Proficy* HMI/SCADA - iFIX

SECURE DEPLOYMENT GUIDE

Version 1.0

December 2012

Disclaimer of Warranties and Liability

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

Notice

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

doc@ge.com

Table of Contents

About this Guide

The iFIX Secure Deployment Guide e-book is intended for process control engineers, integrators, IT professionals, and developers responsible for deploying and configuring iFIX.

What is Security?

Security is the process of maintaining the confidentiality, integrity, and availability of a system:

- Confidentiality: Ensure only the people you want to see information can see it.
- Integrity: Ensure the data is what it is supposed to be.
- Availability: Ensure the system or data is available for use.

GE Intelligent Platforms recognizes the importance of building and deploying software with these concepts in mind and encourages customers to take appropriate care in securing their GE Intelligent Platforms products and solutions.

Defense in Depth

Defense in Depth is the concept of using multiple layers of security to raise the cost and complexity of a successful attack. To carry out a successful attack on a system, an attacker would need to find not just a single exploitable vulnerability, but would need to exploit vulnerabilities in each layer of defense that protects an asset.

For example, if a system is on a network protected by a firewall, the attacker only needs to circumvent the firewall to gain unauthorized access. However, if there is an additional layer of defense, say a username/password authentication requirement, now the attacker needs to find a way to circumvent the firewall and the username/password authentication.

More information on security

For more information on security, including GE Intelligent Platforms security advisories and security patch notifications please visit our website at http://www.ge-ip.com/security.

Functional Overview

The information in the section is intended to assist with infrastructure configuration such as firewall configuration and Windows account set up.

Required Ports and Services

Network-based and host-based firewalls should be configured to only allow expected and required network traffic. The ports, services, and executables below are the only items required by iFIX application software to function. Note that this list does not consider the ports required by the Microsoft Windows operating system or other third-party applications that may be installed on an iFIX node.

SCADA Node

iFIX uses the following ports and services on a SCADA node:

Port	Protocol	Executable	Description	Direction
2010	TCP	TCPTASK.EXE	iFIX networking	Inbound
8989	TCP	IFIXNOTIFICATIONBG.EXE	iFIX Notification via .NET remoting	Inbound
14000	TCP	IHFIXCOLLECTOR.EXE	Historian FIX collector (if enabled)	Outbound
53014	UDP	ScadaSync.exe	Failover synchronization between SCADA pair	Both

NOTE: Port 1947 is used by the HASP License Manager installed with iFIX. This port can be closed without impacting iFIX functionality.

View Node (Client)

iFIX uses the following ports and services on a client:

Port	Protocol	Executable	Description	Direction
2010	TCP	TCPTASK.EXE	iFIX networking	Outbound
8989	TCP	IFIXNOTIFICATIONBG.EXE	iFIX Notification via .NET remoting	Inbound
14000	TCP	WORKSPACE.EXE	Proficy Historian data access for trending or data links (if enabled)	Outbound

NOTE: Port 1947 is used by the HASP License Manager installed with iFIX. This port can be closed without impacting iFIX functionality.

WebSpace Server

iFIX uses the following ports and services on a Webspace server:

Port	Protocol	Executable	Description	Direction
80	TCP	[System]	IIS server for iFIX WebSpace (configurable)	Incoming
491	TCP	APS.EXE	iFIX	Incoming

			WebSpace service (if enhanced failover is enabled)	
492	TCP	CLMWINDOWSSERVICE.EXE	Relay server licensing (between relay & SCADA servers)	Both
2010	TCP	TCPTASK.EXE	iFIX networking functionality	Outbound
14000	TCP	WORKSPACE.EXE	Proficy Historian data access for trending or data links (if enabled)	Outbound

System Account Requirements

Installation

iFIX can be installed using any Windows account with Administrator privileges. A different, non-Administrator account should be used to run the application after installation.

Operation

The iFIX SCADA node should be configured to run using a low-privileged Windows account specifically configured for the purpose of running the iFIX application. The iFIX SCADA node can run as a regular user – it does not have to be in the Administrators group.

iFIX SCADA node executables can also be run as a service with the *LocalSystem* account or a named account with Administrator privileges. If you want the user or group to run iFIX as a service, then you must grant the following Service Security and Access Rights for the Windows Service Control Manager (SCM):

- SERVICE_START
- SERVICE_STOP
- SERVICE_PAUSE_CONTINUE

Default Accounts

Default accounts are easily guessed and could provide an avenue for unauthorized system access. Immediately after installation, you should change the password on default accounts, rename/disable the

accounts, or delete the accounts altogether.

Default System Accounts

If you've installed an I/O Driver from GE Intelligent Platforms and you've configured it to run as a service, the Driver installation may have added an Administrative-level Windows account on the system called *FixIOUser*. This account has a well-known password and should be disabled or removed.

To check for the account, follow these instructions:

1. From the Windows Start menu, select Run.

2. Enter the following command and click OK:
   compmgmt.msc

3. Expand the "Local Users and Groups" tree and select "Users"

If the FixIOUser account exists, disable and remove the account using one of the options below. This process must be followed for all I/O Drivers installed on the system.

Removal Option 1 – Reinstall I/O Drivers:

The latest versions of the following iFIX I/O Drivers installers automatically remove the FIXIOUSER account and reconfigure the driver: ABR, EGD, GE9, MB1, MBE, OPC, S2G, SI7.

To obtain the latest version of an I/O driver please visit our website at http://support.ge-ip.com. If the driver you are using is not listed above, you must follow removal option 2 to manually remove the account.

Removal Option 2 – Remove manually:

Note: The example below describes the procedure for removing the OPC driver installed with iFIX. To remove other drivers, simply replace the "OPCDrv" command with "XYZDrv" where XYZ is the three-letter code for the driver you'd like to remove.

1. From the Windows Start menu, select Run.

2. Enter the following command to de-register the service and click OK:
   OPCDrv REGSERVER

3. Enter the following command and click OK:
   OPCDrv REGSERVICE

   The Logon Account for Running As A Service dialog box appears, and the registration process now allows the user to specify a logon account. Do NOT select the FixIOUser option. Instead, select one of the two options below:

   - **System Account** – uses the LocalSystem account to log on the I/O Server.

     NOTE: *The local system account cannot be used to access remote OPC servers. If this OPC Client accesses remote OPCDrv servers, you must define another account using This Account.*

- **This Account** – uses an account specified by the user to log on the I/O Server. The account used here must be an existing account with both Administrator and Logon as a Service privileges to run the server as a service. Use the Local Security Policy Setting tool to grant the account Logon as a Service privilege.

Then, to remove the FIXIOUSER account from Windows, follow steps 4 through 8 below. Note that these instructions may vary based on the version of Microsoft Windows you are running:

4. From the Windows Start menu, select Run.
5. Enter the following command and click OK:
   compmgmt.msc
6. Expand the "Local Users and Groups" tree and click "Users"
7. Select the FIXIOUSER account
8. Click "Action > Delete" in the File menu and click "Yes" to confirm deletion of the account.

Application Accounts

The iFIX installer creates the following iFIX application accounts by default:

- *ADMIN*
- *GUEST*

IMPORTANT: Both of the default accounts should be deleted using *a separate administrator account*. While this removes potential "backdoors" to the system, you will now need to be careful to remember the credentials to the remaining administrative-level accounts you created.

Security Capabilities

This section describes the iFIX capabilities and security features which can be used as part of a defense-in-depth strategy to secure your control system.

Authentication

iFIX authentication can be configured as follows:

Option 1: Windows Authentication (Recommended)

With Windows authentication enabled, iFIX clients send credentials to the server where they are validated by the Windows operating system on the server. This allows domain-based authentication if the iFIX server belongs to an Active Directory domain and domain credentials are provided.

In addition, GE-IP recommends implementing additional controls to protect the iFIX security files from change:

- Add a Windows file system Access Control List (ACL) on the file or directory where the security files are stored – restrict access

- Consider using third-party file integrity monitoring software to generate logs or alerts when this file is accessed or changed

Option 2: iFIX Authentication

With iFIX authentication enabled, iFIX clients send credentials to server where they are checked against iFIX security files which reside on the Windows file system. Credentials are obfuscated, but not encrypted in this file.

If iFIX authentication must be used, GE-IP recommends implementing additional controls to protect the iFIX security files from disclosure or change:

- Add a Windows file system Access Control List (ACL) on the file or directory where the security files are stored – restrict access

- Do not use Windows file sharing to allow multiple iFIX nodes to access the files. Transmission of the file via this mechanism is unencrypted and could allow sensitive data to be intercepted.

- Consider using third-party file integrity monitoring software to generate logs or alerts when this file is accessed or changed

Option 3: No Authentication (Default)

By default, iFIX authentication is turned off meaning that any client software can access the server. GE-IP recommends changing this default setting for most installations.

Authentication should only be disabled in cases where the SCADA is physically secured and deployed in standalone mode or in rare cases where network access can be tightly controlled.

Access Control and Authorization

iFIX contains configurable options to create roles and groups based on the concepts below.

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.

For more information on how to configure iFIX role-based access control and authorization, consult the "Configuring iFIX Security Features" manual.

Managing Users and Privileges

For more information on how to manage and configure iFIX users and privileges, consult the "Configuring iFIX Security Features" manual.

Logging and Auditing

Log	Location	Contents
yymmdd.LOG	C:\Program Files\Proficy\Proficy iFIX\ALM	iFIX Alarms, Events, and Security Audit trail.
aps_yyyy-mm-dd-xx-xx-xx-xx.html	C:\Program Files\Proficy\iFIX WebSpace\	WebSpace Application data, and Session connection entries.

Securing Network Communications

iFIX Trusted Network Computing can be enabled by checking the Enforce Trusted Computing checkbox in the Network section of the SCU.

Trusted Network Computing adds a shared secret as an authentication token for SCADA/Client communications. The token is passphrase based and must be entered on both the SCADA and the client via the SCU. GE Intelligent Platforms recommends changing the default password ("INETWORK").

Environment Protection

iFIX contains features that prevent users from performing tasks on the native operating system – such as "<Ctrl> <Alt> <Del>" and "File > Open". The ability to disable certain tasks is called Environment Protection. Environment Protection is particularly useful for iFIX installations on open, shared PCs (i.e. control room or shop floor) as it can limit the user's ability to use other applications on the PC or perform actions on the underlying operating system.

To configure Environment Protection for iFIX, use the Environment Protection tab of the User Preferences dialog box of the Proficy iFIX WorkSpace.

Electronic Signatures

Electronic signatures require that operators re-enter their username and password to electronically sign for certain actions such as process changes and alarm acknowledgements.

Detailed 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 an audit trail detailing the history of your

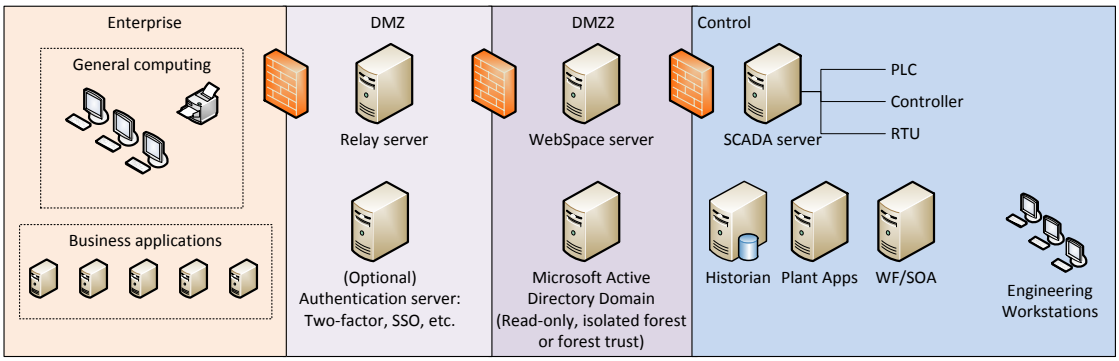
process.

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

Network architecture & secure deployment

This section describes security recommendations for deploying remote access via iFIX WebSpace.

Reference architecture



The figure above shows a reference deployment of iFIX components. The control system network is segregated from other untrusted networks such as the enterprise network (also referred to as the business network, corporate network, or intranet) and the internet. Process control network data and applications are authenticated and are exposed in a limited fashion using web-based applications and reporting capabilities.

Using Demilitarized Zones (DMZ)

A DMZ architecture uses two firewalls to isolate servers that are accessible from untrusted networks. Never expose an iFIX SCADA node directly to the internet. Instead, place a relay server or WebSpace in a DMZ configuration. For additional isolation, three firewalls can be deployed to create a "double-hop" DMZ configuration in which both the relay server and the WebSpace server can be deployed in their own DMZ.

Configuring SSL for WebSpace

GE Intelligent Platforms recommends configuring WebSpace to use SSL. By default, WebSpace client-server communications occur over TCP and are encrypted using 56-bit DES encryption.

SSL certificates are required to use SSL. You can obtain a certificate from a Certificate Authority (CA) such as Verisign or Thawte, or you can create a self-signed certificate. The certificates must be in .pem

format.

To configure iFIX WebSpace to use SSL:

1. From the iFIX WebSpace Administration, in the server tree, select the desired server from the list.
2. On the Tools menu, click Server Options. The Server Options dialog box appears.
3. Click the Security tab.
4. In the Transport drop-down list, select TCP or SSL.
5. When selecting SSL transport, type or browse to the path of the server's certificate in the SSL Certificate box.
6. Click OK.

When the SSL transport is selected, all connections to that iFIX WebSpace Server use the SSL transport and the selected encryption algorithm, including connections from iFIX WebSpace sessions. iFIX WebSpace sessions that do not support SSL will be unable to connect to the server using the SSL transport unless the "Use TCP as fallback" option is enabled.

Other Recommendations

This section describes additional recommendations and frequently asked questions.

Anti-virus software

GE Intelligent Platforms encourages customers to use third-party anti-virus software of their choice and to keep it up-to-date with the latest updates.

While GE Intelligent Platforms does not specifically certify any particular anti-virus supplier's software, we do test our products with GE's corporate standard (currently Sophos Antivirus) installed and running on all test and system lab machines. In the event there is a Proficy product defect discovered while running any anti-virus software, GE Intelligent Platforms will make all reasonable efforts to provide a solution. However, if the issue is found to be based on specific behavior of the AV software, the customer might be advised to work with the AV software vendor and/or switch to another AV software vendor to get resolution to their issue.

Data Execution Prevention (DEP)

GE Intelligent Platforms products function with Microsoft Windows Data Execution Prevention (DEP) enabled and GE recommends that customers enable this feature as an added protection against the exploitation of application security vulnerabilities such as buffer overflows.

In the event there is a Proficy product defect discovered while running DEP, GE Intelligent Platforms will make all reasonable efforts to provide a solution.

Patching

Patching GE Intelligent Platforms Proficy software

GE Intelligent Platforms recommends that customers keep Proficy software up-to-date by applying the latest Software Improvement Module (SIM) to their deployed Proficy products. SIMs add new functionality, fix bugs, and address security vulnerabilities.

Security advisories and security-related SIMs can be found on the GE Intelligent Platforms website at http://www.ge-ip.com/security. Customers can also sign up for notification of new SIMs and security advisories on the website.

Patching third-party software

GE Intelligent Platforms also recommends that customers keep operating systems, databases, and other third-party software in their environment up-to-date with the latest security patches from the software vendor.

GE Intelligent Platforms regularly validates the compatibility of selected GE Intelligent Platforms products with third-party operating system security patches. More information on this process can be found on the GE Intelligent Platforms Support website at http://www.ge-ip.com/security.

Platform configuration and hardening

GE Intelligent Platforms recommends configuring operating systems, databases, and other platforms as per vendor recommendations or industry standards.

The following organizations publish best practices, checklists, benchmarks, and other resources for securing systems:

- Center for Internet Security – http://www.cisecurity.com
- NIST – http://checklists.nist.gov
- Microsoft - http://technet.microsoft.com/security/default.aspx