GE VERNOVA

PROFICY®SOFTWARE & SERVICES

PROFICY iFIX HMI/SCADA

Using Remote Desktop Services with iFIX

GE VERNOVA

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

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

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

All other trademarks are the property of their respective owners.

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

Table of Contents

Using Remote Desktop Services with iFIX

Using Remote Desktop Services with iFIX is intended for system integrators, IT administrators, and process control engineers responsible for setting up and optimizing your iFIX with Remote Desktop Services environment.

This help assumes familiarity with Microsoft® Windows® Server, Remote Desktop Services (Terminal Services) and/or Citrix® technologies including licensing, and your network environment.

IMPORTANT: Be aware, that starting with Windows Server 2008 R2, Remote Desktop Services was renamed Remote Desktop Services.

Reference Documents

For more information on iFIX, the System Configuration Utility (SCU), iFIX Security, and the iFIX Environment, refer to the following:

- Optimizing Your iFIX System
- Mastering iFIX
- Configuring Security Features
- Setting up the Environment

For more information on installing and configuring Microsoft Terminal Services, refer to the Microsoft Remote Desktop Services online documentation and the Microsoft Windows Server Help. To access the Microsoft Windows Help, position your cursor over any empty space on the Windows desktop and press F1.

Introduction to Remote Desktop Services

Remote Desktop Services allow you to centrally manage and execute iFIX. The Remote Desktop Services environment is a thin-client architecture where all application processing occurs centrally on the Server.

By installing a small piece of thin-client software from Microsoft or connecting through a Microsoft browser, thin clients are able to initiate and run individual instances of iFIX on the Server. Only graphic, keyboard, and mouse instructions are sent back and forth between the client and the Server, minimizing network traffic.

NOTE: Remote Desktop Services should only be used for Remote Desktop (Terminal Server Client) Connections to run iFIX in a remote desktop client session. Microsoft's Remote Desktop Connection is not supported for installing software. If you need to install software, use tools such as Team Viewer, VNC, or vSphere Web Client software.

Using Remote Desktop Services with iFIX provides:

Ease of maintenance – You can install one copy of iFIX onto the Server, allowing multiple users to run clients from the Server. Upgrades and SIMs only need to be installed on the Server.

Shared pictures – Each user accesses the same set of pictures. When one picture is changed, all users get the changes.

Remote access – Using the Remote Desktop Services Advanced Client (TSAC) or Remote Desktop Protocol (RDP), clients can connect to the iFIX Server/Remote Desktop Session Host and access iFIX through Internet Explorer 5.5 or higher.

Built-in RDP in Windows – Windows Clients can connect using Remote Desktop Protocol (RDP) and access iFIX through Internet Explorer.

Security – Data between the iFIX Remote Desktop Session Host and the client session is encrypted. There is also additional security between the client machines and the iFIX Remote Desktop Session Host.

Lightweight client machines – The iFIX Remote Desktop Session Host locally processes the software that the clients execute. Clients connecting to the Server do not need the processing power usually required to run iFIX. This allows clients running platforms from other Windows platforms to execute iFIX through Remote Desktop Services.

Specialized environments – Terminal Services allows you to tightly control user accounts. For example, you can configure a user account to start and execute a single program (iFIX). iFIX automatically starts at log in, and the user does not have access to the Windows desktop. When the user exits iFIX, he logs out of the Terminal Server account.

Handheld environments – Terminal Services gives you the ability to use wireless handhelds to display iFIX screens.

Controlled access to files – Using the Windows file protection, you can limit the directories users are allowed to access and modify. File protection also allows you to create safe and separate environments for developing and testing new pictures.

Using iClientTS

iClientTS™ provides a multi-session version of iFIX client software (iClient) that runs on a machine with Remote Desktop Services enabled. The multi-session environment allows multiple thin clients to log on to the Server and initiate individual sessions of iFIX. iFIX is not installed on the individual client machines, only on the Remote Desktop Session Host. The user's experience is nearly identical to running iFIX on their local node. From the client, it is not obvious that a user is in a Remote Desktop session. Virtually all iFIX client functions work including scripts, trending, alarms, and security. iClientTS also allows you to remotely support iFIX from any computer on your network or anywhere in the world.

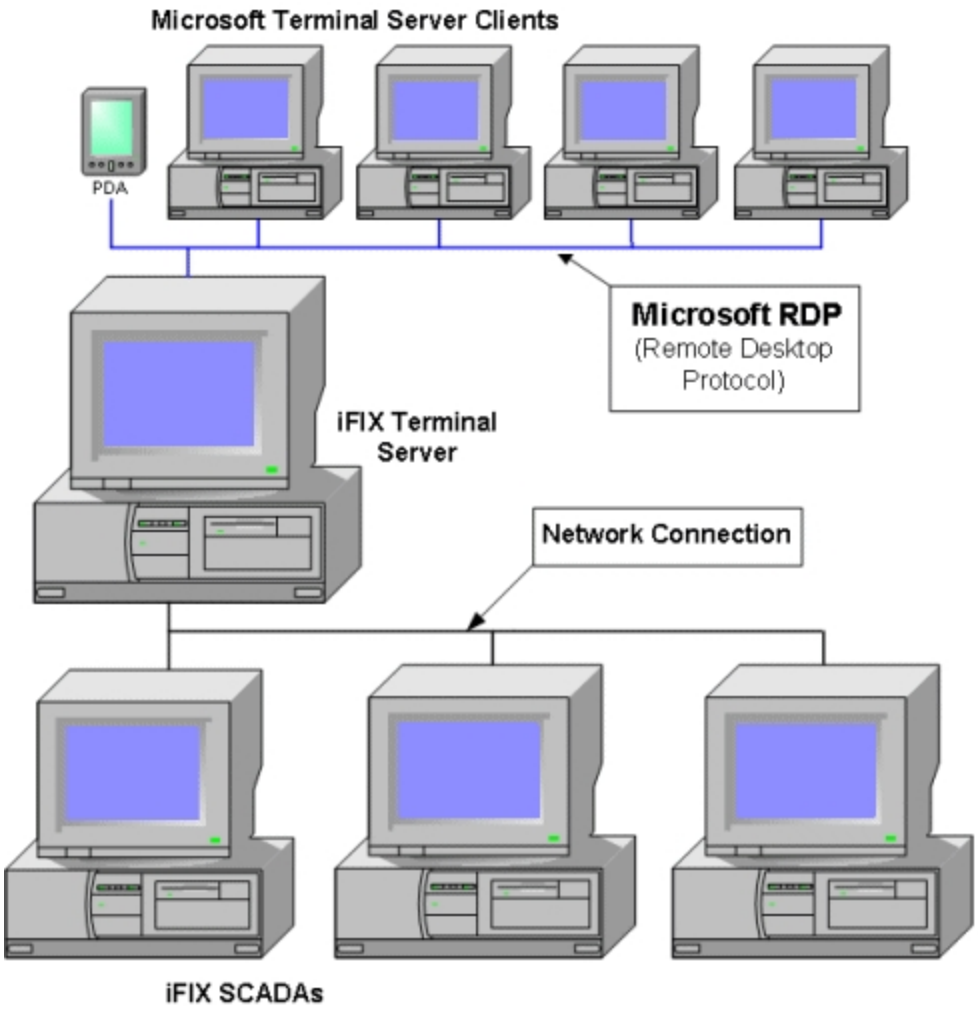
The following table compares iClient and iClientTS features.

Comparison of iClient and iClientTS

Feature	Standard iClient	iClientTS
Requires software on client	Yes	No
iFIX compatibility (Pictures/Schedules)	100%	100%
Picture navigation	Yes	Yes
Tag Group support	Yes	Yes
Write Access/Alarm ACK	Yes	Yes
Historical charts and Historical datalinks	Yes	Yes
VBA scripting	Yes	Yes
ActiveX support	Yes	Yes
Development/run time support	Yes	Yes
Color support	Unlimited	Unlimited for Windows Server with RDP 6.0 or greater Client
Runs in browser	No	Yes (IE)
Security	iFIX, Windows Server	iFIX, Windows Server
iFIX Environment protection	Yes	No
Runs applications requiring services in Windows	Yes	Yes (if iFIX is configured to run as a service)
Server platforms supported	Yes	Yes
Number of clients talking to a SCADA node	Each client = 1 connection	Each client = 1 connection
iFIX SCADA	Yes	Yes
Change Management	Yes	Not supported

Understanding the iFIX and Remote Desktop Services

iFIX with Remote Desktop Services allows multiple clients to run individual instances of iFIX from one Server. A sample iFIX with Remote Desktop Services environment, illustrated in the following figure, includes a Server, one or more iFIX SCADA nodes, and multiple clients.

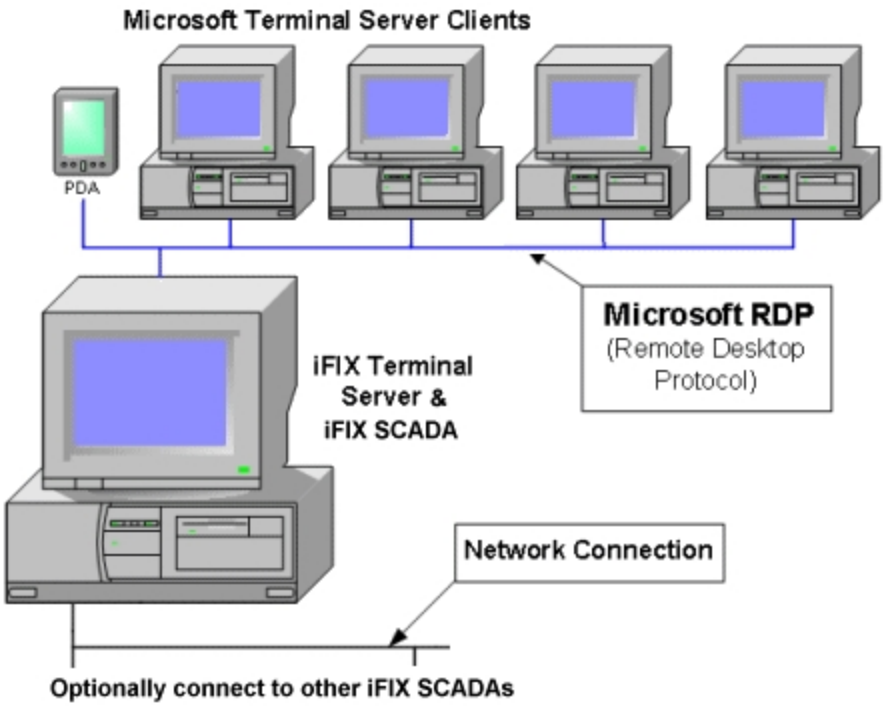


Sample 1: iFIX Terminal Server Environment

Thin clients access the Remote Desktop Session Host through Microsoft Remote Desktop Protocol (RDP) or Citrix Independent Computing Architecture (ICA) protocol. Each thin client accesses applications on the Server by connecting to the Remote Desktop Session Host machine either through an RDP client or ICA. No iFIX software is installed or runs on the thin client machine.

A separate session of iFIX runs on the Remote Desktop Session Host for each thin client. This allows very thin clients with minimal client-side resources to execute an individual instance of iFIX. The user's experience is nearly identical to running iFIX on their local machine. If you have clients and SCADAs in your iFIX with Remote Desktop Services environment, you can access and manage any of the SCADAs from a thin client. For example, from a thin client machine, you can build graphics, add tags, and change setpoints on a networked SCADA.

Another sample iFIX with Remote Desktop Services environment, illustrated in the following figure, includes a Remote Desktop Session Host that runs the iFIX SCADA server as a service on the same computer, and includes multiple Terminal Server clients.



Sample 2: iFIX Terminal Server Environment

For more information on the Remote Desktop Services environment, refer to the Remote Desktop Services Configuration Overview section of the Microsoft Windows operating system Help.

File System Support

Windows provides three types of file systems for disk partitioning: NTFS, FAT, and FAT32. It is recommended that you use NTFS with iFIX Terminal Server.

NTFS provides greater file-level security for users in a multi-session environment. For more information on file systems and configuring file system security, refer to the Choosing a File System section of the Microsoft Windows operating system Help.

IMPORTANT: Be aware that you can configure directory level security in NTFS and the Windows operating system. Use caution when doing so. Any enhancement to security that you make at the folder or directory level is not managed within iFIX. You must manage these security settings outside of iFIX.

Where to Find More Information on Remote Desktop Services

For the most up to date information on managing Remote Desktop Services, visit Microsoft's web site:

https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/welcome-to-rds

IMPORTANT: Be aware, that starting with Windows Server 2008 R2, Remote Desktop Services was renamed Remote Desktop Services.

Getting Started

Before installing iFIX on a Windows Server computer, you must enable and set up the Windows Remote Desktop Services. However, before you get started you should be aware of the iFIX Terminal Server limitations and software and licensing requirements. You should also spend some time planning a sound network and security strategy, and user and machine naming conventions.

This chapter describes the information that you need to know before installing and running iFIX with Remote Desktop Services. It includes the following topics:

iFIX and Remote Desktop Services Limitations

The following is a list of iFIX and Remote Desktop Services Limitations and assumptions:

- The Remote Desktop Session Host computer must have a supported version of Windows for Remote Desktop installed. For specific versions supported by iFIX (with Service pack mentions) refer to the System Requirements tab of the iFIX IPI.
- iFIX does not support running a Remote Desktop session on Windows Vista.
- Change Management is not supported from a Remote Desktop client session.
- Running iFIX on Windows NT 4.0, Windows 2000, or Windows 2003 is not supported.
- Remote Desktop Services does not solve the iFIX limitation of 200 iClients connecting to a single SCADA node.
- Running FIX32 and iFIX on the same computer is not supported on Remote Desktop Session Host.
- Although Windows allows machine names of up to 15 characters, iFIX node names are limited to eight characters.
- NETBIOS is not supported for connecting View (Remote Desktop Session Host computer) to SCADA.
- Depending on your settings, some keyboard shortcuts (such as Ctrl+ALT+DEL) may be disabled or remapped.
- Alarm printing at the client side is not supported.
- User accounts must be created and accessed after installing iFIX.

- When using iFIX with Remote Desktop Services and all clients share the same iFIX folders, toolbars can be configured separately on each client. Refer to the iFIX WorkSpace Toolbars and Remote Desktop Services section for more details.
- The iFIX Screen Saver does not work on Remote Desktop clients because Microsoft disabled screen savers for Remote Desktop sessions.

Scalability

The number of clients allowed per Server varies according to the Server's processing power and memory. iClientTS performance depends on the design of the application. If you use good optimization techniques and avoid unnecessary animations when developing your application, you should be able to run more clients with better performance per Server.

The Microsoft Performance Monitor can help you to determine the optimal number of iClientTS sessions your Server can handle. For more information on optimizing your iClientTS performance, refer to the Optimizing iFIX with Remote Desktop Services chapter.

TIP: Be aware that if your SCADA Server runs as a service on your Remote Desktop Session Host, your processor speed and optimization routines become even more important. Be sure to read the Optimizing iFIX with Remote Desktop Services section.

Hardware Requirements

iFIX with Remote Desktop Services - Less than 5 Clients

The following minimum hardware recommendations apply when using the iFIX and Remote Desktop Services on a low-end machine supporting less than five iFIX Terminal sessions, and iFIX projects with pictures that have a small amount of animation, shapes, and bitmaps:

- A 3.0 GHz Intel® Core™ i5 Processor or equivalent. For better performance, please consider using higher.
- SpeedStep® technology is not supported and must not be enabled.
- For time synchronization, the Windows Net Time and W32tm commands are both supported. However, if using the W32tm command, be sure to use the /nowait instruction when resynchronizing the clock. For example: W32tm /resync /nowait. The /nowait parameter instructs the operating system to make a stepping adjustment against the time server.
- The power save settings on your computer must be disabled. **Do not** use any power setting features that affect CPU clock speed.
- A minimum of 16 GB RAM. For better performance, please consider using more.

  NOTE: To use more than 4 GB of memory on a 32-bit platform you need to use Physical Address Extension (PAE). For more information on PAE please reference http://msdn.microsoft.com/en-us/library/windows/desktop/aa366796%28v=vs.85%29.aspxs
- A minimum of 40 GB of free hard drive space. It is strongly recommended that many GBs of additional free space exist on the hard drive to avoid performance issues.

  Be aware that iFIX alarm and historical data files grow dynamically. If you plan to perform extensive alarm or data collection on a node, you may need more disk space on that particular node.

- Other Proficy products, such as Plant Applications and Proficy Historian, impose additional requirements. Refer to the Important Product Information (IPI) topic in the product's electronic books for specific system requirements. Click the System Req. tab in that product's IPI for details.
- 100 MBit or faster Full Duplex TCP/IP-compatible network interface adapter for iFIX network communication between SCADA and Client nodes. Since the server bandwidth scales linearly with the number of clients connected, the speed of the network card on the server should be able to accommodate these connections.

  NOTE: iFIX does not support IPv6. If you disable IPv6 to use iFIX with Remote Desktop Services, make sure that your local HOSTS file does not contain any IPv6 references. For example, remove the "::1 localhost" lines from the HOSTS file, and replace them a line that references the IP address and the local host name (if necessary).
- One free direct-connect USB port. Some touch screens, pointing devices, and I/O drivers require a serial port. Additional ports for I/O hardware should be ordered with the computer.
- SVGA or better color monitor with a 24-bit (16,777,216 colors) graphics card capable of at least 1024x768 resolution.
- Two-button mouse or compatible pointing device (such as a touch screen) that is capable of opening a context menu.
- For best performance using iFIX in the Remote Desktop Services environment, please refer to iFIX Electronic Books, Optimizing iFIX for use with Remote Desktop Services

iFIX with Remote Desktop Services - Up to 25 Clients

The following minimum hardware recommendations apply when using the iFIX on a high-end machine that can support up to 25 clients:

- Intel® Xeon® Quad-Core Processor, running at 3.2 GHz or better. For better performance, please consider using higher. Be aware that the computer must be at least Quad-Core; a single core is not supported (with or without hyper-threading). Hyper-threading is also not supported on multiple core computers.
- SpeedStep® technology is not supported and must not be enabled.
- For time synchronization, the Windows Net Time and W32tm commands are both supported. However, if using the W32tm command, be sure to use the /nowait instruction when resynchronizing the clock. For example: W32tm /resync /nowait. The /nowait parameter instructs the operating system to make a stepping adjustment against the time server.
- The power save settings on your computer must be disabled. Do not use any power setting features that affect CPU clock speed.
- A minimum of 64 GB RAM. For better performance, please consider using more.

  NOTE: To use more than 4 GB of memory on a 32-bit platform you need to use Physical Address Extension (PAE). For more information on PAE please reference http://msdn.microsoft.com/en-us/library/windows/desktop/aa366796%28v=vs.85%29.aspxs
- A minimum of 40 GB of free hard drive space. Even after allowing for an extra GB for iFIX, it is strongly recommended that many GBs of additional free space exist on the hard drive to avoid performance issues.

Be aware that iFIX alarm and historical data files grow dynamically. If you plan to perform extensive alarm or data collection on a node, you may need more disk space on that particular node.

- Other Proficy products, such as Plant Applications and Proficy Historian, impose additional requirements. Refer to the Important Product Information (IPI) topic in the product's electronic books for specific system requirements. Click the System Req. tab in that product's IPI for details.
- 100 MBit or faster Full Duplex TCP/IP-compatible network interface adapter for iFIX network communication between SCADA and Client nodes. Since the server bandwidth scales linearly with the number of clients connected, the speed of the network card on the server should be able to accommodate these connections.

  NOTE: iFIX does not support IPv6. If you disable IPv6 to use iFIX Terminal, make sure that your local HOSTS file does not contain any IPv6 references. For example, remove the "::1 localhost" lines from the HOSTS file, and replace them a line that references the IP address and the local host name (if necessary).
- One free direct-connect USB port. Some touch screens, pointing devices, and I/O drivers require a serial port. Additional ports for I/O hardware should be ordered with the computer.
- SVGA or better color monitor with a 24-bit (16,777,216 colors) graphics card capable of at least 1024x768 resolution.
- Two-button mouse or compatible pointing device (such as a touch screen) that is capable of opening a context menu.
- For best performance using iFIX in the Remote Desktop Services environment, please refer to iFIX Electronic Books, Optimizing iFIX for use with Remote Desktop Services

Software Requirements

iFIX with Remote Desktop Services requires one of the following operating systems:

- Microsoft Windows Server 2022.
- Microsoft Windows Server 2019.
- Microsoft Windows 11.
- Microsoft Windows 10.

NOTE: It is highly recommended that you install the latest Service Pack and Windows Updates.

Licensing Requirements

It is recommended that you install your Remote Desktop Session Host on a computer that is not a domain controller. Make sure that you back up the terminal server licenses regularly, so as not to lose data.

For the most up to date Remote Desktop Services license information, visit Microsoft's web site.

iFIX Remote Desktop Clients

When a Windows Server client connects to the Remote Desktop Session Host with External Connector Licensing disabled, the license from the client is used. The first time that you connect to the Server, that license is activated.

External Connector Licensing was formerly known as Internet Connector Licensing. External Connector Licensing is not supported with iFIX. By default, External Connector Licensing is disabled on the Remote Desktop Session Host.

If you are running a non-Windows Server 2012 client computer, you need to purchase Windows Remote Desktop Services Client Access Licenses (TSCALs) from Microsoft. When you first set up the iFIX with Remote Desktop Services, you have a 120 day temporary license to run a maximum of 10 client machines from the Server. The first 10 Windows 9x and NT client machines that connect to the Server will reserve the licenses.

NOTE: Remote Desktop Services Client Access Licenses (TSCALs) are counted per device and are not concurrent.

WARNING: Once you activate a TSCAL, it is permanently associated with that machine. You cannot reboot the machine to clear your license use. If you reformat the machine, you must contact Microsoft to obtain a replacement license.

iClientTS Licensing and Keys

An iClientTS Hardware Key is required on the Remote Desktop Session Host computer to enable iFIX to run in Remote Desktop Session Host mode. No hardware keys are required on the thin client machines.

If you purchased iClientTS, you are responsible for ensuring that your licenses are used correctly. Using Remote Desktop Services capability, you can limit the number of incoming client connections to the number of iClientTS licenses that you have purchased. You can also use Remote Desktop Security and iFIX Security to limit the users who can initiate iClientTS sessions on the Remote Desktop Session Host.

If you have iClientTS licenses that enable a mixed environment of Developer, Run Time, and Read-Only users, your Hardware Key will be enabled for Developer use. To limit users to:

Run Time only – Implement iFIX security and authorize only the ability to use the WorkSpace Run-Time application.

Read-only – Select a single security area and apply this security area to all tags. Configure iFIX security so that read-only users are not authorized for this security area.

You can also limit your users to Read-Only capability by providing a user environment that does not provide any opportunity to change values. For example, you could use Data Entry Type = None for all data links when creating displays. Or when using Alarm Summaries, clear all of the items on the Operator tab in the Alarm Summary Configuration dialog box.

If you have iClientTS licenses that enable a mixed environment of Run Time and Read-Only uses, your Hardware Key will be enabled for Run Time use. To limit users to Read-Only, use the methods described above.

For more information on setting up your licensing system and iFIX Security, refer to the Configuring Security Features manual.

Hardware Key Licensing Considerations

All hardware keys distributed to run iFIX contain software to enable licensing for Remote Desktop client computers. For example, if you purchase a ten-client license, software embedded in the key enables ten concurrent client users, and prevents an eleventh client access to iFIX. When a client disconnects from Remote Desktop Session Host, the eleventh client can then access it.

NOTE: You still need enough TSCALs to license all the devices that will connect to the server. Be aware that even though you may have the appropriate number of iClientTS licenses enabled, if performance issues exist, you may not be able to connect.

Setting Up Windows Server for Remote Desktop Services

This section describes the configuration steps you need to enable and set up Microsoft Remote Desktop Services. These steps must be performed before you install the iFIX product. The Remote Desktop configuration steps include:

For Windows Server 2022 and 2019:

- Enabling Remote Desktop Services in Windows Server 2022 and 2019 for iFIX
- Activating a License Server in Windows Server Through the Internet

For Windows Server 2012:

- Enabling Remote Desktop Services on Windows Server 2012
- Activating a License Server in Windows Server Through the Internet

For more information, refer to the Remote Desktop Services section of the Windows Server Help.

Enabling Remote Desktop Services in Windows Server 2022 or 2019 for use with iFIX

It is recommended that you use Server Manager to enable Remote Desktop Services (Terminal Services). You must be logged in as an administrator.

The steps that follow explain how to install Remote Desktop Services (Terminal Services) on your Windows Server computer, and then install iFIX.

▶ To install Remote Desktop Service on a Windows Server computer:

1. Launch the Windows Server Manager. The Server Manager dashboard appears.
2. Select Manage from the toolbar on the top right of the screen. A drop-down menu appears.
3. From this menu, select Add Roles and Features.
4. If the Before you Begin screen appears, read the information and click Next.

   NOTE: You can confirm the destination server at any time by verifying the name of the destination server in the upper right hand corner of the wizard.
5. On the Select Installation Type screen, you are offered two options for installing roles and features. Select Role-based or Feature-based installation, and click Next.

6. On the Select Destination Server screen, select the server on which you want to install the Remote Desktop Services, then click Next. Destination options allow you to:
    - Select a server from the server pool. Use this option to select a server from the server pool on your local computer. Confirm the destination by verifying the destination server in the upper right hand corner of the wizard.
    - Select a virtual hard disk. Use this option to select a local or remote Windows Server virtual hard disk file. Only virtual hard disks that contain a Windows Server 2022 or 2019 operating system are valid destinations. Blank virtual hard disks or hard disks, which contain an operating system other than Windows Server 2022 or 2019, will fail.
7. On the Select Server Roles screen, click the check box for Remote Desktop Services, and then click Next. When you select a role, a description of that role appears in the rightmost pane.
8. On the Select Features screen, check one or more features to install on the server that you selected. Then, click Next. This installs Windows-defined features from the destination server. The Remote Desktop Services screen appears.
9. Read the Remote Desktop Services description, and then click Next.
10. From the Select Role Services screen, select the following five services, and then click Next:
    - Remote Desktop Connection Broker
    - Remote Desktop Gateway
    - Remote Desktop Licensing
    - Remote Desktop Session Host
    - Remote Desktop Web Access

    NOTE: Installing the above features window appears to add some features related to above services.
11. Click Add to add features. The Network Policy and Access Service screen displays.
12. Read the description on this page before clicking Next. The Select Role Services screen appears.
13. Accept the default selection, Network Policy Server, and then click Next. The Confirm Installation Selections screen appears.
14. Click Install. This screen displays the previously selected roles and features targeted for addition from the destination server. Additional options are available on the confirmation pane. A progress bar appears for this feature installation.
15. After the installation completes, click Close.
16. Restart your computer.

To install iFIX on the Remote Desktop:

1. Log on to the Remote Desktop (Terminal Server) as a member of Administrator group for the local machine.
2. Insert the iFIX installation DVD.

    NOTE: Follow steps 3-4 or just insert the DVD. The iFIX install selects the correct install mode.
3. From the Windows Control Panel > All Control Panel Items, select Install Application on Remote Desktop. The Install Program from Floppy Disk or CD-ROM screen appears.
4. Click Next. The iFIX startup screen appears.
5. Click Install iFIX.

    IMPORTANT: Do NOT click the Finish or Cancel button before the installation has ended.
6. When the product install prompts you to choose an install type, select Complete.
7. Follow through the rest of the installation.

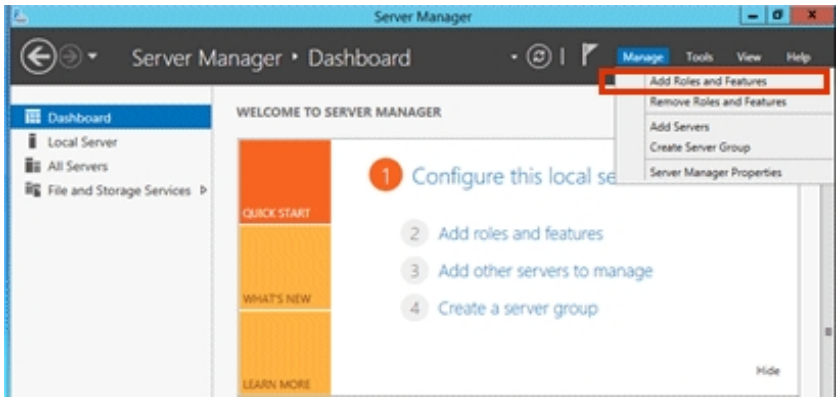
8. After the installation completes, on the Finish Admin Install screen, click Finish.
9. Restart your computer.

Enabling Remote Desktop Services in Windows Server 2012 for iFIX

The Server Manager in Windows Server 2012 allows you to select roles and features to install and configure the Remote Desktop Service (RDS).

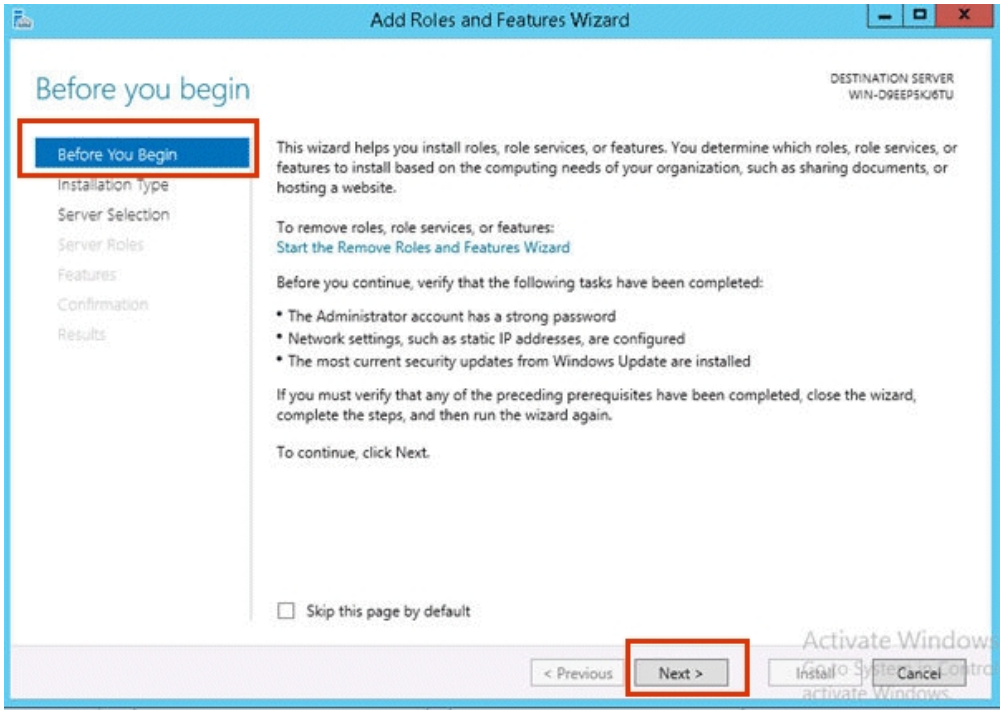
To install the Remote Desktop Service:

1. Launch the Server Manager. The Server Manager dashboard appears.
2. Select Manage from the toolbar on the top right of the screen.
3. A drop-down menu appears. From this menu, select Add Roles and Features.

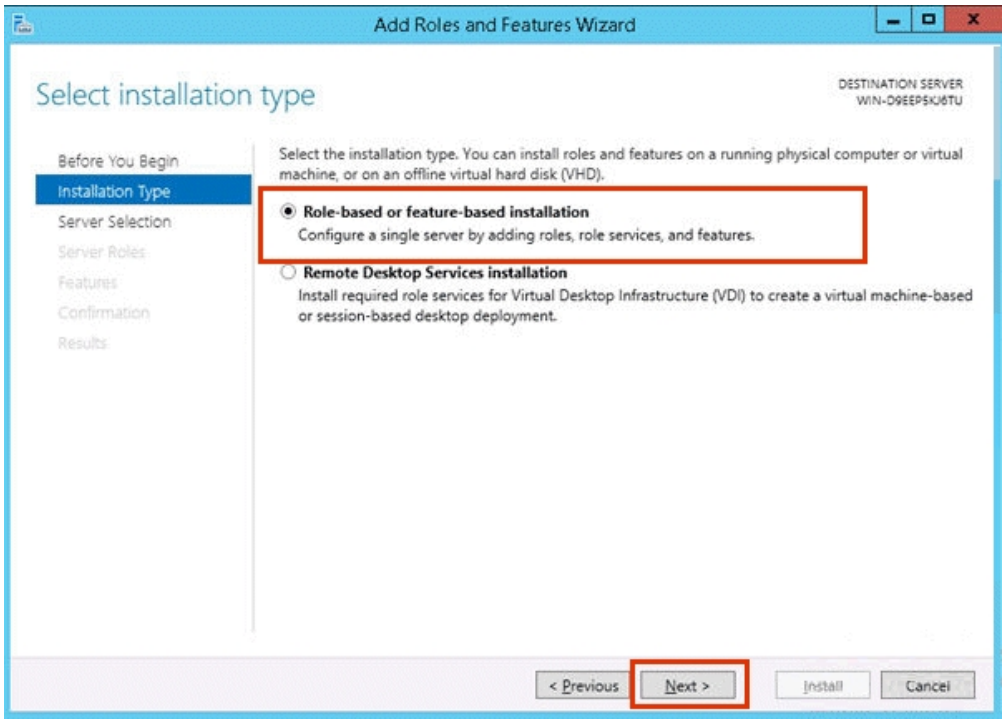


3. If the Before you Begin screen appears, read the information and click Next.

   NOTE: You can confirm the destination server at any time by verifying the name of the destination server in the upper right hand corner of the wizard.



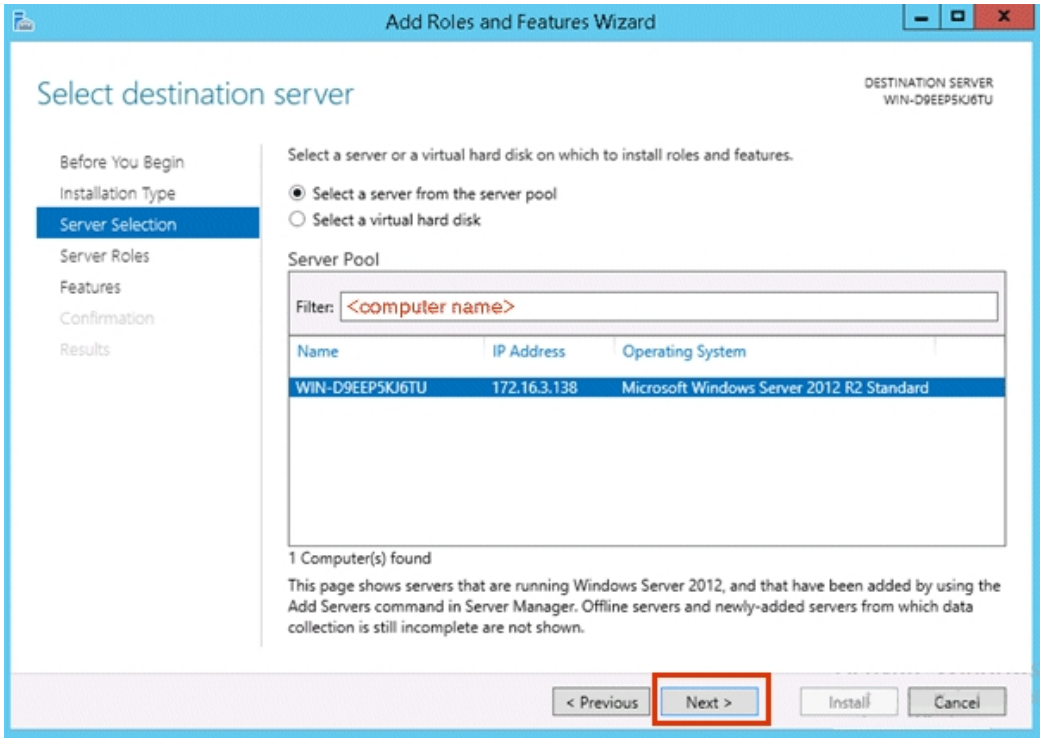
4. On the Select Installation Type screen, you are offered two options for installing roles and features. Select Role-based or feature-based installation. Click Next.



5. On the Select Destination Server screen, select the server on which you want to install the Remote Desktop Services, Then, click Next.

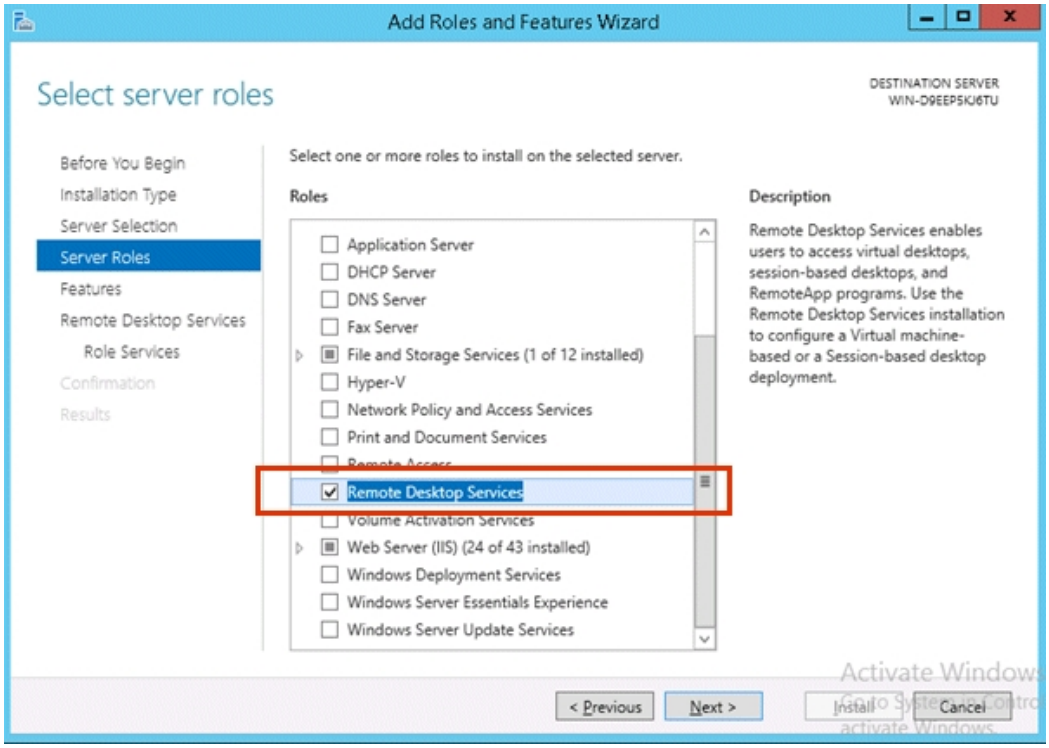
   Destination options allow you to:

- Select a server from the server pool. Use this option to select a server from the server pool on your local computer. Confirm the destination by verifying the destination server in the upper right hand corner of the wizard.
- Select a virtual hard disk. Use this option to select a local or remote Windows Server virtual hard disk file. Only virtual hard disks that contain a Windows Server 2012 operating system are valid destinations. Blank virtual hard disks or hard disks, which contain an operating system other than Windows Server 2012, will fail.

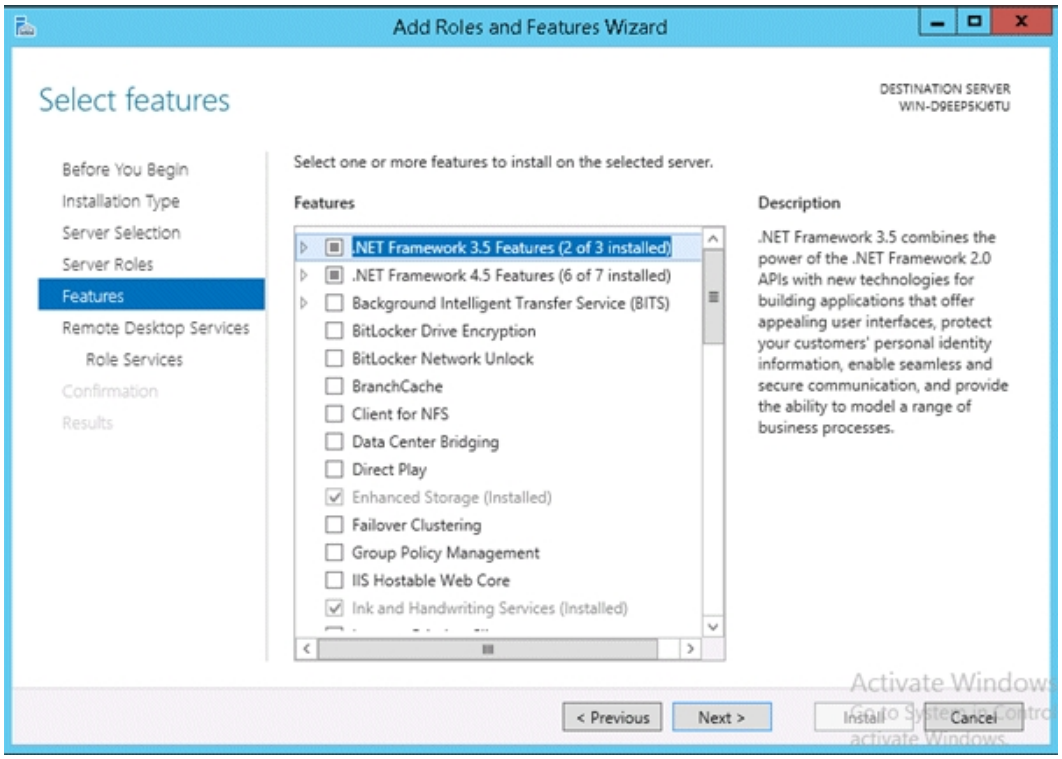


6. On the Select Server Roles screen, click the checkbox before Remote Desktop Services. Then, click Next.

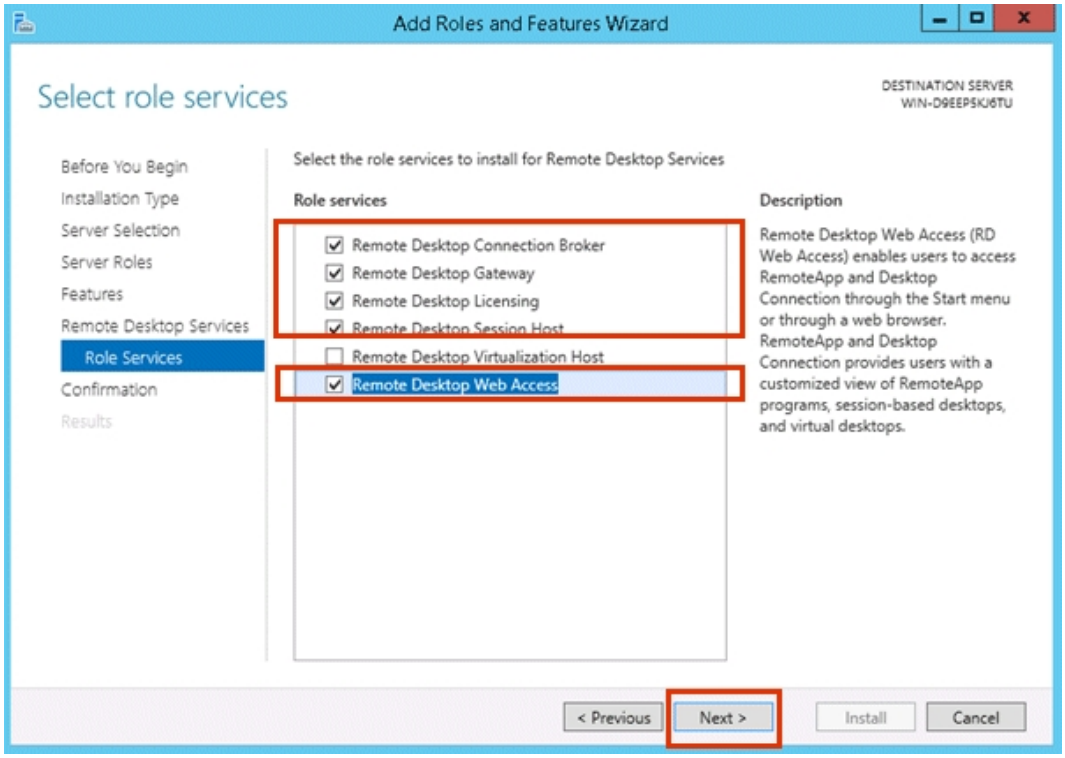
   When you select a role, a description of that role appears in the rightmost pane.



7. On the Select Features screen, check one or more features to install on the server you selected. Then, click Next.
   This installs Windows-defined features from the destination server.



8. The Remote Desktop Services screen appears. Read the Remote Desktop Services description. Then, click Next.
9. From the Select Role Services screen, select the following five services. Then, click Next.
   - Remote Desktop Connection Broker
   - Remote Desktop Gateway
   - Remote Desktop Licensing
   - Remote Desktop Session Host
   - Remote Desktop Web Access



10. The Network Policy and Access Service screen displays. Read the description on this page before clicking Next.
11. The Select Role Services screen appears. Accept the default selection, Network Policy Server, and then click Next.
12. The Confirm Installation Selections screen appears. Click Install.

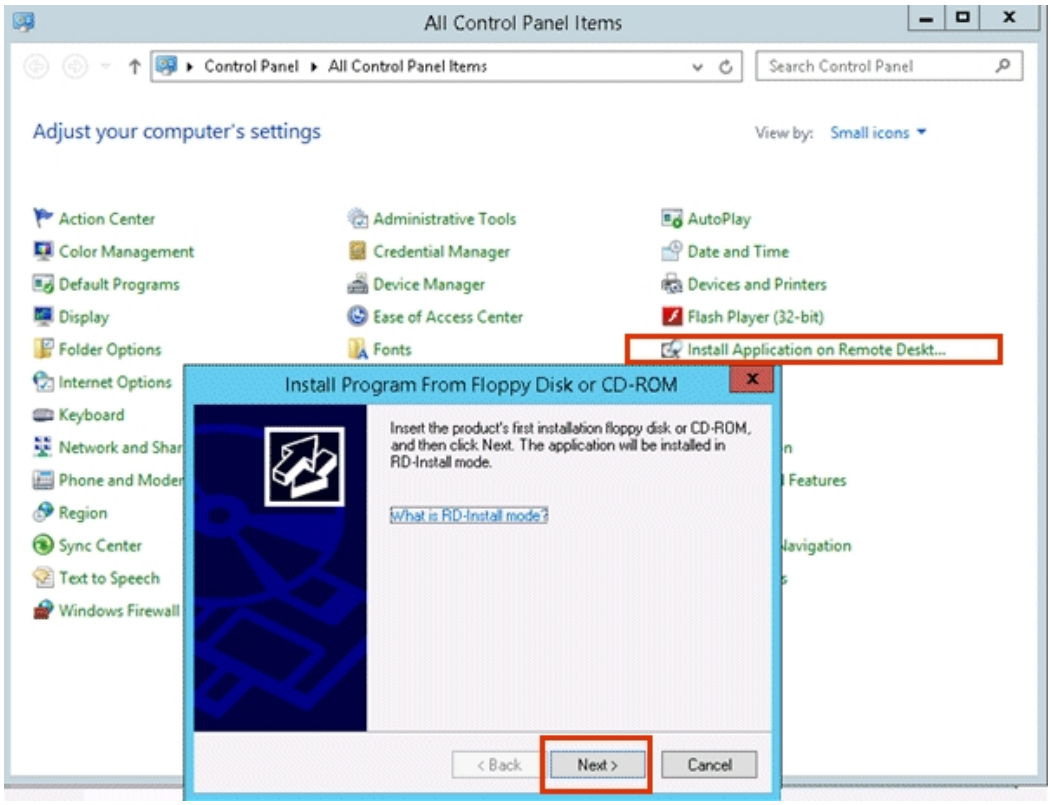
    This screen displays the previously selected roles and features targeted for addition from the destination server. Additional options available on the confirmation pane include:The roles, services, and features you have selected are install. A progress bar appears for this feature installation.

    a. When the installation completes, click Close.

    b. Restart your machine.

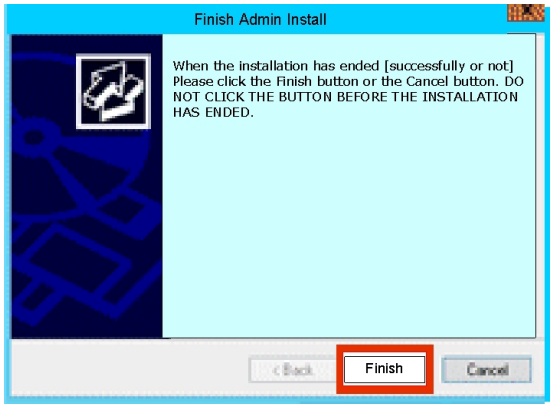
NOTE: Follow steps 13-14 or just insert the DVD. The iFIX install selects the correct install mode.

13. Navigate to Control Panel > All Control Panel Items. Select Install Application on Remote Desktop.
14. The Install Program from Floppy Disk or CD-ROM screen opens. Click Next.



15. The iFIX startup screen appears. Click Install iFIX.
16. When the installation completes, on the Finish Admin Install screen, click Finish.

    NOTE: Do NOT click the Finish or Cancel button before the installation has ended.



17. Restart your machine.

Activating a License Server in Windows Server Through the Internet

A license server stores all client licenses installed on a Terminal Server and provides a secure way of tracking the licenses that have been issued to Remote Desktop clients. You need to install the license server, activate it through the Microsoft Clearinghouse, and install license key packs onto the license server before issuing Remote Desktop (Terminal Server) client licenses. For more information on the license server, refer to the Client Services section of the Windows Server Help.

The following instructions allow you to activate the license server through the Internet. If you want to activate your server through telephone, fax, or World Wide Web, refer to the Windows Server Help.

To activate the license server through the Internet:

1. Open the Remote Desktop Licensing Manager.
2. Right-click the server you want to activate in the console tree and then click Activate Server. The Activate Server wizard starts.
3. On the Connection Method page, in the Connection method list, select Web Browser, and then click next.
4. On the License Server Activation page, click the hyperlink to connect to the Remote Desktop Services Licensing web site.

   NOTE: If you are running Remote Desktop Services Licensing Manager on a computer that does not have Internet connectivity, note the address for the Remote Desktop Services Web site, and then connect to the Web site from a computer that has Internet connectivity.
5. Under Select Option, click Activate a license server, and then click Next.
6. In the Product ID boxes, enter your Product ID. Your Product ID is displayed on the License Server Activation page of the Activate Server Wizard. Complete the name, company, and country/region fields. Specify any other information that you want to provide, such as e-mail and company address, and then click Next.
7. Confirm your entries, and then click Next. Your license server ID is displayed.
8. On the License Server Activation page in the Activate Server Wizard, enter the license server ID that you received in the previous step, and then click Next. Your license server is activated.
9. On the Completing the Activate Server Wizard page, do one of the following:
   - To install Terminal Services client access licenses (TS CALs) onto your license server, select the Start Install Licenses Wizard check box, click Next, and then follow the instructions.
   - To install TS CALs later, clear the Start Install Licenses Wizard now check box, and then click Finish.

Configuring Users to Use Remote Desktop Services

After adding users to Windows, you must grant them access rights to Remote Desktop Services. You can use the Computer Management Console in the Administrative Tools menu to provide users with access to the Remote Desktop Session Host.

To grant access to users for Terminal Server on Windows Server:

1. Open Computer Management tool.
2. From the System Tools tree, expand the Local Users and Groups options, click the Users folder.

3. Double-click the user you want to enable to log on as a Remote Desktop client in Windows.
4. On the Rrmote Desktop Services Profile tab, ensure that the Deny this user permission to log on to Remote Desktop Services is unchecked.
5. On the Member Of tab, add the group which allows Remote Desktop users.
6. Click OK out of all dialogs.

CAUTION: The Windows Logon Locally User Right introduces a degree of risk to your Server. To minimize the risk of unintentional or malicious modification to the Server, refer to the Security and Policies topics in the Microsoft Windows Help.

If you configured a user to automatically start a specific iClientTS session, you must prevent that user from starting a second Remote Desktop Session Host. Multiple sessions running the same node name or running multiple node names on the same network can cause connection not established errors. Refer to the Microsoft Knowledge Base for information on limiting a user's concurrent connections.

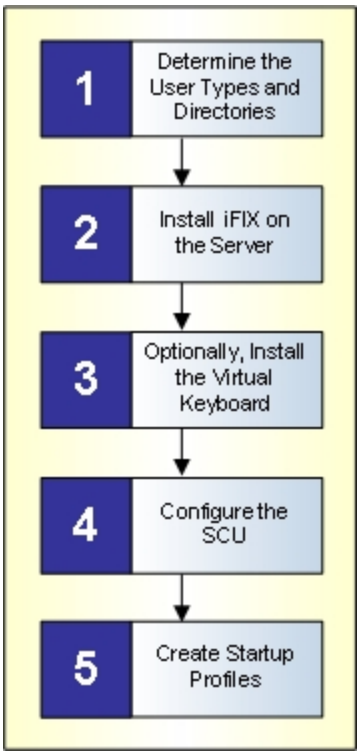
Installing and Configuring iFIX with Windows Remote Desktop Services

The following sections describe the steps you need to follow after enabling Remote Desktop Services and its licensing. For a description of the overview steps, refer to the Overview of the Remote Desktop Services Setup Steps section.

Refer to the Setting Up the Environment manual for more general details on iFIX setup information.

Overview of the Setup Steps for Remote Desktop Services

Once you have set up your Remote Desktop Services, perform the following steps described in the following figure. Click a block in the diagram to jump to that section.



Overview of iFIX Configuration for Remote Desktop Services

Step1: Determining User Types and Directories

This section describes actions you should consider when determining user types and directories for your iFIX application. These actions include:

- Planning User Types
- Planning SCU Directories for iFIX

- Planning Shared Directories
- Understanding Project Directory Paths

Planning User Types

Before defining your user types, determine what types of users you need. Which of your users will:

- Share the same preferences?
- Be able to configure their own historical collection settings?
- Work with recipes?
- Develop pictures?
- Have development rights?
- Have run-time rights?
- Work with one or more iFIX projects?
- Require additional directory permissions to be set outside of iFIX?

Anticipating the needs of your users allows you to successfully determine the configuration of your user types. For each user type, you will then create a project. You define projects paths in the iFIX System Configuration Utility (SCU). Each project can have multiple users. To define a profile for each user, use the Startup Profile Manager.

Planning SCU Directories for iFIX

Planning the directory paths for specific SCUs to provide enhanced or unique functionality per user type, thin client, or group, should be well planned. The design scheme for this type of implementation is similar to implementing the same scenario in a traditional environment (non TS) where SCU paths are using a mapped network drive on a file server. Careful planning is needed to prevent multiple users from performing conflicting actions, such as downloading recipes or modifying database values.

Incorporating iFIX security to limit applications and area access in the Remote Desktop Services environment is highly recommended. For more information on setting security options in iFIX, refer to the Configuring Security Features manual.

IMPORTANT: Be aware that if you configure directory level security in NTFS and the Windows operating system, to something other than the default, use caution when doing so. Any enhancement to security that you make at the folder or directory level is not managed within iFIX. You must manage these security settings outside of iFIX.

For each new project, by default, iFIX creates the following directory structure, unless you specify that the project use one or more shared folders instead:

Directory	Description
ALM	Stores the Alarm file and event log. Share this directory. This allows events from different sessions to be logged to the same .EVT files for simpler troubleshooting of iFIX under Remote Desktop Services. Do not allow more than one iFIX client to use Alarm File Services while sharing the ALM

	directory.
APP	Share or do not share this directory depending on user types and rights.
HTR	Stores Historical collection preferences. If more than one client will collect historical data, give each user a separate directory.
HTRDATA	Stores collected historical data. If clients view the same historical data charts, share the directory.
LOCAL	Stores the user-specific files including Toolbars, User preferences, .INI files, and the .SCU file. If your users are restricted to run mode, they can share the same directories. If your users require special user preferences or configure rights, create unique directories.
PDB	Stores the Database files. Schedules are also saved in this directory. If schedules are shared by clients, share this directory.
PIC	Stores pictures (.GRF), dynamo sets (.FDS), Global color tables (.FTB), and other files (.FXG). Generally, share this directory.
RCC	Stores recipe files. For run-time users, share the directories. Create unique directories for developers or restricted nodes.
RCM	

You can share directories outside the project, instead of creating each of these directories within the same project path. For instance, you may want all projects to share the C:\Program Files (x86)\Proficy\iFIX\PIC path, so that all users share the same pictures, but have different project paths for the other folders. For instance, you may create projects for iFIX operators (C:\Program Files (x86)\Proficy\iFIX\Operators) and supervisors (C:\Program Files (x86)\Proficy\iFIX\Supervisors) that share the PIC path in C:\Program Files (x86)\Proficy\iFIX\PIC, but retain separate folders for all other settings.

Planning Shared Directories

For each project, it is recommended that certain types of users only share specific directories. The following table outlines these recommendations.

User Types and Directories to Share

Project	Project-Specific (Unshared) Directories	Shared Directories	Example User Type
Run Time Only	LOCAL	PDB, PIC, APP, HTR, HTRDATA, ALM, RCM, and RCC	Operator
Run Time with Historical Collection	LOCAL, HTR	PDB, PIC, APP, HTRDATA, ALM, RCM, and RCC	Supervisor
Special Alarming Run Time	LOCAL, ALM	PDB, PIC, APP, HTR, HTRDATA, RCM, and RCC	Supervisor
Development	LOCAL, PDB, PIC, APP, HTR, HTRDATA, ALM, RCM, and RCC	None. Developers should have all unique directories except for NLS and the BASE path, which should always be shared.	Developer

Refer to the Planning SCU Directories for iFIX section for descriptions of the different iFIX directories.

Understanding Project Directory Paths

If you are using iFIX Project Configuration with Remote Desktop Services, make sure that the Base and Language Paths are the same for each project. The locations of the project paths can differ, depending upon the user type. However, the Base and Language Paths should be the same for each project.

For instance, if you leave the Base and Language set to the defaults, the Base is set to C:\Program Files (x86)\Proficy\iFIX and the Language is set to C:\Program Files (x86)\Proficy\iFIX\NLS for each project.

Step 2: Installing iFIX

IMPORTANT: Installing or uninstalling iFIX via a remote desktop connection or through a Remote Desktop session is not supported.

To install iFIX:

1. Log on to the Terminal Server as a member of the local machine's Admin group.
2. From the Windows Control Panel > All Control Panel Items, select Install Application on Remote Desktop.
3. Insert the iFIX installation DVD.
4. Click Install iFIX in the iFIX installation program screen.
5. When the product install prompts you to choose an install type, select Complete.
6. Continue through the installation.
7. Restart Windows.

Installing iFIX over an Uninstall

If you used Uninstall to uninstall a previous version of iFIX, note that Uninstall does not delete all of the shipped toolbar files. For example, Uninstall does not remove any files from the LOCAL directories created for Remote Desktop clients.

Only the files in the main LOCAL folder and the LOCAL folder under the SampleSystem directory are deleted automatically.

Running iFIX as a Service on the Remote Desktop Session Host

If you plan to run iFIX as a service on the Remote Desktop Session Host computer, you need to configure the iFIX SCADA Server to run as a service in the System Configuration Utility (SCU). To do this, shut down iFIX, log in as an Administrator, and open the Local Startup Definition dialog box from the SCU's Configure menu by clicking Local Startup. Select the *Run iFIX as a Service* check box. This check is unavailable when iFIX is running. Restart iFIX to apply your changes. For more information about configuring iFIX to run as a service, refer to the Running iFIX as a Service section.

IMPORTANT: Be aware that if your SCADA Server runs as a service on your Terminal Server, your processor speed and optimization routines become even more important. Be sure to read the Optimizing iFIX with Remote Desktop Services section.

If you want to configure other tasks, such as scheduler events (with the FixBackgroundServer.EXE), to run as a service in the background, you need to configure these tasks in the SCU's Task Configuration dialog box. For more information on task configuration, refer to the Configuring Startup Tasks section. When iFIX starts as a service, these tasks will also start as services.

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

Additionally, when you run iFIX on the Remote Desktop Session Host, you should Enable SCADA support in the SCU. To do so, on the SCU's Configure menu, click SCADA to open the SCADA Configuration dialog box. In the SCADA support area, select Enable. For more information, refer to the Enabling SCADA Support section.

TIP: When iFIX runs as a service on the Remote Desktop Session Host, for each SCU used by a Terminal Server client, Disable SCADA support.

Step 3: Installing the Virtual Keyboard on Remote Desktop Session Host and Clients

iFIX provides a virtual keyboard that allows you to work in touch-screen environments or to use a mouse to enter passwords and other data. Install the virtual keyboard on the Server to make it available to each client licensed for iFIX.

To install the virtual keyboard:

1. Double-click the LICENSE.EXE file in the iFIX directory on your Server. The IMG License Manager dialog box appears.
2. Click Install Service to install the virtual keyboard licenses.
3. Click Administration Options & Help. The Terminal Server Administration Option dialog box opens.
4. Click Copy Global Settings to All User Folders, then click Yes to confirm.
5. Click OK to return to the IMG License Manager dialog box.
6. Click Start Service to activate the virtual keyboard for all licensed clients.

Step 4: Configuring the SCU

The System Configuration Utility (SCU) is the tool that you use to configure the iFIX startup options and default directories. For each user type, you create a separate SCU file with different startup options and project paths. Multiple users can share the same SCU file (when communicating with iFIX SCADAs). For instance, you may want to create a separate SCU file for Operators and another SCU file for Supervisors. While user types are maintained as projects in the SCU, individual user profiles are maintained in the Startup Profile Manager, as described in the Step 5: Creating Startup Profiles section.

When configuring an SCU file for use with Remote Desktop Services, follow the steps outlined in these sections:

- Defining Project Directory Paths
- Disabling SCADA Support for Client SCUs
- Defining iFIX Global Security Paths
- Upgrading SCU Files from a Previous iFIX Release
- Configuring User Accounts to Use a Unique Set of Schedules

Defining Project Directory Paths

After you finish planning user types and directories, you are ready to create projects that organize these user types and directories. To create projects, you use the iFIX System Configuration Utility (SCU). For each project there is a separate, unique SCU file.

IMPORTANT: The SCU file for each project must be saved into the Local folder for that project.

To access the SCU, in the iFIX WorkSpace system tree, double-click the System Configuration icon, or click the Start button and point to Programs, iFIX, and then System Configuration. You can also start the SCU directly from the iFIX Startup dialog box, also known as the Launch application. Make sure you shut down iFIX before starting the SCU.

To create a project in the SCU:

1. Start the SCU.
2. On the Configure menu, click Paths. The Path Configuration dialog box appears.

   IMPORTANT: The Base and Language Paths should be the same for each project. For instance, if you leave the Base and Language set to the defaults, the Base is set to C:\Program Files (x86)\Proficy\iFIX and the Language is set to C:\Program Files (x86)\Proficy\iFIX\NLS for each project. Leave the Base and Language paths set to the default, and proceed by editing the Project path fields.
3. In the Project field, enter a path for the project. For example, a valid path that you might enter for a developer would be: C:\Program Files (x86)\Proficy\iFIX\Projects\Developer1.
4. Click the Change Project button. A message box appears asking if you want to add the default iFIX files to the new project.

   IMPORTANT: The SCU will not copy the files from the existing directories to the new directories.
5. Click Yes. The project path information from the Project field is appended to the other project path fields, such as Local, Database, Picture, Application, and so on.

   For instance, if you enter C:\Program Files (x86)\Proficy\iFIX\Projects\Developer1 in the Project field, the SCU automatically adds \Projects\Developer1 to the other project fields as well. For instance, the Local path in this dialog box would now read: C:\Program Files (x86)\Proficy\iFIX\Projects\Developer1\Local. The Database path would read: C:\Program Files (x86)\Proficy\iFIX\Projects\Developer1\PDB, and so on.

   NOTE: While the paths displayed in the Path Configuration dialog box appear to be added at this point, the actual folders for these paths have not been created yet. While you can view the new paths from this dialog, you will not be able to view them from the Windows Explorer until you complete the remaining steps in this section.

6. If there are any paths that you want to change, such as to a shared directory, manually edit the path fields.
7. From the Path Configuration dialog box, click OK. A message box appears asking you to create the folders for the configured paths.
8. Click Create All. A message box may appear indicating you do not have a valid Alarm Area Database file.
9. Click Proceed to continue.

   iFIX creates the paths for the project folders. You should be able to view the new folders in Windows Explorer.

   IMPORTANT: Be aware that iFIX generates these paths with the “user” permissions required by the iFIX product. Use caution when changing the security permissions of these folders outside of iFIX. If you do not have the permissions necessary for iFIX, iFIX will not run.
10. On the File menu, click Save As. The Save File As dialog box appears.
11. Browse to the Project's Local folder. For instance, for Developer1 browse to the C:\Program Files (x86)\Proficy\iFIX\Projects\Developer1\Local folder.
12. Enter a name for the SCU file.

    Valid SCU file names can be up to eight characters long. SCU file names can include alphanumeric characters, but must begin with a letter. Special characters, such as symbols and punctuation marks, cannot be used.

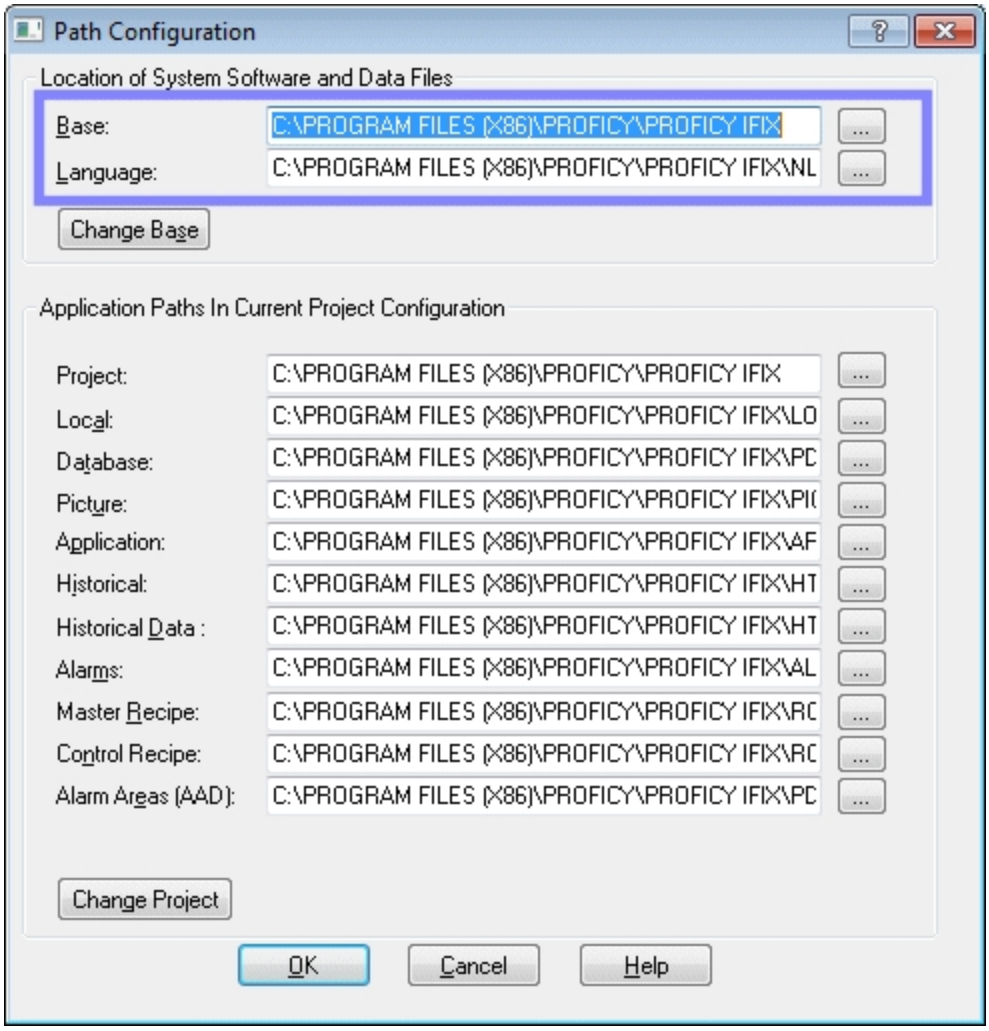
    For example, for Developer1 you might enter Dev1.
13. Click Save. A message box appears asking you if this is the SCU file that you want to use next time you restart iFIX.
14. Click No.
15. If you have a template folder with iFIX files that you want to copy into one or more project folders, use the Windows Explorer to copy the files from the template folders into the new project folders.
16. Repeat steps 2-15 for each project.

Once you have created all the projects, you can go back later and edit all the other SCU settings for each project that require changing. For more detailed information about configuring the rest of the options for the SCU files, refer to the Configuring iFIX Using the SCU chapter in the Setting Up the Environment manual.

Notes on Project Paths

If you are using iFIX Project Configuration with Remote Desktop Services, make sure that the Base and Language Paths are the same for each project. The locations of the project files can differ, depending upon the user type. However, the Base and Language Paths should be the same for each project. For instance, if you leave the Base and Language set to the defaults, the Base is set to C:\Program Files (x86)\Proficy\iFIX and the Language is set to C:\Program Files (x86)\Proficy\iFIX\NLS for each project.

To access the Base and Language path settings, click Start and point to Programs, iFIX, and then System Configuration. To open the Path Configuration dialog box, on the Configure menu, click Paths. The following figures shows an example of this dialog box, with the Base and Language paths highlighted. You will notice that these paths are both set to the default in this figure.



Path Configuration Dialog Box in the SCU

Disabling SCADA Support for Client SCUs

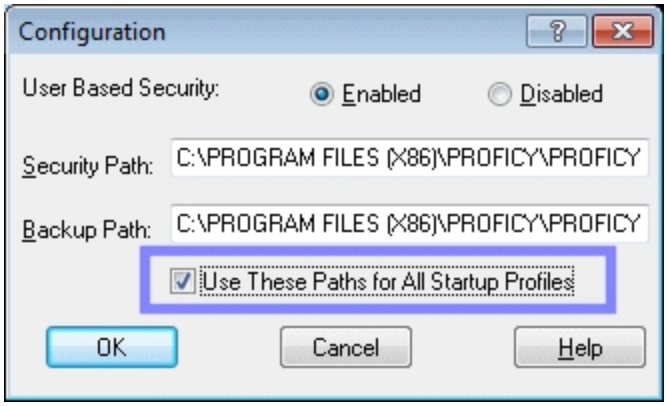
For each SCU that you plan to use on a Remote Desktop client, you should disable SCADA support. To do this in iFIX, on the SCU's Configure menu, click SCADA to open the SCADA Configuration dialog box. In the SCADA support area, select Disable.

NOTES:

- When you run iFIX as a service on the Remote Desktop Session Host, enable SCADA support on that node.
- When you enable SCADA support, the local node becomes a SCADA server capable of accessing your process hardware.
- For more information on Running iFIX as a Service on the Remote Desktop Session Host, refer to the Running iFIX as a Service on the Remote Desktop Session Host section.

Defining iFIX Global Security Paths

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



Configuration Dialog Box, Global Security Paths Enabled

If you do not enable global security paths, you will need to individually configure security within each Remote Desktop Services user session. For instance, previous to iFIX 3.5, you would need to configure an SCU for each Terminal Server user. If you are upgrading from a release previous to iFIX 3.5, this may be a consideration.

Upgrading SCU Files from a Previous iFIX Release

In the first iFIX release that included support for Remote Desktop Services, iFIX 2.5, iFIX required that you generate a complete application environment for each remote user. For example, if there are 50 iFIX users, there must be 50 sets of SCU files, with each SCU file unique to that specific user. With the Startup Profile Manager, all user profiles are stored in a master list, making it easy to maintain and modify profiles for use with Terminal Services.

If you are upgrading from an iFIX release previous to iFIX 3.5, your existing SCU startup configurations from these previous iFIX releases run unchanged. If you later choose to create new startup profiles, as described in the Step 5: Creating Startup Profiles section, the Startup Profile Manager includes an option that allows the new profile settings to override the pre-existing configurations. For more information on the override setting, refer to the Configuring the Options for the Startup Profile Manager section in the Setting Up the Environment manual.

The use of a default profile will help you in migrating from the multiple SCU files to the easier configuration in the Startup Profile Manager. For more information, refer to the Configuring the Default Profile section.

After upgrading, you will need to update the iFIX default files in each of your projects.

To upgrade the iFIX default files:

NOTE: This procedure must be performed for every project.

1. Start the SCU.
2. On the Configure menu, click Paths. The Path Configuration dialog box appears.
3. Click Change Project. A message box appears asking if you want to generate the default iFIX files to the project.
4. Click Yes, and then OK.

Configuring User Accounts to Use a Unique Set of Schedules

If you share the SCU Database (PDB) path among user accounts, all user accounts share the same set of schedules.

To configure user accounts to use a unique set of schedules:

1. Create a unique folder for each schedule grouping you want to use. This folder will be used as the PDB path for users of these schedules.

   The schedule groupings can be unique for each user or grouped by any other logical scenario.
2. Copy the appropriate .EVS files to the directories specified, or:
   a. Configure the SCU with the PDB path pointing to the folder you want.
   b. Start the Client.
   c. Create the .EVS files.

Configuring user accounts to use a unique set of schedules provides flexibility in a Remote Desktop Services environment where all schedules do not need to be available to every user session.

If you use separate schedules per user account or groups of user accounts, and these user accounts or groups of user accounts have any of the same SCADA nodes in the remote nodes list, it creates an environment in which several separate events could fire in response to a single action. You must ensure that none of the events will conflict. Therefore, if you use schedules for direct process control, quality control, or safety-related actions, consider moving this functionality out of the schedules into PLC logic or the process database.

Step 5: Creating Startup Profiles

With the Startup Profile Manager, you create iFIX user profiles. Each profile associates a Windows user name with a specific iFIX Project Configuration. The iFIX Project Configuration includes:

- SCU path and file name that you want the specified Windows user to use when starting iFIX.
- Node name that you want the specified Windows user to use when starting iFIX.
- Restrictions on whether the user can modify the Nodename or SCU fields in the iFIX Startup dialog box (Launch.exe).

iFIX must be running in order to use the Startup Profile Manager application to create startup profiles. To access the Startup Profile Manager, double-click the Startup Profile Manager icon in the system tree in the iFIX WorkSpace. The Startup Profile Manager can also be accessed from the Start menu by pointing to Programs, iFIX, Tools, and then Startup Profile Manager.

When working with the Startup Profile Manager be sure to perform the following tasks:

- Configuring the Options for the Startup Profile Manager
- Configuring the Default Profile
- Adding Startup Profiles

Configuring the Options for the Startup Profile Manager

Before you begin working with the Startup Profile Manager, you should configure the options that you want the Startup Profile Manager to use. To do this, use the Options dialog box in the Startup Profile Manager.

To change the options for the Startup Profile Manager:

1. On the Settings menu, click Options. The Options dialog box appears.
2. Select the *Startup Profiles defined in this application override iFIX Startup command line parameters* check box, if you want the profiles created in this application to override the ones used when you start iFIX from the command line.

   IMPORTANT: For the override to work, the user must be defined in the Startup Profile Manager, or if the user is not defined, the default profile must be enabled. This override only applies to the /n, /s, and /l command line options.
3. Enter a string for the default iFIX node name prefix to use if the first 8 characters of the Windows user name cannot be used to generate a valid iFIX node name.

   The Windows user name is an invalid iFIX node name, for instance, when the name starts with a number. Valid node names can be up to eight characters long. Node names can include alphanumeric characters, but must begin with a letter. Special characters, such as symbols and punctuation marks, cannot be used.

   For each startup profile using the default iFIX node name, a number is also added to the end of the default node name, starting with the number 1. For example, if you enter NODE as the prefix, the default iFIX node names used are: NODE1, NODE2, NODE3, and so on. Each default user who starts iFIX receives a different node name.

   NOTE: When you use the Nodename Prefix field, you cannot use the iFIX automatic login feature unless you generate automatic login configurations for each of the possible node names for the defined prefix. For example: Node1, Node2, Node3, and so on. Since you will not know the name of the user logging in under that node name (since the name is generated at iFIX startup), you should also associate the auto logins with a guest or limited-access account. For more information on automatic login, refer to the iFIX Automatic Login section.
4. Click OK.

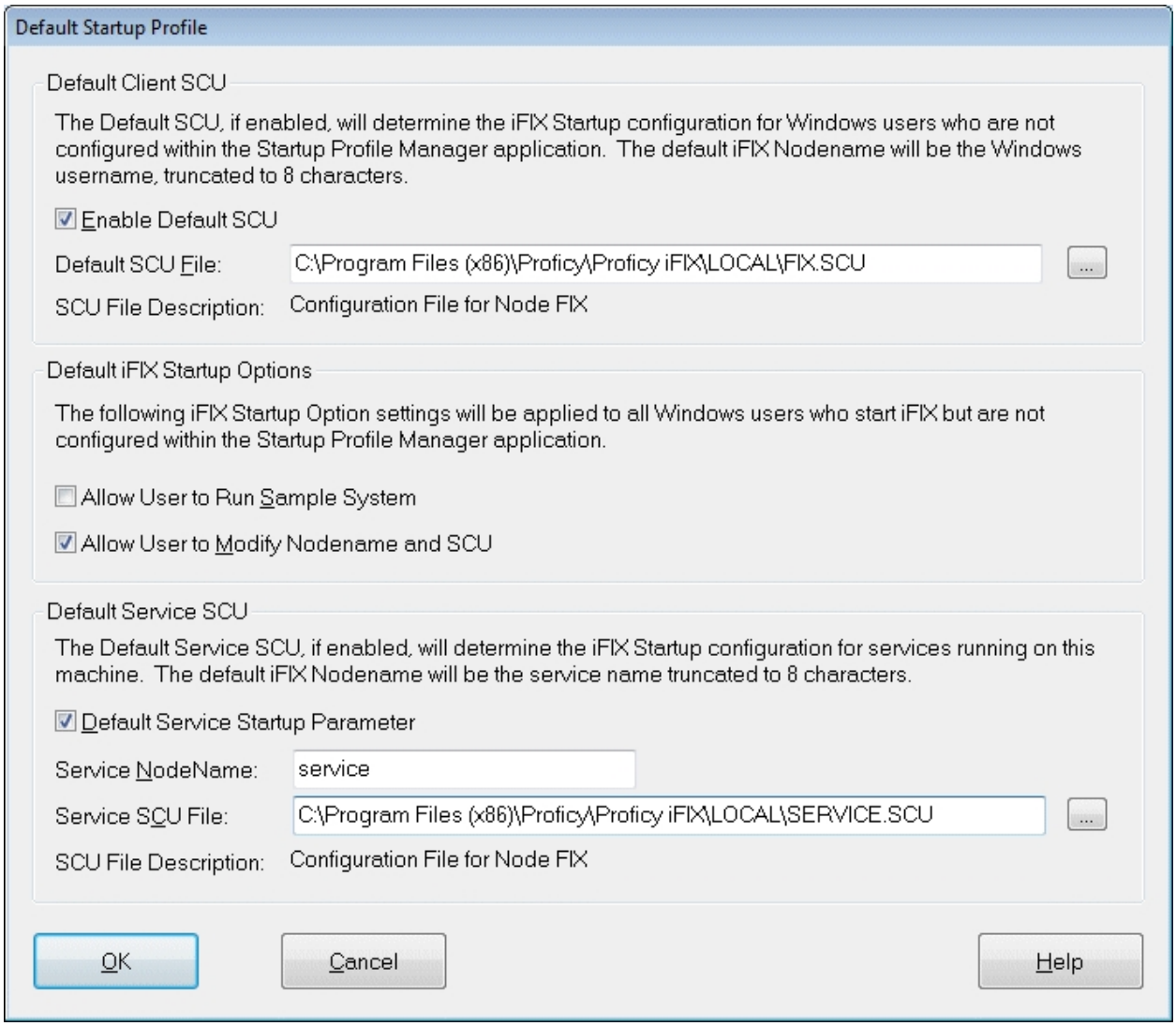
Configuring the Default Profile

After configuring the application options for the Startup Profile Manager, you should define a default profile, if your iFIX configuration requires it. For instance, when using Remote Desktop Services with the Startup Profile Manager, you will most likely want to configure a default profile so that a separate profile does not need to be created for every user.

If a user attempts to start iFIX and a profile does not exist for that user yet, iFIX starts with the default profile information.

NOTE: Only one iFIX node (the SCADA node) can be enabled to run as a service, when it also resides on the Remote Desktop Server.

To configure the SCU and iFIX Startup options for the default profile, use the Default Startup Profile dialog box, as shown in the following figure.



Default Startup Profile Dialog Box

To define the default profile:

1. On the Settings menu, click Default Startup Profile. The Default Startup Profile dialog box appears.
2. Select Enable Default SCU.
3. Enter or select the default SCU and iFIX startup options that you want to apply to all iFIX users without a startup profile.

4. If you want to run iFIX as a service on the Remote Desktop Session Host, select the Default Service Startup Parameter option. Enter the Node name and SCU file for the iFIX service. When iFIX runs as a service, it will always use these settings.
5. Click OK.

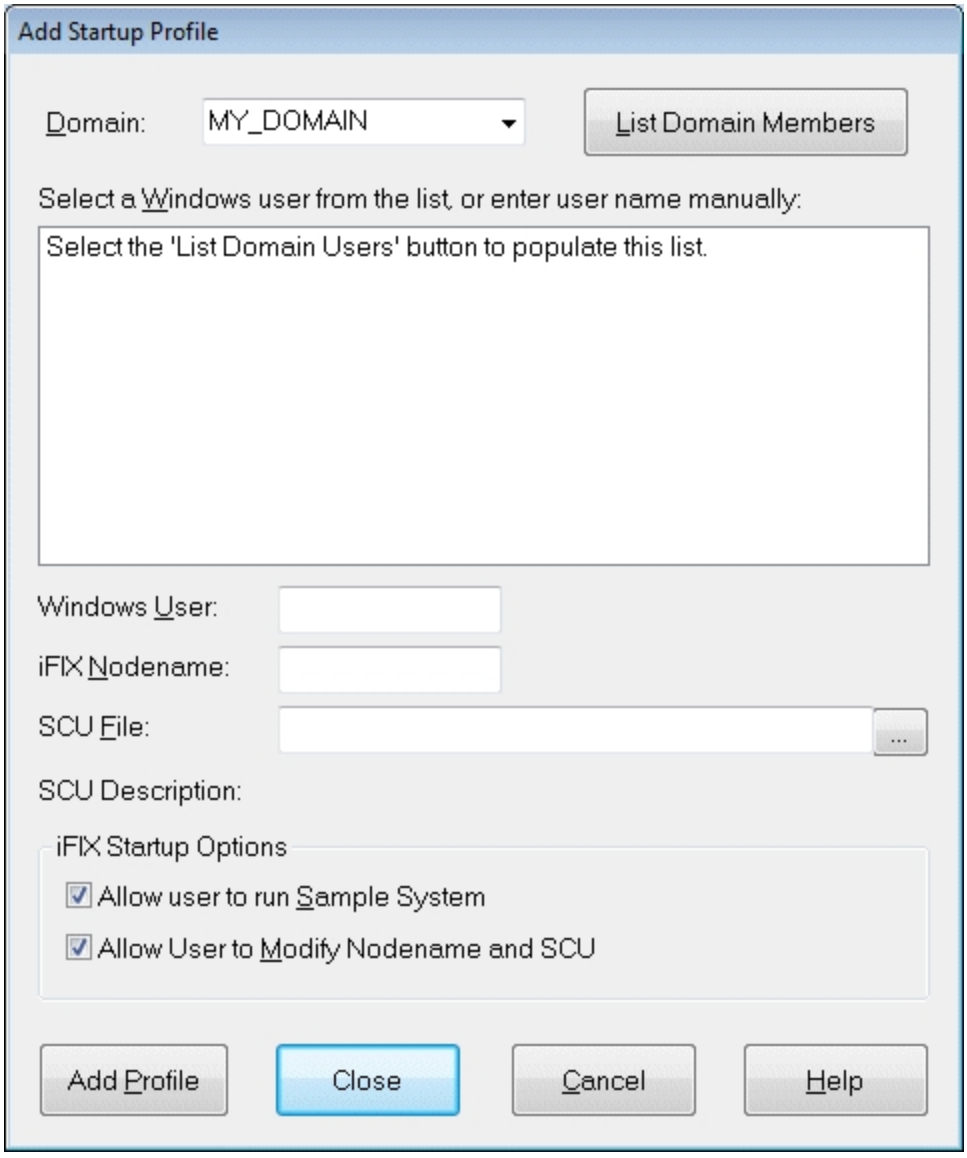
NOTE: If you select the Enable Default SCU option, make sure you also enable the global security paths (Use These Paths for All Startup Profiles) option in the Configuration dialog box in the Security Configuration application.

Adding Startup Profiles

The following steps describe how to add a startup profile.

To add a startup profile:

1. Click the Add button, or double-click any empty column. The Add Startup Profile dialog box appears, as shown in the following figure.



Add Startup Profile Dialog Box

2. Select a domain from the drop-down list.
3. Optionally, click the List Domain Members button to view a list of users that you can pick from.

   NOTE: Depending on the size of your domain and speed of your network, this action could take a few moments or several minutes.
4. Select a Windows user from the list, or enter one manually in the Windows User field. You do not have to be connected to the domain if you enter the name manually. This user must be a member of Remote Desktop User group, if you want start iFIX with Remote Desktop Services.
5. Accept the default iFIX Node Name, or enter another one.

   NOTE: If you manually entered a Windows user name, you must also manually enter an iFIX node name. The default name is not used in this case.

6. Enter the location and name of the iFIX SCU file that you want to associate with this user. For example, you might enter C:\Program Files (x86)\Proficy\iFIX\LOCAL\FIX.SCU. If a default iFIX SCU name is supplied, you can use it or enter another one.

   Optionally, you can browse for an SCU file, by clicking the Browse (...) button.

7. Select the options that you want to make available for the specified user from the iFIX Startup dialog box.
   - If you select the Allow User to Run Sample System check box, the specified Windows user can start the sample system. The Sample System is a legacy product option and no longer shipped as part of iFIX 5.8.
   - Similarly, if you select the Allow User to Modify Nodename and SCU check box, these fields are available for editing when the specified user attempts to start iFIX.
   - If you clear both the Allow User to Run Sample System and the Allow User to Modify Nodename and SCU check boxes, the iFIX Startup dialog box does not appear for the specified user.
8. Click Add Profile.

More on Startup Profiles

iFIX does not use a startup profile until the specified user attempts to start iFIX from the iFIX Startup dialog box or from the iFIX Startup command line (from a desktop shortcut or the Run dialog box, for example). If no iFIX startup profile exists for the user and you do not define any settings in the Default User Profile dialog box or provide command line settings to the iFIX Startup application, when you restart iFIX, it displays the information from the last time iFIX was run.

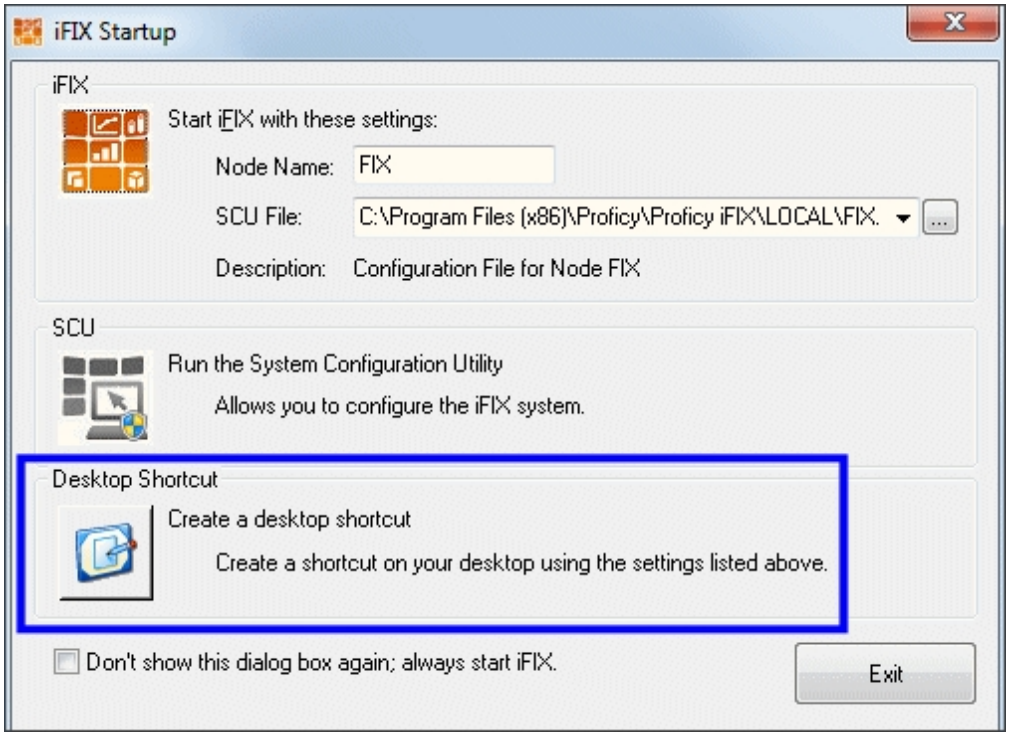
For more detailed information on the Startup Profile Manager, refer to the to Using the Startup Profile Manager section in the Setting up the Environment manual.

TIP: Creating User Defined Desktop Shortcuts to Start iFIX

Use the iFIX Startup dialog box to create desktop shortcuts to start iFIX.

To create a desktop with the settings currently specified in the iFIX Startup dialog box:

1. Start iFIX. The iFIX Startup dialog box appears.
2. Click the Desktop Shortcut icon. The following figure highlights the Desktop Shortcut button on the iFIX Startup dialog box.



iFIX Startup Dialog Box, with Desktop Shortcut Button Highlighted

The Desktop Shortcut dialog box appears.

3. Enter a shortcut name.
4. Click OK.

A shortcut is created for the currently logged in Windows user.

TIP: Using the Application Validator to Take a Snapshot of Your Project Folders

Once you configure your iFIX projects for use with Remote Desktop Services, you can create a baseline of the files and folders associated with your projects using the Application Validator. At a later time, you can then monitor which files and folders changed since you last created the baseline.

For instance, if you ever run into problems with your iFIX configuration and want to go back to an original configuration, you can use the Application Validator to determine which files were changed or added, and then you can manually rollback to that configuration.

To access the Application Validator, double-click Application Validator icon in the system tree in the iFIX WorkSpace. You can also access the application by locating and running the AppValidator.exe file in the iFIX folder, which is the folder where you installed iFIX.

For detailed steps on how to create a baseline, refer to the General Overview of the Steps for Using the Application Validator section in the Mastering iFIX manual.

For more general information on the Application Validator, including the command line options, refer to the Validating an Application section in the Mastering iFIX manual.

EXAMPLE: Configuring Remote Desktop Services with iFIX Running As a Service

The following steps explain how to configure iFIX to run as a service on the Remote Desktop Session Host. These steps assume you have already installed your Windows Remote Desktop Services software as described in the Getting Started section, as well as iFIX, as described in the Installing iFIX section. These steps also assume that you have not enabled iFIX security yet.

To start, we create a separate SCU to run iFIX as a service, named SERVICE. We then create two more SCU users on the Remote Desktop Services:

- A default user, named GUEST, with limited security privileges. The path to this user's iFIX project is C:\ProjectA. When iFIX starts with this SCU, the iFIX Startup dialog box *doesnot* appear.
- An administrative user, named PAUL, with full rights. The path to this user's iFIX project is C:\ProjectB. When iFIX starts with this SCU, the iFIX Startup dialog box *does* appear.

Both these users have iFIX networking enabled and can log in from thin clients. The FIXBackgroundServer.exe runs as a service on the server, so that you can later add scheduled events.

The steps below are outlined in the order that you want to perform them.

To build the service SCU on Terminal Server:

1. Shut down iFIX.
2. Ensure that you are logged in as an Administrator.
3. On the Start menu, point to Programs, iFIX, and then System Configuration. The System Configuration Utility (SCU) window appears.
4. From the SCU's Local Startup Definition dialog box, select the Continue Running After Logoff check box. For steps, refer to the Running iFIX as a Service section.

   NOTE: This setting is a system-wide setting, and will make changes to your registry. If iFIX is running as a service, all SCUs should have this option enabled.
5. From the SCU's SCADA Configuration dialog box, enable SCADA Support. For steps, refer to the Enabling SCADA Support section.
6. From the SCU's Task Configuration dialog box:
   - Make sure that the WorkSpace.exe task starts in Normal mode.
   - Add the FixBackgroundServer.exe to the startup task list, in Background mode. This starts the FixSchedulerService, allowing you to add scheduled events from the iFIX Scheduler.

   For information on how to use the Task Configuration dialog box, refer to the Configuring Startup Tasks section.
7. From the SCU's Network Configuration dialog box, enable TCP/IP networking. For more information on networking configuration, refer to the Configuring Network Connections section.
8. From the SCU's File menu, click Save as. The Save File As dialog box appears.

9. In the File name field, enter SERVICE.SCU and click Save. In the message box that appears, click Yes to use this SCU when iFIX restarts.
10. Exit the SCU.
11. Start iFIX.
12. Run the Startup Profile Manager.
13. From the Startup Profile Manager's Default Startup Profile dialog box, configure the Default Service SCU. For steps, refer to the Configuring the Default Profile section.
14. Save your changes and exit the Startup Profile Manager.
15. Start the Security Configuration utility. In the Configuration dialog dialog box, select the Use These Paths for All Startup Profiles check box to enable global security paths. For steps, refer to the Defining iFIX Global Security Paths section.
16. Save the Security Configuration and exit the program.
17. Shut down iFIX.
18. Restart iFIX to confirm it runs as a service.

To create the guest SCU:

1. Shut down iFIX.
2. Start the SCU.
3. On the File menu, click New.
4. From the SCU's Path Configuration dialog box:
    - In the Project field, enter C:\ProjectA as the project.
    - Click Change Project. A message box appears, click Yes to continue.
    - Click OK, and another message box appears.
    - Click Create All.
    - In the message box that follows, click Proceed.
5. From the SCU's Local Startup Definition dialog box:
    - Change the local and logical node name to GUEST.
    - Select the Continue Running After Logoff check box.

    For more information on configuring iFIX to run as a service, refer to the Running iFIX as a Service section.
6. From the SCU's SCADA Configuration dialog box, disable SCADA Support.
7. From the SCU's Task Configuration dialog box:
    - Make sure that the WorkSpace.exe task starts in Normal mode.
    - Add the FixBackgroundServer.exe to the startup task list, in Background mode.

    For information on how to use the Task Configuration dialog box, refer to the Configuring Startup Tasks section.
8. From the SCU's Network Configuration dialog box:

- Enable TCP/IP networking.
- Add a remote SCADA node.

For more information on networking configuration, refer to the Configuring Network Connections section.

9. From the SCU's File menu, click Save as. The Save File As dialog box appears.
10. In the File name field, enter GUEST.SCU and click Save. In the message box that appears, click No, so that the SERVICE SCU is used when iFIX restarts.

To create the administrative SCU:

1. On the SCU's File menu, click New.
2. From the SCU's Path Configuration dialog box:
   - In the Project field, enter C:\ProjectB as the project.
   - Click Change Project. A message box appears, click Yes to continue.
   - Click OK and another message box appears.
   - Click Create All.
   - In the message box that follows, click Proceed.
3. From the SCU's Local Startup Definition dialog box:
   - Change the local and logical node name to PAUL.
   - Select the Run iFIX as a Service check box.

   For more information on configuring iFIX to run as a service, refer to the Running iFIX as a Service section.
4. From the SCU's SCADA Configuration dialog box, disable SCADA Support.
5. From the SCU's Task Configuration dialog box:
   - Make sure that the WorkSpace.exe task starts in Normal mode.
   - Add the FixBackgroundServer.exe to the startup task list, in Background mode.

   For information on how to use the Task Configuration dialog box, refer to the Configuring Startup Tasks section.
6. From the SCU's Network Configuration dialog box:
   - Enable TCP/IP networking.
   - Add a remote node.

   For more information on networking configuration, refer to the Configuring Network Connections section.
7. From the SCU's File menu, click Save as. The Save File As dialog box appears.
8. In the File name field, enter PAUL.SCU and click Save. In the message box that appears, click No, so that the SERVICE SCU is used when iFIX restarts.

To create startup profiles for your users:

1. Start iFIX.
2. Run the Startup Profile Manager.

3. To configure the GUEST user, from the Startup Profile Manager's Default Startup Profile dialog box:
    - Configure the Default Client SCU area. In the Default SCU field, enter or browse to C:\ProjectA\LOCAL\GUEST.scu.
    - Remove the check marks from the Allow User to Run the Sample System and the Allow User to Modify Node Name and SCU check boxes.
    - Click Add Profile.
    - Click Close to exit the Add Startup Profile dialog box.

    For steps, refer to the Configuring the Default Profile section.
4. From the Startup Profile Manager's Options dialog box, select the top check box, Startup Profiles defined in this application override iFIX Startup command line parameters, and click OK. This enables the GUEST account as the default.
5. To configure the PAUL user, from the Startup Profile Manager main screen:
    - Click Add.
    - Enter a Windows User name. For instance, say you enter PAULC as your Windows User name.
    - In the iFIX Node Name field, enter PAUL.
    - In the SCU File Name field, enter or browse to C:\ProjectB\LOCAL\PAUL.SCU.
    - Select the Allow User to Modify Node Name and SCU check box.
    - Click Add Profile.
    - Click Close to exit the Add Startup Profile dialog box.

    When the specified user name logs on, he will have more rights, as indicated by the enabled check box.

    TIP: You can restrict even more access by enabling iFIX security. For more information, refer to the Understanding iFIX Security section.
6. Save your changes and exit the Startup Profile Manager.
7. Restart iFIX.

To verify that the administrative account logs in with the PAUL startup profile:

1. On the iClientTS, open the Remote Desktop Connection dialog box.
2. In the Computer field, enter the computer name of the iFIX SCADA Server.
3. Click Connect. A login dialog box appears.
4. In the User name field, enter the user name from step 5 of the previous set of steps. For example: PAULC.
5. In the Password field, enter the Windows password.
6. Click the iFIX icon to start iFIX.
7. Verify that the iFIX Startup dialog box appears.

8. Verify that the Node Name field is PAUL, and the SCU field is C:\ProjectB\LOCAL\PAUL.SCU. This confirms that you are starting iFIX with the administrative user, PAUL, as defined in the Startup Profile Manager.
9. Start iFIX and verify the SCU starts.

To verify that other users log in with the GUEST startup profile:

1. On the iClientTS, open the Remote Desktop Connection dialog box.
2. In the Computer field, enter the computer name of the iFIX SCADA Server.
3. Click Connect. A login dialog box appears.
4. In the User name field, enter any other Windows user name.
5. In the Password field, enter the Windows password for that user.
6. Click the iFIX icon to start iFIX.
7. Verify that the iFIX Startup dialog box does *not* appear. This happens because you are using the settings defined for the default startup profile (the GUEST startup profile) in the Startup Profile Manager.

TIP: If you want to secure this environment you just created, see Securing the Remote Desktop Services Environment for steps on how to specify the program that starts when the user logs on to the Remote Desktop Session Host (the Launch.exe for iFIX, for instance) and to restrict the Ctrl+Alt+Delete function.

iFIX WorkSpace Toolbars and Remote Desktop Services

When using iFIX with Remote Desktop Services and all clients share the same iFIX folders, toolbars can be configured separately on each client. This is because each client has it's own file for toolbar preferences, as well as temporary toolbar files stored in each client's temp folder.

Also, be aware that only one user at a time can import a toolbar into the iFIX WorkSpace when all clients share the same iFIX folders. After you import a toolbar you also should close the WorkSpace, so that the toolbar file is released, allowing other clients to import it. You then can immediately restart the WorkSpace.

The iFIX WorkSpace toolbars can only be seen by those users that have rights for developing pictures. Operators in a run-time environment do not see the toolbars.

Securing the Remote Desktop Services Environment

Although iFIX Environment Protection is not supported on the iClientTS computer, you can still create a secure environment that prevents operators from performing unauthorized actions, such as using the Ctrl+Alt+Delete key combination to shut down the Remote Desktop Session Host. You can configure this in Windows, with user properties and group policies.

For instance, you can configure which Windows users have access to log in to from the thin client. After logging in, you can restrict them from running anything other than the iFIX startup program. By configuring iFIX startup tasks, in the SCU, you can control which tasks are available after startup.

You can even configure the rights available to the user when he is logged in. For instance, you can disable the Ctrl+Alt+Delete feature. This prevents the user from shutting down the Remote Desktop Session Host. Instead, the user can only disconnect.

The steps below explain how to perform some of these tasks. Refer to the Windows online help for more information.

To specify the program that starts when the user logs on to the Remote Desktop Services:

1. Log in to Windows as an administrator, if you have not already.
2. Click the Start button, and point to Settings, Control Panel, Administrative Tools, and then Computer Management. The Component Services Microsoft® Management Console (MMC) snap-in appears.
3. In the System Tools folder, double-click the Local Users and Groups item.
4. Double-click the Users folder.
5. Right-click the user you want to configure and select Properties. The Properties dialog box appears.
6. Click the Environment tab.
7. In the Starting Program area, select the Start the following program at logon check box.
8. In the Program File Name field, enter the path to the iFIX Startup (Launch.exe) program. For instance, if you installed iFIX to the default location, enter:

   ```
   C:\Program Files (x86)\Proficy\iFIX\Launch.exe
   ```

9. In the Start in field, enter the path of the iFIX product. . For instance, if you installed iFIX to the default location, enter:

   ```
   C:\Program Files (x86)\Proficy\iFIX
   ```

10. Click OK.
11. Repeat steps 5 to 10 for each user you want to configure.

To disable the Ctrl+Alt+Delete function:

1. Log in to Windows as an administrator, if you have not already.
2. On the Start menu, point to Run. The Run dialog box appears.
3. Enter `gpedit.msc` and then click OK. The Group Policy dialog box appears.
4. In the Local Computer Policy folder, double-click User Configuration.
5. In the User Configuration folder, double-click Administrative Templates, and then System.
6. Select the Ctrl+Alt+Delete options.
7. In the setting area, double-click the Remove Task Manager setting. The Remove Task Manager Properties dialog box appears.
8. Select the Enabled option and click OK.
9. When you are finished, on the File menu, click Exit. This closes the Group Policy dialog box.

Be aware that you can use iFIX security to define the rights each user has in iFIX after logging in. For instance, you can add further restrictions in iFIX by defining the application features available for the user. For more information, refer to the Understanding iFIX Security section.

Additionally, be aware that any iClientTS starting on a Remote Desktop Session Host (not a SCADA) does not accept unsolicited incoming connections. A client/SCADA that cannot accept incoming connections is called a non-listening client. This is a built-in network security feature. For more information on non-listening clients and other built-in security features, refer to the Configuring Network Security section.

Installing and Configuring Remote Desktop Sessions

This section describes how to install and configure Remote Desktop Servics. It includes the following sections:

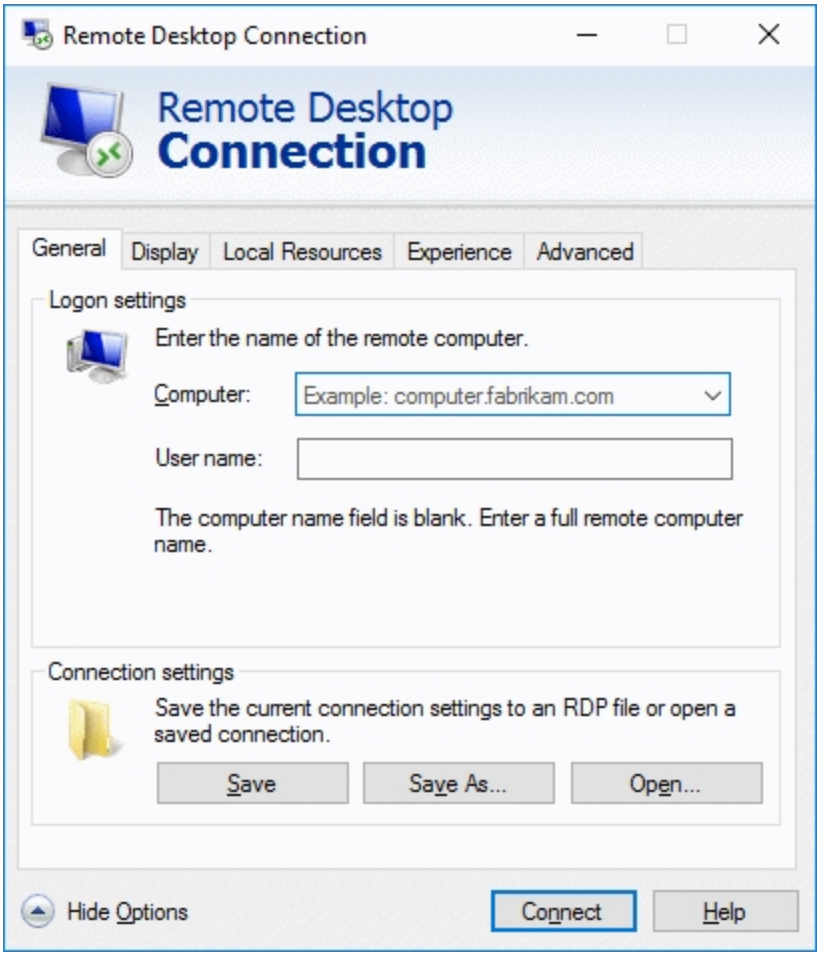
- Configuring a Remote Desktop Connection
- Logging on to a Remote Desktop Web Connection

Configuring Remote Desktop Services to Connect to a Host with iFIX

You can configure and connect a client to connect to the Remote Desktop Session Host using the Remote Desktop Communication dialog box.

To connect a client to Remote Desktop Session Host in Windows:

1. Open the Remote Desktop Communication application.
2. In the Computer field, enter or browse for your Remote Desktop Session Host machine name or IP address. To configure optional parameters for your remote desktop connection, go to Step 3. Otherwise, go to Step 14.
3. Click the Options button. The tabs for each of the options appear in the dialog box, as shown in the following figure.



Remote Desktop Connection Dialog Box with Tabs Displayed

4. In the Computer field, enter or browse for your Remote Desktop Session Host name or IP address.
5. In the User Name field, enter a valid Remote Desktop user existing on the Remote Desktop Session Host, using the format <TS machine name>\<user>, for example, MyTSmachine\operator1 or 169.127.123.89\operator1.
6. Click the Display tab.
7. Leave the default remote desktop size, but change the color setting to the lowest color setting that the pictures were designed to use. By using the least amount of colors, you reduce the load on the network and enhance performance.
8. Click the Local Resources tab.
9. Select the options that your application requires.

   For instance, you probably want to enable Printer sharing by selecting the Printer check box under the Local Device Settings. The other options you will probably set to the defaults, though you are not restricted to do so.

10. Click the Programs tab.
11. If you want to start a program when the designated user starts a Remote Desktop session, select the check box and enter the name and path, along with the folder that you want the program to start in if it is different from the application path.
12. Click the Experience tab.
13. Select the performance options that your client requires. It is recommended that you clear all check boxes except Persistent Bitmap Caching and Reconnect if connection is dropped.
14. Click Connect to connect to the remote Remote Desktop Session Host.

Logging on to a Remote Desktop Web Connection

If Remote Desktop Web Access is enabled on your Remote Desktop Session Host you can use Internet Explorer's Microsoft Remote Desktop Services Client Control (ActiveX control) on remote machines to open Remote Desktop client sessions.

If the Microsoft Remote Desktop Services Client Control is not installed and enabled, the first time you try to connect from a Remote Desktop client machine, you will be prompted to do so. When attempting to connect through IIS and the Remote Desktop Services Advanced Client ActiveX control, if the ActiveX Client Control is not found on the client computer, or if an older version of the control is found, it will be installed at this time.

NOTES:

- Multiple users cannot log on using the same account.
- If you configured the user account with the application startup command, iFIX starts automatically. If you did not configure the user account to auto launch, use the Launch icon to start iFIX. Do not use the iFIX Startup icon.

TIPS:

- When the Web Connect or Remote Desktop Services Web Access screen opens, you can create a shortcut to this page by making it a Favorite in Internet Explorer. Adding it to your Favorites list allows you to initiate future connections by clicking on the shortcut.
- If the Full Screen option is not available at connect time due to security limitations or settings, you can access it after connection by pressing Ctrl+Alt+Pause.

To connect to a Remote Desktop Services:

1. Open Internet Explorer.
2. Enter the URL, in the following format: http://TSmachinename/RDweb/Pages/en-Us/Default.asp

Optimizing iFIX for use with Remote Desktop Services

This chapter discusses some ways to improve your Remote Desktop Services performance within iFIX and Windows. It includes the following sections:

- Optimizing iFIX
- Optimizing the Remote Desktop Session Host
- Third-party Thin Client Software and Hardware
- Optimizing New iFIX Pictures for Use with Remote Desktop Capable Devices

For more optimization ideas and tips, refer to the Optimizing Your iFIX System manual.

Optimizing iFIX

This section provides some optimization ideas and tips to enhance your iFIX with Remote Desktop Services environment. It includes the following topics:

- Using Deadband Values
- Using Refresh Rates
- Disabling Picture Caching
- Using Bitmaps
- Using Traditional Clients
- Disabling Smooth Scrolling
- Using Auto Scale

Using Deadband Values

You may want to use deadband values to reduce the number of updates sent back and forth to the Server. Deadband values, set in the iFIX Expression Editor, specify the maximum fluctuation you want for the current connection before iFIX updates it. By entering a deadband value, you create a +/- dead zone around the connection's current value. As long as the value is within this range, iFIX does not update the value. However, once the value exceeds the maximum or minimum deadband, the value is updated.

Using Refresh Rates

The iFIX WorkSpace provides a Refresh Rate Expert in the Expression Builder that determines how often the data source connection updates, in seconds. The default is 1 second on new animations. But, previous to iFIX 6.0, the default refresh rate was 0.10000 which caused the connection to refresh 10 times per second. If your application does not need the connection to be refreshed this often, you can gain considerable performance by reducing the refresh rate and the deadband.

Refresh rates on pictures can also impact performance. In the iFIX Terminal Server setup, by default, datalinks, animations, and charts (Enhanced and Standard) in pictures will refresh as configured. But you can throttle these rates by placing the following parameters in the FixUserPreferences.ini file. You can adjust these default settings without opening any pictures. By default the throttling is disabled on the Remote Desktop Services Host.

1. Open the FixUserPreferences.ini file. (By default, for iFIX, this file is located in the C:\Program Files (x86)\Proficy\iFIX\LOCAL folder.)
2. Scroll to the [TerminalServicesPreferences] section and enter larger numbers. A larger number for these settings provides a slower refresh rate, which is intended to improve performance.

```
[TerminalServicesPreferences]
DataRefreshThrottleInSecs=1.0
AlarmSummaryThrottleInSecs=5.0
EnableTerminalServicesRateControls=1
```

3. Save the file.

After modifying the above datalinks, animations, and charts (Enhanced and Standard), pictures will refresh at a rate no faster than once per value specified for “DataRefreshThrottleInSecs “.

For example, in the Expression Builder, if you enter .1 or .5 as the refresh rate for your data source, it will NOT be adhered to. The historical update rate for both Enhanced and Standard charts will also be adjusted accordingly. For the alarm blink rate, alarm fetch rate, and alarm data refresh rate in the Alarm Summary objects, iFIX will refresh the data no faster than value specified for “AlarmSummaryThrottleInSecs” seconds. For instance, even if you set the refresh rates in the Alarm Summary object to be faster, iFIX will not allow a rate faster than “AlarmSummaryThrottleInSecs”.

Disabling Picture Caching

By default, picture caching is enabled in iFIX. Although this does speed up picture performance, it can also slow down processing on the Server. If you need to free up memory on the Server, disable picture caching.

Using Bitmaps

You may want to limit your use of bitmaps. Bitmaps usually require more processing than other graphical file formats. Compressed or vector graphics are easier to process and often have reduced color depth, improving its display in 256 colors.

If you use bitmaps, avoid using moving bitmaps. Moving bitmaps require that the Server constantly redraw the image, continuously taking up processing resources.

Disabling Smooth Scrolling

You may want to disable smooth scrolling on Internet Explorer 5.5 to improve viewing on the thin client.

To disable smooth scrolling:

1. Open Internet Explorer and select Tools.
2. Select Internet Options from the drop-down menu.
3. Click the Advanced Tab.
4. Clear the Smooth Scrolling check box from the Browsing options.

Using Auto Scale

Using Auto Scale in your pictures may significantly decrease performance with Remote Desktop Services and impact the number of client sessions you can run under Remote Desktop Services. To access the Auto Scale feature, in Ribbon view, on the Home tab, in the WorkSpace group, click Settings, and select User Preferences or in Classic view, on the WorkSpace menu, select User Preferences. The Disable Auto Scale Feature check box is located on the Picture Preferences tab. To enable the Auto Scaling, clear this check box.

Optimizing the Remote Desktop Session Host

This section provides some optimization ideas and tips to enhance your Remote Desktop Session Host. It includes the following topics:

- Modifying the Encryption Rate
- Disabling Client Wallpaper
- Deleting Temporary Folders
- Disabling Active Desktop

For more Remote Desktop Services optimization ideas and tips, refer to the Client Services section of the Windows Server Help.

Modifying the Encryption Rate

The lower your encryption rate, the better the RDP protocol performs.

To change the encryption rate:

1. Open the Remote Desktop Services Configuration Administrative Tool.
2. Select the Connections folder in the Remote Desktop Services Configuration tree.
3. Right-click the RDP-TCP connection.
4. Select Properties from the right-click menu. The RDP-TCP Properties dialog box appears.
5. Click the General Tab.
6. Modify the Encryption Level field.

Disabling Client Wallpaper

Displaying wallpaper on the client's desktop forces the screen to redraw and uses up Server resources.

To disable the wallpaper:

1. Open the Remote Desktop Services Configuration Administrative Tool.
2. In the Remote Desktop Services Configuration tree, select the Connections folder.
3. Right-click the RDP-TCP connection.
4. Select Properties from the right-click menu. The RDP-TCP Properties dialog box opens.
5. Click the Environment Tab.
6. Select the Disable wallpaper check box.

Deleting Temporary Folders

Deleting temporary folders on exit prevents the loss of disk space resources over time.

To delete temporary folders upon exiting:

1. Open the Remote Desktop Services Configuration Administrative Tool.
2. In the Remote Desktop Services Configuration tree, select the Server Settings folder.
3. Double-click the Delete temporary folders on exit setting. The Delete Temporary Folders dialog box opens.
4. Select Yes and click OK.

Disabling Active Desktop

Active Desktop is a display option in Windows that gives your desktop the look and feel of a web page. You can disable the Active Desktop feature to conserve server memory and CPU resources.

To disable Active Desktop:

1. Open the Remote Desktop Services Configuration Administrative Tool.
2. In the Remote Desktop Services Configuration tree, select the Server Settings folder.
3. Double-click the Active Desktop setting. The Active Desktop dialog box opens.
4. Select the Disable Active Desktop check box and click OK.

Third-party Thin Client Software and Hardware

While designing your Remote Desktop Services environment, you can integrate a third-party client application to enhance the performance and ease of management of your Remote Desktop Services environment. Two examples of third party applications that you can use are described in the following sections:

- Citrix Presentation Server
- Automation Control Products (ACP) ThinManager

Other virtual application solutions like Microsoft's RemoteApp may also work but have not been tested or validated with iFIX.

Citrix Presentation Server

The Citrix Presentation Server is one application that you can use to enhance the performance and ease of management of your Remote Desktop Services environment.

NOTE: Citrix® MetaFrame™ 1.8, Feature Release 1, provided extensive color support and Netscape support. This support was merged into the Citrix Presentation Server product in 2004.

Citrix's Independent Computer Architecture (ICA) protocol allows both Microsoft and non-Microsoft clients, including UNIX and Macintosh, to connect to a Remote Desktop Services Session Host.

For more information on the Citrix Presentation Server product, visit www.citrix.com.

Automation Control Products (ACP) ThinManager

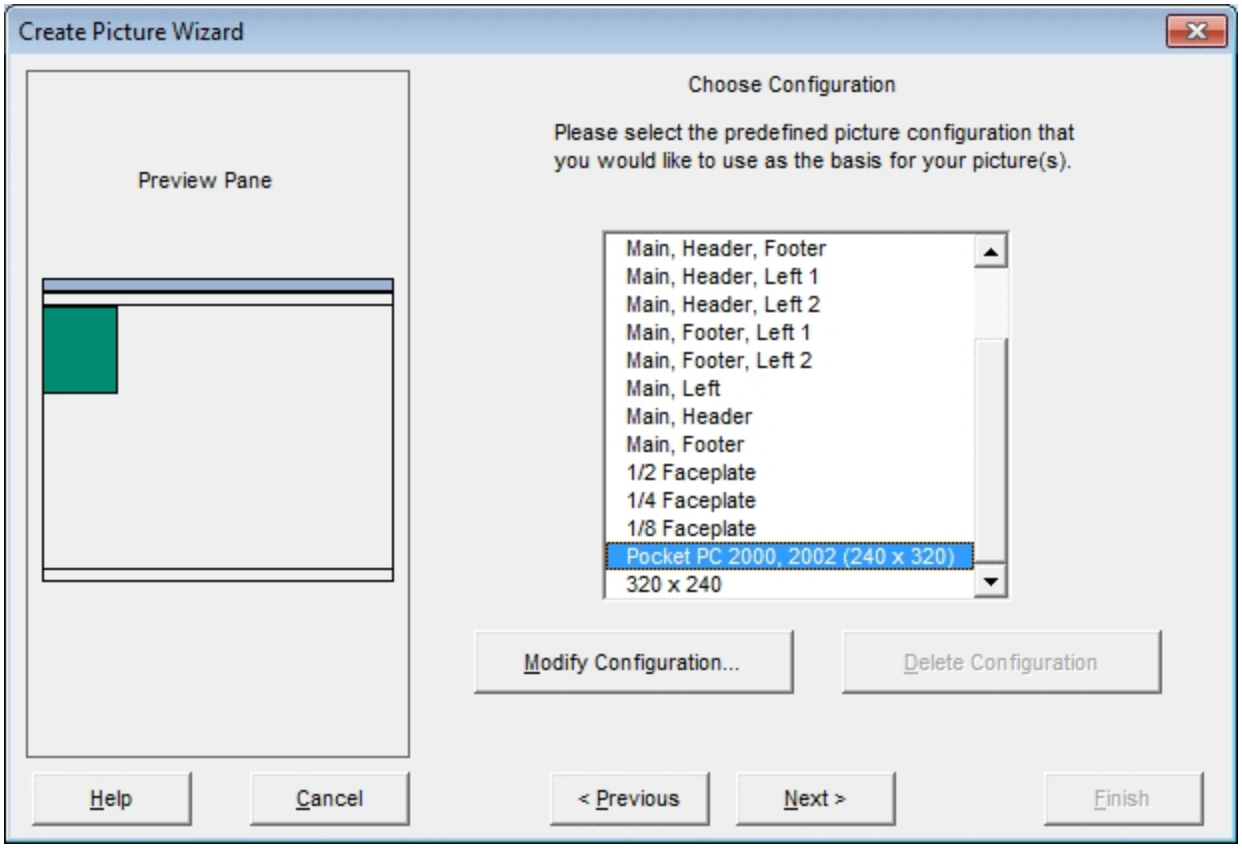
ACP ThinManager™ provides At-A-Glance management of your Remote Desktop Services Environment. The ThinManager software runs on any computer networked in your environment and provides an easy-to-use GUI that monitors your ACP Thin Client machines.

ThinManager allows you to manage clients from a single location. It visibly displays the on/off status of each client and allows you to reboot clients and organize clients by group. It also includes Server and fail-over support. ACP also provides ACP Hardware and Enabled Hardware for use with your Remote Desktop Services environment.

Optimizing New iFIX Pictures for Use with Remote Desktop Capable Devices

The iFIX Create Picture Wizard includes new screen definitions for handheld Remote Desktop Services capable devices. Form factors include 240x320 and 320x240. Remote Desktop users may find this option especially helpful.

The following graphic shows the new configuration options as they appear in one of the screens in the Create Picture wizard.



Choose Configuration Screen, Create Picture Wizard

Troubleshooting Your iFIX and Remote Desktop Services Environment

To successfully troubleshoot your iFIX with Remote Desktop Services Environment, you first need to isolate the source of your problem. Once you have isolated your problem area, refer to the Troubleshooting Specific Issues with Remote Desktop Services table for more troubleshooting information.

This chapter provides the following topics to help you isolate and troubleshoot your iFIX with Remote Desktop Services Environment:

- Isolating Your Remote Desktop Connection Problem
- Troubleshooting Specific Issues with Remote Desktop Services
- Troubleshooting Known Issues with Remote Desktop Services

Isolating Your Remote Desktop Connection Problem

If you experience problems while running iFIX in the Remote Desktop Services Environment, create a new user and follow the steps in the following table to isolate the problem.

If you are unable to complete one of the steps, try troubleshooting the corresponding problem area. Refer to the Troubleshooting Specific Remote Desktop Services Problems table for more information on troubleshooting specific problem areas.

If you are unable to complete this step...	Troubleshoot this area...
1. Connect to the Remote Desktop Session Host via a RDP client session using a local Admin account.	Connection
2. Add an application to start up on logon in the users properties: `C:winnt\system32\notepad.exe`	Environment or Configuration
3. Run a unique iClientTS session using the command line Change user install.	Remote Desktop installation or configuration. Check the documentation on ROOTDRIVE or refer to the Windows Server Help.
4. Create a simple iFIX configuration: one picture, one data link, one user.	SCU Configuration and Startup, File Conflicts, or Configuration.

Troubleshooting Specific Issues with Remote Desktop Services

Once you have isolated your problem area, use the information in the following table to begin troubleshooting.

Troubleshooting Specific Terminal Server Problems

For this problem area....	Verify...
Performance	• Have you optimized your iFIX with Remote Desktop Services Environment? Refer to the Optimizing iFIX with Remote Desktop Services chapter for more information. • Should you run fewer clients? Note that Server performance increases with the following: • Faster processors • More processors (dual, quad) • More memory • Reduced graphic refresh rate on clients
Connection	• Is your connection problem for all connections or user specific? • Can the Administrator start a session locally and remotely?
SCU Configuration and Startup	• Are there duplicated node names on the network? Run NETHIS.exe on the client nodes. If you see 'Connection is established' and 'Connection NOT Established' messages repeatedly, then you may have a duplicate iFIX node name.
File Conflicts	• What is the directory structure? • Is this reproducible in a non-Remote Desktop Services environment using a mapped drive in the path?

	• Are there directory permissions set outside of iFIX? If so, be sure that you use relaxed permissions.
Environment	• Can you create a session on the Server? • Is the problem the same for all users including Admin? • Can you create a new client session? Can you create a client that opens NotePad?
Configuration	• Are the Paths correct? • Is the Launch command accurate, or are the startup profiles in the Startup Profile Manager configured correctly? • Can you create a new SCU/New User, pointing all paths to the base path folder? • Are the paths pointing to a mapped drive? Have the SCADA map to the Remote Desktop Session Host machine. • Does the mapped drive have additional directory permissions configured? • Are there greater than 20 users (Windows limitation) trying to map to the network drive?

For more information, suggestions, and tips for troubleshooting your iFIX with Remote Desktop Services environment, refer to the Windows Server Help, and the Microsoft Remote Desktop Services online documentation.

Troubleshooting Known Issues with Remote Desktop Services

The following table lists some specific troubleshooting information for known Remote Desktop Services issues.

Troubleshooting iFIX and Remote Desktop Services

Problem	Solution
Registry locks, behaves like "Duplicate Node Names" on the network.	You have started multiple sessions at the same time or multiple users have logged on using the same account. Multiple users cannot log on using the same account. Start one session at a time. If the same user is logged on multiple times, consider using the End Session setting. The End Session setting logs off the user upon disconnect. To use this set-

	ting, select the End Session check box located under Override User Settings in the RDP Properties of the Remote Desktop Services Configuration Console.
You modify a file, but the changes are not saved. There is no file version control.	Two users are attempting to modify the same file. If users are sharing files, they must organize file modification. For more information, refer to Step 1: Determining User Types and Directories.
When opening certain toolbar items, you receive a Windows Installer dialog box that states the following: `Please wait while Windows configures Microsoft Office edition.`	You have installed Microsoft Office without modifying the registry. Refer to the Microsoft Knowledge Base article Q274473.
The text insertion cursor in an iFIX Text object does not appear.	The cursor blink rate in the control panel is set to the lowest setting for Remote Desktop Services. Set the blink rate to 1 above the slowest setting.
ODBC setting set for one user appears in the SCU of another user.	You must start iFIX before modifying the Alarm ODBC settings in the SCU.

Index

U

V

W