GE VERNOVA

DIGITAL

PROFICY iFIX HMI/SCADA

Secure Deployment Guide

Version 1.10, March 2024

GE VERNOVA

Proprietary Notice

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

Trademark Notices

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

Table of Contents

1 Security Overview

Proficy iFIX® is a Windows-based HMI/SCADA component of the Proficy family of software automation products. Based on open, component-based technology, iFIX is designed to allow easy integration and interoperability between the plant floor and business systems. It includes functional and architectural features that reduce the design time for automation projects, allow simple system upgrades and maintenance, provide seamless integration withthird-party applications, and increase productivity.

The SCADA portion of iFIX provides monitoring, supervisory control, alarming, and control functions.

The HMI portion of iFIX is the window into your process. It provides all the tools you need todevelop pictures that operators can use to monitor and perform supervisory control of the process.

This *Secure Deployment Guide* describes the optimal security architecture and configuration for the iFIX nodes, and communication between the iFIX nodes, and the integration with other GE Digital solutions. Some security guidance is applicable to all iFIX installations and other security recommendations should be evaluated based on the size, complexity, and criticality of the process being monitored and controlled.

Throughout this *Secure Deployment Guide*, readers will encounter “Want to Learn More?” sections and the majority direct users to the Getting Started Guide that is part of the product documentation and supplied on the shipping media as a CHM file. If the information referenced resides outside the product information, clarification is provided in those instances.

1.1 Sensitive Data

iFIX involves the management of sensitive data at many levels. A comprehensive training plan for all users, including employees and subcontractors, addresses the protection of sensitive data. It is recommended that you track participants of such a training program for audit purposes.

NOTE: This document is not a replacement for GE Digital installation and other reference documents, which include more detailed information about security features that are outlined in this document. Pointers to additional helpful documentation are included in “Want to Know More” tipsincluded in this document.

1.2 Security Protections

Cybersecurity requires a robust and ongoing process to ensure steps are continually being taken to protect assets. It is recommended that ongoing assessments, testing and other security measures be built into the industrial control system (ICS) deployment and cyber maintenance plan. Examples may include vulnerability scanning, penetration testing, robustness testing, and white/gray/black box testing.

iFIX undergoes a rigorous process itself but because iFIX supports multiple use cases, users must evaluate and incorporate cybersecurity protections for each application on a case-by-case basis.

2 Sample Reference Architectures

The iFIX system supports a wide variety of industry sectors, types of industrial control systems (ICS), and organizational models. The appropriate architecture for an installation varies based on these and other factors. This section provides sample reference architectures along with an explanation of the security benefits and applicability of the architecture choices.

Use these sample architectures as guidance to design an appropriate architecture for anICS. The appropriate architecture may be a variant of these samples based on an organization's operational needs and risk management decisions.

The sample architectures use the concept of security zones and conduits that are used in IEC62443 standards and most other ICS security standard and guidance documents. The Control System Zone provides the highest level of trust. Each zone extending from this zone is a lower level of trust with the Corporate Zone being the least trusted one. In descending order, the network segment with the highest level of trust to the lowest level of trust is as follows:

- **Control System Zone**
- **Control System DMZ**
- **Support DMZ**
- **Corporate Zone**

A good security practice is to limit the conduits, or communication, between security zones. These conduits should be governed by a least privilege or whitelist approach where only required and approved communication is allowed through the conduit. The more trusted zone should originate communication to lower trust zone wherever possible. For example, aprocess in the Control System Zone can pull patch and anti-virus updates from the Support DMZ, as shown in Figure 2.

2.1 Single Computer, Stand-Alone Node in the Control System Zone

A single computer can perform the SCADA input/output (I/O) functions to communicate with the PLCs, the engineering workstation functions that design and automate the process, and an HMI used by an Operator to monitor and control the process (see Figure 1). This is referred to as a Stand-Alone node (all iFIX computers are referred to as nodes). This architecture is only recommended for small, non-critical installations.

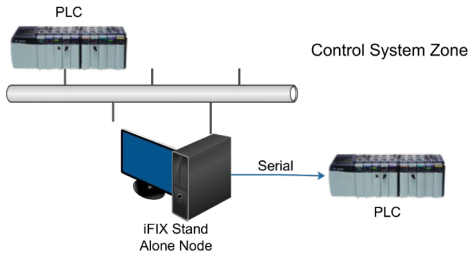


Figure 1 iFIX Stand Alone Node Architecture

Place this Stand-Alone node in a Control System Zone that is isolated from the Corporate Zone, internet, and all less-trusted zones by a firewall, one-way data diode, or air gap (no communication path available between the Control System Zone and other zones).

2.2 Distributed Process Control with Support DMZ

An iFIX node can monitor and control the process directly through communication with PLCs, and it can establish a remote connection with other iFIX nodes that perform the SCADA I/O function with other PLCs. This reference architecture is commonly used in cases where the control is physically close to the process and the Operator may want to view other parts of the Plant. It is also used where there is supervisory control from iFIX nodes in a Control Room, but the direct operation occurs at an iFIX node that is physically close to theprocess. All iFIX nodes are located on the Control System Zone.

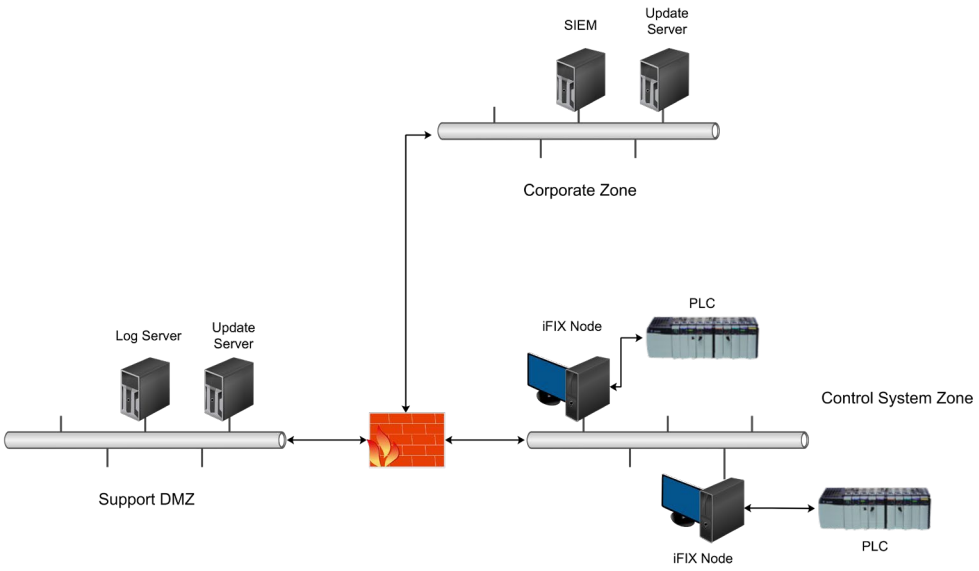


Figure 2 Distributed Process Control with a Support DMZ

A semi-trusted Support De-Militarized Zone (DMZ) is introduced in this architecture for cyber maintenance of the increased number of computers and network infrastructure, such as bringing security patches, anti-virus signatures, and other software updates into the Control System Zone.

Best security practices for Support DMZ include:

- Implement a least privilege methodology in the firewall ruleset by limiting each rule to the minimum set of source IP addresses, destination IP addresses, and destination TCP/UDP ports required for operations.
- Select support methods or protocols that use TCP, rather than UDP, and a small number of ports when possible. UDP is more easily spoofed because there is no initial handshake. The ideal protocol uses a single TCP port to provide the support or update service.
- Initiate the TCP communication from the more trusted zone. In other words, the computer in the more trusted zone pulls the updates from the less trusted zone. In Figure 2, the Update Server in the Support DMZ initiates a TCP session with a computer in the Corporate Zone to pull updates. Similarly, the iFIX nodes in the Control System Zone initiate TCP sessions with the Update Server in the Support DMZ to retrieve the updates.

The second purpose of Support DMZ is to support network and security monitoring in the Control System Zone. Many organizations have developed a monitoring and incident response capability and team that resides in the Corporate Zone. This capability and team may be leveraged to monitor the ICS but it is needed to send log files to the Corporate Zone.

Figure 2 shows a Log Server with the role to receive log files from the Control System Zone and forward them to the Corporate Zone. These log files could be syslog files from switches, routers, firewalls or servers, alerts from anti-virus or intrusion detection systems (IDS), alertsfrom PLCs, sensors, and anything else that can send a message in the network.

The best security practice for this communication is similar to the practices previously listed.Initiate the TCP session on the more trusted zone and use a minimum number of ports (preferably one). The difference is that the logs and alerts are pushed out from the Control System Zone to Support DMZ and then to the Corporate Zone rather than pulled as they arein the Update Server example.

2.3 Centralized Process Control with Historian in Control System DMZ

Another approach to using iFIX is to have a small number of iFIX nodes perform all SCADA I/O with the PLCs and other Level 1 devices. A larger number of iFIX nodes used by Operators and View Only users would be clients for this centralized process control.

This architecture can provide benefits in both performance and security. Performance can be improved by deploying higher performance computers with redundancy for the centralized SCADA I/O nodes. Security can be improved by limiting communication to the PLCs to the centralized SCADA I/O nodes, physically securing the centralized SCADA I/O nodes, limiting users who are allowed to login directly to a centralized SCADA I/O node, and using the iFIX security features to restrict Operator and View Only user actions on the client iFIX nodes.

Additional areas for centralizing the iFIX system should be considered in this reference architecture including:

- Centralizing user authentication with Microsoft’s Active Directory
- Centralizing iFIX security files on a File Server
- Centralizing backup
- Centralizing anti-virus management and other security and network tools

Centralization of these tasks should be considered where it reduces the lifecycle workload, reduces the opportunity for mistakes with a security impact, or improves the security of the system.

This third reference architecture adds the sharing of control system data with networks and systems outside the Control System Zone. Sharing historical control system data with systems in the Corporate Zone is the most common case. However, data may be shared witha cloud for big data analysis, mobile devices for alarm monitoring or key performance indicators, external organizations for maintenance and efficiency purposes, as well as a variety of other cases. The general industry trend is to share more control system data with outside systems and find ways to extract information and value from this data.

Figure 3 shows the addition of a Control System DMZ to the Figure 2 architecture. Many organizations combine the Control System DMZ and Support DMZ into a single DMZ but by separating them, you can gain these security advantages:

- The community of systems and users that requires access to these DMZs can vary greatly. Often, the number of users in the Corporate Zone that require access to the Control System DMZ can be large. Some organizations let all users access historical ICS data on the Control System DMZ. The computers in the Support DMZ typically communicate with a very small number of servers in the Corporate Zone. Separating the two DMZs eliminates the risk of attackers with access to the Control System DMZ being able to access the Support DMZ.
- The Support DMZ may require more TCP ports with more administrative purposes allowed through the firewall. This is a different attack surface than is commonly required in the Control System DMZ. By separating the two DMZs, the attack surface of each DMZ is reduced.
- It is easier to physically disconnect each DMZ to address an immediate threat without removing services from devices or services not at risk to the threat.

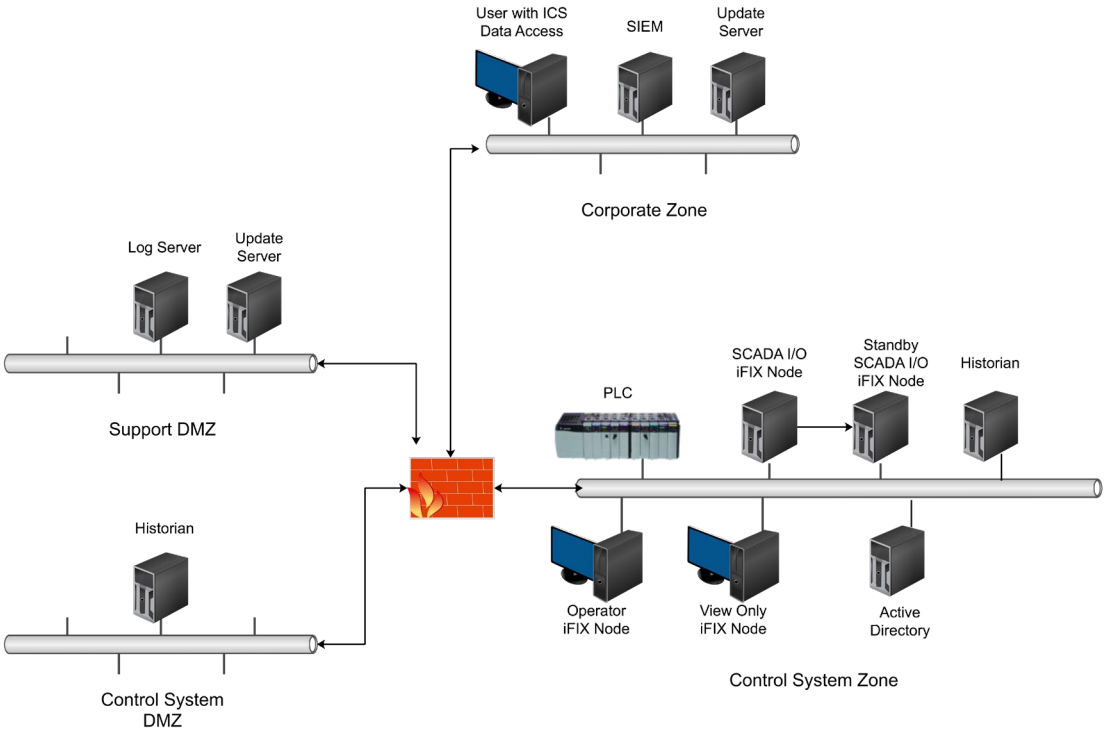


Figure 3 Centralized Process Control and the Addition of a Control System DMZ

The cost of an additional DMZ is minimal (an additional network switch) given that most firewalls have four or more network ports. However, the implementation of a good security practice firewall ruleset has a much greater impact on risk reduction than deploying a separate Control System DMZ for pushing control system data to the Corporate Zone. A single DMZ combining computers in the Control System DMZ and Support DMZ meets the security recommendations in most ICS security standards and guideline documents and is the most common DMZ architecture in ICS.

The Control System DMZ shows the Proficy Historian sharing iFIX data with the Corporate Zone and other external zones. A Proficy Historian may exist in the Control System Zone to provide historical data to operators and engineers working on an ICS. An additional Proficy Historian can be deployed in the Control System DMZ to provide historical data to users and systems in the Corporate Zone and other external networks.

The historical data is pushed from one or more iFIX nodes in the Control System Zone to Proficy Historian in the Control System DMZ. This firewall rule supports this communication:

Source IP	Destination IP	Destination Port
iFIX node(s)	Proficy Historian in DMZ	TCP/14000

The historical information could be pushed from Proficy Historian in the Control System DMZ to a server in the Corporate Zone, such as another Proficy Historian, SQL Database Server, or any server that supports a communication protocol available in Proficy Historian. The more common, but less secure case, is for users and servers in the CorporateZone to access Proficy Historian in the Control System DMZ. In either case, a single destination port, TCP/14000, must be allowed through the firewall between Proficy Historian and the other permitted communicating computers.

2.4 Remote Access to iFIX Screens Using Webspace

The reference architecture in Section 2.3 provides ICS historical data to users and applications outside the Control System Zone. The risk of this data sharing approach is minimized by the architecture and the fact that a user or application in a less trusted zone does not have access to an iFIX node that could perform control functions.

iFIX is part of a versatile product line that offers additional methods to view ICS information and perform remote control, as explained in this section and 2.5 Emergency Remote Access for Control and Administration. These methods introduce additional risk that is partially mitigated by additional security controls, and these risks and mitigations should be considered in the Design Phase of an iFIX project.

Some organizations want the ability to view the same screens as an Operator or Engineer in the Control System Zone from the Corporate Zone or some other less trusted zone. GE's Webspace functionality makes this easy to deploy and offers important security controls.

The first control is to prevent a user in the Corporate Zone from accessing a SCADA Server inthe Control System Zone. By placing a Webspace Server, in the Control System DMZ (see Figure 4), users in the Corporate Zone only need to access Control System DMZ rather than the Control System Zone.

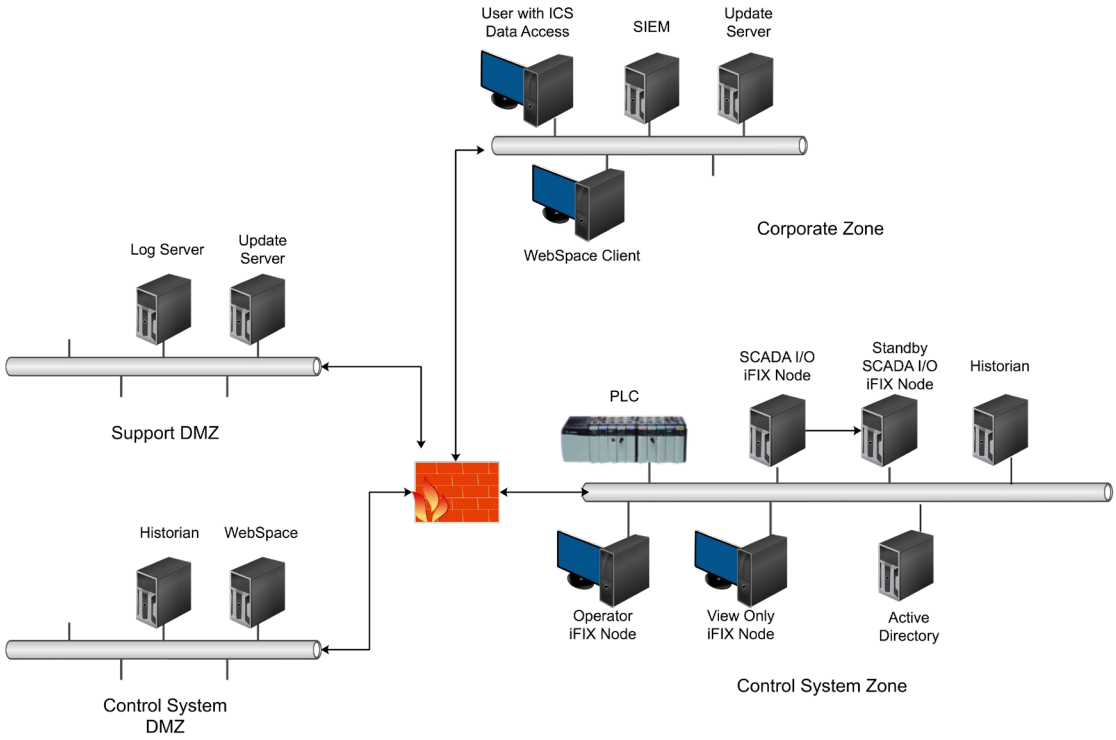


Figure 4 Remote Access to iFIX Using Webspace

The Webspace Server in the Control System DMZ is either running iFIX, preferred, or has access to the iFIX node in the Control System DMZ to get the required information. The firewall rules required to support this architecture include:

Source IP	Destination IP	Destination Port
Client in Corporate Zone	Webspace Server	TCP/443
iFIX Node in Control System Zone	Webspace Server with iFIX	TCP/2010
Webspace Server with iFIX	iFIX Node in Control System Zone	TCP/2010

Section 5.2 has details on securing the Webspace Server for remote access to iFIX pictures.

2.5 Emergency Remote Access for Control and Administration

A secure deployment of Webspace keeps control and administration of the ICS within the Control System Zone. However, in emergency situations, remote key support personnel and administrators may require control or the ability to modify the configuration outside of the Control System Zone. Some organizations allow regular remote access for control and administration purposes to save support costs. The type and frequency of remote access for control and administration is a risk decision that an organization must make.

It is usually better to have a secure remote access capability for control and administration available so that an insecure method is not cobbled together when needed in an emergency. The Webspace solution could be used for remote control of the process if the User security is configured to allow this, but the iFIX Configure WorkSpace required to modify and manage iFIX is not available through Webspace.

A Terminal Server in the Support DMZ can provide this emergency capability. The iFIX application can be deployed on this Terminal Server to provide emergency remote access for both control of the process and configuration of the iFIX application, see Section 5.3.

In addition, this Terminal Server can be used to provide a remote desktop (RDP) to certain key machines in the Control System Zone for management of the Operation System (OS), network devices and other software and hardware.

Source IP	Destination IP	Destination Port
Client in Corporate Zone	Terminal Server	TCP/443
Terminal Server	iFIX node in Control System Zone	TCP/2010
iFIX Node in Control System Zone	Terminal Server	TCP/2010
Terminal Server	RDP to Selected Servers	TCP/3389

Some organizations with experience and a support capability for Terminal Services prefer using a Terminal Server rather than Webspace to provide View Only capability to users in the Corporate Zone or other less trusted zones. In this case, View Only restrictions are configured and enforced by the iFIX application and the Terminal Server should be placed in the Control System DMZ.

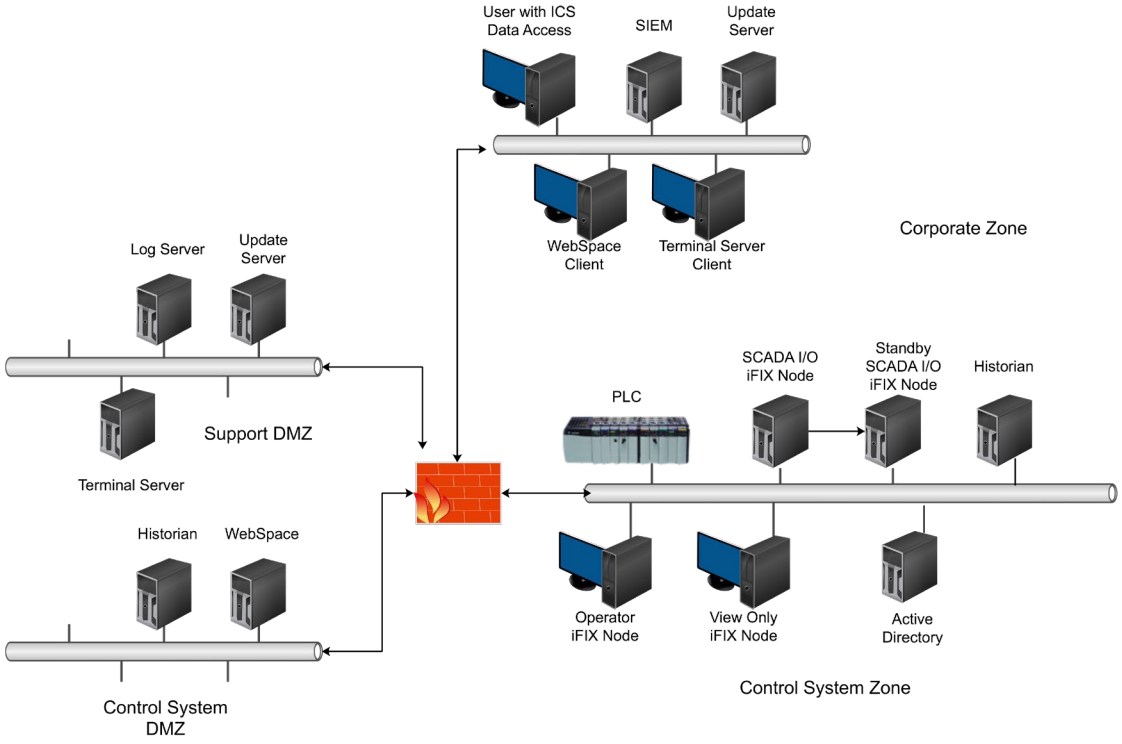


Figure 5: Emergency Remote Control and Administration Using a Terminal Server Solution

2.6 Enhancing iFIX Security Through Use of a 3rd Party Appliance, Featuring Bayshore OTfuse for iFIX

For iFIX customers who desire higher layer network security controls and policy enforcement, they can install the Bayshore OTfuse appliance, which supports iFIX proprietary protocols. Bayshore's OTfuse is an automatically configured, industrial firewall appliance with a proprietary intelligent Intrusion Prevention System (IPS) and policy engine, designed for easy deployment and use by automation engineers. It is a physical device that sits in front of critical endpoints, creating an enhanced secure zone for the PLCs and other industrial assets behind it. The OTfuse industrial firewall appliance automatically analyzes industrial network traffic, proposes its own firewall rules, enforces normal operations for each plant environment, and actively reduces threats to OT assets in real-time, now with native support for iFIX's version 6.X protocols.

OTfuse iFIX provides five separate security controls to protect iFIX standalone, SCADA, and view nodes as they Interact with each other and the broader OT/IT network. These controls Include:

- Rogue Node Detection
- Scheduled Maintenance Enforcement
- Reconnaissance Detection and Prevention
- DOS/DDOS Protection
- Anti-Spoofing Protection

For more Information, please contact Bayshore Networks or refer to the Bayshore Networks product documentation. A reference architecture Is provided below.

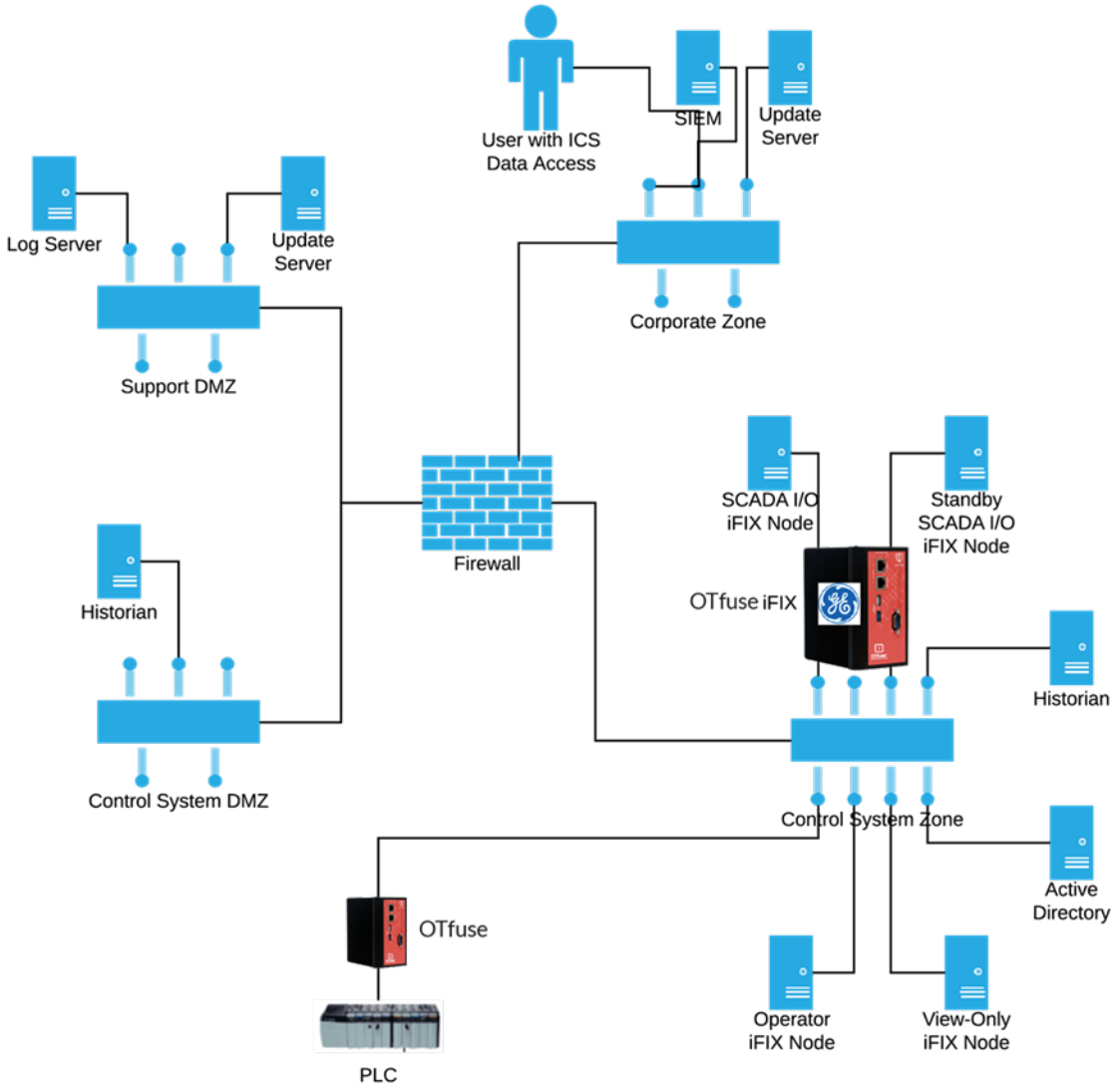


Figure 6: Reference architecture with Bayshore OTfuse appliance

Want to Know More?

- For information on Microsoft's terminal device commands for managing remote connections, go to https://technet.microsoft.com/en-us/library/jj215449(v=wps.630).aspx

2.7 Securing OPC UA and Web Configuration Client

This table describes the data flow connections for OPC UA Client and Server connections in iFIX, as well as the Web Configuration Client. This table describes the default assigned ports. We recommend the non-external facing ports are blocked from access from outside of the server.

Service	Default Port	External Facing
iFIX OPC UA configuration microservice for OPC UA Client	TCP/4855	
iFIX Project Configuration service	TCP/4877	
iFIX Configuration Hub System service	TCP/4873	
iFIX OPC UA browse microservice for OPC UA Client	TCP/4869	
Web server for iFIX configuration	TCP/9444	Yes
OPC UA Server	TCP/51400	Yes
Model Editor microservice	TCP/4861	
iFIX tag microservice	TCP/4864	
iFIX Model microservice	TCP/4865	
IGS Browse microservice	TCP/4867	
Proficy Authentication Redirection Port for iFIX	TCP/4871	
iFIX Façade (entry point to iFIX configuration) microservice	TCP/4859	
Web server for Configuration Hub	TCP/5000	Yes
Container microservice	TCP/4890	
Web server for Interop	TCP/5200	Yes
Interop Admin microservice	TCP/5620	
Interop Connection microservice	TCP/5600	
Web server for Proficy Authentication	TCP/443	Yes
Proficy Authentication Tomcat server	TCP/9480	
Proficy Authentication Postgres server	TCP/9432	

3 Securing iFIX Computers

The iFIX application runs on computers that have a Windows operating system. Good security practice requires the computing platform be deployed and maintained in a secure manner. This section covers:

- Securing the Windows Operating System
- Installation of the iFIX application

This section covers only security related issues to installation of the iFIX system.

Want to Know More?

For more information on installing iFIX, see *Getting Started with iFIX.*

3.1 Securing the Windows Operating System (OS)

You can install the iFIX application on a variety of Microsoft Windows OS. It is a good security practice to always run supported software where security patches and other operating system support fixes are provided by Microsoft. Deploying the iFIX application on the latest supported version of the Microsoft OS provides the longest time period until the OS needs upgrading.

At the time that this Secure Deployment Guide was written, iFIX application supports Windows Server 2019, recommended for iFIX Server installations, and Windows 10, recommended for iFIX Client installations.

While deploying iFIX nodes on the latest supported OS increases the lifetime until an OS upgrade is required, owners/operators must ensure that support exists within the organization for whatever OS is used in the deployment. Available support capabilities may result in deploying the iFIX application on an older OS even with the knowledge that the lifetime is reduced until an OS upgrade is required.

Want to Know More?

See "General Installation Information" in the *Getting Started with iFIX.*

3.1.1 Minimize Attack Surface

Every listening port, running service, and installed application is a potential software vulnerability. Before installing the iFIX application, follow these security practices to minimize the attack surface:

1. Remove unnecessary software, such as third-party applications, utilities, andlibraries.
2. Stop unnecessary running services.
3. Close listening TCP and UDP ports that are not needed.
4. Remove or disable user accounts that should not be using iFIX, including the Guest account (on the computer where iFIX is installed). Users who are not intended to be using iFIX should not be given accounts on iFIX machines.

Perform the tasks in that order to reduce the hardening effort.

The following PowerShell command will create a list of all software on the computer:

```
Get-ItemProperty
HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\* |
Select-Object DisplayName, DisplayVersion, Publisher, InstallDate | Format-
Table –AutoSize > filepath\filename.txt
```

Alternately hover over the Start tile, right click the mouse, and select Apps to display the installed software. Uninstall any software that is not required.

Each running service increases the attack surface, and many running services will open listening ports. Press the Windows+R keys to open the Run dialog, type services.msc, and press Enter, Alternately, open the Control Panel, click on the Administrative Tools icon, and double click on Services shortcut. All services not required for operation should be stopped and have the Startup Type set to Disabled (preferred) or Manual.

Unnecessary listening TCP and UDP ports are the most important item to restrict because they increase the attack surface for an adversary or malware on the network. Listening TCP and UDP ports can be identified with the Nmap scanning tool. Use this recommended command line for Nmap:

```
nmap -Pn -n -sS -sU --O -pU:0-65535,T:0-65535-v <host IP address>
```

This command completes in approximately 30 to 45 minutes. Alternately running `netstat – abno` in a Command prompt window will more quickly and accurately identify all listening TCP and UDP ports and the executable and process associated with each listening port.

Verify that all listening ports are required for the node. If there are unnecessary listening ports use the associated executable and process information to close the port, reboot the computer and retest.

3.1.2 Secure, Hardened OS Configuration

Windows operating systems have hundreds of security settings. In recent years, Microsoft has configured the OS installation to be secure by default for most security configuration settings, but many of these settings are still not in optimal secure status.

Microsoft provides guidance documents that represent the industry consensus for the optimal security configuration for each operating system, as well as Group Policy Objects (GPO) that make setting this optimal security configuration simple. Similar recommendations are also available from the Center for Internet Security, www.cisecurity.org, and other organizations.

Organizations should establish and implement a secure Windows OS configuration on the computer before installing the iFIX application.

3.1.3 Security Patching

Microsoft issues security patches monthly, therefore all but the very recently released software packages are missing security patches. Apply all security patches to the OS and other Microsoft and third -party software before installing the iFIX application.

3.1.4 Antivirus Software

Antivirus software does not stop custom malware or new malware that was not yet discovered by antivirus vendors. It does, however, stop mass market malware that is the most common cause of cyber security incidents in control systems. Install antivirus software on every iFIX node, update the antivirus signatures, and run a full scan on the server before deploying the iFIX application.

3.1.5 Windows Firewall

The Windows firewall can limit network access to computer, and the iFIX application can configure the Windows firewall to allow the required iFIX communication. Turn the Windows firewall on prior to installing the iFIX application.

3.1.6 IPSEC

The IPSEC protocol can protect the communication between Windows computers in an iFIX deployment. IPSEC encryption protects the confidentiality of the communication. An attacker who can eavesdrop on the communication will only be able to recover encrypted communication that will appear as random data. An attacker who attempts to modify or spoof iFIX communication will fail because IPSEC authentication will detect the data packet has been modified after the IPSEC authentication was applied.

If an organization requires encrypted traffic between iFIX nodes, IPSEC must be enabled andconfigured.

IPSEC is part of the Windows operating system. No additional software needs to be deployed, but the IPSEC tunnels need to be configured on each computer that will send and receive IPSEC protected communications.

Want to Know More?

See the *How to Configure Microsoft's Internet Protocol Security (IPSec) for Use with iFIX Networking* in Appendix A.

3.1.7 Data Execution Prevention (DEP)

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

In the event there is an iFIX defect discovered while running DEP, GE Digital will make all reasonable efforts to provide a solution.

3.2 iFIX Application Installation

The first step before installation is to ensure that the downloaded iFIX software is authentic.GE Digital provides a SHA256 hash file associated with each software download. Authenticate application software downloads by calculating the SHA256 for each download and verifying it against the GE-provided hash.

The new installation will require the appropriate iFIX license keys. GE Digital supports a number of hardware and software licensing options that can be managed locally or centrally. Information on iFIX licensing is available at http://support.ge-ip.com/licensing.

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. Centralized iFIX SCADA nodes that perform I/O, should be configured to run using a low-privileged Windows account specifically configured for the purpose of running the iFIX application (see Section 2.3).

iFIX SCADA node executables can also be run as a service with the Local System account or anamed 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

If the Windows Firewall is turned on, a message box will appear asking:

“Enable iFIX through the firewall”

Select Yes so that the necessary iFIX communication is allowed into and out of the iFIX node.

3.2.1 Installing iFIX with Access Controls - iFIX 6.5 and later

With the release of iFIX 6.5, users can install iFIX using Access Controls (Secure Mode), which secures the Windows resources by restricting access to registry keys, files and folders, and runtime shared objects to authorized users that belong to a Windows User Group defined during install.

NOTE: The default for the iFIX installation is for Access Controls to be disabled. For secure environments, it is recommended that Access Controls be enabled at install time.

The iFIX 6.5 release includes the ConfigureWizard.exe, that can be run directly to change these settings after install. You can find this wizard in the iFIX install directory or from the "Setup Access Controls" shortcut added to the iFIX start menu folder. For instance, if you choose not to install securely initially, you can use this wizard to change to Access Controls in the future.

The Windows OS Security functionality allows administrators to create security groups that can be used to manage permissions on various system-wide objects including folder and file as well as registry access.

For an additional layer of security, iFIX system administrators should choose to install iFIX with Access Controls. Once iFIX has been installed with Access Controls, only members of the Windows user group specified during installation will have access to the installation folder and files and registry keys of iFIX. This will limit the ability to launch the application, browse application folders, and modify application files and registry entries to only those users who are members of the group.

The iFIX administrator can follow the procedure below to implement iFIX with Access Controls. Before installation, be sure to:

- Identify a Windows user group name (local or domain) for users who will be authorized to use iFIX in the Windows system. By default, the "IFIXUSERS" group on the local system is identified. Note that if a domain group is identified, ensure that the group exists before installation.
- If a local group is identified, the installer will create the group if it does not exist.
- The user installing iFIX will be added to this group if the installer has the privileges to do so.
- Identify a Windows user account that iFIX will run under when running as service. Note that this user must exist on the same Windows system before installation.
- This user will be added to the Windows user group identified earlier if the installer has the privileges to do so.
- Identify other Windows users who will need to use iFIX on the computer. Note that all these users will need to be added manually to the Windows user group identified earlier in the installation.
- During installation, in the iFIX Install Mode dialog, choose the Install iFIX with Access Controls and enter the following information that was used earlier: The local or network domain name and Windows group name, and the user name and password of iFIX service account.
- After installation, manually add all those users who have been identified prior to the Windows user group. Create new Windows users if needed and add them to the group.

3.2.2 Access Controls with the Integrated Installer new in iFIX 2022

In the iFIX 2022 Release an Integrated Installer is available to perform the installation of multiple Automation products commonly used together to provide customer solutions. The product installs are done silently by the Integrated Installer. It should be noted that in this scenario iFIX is installed with Access Controls disabled. For secure environments, it is recommended that post installation using the Integrated Installer user enable iFIX Access Controls by launching the ConfigureWizrd.exe application directly or through the "Setup Access Controls" shortcut added to the iFIX start menu folder. The steps to enable iFIX Access Controls are outline in section 3.2.1.

3.2.3 Securing iFIX Files and Registry Entries in Releases Prior to iFIX 6.5 by Creating a Local "iFIXUsers" Windows Security Group

The Windows OS Security functionality allows administrators to create security groups that can be used to manage permissions on various system-wide objects including folder and file as well as registry access. For an additional layer of security, iFIX system administrators can create an "iFIXUsers" group on the local system where iFIX has been installed. With this group created, the iFIX administrator can then add only specific configured users that are going to be authorized iFIX users.

Once the "iFIXUsers" group has been created, the default security permissions of an iFIX installation can be modified to allow only members of the "iFIXUsers" group to have access to the installation folder and files and registry keys. This will limit the ability to launch the application, browse application folders and modify application files and registry entries to only those users who are members of the group.

The iFIX administrator can follow the procedure below to implement "iFIXUsers" group-based application access.

1. Create the "iFIXUsers" group using the Windows Computer Management utility.
2. Add existing users to the "iFIXUsers" group that will require access to iFIX folders and files. This does not need to include iFIX users configured within iFIX security, only user profiles that are required to launch, browse, and edit iFIX application folders and files should be added to the group.
3. Create new user profiles if required and add them to the "iFIXUsers" group.
4. After the installation of iFIX is complete, browse to the base installation directory for iFIX application files.
5. Right-click on the folder and select the "Properties" option.
6. Select the "Security" tab in the Properties dialog.
7. Click the "Edit" button under the "Groups or user names" section.
8. Click the "Add" button and either type or browse to the "iFIXUsers" group created previously and click OK.
9. Highlight the newly added group and ensure that Modify, Read & Execute, List folder contents, Read and Write permissions are enabled by licking the Allow box.
10. Click Apply to save the edits and return to the Security tab.

11. Close the Properties dialog box.
12. Similarly, several important registry entries created during the iFIX install can be protected with the “iFIXUsers” group permissions. These entries are listed below and include sub entries.

    - HKEY_LOCAL_MACHINE\SOFTWARE\Classes\FIX32
    - HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SOFTWARE\Fix Dynamics

13. To update the permissions on these registry entries, launch the regedit.exe applicationwith administrator privileges.
14. Navigate to each registry entry listed above then right-click and select “Permissions…”
15. Click “Add…” to apply the “iFIXUsers” group. You can type in the group directly or select“Advanced” and “Find Now” to search for the group and add.
16. Select any generic user groups that should not have access to iFIX entries and select“Remove”. This likely will include the generic “Users” group.
17. If you want these setting to apply to the currently logged in users, have all users log outand log back in.

NOTE: Follow this procedure after a new installation of iFIX, as well as after each upgrade installation of iFIX.

3.3 Patching iFIX

The iFIX application, like all software, should be periodically patched to address security and other known software issues. Apply all iFIX security patches prior to configuring the iFIX node. You can find security patches issued by GE Digital at https://ge-ip.force.com/communities/CC_Knowledge?product=iFIX c&contents=Service_Packs c

Installation instructions are included in the ReadMe file of each SIM.

NOTE: iFIX patches are cumulative and installing the most current SIM ensures users have all available fixes.

3.4 iFIX SCADA Server Node Redundancy

ICS owners/operators have recognized the importance and value of redundancy for many decades. As shown in the Section 2 sample reference architectures, there are many ways of distributing the monitoring and control of a process in iFIX to provide enhanced availability.

An iFIX SCADA Server node that is responsible for centralized communication with PLCs and other Level 1 devices can be deployed as an Active / Standby server pair using the iFIX Enhanced Failover feature. This redundant iFIX SCADA Server node can prevent a software, hardware, or network fault in the primary iFIX SCADA Server from causing a loss of ICS availability. Server redundancy is unlikely to prevent a cyberattack from compromising both

servers in the Enhanced Failover pair because the servers will have the same security posture.

In an Enhanced Failover SCADA Server pair, the Active node continuously pushes a copy of the memory-based process database (PDB) to the Standby node. The active node synchronizes its process database with the standby node. SCADASync.exe is the iFIX application that performs the synchronization. SCADARoleMgr.exe is the iFIX application that decides if the SCADA node is active or standby.

iFIX nodes that are clients to the Enhanced Failover SCADA Server pair will automatically communicate with the Active node.

The following port is used for Enhanced Failover:

Service	Default Port	External Facing
iFIX Port for SCADA Sync / Failover	TCP/53014	No

NOTE: When UDP is used for Enhanced Failover, you will need to open TCP port 53014 and UDP port 500. When TCP is used for Enhanced Failover (available as an option in iFIX 2023 or later), you only need to open TCP port 53014. You can also choose to have Enhanced Failover to use a different TCP port.

Want to Know More?

See the *Enhanced Failover* document.

4 iFIX Application Security

iFIX offers a variety of security controls that can be tailored to meet your operational environment and security needs. This section describes the iFIX security controls and provides examples of how they are commonly applied in ICS.

Security controls can be enforced based on the User that is logged into the application or the iFIX node that is performing the monitoring or control. Organizations with a complex environment will use a mix of iFIX User and iFIX node-based security measures.

4.1 User Based Security

iFIX Users are authenticated and then authorized to perform approved monitoring, control and administrative actions based on privileges assigned in User based security controls. iFIX supports a very granular application of privilege assignment, and iFIX supports grouping of Users and privileges to make the management of User privileges easier.

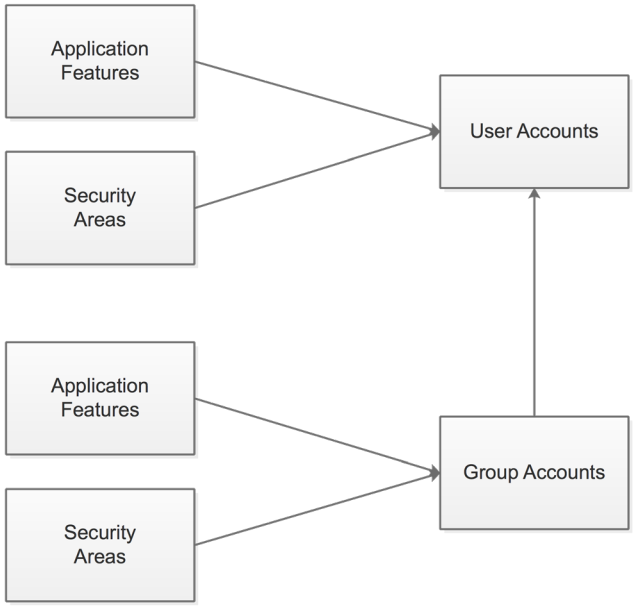


Figure 6: User Based Security Concept

Figure 6 shows an overview of User based security concept.

1. Security Areas are created to restrict what part of the process can be controlled.
2. Groups are created to support role-based access control
3. Security Areas and Application Features are assigned to each Group
4. Users are created and assigned to one or more Groups based on their roles
5. Additional privileges are granted or removed from Users to address any required variances from the assigned Group privileges

4.1.1 Security Areas

A Security Area can consist of blocks, also called tags or points in control systems, that can be written to and monitored. A Security Area can also consist of pictures, schedules and recipes that can be read or viewed. Security Areas provide a way to grant a user privileges for only part of the overall process that is monitored and controlled by iFIX. This access control method is sometimes referred to Area of Control or Area of Responsibility in control systems.

For example, a pipeline SCADA system could monitor and control three different pipelines. Blocks and pictures for each pipeline could be placed in its own Security Area, and Operatorscould be restricted to only operating a single pipeline by placing them in the

appropriate Security Area. iFIX supports up to 254 Security Areas and each security area can include anywhere from one block or picture to all blocks and pictures. iFIX has the authorization granularity to support almost any authorization scheme.

4.1.2 Application Features

While Security Areas control what part of the process various control and monitoring commands can be performed, the Application Features control what iFIX application features are accessible by a User. Application Features are commonly referred to as User / Group Permissions or User / Group Privileges in information security terminology. The security related Application Features covered in this section are configured in Application Feature Selection dialog box, see Figure 7.

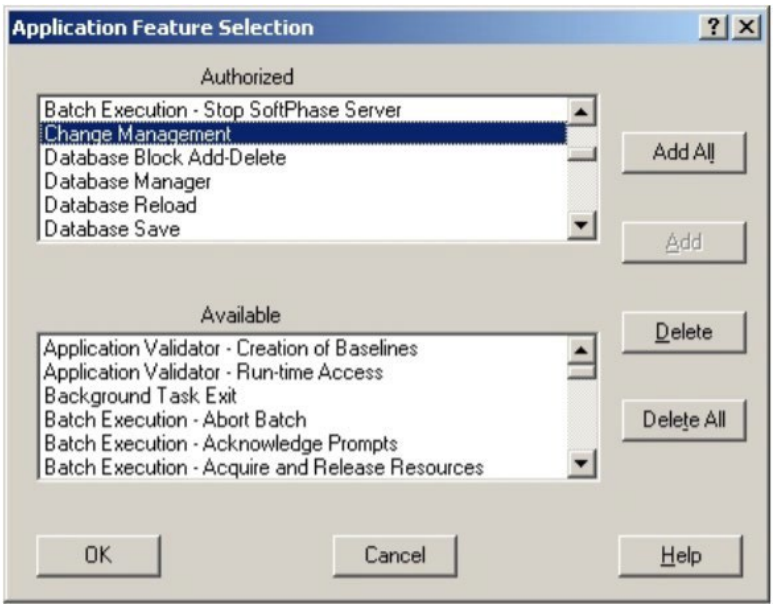


Figure 7: iFIX Application Feature Selection

Many of the Application Feature security controls can be applied in the Environment Runtime Protection portion of node-based security, see Section 4.2.4. A common approach is to apply the most typical configuration through Environment Runtime Protection and thenimplement exceptions through the Application Features, as the User based security takes precedence in the case of conflict with node-based security.

Want to Know More?

See the “Application Feature Descriptions” table in the *Configuring Security Features* document.

Workspace Change and Restrict Exit from Runtime Mode

There are two modes for an iFIX WorkSpace: Configuration and Runtime. Runtime is used

byOperators to monitor and control the process. Configuration is used by Engineers and Administrators to modify the iFIX configuration, such as creating or modifying blocks and pictures. There are Application Features that can be added to a Group or User account to allow or disallow switching between the WorkSpace modes.

- *WorkSpace Configure*: Allows the user to switch from Runtime to Configuration mode

- *WorkSpace Runtime*: Allows the user to run in Runtime mode.

The most common security use of these Application Features is to restrict Operators and View Only Users from switching to the Configuration WorkSpace by not granting these roles to the *WorkSpace Configure* Application Feature.

Restrict Exit from Runtime Mode

Operator node and View Only nodes are often dedicated to this purpose, and there should be no reason for a User in Runtime mode to access anything but the iFIX Runtime WorkSpace. The Application Feature *Enable Ctrl-Alt-Del* can allow or prevent a User from accessing the Task Manager, as well as preventing log off, shutdown or changing a password.

The Application Feature *Enable Task Switching* can similarly prevent a User from accessing other applications outside of the iFIX Runtime Workspace, but still allow the User to shut down or logoff of Windows.

Environment Protection must be enabled for the *Enable Ctrl-Alt-Del* and *Enable Task Switching* Application Features to be used.

Shutdown iFIX

Two Application Features can control what Users can exit the iFIX application and related tasks:

- *iFIX - System Shutdown*

- *Background Task Exit* - Stops any background iFIX tasks such as SAC, Session Monitor, or Historical Collect

Electronic Signature

The capability to generate and verify electronic signatures are Application Features that can be assigned to a Group or User account, *Electronic Signature - Performed by* and *Electronic Signature - Verified By* respectively. This Application Feature enables the capability, but Electronic Signatures need to be further configured, see Section 4.4.

Security Configuration

The Application Feature *Security Configuration* controls access to the Security Configuration

Utility. This Utility is used to configure the security system, create, and delete User and Group accounts, name Security Areas, and perform other security configuration activities.

This *Security Configuration* Application Feature provides the capability to weaken or disable iFIX security controls and should be carefully assigned. Many iFIX systems will allow most or all Engineers to access the Configuration WorkSpace, but limit who is able to access the Security Configuration Utility. However at least one User must have this Application Feature.

The *Security Configuration* Application Feature can only be assigned to Groups or Users. It cannot be assigned to a node as part of the node-based security configuration.

Backup / Restore

The Application Feature *Project Backup-Restore* provides a User with these capabilities. The privilege to restore a Project does carry with it security risk. An attacker could modify the security features, as simple as disabling security, and restore a Project to subvert existing iFIX security controls. This capability should typically only be assigned to User accounts with a *Security Configuration* Application Feature.

Change Management

The *Change Management* Application Feature allows a User to access the Change Management version control features in iFIX.

4.1.3 Group Accounts / Roles

Role-based access control makes user administration easier and less prone to errors with a security impact. Assign privileges to roles, and then users placed in these roles inherit those privileges. Privileges are managed in a small number of roles rather than for each individual User account.

ICS typically have a small number of roles, such as Operator, Engineer, Supervisor, Administrator and View Only. Role-based access control is used in most ICS applications, including iFIX. iFIX implements role-based access control with Group accounts. A Group is created and assigned Security Areas and Application Features in the Group Profile Dialog Box.

4.1.4 User Accounts

There are two default accounts that are created during the iFIX installation:

Default Username	Default Password
Guest	Guest
Admin	Admin

These default accounts should be removed.

A good security practice is to create and assign a unique user account to each person requiring an iFIX login. This allows any action recorded during login to be attributed to the specific owner of the account performing the action. Shared accounts make this attribution through logs impossible, and it is very common for shared account credentials to be widely known in the Operations Group over time.

This good security practice is often violated by ICS owners/operators, particularly with Operators in a control room, for a variety of reasons. Issuing unique user accounts to individuals is most important for:

- Highly privileged accounts, such as accounts with access to the Configuration WorkSpace
- Accounts used on an iFIX node that is in a physically insecure location or a location that is not manned 24x7

If a shared user account is part of the security design, then another security control should be implemented by policy or other means to hold an individual responsible for the action taken with the shared user account. For example, Operators using a positional shared user account, for use by any Operator on a specific iFIX node, could be held accountable for all actions taken on that node while an Operator is on shift.

The privileges assigned to a user account are based on:

- Group membership, which carries with it the Security Areas and Application Features assigned to the Group
- Security Areas, that are assigned individually to the User account rather than through a Group
- Application Features, that are assigned individually to the User account rather than through a Group
- Login timeout, see below

Each user account can be configured for a maximum login time interval. The iFIX application will automatically logout the user when this login time interval is reached. Two of the more common uses of this security feature are:

1. Insuring Operators and other shift workers that have unique accounts log out at the end of their shift, and the new shift logs in. If shifts are set for 8 hours, then this value could be set to 8 ½ hours.
2. Prevent a high privilege user account from remaining logged in or forgetting to log out on nodes where the iFIX Screen Saver security cannot be used.

4.1.5 User Authentication

iFIX supports integrating authentication with Windows or using the native authentication in the iFIX application. If the security of User authentication is a concern, as it should be in most deployments, then Windows Authentication should be used. The native iFIX authentication is included in the iFIX application for use in legacy iFIX installations where an upgrade to Windows authentication is determined to be impractical.

Windows Authentication

Microsoft has developed robust user authentication in their Windows OS and User management components, and these are well understood by most owner/operators. When Active Directory is used, Users can be managed in a single location which eases adding, modifying, removing, and auditing User accounts.

Password security controls are also improved when iFIX authentication is integrated with Windows. This allows iFIX to leverage the Windows Password Policy and Account Lockout Policy features available for Windows in both Active Directory and local account management. iFIX can set and enforce security parameters such as password age, password length and complexity, password change, and account lockout due to excessive login failures.

If Active Directory exists in the control system zone, then authenticating Users to this Active Directory domain is strongly preferred. Owner/operators with all but small iFIX installations should consider deploying Active Directory in the control system zone if it does not currentlyexist.

When a User attempts to login to the iFIX application, iFIX securely forwards the authentication credentials to the local Windows computer or the Domain, as configured, and acts on the success or failed response from the computer/Domain.

Windows Security is configured on each User account in the User Profile Dialog Box. Select the Use Windows Security check box and enter the Windows username and domain name, ifapplicable.

Want to Know More?

See “User Profile Dialog Box” in *Configuring Security Features* document.

Windows Authorization (Privileges)

Privileges are typically assigned to Groups and User accounts in the iFIX application, see Section 4.1.3 and 4.1.4, and this is the recommended security approach for most iFIX installations.

The iFIX Security Synchronizer feature allows Active Directory Group Membership to determine what privileges are assigned to a User. In this case, an Active Directory Group is created for each iFIX privilege that will be assigned to one or more users. Windows User

accounts are then added in the appropriate Active Directory Groups for the required privileges.

Running the iFIX Security Synchronizer will bring in the Active Directory Group information and alters the corresponding iFIX privileges for each user to match the Active Directory Group. The Security Synchronizer must be run each time a User or User privilege is changed.

Using Active Directory Groups to manage iFIX privileges adds unnecessary complexity to most installations. It may be applicable to organizations where a centralized control system zone has an Active Directory that supports many iFIX installations with a similarprivilege approach and centralized Active Directory User management for all iFIX installations.

Want to Know More?

See "Security Synchronizer" in the *iFIX Configuring Security Features* guide.

iFIX Authentication

The iFIX application supports creating and managing of users directly in the application, but this should only be used in legacy installations where use of Windows authentication is not practical. If the *Use Windows Security* check box is not selected in the *User Profile Dialog Box,* then iFIX authentication will be used.

4.2 iFIX Node Based Security

iFIX node-based security controls are applied to all Users on an iFIX node. These security controls secure the iFIX application environment and access to other applications and privileges on the computer. The User based security configuration takes precedence when there is a conflict between the User based security controls and Node based security controls.

There is significant overlap in the User based Application Features and the node-based Runtime Environment Protection. This provides flexibility for the owner/operator in creatingthe security scheme. In most cases, it is recommended to apply node-based Runtime Environment Protection first and then apply User based Application Features for exceptions to the Runtime Environment Protection and the small number of settings that are only available through the Application Features.

4.2.1 Site Specific Authentication

iFIX communications at a Plant or other site can be restricted to authorized iFIX nodes by enabling the Enforce Trusted Computing option and setting the password in the Network Password field of the Network Configuration dialog box in the System Configuration Utility (SCU), see Figure 8. This password is used to authenticate two nodes as part of establishing iFIX communication.

The same password must be entered for all iFIX nodes that need to communicate. Two or

more iFIX systems in the same company and on the same network can be prevented from communicating with each other by using this security feature and entering a different password for each system.

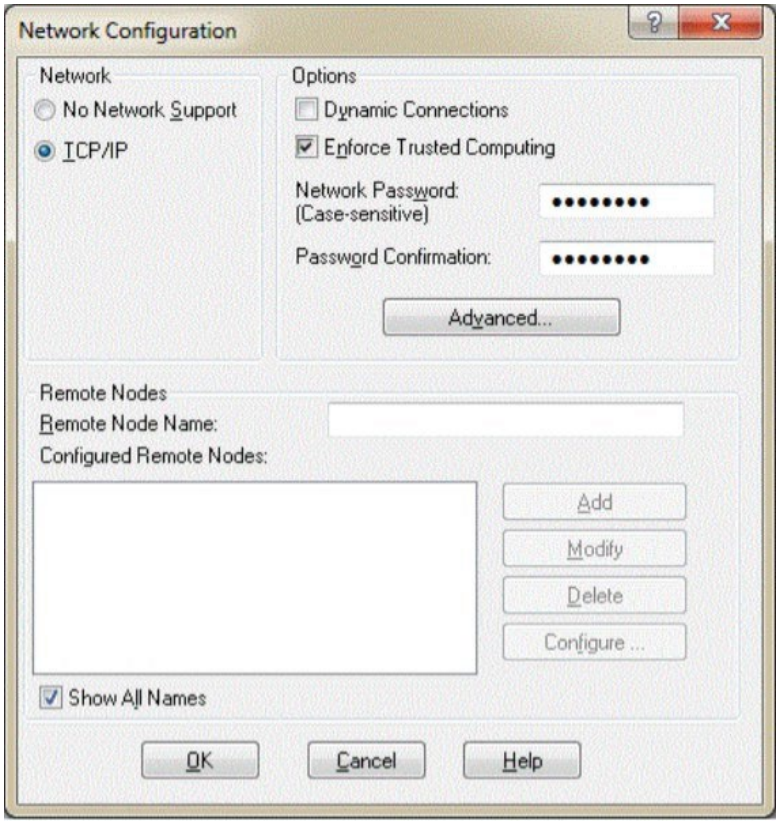


Figure 8: Site Specific Authentication

4.2.2 iFIX Node-Based Access Control

iFIX Security Areas, described in Section 4.1.1, are the security control in iFIX for User or Group based access control to blocks, pictures and recipes. There are instances where a User with the privileges to monitor or control a part of the process should only be allowed this access from specific iFIX nodes. For example, a Plant may want to only allow control of part of a process from an iFIX node that is physically located by that part of the process for safety reasons. Other iFIX nodes on the Plant floor may not need to be able to view the status of that physically remote part of the process, but the iFIX nodes in the Control Room have a need to monitor the entire process. Node based access control can enforce this and many other scenarios.

Node based access control is defined in each iFIX node's NETWORK.INI file. The default configuration of the NETWORK.INI file at install accepts all remote iFIX connections and allows all remote connections to write to the database, assuming the remote User has the

appropriate Security Area privileges. The NETWORK.INI file can be modified to restrict what iFIX nodes are allowed to establish a remote connection and what iFIX nodes are allowed to write to the iFIX node's database.

To implement least privilege for remote node connections, set accept_unknown_host=OFF and add all the hosts that are allowed remote connections, for example:

accept_unknown_host=OFFHost1=HMI1
Host2=HMI2 Host3=SCADASERVER2

If the process requires all iFIX nodes have remote connections to all other iFIX nodes, then a complete list of iFIX nodes would be added to each iFIX node's NETWORK.INI file.

The ability to write to an iFIX node's database can be similarly restricted in the NETWORK.INI file. Continuing the example from earlier in this section:

accept_unknown_write=OFFwritenode1=HMI1 writenode2=SCADASERVER2

HMI1 and SCADASERVER2 would be allowed a remote connection with write access to the database / control of the process. HMI2 would be allowed remote access to view the iFIX node but would be unable to write to the database /control the process.

Access to the NETWORK.INI file should be restricted using access control lists through File and Folder permissions.

4.2.3 Changing the Security Path

Each iFIX node has a set of security files that define the security configuration for the node. The default for the primary security path is locally on the iFIX node. This can be altered in the Security Configuration program, and a backup security path can be set.

If users want an iFIX node to have its own set of accounts, keep the local path. However, if User and group accounts are to be shared with other computers, specify a file server (network) path as the security path and have all iFIX nodes use this path.

Read-write access must be granted to the security path designated when entering the path. After entering a path, the Security Configuration program creates lock files (SECLOCK.LCK and SECLOK2.LCK) allowing use of the program with read-only access to the security path.

It is a good security practice to have at least one of the security path locations be to a file server in the Control System Zone, even when a local file is used as the primary security path, that is backed up on a regular basis. The appropriate folder permissions should be applied to restrict access to these iFIX files stored on the file server.

When enabling 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 iFIX startup profiles created in the Startup Profile Manager are

used, it is likely users will 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 iFIX system also supports a Global Security Path. This is most applicable when a Terminal Server is used, see Section 5.3.

4.2.4 Enable Security Protection

The default setting for all iFIX nodes is Security disabled at initial install. While security is disabled, anyone can use and administer iFIX without restriction. **It is essential that Security Protection be enabled via the Security Configuration application on every iFIX node.**

4.2.5 Runtime Environment Protection

Runtime Environment Protection provides the granular security controls for node-based security and has a significant overlap with the user-based security controls in Application Features.

In many ICS environments, there are nodes that are dedicated to Operators who should onlyhave a process monitoring and control capability. Similarly, many ICS environments will haveView Only nodes that should never be used for control or process modification. The RuntimeEnvironment Protection is a method to configure security for all Users on the local iFIX node rather than to a specific User logged into the local iFIX mode.

Runtime Environment Protection must be enabled while in the Configuration WorkSpace. It is enabled in the Environment Protection tab of the User Preferences Dialog Box. Once enabled the protection can be configured for the local iFIX node. The iFIX Runtime Environment Protection features often applicable to Operator and View Only nodes include:

- *Disable Task Switching*: Prevent User from accessing 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. The Windows taskbar will be unavailable even when no User is logged into the iFIX application.

- *Disable Title Bar & Menu Bar:* Prevent User from exiting the Runtime WorkSpace and closing the current picture.

- *Disable "WorkSpace" Menu Pulldown:* A less restrictive set of controls than the disabling the entire menu bar. Select this if Users should be allowed to close and open Pictures but should not be able to switch from Runtime to Configuration WorkSpace.

- *Disable VBE Access*: Prevent User access to the Visual Basic Editor. Users are not able to create or modify scripts.

- *Disable <Ctrl><Alt><Del>:* Prevent User access to Ctrl-Alt-Del options thereby restricting accessing to the Task Manager, Shutdown, Log Off and Change Password.

- *Disable Open Accelerator:* This prevents access to a number of capabilities in the File menu including opening pictures and switching to the Configuration WorkSpace.

Want to Know More?

- See "Creating a Recipe User Account" in the *iFIX Configuring Security Features* guide.

4.2.6 iFIX Application Screen Saver Security

NOTE: This section is specific to Windows 7 and is not supported in iFIX 6.5 and later.

The iFIX application screen saver offers additional security controls over the Windows screen saver. It is often used on iFIX nodes that should remain logged in under a specific shared user account, such as an Operator account in a Control Room or an account with View Only privileges in a general access area.

If an Engineer, Administrator, or high privileged user logs into this node and fails to logout when finished, the iFIX application screen saver can automatically logout the high privileged user and login the intended standard account for the node.

Select the *Log out of iFIX* box and enter the credentials in the *After logging out, log in this user* area in the iFIX Screen Saver Settings dialog box, see Figure 9.

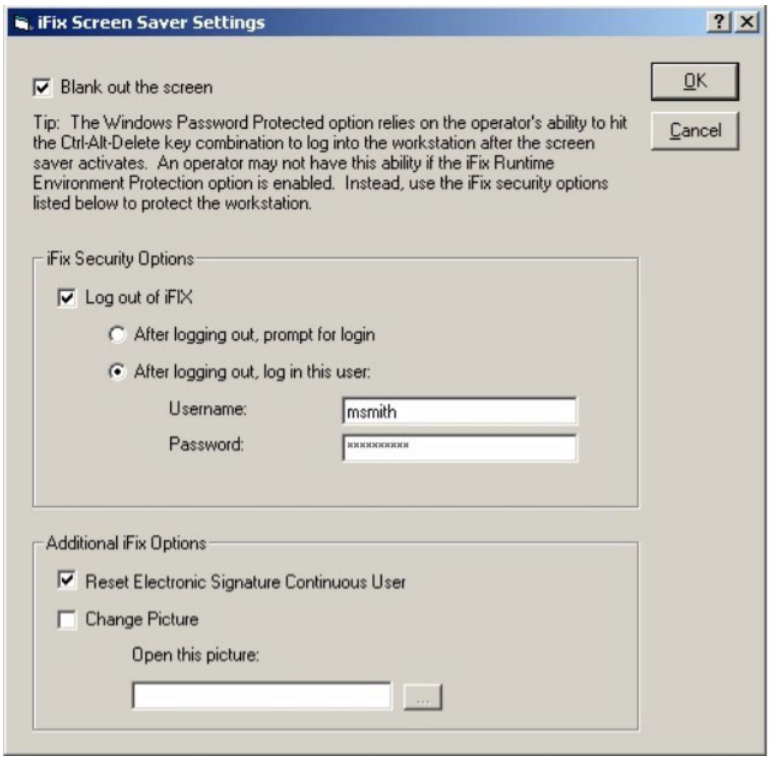


Figure 9: iFIX Screen Saver Settings

Care should be taken to ensure the iFIX and Windows screen saver settings and the CTRL-ALT-DELETE restrictions do not lock out Users that require access to the node.

4.3 Automatic Login

Each iFIX node can be configured to automatically login to iFIX in the Security Configuration Utility. The Application User must be specified when a node is set to automatic login. A System User must also be specified if the Security Synchronizer is used.

Automatic login eliminates iFIX user authentication and typically does not have any session timeouts. The node is available with the iFIX Application User privileges to whomever can physically access the node. Nodes with automatic login should be restricted to:

- Physically secure and manned locations where access control is enforced by physical security measures, such as a 24x7 manned control room. However even in this instance it is more secure to require User login.

- Nodes that have View Only or Local Control privileges and the Environmental Runtime Protections to make node misuse difficult.

The login to Windows is not affected by the iFIX Automatic Login. Automatic login to Windows at boot is set through Windows configuration.

The Startup Profile feature in iFIX can configure the iFIX node environment based on the Windows user name. This offers a single sign-on feature for iFIX, and it is often used when the iFIX client is accessed in a Terminal Server environment.

When starting, iFIX checks the currently logged in Windows user name to determine if the user has a profile listed in the Startup Profile Manager. If a profile is identified, iFIX loads that profile. Otherwise, the default profile is used if it is enabled.

Want to Know More?

See "Using the Startup Profile Manager" in the *Setting Up the Environment* document.

4.4 Electronic Signatures

While all process changes and alarm acknowledgements create a log event that includes theiFIX User logged into the node that performed the action, there are instances where additional user authentication is preferred or required including:

- Some industry regulations require additional authentication and verification prior to certain changes or alarm acknowledgements.

- Some asset owners require additional authentication and verification prior to high consequence changes or alarm acknowledgements.

- Some nodes are shared or accessible by multiple individuals who do not login / logout after each use of the node. In this case, electronic signatures can provide a record of what individual performed the action even if the User logged into the iFIX node is shared.

Electronic signature authentication and verification are applied to tags in the Advanced tab of the Tag's dialog box. The default setting is None (no electronic signature requirement). If electronic signatures should be required to write to the tag / perform a control action, then either the *Perform Only* or *Perform and Verify* check box should be selected, see Figure 10. Verify requires a second User to verify the action.

A tag can be configured to require electronic signatures for write actions to the tag, but not require authentication for alarm acknowledgements for the tag by selecting *Exempt Alarm Acknowledgement*.

Electronic signatures and verification can be optional or mandatory for each tag based on the *Handle Unsigned Writes* setting for a tag that was set to *Perform Only* or *Perform and Verify*. Settings of *Accept* and *Log* will allow a write to the tag even without User account authentication for the electronic signature. The default setting is to *Reject* the write if the User does authenticate when requested for the electronic signature and verification.

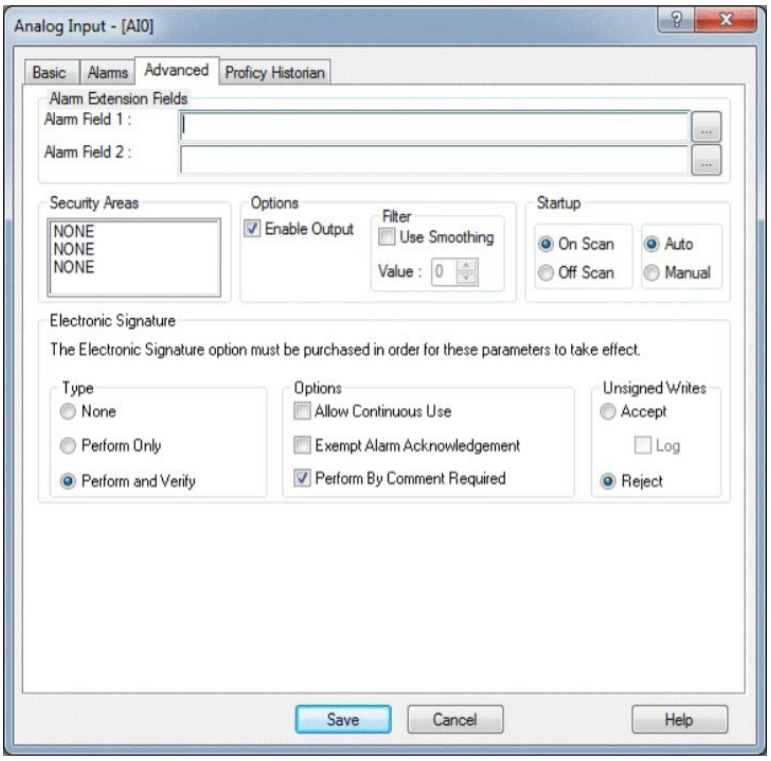


Figure 10: Configuring Electronic Signature on a Tag or Picture

4.5 Change Management

Note: Change Management Is no longer a GE Digital product.
The GE Digital Change Management add-on for iFIX can assist with managing iFIX project files and tracking changes to these files. In addition to controlling changes, it also provides useful information for after-incident analysis.

If the Change Management feature is purchased, then it is available in the iFIX ConfigurationWorkSpace for Users with the Change Management Application Feature. First, enable the Change Management Server connection from the *iFIX User Preferences* dialog box in the Configuration WorkSpace. Next, configure the login options that specify the Change Management Server to log into and the User credentials to use for the login.

To log in to the Change Management Server when iFIX starts up, select the Logon at WorkSpace Startup check box in the *Change Management User Preferences*, see Figure 11. Otherwise, with this check box cleared, you can right-click the node name in the system tree, point to Manage, and then click Logon. If the Prompt for User Name and Password at Logon check box is selected, the *Change Management Logon* dialog box appears.

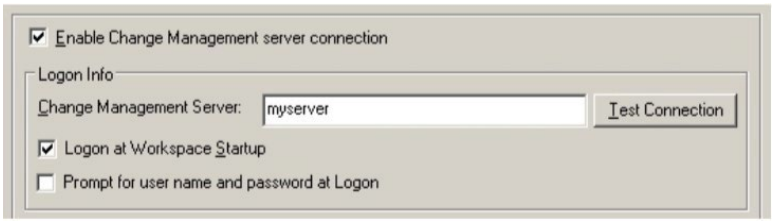


Figure 11: iFIX Screen Saver Settings

Right clicking on items in the Configuration WorkSpace System Tree will access the Change Management configuration for individual items.

Another useful security feature in Change Management is the ability to identify changes between the current system and what is expected based on Change Management. Change Management can perform a text compare of pictures (including VBA), process databases, Dynamos, SCU files, and user.fxg changes. This process can be combined with the periodic backup for a detection capability in cyber maintenance.

Want to Know More?

See the *Change Management and iFIX* document and *GE Digital Change Management* online help.

4.6 Security Logging and Alarm Routing

Security logging plays a part in cyber incident and attack detection and is essential for after-incident analysis. iFIX 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 161023.LOG contains the audit trail for October 23, 2016. If the Alarm ODBC Service is configured and the relational database, iFIX writes these messages to the relational database.

By reviewing the audit trail log file, it can be learned:

- When User accounts logged in and out (also available in Active Directory logs with Windows integration)
- Unsuccessful login attempts to iFIX (also available in Active Directory logs with Windows integration)

- When a user attempts to access a Security Area or Application Feature that the user did not have privileges to access

- When a User successfully or unsuccessfully generates an electronic signature or verification for a data entry or alarm acknowledgement action

- When a User exceeds the length of time allowed to remain logged in

Configuration changes, Operator actions and many other iFIX actions are logged, and these logs can also be helpful in detection and after-incident investigations.

Alarms can be assigned to one or more alarm areas. Each alarm area is configured to send alarms to specified alarm destinations. Operator and application messages can also be assigned to alarm areas and distributed to specified alarm destinations. This allows the iFIX administrator to determine what Users and nodes receive each alarm area.

SCADA Servers act as alarm servers and distribute alarms and messages over the network. Other nodes act as alarm clients and receive alarms. When you set up a SCADA Server to distribute alarms over the network, it sends the alarms and messages to every node that hasa session established with it.

A non-SCADA Server node that generates operator messages and system alarms directs those messages to SCADA Servers it has sessions with.

5 Server Connections

iFIX systems will often connect to external GE Digital servers to perform functions not supported by iFIX or better provided through GE Digital. GE Digital is a full featured product family, and only some of the more commonly used Servers such as an Historian or support for remote connection methods are covered in this section.

5.1 Proficy Historian

Proficy Historian is commonly used in the Control System Zone by Operators and Engineers to view data trends. ICS data from iFIX is also commonly pushed to a Proficy Historian in a Control System DMZ. From there it can be made available to users and applications on the Corporate Zone or other less trusted zone without providing direct access to the Control System Zone.

Small systems can run the Proficy Historian on the same computer as an iFIX SCADA Server node, but most installations should run a Proficy Historian on a dedicated server.The connection to the Proficy Historian is set in the *Configure the Proficy Historian Server(s)* dialog box.

iFIX nodes that are configured as a Proficy Historian collector will send specified process

data to one or more Proficy Historians. An iFIX collector establishes a TCP session to Proficy Historian on TCP port 14000. If the iFIX node and Proficy Historian are in differentsecurity zones, deploy the appropriate firewall rule to allow this communication.

Want to Know More?

See “Configure the Proficy Historian Server(s) Dialog Box” in the *Understanding iFIX* document and the *Historian e-book.*

5.2 Proficy Webspace

Proficy Webspace is a server-based, thin client solution that is optimized for reliable, secure, and scalable remote iFIX screen monitoring and control. Users access the Webspace Web Server, typically installed as an application on an iFIX SCADA Server node, using a web browser. This web client to web server communication can be protected using the encryption and authentication features available in SSL/TLS.

The most common and appropriate deployment case is to place a Proficy Webspace Server in a Control System DMZ to provide the ability to view process status via iFIX pictures.There are technical limitations and security concerns, described below, that make Webspace not an ideal solution for frequent remote control or for the process or remote configuration of iFIX.

Proficy Webspace supports the Runtime WorkSpace. If a thin client solution is requiredfor the Configure WorkSpace, then consider deploying a Terminal Server as described in Section 5.3. In addition, several configuration tools (such as Key Macro Editor, Visual Basic Editor, Startup Profile Manager, and others) will not open in the Proficy Webspace session.

Proficy Webspace does not support Runtime Environment Protection. Therefore, iFIX configuration must rely on the use of Application Feature and other User based security controls to restrict Webspace iFIX sessions. Use care when allowing application features that could allow write access, such as the "Database Save/Reload" and "Runtime Visual Basic Editor" features, as well as creating pictures with Datalinks, or any other means to write values into tags. It may be appropriate to create new pictures that have no write valueinto tags rather than using the identical pictures used by Operators in a control room.

Use Security Areas and Security Groups to further restrict access. Also, use care when creating and sharing schedules in iFIX, so that unintended VBA code is not activated inadvertently by web sessions.

All iFIX users that will login through Webspace must be configured for Windows authentication.

The Webspace application includes a whitelist feature, called Sandbox, that can restrict iFIX user access to files and programs on the Webspace Server. This feature requires manual editing of the WorkspacePropertyDefinitions.xml file (typically in the C:\ProgramData\Proficy\WorkspacePropertyDefinitions.xml folder) to add files and programs to the whitelist for a Webspace host installation. The Sandbox feature for files

and/or programs must be enabled before specifying whitelist entries.

Want to Know More?

See “Secure Deployment and Whitelisting” in the Webspace *Getting Started: Installation and Setup* document.

Administering User Accounts

To access applications on a Proficy Webspace server, clients must sign into the server machine. When users start a Webspace client, they are prompted for their user name and password. This information is optionally encrypted and passed to the Application Publishing Service running on the Proficy Webspace server. The Application Publishing Service then performs the login operation using the standard multi-user features of Windows.

When a user signs into a host and a domain is not specified, the service first attempts to authenticate the account on the local machine, followed by the machine’s domain, and lastly the trusted domains. Users can override this default behavior and specify a domain by typing the domain name followed by a backslash (\) and their network user name in the User name box of the Sign In dialog, such as NORTH\johng. When a local user name on the Webspace server is the same user name as a domain account, each with a different password, Webspace treats them as two separate accounts.

Once a user is signed in, Webspace relies on the server's operating system to provide the security necessary to run applications safely in a multi-user environment. Applications run inthe security context of the client user to ensure private sessions. Access to all machines and network resources is governed by the operating system and the rights granted to individual user sessions.

Users must be able to log in interactively (locally) on the Webspace server. Users must have local login rights in Local Security Policy, Domain Security Policy, and Domain Controller Security Policy.

Want to Know More?

See the *Getting Started, Installation and Setup, Proficy Webspace* manual.

5.3 Terminal Services

Microsoft’s Terminal Services can run the iFIX application in a DMZ to provide a more secureenvironment and make deployment easier.

The primary security benefit is that an organization can focus on securing a small number of computers running terminal services rather than every client computer. These Terminal Servers, typically located in a DMZ, can be scheduled for prioritized security patching and enhanced security monitoring.

An iFIX client node need only be installed and maintained on the Terminal Servers rather

than on each user computer in the Corporate Zone. The same iFIX User and node-based security controls described in Section 4 can be applied to iFIX installed as a terminal services application in a DMZ.

The iFIX client on the Terminal Server should not be a SCADA Server node that communicates with PLCs and other Level 1 devices. To disable SCADA in iFIX, go to the Security Configuration application's Configure menu, click SCADA to open the SCADA Configuration dialog box. In the SCADA support area, select Disable.

Consider using the Global Security Path feature so that all iFIX user sessions on the Terminal Server share the same security configuration. If not enabling Global Security Paths, individually configure security for each Terminal Server User.

The reference architecture, in section 2.5 Emergency Remote Access for Control and Administration, shows a Terminal Server being used for a remote-control capability from an untrusted zone in the case of emergencies. Organizations should examine the need for remote control and the risk of remote control and determine if it is prohibited to emergency use only, or allowed for some regularly occurring remote control. If remote control is allowed, the Terminal Server architecture represents the lowest risk method of providing this remote control.

There are numerous resources on how to deploy and secure Terminal Services, and there is nothing unique about using Terminal Services in iFIX that alters this guidance. Here are some main considerations:

- **RDP Full Connection vs. RDP Web Connection**
  RDP Full Connection offers encryption but is vulnerable to a man-in-the-middle attack if certificates are not deployed. Most organizations find that an RDP web connection, (as long as https, a web site certificate, and good web server securitypractices are used) to be more secure and easier for user interaction.

- **Changing the Default RDP/Terminal Services Port**
  Changing the default Microsoft Terminal Services Port (TCP/3389) can prevent automated attacks from identifying the Terminal Server but may not stop a skilled attacker.

- **Limit Terminal Server Access to Control System Zone with Firewall Rules**
  The firewall forming the security perimeter between the Support DMZ and Control System Zone limit Terminal Server access to servers and devices in the Control System Zone with a least privilege firewall ruleset.

Want to Know More?

See the *Using Terminal Server with iFIX* document.

5.4 Web HMI

Note: Web HMI is not supported by iFIX 6.5 and later releases.

GE Web HMI enables you to monitor and control production equipment and processes though a web browser based human machine interface (HMI) that is securely communicating to your SCADA system via an on-premises web server.

GE Web HMI presents information organized by an asset model with animated process diagrams called mimics associated with each asset type. A navigation hierarchy allows real-time views that can present summarized overview displays and allow rapid drill down into higher levels of detail for individual assets. For example, a real-time alarm visible at an overview level of the model can provide guidance to an operator to investigate more details of a specific asset that provides the data and control mechanism to resolve the alarm condition. See the security notes that are part of the Web HMI documentation for information about securing the Web HMI server.

6 Cyber Maintenance

The iFIX system and associated products, applications, and networks comprising ICS require maintenance just as physical equipment that is monitored and controlled in your physical process requires maintenance.

If iFIX components are installed and not maintained, they are operating in a “run to fail” maintenance plan. This maintenance approach is rarely recommended or used due to the failure unpredictability, increased outage times, and cost after failure. Without a cyber-maintenance plan, any cyber system degrades over time into a less secure and more fragile system. Therefore, it is essential to design and implement a cyber maintenance plan for youriFIX system.

This section covers some of the key elements of a cyber maintenance plan. Risk management teams must determine the specific requirements for each of these elements, particularly requirements related to frequency and time.

6.1 Backup and Recovery

CS has traditionally relied on redundancy, such as redundant servers, networks, and control rooms, to prevent a cyber incident from causing an ICS outage. Redundancy is typically not an effective control against a cyber-attack because the redundant system is identical to the primary system and is vulnerable to the same attack. Assume that a cyber-attack always takes out the primary and any redundant systems, and these systems must be completely rebuilt.

The appropriate level of management should set a Recovery Time Objective (RTO) for the iFIX system. The RTO should be based on a capability rather than on the entire set of computers, applications, and networks, and an RTO may vary for different functions of an ICS. For example, an organization may have an RTO of six hours to recover the ability to monitor and control a process using iFIX, and an RTO of 48 hours to recover the ability to

share historical data with the Corporate Zone.

The RTO may not require all systems of a specific type to be recovered. For example, a Control System Zone with redundant iFIX SCADA Servers, 15 iFIX Clients and redundant localarea networks (LANs) may have an RTO that requires a single SCADA Server, two iFIX Clients,and a single LAN to provide the required monitoring and control capability.

Once management has set one or more RTOs, then the recovery capability should be designed, implemented, and periodically tested. Very short RTOs are achievable, but in general, the cost of recovery increases as an RTO is decreased.

The first step in a recovery program is to make sure the necessary software and hardware is available. For iFIX, you need the software to rebuild the platform/OS, the software to install iFIX and associated Proficy applications, and iFIX project specific data. Implement a backup process and schedule and periodically check this process. The frequency of the backup is determined by a Recovery Point Objective (RPO), which also should be set by the appropriate level of management.

The RPO determines the amount of historical data and ICS configuration changes that management is prepared to lose. The RPO in an ICS is often longer than the RPO on a Corporate Zone computer because an ICS configuration typically does not change often, andimportant historical data is often exported from iFIX to the Proficy Historian or other storage in another security zone.

The RTO and RPO guide the decision on how to recover the iFIX nodes and other devices. For example, recovery can use back-up material, such as media, image, or a virtual machine,or it can involve connecting a cold standby server for a very short RTO.

Want to Know More?

See "Backing Up and Restoring Files" in *Understanding iFIX.*

6.1.1 Backup iFIX Project Data

The iFIX application includes a Backup and Restore Wizard, see Figure 12, that simplifies the process of backing up the data related to an iFIX project, and this wizard can be run periodically in a script to automate periodic backup. Select full backup to backup all iFIX project data that is needed to recover the system, such as tags, pictures, recipes, and security configuration.

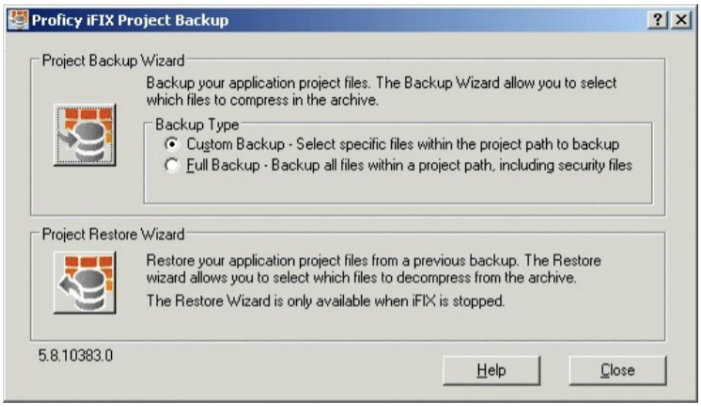


Figure 12: iFIX Project Backup Wizard

All iFIX nodes should periodically have an iFIX project data full backup stored off network so that a compromise of the iFIX system will not also compromise the backup files needed to recover. A good practice method to simplify this is to configure the Security Path, see Section 4.2.2, to store all backups in a directory structure on a File Server. Then this directory structure on a single server can be backed up and stored off network.

A full backup using the wizard will overwrite the previous full backup. Therefore, to ensure an unacceptable number of changes to iFIX are not lost, the iFIX full backup files on the File Server should be backed up and stored offsite at least as often as the RPO time.

6.1.2 Backup Entire System

To minimize downtime and speed recovery, perform full backups of each machine. Consider a backup software solution that provides encryption, verification, incremental backups, audit logging, and secure offsite storage.

Update the full system backups when patches are installed. Consider the availability of offline spare hardware as part of the backup solution, and the use of virtualized systems for an automation solution.

Many hardware virtualization platforms have their own backup issues to evaluate. It may bedesirable to perform back up operations at the host layer instead of at the guest OS layer. Review best practices for backups in virtualization systems in an automation solution. Virtualization provides the maximum flexibility for restoring machine images.

The key is the backup solution must be reliable and support the RTO. The shorter the RTO, the more important it is to look for solutions that speed the restoration process of the system

6.1.3 Restoration from Backup

The first step in recovering an iFIX node is to restore the OS and prepare the computer for installation of iFIX. Then the iFIX application is installed. This could be done as a new install as described in Section 3, but it likely will be faster if a full system backup, as described in Section 6.1.2, is used for restoration.

The iFIX license will need to be reactivated on the restored computer. This may not require any action if using a USB license key or an accessible license server. In other cases, it may require additional steps such as generating a license through GE Digital support or via the cloud.

Once the OS and applications are restored, then the iFIX data for the ICS can be restored using the iFIX Backup and Restore Wizard. Select *Use SCU file from archive* and *Delete all existing files under target project path before the restore* to do a complete restore of the iFIX project from backup, see Figure 13.

The ability to restore from backup should be tested periodically to ensure the backup is sufficient, confirm the skillset required to perform the restore, and confirm the RTO can be met.

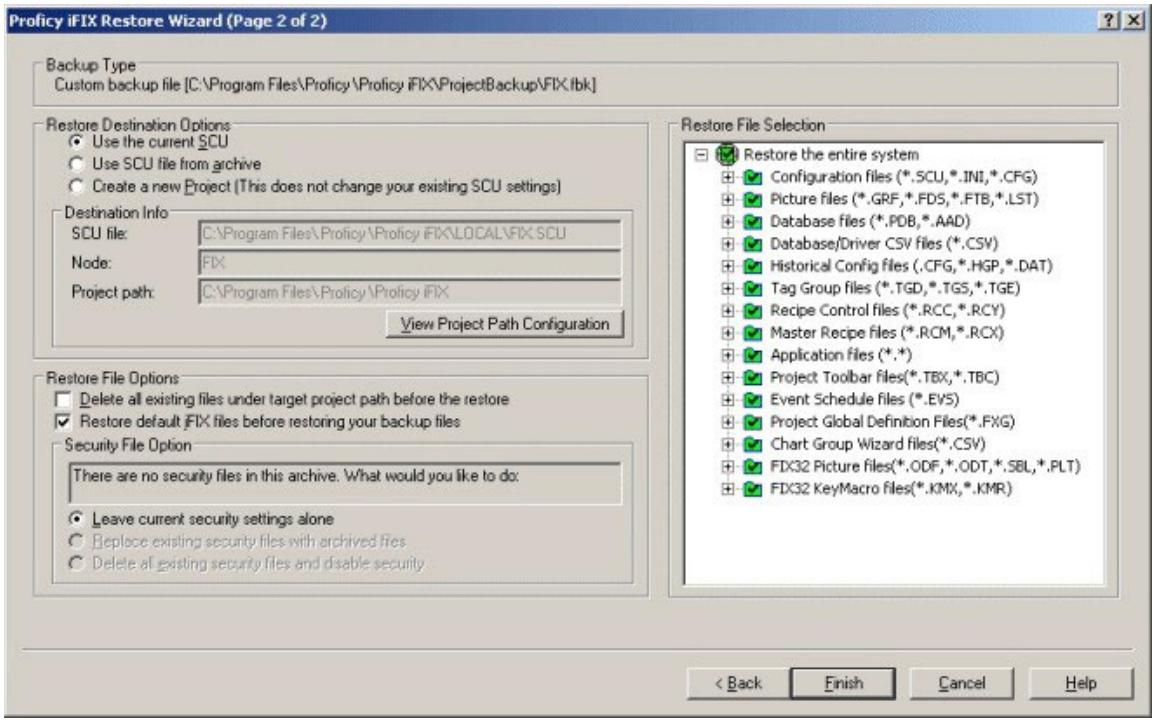


Figure 13: iFIX Restore Wizard

6.2 Security Patching and Software Updates

Cyber maintenance includes updating software to apply security patches and ensure the software is on a supported version. Create and maintain software inventory to assist with this aspect of cyber maintenance.

All software that runs on an ICS must be supported by the vendor. GE, Microsoft, and third-party application vendors who typically provide years of advance notice before declaring a version end of life/out of support. Annually review the end of life/out of support status of allsoftware. Develop and implement a plan to update the OS, iFIX, and other Proficy applications, and all required third-party applications before reaching end of life/out of support.

The frequency of applying security patches and updating software is a business and risk management decision. When making this decision, answer the following questions:

- Is the computer or device that is being patched accessible from a less trusted zone? In the sample reference architectures, see Section 2, first focus on security patching on computers and applications in DMZ, and then to the iFIX nodes in the Control System Zone sending data to applications in the Control System DMZ.
- Does the installation have a test system where the security patches are tested before deployment?
- Does the ICS have redundancy so that one instance of a computer or application can be patched while leaving the other instance as-is for a set time to verify that the security patch does not affect operations? Leveraging redundancy and applying security patches in phases significantly reduces the time of an outage in the rare case of a security patch problem.

Due to the testing and phased rollout required to prevent outages caused by security patch incompatibility, you may not be able to apply security patches once a month to the Control System Zone like you can in the Corporate Zone or DMZs. Consider different security patching frequencies for systems based on where they are accessed but ensure sure all software is patched periodically.

6.3 Periodic Project, User, Role and Resource Auditing

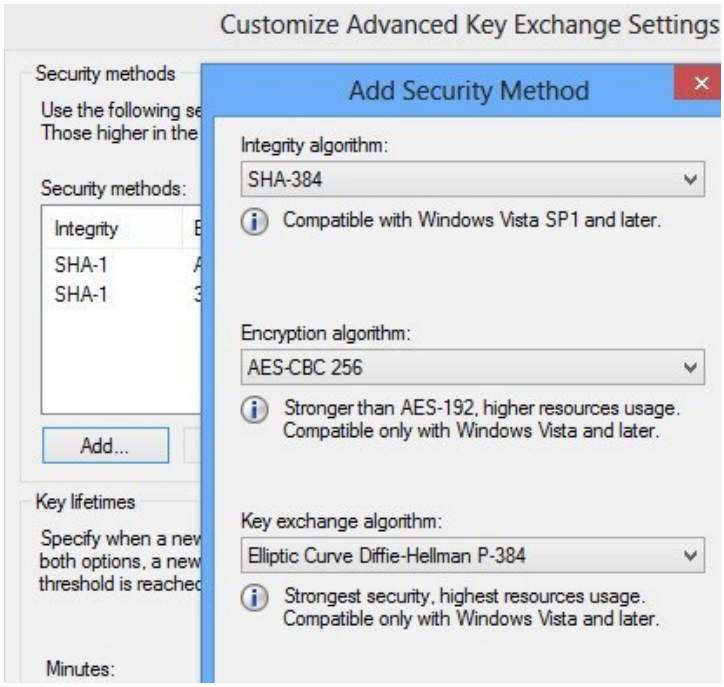
Section 4 discusses the security-related configuration decisions made for iFIX Users, Groups, Security Areas, Application Features and Runtime Environment Protection. The configuration of these items determines the security controls in the iFIX system.

The security posture of a system can degrade over time, particularly with User privileges. Users leave an organization, change roles, or require temporary privileges and other status changes that often are not addressed in an iFIX or Active Directory User management. Moretroubling are instances where a User is granted privileges without following the approved process.

A good security practice is to periodically verify, typically once a year, that all security settings have the correct controls, and the user management settings are up to date. If thereare significant variances between the actual settings and privileges and the expected settings and privileges, perform an investigation to determine how this gap occurred and which processes to enforce or change to prevent this in the future.

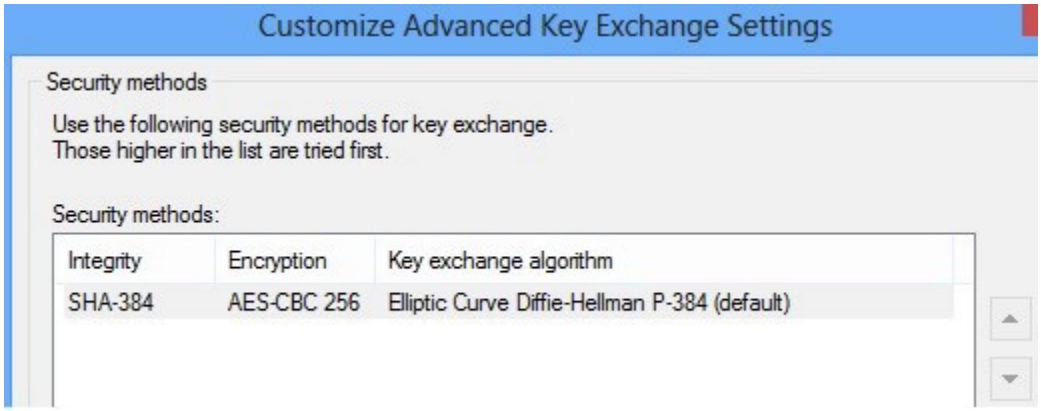
People, processes, and technology related to the security posture should also be periodicallyaudited to verify they are current and effective. For example, software and hardware inventory should be periodically verified. Another example would be verification of securityrelated audit logging and monitoring.

Appendix A: Configuration IPSEC

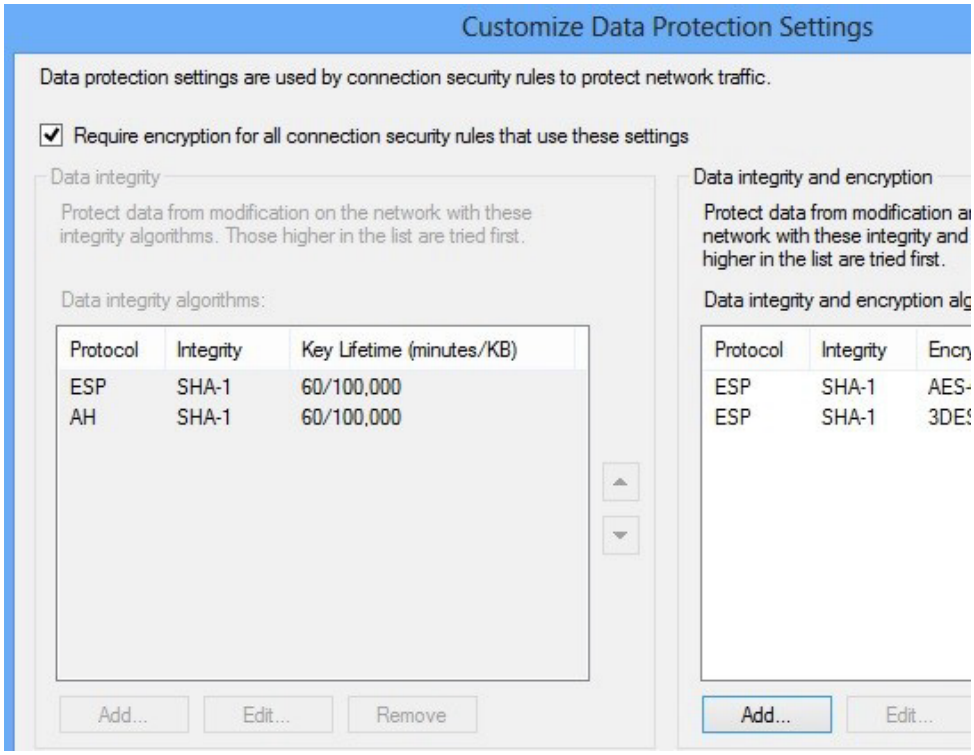


A typical example would be to set Integrity algorithm to SHA-384; Encryption algorithm to AES-CBC 256; Key Exchange algorithm to Elliptic Curve Diffie-Hellman P-384, and then clickOK.

1. Back in Customize Advanced Key Exchange Settings dialog box, move SHA-384… to top of list. It is recommended to “Remove” all other options, and then click OK.

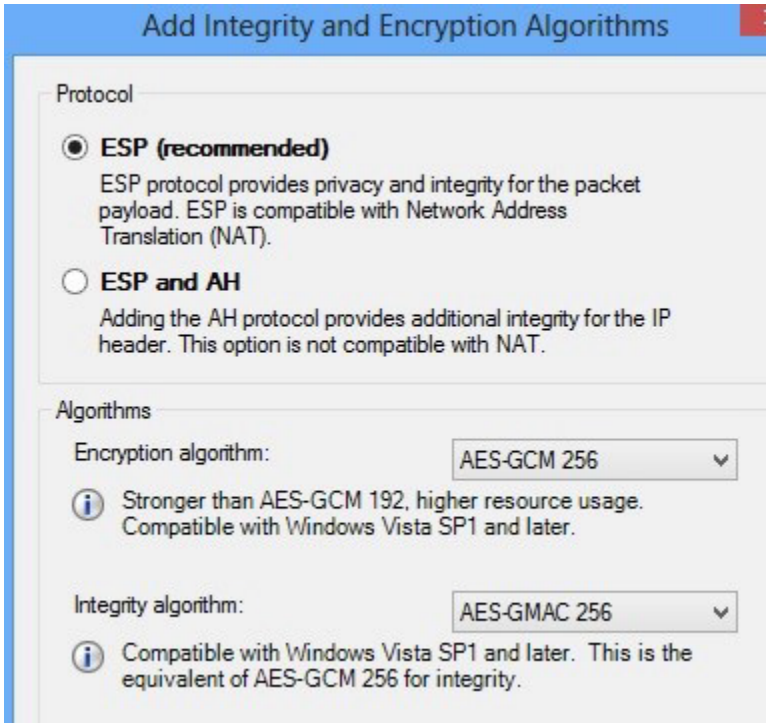


2. Back in Customize IPsec Defaults dialog box, in Data Protection (Quick Mode) area, select the Advanced option, and then click Customize.
3. In Customize Data Protection Settings dialog box, select the "Require encryption for all connection and security rules that use these settings" check box.
4. In Data Integrity and encryption area, click Add.

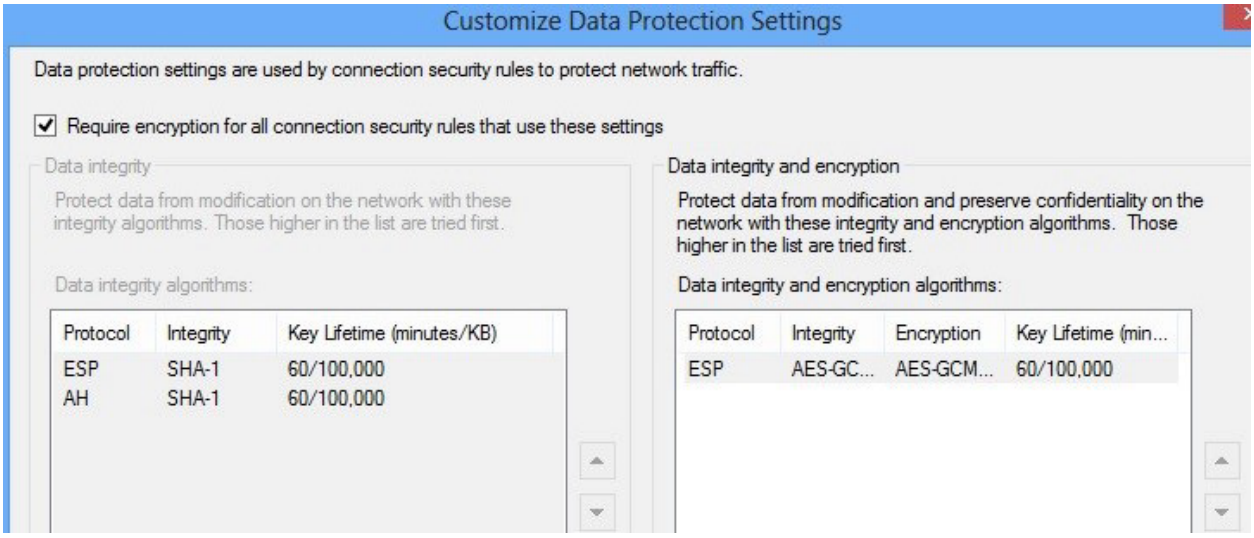


5. In Add Integrity and Encryption Algorithms dialog box, click the ESP option and set your desired Algorithms. For example, set Encryption Algorithm to AES-GMC 256; Integrity

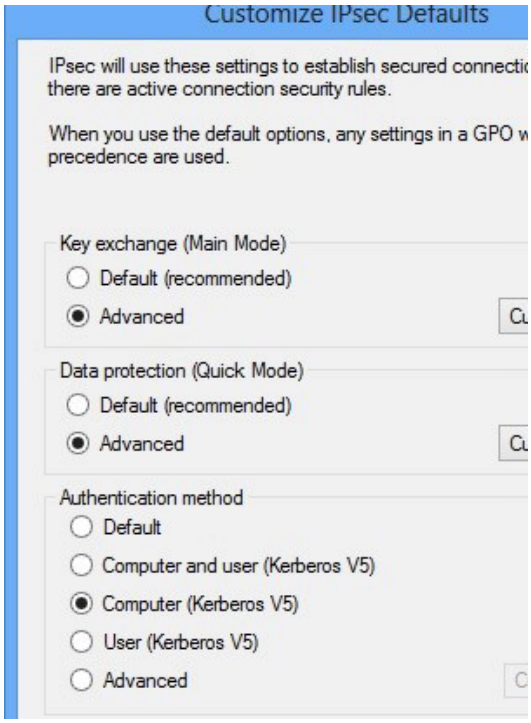
Algorithm to AESGMAC 256, and click OK.



6. In Customize Data Protection Settings, move ESP AES-GCM 256… to top of list. It is recommended to “Remove” all other options, and then click OK.

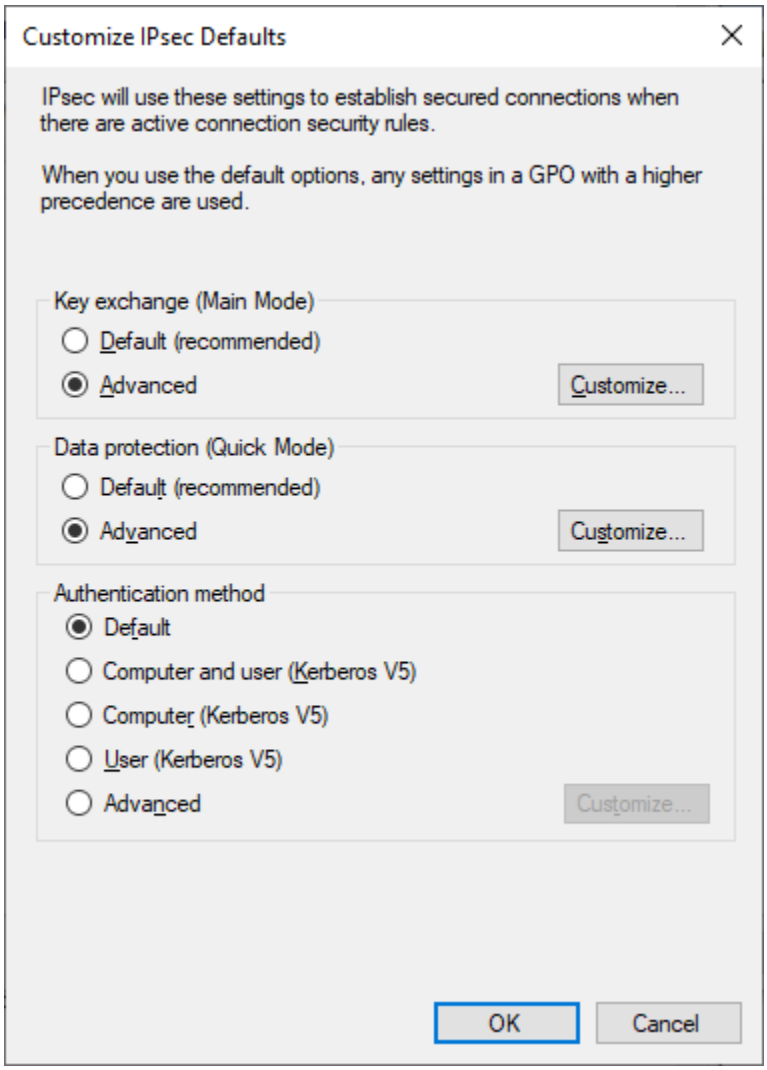


7. In Customize IPsec Defaults dialog box, in Authentication Method area, select desired authentication method (Kerberos V5 etc.).

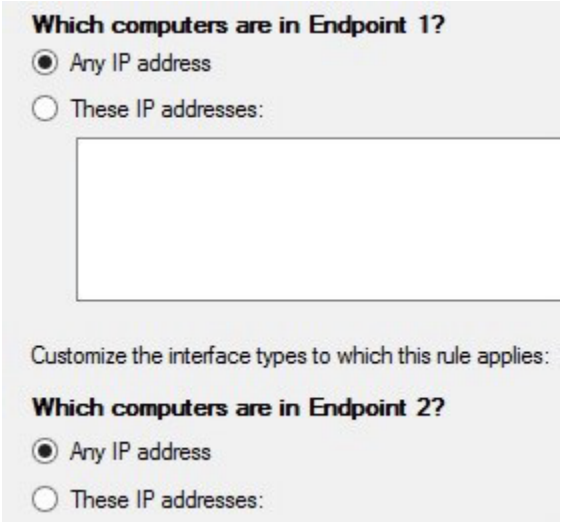


IMPORTANT: During testing, a pre-shared key was used. This is *not* recommended in a production environment. As an example, though, the next instructions described how to set a pre-shared key. Although, this is also where you would set your security "certificate" if you areusing that authentication method.

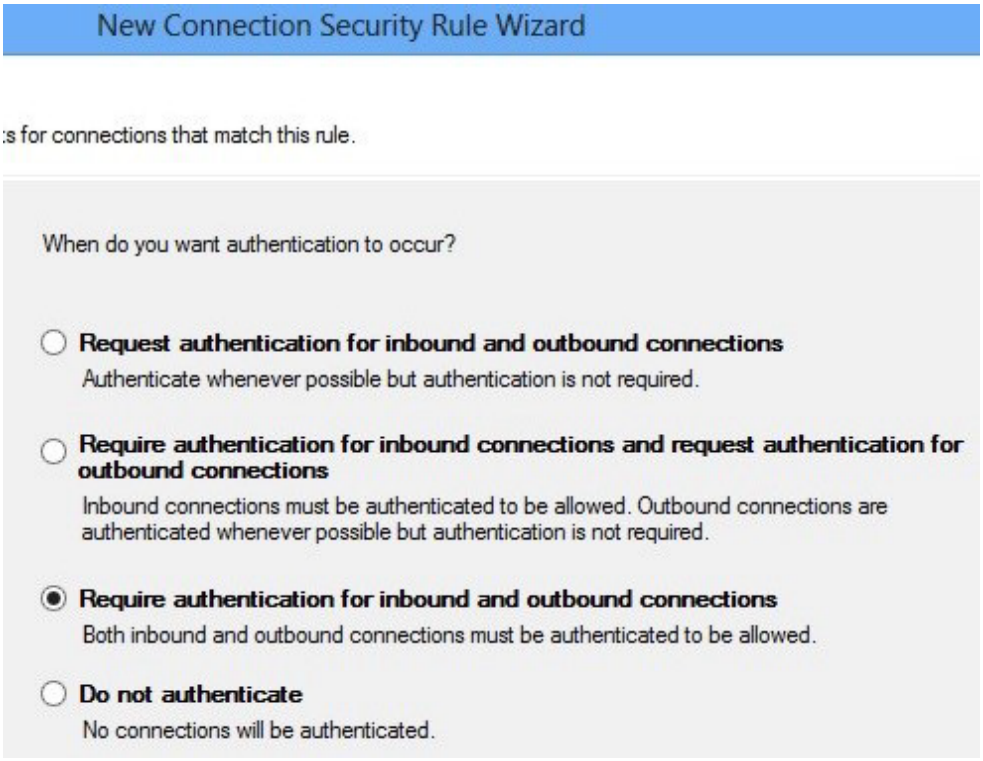
8. In the Authentication Method area, select the Advanced option and then click Customize.



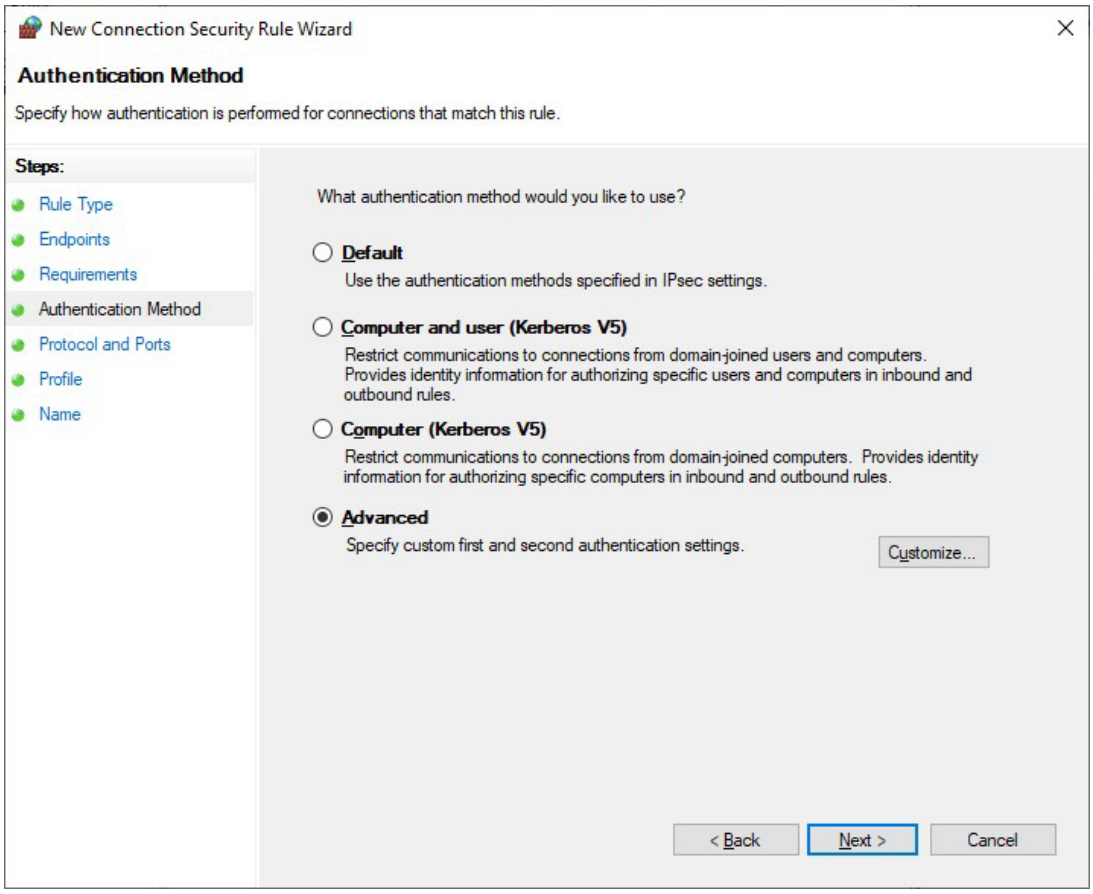
9. In the tree, select “Connection Security Rules” and then from the main menu select Action, and then New Rule to open New Connection Security Rule Wizard.
10. On Rule Type screen, select the Custom option and then click Next.
11. On Endpoints screen, select Any IP address option for both Endpoint 1 and Endpoint 2, and then click Next.



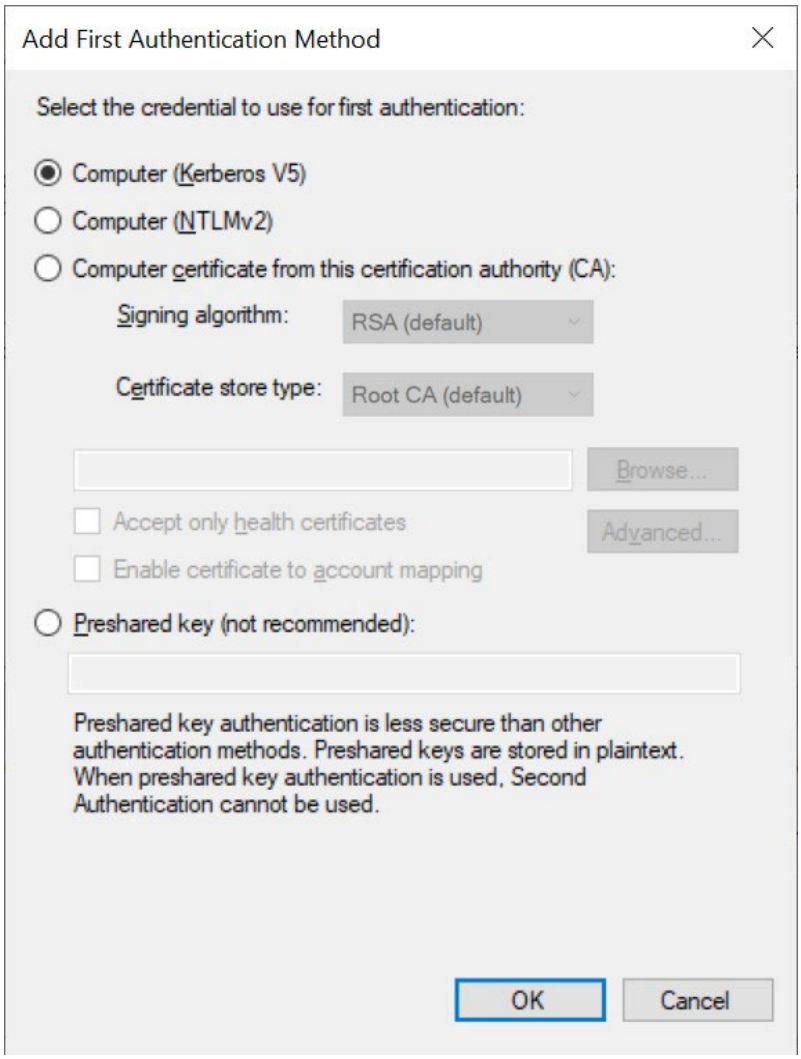
12. On Requirements screen, select the “Require authentication for inbound and outbound connections” option, and then click Next.



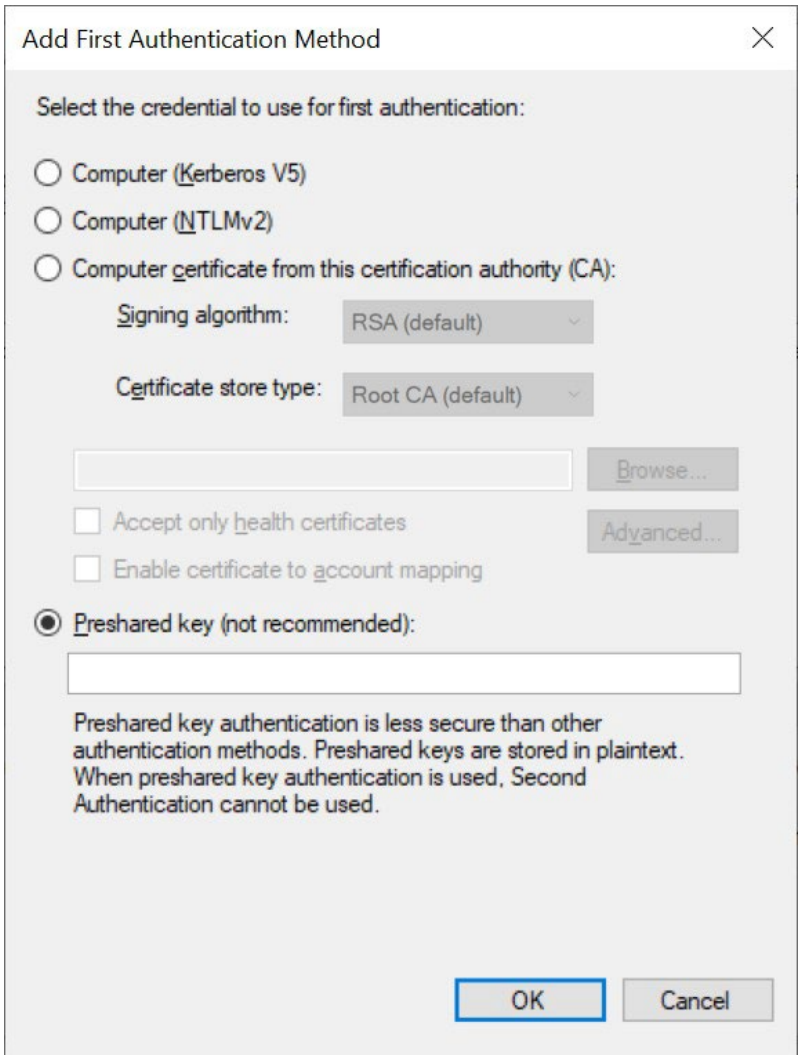
13. On Authentication Method screen, select the Advanced option and then click Customize.



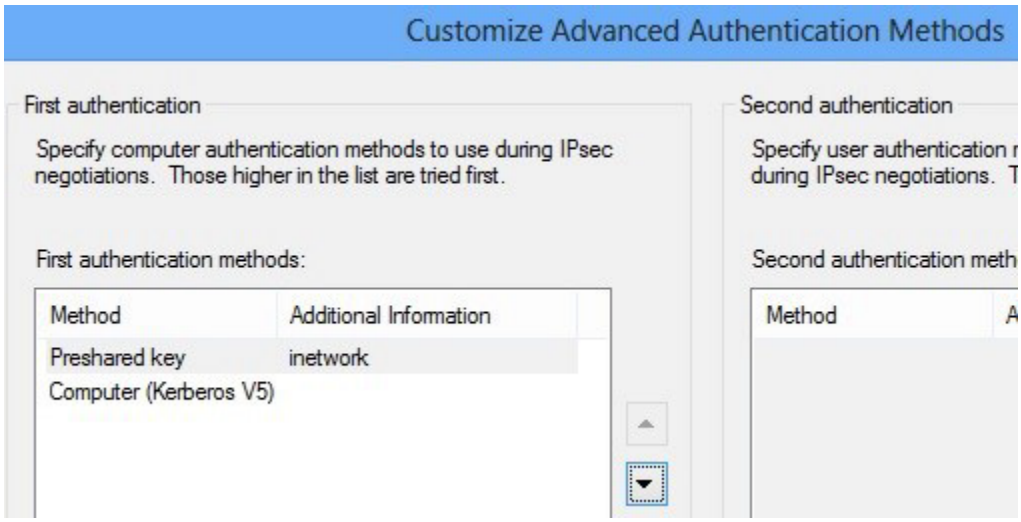
14. In Customize Advanced Authentication Methods dialog box, in the First Authentication methods area, click Add.



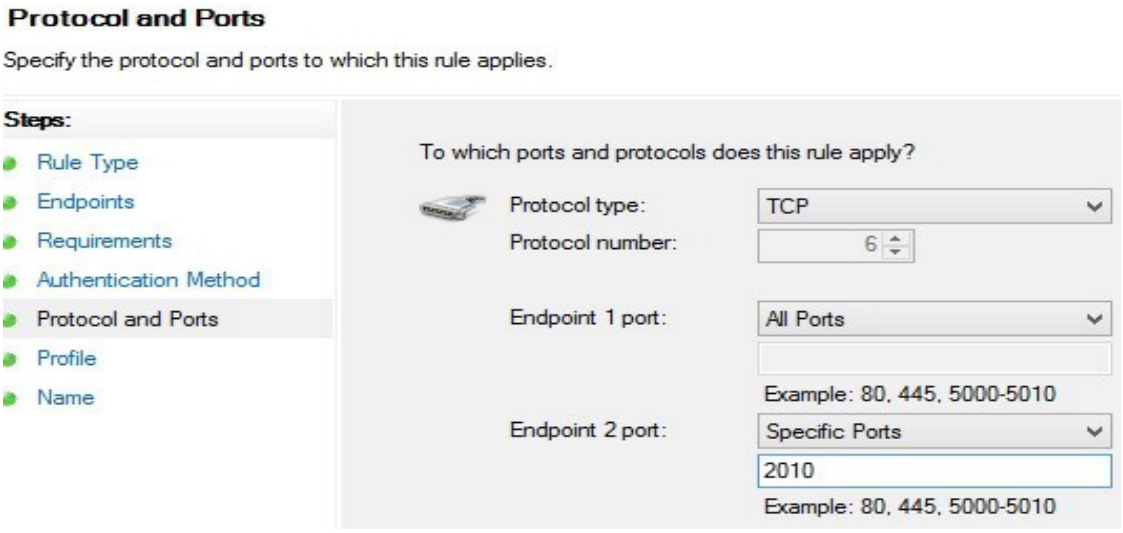
15. Select the pre-shared key option and enter any name. For example: inetwork, then click OK.



16. In the Customize Advanced Authentication Methods dialog box, move your desired method (in this example: pre-shared key) to top of list, then click OK.



17. Back in Customize IPsec Defaults dialog box, click OK. Return to Authentication Method screen, and click Next
18. On Protocol and Ports screen, set the Protocol Type to TCP; Endpoint 1 port to All Ports; Endpoint 2 port to Specific Ports and port 2010, then click Next.

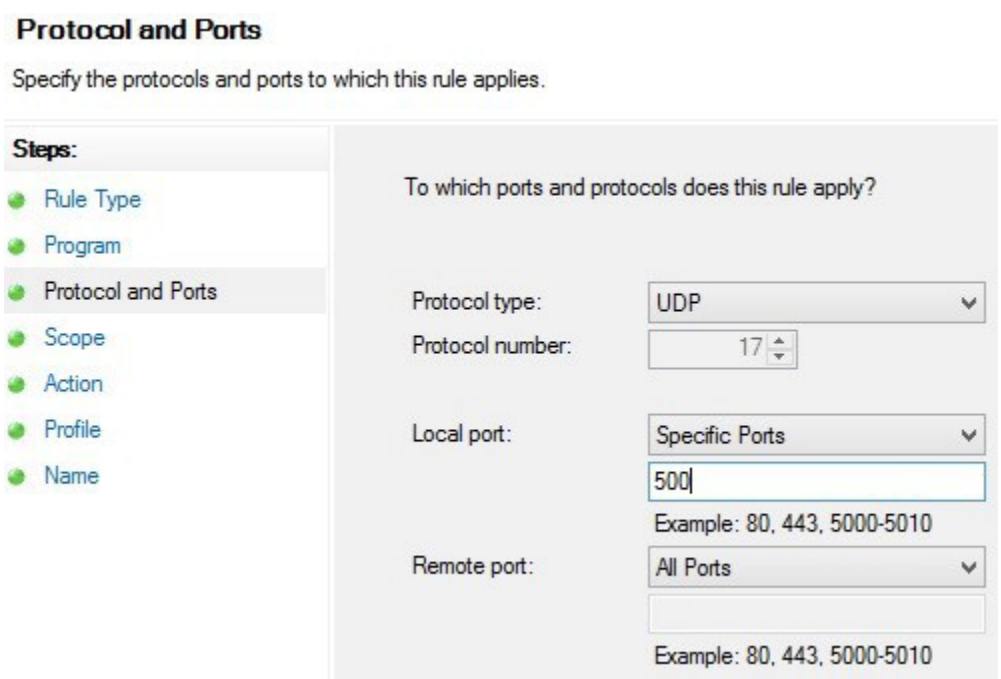


19. On Profile screen, select when to apply rule, as appropriate (Domain, Private and/or Public), then click Next.
20. On Name screen, enter any name, for example: iFIX Protocol, and optional Description, and then click the Finish button.
21. Confirm that your rule displays in the Connection Security Rules list. Confirm that the Enabled field is set to Yes. If not, right-click the rule and select Enable Rule.

NOTE:

When UDP is used for Enhanced Failover, you will need to open TCP port 53014 and UDP port 500. When TCP is used for Enhanced Failover (available as an option in iFIX 2023 or later), you only need to open TCP port 53014. If you have configured Enhanced Failover to use a different port, please update your TCP port accordingly.

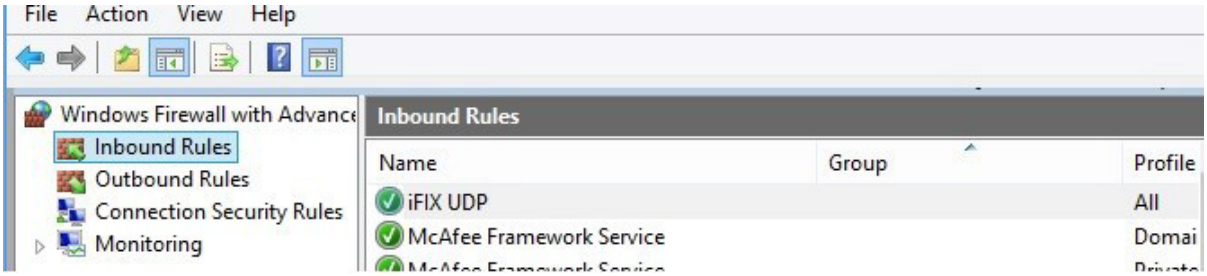
1. "Run" wf.msc to open Windows Firewall with Advanced Security.
2. In the tree, highlight Inbound Rules, and then from the main menu select Action, and thenNew Rule to open the New Inbound Rule Wizard.
3. On Rule Type screen, select the Custom option, and click Next.
4. On Program screen, select All Programs option, and click Next.
5. On Protocol and Ports screen, set Protocol Type to TCP or UDP; Local Port to Specific Ports to the specific port numbers (53104 for TCP and 500 for UDP), and then click Next.



6. On the Scope screen, select the Any IP address option for both Local OP and

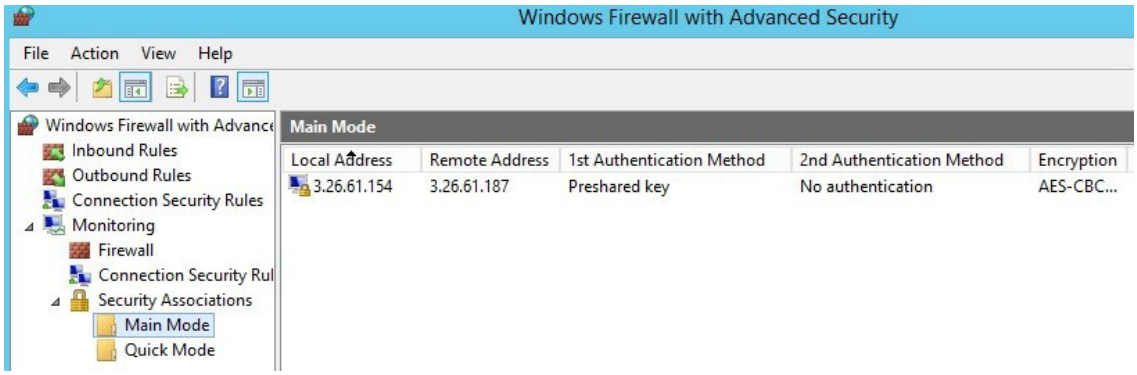
Remote IP, andthen click Next.

7. On the Action screen, select the Allow the Connection option, and then click Next.
8. On the Profile screen, select when to apply the rule as appropriate (Domain, Private and/orPublic), and then click Next.
9. On the Name screen, enter any name, for example: iFIX UDP, and optional Description, andthen click the Finish button.
10. Confirm that your rule now displays in the Inbound Rules list. Confirm that the Enabledfield is set to Yes. If not, right-click the rule and select Enable Rule.



To Verify that IPsec Cryptology is Being Used

1. Start iFIX on the SCADA node, and on the iClient/View node machines (or Proficy Webspace Client session).
2. On the SCADA and iClient/View node (or Proficy Webspace *server*), “run” wf.msc to open the Windows Firewall with Advanced Security application.
3. In the tree, in Monitoring > Security Associates, select Main Mode. Main Mode list box displays a line containing information about the connection.



4. Observe the results. If nothing is listed, and your view node (or Webspace client session) is displaying data from SCADA node, then your setup is invalid, and IPSec is not being used.

IMPORTANT: iFIX was tested with the default IPsec Key Exchange settings of SHA-1, AES-CBC 128, Diffie-Hellman Group2, and the default Data Protection settings of ESP, AES-CBC 128, SHA-1. This level of cryptology is believed to be compromised in real world attacks and is no longer

considered to be secure in a production environment. We also tested with more stringent and recommended IPsec Key Exchange settings of SHA-384, AES-CBC 256, Elliptic Curve Diffie Hellman P-385, and Data Protection settings of ESP, AES-GCM 256, AES-GMAC 256.