defining a file server path as the security path, you can specify an automatic login configuration for any computer from any node on the network.

### Automatic Login and Application Users

Automatic login configurations require you to specify an application user. An application user is the name of the operator you want logged in automatically. This name must be the full name defined in a user account. Once logged in, operators have access to the privileges assigned to the specified user account.

## Creating a Public Account

Depending on your security requirements, you may want to create a public account that is available to everyone in non-critical areas of your process. This account would have no password and would automatically log in when you start iFIX. This account would also provide access to the iFIX WorkSpace runtime environment.

By default, the Guest account is installed with iFIX. This account has no password, but is not automatically logged on.

### Deleting an Automatic Login Configuration

You can delete any automatic login configuration that you no longer need by selecting the name of the node you want to remove.

## Importing and Exporting the Security Configuration

The Security Configuration program allows you to import and export your security configuration. Exporting the configuration creates a security configuration file, SECURITY.RPT, by default, in the security path. This file contains the following information:

- Whether security is enabled or disabled.
- Security area names.
- Defined group and user accounts.
- Whether a password is case sensitive or not.

After you create a security configuration file, you can copy it to another computer and import the data. Importing a configuration file does one of the following:

- Replaces the existing security configuration with the one defined in the configuration file; or
- Adds any new group and user accounts from the configuration file to the existing security configuration. Any account with a full name or a login name that matches an existing account is ignored. Also adds any new security areas from the configuration file in the existing security configuration.

By exporting and importing a security configuration, you can cut your development time creating user and group accounts particularly when you want to create many similar accounts on multiple nodes. For example, suppose you want to create the same user account on five nodes. Instead of creating same account five times, you can:

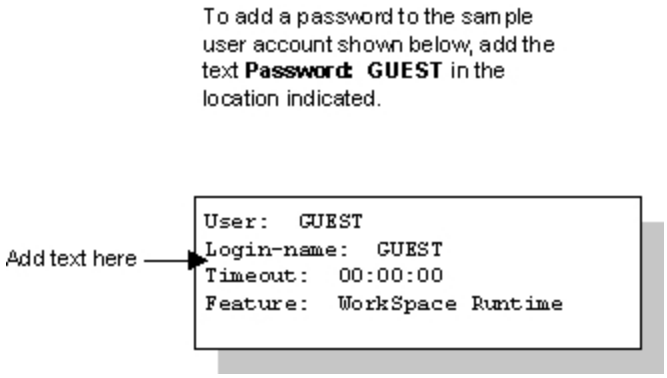
1. Create one user account.
2. Export the user account.
3. Import the user account into the remaining 4 nodes.

### Importing User Account Passwords

Exported security configuration files do not include user account passwords in order to protect them. Similarly, when you import a configuration file, the Security Configuration program creates user accounts without passwords.

You can avoid this situation by adding a password to each account in the configuration file. When you import the edited configuration file, the Security Configuration program assigns a password for each user account you modified.

The following figure shows what part of the configuration file to edit.




*Adding Passwords to a Security Configuration File*

**NOTE:** You do not need to add passwords to user accounts that use Windows security. However, in order to protect your passwords, if you add passwords to a security configuration file prior to importing it, delete the file when you finish importing the data. If you need a text copy of the security configuration, export the configuration again.

## Exporting the Security Configuration from a Command Line

To export your security configuration from a command line, use the /X parameter for the Security Configurator (SECCFG.EXE).

In order to successfully export the security configuration using the /X parameter:

1. iFIX must be running.
2. The currently logged in user must have access to the Security Configuration security feature.
3. There must be no other instances of the Security Configurator or Security Synchronizer running.

**IMPORTANT:** The Security Configurator cannot be run in a Webspace session.

The /X parameter has the following format:

```
SECCFG.EXE /Xname
```

where *name* is the name of the export file.

The file is created in the iFIX LOCAL folder. If the exported file already exists, it will be overwritten. For example, the following command will export the security configuration to the file named Security080119.RPT in the iFIX LOCAL folder:

```
SECCFG.EXE /XSecurity080119.RPT
```

If the file name is omitted, the default filename of "SECURITY.RPT" is used.

## Defining the Security Path

The security files that you create reside in a path called the security path. The Security Configuration program sets this path to the iFIX Local path by default, but you can change it to any other local or network path.

Determining the path to specify as the security path depends on your needs. If you want a node to have its own set of accounts, define a local path. However, if you want to share user and group accounts with other computers, specify a file server (network) path as the security path.

**IMPORTANT:** Be aware that when you enter a security path you must have read-write access to the path you designate. After you enter a path, the Security Configuration program creates lock files (SECLOCK.LCK and SECLOK2.LCK) allowing you to use the program with read-only access to the security path.

Before you define the path, verify that it exists. If it does, the Security Configuration program prompts you to copy the files to the new path. If the path does not exist, the following text appears:

```
Security path invalid or unavailable. Continue?
```

Click Cancel or the No button to abort the process and create the path you want to use. If you plan to create the path later, click the Yes button. The following text appears:

```
Security Files must be manually copied from oldpath
```

Click OK to acknowledge the message and copy the security files to the path you specified. If you do not create the new path or copy the security files to it, you will be unable to restart the Security Configuration program.

### Defining the Backup Path

In addition to the security path, you can define a backup path that contains a copy of the files in the security path. These files are updated whenever you save a modified security configuration. The configuration is saved to the security path, as well as the backup path of the machine where you perform the save. If there are other nodes that share the security path and have the backup path pointing to the local hard drive, the backup is not performed on those machines.

iFIX uses the files in the backup path when the security path is unavailable. For example, if you define a file server path as your security path, and the file server becomes inaccessible, iFIX uses the backup path to allow operators to log in.

Like the security path, iFIX sets the backup path, by default, to the iFIX Local path, but you can change it to any other local or network path. If you plan on using a network path as your security path, use a local path for the backup path.

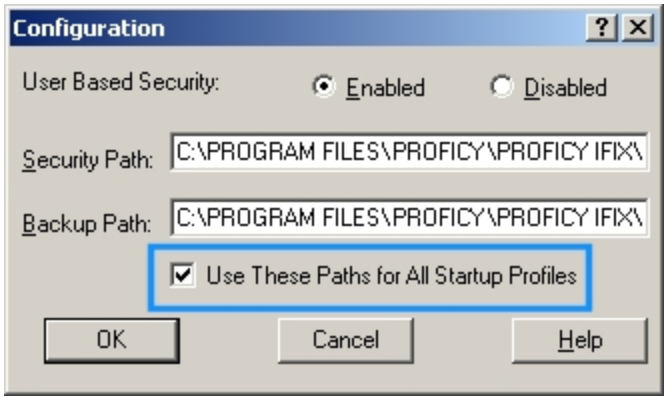
The backup path you specify must exist. Otherwise, the following text appears:

```
Invalid path specified
```

Click OK to acknowledge the message and create the path you want to use.

## Configuring Global Security Paths

When you enable the global security paths option in the Configuration dialog box (of the Security Configuration application), all iFIX user sessions on a computer share the same security configuration. If you use iFIX startup profiles created in the Startup Profile Manager, you most likely want to enable this option. To enable global security paths, select the Use These Paths for All Startup Profiles check box in the Configuration dialog box. The following figure shows an example of the Configuration dialog box with the global security paths check box highlighted.




*Configuration Dialog Box, Global Security Paths Enabled*

For example, in a Terminal Server environment, enable this option if the default SCU is enabled in the Startup Profile Manager. If you do not enable global security paths, you will need to individually configure security within each Terminal Services user session.

**IMPORTANT:** For global security paths to work correctly, the Base and Language paths in the SCU's Path Configuration dialog box must be the same for all users. Project paths can differ, however. To open the SCU, click the Start button, point to Programs, iFIX, and then select System Configuration. Click the Path Configuration button to open the Path Configuration dialog box. The default Base path is C:\Program Files (x86)\Proficy\iFIX, while the default Language path is C:\Program Files (x86)\Proficy\iFIX\NLS.

For more information on working with Terminal Services, refer to the Using Terminal Server manual. For more information on the Startup Profile Manager, refer to the Using the Startup Profile Manager chapter in the Setting up the Environment manual.

## Restricting Access in the Run-time Environment

You can secure the run-time environment by enabling environment protection from the iFIX WorkSpace. Refer to the Run-time Environment Protection section. Once you enable environment protection, you can choose the specific actions you want to restrict.

**NOTES:**

- Some computer keyboards have special buttons that allow users to directly launch e-mail, searches, or internet browsers. Because these special buttons could circumvent iFIX environment protection, you may want to uninstall the software that operates the special buttons.
- For Microsoft Windows 8 and Windows Server 2012, the only on-screen keyboard for use with iFIX and touch screens is the tabtip keyboard (tabtip.exe). This on-screen keyboard will launch automatically if no physical keyboard is detected, and if the screen focus is on an edit field in the WorkSpace (when the I-Bar cursor is displayed in the edit field).

**IMPORTANT:** To launch the keyboard automatically from iFIX on Windows Server 2012 systems, there is additional configuration. In the Server Manager, you must install the Desktop Experience feature included in the User Interface and Infrastructure features. (By default, this feature is already enabled in Windows 8). After enabling the feature and restarting Windows, the on-screen keyboard, tiptap.exe, will be available and will display automatically when focus is on an edit field in iFIX.

The following table provides other common tasks you may want to restrict operators from, and the options to do so.

**Restricting Access in the Run-time Environment**

| To restrict an operator from... | Select the check box(es)... |
|---|---|
| Switching to another application that may be running. | Disable Task Switching. If security is disabled, task switching is disabled when Disable Task Switching is selected.<br><br>**NOTE:** The Shift + F10 key macro does not work if you select this option.<br><br>**IMPORTANT:** If security is enabled, task switching is disabled when the logged-in user does not have task switching rights or there is no user logged-in. The task switching right can be assigned by adding the Enable Task Switching application feature to the user profile in the iFIX Security Configuration application. |
| Exiting from the iFIX WorkSpace. | Disable Title Bar and Menu Bar.<br><br>**IMPORTANT:** Users who have iFIX WorkSpace runtime exit privileges should also be assigned task switching rights or the WorkSpace runtime shutdown will be blocked. |
| Exiting from the iFIX WorkSpace with the ALT + F5 key combination | Enable ALT+F4<br><br>When selected, a user with the Enable Task Switching and Workspace Runtime Exit security features to exit the WorkSpace application in Run mode using the ALT+F4 key combination even if the WorkSpace title bar is disabled. If the option is cleared, no user will be able to exit the WorkSpace application in Run mode using the ALT+F4 key combination when the WorkSpace title bar is disabled. |
| Restarting the computer using Ctrl+Alt+Del or logging out of Windows. | Disable Ctrl+Alt+Del. When iFIX security is enabled, this option is overridden by the logged in user's permissions. |
| Closing the current picture. | Disable Title Bar and Menu Bar. Also select the Full Screen in Run mode check box from the General tab and clear the Title bar and Resizeable check boxes from the Picture Preferences tab. |
| Using the WorkSpace menu or switching to the configuration environment. | Disable "WorkSpace" Menu Pulldown. |
| Accessing the Visual Basic Editor. | Disable VBE Access.When iFIX security is enabled, this option is overridden by the logged in user's permissions. |

## Locking Down the Windows Taskbar

You can control the accessibility of the Windows taskbar in Full Screen mode only, with the "Disable Task Switching" option located on the Environment Protection tab of iFIX WorkSpace User Preferences dialog box. If the "Disable Task Switching" option is selected, the Windows taskbar will not be accessible when the iFIX WorkSpace is running (in Full Screen mode only). If you are not in Full Screen mode

or if the "Disable Task Switching" option is cleared, the Windows taskbar will be accessible by pressing the Windows key on the keyboard.

**NOTE:** The Enable Task Switching security application feature can be used to override the "Disable Task Switching" option for Environment Protection, but only when a user with this privilege is logged in. This override has no effect on the Window taskbar. However, if a user with this override privilege is logged in, this user can use Alt+Tab and the Windows keys to see what tasks are running and to switch to other tasks.

### Important Task Switching Information

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

Be aware of the following when using task switching in Microsoft Windows 8 and greater:

- When you disable task switching on Windows 8 and greater, iFIX disables the Windows shell which includes the task bar, the start menu, the desktop, file and folder access, the Charms bar, and hot corners that allow access to the Start screen.
- When security is enabled and iFIX is running, a user with task switching rights must be logged in for the shell to run and the desktop to be accessible. (When security is enabled, the rights of the logged in user will always take precedence over the environment protection settings configured in the iFIX WorkSpace User Preferences.) If there is no user logged in, task switching will be disabled, the shell will be disabled, and the system will become inaccessible.
- The Windows shell may be disabled when switching from run to configure mode in iFIX. To avoid this issue, make sure the logged-in user has both task switching rights and WorkSpace configure access, so that the desktop is always available in configure mode. The task switching right can be assigned by adding the Enable Task Switching application feature to the user profile in the iFIX Security Configuration application. The WorkSpace configure access can be assigned by adding the WorkSpace Configure application feature to the user profile.
- When a user with task switching rights is logged in, the Taskbar may be displayed on top of the Workspace. Enable the Auto-Hide the Taskbar property in Windows to push the Taskbar behind the Workspace.
- If the iFIX WorkSpace is not configured as a startup task in the SCU, you must configure a user to be logged in automatically who has task switching rights or the desktop will not be available and the system will become inaccessible when iFIX starts up.
- All users who have iFIX WorkSpace runtime exit privileges must also be assigned task switching rights or the iFIX WorkSpace runtime shutdown will be blocked.

### Working with Touch Screens

Be aware that for Microsoft Windows 8 and Windows Server 2012:

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

- For Microsoft Windows 8 and Windows Server 2012, the only supported on-screen keyboard for use with iFIX and touch screens is the tabtip keyboard (tabtip.exe).
- To launch the keyboard automatically from iFIX on Windows Server 2012 systems, there is additional configuration. In the Server Manager, you must install the Desktop Experience feature included in the User Interface and Infrastructure features. (By default, this feature is already enabled in Windows 8). After enabling the feature and restarting Windows, the on-screen keyboard, tiptap.exe, will be available and will display automatically when focus is on an edit field in iFIX.
- To automatically display the on-screen keyboard when the focus is set to WorkSpace objects that have the ability to accept user inputs, enable PROFICYENABLEFOCUSTRACKING.EXE by adding the following lines to your FIX.INI file (located in the LOCAL folder) in the [OTHERS] section:

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

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

### Example: Securing the Run-time Environment

Let's assume you enable environment protection in the iFIX WorkSpace and you want to provide John with rights to run Recipe Builder, download control recipes, and task switch between the run-time environment and the Recipe Builder. To do this, you must assign the following application features to John's user account:

- Task Switching.
- Recipe Builder Operations Window.
- Recipe Download from Recipe Builder.

These application features override the run-time environment settings and enable John to perform the specific actions you want.

## Using iFIX Security

Operators can log into iFIX manually or automatically. By logging in, operators identify themselves as iFIX users and gain access to pictures, recipes, and applications that they are authorized to use. Refer to the following sections for more details:

- Logging in to iFIX Manually
- Logging out of iFIX Manually
- Understanding the Security Log File

## Logging in to iFIX Manually

Operators can log into iFIX manually using the Login program. When the Login program starts, it allows operators to enter their login name and password.

The Login program gives operators three attempts to enter their login name and password correctly. After the third unsuccessful attempt, the Login program exits. Operators can try to log in again by restarting the Login program.

If Windows security is authenticating the login name and password, operators can change their password after they log in. Windows passwords are case-sensitive.

**NOTE:** Each time an unsuccessful attempt is made to access the iFIX system, a message is sent to the alarm system. If you have configured the Alarm ODBC Service and your relational database, these messages are also written to your relational database, and can be included in the audit trail of your process.

**To log into iFIX:**

1. In Classic view, in the iFIX WorkSpace, in the Application toolbar, click the Login button.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click Security, and then click Security Login.
2. Enter your login name and password.
3. Click Login.

**TIP:** Other ways you can login to iFIX are from the Options menu in the iFIX Startup window, or the quick access toolbar in the iFIX WorkSpace in run mode

### Password Expiration Considerations

When iFIX security is synchronized with Windows security, passwords can expire. If the Windows password has expired, the user is notified and prompted to change the password. If the Windows password is about to expire, a notification message displays, reminding the user to change the password.

For more information about synchronizing iFIX security with Windows security, refer to the Using iFIX with Windows Security chapter.

## Changing the Account Password

The steps that follow describe how to change a Windows account password for the logged in user. Security must be enabled to perform these steps.

**To change the account password:**

1. In Classic view, in the iFIX WorkSpace, in the Application toolbar, click the Login button.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click Security, and then click Security Login.
2. Click Change Password. The Change Windows Password dialog box appears.

   **NOTE:** The Change Password button is only available for Windows user accounts.

3. In the Old Password field, enter your current password.
4. In the New Password field, enter your new password.
5. To confirm the change to your password, in the Confirm New Password field, enter your new password again.

## Logging out of iFIX Manually

Operators can log out of iFIX by exiting all protected iFIX applications, starting the Login program, and clicking Logout.

**To log out of iFIX:**

1. In Classic view, in the iFIX WorkSpace, in the Application toolbar, click the Login button.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click Security, and then click Security Login.
2. Click Logout.

**TIP:** Other ways you can logout of iFIX are from the Options menu in the iFIX Startup window, or the quick access toolbar in the iFIX WorkSpace in run mode.

## Understanding the Security Log File

iFIX security generates an audit trail of security-related actions taken by iFIX users. The security audit trail log file resides in the default iFIX alarm path and has the name format *YYMMDD*.LOG. For example, the file 031023.LOG contains the audit trail for October 23, 2003. If you have configured the Alarm ODBC Service and your relational database, iFIX writes these messages to your relational database.

By reviewing the audit trail log file you can learn:

- Who logged in and out.
- Each time there is an unsuccessful attempt to access iFIX.
- When an operator failed to complete the login process three times.
- When someone attempted to access a security area or application feature for which they had no privilege.
- When someone successfully or unsuccessfully signed for a data entry or alarm acknowledgement action.
- When an operator exceeded the length of time he or she can remain logged in.

Refer to the Setting up the Environment manual for more information about the iFIX Alarm path.

# Using iFIX with Windows Security

You can connect iFIX user accounts to Windows user accounts. This allows you to use your existing Windows user accounts for password validation. Both local and domain Windows accounts are supported.

You also gain the following advantages of Windows security:

- Case-sensitive passwords.
- Passwords that expire.
- Online password changes.
- Ability to specify minimum password requirements.
- Account lockout.

An operator can log into iFIX by entering his or her Windows user name and password. iFIX sends this information to Windows for authentication. If the operator's account specifies a Windows domain name, the user name and password are sent to a Windows domain controller for authentication. If Windows verifies the user name and password, iFIX completes the login process. Otherwise, it logs an error. Refer to the chapter Using iFIX Security for more information about logging into iFIX.

For information on setting up Windows user accounts for use in iFIX, refer to the section Configuring Windows User Accounts.

There are two basic ways that you can configure iFIX to use your Windows security accounts:

- Configure each account using the iFIX Security Configuration program. Refer to the section Using the Security Configuration Program.
- Use the Security Synchronizer program to update all your accounts at once. Refer to the section Using Security Synchronizer.

## Configuring Windows User Accounts

When you are setting up Windows user accounts for use with iFIX security, you should configure the passwords, set account lockout thresholds, and configure the account disabled message. Refer to the following sections for more details:

- Setting Passwords to Expire
- Limiting the Number of Invalid Login Attempts
- Configuring the Account Disabled Message in iFIX
- User Accounts that Log in to Windows
- Domain Users Logging Into Windows
- Control How iFIX Security Authenticates Windows Accounts
- Domain Caching

### Setting Passwords to Expire

One of the benefits of using iFIX with Windows security is that you can set Windows passwords to expire.

**To configure the local password expiration policy:**

1. In the Control Panel, from the Administrative Tools folder, select the Local Security Policy.
2. From the Local Security Settings window, select Account Policies.
3. From the Account Polices folder, select Password Policy.
4. On the right-side of the window, double-click the Maximum password age.
5. Set the number of days after which passwords expire.
6. Click OK.

## Limiting the Number of Invalid Login Attempts

When an iFIX user account is connected to a Windows user account, the application developer can set an account lockout threshold, which prevents a user from accessing the account after he enters the incorrect user name or password beyond the number of acceptable times. Once the account lockout threshold has been reached, the account is disabled. For more information on the message displayed for a disabled account, refer to Configuring the Account Disabled Message in iFIX.

**To set the account lockout threshold:**

1. From the Administrative Tools folder, select Local Security Policy.
2. Select the Security Settings folder from the folder list in the Local Security Settings dialog box.
3. Select the Account Policies folder.
4. Select the Account Lockout Policies folder.
5. Select Account Lockout Threshold.
6. Select the number of invalid login attempts before the account is disabled.

## Configuring the Account Disabled Message in iFIX

At run time, when a user logs in or enters an electronic signature, he receives an error if the account has been disabled. The application developer can configure the message to display, such as a telephone number or the name of a contact person; otherwise, a general message displays.

**To configure the account disabled message:**

1. In Classic view, on the WorkSpace menu, click User Preferences.

   -Or-

   In Ribbon view, on the Home tab, in the WorkSpace group, click Settings, and then click User Preferences.
2. Select the General tab.
3. In the User Account Disabled Message field, enter a descriptive message indicating an action the user might take to correct the problem, such as:

```
Account is Disabled. Contact Security Services.
```

You can enter up to 100 characters in this field.

## User Accounts that Log in to Windows

When you use Windows security in iFIX on computers that do not run Windows Server 2008, user accounts that need to log in to a machine must have the "Act as Part of the Operating System" right enabled in the local security policy.

**NOTE:** User accounts that are not used to log in to Windows should not have this right.

**To add the Act as Part of the Operating System right:**

1. In the Control Panel, from the Administrative Tools folder, select Local Security Policy.
2. In the Local Security Settings dialog box's folder list, select the Local Policies folder.
3. Select the User Rights Assignment folder.
4. In the Rights list, double-click Act as Part of the Operating System.
5. Add the users you want to have this right to the list.
6. Log out of Windows and log in again for your changes to take effect.

## Domain Users Logging Into Windows

If you are using Windows user names and passwords within iFIX Security, be aware that Windows user accounts must have the policy "Access this computer from the network" applied under "Local Security Settings". By default, this policy is assigned to the groups "Users" and "Everyone" on the local machine. If the domain policy overrides the local policy settings by removing these groups, then the Windows user names and passwords will fail with insufficient rights when trying to log in from iFIX. If domain administrators wish to restrict this right, then they must do one of the following tasks in order to continue to use Window user names and passwords within iFIX:

- Create a Domain Group that contains all the Domain Users that will be used within iFIX Security, add this group to the domain policy "Access this computer from the network", and deploy this policy to all machines running iFIX.
- Add the Domain Users group to the domain policy "Access this computer from the network", and then deploy this policy to all machines running iFIX.
- Add Authenticated Users to the domain policy "Access this computer from the network", and then deploy this policy to all machines running iFIX. Be aware that this group requires each user to log on to the domain at least once to be considered an authenticated user.
- Leave at least the Users group in the domain policy "Access this computer from the network". If you choose this option, be aware that the Anonymous user and the Guest user are not part of the Users group.

Be aware that when configuring your Windows users in iFIX Security, the Domain Name entry needs to be your domain's NetBIOS name.

## Control How iFIX Security Authenticates Windows Accounts

iFIX security allows local and domain accounts in Windows to be configured for authentication within iFIX. Beginning with iFIX 3.5, iFIX security also allows you to configure the Windows API that connects to the domain controller for authentication. You can configure the following Windows APIs for use with iFIX:

- **NetGetDcName** - An older function that iFIX originally used with Network Basic Input/Output System (NETBIOS) to discover the IP address of the primary domain controller (PDC). This function does not support DNS-style names, will not detect a backup domain controller (BDC), and is not recommended when in a Windows environment that uses Domain Name System (DNS) for name resolution without NETBIOS or a Windows Internet Name Service (WINS) server.
- **NetGetAnyDcName** - This function returns the name of any domain controller for a domain that is directly trusted by the specified server. To use this function, the computer must have a trusted connection with the server.
- **DsGetDcName** - The default function call made by iFIX security. This function uses Active Directory to return the name of a domain controller.

**NOTE:** If domain logon caching is enabled on the server, be sure that you configure the Interactive logon: Number of previous logons to cache setting in the Windows security policies to something other than 0. For example, if the value is 5, the server caches logon information for 5 users. This security policy can be found in Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options. Domain caching allows users to log on even when they are not connected to a domain, such as when connected to a corporate network. Be sure that other security countermeasures are enforced, such as strong passwords, if this feature is enabled.

Use the secnet.ini file to configure the settings for the name resolution call. You can find this file in the <iFIX directory>\LOCAL folder.

In the secnet.ini file, the DomainRetrieverCall value can be modified to 0, 1, or 2, which correspond to one of the following methods:

- 0 - Use NetGetDcName
- 1 -Use NetGetAnyDcName
- 2 - Use DSGetDcName (Default)

**Example Entry in Secnet.ini File**

The following is an example of the text in the secnet.ini file that sets the Windows API function call. The example sets the DsGetDcName function (Active Directory) to return the name of a domain controller:

```
[SECNET]
DomainRetrieverCall=2
```

**NOTE:** iFIX reads the secnet.ini file during iFIX startup. If you modify this file, you must restart iFIX for the changes to be applied. Be aware that if you make any modifications to this file and later upgrade your iFIX system, you should review your custom settings in the secnet.ini file after the upgrade. Depending on the date of the modifications, there is a slight chance that you may need to enter your changes again, as the upgrade process typically overwrites the secnet.ini file with a newer version.

## Domain Caching

When iFIX Security is enabled, Domain Caching allows users to log into iFIX even when they are not connected to a domain, such as when connected to a corporate network. Only the logon information is persisted (not the full user name, for instance) to comply with Microsoft security policies.

When using domain caching, be sure that other security countermeasures are enforced, such as strong passwords.

Domain Caching is disabled by default in iFIX. To enable it, you need to update the secnet.ini file in the iFIX/Local folder. Change the EnableDomainLogonCache setting from 0 to 1, like this:

```
EnableDomainLogonCache=1
```

Save the secnet.ini file and restart iFIX.

Domain caching should be enabled where ever you want to cache the login. For instance, on the iFIX Server and iClient (View) nodes.

**NOTE:** In Microsoft Windows, If domain caching is enabled for logins, be sure that you configure the Interactive logon: Number of previous logons to cache setting in the Windows security policies to something other than 0. For example, if the value is 5, the server caches logon information for 5 users. This security policy can be found in Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options.

For more information on the secnet.ini file and other changes you can make to configure the Windows API that connects to the domain controller for authentication, refer to the "Control How iFIX Security Authenticates Windows Accounts" on page 41 topic.

## Using the Security Configuration Program

To connect your Windows and iFIX user accounts using the iFIX Security Configuration program, follow the steps below.

**To connect your Windows and iFIX user accounts:**

1. Create your Windows user accounts locally or on a domain controller. To ensure a secure environment, do not create any local accounts if you are using domain accounts. For more information on using a domain controller with Windows, refer to your Windows operating system documentation.
2. If a user account needs to log in to Windows in addition to iFIX, configure that Windows account with necessary rights, as described in the section User Accounts that Log in to Windows.
3. Run the iFIX Security Configuration program. In the User Profile dialog box for each iFIX user account, select Use Windows Security, and enter the Windows user name. If the account is local, leave the domain field blank; otherwise enter the name of the domain controller.

   The user and domain names you enter must match the names used by a Windows user account. Although iFIX login names can only be six characters for standard iFIX users, iFIX users who have Windows security enabled can have login names of up to twenty characters.

   For information on accessing the Security Configuration program, refer to the section The Security Configuration Program. For information on creating and modifying iFIX user accounts, refer to the sections Creating Group and User Accounts and Modifying Group and User Accounts.

## Using the Security Synchronizer

The Security Synchronizer is an application that allows you to assign iFIX security privileges to iFIX user accounts based on a Windows security configuration. This model enables you to use Windows security as a central source of configuration for both Windows and iFIX user accounts. This centralized security environment, consequently, assists you in compliance with FDA 21 CFR Part 11.

The Security Synchronizer supports Windows group membership at the local or domain level. Nested groups within a Windows domain are also supported, which allows for finding of users who are members of groups within the groups.

**NOTE:** Current iFIX software must be installed and running on the machine using the Security Synchronizer. The Security Synchronizer only synchronizes iFIX groups.

## Operational Overview

First you create Windows groups for each iFIX privilege you want to assign. This includes iFIX security areas, application features, and groups. Then you assign Windows users to these Windows groups. The Synchronizer accesses this Windows account information, and then adds, modifies, and deletes iFIX security user accounts based on this information. The Synchronizer modifies only those iFIX security user accounts configured to use Windows security. However, you can configure the Synchronizer to delete non-Windows users from iFIX. Refer to the /R parameter in the Using the Command Line section for more information about deleting users.

You can periodically run the Synchronizer as a background task or you can manually run the Synchronizer. Refer to Scheduling Security Synchronizer for more details.

**NOTE:** You must assign the Security Synchronizer application feature to the iFIX user that runs or schedules the Security Synchronizer.

You run the Synchronizer in these security storage configurations:

- Windows user and group accounts configured on the local computer.
- Windows user and group accounts configured on a domain controller.
- A combination of these two configurations.

**TIP:** If you run the Security Synchronizer and you have Change Management enabled, be aware that the security files may be under someone else's source control and you cannot modify them. Refer to the Check Out section for more information on Change Management rules. Check the alarm log file for Security Synchronizer results. If you installed iFIX to the default location, you can find this .log file in the C:\Program Files (x86)\Proficy\iFIX\ALM folder.

In addition to being able to run the Synchronizer in a number of configurations, Security Synchronizer also provides these features:

- Ability to run regardless of whether a user is logged into iFIX, or whether a logged-in user has sufficient iFIX security privileges.

  **NOTES:**

  - This feature depends on the system user having Automatic login privileges and the Security Synchronizer application feature assigned.
  - If Change Management is enabled and you want to use the Security Synchronizer: there must be an iFIX logged-in user, and that logged in user must have sufficient security privileges to use Change Management.
- An audit trail that lists all changes made to the iFIX security configuration through the security log and optionally through alarm messages.

- Added security that prevents you from accidentally running the Synchronizer. This is accomplished by requiring command line parameters for the program to run, and by requiring the system user to have the Security Synchronizer application feature assigned.
- A robust set of parameters you can use to customize the command line that runs the Synchronizer. For example, you can supply a time-out value to any new iFIX user accounts created by the Synchronizer, and you can remove all iFIX user accounts not configured to use Windows security. Refer to Using the Command Line for more information on command line parameters.
- Ability to process nested groups, finding users who are members of groups within the groups.

## Administrative Considerations

Before running the Synchronizer, you should be aware of the following considerations and potential constraints:

- You may schedule the Synchronizer to run at routine intervals. Because you cannot always determine which user may be logged-in when the Synchronizer runs, you may want to consider creating a "special" security user that has the appropriate rights and permissions to the Synchronizer. iFIX Security's System Autologin User option can be used to "impersonate" a certain user when the Synchronizer runs. Refer to the Node-based Security section for information about using the Autologin feature with Security Synchronizer.
- To ensure that the correct information is accessed when you use domain security, you may want to consider locating all Windows users in the same domain. If you use domain security in your configuration, the current Windows user must log in to Windows and the appropriate domain for the Synchronizer to retrieve the necessary user account information. Inability to access the domain can result in incomplete configuration information.

  **NOTE:** You do not need access to the domain if you use local security.
- The Security Synchronizer application is not intended to run as a service.
- iFIX security file structure prevents iFIX security users from being members of more than 12 iFIX security groups at the same time.
- You can assign no more than 20 characters when naming global groups on domain controllers that are configured to support access by users on systems earlier than Windows 2000.

  This restriction affects users who use domain-based Windows security when synchronizing iFIX security privileges. Because several iFIX security privilege names exceed 20 characters, shorter aliases are provided for these application features. Refer to the section Application Feature Name Aliases for a complete list of aliases.
- Be aware that when configuring your Windows users in iFIX Security, the Domain Name entry needs to be your domain's NetBIOS name.
- When iFIX security is enabled, you must ensure that at least one iFIX user has access to the iFIX Security Configuration application feature. The system will not delete the last remaining account with Security Configuration privileges; a message is logged to the audit trail indicating this situation.
- The Security Synchronizer uses the Windows security configuration as the master or source of the security data when it runs. Manual changes to a user's security privileges through the iFIX

Security Configuration utility are overwritten when Security Synchronizer runs if those changes do not match the Windows security configuration for that user.

Security Synchronizer does not change the domain name or Login Time-out values for existing user accounts in iFIX security; it does change the security privileges for security areas, application features, and iFIX groups assigned to the account.

**NOTE:** The Synchronizer may replace an existing iFIX account from one domain with a new account from another domain if the Windows user account has moved. In this case, the Synchronizer treats this as a new account, and not as a modification of an existing account. The Synchronizer deletes the original iFIX account and creates a new iFIX account with the appropriate domain and login time-out values.

## How the Security Synchronizer Works

The Security Synchronizer maps Windows group names to iFIX security privileges. You assign iFIX security privileges to users who are members of the Windows groups that represent these privileges. iFIX security privileges are revoked from users who are not members of Windows groups that represent these privileges.

The Security Synchronizer performs the following steps to synchronize iFIX security users with their Windows user accounts, based on Windows group memberships:

1. Reads the current iFIX security configuration to determine the currently-available security areas, application features, and iFIX group names. These names are used to determine the Windows group names that represent each iFIX privilege.
2. Determines which Windows users belong to each of the Windows group names.
3. Modifies the user account of the same name in iFIX security for each Windows user account that belongs to any of the valid group names.

   Only iFIX user accounts configured to "Use Windows Security" are modified. The Security Synchronizer makes modifications by assigning the user those privileges that map to the Windows groups for which they are a member, and deleting privileges that map to Windows groups for which they are not a member.
4. Creates a new iFIX security user account if the Windows user account name does not match an existing iFIX security user account. The appropriate iFIX security privileges are applied to the new account.
5. Removes any iFIX user from the security configuration who is not a member of at least one of the mapped Windows groups that represent an iFIX privilege.

   iFIX users not configured to "Use Windows Security" are removed in this manner only if the /R parameter is used in the Security Synchronizer command line. Refer to the Using the Command Line section for more information on the Security Synchronizer command line.

   **NOTE:** The Autologin user accounts are never removed from the security configuration, regardless of whether they use Windows security or belong to any Windows groups. If security is enabled, the last user account to have the Security Configuration application feature assigned to it will not be deleted. Also, if a user account is currently logged in to iFIX it will not be deleted.
6. Writes an audit trail message to the iFIX security log. The log message includes a record for each added and deleted iFIX user account, other account modifications, and errors encountered during

processing.

**NOTE:** These messages can also be sent to the iFIX alarm destinations as text messages. Refer to the Using the Command Line section for more information.

7. Writes analog and digital values to the iFIX database to indicate the success or failure of the synchronization. Writes are performed in this manner only if one or more of the Node.Tag.Field parameters are used in the command line. Refer to the Using the Command Line section for more information on the Security Synchronizer command line.

## Preparing to Run the Security Synchronizer

You must follow each of these steps to prepare the Security Synchronizer to run. Details for each step follow these summarized steps:

1. Decide the Source of Windows Security Information – Decide whether you want to use domain security, local node security, or both.
2. Create Windows Users - Create Windows users on the domain or local computer, as decided in the first step.
3. Create Windows Groups – Create Windows groups on the domain or local computer, as decided in the first step. You can use The CreateWindowsGroups Tool for this step.
4. Assign Users to Windows Groups and Grant Privileges – Assign the Windows groups created in the previous step to the appropriate Windows user accounts.
5. Configure iFIX Security – Create at least one iFIX account with the appropriate privileges to run the Security Synchronizer. Ensure that one of these users is logged in when the Security Synchronizer application is running.

   **NOTE:** You must perform this step only if you run Security Synchronizer while security is enabled.

### Decide the Source of Windows Security Information

The first step you must take in preparing to run the Security Synchronizer is to decide the source of Windows security information. You can create Windows groups in the local computer's security configuration or on a domain controller. You must determine if the security information should come from a Windows domain, the local computer, or both. One factor to consider when making this decision is the network configuration at the site where the Security Synchronizer is used.

**NOTE:** It is important to understand that the source of Windows security information determines where Windows groups are to be located, not where the Windows user accounts are to be found. Depending on whether local or domain security groups are used, the members of these Windows groups can be local user accounts, domain user accounts, or both. Domain groups may only contain domain user accounts, while a local group can contain both local and domain user accounts.

### Create Windows Users

Create your Windows user accounts locally or on a domain controller. To ensure a secure environment, do not create any local accounts if you are using domain accounts. For more information on using a domain controller with Windows, refer to your Windows operating system documentation.

If a user account needs to log in to Windows in addition to iFIX, configure that Windows account with necessary rights, as described in the section User Accounts that Log in to Windows.

## Create Windows Groups

Before using the Security Synchronizer, you must create Windows groups for all iFIX application features, security areas, and security groups to be assigned to iFIX users. You can use the CreateWindowsGroup tool to create these groups. Refer to The CreateWindowsGroups Tool for more information on using this tool.

Once you create Windows groups, you can use the Windows User Manager or a similar Windows security configuration tool to grant individual membership in the groups to Windows user accounts.

The following subjects are discussed in this topic:

- Configuration Strategy
- Limitations on Global Group Names

**Configuration Strategy**

You can reduce the number of Windows groups that must be created by grouping iFIX application features into iFIX security groups. Each iFIX security group can represent a set of application features that apply to a certain level of user, such as operators or supervisors.

You can then assign Windows users to the Windows group that represents the iFIX security group that represent their user level, such as "iFIX Security Group - Operators." Assigning users to groups in this manner:

- Eases the configuration process by grouping similar application features into a single security group.
- Helps you avoid assigning Windows users to every application feature privilege that they are to be granted.

Because iFIX security prevents an iFIX user from belonging to more than 12 security groups, you may still need to assign some application feature privileges individually. You should always assign security area privileges individually, since typically there are more application feature privileges than security areas.

Each Windows group name represents a single iFIX security privilege. An iFIX security privilege can be any of the following:

**iFIX Application Feature Name** – predefined in the iFIX security system.

**Security Area Name** – user-defined in the iFIX Security Configuration program. These names have default letter values of A through P when iFIX is installed.

**Security Group Name** – user-defined in the iFIX Security Configuration program.

Windows group names that represent each iFIX privilege are created by combining a prefix string indicating the type of iFIX privilege with the name of the iFIX privilege. There are long and short forms of the prefix string. The following table shows each type of iFIX privilege and its long and short prefix strings.

**Windows Group Names**

| iFIX Privilege | Long Prefix String | Short prefix string |
|---|---|---|
| Application Features | FIX Application Feature - | FAF - |
| Security Areas | FIX Security Area - | FSA - |
| Security Groups | FIX Security Group - | FSG - |

**NOTE:** You must use the correct syntax in prefix strings. Spaces before and after the dash are required in the long prefix string. Spaces before and after the dash are prohibited in the short prefix string.

The following table shows examples of iFIX privilege names and their corresponding Windows group names. It is assumed that an iFIX security area named "Plant Floor" and an iFIX security group named "Supervisors" has been configured in iFIX security for this example.

**Privilege Names and Corresponding Windows Groups**

| iFIX Privilege | Windows Group Name - long form | Windows Group Name - short form |
|---|---|---|
| Plant Floor Security Area | FIX Security Area - Plant Floor | FSA - Plant Floor |
| Supervisors Security Group | FIX Security Group - Supervisors | FSG - Supervisors |

**Limitations on Global Group Names**

You must limit the size of each Windows global group name to 20 characters if you synchronize iFIX security with Windows security groups that exist on either of the following domains:

- A Windows NT 4.0 domain
- Windows 2000 domain controllers that are configured to support access by users on systems earlier than Windows 2000.

Because many iFIX application feature names exceed this limit, to successfully use Security Synchronizer in this situation, you must do either of the following:

- Use aliases for iFIX application features that exceed 16 characters. Refer to Application Feature Name Aliases for a complete list of pre-defined Windows group name aliases for application feature names.
- Use the short prefix strings, described in the Windows Group Names table.

The 20-character limit on the size of the Windows global group name also affects user-defined iFIX security groups, which can be up to 30 characters long, and iFIX security area names, which can be up to 20 characters long. If you use the Windows NT 4.0 domain as the source of Windows security information, do not use more than 16 characters when naming iFIX security areas and iFIX security groups. This technique reserves four characters for the short prefix strings.

The 20-character limit does not apply to:

- Windows groups defined on a local computer (also referred to as local groups), since they can be up to 256 characters long.

- Windows XP domains or Windows 2000 domains with no access by users on systems earlier than Windows 2000, since global group names on these domains can be up to 64 characters long.

As an alternate solution to the global group name character limitation, you can also use Windows local groups to contain global groups. You can create local groups with the full application feature names and you can assign global groups with an arbitrary name to the appropriate local groups.

If you are a Windows user who belongs to the global group, you also belong to the local group that contains the global group. Therefore, you will be assigned the privilege associated with that local group name.

Since creating and maintaining local groups across multiple computers adds complexity to the configuration required to use the Security Synchronizer, you should use this alternate solution only when a single node is running the Security Synchronizer to synchronize a shared set of security files. If multiple nodes are running the Security Synchronizer to synchronize multiple copies of the iFIX security data, then you should use the application feature name aliases with global groups. Refer to Application Feature Name Aliases for a complete list of pre-defined Windows group name aliases for application feature names.

**CAUTION:** If you do not follow these procedures when using Windows NT 4.0 domain security with Security Synchronizer, an incorrect iFIX security configuration based on the Windows configuration may result.

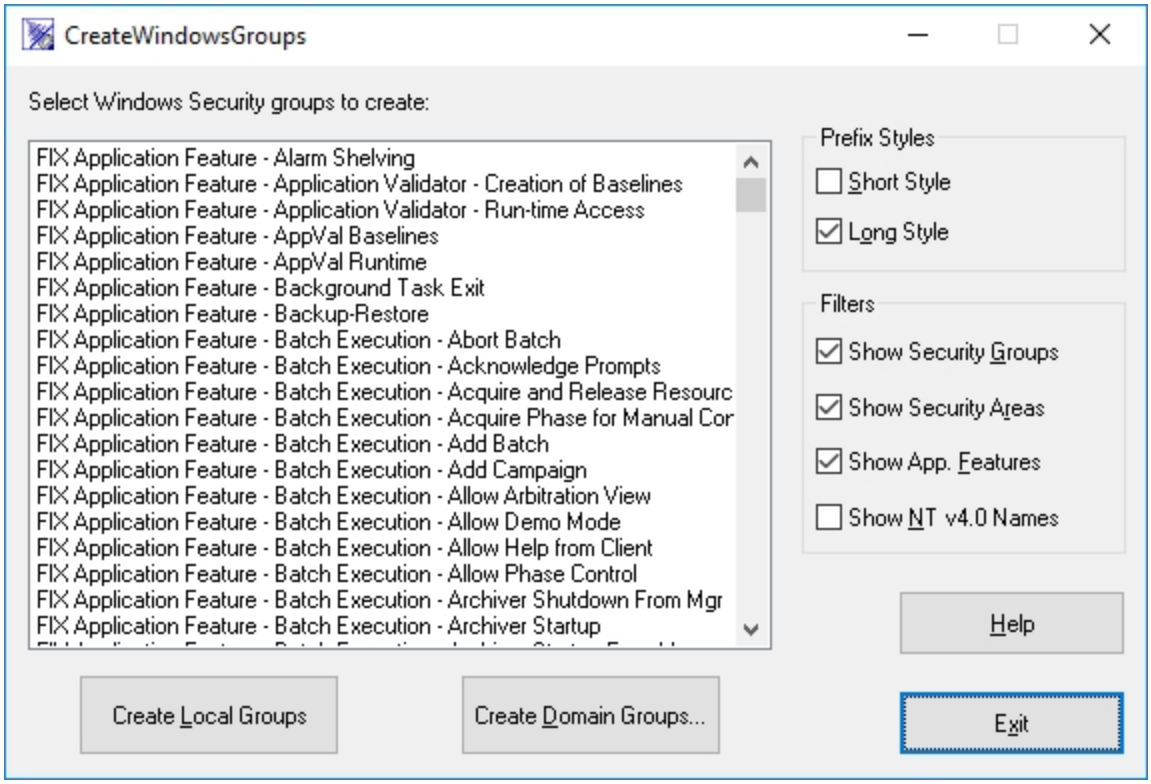
## The CreateWindowsGroups Tool

The CreateWindowsGroups tool helps you to quickly create Windows groups that map to iFIX privileges:

- Eliminate typographical errors when creating Windows security groups using the appropriate names to map to iFIX security privileges.
- Use the correct syntax when creating Windows security groups.
- Create Windows global and local groups, using the appropriate names for iFIX security privileges.

Before using this tool, you must log in to Windows as a member of the Administrators or Account Operators group on either the local computer or the Windows domain, depending on whether you create the Windows groups on the local computer or on the domain. However, iFIX does not need to be running to use this tool.

The following figure shows the CreateWindowsGroups tool. Use the procedures following this figure to create Windows security groups.




*The CreateWindowsGroups Tool*

**To create Windows groups using the CreateWindowsGroups tool:**

1. Run CreateWindowsGroups.exe from the iFIX directory. A list of Windows group names displays in a list box. The Windows group names are derived from the current iFIX security configuration, including the user-configured security group and security area names.

   **NOTE:** Windows group names display in the list box only if you establish all group and security area names in the iFIX Security Configuration program before using the CreateWindowsGroups tool.

2. Select the appropriate filters and prefix style for the Windows groups you wish to create. If you are creating groups on a Windows NT 4.0 domain, you must select the Show NT 4.0 Names filter.

3. Select the groups you want to create in Windows security from the list box of group names. The list may include different group names that represent the same iFIX security privileges.

   **NOTE:** Use Ctrl/Click to select multiple group names in the list box. Use Shift/Click to select a range of group names in the list box.

4. Click Create Local Groups to create the groups currently selected in the list box if you are creating Windows groups on the local computer.

5. Click Create Domain Groups. The Specify Domain for Group Creation dialog box appears.

6. In the Create Groups on this Domain edit box, specify a domain name, if you are creating Windows groups on the Windows domain.

7. Click OK.

## Assign Users to Windows Groups and Grant Privileges

Once you create the Windows groups that you need, you can assign Windows user accounts to the groups that correspond to iFIX security privileges. You use the Windows User Manager tool to assign users to groups that represent the iFIX privileges that they should be granted.

## Configure iFIX Security

You can run the Security Synchronizer using a node-based or user-based approach to iFIX security.

**Node-based Security**

Choose this method if you want to run the Security Synchronizer on a node, regardless of who, if anyone, is logged into iFIX. Using the iFIX security Autologin feature, you must specify an iFIX user account as the system user. This account is automatically logged in as the system user the next time iFIX is started. You cannot log this user off unless you remove the associated account from the System User field in the Automatic Login Node dialog box, located in the Security Configuration program and restart iFIX.

**NOTE:** The system user you create here is recognized only by the Security Synchronizer. Other iFIX features and programs do not recognize the system user; therefore, this user cannot be used to provide access to any security privilege other than running the Security Synchronizer.

**To specify the system user:**

1. Open the Security Configuration program.
2. On the Edit menu, click Autologin.
3. Click Add.
4. In the Node field, enter the iFIX node name. This is the node where the Security Synchronizer will be run.
5. In the System User field, select an account.
6. Click OK.

Refer to the chapter Defining and Assigning Security Privileges for more information on the Security Configuration program.

The user account logged in as a system user must have these two application features to be able to execute the Security Synchronizer:

**Security Synchronizer** – needed to actually run the Security Synchronizer.

**System User Login** – needed for the user to be logged-in as the system user.

If you follow this method, the Security Synchronizer can run, providing these conditions are true:

- iFIX is running.
- Security Configuration program is not running.
- A user is logged in to Windows.

The Security Synchronizer can run even if a non-system user, such as an operator with limited security privileges, is logged in. iFIX logs the system user in at startup, and the Security Synchronizer checks for the system user when it executes.

The iFIX user account specified as the system user is not modified or deleted by Security Synchronizer, even if the /R parameter is specified. Refer to the Command Line Parameter Errors section for more information on the run-time parameters. When this iFIX user account is used, its privileges to run the Security Synchronizer cannot be revoked. Therefore, you should create a separate iFIX user account that represents the system user with only the necessary security privileges. You should avoid using an existing iFIX user's account.

**NOTE:** Once you add a system user to the Autologin configuration, you must restart iFIX for that user to become logged-in.

**User-based Security**

To use this method, the currently logged in iFIX user must have the privileges necessary to run the Security Synchronizer. You must assign the Security Synchronizer application feature to the appropriate user accounts. If you do not specify a system user in the iFIX Autologin configuration, then, by default, user-based security is used.

Under user-based security, if the current user does not have the appropriate Security Synchronizer application feature privilege or if no user is logged in, the Security Synchronizer does not run and a message is sent to the audit trail file.

## Running the Security Synchronizer Application

You should run Security Synchronizer from only one location for each set of iFIX security files you maintain. If all nodes on a company network use a shared set of iFIX security files that are stored on a file server, then only one node on the network should run Security Synchronizer to update the security configuration. If each iFIX node maintains its own set of iFIX security files, then you must run Security Synchronizer on each node in order to update the security configuration for each node.

**NOTE:** Actions on an iClient node that affect data in the iFIX database require that the iFIX user have the proper privileges on both the SCADA and View node; this requires that iFIX security configurations are identical on both nodes. You may want to update all iFIX security configurations using Security Synchronizer at or near the same time to keep separate security configurations synchronized with each other.

Because the Security Synchronizer runs as a background task, you must execute it from a command prompt window or use a similar method to supply command line parameters to the program.

You cannot start the Security Synchronizer by double-clicking the file in Windows Explorer because you need to supply command line parameters to start the synchronization process. This inability to launch the Synchronizer provides added security by preventing you from clicking the program icon in Explorer and initiating the synchronization process at an inappropriate time, which could lead to an incorrect security configuration.

You can, however, execute the program using an icon you create that contains the appropriate command line parameters. You can create a Windows shortcut that points to the Security Synchronizer program and supplies the command line parameters. Use the Shortcut tab of a shortcut to the SecuritySynchronizer.exe to enter the appropriate information to create your shortcut.

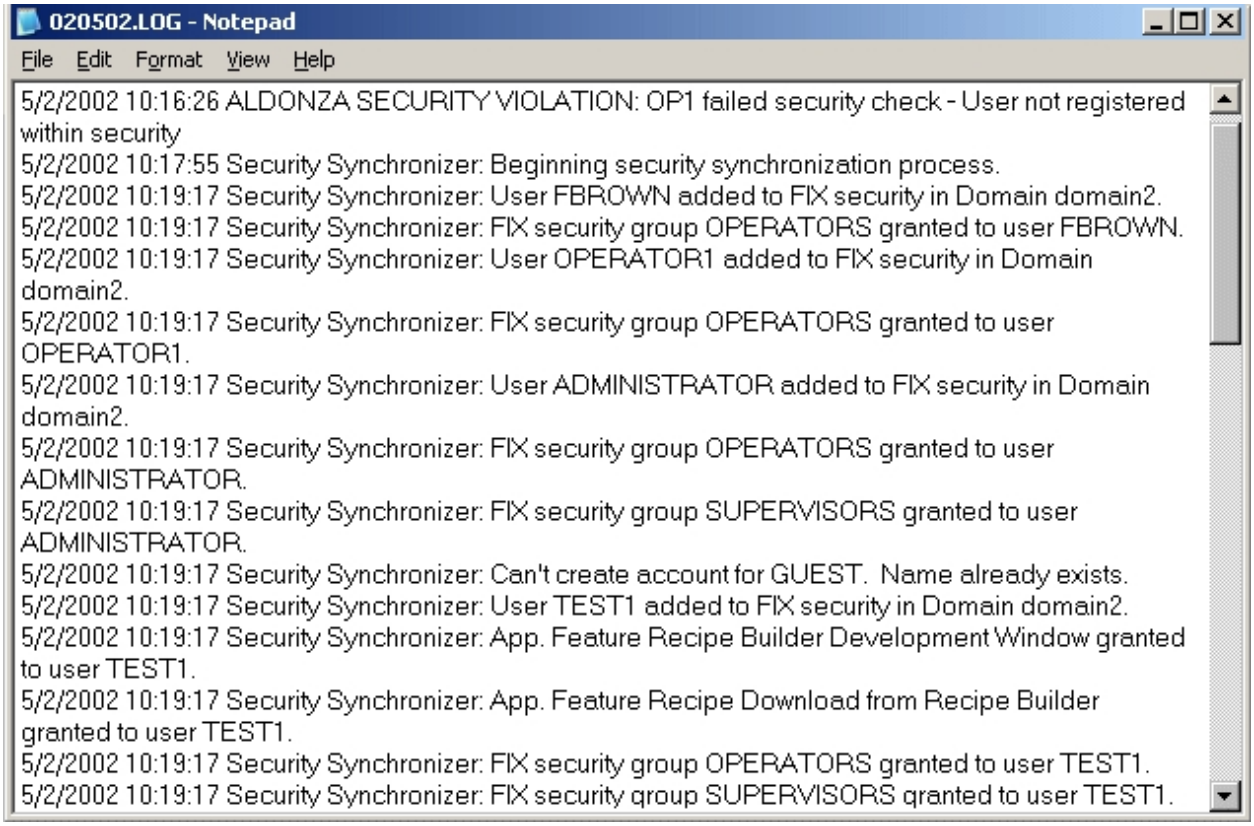
**NOTE:** The Security Synchronizer only synchronizes iFIX groups.

To run Security Synchronizer, you must:

- Install iFIX on the computer that will run Security Synchronizer.
- Log the computer into the Windows domain from which user accounts will be retrieved, either the local computer domain or a global domain.

All output that results from running the Security Synchronizer is directed to the security log file. The security log file is located in the iFIX Alarm path. Optionally, these messages can be directed to the iFIX alarm destinations as text messages. Refer to Using the Command Line for more information.

The following figure shows typical messages written to the security log file while the Security Synchronizer runs. In this example, several users, such as FBROWN and OPERATOR1, configured to use the domain2 domain in the Windows Security configuration, are added to the iFIX security configuration.




*Security Log/Audit Trail*

You cannot run the iFIX Security Configuration program and the Security Synchronizer at the same time. The system prevents the two from running simultaneously, which prevents one program from overwriting changes that the other program is currently trying to make to the security files.

To determine if the Security Synchronizer has completed, you can:

- Check the alarm destinations or security log file for a message indicating this state. An alarm destination can be the alarm history, alarm file, or alarm printers.
- Use the Completion Status tag command line parameter.

## Using the Command Line

The following table describes each option in the command line.

**SecuritySynchronizer.exe Command Line Parameters**

| Command Line Option | Description |
|---|---|
| /D*"domain1 domain2 domain3"* | Supplies the name of the domain where the Windows groups are located. You must supply either this parameter or the /L parameter (or both parameters) to enable the Security Synchronizer to locate the Windows groups.<br><br>An example when using multiple domains:<br><br>/D"name1 name2 name3"<br><br>An example when using a single domain:<br><br>/Dname1 |
| /N | Supports the processing of nested groups within a Windows domain; finding users who are members of groups within the groups. For example:<br><br>SecuritySynchronizer.exe /D"domain1" /N |
| /L | Indicates that the local computer security configuration where the Windows groups are located. You must supply either this parameter, or the /D<domain name> parameter, or both parameters to enable the Security Synchronizer to locate the Windows groups. |
| /R | Indicates that all iFIX user accounts not configured to use Windows security will be removed from the security configuration.<br><br>Any accounts that do not have the Use Windows Security check box selected in the iFIX Security User Configuration dialog box will be removed from iFIX security with the following exceptions:<br><br>• The Application and System User Autologin accounts are not deleted from iFIX security.<br>• The user account that is currently logged in is not deleted from iFIX security. |
| /E *Node.Tag.Field* | Supplies the name of an analog iFIX database tag and floating point (F_) field to which a value is written after the Security Synchronizer completes. The value written to this tag indicates the most serious error, if any, encountered during the synchronization process. A value of 0 indicates that no errors were encountered.<br><br>Refer to Understanding Security Synchronizer Messages for a list of error codes. |
| /F *Node.Tag.Field* | Supplies the name of a digital iFIX database tag and floating point (F_) field to which a value is written after the Security Synchronizer completes. A value of 0 indicates that no errors were encountered. A value of 1 indicates that an error was encountered.<br><br>You can determine the specific error encountered by checking the security log file or the Analog Error tag, specified using the /E parameter. |
| /C *Node.Tag.Field* | Supplies the name of a digital iFIX database tag and floating point (F_) field to which a value is written that indicates that the Security Synchronizer has completed. The value 1 is written when the synchronization has completed. |

**NOTE:** You must manually set this tag's value to 0 before running the Security Synchronizer if you want to determine whether the process has completed.

/T# *seconds* — Supplies an iFIX Login Time-out value to apply to any new iFIX user accounts created by Security Synchronizer.

If you do not use this parameter, the default value of 0 seconds (no Login Time-out) is used for all new iFIX user accounts.

The maximum value allowed is 86399 seconds, or 23:59:59.

For more information, refer to the Limiting Login Time section.

/M*map mode* — Indicates the security mapping scheme to be used by Security Synchronizer to perform the synchronization.

In iFIX 4.0, 3.5, and 3.0 only the default mapping scheme is valid. The mapping scheme refers to how Windows group names are mapped to iFIX privileges.

**NOTE:** This parameter is intended for future use only. Do not use this parameter.

/A — Indicates that all messages sent to the security log file should also be sent to the alarm destinations as text messages. If this parameter is not supplied, most messages are not sent to the alarm destinations.

**Command Line Parameter Example**

A fictitious PlantA domain is used in this example. This command line will:

- Retrieve Windows Security groups from the PlantA domain.
- Leave iFIX user accounts intact if they are not using Windows security.
- Write the final error code to the iFIX database on node SCADA1 (tag name SYNCERROR).

The command line required by the PlantA domain in this example is:

```
SecuritySynchronizer.exe /DPlantA /ESCADA1.SYNCERROR.F_CV
```

The following conditions result because the indicated parameters are not used in the previous command line example:

- iFIX accounts not using Windows security are not removed because the /R parameter is not used.
- Local Windows security information is ignored because the /L parameter is not used.
- No digital failure value is written to an iFIX database because the /F parameter is not used.
- No completion status value is written to an iFIX database because the /C parameter is not used.
- A default Login Time-out value of 0 seconds is applied to new iFIX user accounts created by the Security Synchronizer because the /T parameter is not used. This causes time-out to be disabled.
- Messages are not written to the alarm destinations because the /A parameter is not used.

**NOTE:** You must run the command line while a Windows user is currently logged in to the PlantA domain. Otherwise, the Security Synchronizer fails because it cannot retrieve the Windows security information.

## When to Run the Security Synchronizer

You should run the Security Synchronizer:

- Whenever you make changes to the Windows security configuration that affects iFIX users, such as when you add or remove users from mapped Windows groups.
- After you add, change, or remove iFIX security groups or security area names, as these changes affect the Windows groups that map to these privileges.

## Scheduling Security Synchronizer

You may want to implement a scheduling strategy if you make frequent changes to the Windows security configuration that will affect the iFIX security configuration.

The Security Synchronizer application does not have a self-scheduling function, but you can use scheduling software or a third-party scheduling tool to run the application at specified times or intervals.

iFIX offers a scheduling tool, called the Scheduler, that helps you easily run the Security Synchronizer at designated times. Refer to the Mastering iFIX manual for details on using this tool.

You may want to consider using the Scheduled Task Wizard located on the Control Panel to schedule the Security Synchronizer.

### Using the Task Scheduler Service

You can use this service to schedule programs at designated times and intervals.

**To use the Windows Task Scheduler:**

1. Log in to Windows as a member of the local Administrator group. Only members of this group can schedule tasks for execution.
2. Ensure that the Task Scheduler service is running by checking the Services dialog box from Control Panel. The Task Scheduler service displays in the list.
3. Open a command prompt window and type the At command, followed by the appropriate parameters to indicate the name of the task and the time of execution. Refer to Windows Help for more information about the At command and command line parameters used by the Task Scheduler.
4. View the task you scheduled by typing "at" at the command line. Do not supply any parameters. The list of scheduled tasks displays.

### Examples

To schedule the SecuritySynchronizer.exe program to run on a local computer every Monday and Thursday at 3:00 a.m., you should enter the following command:

```
at 3:00 /every:M,Th SecuritySynchronizer.exe command line parameters
```

where <*command line parameters*> represents the command line parameters to be passed to SecuritySynchronizer.exe, such as /L and /R. Refer to Using the Command Line for more information on command line parameters.

To schedule the SecuritySynchronizer.exe program to run on the 25th day of each month at 6:00 p.m. on a computer named View3, you should enter the following command:

```
at\\View3 18:00/next:25 SecuritySynchronizer.exe <command line parameters>
```

### Using an iFIX Database Program Block

You can use an iFIX database Program block to schedule the run time for Security Synchronizer. Due to the limit on the length of command lines in Program blocks, you must create a Windows command file that executes from the Program block.

A Windows command file is a text file that contains the command line to run, including the program name and any command line parameters. The command file must end with the .CMD file extension.

The Windows command file you use must reside in the iFIX root directory (C:\Program Files (x86)\Proficy\iFIX) if no path is specified on the Program block command line, or you must specify the full path to the file in the Program block command line.

An example of the text of a command file used to run the Security Synchronizer:

```
SecuritySynchronizer.exe /DPlantA /L /T /R
```

**NOTE:** This command file is saved as SecSync.cmd.

An example of a Program block command line that runs the above command file using the Program block's RUNTASK command if the SecSync.cmd file is in the iFIX base path:

```
RUNTASK SecSync.cmd
```

An example of a Program block command line that runs the above command file using the Program block's RUNTASK command if the SecSync.cmd file is in the C:\ directory:

```
RUNTASK C:\SecSync.cmd
```

## Using the Security Synchronizer Automation Interface

The Security Synchronizer program is a background task that you use with command line parameters to execute the security synchronization process.

You can also program the synchronization process using the SecuritySynchronizer Automation object. This object provides the properties and methods you need to synchronize iFIX security with your Windows security configuration. You have the ability to write custom applications or scripts that automate how and when the security synchronization process executes.

For a description of the SecuritySynchronizer object and the properties and methods available through it, see the iFIX Automation Interfaces Help file.

## Application Feature Name Aliases

You can use the aliases listed in this section to represent the indicated application feature name. These aliases are provided only for iFIX application feature names that exceed 16 characters. These aliases allow you to create domain groups without exceeding the 20-character group name limit imposed by the systems listed above.

The following table lists all application feature name aliases for iFIX.

**iFIX Application Feature Name Aliases**

| iFIX Application Feature Name | Windows Group Name Alias or Aliases |
|---|---|
| Alarm Shelving | FAF - Alarm Shelving |
| Application Validator - Creation of Baselines | FAF–Application Validator - Creation of Baselines<br>FAF–AppVal Baselines |
| Application Validator - Run-time Access | FAF–Application Validator - Run-time Access<br>FAF–AppVal Runtime |
| Background Task Exit | FAF–Background Task Exit<br>FAF–BG Task Exit |
| Change Management | FAF–Change Management<br>FAF–PCM |
| Data Provider Service | FAF–Data Provider Service |
| Database Manager | FAF–Database Manager |
| Database Reload | FAF–Database Reload |
| Database Save | FAF–Database Save |
| Database Block Add-Delete | FAF–Database Block Add-Delete<br>FAF–DB Block Add-Del |
| EDA Feature [1-55] | FAF–EDA Feature [1-55] |
| Electronic Signature – Bypass | FAF–Electronic Signature - Bypass<br>FAF–ESig-Bypass |
| Electronic Signature – Perform By | FAF–Electronic Signature - Perform By<br>FAF–ESig-Perform By |
| Electronic Signature – Verify By | FAF–Electronic Signature - Verify By<br>FAF–ESig-Verify By |
| Enable Ctrl-Alt-Del | FAF–Enable Ctrl-Alt-Del<br>FAF–Ctrl-Alt-Del |
| Enable Task Switching | FAF–Task Switching<br>FAF–Enable Task Switching |
| Fix32 – Alarm Summary Display | FAF–Fix32 - Alarm Summary Display<br>FAF–F32 - Alm Sum |
| Fix32 – Historical Display Configuration | FAF–Fix32 - Historical Display Configuration<br>FAF–F32 - HTDCFG |
| Fix32 – Historical Trend Display | FAF–Fix32 - Historical Trend Display<br>FAF–F32 - HTD |
| Fix32 – Historical Trend Display View Only | FAF–Fix32 - Historical Trend Display View Only<br>FAF–F32 - HTDView |

| | |
|---|---|
| Fix32 – Key Macro Editor | FAF–Fix32 - Key Macro Editor<br>FAF–Fix32 - KME |
| Fix32 – Operating System Window | FAF–Fix32 - Operating System Window<br>FAF–F32 - OS Win |
| Fix32 – Report Creator | FAF-Fix32 Report Creator<br>FAF-F32 RepCre |
| Fix32 – Report Generator | FAF-Fix32 Report Generator<br>FAF-F32 RepGen |
| Fix32 – Run a Task from View | FAF–Fix32 - Run a Task from View<br>FAF–F32 - RUNTASK |
| GE OEM Reserved 1 | FAF–GE OEM Reserved 1<br>FAF–OEM Reserved 1 |
| GE OEM Reserved 10 | FAF–GE OEM Reserved 10<br>FAF–OEM Reserved 10 |
| GE OEM Reserved 11 | FAF–GE OEM Reserved 11<br>FAF–OEM Reserved 11 |
| GE OEM Reserved 12 | FAF–GE OEM Reserved 12<br>FAF–OEM Reserved 12 |
| GE OEM Reserved 2 | FAF–GE OEM Reserved 2<br>FAF–OEM Reserved 2 |
| GE OEM Reserved 3 | FAF–GE OEM Reserved 3<br>FAF–OEM Reserved 3 |
| GE OEM Reserved 4 | FAF–GE OEM Reserved 4<br>FAF–OEM Reserved 4 |
| GE OEM Reserved 5 | FAF–GE OEM Reserved 5<br>FAF–OEM Reserved 5 |
| GE OEM Reserved 6 | FAF–GE OEM Reserved 6<br>FAF–OEM Reserved 6 |
| GE OEM Reserved 7 | FAF–GE OEM Reserved 7<br>FAF–OEM Reserved 7 |
| GE OEM Reserved 8 | FAF–GE OEM Reserved 8<br>FAF–OEM Reserved 8 |
| GE OEM Reserved 9 | FAF–GE OEM Reserved 9<br>FAF–OEM Reserved 9 |
| Historical Trend Assign | FAF–Historical Trend Assign |

| | |
|---|---|
| | FAF–HTA |
| Historical Trend Collection | FAF–Historical Trend Collection<br>FAF–HTC |
| Historical Trend Export | FAF–Historical Trend Export<br>FAF–HTD Export |
| iFIX – System Shutdown | FAF–iFIX System Shutdown<br>FAF–iFIX Shutdown |
| Manual Failover | FAF–Manual Failover |
| OPC UA Configuration Tool | FAF-OPC UA Configuration Tool |
| Project Backup-Restore | FAF–Backup-Restore<br>FAF–Project Backup-Restore |
| Recipe Save from Recipe Builder | FAF–Recipe Save from Recipe Builder<br>FAF–RCP Builder Save |
| Recipe Builder Development Window | FAF–Recipe Builder Development Window<br>FAF–RCP Dev Window |
| Recipe Download from Recipe Builder | FAF–Recipe Download from Recipe Builder<br>FAF–RCP Download |
| Recipe Builder Operations Window | FAF–Recipe Builder Operations Window<br>FAF–RCP Op Window |
| Recipe Text Output from Recipe Builder | FAF–Recipe Text Output from Recipe Builder<br>FAF–RCP Text Output |
| Recipe Upload from Recipe Builder | FAF–Recipe Upload from Recipe Builder<br>FAF–RCP Upload |
| Recipe Load | FAF–Recipe Load |
| Recipe Save | FAF–Recipe Save |
| Runtime Visual Basic Editor Access | FAF–Runtime Visual Basic Editor Access<br>FAF–Runtime VBE |
| Security Configuration | FAF–Security Configuration<br>FAF–Security Config |
| Security Synchronizer | FAF–Security Synchronizer<br>FAF–Security Synch |
| Startup Profile Manager | FAF–Startup Profile Manager<br>FAF–SU Profile Mgr |
| System User Login | FAF–System User Login<br>FAF–Sys User Login |
| System User Logout | FAF–System User Logout |

| | |
|---|---|
| | FAF–Sys User Logout |
| System Configuration | FAF–System Config<br>FAF–System Configuration |
| Tag Group Editor | FAF–Tag Group Editor |
| Tag Status | FAF–Tag Status |
| VisconX Writes | FAF–VisiconX Writes |
| WorkSpace Configure | FAF–WS Configure<br>FAF–WorkSpace Configure |
| WorkSpace Runtime | FAF–WS Runtime<br>FAF–WorkSpace Runtime |
| WorkSpace Runtime Exit | FAF–WS Runtime Exit<br>FAF–WorkSpace Runtime Exit |

The following table lists all application feature name aliases for Batch Execution.

**Batch Execution Application Feature Name Aliases**

| Batch Execution Application Feature Name | Application Feature Name Alias |
|---|---|
| Batch Execution – Abort Batch | FAF–BE Abort Batch<br>FAF–Batch Execution - Abort Batch |
| Batch Execution – Acknowledge Prompts | FAF–BE Ack Prompts<br>FAF–Batch Execution - Acknowledge Prompts |
| Batch Execution – Acquire and Release Resources | FAF–BE Acq-Rel Res<br>FAF–Batch Execution - Acquire and Release Resources |
| Batch Execution – Acquire Phase for Manual Control | FAF–BE Acquire Phase<br>FAF–Batch Execution - Acquire Phase for Manual Control |
| Batch Execution – Add Batch | FAF–BE Add Batch<br>FAF–Batch Execution - Add Batch |
| Batch Execution – Add Campaign | FAF–BE Add Cmpn<br>FAF–Batch Execution - Add Campaign |
| Batch Execution – Allow Arbitration View | FAF–BE Arbit View<br>FAF–Batch Execution - Allow Arbitration View |
| Batch Execution – Allow Demo Mode | FAF–BE Allow Demo<br>FAF–Batch Execution - Allow Demo Mode |
| Batch Execution – Allow Help from Client | FAF–Batch Execution - Allow Help from Client<br>FAF–BE Client Help |
| Batch Execution – Allow Phase Control | FAF–BE Phase Control |

| | |
|---|---|
| | FAF–Batch Execution - Allow Phase Control |
| Batch Execution – Archiver Startup | FAF–BE Arch Start<br>FAF–Batch Execution - Archiver Startup |
| Batch Execution – Archiver Startup from Mgr | FAF–BE Arch Start AM<br>FAF–Batch Execution - Archiver Startup from Archiver Manager |
| Batch Execution – Archiver Shutdown from Mgr | FAF–BE Arch Stop AM<br>FAF–Batch Execution - Archiver Shutdown from Archiver Manager |
| Batch Execution – Change Formulation Status | FAF–BE Ch Forml Stat<br>FAF–Batch Execution - Change Formulation Status |
| Batch Execution – Change to Auto/Manual Mode | FAF–BE Change Mode<br>FAF–Batch Execution - Change to Auto-Manual Mode |
| Batch Execution – Clear All Failures | FAF–BE Clear Failure<br>FAF–Batch Execution - Clear All Failures |
| Batch Execution – Client Startup | FAF–BE Client Start<br>FAF–Batch Execution - Client Startup |
| Batch Execution – Client Shutdown | FAF–BE Client Stop<br>FAF–Batch Execution - Client Shutdown |
| Batch Execution – Configuration | FAF–BE Config<br>FAF–Batch Execution - Configuration |
| Batch Execution – Configure Campaign | FAF–BE Config Cmpn<br>FAF–Batch Execution - Configure Campaign |
| Batch Execution – Configure the Client | FAF–BE Client Cfg<br>FAF–Batch Execution - Configure the Client |
| Batch Execution – Create Equipment Configuration | FAF–BE Create Eq Cfg<br>FAF–Batch Execution - Create Equipment Configuration |
| Batch Execution – Create New Project in iFIX WorkSpace | FAF–BE New Project<br>FAF–Batch Execution - Create New Project in iFIX WorkSpace |
| Batch Execution – Create Recipes | FAF–BE Create Rcp<br>FAF–Batch Execution - Create Recipes |
| Batch Execution – Duplicate Campaign | FAF–BE Duplicate Cmpn<br>FAF–Batch Execution - Duplicate Campaign |
| Batch Execution – Equipment Editor Startup | FAF–BE Eq Edt Start |

| | |
|---|---|
| | FAF–Batch Execution - Equipment Editor Startup |
| Batch Execution – Go to HMI | FAF–BE Go to HMI<br>FAF–Batch Execution - Go to HMI |
| Batch Execution – Hold Batch | FAF–BE Hold Batch<br>FAF–Batch Execution - Hold Batch |
| Batch Execution – Launch Campaign | FAF–BE Launch Cmpn<br>FAF–Batch Execution - Launch Campaign |
| Batch Execution – Misc Item Deletion from iFIX WorkSpace | FAF–BE Misc Item Del<br>FAF–Batch Execution - Misc Item Deletion from iFIX WorkSpace |
| Batch Execution – Modify Campaign | FAF–BE Modify Cmpn<br>FAF–Batch Execution - Modify Campaign |
| Batch Execution – Pause Campaign | FAF–BE Pause Cmpn<br>FAF–Batch Execution - Pause Campaign |
| Batch Execution – iFIX WorkSpace Startup | FAF–BE WS Startup<br>FAF–Batch Execution - iFIX WorkSpace Startup |
| Batch Execution – Recipe Editor Startup | FAF–BE Rcp Edt Start<br>FAF–Batch Execution - Recipe Editor Startup |
| Batch Execution – Rebind Unit Procedure | FAF–BE Rebind UP<br>FAF–Batch Execution - Rebind Unit Procedure |
| Batch Execution – Rebuild Recipe Directory | FAF–BE Rebuild Dir<br>FAF–Batch Execution - Rebuild Recipe Directory |
| Batch Execution – Release Recipes to Production | FAF–BE Release Rcp<br>FAF–Batch Execution - Release Recipes to Production |
| Batch Execution – Remove Batch | FAF–BE Remove Batch<br>FAF–Batch Execution - Remove Batch |
| Batch Execution – Remove Campaign | FAF–BE Remove Cmpn<br>FAF–Batch Execution - Remove Campaign |
| Batch Execution – Remove Formulation | FAF–BE Remove Forml<br>FAF–Batch Execution - Remove Formulation |
| Batch Execution – Remove Recipes | FAF–BE Remove Rcp<br>FAF–Batch Execution - Remove Recipes |
| Batch Execution – Restart Batch | FAF–BE Restart Batch<br>FAF–Batch Execution - Restart Batch |
| Batch Execution – Restart Campaign | FAF–BE Restart Cmpn |

| | |
|---|---|
| | FAF–Batch Execution - Restart Campaign |
| Batch Execution – Save Equipment Configuration | FAF–BE Save Eq Cfg<br>FAF–Batch Execution - Save Equipment Configuration |
| Batch Execution – Save Formulation | FAF–Batch Execution - Save Formulation |
| Batch Execution – Save from iFIX WorkSpace | FAF–BE WS Save<br>FAF–Batch Execution - Save from iFIX WorkSpace |
| Batch Execution – Save Recipes | FAF–BE Save Rcp<br>FAF–Batch Execution - Save Recipes |
| Batch Execution – Server Startup | FAF–BE Server Start<br>FAF–Batch Execution - Server Startup |
| Batch Execution – Server Shutdown | FAF–BE Server Stop<br>FAF–Batch Execution - Server Shutdown |
| Batch Execution – Shutdown Campaign | FAF–Batch Execution - Shutdown Campaign |
| Batch Execution – Simulator Startup | FAF–BE Sim Start<br>FAF–Batch Execution - Simulator Startup |
| Batch Execution – Start Batch | FAF–BE Start Batch<br>FAF–Batch Execution - Start Batch |
| Batch Execution – Start Campaign | FAF–BE Start Cmpn<br>FAF–Batch Execution - Start Campaign |
| Batch Execution – Start iWorkInstruction Editor | FAF–BE Start iWI Ed<br>FAF–Start iWorkInstruction Editor |
| Batch Execution – Start SoftPhase Server | FAF–BE Start SoftPhs<br>FAF–Start SoftPhase Server |
| Batch Execution – Stop Batch | FAF–BE Stop Batch<br>FAF–Batch Execution - Stop Batch |
| Batch Execution – Stop SoftPhase Server | FAF–BE Stop SoftPhs<br>FAF–Batch Execution - Stop SoftPhase Server |
| Batch Execution – View Campaign | FAF–BE View Cmpn<br>FAF–Batch Execution - View Campaign |

## Using iFIX with Proficy Authentication

Proficy Authentication provides support for mufti-factor authentication. It also provides centralized management of Proficy users and groups, and a common security model across Proficy products such as Historian and Operations Hub.

**NOTE:** For iFIX security to work in the network, all the iFIX nodes must be connected to a same Proficy Authentication server. If you have any previous versions of iFIX SCADA or view nodes, you can continue to log in to iFIX 2022 using the existing security users.

You can use Proficy Authentication in the following scenarios:

- You want to use a common, multi-factor authentication to log in to iFIX and other Proficy products, regardless if you are using Configuration Hub.
- You installed iFIX, Configuration Hub, and the Proficy Authentication (UAA) server, and you want to use Configuration Hub with iFIX .

  **NOTE:**If you are using Windows Server operating system, you must disable Internet Explorer Enhanced Security Configuration, else it might cause an issue while logging in to iFIX using Proficy Authentication. This is enabled by default on Windows Servers. Follow the instructions documented here on the Microsoft web site: FAQ about Internet Explorer Enhanced Security Configuration (ESC).

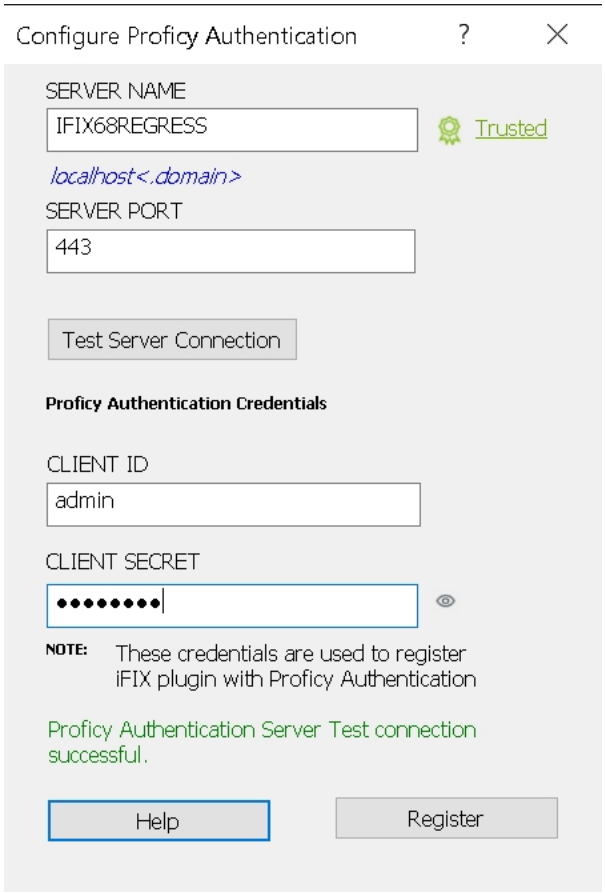
## Registering iFIX with Proficy Authentication Server

You can register iFIX with the Proficy Authentication server and log in to iFIX using Proficy Authentication option. This type of registration is more suitable for the nodes that do not have interaction to Configuration hub. This enables you with a common authorization access that is similar to single sign on (SSO).

Before you begin to register iFIX to Proficy Authentication server, you must enable security. For more information, refer to the section "Enabling and Disabling Security " on page 26.

To register iFIX with the Proficy Authentication server:

1. Open the iFIX application.
2. Log in to iFIX. For information on how to log in, refer to the section "Logging in to iFIX Manually" on page 37.
3. In Ribbon view, on the **Applications** tab, in the **System & Security** group, click **Security**, and then click **Security Configuration Utility**.
   The **Security** dialog box appears.
4. Click **OK**.
   The **Security Configuration** window appears.
5. In the **Security Configuration** window, click **Edit**, and then click **Configure Proficy Authentication**.
   The **Configure Proficy Authentication** dialog box appears.




6. Enter the following details:

| Field | Description |
|---|---|
| **SERVER NAME** | The name of the Proficy authentication server to which you want to register. In the <Fully qualified domain name> format. |
| **SERVER PORT** | The port number of the Proficy authentication server to which you want to register. The default port number of the Proficy authentication server is 443. |

7. If the root certificate of the Proficy authentication server is trusted, you will see **Trusted**. If not, you will see **Not trusted**; then you must manually trust the certificate. For more information, refer to the section "Trust an Untrusted Certificate while Registering iFIX to Proficy Authentication Server" on page 69.
8. To test the connection, click **Test Server Connection**.

   If the connection to the Proficy authentication server is successful, you will receive a success dialog. If your connection is unsuccessful, retry to connect to another valid Proficy authentication server.
9. In the **Proficy Authentication Credentials**, enter the following details:

| Field | Description |
|---|---|

| | |
|---|---|
| **CLIENT ID** | Client ID of the Proficy authentication server. This is the client ID that you entered for the Proficy Authentication, during the iFIX installation. |
| **CLIENT SECRET** | Client secret of the Proficy authentication server. This is the client secret that you entered for the Proficy Authentication, during the iFIX installation. |

10. Click **Register**.

    The **Proficy Authentication Client Configuration** dialog box appears with a success message. You can use the security configuration utility in Proficy Authentication and create new users. For more information, refer to the section "Create Users in Proficy Authentication" on page 74.

11. Click **OK**.

    The **Proficy Authentication Client** dialog box is closed leaving the **Security Configuration** window open.

12. To save the configuration, in the **Security Configuration** window, click **File**, and then click **Save**.

    The configuration is saved successfully. Now you can close the **Security Configuration** window.

    By default, ch_admin user is created with the password same as Proficy Authentication secret. As the next step, you must assign the Group membership to the user. For more information, refer to the section "Assign iFIX Groups to the Newly Created User" on page 76.

## Logging into iFIX Manually using Proficy Authentication

**Before you begin**: Ensure that you enable Security to log in using Proficy Authentication.

1. In Classic view, in the iFIX WorkSpace, in the Application toolbar, click the Login button.
   -Or-
   In Ribbon view, on the Applications tab, in the System & Security group, click Security, and then click Security Login.
2. Select the **Proficy Authentication Logi**n check box.
3. Click **Login**.
4. The **Proficy Authentication** dialog box appears.
5. Enter the default user name that was created during iFIX registration with Proficy Authentication and the password same as the Proficy Authentication secret.
6. Click **SIGN IN**.
7. The **iFIX WorkSpace** opens.

## Trust an Untrusted Certificate while Registering iFIX to Proficy Authentication Server

While you register iFIX with the Proficy Authentication server, if iFIX could not find the Proficy Aauthentication server's root certificate in the local computer's trusted certificate folder, you can manually trust the certificate.

To manually trust the certificate:

1. In the **Configure Proficy Authentication** window, click the **Not trusted** link.
   The **Certificate Details** dialog box appears displaying the details of the certificate.
2. If you want to add the certificate to the trusted folder, click **Trust**.
   The certificate is added to the local computer's trusted certificate folder. You can now proceed with the iFIX registration with the Proficy Authentication server. For more information, refer to the section "Registering iFIX with Proficy Authentication Server" on page 66.
3. If you do not trust the certificate, click **Don't Trust**.
4. If the certificate details cannot be retrieved due to network issue, you can click the **Browse** button and manually locate the certificate in your local machine, and then Trust the certificate.

## Trust an Untrusted Certificate while Registering iFIX with Configuration Hub and Proficy Authentication server

While you register iFIX with Configuration Hub and Proficy Authentication server and also register (Configuration Hub with Proficy Authentication server in the background), if iFIX could not find Configuration Hub's or Proficy Authentication server's root certificate in the local computer's trusted certificate folder, you must manually trust the certificate.

To manually trust the certificate:

1. In the **Configuration Hub Server Registration** page, if you want to trust the certificate, click the **Not trusted** link.
   The **Certificate Details** dialog box appears displaying the details of the certificate.
2. If you want to add the certificate to the trusted folder, click **Trust**.
   The certificate is added to the local computer's trusted certificate folder. You can now proceed with the registration of iFIX with Configuration Hub and Proficy Authentication server and also register (Configuration Hub with Proficy Authentication server in the background). For more information, refer to the section Registering iFIX with Configuration Hub, Proficy Authentication (for SCADA nodes).
3. If you do not trust the certificate, click **Don't Trust**.
4. If the certificate details cannot be retrieved due to network issue, you can click the **Browse** button and manually locate the certificate in your local machine, and then Trust the certificate.

## Creating a Group Account to Proficy Authentication

By default, all iFIX security groups are added to Proficy Authentication at the time of registration. As per your requirement, you can modify the permissions. Whenever you register iFIX with Proficy Authentication, those groups along with the configured permissions are added to the Proficy Authentication server.

**NOTES**:

The following groups **IFIX_PROFICY_AUTH_ADMIN** and **APPLICATION_DESIGNER** are not available by default in IFIX if you have upgraded from iFIX 6.1 or 6.5 . You must manually create those groups with all the iFIX application features as needed.

Once you delete a group in iFIX, Proficy Authentication will not recognize that the group is deleted in iFIX. So the Proficy Authentication users in that group will not have the permission to log in to iFIX.

To create a new group and add to Proficy authentication, perform the following:

1. In Classic view, the iFIX WorkSpace, click the **Security Configuration** button on the toolbar.
   -Or-
   In Ribbon view, on the **Applications** tab, in the **System & Security** group, click **Security**, and then click **Security Configuration Utility**.
2. Click the **Group Account** button on the **Security** toolbox.
3. Click **Add**.
4. In the **Group Name** field, enter a name for the group account that you want to create.

   **NOTE**: Ensure that there is no empty space in between the group name. For example, "iFIX Group1" is not accepted, instead, it can be "iFIX_Group1".
5. Add security areas.
6. Add application features.
   For more information on the application features and the security groups, refer to the section Built-in Application Features and Security Groups in Proficy Authentication.
7. Click **OK** to save the group account in memory.
8. In the **Group Accounts** dialog box, in the **Add to Proficy Auth** group, select the following:

| Field | Description |
|---|---|
| **Shared prefix** | The name of the group that you created is added to the Proficy authentication server with **scada.ifix_shared** in the prefix. For example, if you created a group called **iFIX_Group1** in iFIX, the group is added as **scada.ifix_shared.iFIX_Group1**. The Shared Prefix essentially saves you from having to add the same groups from each iFIX node in the system; you only need to add it once to Proficy Authentication. |
| **Node Name prefix** | The name of the group that you created is added to the Proficy authentication server with **<scada>.nodename** in the prefix. For example, if the node name is **FIX**, and the group name you created in iFIX is **iFIX_Group1**, the group is added as **scada.FIX.iFIX_Group1**. The Node Name Prefix enables you to use the same group |

names across different nodes but with different privileges.

9. Click **Add Groups**.
   The selection is added to the Proficy authentication.
10. Click **OK** again to close the Group Accounts dialog box.
11. On the File menu, click **Save**.

## Built in iFIX Groups that Appear in Proficy Authentication

By default, built in iFIX security groups are added to Proficy Authentication. The following table describes these groups in iFIX and in Proficy Authentication, and the associated iFIX application features that are associated with each group.

**NOTE**:Once you delete a group in iFIX, Proficy Authentication will not recognize that the group is deleted in iFIX. So the Proficy Authentication users in that group will not have the permission to use the associated iFIX application features.

| Proficy Authentication Group | iFIX Security Group | Description | iFIX Application Features |
|---|---|---|---|
| scada.ifix_shared_IFIX_PROFICY_AUTH_ADMIN | IFIX_PROFICY_AUTH_ADMIN | This group allows access to all iFIX application features. So, any Proficy Authentication user who is a member of this group will have privileges similar to a native iFIX ADMIN user (except the access to security areas).<br><br>Proficy Authentication users who want to directly log in to iFIX can use this group.<br><br>**NOTE:** This group is not available by default when you upgrade from | • All |

| Proficy Authentication Group | iFIX Security Group | Description | iFIX Application Features |
|---|---|---|---|
| | | iFIX 6.1 or 6.5. You must manually create this group with all the iFIX application features as needed. For more information on how to create groups, refer to the section "Creating a Group Account to Proficy Authentication" on page 69. | |
| scada.ifix.shared.APPLICATION_DESIGNER | APPLICATION_DESIGNER | This group allows a user to access Configuration Hub and provides use of iFIX features such as iFIX connection, database, and model management. It does not include support for the new features introduced in Configuration Hub 2022 (for the SCU and iFIX Security Configuration).<br>**NOTE:** This group is not available by default when you upgrade from iFIX 6.1 or 6.5. You must manually create the group with all the iFIX application features as | • Database Block Add-Delete<br>• Database Manager<br>• Database Reload<br>• Database Save<br>• Enable Task Switching<br>• OPC UA Confiugration Tool<br>• Runtime Visual Basic Editor Access<br>• WorkSpace Configure<br>• WorkSpace Runtime<br>• WorkSpace Runtime Exit |

| Proficy Authentication Group | iFIX Security Group | Description | iFIX Application Features |
| --- | --- | --- | --- |
| | | needed. If upgrading from iFIX 2022, this group does appear but does not have the Security Configuration or System Configuration features included for the new project management and deployment features.<br><br>**IMPORTANT:** If you want to create a new iFIX security group that has support for the all the new features, at a minimum, you need to include the following features:<br>• Security Configuration<br>• System Configuration<br>• Database Block Add-Delete<br>• Database Manager<br>• Database Reload<br>• Database Save<br><br>For information on how to create groups in Proficy Authentication | |

| Proficy Authentication Group | iFIX Security Group | Description | iFIX Application Features |
|---|---|---|---|
| | | see: "Creating a Group Account to Proficy Authentication" on page 69. | |
| scada.i-fix.shared.OPERATORS | OPERATORS | This group provides run mode only access for a user in iFIX. | • Fix32 - Alarm Summary Display<br>• Fix32 - Historical Trend Display<br>• WorkSpace Runtime |
| scada.i-fix.shared.SUPERVISORS | SUPERVISO-RS | This group provides access to WorkSpace run and configure mode, as well as access to background task exit, iFIX system shut down, and iFIX system user login. | • Background Task Exit<br>• Fix32 - Alarm Summary Display<br>• Fix32 - Historical Trend Display<br>• Fix32 - Operating System Window<br>• Fix32 - Run a Task from View<br>• Historical Trend Assign<br>• iFIX - System Shutdown<br>• System User Login<br>• WorkSpace Configure<br>• WorkSpace Runtime |
| scada.project.admin | N/A | This group allows the Proficy Authentication user access to the Projects panel and to the Deploy operations from Configuration Hub. | N/A |

## Create Users in Proficy Authentication

By default ch_admin user is created after you register iFIX to Proficy Authentication or to Configuration Hub. For the first time, you can log in to Configuration hub using ch_admin and the password same as

Proficy authentication secret. After you log in to Configuration Hub, as an administrator, you can create new users based on your requirement using the Security configuration utility.

**NOTE:** The Proficy Authentication user gets only the permissions based on the iFIX group that is assigned to the user.

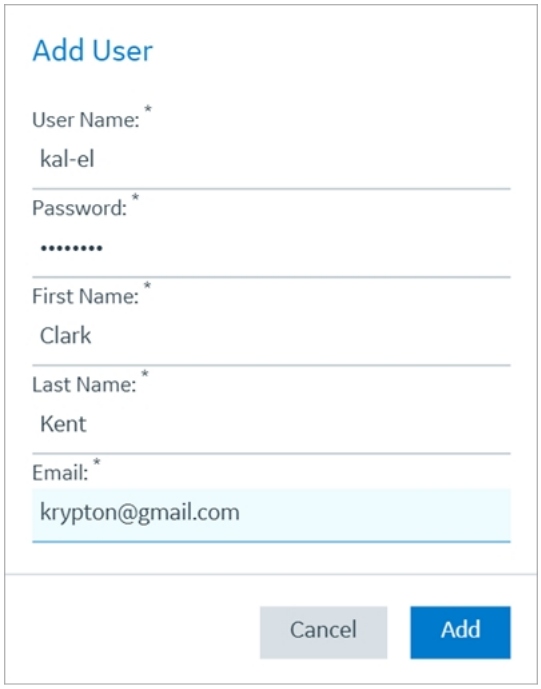
To create a new user, perform the following:

1. Open the iFIX application.
2. Log in to iFIX. For information on how to log in, refer to the section "Logging in to iFIX Manually" on page 37.
3. In Ribbon view, on the **Applications** tab, in the **Configuration Hub** group, click 

.
The **Configuration Hub** login page opens.
4. Log in to Configuration Hub with the user credentials that were created while you registered iFIX with Configuration Hub and Proficy authentication server .
5. Go to **Security-UAA** > **Users**.
The existing list of Proficy Authentication user accounts appear.
6. Select **+**.
The **Add User** screen appears.
7. Enter the following details for the new user account.

| Field | Description |
|---|---|
| **User Name** | The user name to log in to Proficy Authentication. |
| **Password** | The password to log in to Proficy Authentication. |
| **First Name** | User's first name. |
| **Last Name** | User's last name. |
| **Email** | User's email address. |

8. Select **Add**.




The user is created and added to the list of user accounts on the Users tab. The new user account is also associated to default Proficy Authentication groups, which cannot be deleted or modified.

Every user/client must possess the following three scopes to access the Security plugin via. Configuration Hub. If these scopes are not added, then a warning message alerts the user to contact Admin.

| Scope | Description |
|---|---|
| `uaa.admin` | This scope indicates that this is a superuser. |
| `clients.write` | This scope resets the Security plugin's admin client secret. |
| `password.write` | This admin scope enables to change the user password.<br>**NOTE**: This scope is assigned to all the UAA/LDAP/SAML users by default without the need to assign manually. |

9. Once you create a new user, you must manually assign the iFIX related group membership to the newly created user. For more information, refer to the section "Assign iFIX Groups to the Newly Created User" below.

## Assign iFIX Groups to the Newly Created User

By default, ch_admin user is created after you register iFIX to Proficy Authentication or to Configuration Hub. For the first time, you can log in to Configuration Hub using ch_admin and the password same as

Proficy authentication secret. After you log in to Configuration Hub, as an administrator, you can create new users based on your requirement using the Security configuration utility. For more information, refer to the section "Create Users in Proficy Authentication" on page 74. However, to log in to iFIX using Proficy Authentication, you must assign iFIX related group memberships to the ch_admin user or the user that you create.

To assign a group to a user, perform the following:

1. Log in to Configuration Hub with the user credentials.
   **NOTE:** If you are logging in for the first time, use ch_admin and the password same as Proficy Authentication secret.
2. Go to **Security-UAA** > **Users**.
   The existing list of Proficy Authentication user accounts appear.
3. Select the user as needed.
4. On the right side pane, next to **Group Membership**, select  .
   The Group Membership dialog box appears listing all the available groups.

   **NOTE:** The default iFIX related groups will be listed only after you register iFIX to Proficy Authentication and Configuration Hub.
5. Select the iFIX related groups as needed.
   The users will get the permission based on the group application features assigned in iFIX.

   **NOTE:** If you did not create any specific iFIX groups, you can select the following group memberships, as they will have all the required permissions to use iFIX in Configuration Hub: **scada.ifix_shared.IFIX_PROFICY_AUTH_ADMIN** and **scada.project.admin**.
6. Select **Apply**.
   The selected group membership is assigned to the user. You can now log out and log in to Configuration Hub and then log in to iFIX using Proficy Authentication.

# Troubleshooting

The following table explains how to address common problems that can arise when using security.

**Handling Common Security Problems**

| If you... | You must... |
|---|---|
| Lock yourself out of iFIX. | Log in with an administrative user account and create for yourself a new user account. The initial login name for such an account is ADMIN and the initial password is ADMIN. |
| Forget your password. | Log in with an administrative user account and enter a new password for your user account. The initial login name for such an account is ADMIN and the initial password is ADMIN. |
| Do not want security to automatically logoff operators. | Enter **00:00:00** as the time-out interval for your user accounts. |

| | |
|---|---|
| Want to login into iFIX from a picture. | 1. Add a push button to your picture.<br>2. Name the button Login.<br>3. Write a script to call the *LogIn* subroutine.<br>For more information, refer to the iFIX Automation Interfaces Help file. |
| Want to protect the Alt+F4 keystroke. | Start the Security Configuration program, click the Configuration button from the Security toolbox, and click Enabled from the Configuration dialog box. |
| Want to access the Security Configuration program without starting the SCU. | Start the iFIX WorkSpace and click the Security Configuration button from the Application toolbar (Classic view) or on the Applications tab, in the System & Security group, click Security and then click Security Configuration Utility (Ribbon view). |

## Understanding Security Configuration Messages

If you see a message that you do not understand when running the Security Configuration program, refer to the following table for a possible explanation and response. Be sure to click OK to acknowledge the message before taking the recommended action.

**Security Configuration Messages**

| When you see the message... | Then... |
|---|---|
| Application user not found. Reenter. | You entered a full name in the Application User field that security could not find. Click the browse (...) button and select a name from the list of user accounts that appears. If no user account appears with the name you want, create the account first. |
| CAUTION: Backup security path currently in use. | You attempted to change the security configuration of your computer while the security path is unavailable. While you can reconfigure the security system now, you will need to repeat this task when the security path becomes available. |
| Configuration has changed. Save new changes? | You selected Exit from the File menu without saving your changes. Click Yes to save the changes or click No to quit without saving your changes. To continue using the Security Configuration program, click Cancel. |
| Copy existing configuration to new path? | You redefined the security path. Click Yes to move the user and group accounts to the new path, click No to leave the files in the current location, or click Cancel to return to the Security Configuration program. |
| Delete existing security configuration? | You selected Clear from the File menu. Click Yes to delete all user and group accounts. Click No to cancel. |
| Disable security or give a user access to this program before exiting. | You have enabled security without creating any user accounts that can access the Security Configuration program. Create at least one user account that can access the program before you exit. |
| Failure exporting security | The Security Configuration program could not export its current settings. Verify that you have enough free hard disk space. If you do not, back up any unnecessary files, delete |

| | |
|---|---|
| configuration. | them, and try exporting the security configuration again. |
| Failure reading security configuration. | The Security Configuration program could not import the file you specified. Verify the file is not damaged or stored in bad sectors of your hard disk. |
| Failure writing security files. Check disk space. | The Security Configuration program could not save its current settings. Verify that you have enough free hard disk space. If you do not, back up any unnecessary files, delete them, and try saving the security configuration again. |
| Full name must be alphanumeric. | You entered non-alphanumeric characters (such as punctuation marks) in the full name of a user account. Retype the name including only alphanumeric characters. |
| Group name needed to save a group. | You attempted to create a group account without naming it. Enter a name of up to 20 alphanumeric characters in the Group Name field and click OK to create the account. |
| Invalid path specified. | You specified a path in the Backup Path field that does not exist. Either create the directory or specify a path that exists. |
| Invalid timeout value entered! | Either you specified a non-numeric value for the Login Timeout field, or you entered a numeric value in a format the Security Configuration program does not recognize. Type a numeric value in the field using the format: *hh:mm:ss.* |
| Login name must be alphanumeric. | You entered non-alphanumeric characters (such as punctuation marks) in the login name of a user account. Retype the login name in this field including only alphanumeric characters. |
| New path has no security files. Copy files or CANCEL change. | You clicked No when the Security Configuration program prompted you to copy the user and group accounts. Because no account files already exist in the specified security path, you must click Yes or Cancel instead. |
| Ok to DELETE this group? | The Security Configuration program is about to delete the selected group account. Click Yes to delete the account or click No to keep it. |
| Ok to DELETE this user? | The Security Configuration program is about to delete the selected user account. Click Yes to delete the account or click No to keep it. |
| Ok to lose current changes? | You clicked Cancel on a dialog box. Click Yes to abort the changes you have made or click No to continue making changes. |
| Old configuration not found! | The Security Configuration program could not find the back-up of the previous security configuration and saved the current one instead. This can occur when the files have been renamed or deleted. The backup path may have also been changed. |
| Overwrite existing export file? | The name of the file you entered already exists. Click Yes to overwrite the file, click No to enter a new file name, or click Cancel to abort the process. |
| Password confirmation failed. Save Aborted. | The password you typed does not match the one you entered for the current user account. Click OK and retype the password when prompted. |
| Replace or add to existing con- | The Security Configuration program is about to import a security configuration. Click Replace to overwrite all the existing group accounts, user accounts, and the security areas with the information in the import file. Click Add to append the new accounts to |

| | |
|---|---|
| figuration? | your existing ones. |
| Save failed! | The Security Configuration program could not save its current settings. Verify that you have enough free hard disk space. If you do not, back up any unnecessary files, delete them, and try saving the security configuration again. |
| Security configuration corrupted. | The Security Configuration program cannot find the security files in the specified security path. Contact GE Support for more information. |
| Security Files must be manually copied from <*old_path*>. | The security path you specified does not exist. Consequently, the Security Configuration program cannot copy the user and group accounts to the specified path. You must copy the files to this path once it becomes available. If you do not, the Security Configuration program assumes someone has tampered with security and will not allow you to restart the program. |
| Security path invalid or unavailable. Continue? | iFIX could not find the security path you specified. Verify it exists and try again. If the path points to a file server, make sure the server is functioning properly. |
| Should default user and group accounts be created. | You have selected Clear to delete all user and group accounts. To prevent you from accidentally locking yourself out the program, the Security Configuration program allows you to create sample user and group accounts. To create these accounts, click Yes. To skip creating these accounts, click No. |
| System user not found. Reenter. | You entered a full name in the System User field that security could not find. Click the browse (...) button and select a name from the list of user accounts that appears. If no user account appears with the name you want, create the account first. |
| Unauthorized access to Security Configurator. | You attempted to start the Security Configuration program but your user account does not provide access to the program or you are not logged in. Log into iFIX, if necessary, and try again. If you are using Windows security, verify that you entered the password exactly as defined. If the problem persists, verify that the Windows user account you are using exists and is configured as described in the section Using the Security Configuration Program. |
| Unique login and full names required for each user. | You entered a login name or full name already in use by another user account. Enter a login name or full name not in use by any other account and click OK. |
| Warning: imported user accounts may not have passwords! Continue? | The Security Configuration program is about to import a security configuration file. Click Yes to continue importing the file or click No to abort the procedure. To import a file with passwords, edit it with a text editor and type the text PASSWORD**:***password* on the line immediately following the login name. Refer to the section Importing User Account Passwords for an example of editing an import file. |

## Understanding Security Synchronizer Messages

You may encounter the errors listed in this section in the iFIX alarm destinations or the iFIX security log file while Security Synchronizer is running. Error codes can range from 0, indicating that no errors have been detected, to 299.

The error code associated with a specific error is written to the analog error tag, if a valid tag is specified with the /E parameter. If more than one error occurs during the security synchronization process, then the most severe error code is written to the analog tag. If more than one error of the same severity is encountered, then the last error generated of that severity is written to the analog tag.

If an error is encountered while the security synchronization is processing, then the digital error tag is set to 1.

Error messages that contain user names display the Windows user name in the message. Refer to the following sections for more information about error messages:

- Error Severity Categories
- Application Error Codes (200-299)
- User Account Error Codes (100-199)
- General Error Codes (1-99)
- Command Line Parameter Errors

## Error Severity Categories

Errors are categorized into three levels of severity, listed here from highest to lowest:

**Application Errors** – Security Synchronizer terminates without performing or completing synchronization. Error codes range from 200-299.

**User Account Errors** – Errors are encountered for individual user accounts, but the synchronization process completes. Error codes range from 100-199.

**General Errors** – Errors such as the inability to write to iFIX database tags are detected, but the synchronization process completes. Error codes range from 1-99.

You may encounter a fourth type of error caused when an invalid command line parameter is passed to the Security Synchronizer. This type of error does not cause values to be written to the iFIX database, but it does cause messages to be written to the security log file and the iFIX alarm destinations.

You can configure error conditions to be reported in the Alarm Summary or other alarm destinations through the use of iFIX database tags. If the /E parameter is used to specify an analog error tag, you can configure that tag to alarm on the error value. For example, you can configure an Analog Input block that receives the error value to generate a HI alarm when the error value exceeds 99 or a HIHI alarm when the error value exceeds 199.

## Application Error Codes (200-299)

The following table lists the application error codes. These errors cause the Security Synchronizer process to terminate without performing or completing synchronization. These errors have the highest severity.

**Application Error Codes**

| Err-Error Message or Code | |
|---|---|
| 201 | Security Synchronizer: Unable to perform security synchronization. FIX system is not running |
| 202 | Security Synchronizer: User has insufficient FIX privileges to run Security Synchronizer. |
| 203 | Security Synchronizer: Attempt to execute synchronization while already running. Second attempt aborted. |
| 204 | Security Synchronizer: Function is not enabled on this node; check license/key. |
| 205 | Security Synchronizer: Security Configurator is running. Synchronization aborted. |
| 210 | Security Synchronizer: Insufficient memory to complete synchronization process. Synchronization aborted. |
| 220 | Security Synchronizer: Source of Windows security not specified (Domain, Local). Synchronization aborted. |
| 230 | Security Synchronizer: Unable to retrieve security info from Windows Domain. Synchronization aborted. |
| 240 | Security Synchronizer: Unable to retrieve Windows security information from local PC. Synchronization aborted. |
| 250 | Security Synchronizer: No group names found in Windows that map to FIX privileges. Synchronization aborted. |
| 251 | Security Synchronizer: No Windows users belong to groups which map to FIX privileges. Synchronization aborted. |
| 270 | Security Synchronizer: Unable to retrieve FIX security data. Synchronization aborted. |
| 271 | Security Synchronizer: Unable to retrieve FIX security Area data. Synchronization aborted. |
| 272 | Security Synchronizer: Unable to retrieve FIX Application Feature data. Synchronization aborted. |
| 273 | Security Synchronizer: Unable to retrieve FIX Security Group data. Synchronization aborted. |
| 280 | Security Synchronizer: Security paths unavailable or security has been tampered with. Synchronization aborted. |

## User Account Error Codes (100-199)

The following table lists the user account error codes. These errors are encountered for individual user accounts, but the synchronization process continues. These errors have medium severity. The %s character used in the following list of user account error message is replaced by the appropriate string for each instance of the message:

**User Account Error Codes**

| Err-Error Message or Code | |
|---|---|
| 101 | Security Synchronizer: Can't create account for %s. Name already exists. |

102 Security Synchronizer: Can't create account for %s. Invalid characters in name.
110 Security Synchronizer: Can't save changes to user %s. Error writing to file.
120 Security Synchronizer: Can't add FIX group %s to user %s (>12).
130 Security Synchronizer: Can't delete FIX user %s. Last user with access to Security Config.
131 Security Synchronizer: Can't remove security configuration rights from user %s.
140 Security Synchronizer: Can't remove user %. User no longer exists in FIX security.
141 Security Synchronizer: Can't delete user %s. Error occurred writing to disk.
150 Security Synchronizer: Error sorting FIX security users. Use FIX Security Configuration program to save configuration.
160 Security Synchronizer: Unable to restore security data due to disk problems. Security may be corrupted.
161 Security Synchronizer: Unable to backup security data due to disk problems. No FIX users were deleted.
162 Security Synchronizer: Unable to save security data due to disk problems. No FIX users were deleted.

## General Error Codes (1-99)

The following table lists the General Error codes. These errors have the lowest severity.

**General Error Codes**

| Error Code | Error Message |
|---|---|
| 20 | Security Synchronizer: Can't write to Analog Error tag %s in FIX database. |
| 21 | Security Synchronizer: Can't write to Digital Error tag %s in FIX database. |
| 22 | Security Synchronizer: Can't write to Completion tag %s in FIX database. |
| 30 | Security Synchronizer: Security Area name %s does not exist in FIX security. |
| 31 | Security Synchronizer: application feature name %s does not exist in FIX security. |
| 32 | Security Synchronizer: Security Group name %s does not exist in FIX security. |

## Command Line Parameter Errors

Values are not associated with command line parameter errors since values are not written to the iFIX database when these errors occur. These errors terminate the synchronization process before it actually begins. These errors are detected only when the SecuritySynchronizer.exe program is running, and not when programming to the Security Synchronizer Automation interface. Refer to the iFIX Automation Interfaces Help file for more information on the Automation interface.

You may encounter one of these command line errors while running Security Synchronizer:

- Security Synchronizer: Invalid Windows Domain name. Synchronization aborted.
- Security Synchronizer: Invalid Login Timeout value. Value must be between 0 and 86399 seconds. Synchronization aborted.
- Security Synchronizer: Invalid MapMode value. Synchronization aborted. FOR FUTURE USE.
- Security Synchronizer: Invalid Analog Error Tag syntax (/E). Synchronization aborted.
- Security Synchronizer: Invalid Failure Tag syntax (/F). Synchronization aborted.
- Security Synchronizer: Invalid Completion Tag syntax (/C). Synchronization aborted.

# Security Configuration Dialog Boxes

The Security Configuration application includes the following dialog boxes (listed in alphabetical order):



## Application Feature Selection Dialog Box

The Application Feature Selection dialog box displays the following items:

### Authorized

Displays the account privileges accessible to this account.

### Available

Displays the account privileges you can assign to the current account.

### Add All

Adds all available account privileges to the Authorized list box.

### Add

Adds the selected account privilege to the Authorized list box.

### Delete

Removes the selected account privilege from the Authorized list box.

### Delete All

Removes all available account privileges from the Authorized list box.

## Automatic Login at Startup Dialog Box

The Automatic Login at Startup dialog box displays the following items:

### Auto Started Nodes

Alphabetically lists the nodes that have been configured for automatic login and lets you select the node you want to edit or delete.

### Add

Lets you create an automatic login file for a node.

### Modify

Lets you modify an existing automatic login file for the selected node.

### Delete

Removes the selected node's automatic login file.

## Automatic Login Node Dialog Box

The Automatic Login Node dialog box displays the following items:

### Node

Displays the name of the node that automatically logs in the specified application user when iFIX starts. To change the node name, enter the name of a new node.

### Application User

Displays the user account that iFIX automatically logs in as the application user. To change the name, enter it, or click the browse (...) button to select a name from the Select User dialog box.

### System User

Displays the account that is automatically logged in as the system user the next time iFIX is started.

For more information, refer to the *Configure iFIX Security* topic in the *Configuring Security Features* guide in the iFIX electronic books (Dynamics.chm).

**NOTE:** Only the Security Synchronizer recognizes the System User. Other iFIX features and programs do not recognize the system user; therefore, this user cannot be used to provide access to any security privilege other than running the Security Synchronizer.

## Configuration Dialog Box

The Configuration dialog box displays the following items:

### User Based Security

Controls whether security is enabled. By default, security is disabled.

### Security Path

Defines the path to your security files. By default, iFIX sets the security path to the Local path.

**NOTE:** If you define a file server directory as your security path, you also need to define a backup path. The backup path allows operators to log into iFIX while the file server is unavailable. The backup path and should be a local drive.

### Backup Path

Defines a second path to your security files. By default, iFIX sets the backup path to the local path.

**NOTE:** If you have defined a file server as your security path, you need to define a backup path.

### Use These Paths for All Startup Profiles

Enables or disables a global security path.

**NOTE:** If you disable global security paths and you are using Terminal Services, you must configure security individually for each iFIX user.

## Edit Security Area Dialog Box

The Edit Security Area dialog box displays the following items:

### Area

Displays the number of the area you chose to edit.

### Name

Allows you to create or rename the selected security area. The name you specify can be up to 20 alpha-numeric characters.

## Group Accounts Dialog Box

The Group Accounts dialog box displays the following items:

### Current Groups

Displays the existing group accounts and lets you select the account you want to modify or delete.

### Add

Lets you add a new group account.

### Modify

Lets you modify the selected group account.

### Delete

Lets you remove the selected group account.

### Add to Proficy Auth

Group box that lets you to add the name of the group with a prefix in the Proficy Authentication Server. After a user is added to Proficy Authentication, privileges are granted through group associations in the Proficy Authentication tool. Groups that are part of iFIX security can be added to Proficy Authentication using this dialog box.

**Shared Prefix**

Lets you to add **scada.ifix_shared** in the prefix of the name of the group that you created. For example, if you created a group called **iFIX_Group1** in iFIX, the group is added as **scada.ifix_shared.iFIX_Group1**. The Shared Prefix essentially saves you from having to add the same groups from each iFIX node in the system; you only need to add it once to Proficy Authentication.

**Node Name Prefix**

Lets you to add **<scada>.nodename** in the prefix of the name of the group that you created. For example, if the node name is **FIX**, and the group name you created in iFIX is **iFIX_Group1**, the group is added as **scada.FIX.iFIX_Group1**. The Node Name Prefix enables you to use the same group names across different nodes but with different privileges.

**Add Groups**

Lets you to add the created group along with the preferred prefix to the Proficy Authentication server.

## Group Membership Selection Dialog Box

The Group Membership dialog box displays the following items:

### Authorized

Displays the account privileges accessible to this account.

### Available

Displays the account privileges you can assign to the current account.

### Add All

Adds all available account privileges to the Authorized list box.

### Add

Adds the selected account privilege to the Authorized list box.

### Delete

Removes the selected account privilege from the Authorized list box.

### Delete All

Removes all available account privileges from the Authorized list box.

## Group Profile Dialog Box

The Group Profile dialog box displays the following items:

### Group Name

Displays the name of the group account you are defining. You add or modify the text by typing a name, up to 30 alphanumeric characters in length.

### Security Areas

Displays the security areas accessible to this account.

### Application Features

Displays the iFIX application features accessible to this account.

### Modify

Lets you add and delete the current account's security areas or application features.

**NOTE:** If you are creating or editing a user account, the Modify button also lets you add and delete the group accounts.

## Password Confirmation Dialog Box

The Password Confirmation dialog box displays the following item:

### Retype Password to Confirm Change

Lets you retype a user account password when you disable Windows security for the user account, and you create or modify the password. After typing the password, select OK to return to the User Profile dialog box.

**NOTE:** The password is not displayed in this dialog box. When you retype a password, the dialog box displays an asterisk (*) for every character you specify.

## Security Area Naming Dialog Box

The Security Area Naming dialog box displays the following items:

### Security Areas

Lists the names of each security area. You can name up to 254 areas.

### Modify

Allows you to create or rename the selected security area.

### Tag Security Areas

Determines how security areas assigned to a tag are evaluated when a user writes to a tag or acknowledges a tag's alarm.

- **Require At Least One (OR)** - Users require access to at least one specified security area.
- **Require All (AND)** - Users require access to all specified security areas.

**NOTE**: It may take up to one minute for this setting to take effect after being saved in the Security Configuration or published from Configuration Hub. During this time, unauthorized users may be able to write to a tag to which they should not be able, or vice versa. For this setting to take effect as quickly as possible, SCADA(s) using that Security Path (as in the case of shared security files) must be re-started to ensure they have the latest value for that setting.

## Security Area Selection Dialog Box

The Security Area Selection dialog box displays the following items:

### Authorized

Displays the account privileges accessible to this account.

### Available

Displays the account privileges you can assign to the current account.

### Add All

Adds all available account privileges to the Authorized list box.

### Add

Adds the selected account privilege to the Authorized list box.

### Delete

Removes the selected account privilege from the Authorized list box.

### Delete All

Removes all available account privileges from the Authorized list box.

## Select User Dialog Box

The Select User dialog box displays the following item:

### Select User List Box

Allows you to choose the user account that iFIX automatically logs in as an application user.

## User Accounts Dialog Box

The User Accounts dialog box displays the following items:

### Current Users

Displays the existing user accounts and lets you select the account you want to modify or delete.

### Add

Lets you add a new user account.

### Modify

Lets you modify the selected user account.

### Delete

Lets you remove the selected user account.

## User Profile Dialog Box

The User Profile dialog box displays the following items:

### Use Windows Security

Enables or disables Windows security for this account. By default, Windows security is disabled and iFIX security validates each operator's login name and password during login. When you enable Windows security, Windows authenticates each login name and password, allowing you to take advantage of features such as case-sensitive passwords and passwords that expire after a number of days.

### Windows Security Enabled

When the Use Windows Security check box is selected, the following items display:

| Item | Description |
|---|---|
| User Name | Displays the full name of the operator whose account you are defining. You can change the text by typing a new name, up to 30 alphanumeric characters in length.<br><br>**NOTE:** The name you enter must be unique. |
| Domain | Displays the account domain name when Windows security is enabled. The domain name can be up to 20 alphanumeric characters.<br><br>**NOTE:** Be aware that when configuring your Windows users in iFIX Security, the Domain Name entry needs to be your domain's NetBIOS name. |
| Login Timeout | Controls the length of time operators can remain logged in. You can enter any time interval from 00:00:01 to 23:59:59. A value of 00:00:00 disables this field. When an operator attempts to access a restricted application feature or security area after the time interval expires, iFIX logs out the operator, requiring him or her to log in again. This feature prevents operators from remaining logged in indefinitely.<br><br>**CAUTION:** This feature does not eliminate the need for operators to manually log out, particularly if you have strict security requirements. If you decide to use this feature, consider it a safety mechanism. |

### Windows Security Disabled

When the Use Windows Security check box is cleared, the following items display:

| Item | Description |
|---|---|

| | |
|---|---|
| Full Name | Displays the full name of the operator whose account you are defining. You can change the text by typing a new name, up to 20 alphanumeric characters in length.<br><br>**NOTE:** The name you enter must be unique. |
| Password | Displays the account password when Windows security is disabled. Entering a password is optional. Each password can be up to 20 alphanumeric characters.<br><br>**NOTE:** The password is not displayed in this field for security reasons. When you create or modify a password, the field displays an asterisk (*) for every character you specify. iFIX user passwords are case insensitive when not using Windows security |
| Login Name | Contains the login name of the operator. You can change the text by entering a new name, up to six alphanumeric characters in length. The operator enters this name when logging in. If you enable Windows security for this account, the login name must match the login name of the operator's Windows user account.<br><br>**NOTE:** The login name you enter must be unique. |
| Login Timeout | Controls the length of time operators can remain logged in. You can enter any time interval from 00:00:01 to 23:59:59. A value of 00:00:00 disables this field. When an operator attempts to access a restricted application feature or security area after the time interval expires, iFIX logs out the operator, requiring him or her to log in again. This feature prevents operators from remaining logged in indefinitely.<br><br>**CAUTION:** This feature does not eliminate the need for operators to manually log out, particularly if you have strict security requirements. If you decide to use this feature, consider it a safety mechanism. |

### Group

Displays the group accounts accessible to the current user account.

### Security

Displays the security areas accessible to this account.

### Application

Displays the iFIX application features accessible to this account.

### Modify

Allows you to modify the group accounts, security areas, or application features listed for this user.

## How Do I...

For more information on the Security Configuration application, click any of the links below:

- Configuring Security Features
- Managing User Accounts
- Managing Group Accounts
- Configuring Security
- Using Electronic Signatures
- Configuring for Automatic Login
- Creating or Renaming Security Areas
- Creating Windows Groups Using the CreateWindowsGroups Dialog Box
- Enabling Environment Protection

## Configuring Security Features

**To implement security in the Security Configuration application:**

1. Create or rename your security areas.
2. Create group and user accounts.
3. If you plan to automatically log operators into iFIX, define each automatic login file.
4. Copy the security files to all of your nodes. If you are using a file server, copy the security files to the file server.
5. Specify a local security and backup path on each node. If you are using a file server, enter the path to the file server as the security path and enter a local path as the backup path.
6. Enable security on all nodes and save the security configuration.
7. If you want all iFIX user sessions to share the same security configuration, enable global security paths on each node. (This step is recommended for terminal server nodes.)
8. If you plan to enable environment protection, start the iFIX WorkSpace and set the run-time environment preferences you want to use on each iFIX node.

## Managing User Accounts

Click any of the following links for more information on managing user accounts:

- Creating a User Account
- Adding and Deleting Account Privileges
- Creating a Recipe User Account
- Deleting a User Account
- Deleting All Group and User Accounts

- Modifying a User Account
- Saving a User Account

## Creating a User Account

**To create a user account:**

1. In Classic view, the iFIX WorkSpace, click the Security Configuration button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click Security, and then click Security Configuration Utility.
2. On the Security toolbox, click the User Account button.
3. Click Add.
4. In the Full Name field, enter a name for the new user account.
5. Depending on the type of security you want to use, do one of the following:
   - If you want to use Windows security, select the Use Windows Security check box, and, in the Full Name and Domain fields, enter the login name and domain name of the Windows user account you want to use. Be aware that when configuring your Windows users in iFIX Security, the Domain Name entry needs to be your domain's NetBIOS name.
   - If you want to use iFIX security, enter the login name and password for the account in the Login Name and Password fields.
2. If you want to limit the time the operator remains logged into iFIX, in the Login Timeout field, enter a timeout value.
3. Add group accounts.
4. Add security areas.
5. Add application features.
6. Save the account.

## Selecting Account Privileges

Click any of the following links for more information on selecting account privileges:

- Adding and Deleting Security Areas in a User Account
- Adding and Deleting Application Features in a User Account
- Adding and Deleting Group Accounts in a User Account

### Adding and Deleting Security Areas in a User Account

**To add or delete security areas in a user account:**

1. In Classic view, the iFIX WorkSpace, click the Security Configuration button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click Security, and then click Security Configuration Utility.
2. From the Edit menu, select User Accounts.
3. Double-click the user account in which you want to add or delete security areas.
4. On the User Profile dialog box, click Modify from the Security Area list box.
5. To add security areas, double-click the ones you want to add from the Available list box. To add all the security areas to the current account, click Add All.
6. To remove security areas, double-click the ones you want to delete from the Authorized list box. To remove all the security areas from the current account, click Delete All.

### Adding and Deleting Application Features in a User Account

**To add or delete application features in a user account:**

1. In Classic view, the iFIX WorkSpace, click the Security Configuration button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click Security, and then click Security Configuration Utility.
2. From the Edit menu, select User Accounts.
3. Double-click the user account in which you want to add or delete application features.
4. On the User Profile dialog box, click Modify from the Application Features list box.
5. To add application features, double-click the ones you want to add from the Available list box. To add all the application features to the current account, click Add All.

   **NOTE:** Clicking Add All does not add the Electronic Signature – Bypass application feature. You must add this application feature explicitly.
6. To remove application features, double-click the ones you want to delete from the Authorized list box. To remove all the application features from the current account, click Delete All.

### Adding and Deleting Group Accounts in a User Account

**To add or delete group accounts in a user account:**

1. In Classic view, the iFIX WorkSpace, click the Security Configuration button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click Security, and then click Security Configuration Utility.

2. From the Edit menu, select User Accounts.
3. Double-click the user account in which you want to add or delete group accounts.
4. On the User Profile dialog box, click Modify from the Group Membership list box.
5. To add group accounts, double-click the ones you want to add from the Available list box. To add all the group accounts to the current user account, click Add All.
6. To remove group accounts, double-click the ones you want to delete from the Authorized list box. To remove all the group accounts from the current user account, click Delete All.

## Creating a Recipe User Account

**To create a Recipe user account:**

1. In Classic view, the iFIX WorkSpace, click the Security Configuration button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click Security, and then click Security Configuration Utility.
2. On the Security toolbox, click the User Accounts button.
3. Click Add.
4. Enter **RECIPE** in the Full Name and Login Name fields. Do not assign a password to this account.
5. Click Modify from the Security Area list box.
6. Double-click each security area you want to add from the Available list box. To add all the security areas to the current account, click Add All.
7. Click OK to save the user account in memory.
8. Click OK to close the User Accounts dialog box.
9. On the File menu, click Save.

## reating a Public Account

**To create a public account:**

1. In Classic view, the iFIX WorkSpace, click the Security Configuration button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click Security, and then click Security Configuration Utility.
2. On the Security toolbox, click the User Accounts button.
3. Click Add.
4. Enter **PUBLIC** in the Full Name field.

5. Enter **PUBLIC** in the Login Name field.
6. Click OK to save the user account in memory.
7. Click OK to close the User Accounts dialog box.
8. Click the Autologin button on the Security toolbox.
9. Click Add.
10. Enter the public account's node name in the Node field.
11. Enter **PUBLIC** in the Application User field.
12. On the File menu, click Save to save your security configuration.

## Deleting a User Account

**To delete a user account:**

1. In Classic view, the iFIX WorkSpace, click the Security Configuration button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click Security, and then click Security Configuration Utility.
2. On the Security toolbox, click the User Accounts button.
3. Select the user account you want to remove and click Delete. The following text appears:

   ```
   OK to delete this user?
   ```
4. Click Yes to delete the user account.
5. Click OK to close the User Accounts dialog box.
6. On the File menu, click Save to permanently remove the account.

## Deleting All Group and User Accounts

**To delete all of your accounts and disable security:**

1. In Classic view, the iFIX WorkSpace, click the Security Configuration button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click Security, and then click Security Configuration Utility.
2. On the File menu, click Clear. The following text appears:

   ```
   Delete existing security configuration?
   ```
3. Click Yes to delete all of your accounts. The following text appears:

   ```
   Should default user and group accounts be created?
   ```
4. Click Yes to create sample group and user accounts or click No to omit this step.

## Modifying a User Account

**To modify a user account:**

1. In Classic view, the iFIX WorkSpace, click the Security Configuration button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click Security, and then click Security Configuration Utility.
2. On the Security toolbox, click the User Accounts button.
3. Double-click the user account you want to modify.
4. Modify the following user account information as needed:
   - The account and login names.
   - The password (iFIX security only) or the domain name (Windows security only).
   - The login timeout value.
   - Any group accounts.
   - The security areas.
   - The application features.
5. Save the user account.

## Saving a User Account

**To save a user account:**

1. In Classic view, the iFIX WorkSpace, click the Security Configuration button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click Security, and then click Security Configuration Utility.
2. Create or modify a user account.
3. On the User Profile dialog box, click OK. If you disabled Windows security for the account, and entered or changed a password, the following text appears in the Password Confirmation dialog box:

   ```
   Retype password to confirm changes
   ```
4. Enter the password for this account in the field provided, and click OK. If the two passwords match, security saves the user account in memory. If the passwords do not match, the following message appears:

   ```
   Password confirmation failed. Save aborted.
   ```
5. Click OK to acknowledge the message and repeat steps 3 and 4.
6. Click OK to close the User Accounts dialog box.
7. On the File menu, click Save.

## Managing Group Accounts

Click any of the following links for more information on managing group accounts:

- Creating a Group Account
- Adding and Deleting Account Privileges
- Deleting a Group Account
- Deleting All Group and User Accounts
- Modifying a Group Account
- Creating Windows Groups Using the CreateWindowsGroups Dialog Box

## Creating a Group Account

**To create a group account:**

1. In Classic view, the iFIX WorkSpace, click the Security Configuration button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click Security, and then click Security Configuration Utility.
2. Click the Group Account button on the Security toolbox.
3. Click Add.
4. In the Group Name field, enter a name for the group account that you want to create.
5. Add security areas.
6. Add application features.
7. Click OK to save the group account in memory.
8. Click OK again to close the Group Accounts dialog box.
9. On the File menu, click Save.

## Adding and Deleting Account Privileges

Click any of the following links for more information on adding and deleting account privileges:

- Adding and Deleting Security Areas in a Group Account
- Adding and Deleting Application Features in a Group Account

### Adding and Deleting Security Areas in a Group Account

**To add or delete security areas in a group account:**

1. In Classic view, the iFIX WorkSpace, click the Security Configuration button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click Security, and then click Security Configuration Utility.
2. On the Security toolbox, click the Group Account button.
3. Double-click the group account in which you want to add or delete security areas.
4. On the Group Profile dialog box, click Modify from the Security Area list box.
5. To add security areas, double-click the ones you want to add from the Available list box. To add all the security areas to the current account, click Add All.
6. To remove security areas, double-click the ones you want to delete from the Authorized list box. To remove all the security areas from the current account, click Delete All.

### Adding and Deleting Application Features in a Group Account

**To add or delete application features in a group account:**

1. In Classic view, the iFIX WorkSpace, click the Security Configuration button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click Security, and then click Security Configuration Utility.
2. On the Security toolbox, click the Group Account button.
3. Double-click the group account in which you want to add or delete application features.
4. On the Group Profile dialog box, click Modify from the Application Features list box.
5. To add application features, double-click the ones you want to add from the Available list box. To add all the application features to the current account, click Add All.

   **NOTE:** Clicking Add All does not add the Electronic Signature – Bypass application feature. You must add this application feature explicitly.
6. To remove application features, double-click the ones you want to delete from the Authorized list box. To remove all the application features from the current account, click Delete All.

## Deleting a Group Account

**To delete a group account:**

1. In Classic view, the iFIX WorkSpace, click the Security Configuration button on the toolbar.

   -Or-

In Ribbon view, on the Applications tab, in the System & Security group, click Security, and then click Security Configuration Utility.

2. On the Security toolbox, click the Group Accounts button.
3. Select the group account you want to remove and click Delete. The following text appears:

   ```
   OK to delete this group?
   ```

3. Click Yes to delete the group account.
4. Click OK to close the Group Accounts dialog box.
5. On the File menu, click Save to permanently remove the account.

   **NOTE:** Be careful which group accounts you delete. Group members lose their account privileges when you delete a group account.

## Deleting All Group and User Accounts

**To delete all of your accounts and disable security:**

1. In Classic view, the iFIX WorkSpace, click the Security Configuration button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click Security, and then click Security Configuration Utility.
2. On the File menu, click Clear. The following text appears:

   ```
   Delete existing security configuration?
   ```

3. Click Yes to delete all of your accounts. The following text appears:

   ```
   Should default user and group accounts be created?
   ```

4. Click Yes to create sample group and user accounts or click No to omit this step.

## Modifying a Group Account

**To modify a group account:**

1. In Classic view, the iFIX WorkSpace, click the Security Configuration button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click Security, and then click Security Configuration Utility.
2. On the Security toolbox, click the Group Accounts button.
3. Double-click the group account you want to modify.
4. Modify the following group account information as needed:
   - The account name.
   - The security areas.

- The application features.

5. Click OK to save the group account in memory.
6. Click OK again to close the Group Accounts dialog box.
7. On the File menu, click Save.

## Configuring Security

Click any of the following links for more information on configuring security:

- Defining the Security Path
- Enabling or Disabling Security
- Enabling or Disabling Global Security Paths
- Exporting the Security Configuration
- Importing the Security Configuration

## Completing the Configuration Dialog Box

Completing the Configuration Dialog Box is a three-step process:

1. Enable security.
2. Specify a security and backup path. If you are using a file server, enter the path to the file server as the security path and enter a local path as the backup path.
3. Specify if you want to use global security paths. If you are using terminal services, it is recommended that you enable this option.

   **NOTE:** With the global security paths option enabled, all iFIX user sessions on this computer share the same security configuration. This is required in order for security to work properly for multiple users in a Terminal Services environment, especially when the default SCU is enabled in the Startup Profile Manager. If you do not enable global security paths, you will need to individually configure security within each Terminal Services user session.

## Defining the Security Path

**To define the security and backup paths:**

1. In Classic view, the iFIX WorkSpace, click the Security Configuration button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click Security, and then click Security Configuration Utility.

2. On the Security toolbox, click the Configuration button.
3. Double-click the Security Path field and enter the path you want to use.
4. Click OK. The following text appears:

   ```
   Copy existing configuration to new path?
   ```

5. Click Yes to move the security files to the specified path.
6. Double-click the Backup Path field and enter the path you want to use.

## Enabling or Disabling Security

**To enable or disable security:**

1. In Classic view, the iFIX WorkSpace, click the Security Configuration button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click Security, and then click Security Configuration Utility.
2. On the Security toolbox, click the Configuration button.
3. Select Enabled to enable security or Disabled to disable security.

## Enabling or Disabling Global Security Paths

**To enable or disable global security paths:**

1. In Classic view, the iFIX WorkSpace, click the Security Configuration button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click Security, and then click Security Configuration Utility.
2. On the Security toolbox, click the Configuration button.
3. Select the Use These Paths for All Startup Profiles check box to enable this option, or clear the check box to disable it.
4. If you cleared the check box to disable this feature, a dialog box appears. Click OK to continue.

   **IMPORTANT:** For global security paths to work correctly, the Base and Language paths in the SCU's Path Configuration dialog box must be the same for all users. Project paths can differ, however. To open the SCU, click the Start button and point to iFIX and then System Configuration. Click the Path Configuration button to open the Path Configuration dialog box. The default Base path is C:\Program Files (x86)\Proficy\iFIX, while the default Language path is C:\Program Files (x86)\Proficy\iFIX\NLS.

## Exporting the Security Configuration

**To export the security configuration:**

1. In Classic view, the iFIX WorkSpace, click the Security Configuration button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click Security, and then click Security Configuration Utility.
2. On the File menu, click Export.
3. In the File Name field, enter the name of the security configuration file you want to create.
4. Click Save. If the name you entered already exists, the following text appears:

   *filename* already exists. Do you want to replace it?
5. Click Yes to overwrite the existing file or click No to re-enter a name for the configuration file and repeat step 3.

## Importing the Security Configuration

**To import a security configuration:**

1. In Classic view, the iFIX WorkSpace, click the Security Configuration button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click Security, and then click Security Configuration Utility.
2. On the File menu, click Import.

   **IMPORTANT:** Be aware that you cannot import a security file exported from another language.
3. Double-click the file you want to import. The following text appears:

   Warning: Imported user accounts may not have passwords! Continue?
4. Click Yes to continue. The following text appears:

   Replace or add to existing configuration?
5. Click Replace to copy the security configuration defined by the import file to the local node, or click Add to merge the two configurations together. Any account with a user name or a login name that matches an existing account is ignored.

# Using Electronic Signatures

Click any of the following links for more information on electronic signatures:

- Entering an Electronic Signature
- Verifying an Action with an Electronic Signature
- Configuring a Tag to Require Electronic Signatures

## Entering an Electronic Signature

The Electronic Signature dialog box appears when you change the value of a database tag or acknowledge an alarm for which electronic signature is required. This dialog box can display only in the iFIX WorkSpace in the run-time environment; it does not display in configure mode.

The Description Area at the top of the Electronic Signature dialog box contains the details about the action. The Performed By section fields are active.

**To enter an Electronic Signature:**

1. In the Electronic Signature dialog box, in the user name field, enter your user name. If your user account is connected to a Windows user account, enter your Windows user name. Otherwise, enter your iFIX login name.

   **TIP**: If you are in continuous use mode, the user name field is filled in with the continuous user name. You can edit this name.
2. In the password field, enter your password.
3. Optionally, complete the following fields:
   a. In the Predefined Comments list box, select a predefined comment.
   b. In the Comment field, enter a free-form comment.
4. Click OK. If verification is required, the Verified By section activates and the Performed By section dims.
5. In the Verified By area, complete the fields, if active.

   **NOTE**: A user other than the one who completed the Performed By section must complete the Verified By section.
6. Click OK. The electronic signature is validated, the Electronic Signature dialog box closes, the new value is written to the tag, and a message detailing your action is written to the Electronic Signature Audit Trail.

   **NOTE**: If your iFIX user account is connected to a Windows user account and you unsuccessfully attempt to enter your user name or password, your account may be disabled after a certain number of tries. This number is determined by your Windows security settings.

## Verifying an Action with an Electronic Signature

Once you complete the Performed By section of the Electronic Signature dialog box, the Verified By section activates. If you have completed the Perform By section, someone else must complete the Verify By section.

**To verify an action that requires an Electronic Signature:**

1. In the Electronic Signature dialog box,, in the user name field, enter your user name. If your user account is connected to a Windows user account, enter your Windows user name. Otherwise, enter your iFIX login name.
2. In the password field, enter your password.
3. Optionally, complete the following fields:

a. Select a predefined comment from the Predefined Comments list box.

b. Enter a free-form comment in the Comment field.

4. Click OK. The electronic signature is validated, the Electronic Signature dialog box closes, the new value is written to the tag, and a message detailing your action is written to the Electronic Signature Audit Trail.

   **NOTE**: If your iFIX user account is connected to a Windows user account and you unsuccessfully attempt to enter your user name or password, your account may be disabled after a certain number of tries. This number is determined by your Windows security settings.

## Configuring a Tab to Require Electronic Signatures

Follow these instructions to configure a tag for electronic signature. To ensure a secure signing environment, you should not edit a current process database with an older-version node.

**To configure a tag to require Electronic Signatures:**

1. In the iFIX Database Manager, navigate to the Advanced tab of the tag's dialog box.
2. Select the type of electronic signature that you want for this tag:
   - **None** – Do not require Electronic Signatures for this tag at run time. This is the default option.
   - **Perform Only** – Require a Performed By signature for any changes or alarm acknowledgements to this tag at run time.
   - **Perform and Verify** – Require both a Performed By and a Verified By signature for any changes or alarm acknowledgements to this tag at run time.
3. Select the options that you want for this tag:
   - **Allow Continuous Use** – Select to allow the operator to repeatedly sign for successive actions by supplying only a password. Continuous use applies only to the person performing an action and does not affect the person verifying an action. This is selected by default.
   - **Exempt Alarm Acknowledgement** – Select to allow operators to acknowledge alarms without entering a signature, even when this tag requires electronic signature for data entry.
4. Select how you want the tag to handle unsigned writes. Your options are as follows:
   - **Accept** – Accept the unsigned write.
   - **Log** – When an unsigned write is accepted, send a message indicating that the tag accepted an unsigned write. This option is only available when the tag is configured to accept unsigned writes.
   - **Reject** – Reject the unsigned write and do not update the database. A message is sent indicating that the tag rejected an unsigned write. (default)

   **NOTE**: You must purchase the Electronic Signature option for these parameters to take effect at run time.

## Configuring for Automatic Login

Click any of the following links for more information on configuring for automatic login:

- Creating or Modifying an Automatic Login File
- Deleting an Automatic Login File

## Creating or Modifying an Automatic Login File

**To add or modify an automatic login file:**

1. In Classic view, the iFIX WorkSpace, click the Security Configuration button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click Security, and then click Security Configuration Utility.
2. On the Security toolbox, click the Autologin button.
3. Click Add or double-click the name of the node you want to modify.
4. In the Node field, enter the name of the node you want to configure.
5. In the Application User field, enter the name of the operator you want to log in automatically.

   **TIP:** Click the browse (...) button to select a user from the Select User dialog box.
6. If a Windows user is defined as an automatic login user, enter a password when prompted.
7. Click OK to save your changes in memory.
8. Click OK again to save the configuration to a file.

## Deleting an Automatic Login File

**To delete an automatic login file:**

1. In Classic view, the iFIX WorkSpace, click the Security Configuration button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click Security, and then click Security Configuration Utility.
2. On the Security toolbox, click the Autologin button.
3. Select the name of the node you want to remove, and click Delete. The Security Configuration program deletes the automatic login file for the selected node.

## Creating or Renaming Security Areas

**To create or rename a security area:**

1. In Classic view, the iFIX WorkSpace, click the Security Configuration button on the toolbar.

   -Or-

   In Ribbon view, on the Applications tab, in the System & Security group, click Security, and then click Security Configuration Utility.
2. On the Security toolbox, click the Security Area button.
3. Double-click the security area you want to create or rename.
4. In the Name field, enter a name and click OK.
5. Click OK again to accept your changes.

## Creating Windows Groups Using the CreateWindowsGroups Dialog Box

**To create Windows groups using the CreateWindowsGroups dialog box:**

1. Log in to Windows as a member of the Administrators or Account Operators group on either the local computer or the Windows domain.
2. Double-click CreateWindowsGroups.exe in the iFIX folder. By default, this folder is: C:\Program Files (x86)\Proficy\iFIX.

   The Create Windows Groups dialog box opens, displaying a list of Windows group names. The CreateWindowsGroups.exe derives the Windows group names from the current iFIX security configuration.

   **NOTE:** Windows group names display in the list box only if you establish all group and security area names in the iFIX Security Configuration before using the CreateWindowsGroups tool.
3. Select the appropriate filters and prefix style for the Windows groups that you want to create.
4. Select the groups you want to create from the list. The list may include multiple group names that represent some of the same iFIX security privileges due to the alias names.
5. Press the CTRL key and click to select multiple group names in the list box. Press the SHIFT key and click to select a range of group names in the list box.
6. If you are creating Windows groups on the local computer as local groups, click the Create Local Groups button to create the groups currently selected in the list box.
7. If you are creating Windows groups on the Windows domain as global groups, click the Create Domain Groups... button. The Specify Domain for Group Creation dialog box appears. Specify a domain name in which to create the groups currently selected in the list.

   Once you create Windows groups, you can use the Windows User Manager or a similar Windows security configuration tool to grant individual membership in the groups to Windows user accounts.

## Enabling Environment Protection

**To enable environment protection:**

1. In Classic view, on the WorkSpace menu, click User Preferences.

   -Or-

   In Ribbon view, on the Home tab in the WorkSpace group, click Settings, and then click User Preferences.
2. Click the Environment Protection tab.
3. Select the Enable Environment Protection check box.
4. Select the options you want to enable.

# Index

## D

## L



## M



## N



## O



## P

## R



## S

## T



## U