GE VERNOVA

DIGITAL

# PROFICY WEBSPACE

User Guide

GE VERNOVA

## Proprietary Notice

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



## Trademark Notices

GE, the GE Monogram, and Predix are either registered trademarks or trademarks of General Electric Company.

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

# Webspace User Guide

# Contents

# Chapter 1. Important Product Information

## What's New

### IIS and Apache No Longer a Prerequisite for Webspace

Webspace 6.2 includes a new web server functionality. This new functionality makes it much easier to access a Proficy WebSpace host via an internet gateway. This is because only one port needs be opened through the gateway in this configuration, and not two: one port for the web content (80 or 443), and another port for the Proficy Webspace host data (e.g., 491). It also makes configuration with Configuration Hub and Operations Hub easier!

Be aware that if IIS and Apache are not used, port 491 will be required in the Webspace URL. For example:

```
https://w2019:491/proficywebspace/ifix.html

http://w2019:491/proficywebspace/

http://10.10.10.10:491/proficywebspace/
```

If you are upgrading from the previous version of Proficy Webspace, you can continue using Proficy WebSpace with IIS or Apache, or use the new web server embedded with Webspace.

### Strong Encryption

In addition to the TCP 56-bit DES encryption supported in previous releases, Webspace now provides additional strong encryption options for your connections. This is the complete list of encryption support in Webspace:

- Encrypted, 56-bit DES (with certificate)
- Encrypted, 128-bit RC4 (with certificate)
- Encrypted, 168-bit 3DES (with certificate)
- Encrypted, 256-bit AES

Strong encryption (up to 256-bit AES) assists in assuring the security of the data that is transmitted over the network. The option to increase is only available if your license includes the Strong Encryption option. For more information on security settings in Webspace, search for "encryption" to get details.

### Zero-Install Client for Faster Client Deployment

Developed with JavaScript and HTML5, the Webspace app is a now a zero-install client now that allows you to run iFIX and CIMPLICTY applications from popular web browsers on Windows, Mac, and Linux computers without having to install a plugin or add-in. In previous releases, you would need to download

a plugin or add-in when using Webspace from a browser session. This is no longer the case in Webspace. You can now run iFIX or CIMPLICITY directly from your browser without a download.

Be aware that when running the zero-install client, the following features are NOT supported or available (even when enabled on the Webspace server):

- Client sound (such as alarm beeping)
- Printing directly to client printers (using the native Windows Printer drivers on the client)
- Client file access (outside of iFIX pictures and CIMPLICITY screens)
- Copying and pasting to the clipboard through the menu or toolbar
- Serial and parallel ports
- Smart cards
- Running the client in loose windows mode (embed=false). (In Loose mode, the browser opens without the browser window.)

**Important:**
Use of Integrated Windows Authentication is not supported with the zero-install client. To use this feature, you must open the Webspace full app in a web browser. Alternatively, you can install the Windows Desktop Client and use that to run the Webspace session instead.

The following features ARE supported in the Webspace zero-install client:

- Client-side password caching
- Copy and paste between local and remote applications using keyboard shortcuts (using CTRL+C and CTRL+V)
- Printing to local printers via the Preview PDF Printer (using the Universal Printer Driver)

The above limitations can be easily overcome by downloading and installing the full Webspace client app.

**Note:**
If you need to use client sound for your alarms or to provide support for your native Windows printer driver, we recommend that you create a desktop shortcut to open the browser using the full app each time you click it.

This is an example of a desktop shortcut to open the full app:

```
http://WebspaceServerName/ProficyWebspace/iFIX.html?useApp=true
```

In this case, you will automatically be prompted to install the full app if it is not already installed. For more information on creating desktop shortcuts, search for "shortcut" in the documentation.

### Support for the Apple Safari Browser

With Proficy Webspace, the Apple Safari 12 or later is supported for browser sessions on Mac OS X.

### Support for Existing Mobile Apps

You do not need to update the apps on your mobile devices in order to use Webspace. You can use your existing mobile apps with Webspace. Just be aware that some of the newer functionality may not be available on the older mobile apps.

### Support for Previous Versions of the Webspace Clients

Previous versions of Webspace clients will continue to work with the Webspace Server, however it is recommended that you upgrade Windows Desktop Clients to the latest version.

### New Webspace Client Install Paths

The install paths for Webspace Clients have changed. For instance, the previous version of the Webspace Desktop Client installed to the C:\Program Files (x86)\Proficy\Proficy Webspace Client\Client\ folder. In Webspace, the path for the client is C:\Program Files (x86)\Proficy\Proficy Webspace\Client folder. Be aware that after an upgrade, if you have any shortcuts configured, you will need to update them to use the correct path.

### New Language Support

The language of the installed Webspace product no longer needs to match the language of the iFIX or CIMPLICITY software that you are running.

The English language Webspace product can run on any supported regional operating system (OS), but we recommend using English regional settings. For example, for iFIX these languages are: English, Chinese, Japanese, Polish, Russian, French, or German.

For more information on the available product version for each language, contact your regional Sales Representative.

### Updates to CIMPLICITY HTML Files

The HTML file templates for CIMPLICITY have been updated with Webspace. The Webspace installer will update these templates to the new one. The Webspace HTML files for CIMPLICITY need to be generated from these templates. However, if you installed Webspace before upgrading to a newer

version of CIMPLICITY, when you install CIMPLICITY on the same computer as Webspace, the Webspace HTML templates will be overwritten. Be aware that in this type of upgrade scenario, you would need to manually copy the new template file from the Webspace installation folder to CIMPLICITY install folder and generate the HTML file again from CIMPLICITY.

For examples of what the new templates look like, search the help for "CIMPLICITY HTML Files" for more information.

### Updates to Command-line Options

The supported command line options have been updated. For instance, the Windows Desktop Client now supports -geometery, -clientscale, and -clientdpi options. Undocumented browser shortcuts are not supported, such as: bInBrowser, compression, printerconfig, clientframe, multimonitor, width, height, embed, noscale, clientscale, and ClientDPIScalingEnabled.

For a complete list of supported command-line options with Webspace, search the help for "Command-line options" to review the available options for the Browser and Windows Desktop Clients.

## Release Notes

The Release Notes provide the following information:

- Install and Upgrade Information
- Troubleshooting Tips

### Important Information About Licensing and Keys

You must use the license that is included with your Webspace software in order to access all the components of the GE software you purchased. You can only use your Webspace license with the supported versions of iFIX or CIMPLICITY (outlined on the Software Requirements > Compatibility with Other GE Products section).

For information about installing and updating licenses, refer to the following GE Digital Support page: https://ge-ip.force.com/communities/en_US/Article/GE-Intelligent-Platforms-Software-Product-Licensing.

**Important:**
Do not remove the USB hardware key from your node while Webspace is running. If you do, you may need to restart Webspace. You may also damage the USB key if you remove it while Webspace is running.

## Upgrading Webspace

The Webspace software installation automatically upgrades over older versions of Webspace; therefore, it is not necessary to uninstall and reinstall the Webspace software.

When upgrading iFIX with access control in a Webpsace setup, ensure that your Webspace users are part of the iFIX Windows group (IFIXUSERS by default) for access control. If you do not add your Webspace users to this Windows group, you will not be able to launch Webspace after the upgrade.

## Patching GE Software

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

Security advisories and security-related SIMs can be found on the GE website Support at https://digitalsupport.ge.com/en_US/Alert/GE-Security-Advisories. Customers can also sign up for notification of new SIMs and security advisories on the Support website.

## Patching Third-party Software

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

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

## Platform Configuration and Hardening

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

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

- Center for Internet Security: https://www.cisecurity.org
- National Institute of Standards and Technology (NIST) Repository:https://web.nvd.nist.gov/view/ncp/repository
- Microsoft: https://technet.microsoft.com/en-us/security/default.aspx

You can also ask your GE Digital Channel Representative for a copy of the iFIX or CIMPLICITY Secure Deployment Guides which cover Webspace, or visit our web site to download your own copy: https://digitalsupport.ge.com/.

### Prerequisites For Installation and Configuration

- You must be an Admin on the machine you want to install the GE products onto. Webspace must be installed with a local Windows user account with administrator rights. Be aware that you do not have to run Webspace using that account, or as an administrator.
- TCP/IP must be enabled on your computers in your setup. Administrators must have administrative rights on the server to perform the installation, and the server must have TCP/IP as a network protocol.
- Configure any external firewall and any software firewall on the server to allow TCP port 491. (By default, Webspace listens on registered port 491 for TCP packets.)
- You must have Microsoft® Internet Information Server (IIS) or Apache HTTP Server installed on your Web Server. For supported versions, see the Software Requirements topic. A Web Server (Microsoft IIS or Apache HTTP Server) must be available in order to set up the server for browser deployment of Webspace. The Webspace Server will install only if you have a supported version of Microsoft IIS or Apache HTTP Server installed beforehand. If both IIS and Apache are installed, the Webspace install will not prompt you to choose one or the other; the Webspace install defaults to IIS. If Apache is your choice of web server, simply copy over the files from < Webspace TARGET FOLDER>\Web into the Apache htdocs\ProficyWebspace folder.
- You must have Microsoft® .NET Framework 4.5 installed on your Web Server.
- Make sure you have the latest Windows updates and certificates installed (and that your certificate paths are correct). Webspace has been validated using the latest updates as of August 2019.
- The ASP .NET feature must be enabled on your Web Server.
- Proper GE licensing must exist on all computers. The licensing for WebSpace must match the version of WebSpace exactly, and must be compatible with the version of CIMPLICITY or iFIX being used. Your licensing keys must match the products you have installed.
- Decide on a security model and identify the users that you want to allow to use Webspace.
- Confirm that you do not have the "Standard VGA Graphics Adaptor" listed as the display adapter in Windows on your Web Server. Instead, the model name should appear in the list of adapters for your computer. For example, an adapter can be: Intel 82915G/GV/910GL/Express Chipset. If a model is not listed, then you may have issues with the screen resolution upon installation of the Webspace product. To check the display adapter in Windows before installing, right-click the My Computer icon on the desktop and select Properties. In the System Properties dialog box, click the

Hardware tab, click the Device Manager button, and then double-click the Display Adapters icon. If you do not have a specific model listed, and instead only the "Standard VGA Graphics Adaptor" appears, you may need to upgrade your display drivers before installing the Webspace product.

- Be sure that the color depth of the client and server computers are greater than 256 (16 million or greater is recommended).

**Note:**
For detailed requirements, please refer to the Software Requirements and Hardware Requirements topics. For detailed installation requirements on iFIX or CIMPLICITY, refer to that product's IPI for more information.

### Recommended Computer Setup

While running the Webspace Server and either the iFIX or CIMPLICITY Server on the same computer is possible, it is strongly recommended that your Webspace Server resides on a different computer than the production server (the iFIX or CIMPLICITY Server). It is also recommended that your Historian Server (if being used) resides on a different computer than your Webspace Server. Separating the Web Server from your other GE products (and behind a firewall) provides a more secure setup for your data.

**Note:**
Additionally, be aware that you cannot run the iFIX SCADA Server as a service if both servers (SCADA Server and Webspace Server) are on the same machine.

### Webspace Silent Install

You can use the InstallConfig.ini file to modify the default install settings. These settings can be viewed and changed in the Webspace Admin Console once the Webspace product has been installed.

The content of the installconfig.ini file includes:

```
[config]

; transport SSL (Encrypted) or TCP

transport=

; hostPortID 491 (default)

hostPortID=

; encryption None or 56-bit DES

encryption=
```

```
sslCertificate=

; authentication Standard or Integrated

authentication=
```

Use the following Webspace setup.exe command line options (case sensitive) to perform a silent install:

| Command Line Options | Description |
|---|---|
| /quiet | Quiet installation. No user wizard or dialog interaction, only Windows reboot dialog at the end of setup. |
| /SuppressReboot=TRUE | Suppress reboot dialog. The unattended installation still requires a reboot for successful Webspace installation. A combination of /quiet and /SuppressReboot=TRUE is equivalent to a silent installation. |
| /INSTALLDIR=<install path> | Install Webspace to a path other than the default path. |
| /inifile=<path to installconfig.ini> | Auto configuring Webspace Admin Console settings. |

The Webspace Service also sets up an application pool when IIS is detected during the installation of the Webspace product. An administrator account for Windows is required to set this up. This can be specified on the command line during the installation by using the following command line options.

| Command Line Options | Description |
|---|---|
| /pwsapppooluser=<username> | Username for configuring Webspace IIS AppPool. |
| /pwsapppoolpwd=<password> | Password for configuring Webspace IIS AppPool. |

## Installation Steps for Webspace

To install Webspace:

1. On the SCADA Server computer (recommended), install iFIX Server or CIMPLICITY Server.
2. On your Web Server, uninstall any previous builds of Webspace.
3. On your Web Server, if it is not already installed, install the iFIX View node or CIMPLICITY Viewer/Server (for supported versions see the Software Requirements topic, "Compatibility with Other GE Products" section).

> **Tip:**
> For CIMPLICITY, while the Viewer is supported, it is recommended that you use a CIMPLICITY HMI Server 75 I/O Development & Runtime System. This Server is the lowest CIMPLICITY Server I/O count that you can have that allows for network access. It also provides the best flexibility for any centralized client node.

4. Shut down any GE applications or services that run on startup. For instance, if you have Historian for SCADA Collectors configured to start when you start Windows, use the Services window to shut them down.
5. Confirm that a supported version of Microsoft Internet Information Server (IIS) or Apache HTTP Server was installed beforehand. If it is not, install it now, as the Webspace install requires it.
6. If installing on Microsoft Windows 8.x 64-bit, or Microsoft Windows Server 2012 64-bit, ensure that the ASP.NET feature is enabled:
    - In Microsoft Windows 8.x, from the Control Panel > Programs and Features, click, "Turn Windows Features on or off." In the Windows Features list, enable the following option: Internet Information Services > World Wide Web Services > Application Development Features > ASP .NET 4.5 or ASP .NET. Click OK to install.
    - In Microsoft Windows Server 2012, open the Server Manager, and click Add Roles and Features. From the Add Roles and Features Wizard, click the Server Roles link (or click through the wizard until you get to this page). Enable the following role: Web Server (IIS) > Web Server > Application Development > ASP .NET 4.5. Click Next until you get to the Confirmation page, and then click Install.

    > **Note:**
    > Microsoft Windows 8.x and Windows Server 2012 come with ASP .NET pre-installed and registered. Be sure to install the latest Windows updates. If ASP.NET 4.5 has not been registered on the Web server, you need to manually configure your Web server for ASP.NET 4.5 in order for your site to run correctly. For example, to register ASP .NET for IIS on Windows 8, use the command line: %SYSTEMROOT %\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -i. For more information on installing using the command line refer to the Microsoft MSDN web site: http://msdn.microsoft.com/en-us/library/ms229858(v=vs.100).aspx. For more information on installing other ways, refer to MSDN: http://msdn.microsoft.com/

en-us/library/5a4x27ek(v=vs.110).aspx. Also be sure to install the latest Windows updates.

**Important:**
On Microsoft Windows 7, DO NOT enable the Microsoft .NET 3.5.1 > Windows Communication Foundation HTTP Activation feature.

7. Ensure that TCP/IP is enabled prior to installation. Configure any external firewall and any software firewall on the server to allow TCP port 491.
8. Log in as a user with Administrator rights and start the Webspace installation.
9. From the Welcome screen, click Next.
10. On the License Agreement screen, to continue the installation, accept the terms of the license agreement, and click Next.
11. On the Logon credentials screen, enter the User Name and Password for the user you plan to use as the administrator for this Webspace installation (for the IIS Webspace application pool), and click Next.
12. On the Ready to Install the Program screen, click Install to begin the installation.
13. When the installation is completed, click Finish and then restart the computer.
14. Continue with configuration steps for your iFIX or CIMPLICITY software.

### Certificate Installation

If you want to use encryption with certificates, the WebSpace installer provides an Install Certificates option which you can use to create a certificate. When you click the Install Certificates option from the installer menu, the Webspace Certificate Configuration Tool opens. From here you can Create and Bind a self-signed certificate for Webspace. If the Create, Import, and Bind Certificates sections do not appear to update in the tool after the action completes, click the Restart IIS Site option. Then, restart the Webspace Certificate Configuration Tool by clicking the Install Certificates option from the installer menu again, and review the sections again.

After the certificate is created, you can then select the certificate on the Security tab in the Webspace Admin Console.

If you did not buy the strong encryption license option, you do not need to install any certificates.

### iFIX Configuration

On the SCADA Server computer:

1. Update the HOSTS file with the name of the SCADA Server, to ensure the highest reliability for connectivity. If the SCADA Server node name is different from the computer name that it was installed on, you also need to add this name to the HOSTS file. The HOSTS file on the Webspace Server should be identical to the one on the SCADA Server.
2. In Windows (Workgroup or Domain, preferably Domain), add the user accounts that you want to use with the Webspace Server. You must have the privileges to do so.
3. If you want to enable security on the iFIX SCADA node (most likely), add these same users to the iFIX SCADA through the Security Configuration application (Edit > User Accounts). iFIX must be running to access this tool and enable security (Edit > Configuration).

   **Important:**
   It is recommended that if security is enabled, that the iFIX SCADA Server and the Webspace Server reside on the same network. These same user account names will later need to be added to the Webspace Server.

   **Tip:**
   When adding users through the Security Configuration application in iFIX, be sure to select the Windows Security option for the user.

   **Important:**
   When assigning security privileges in iFIX, use care when allowing application features that could allow write access, such as the "Database Save/Reload" and "Runtime Visual Basic Editor" features, as well as creating pictures with Datalinks, or any other means to write values into tags. Use Security Areas and Security Groups to further restrict access. Also, use care when creating and sharing schedules in iFIX, so that unintended VBA code is not activated inadvertently by web sessions. For more information on iFIX Security, refer to the Configuring Security Features e-book in the iFIX online help.

4. In the iFIX System Configuration (SCU) tool, ensure that the Network Configuration is set to TCP/IP (Configure > Network), and that SCADA is enabled (Configure > SCADA).
5. Create your pictures.

On the Web Server computer:

1. Update the HOSTS file with the name of the SCADA Server, to ensure the highest reliability for connectivity. If the SCADA Server node name is different from the computer name that it was installed on, you also need to add this name to the HOSTS file. The HOSTS file on the Webspace Server should be identical to the one on the SCADA Server.
2. In Windows (Workgroup or Domain, preferably Domain), add the user accounts that you want to use with the Webspace Server. If you are on a domain, you may have already done this. You must have the privileges to do so.
3. In the iFIX Security Configuration program, add these same users accounts (Edit > User Accounts), and enable security (Edit > Configuration). iFIX must be running to access this tool and enable security. Unlike the SCADA Server, this step is not optional on the iFIX Webspace Server.

> **Important:**
> It is recommended that if security is enabled, that the iFIX SCADA Server and the Webspace Server reside on the same network. These same user account names will later need to be added to the Webspace Server.

> **Tip:**
> When adding users through the Security Configuration application in iFIX, be sure to select the Windows Security option for the user.

> **Important:**
> When assigning security privileges in iFIX, use care when allowing application features that could allow write access, such as the "Database Save/Reload" and "Runtime Visual Basic Editor" features, as well as creating pictures with Datalinks, or any other means to write values into tags. Use Security Areas and Security Groups to further restrict access. Also, use care when creating and sharing schedules in iFIX, so that unintended VBA code is not activated inadvertently by web sessions. For more information on iFIX Security, refer to the Configuring Security Features e-book in the iFIX online help.

4. In the iFIX System Configuration (SCU) tool:
    a. Open the WEB.SCU file. If an iFIX View node is not installed before you install Webspace, you will need to manually create the WEB.SCU file; the WEB.SCU will not automatically be created if you install Webspace before iFIX View node.
    b. Verify that Network Configuration is set to TCP/IP (Configure > Network), that SCADA is disabled (Configure > SCADA), and that Workspace.exe appears in your tasks list (Configure

> Tasks). By default, these settings are automatically configured during install. If these settings are not correct, update them now.

c. Specify the name of your iFIX SCADA Server in the Remote Nodes list (Configure > Network).

5. Either copy your pictures from the SCADA Server to the PIC folder on the iFIX Webspace Server (recommended for optimum performance), or map a drive to your PIC folder on your SCADA Server. If you map a drive for pictures:
    a. If you are using shared drives with Local Windows users (not on the Domain), make sure that the user is present on both the Webspace Server machine, and the machine which contains the shared folder.
    b. In the SCU on the Webspace Server, open WEB.SCU and point the picture folder to that mapped drive letter (Configure > Paths).
    c. Update the LoginScript.bat file provided in the C:\Program Files\Proficy\iFIX Webspace Server\Programs folder with the mapped drive information, and then add the script name to the Session Startup options in the Webspace Admin Console. For more information, refer to the online help for the Webspace Admin Console.
6. Optionally, in the Webspace Admin Console, configure printer options and other session properties. For more information, refer to the online help for the Webspace Admin Console.
7. If you want to configure multiple input locales for your web sessions, add the input language and keyboard layout for that locale to the Regional Settings on the Webspace Server. For more information, refer to the online help for the Webspace Admin Console.

### Tips for Web Server Setup

- You can find the HOSTS file in the C:\WINDOWS\system32\drivers\etc folder.
- Use a text editor such as Notepad to edit the HOSTS file, and do not add a file extension to the file.
- An example entry in the HOSTS file is as follows: 198.212.170.4 SCADA01.
- If SCADA1 was the iFIX SCADA Server node name, but the computer name where the iFIX SCADA Server was installed was AREA1, you would need to add a second line to the HOSTS file for AREA1: 198.212.170.4 AREA1.
- If you do not know the TCP/IP address of the SCADA computer, run the IPCONFIG command on the SCADA Server.
- The same, identical entries should appear in the HOSTS file for the SCADA Server and the Webspace Server.
- In an Enhanced Failover setup, make sure that the primary and secondary servers are separate from the Webspace server.
- If iFIX is installed after Webspace, manually create and configure a WEB.SCU file if iFIX is to be used with Webspace.

## CIMPLICITY Configuration

- On the Web Server computer, configure Windows-based security or Standard CIMPLICITY security for CIMPLICITY.

  **Important:**
  Make sure the same security is configured for both the CIMPLICITY Server and Webspace servers.

- Make all of the paths (with their folders) that will be shared for the Web Clients read-only. This will avoid running into the Microsoft limitation for sharing files.
- On the CIMPLICITY Server, to publish a web page for a CIMPLICITY CimView screen, right-click the CIMPLICITY Options application and run as Administrator. On the Webspace tab, click the "Create a Web Page" button. The next dialog box allows you to select the screen that you want and creates a web page for it; if it does not pick up the default Webspace directory to place the html file in, you will need to enter it. If it's an Apache server, you will need to browse to the location of the Apache Server; by default, the Apache Server location is: "C:\Program Files (x86)\Apache Software Foundation\ApacheX.Y\htdocs\ProficyWebspace", where X.Y is the Apache version number.
- Run the CimView screen(s) natively in Cimview.exe on the Webspace Server to ensure proper Viewer-to-Server communications are established. Since your CIMPLICITY project server(s) are most likely remote to the Webspace Server, it is highly recommended that CIMPLICITY Deployment is configured to synchronize files with the Webspace Server (and keep them up-to-date).
- Do not use shared CimView screens. If you do, every client that connects will need to create their own share, which could run the server out of resources. This could increase the time it takes a user to log in, and could make the server fail.
- A separate CimView.exe and CimLayout.exe session runs for each Webspace session with CIMPLICITY.
- For the CIMPLICITY Windows Desktop Client, be sure that the command line parameter "-r" specifies the command line parameters for CIMVIEW. For example, -r CIMVIEW "C:\MyProject \screens\MyScreen.cim" will open the correct screen, as long as -r comes after the -a parameter, and all the other parameters are correct. For example: "C:\Program Files (x86)\Proficy\Proficy Webspace\Client\Proficy.exe" -h MyServer -c -a CimView -r CIMVIEW "c:\screens\userscreen.cim"
- Do not configure the Webspace machine for Power Save or Lock; either feature can block Web Clients from connecting or cause them to lose an active connection.
- If the session has been configured to Zoom to Best fit, the CimView screen will fit into the ActiveX container. The ActiveX container will conform to the Internet Explorer size when the URL is accessed.

- The ActiveX Control or plug-in fits into the size of the browser when the URL is accessed; the size does not change when you resize the browser. Therefore, make sure the browser is the size you want before you go to the URL that will start the Webspace session.
- Make sure in a redundant SCADA server setup, that the primary and secondary servers are separate from the Web Space server.
- Optionally, in the Webspace Admin Console, configure printer options and other session properties. For more information, refer to the online help for the Webspace Admin Console.
- If you want to configure multiple input locales for your web sessions, add the input language and keyboard layout for that locale to the Regional Settings on the Webspace Server. For more information, refer to the online help for the Webspace Admin Console.

### Terminal Services Configuration

Do not install Webspace on a CIMPLICITY or iFIX Server that has already been configured as a Terminal Server. This type of installation is not supported.

### Migration from iFIX Webspace or Globalview to Webspace

Direct upgrades from iFIX Webspace or Globalview are NOT supported. To use Webspace, you must first manually uninstall iFIX Webspace or Globalview, and then follow the install steps above. You will need to configure the web.scu (for iFIX) and republish your {cimpscreen}.html to the Web Server again (for CIMPLICITY), and possibly update some security settings.

**Important:**
Before you uninstall the previous version: If you changed any of the default settings in the Host Options dialog box on the Webspace or Globalview Server or any other settings, you will need to re-enter these changes in the Administration application after upgrading. Be sure to take note of these settings before uninstalling the software so that you can enter them again after installing the new Webspace.

Be aware that if you try to install Webspace before uninstalling either of these applications, a message will appear reminding you that you need to manually uninstall the previous product.

If you run Webspace from the URL, be aware that the URL has changed. The new URL is http://<WebspaceServerName>/ProficyWebspace/<filename>.html, (for iFIX filename.html = iFIX.html and for CIMPLICITY it is {cimpscreen}.html), where WebspaceServerName is the computer name of your Webspace Server.

Also, be aware that the iFIX.exe and Globalview.exe executables no longer exist in the new Webspace. The command has been replaced (in the Windows client) by proficy.exe -a iFIX |CimView.

The executable which installs the Windows Desktop Client has also changed in Webspace. The Globalview client installer (globalview-client.windows.exe) and iFIX Webspace client installer (iFIX-client.windows.exe) both have been replaced by proficy-client.windows.exe. You can still find this installer on the Webspace Server computer in the directory where you publish the Webspace files to be hosted by your IIS or Apache server, on the product DVD in the Setup\Proficy\Webspace\WebspaceServer subfolder, or in the Webspace install folder, which is by default the C:\Program Files\Proficy\Proficy Webspace\Web \Clients folder.

**Important:**
The logon.html file that existed in the previous iFIX Webspace and Globalview applications no longer exists. Do not use logon.html with Webspace.

Finally, be aware that if you use a Relay Server configuration for iFIX, there may be changes that need to be made there.

## Troubleshooting Tips

| Issue | Steps to Troubleshoot |
|---|---|
| Client Connection Error | 1. Confirm that the web service is operational, by attempting a connection to the web server, http://ServerName. If it fails, troubleshoot IIS/Apache itself.<br>2. If successful with the connection, confirm that you can connect using http://ServerName/proficywebspace. A successful connection will show a list of GE products (iFIX or CIMPLICITY).<br>3. If it fails, examine the IIS configuration on the Webspace server. Open IIS Manager and view the ProficyWebspace application pool. It should have a running sign. If it shows a stopped status, open its advanced properties and set a local administrator's credentials. Restart the IIS service. |

| Issue | Steps to Troubleshoot |
| --- | --- |
| | 4. If there is still an issue, open your browser and verify that JavaScript is enabled. With JavaScript enabled you should receive the option to connect to iFIX or CIMPLICITY when navigating to http://ServerName/proficywebspace.<br>5. If you receive an error when opening http://ServerName/proficywebspace, view the error description and make sure the prerequisite items are installed (including the ASP .NET and HTTP Activation features).<br>6. If the error indicates something about a conflicting config.ini, locate it and delete it (or rename it).<br>7. If Webspace still does not start, confirm that the user credentials entered during the product install are correct. The user must be an Administrator, and the password must be correctly entered. A user who is not an Administrator or using an invalid password will cause the Webspace to fail during start. Incorrect user credentials cause the WebspaceAppPool to fail. This failure causes an HTTP 503 error (the service is unavailable) when accessing the http://webspaceserver/proficywebspace URL.<br>8. To fix this issue, open the IIS administration tool and locate Application Pools in the left pane, and right-click the ProficyWebspaceAppPool. Select the Identity property, and supply the correct administrator credentials, and then restart the ProficyWebspaceAppPool.<br>9. Attempt to log in again.<br>10. If there is still an issue connecting to http://ServerName/proficywebspace on Apache, |

| Issue | Steps to Troubleshoot |
| --- | --- |
| | make sure that the \proficywebspace folder is copied to Apache's htdocs and that the contents are correct. The contents of the \proficywebspace folder under htdocs must be identical to that of the c:\program files \proficy\proficy webspace\web folder.<br>11. On Apache, also check the spelling of the folders and links. Some versions of Apache might be case-sensitive. |
| HTTP Error 500.19 Internal Server Error appears and session cannot be established | If this error occurs, delete the Web.config file in C:\Program Files\Proficy\ ProficyWebspace\Web folder, and then try to re-establish a connection. |
| Session cannot connect with Strong Encryption enabled | When using the certificate installed with Webspace and strong encryption, you cannot start a Webspace session with the IP address of the WebSpace server. The IP address cannot be used for the host name. Use the Full Computer Name in the URL instead. The option to increase is only available if your license includes the Strong Encryption option. |
| Error with Verify Trust | This error is usually the result of outdated root certificates. Ask your IT department for guidance on how to update them. |
| Webspace Session Connects but Has Other Recurring Server-side Issues | Set the APS log level to 4. You can set the logging level in the Webspace Admin Console, by selecting Tools > Host Options, and then clicking on the Log tab. Enter the logging number in the Output Level field. Repeat test(s) and capture logs to send to GE Digital Support for Analysis.<br>  **Note:**<br>All log files, whether they pertain to the client or server machine, are located on the Webspace Server. The Log folder in the |

| Issue | Steps to Troubleshoot |
|---|---|
| | Webspace install folder contains all the aps_* log files. (A new log file is created each time the Webspace Application Publishing Service is started.) |
| Required Paths and Programs are Missing After Whitelisting is Enabled | The symptoms for this scenario will differ based on what is missing. But the Application Publishing Service log will show that an attempt was made to start and stop those applications. |
| Application Publishing Service fails to start | All the paths and programs are in the list, but the Application Publishing Service fails to start after enabling whitelisting. Try editing the WorkspacePropertyDefinitions.xml file. If the Application Publishing Service will not start after editing the XML file, it may be because of syntax issues (for example, a missing ; or ") or case-sensitivity (the value must be lowercase; for instance: "true" or "false"). |
| Help Not Accessible in Web Sessions | Help has been disabled from web sessions when in whitelist mode. |
| Cmd.exe Excluded from the Whitelist | Since adding cmd.exe introduces the potential for a Webspace user to run operating system commands, it has been removed from the default whitelist. As a secure configuration practice, GE advises against including this command in the list. |
| Third Party Items and Whitelisting Issues | • For any third-party products, the install paths should be added along with any programs with the right permissions to include all sub directories.<br>• Any additional dependencies such as .NET frameworks, and so on, should be included.<br>• When in doubt turn on the SandBoxLog to accurately pick up the missing executable as they will be clearly spelled out in the debug view logs. |

### Using Debug Mode for Whitelisting

An administrator can turn on the whitelisting debug view logs as follows:

1. Add a DWORD registry value named SandBoxLog under the HKLM\Software\Proficy\Proficy Webspace\AppServer key and reboot.
2. If this value exists and is set to a non-zero value, the user SandBox feature will output a debug message any time it blocks access to a process or a file. The message will include the path to the process or file that was blocked.
3. To capture this output, run DebugView on the host and enable both of the kernel options under the Capture menu. You can download DebugView from: https://technet.microsoft.com/en-us/library/bb896647.aspx
4. If the SandBoxLog value exists and is set to 0, the driver will not output debug messages when it blocks access to a file or process.
5. The Administrator will have to manually create the SandBoxLog registry value. Therefore, the option will be off by default. The following is a sample debug view log:

```
00000032 68.71609497 m_ZwCreateSection ERR __110__: C0000022
```

The hexadecimal values of the XML texts used for SandBox access permissions are as follows:

| Description | XML Text | Hexadecimal Value |
|---|---|---|
| No access is allowed. | ACCESS_DENIED | 0x00 |
| Only read access is allowed. | ACCESS_READ | 0x01 |
| Both read and write are allowed. | ACCESS_WRITE | 0x03 (0x02 \| ACCESS_READ) |
| Filter none. Allow files and folders to be listed recursively. | ACCESS_ALLOW_DESCENDANTS | 0x10 |
| Wildcard. Allow all files within a folder to be listed. | ACCESS_ALLOW_ALL_CHILDREN | 0x20 |
| Whitelist. Allow only whitelisted files and folders to be listed. (This bit is for the internal mechanisms of the SandBox and should not be added unless instructed.) | ACCESS_ALLOW_VISIBLE_CHILDREN | 0x40 |

The permissions log can help, for example, if you have added a folder with READ + Visible all, but debug indicates that SandBox is blocking the access to the file. In general, SandBox blocks the handle creation to a given file/folder according to the requested permissions. In other words, even if an application only reads from a certain file, but it requested full access to it (such as WRITE), SandBox will block it from accessing the file in the first place.

Example diagnosis of log: P=0x01 indicates there is a write problem because only read access is allowed. So you would need to go back and open up the Common Files path to have ACCESS_WRITE permissions as well.

### Whitelisting Best Practices

- Wherever possible, you should use environment variables in the whitelist paths (for example, %ProgramFiles(x86)%\Microsoft Visual Studio 9.0\Common7\IDE\devenv.exe;). This will allow the DefaultWorkspaceProperties.xml file to be transferred to systems that might have different versions of Windows.
- Every blocked access entry does not need to be added to the path. Add the entries to the path only if the application is not working correctly.
- Begin by giving all permissions and include the parent path. Once everything is working properly, you can then evaluate folder by folder and analyze each flag to restrict access.
- Be sure to check GE Digital Support (https://digitalsupport.ge.com) for KB articles that may help you in troubleshooting.

## Unsupported Items and Recommendations

The following items are currently not supported by the Webspace product:

- **Not Listed Browsers:** Other browsers such as Netscape and Opera.
- **Microsoft Internet Explorer (64-bit) Browser:** WebSpace does not support running the WebSpace client sessions on a 64-bit Internet Explorer browser; only 32-bit Internet Explorer browsers are supported.
- **Change Management:** Change Management from GE Digital is not supported. For iFIX, be sure that the Logon on WorkSpace Startup option is cleared on the Change Management tab in the User Preferences dialog box in the WorkSpace.
- **Configure Mode for the iFIX WorkSpace:** Webspace sessions in configure mode are not supported. Only the WorkSpace run mode is supported. By default, when you log on to a Webspace session from a supported browser, you automatically enter run mode. Several configuration tools (such

as Key Macro Editor, Visual Basic Editor, Startup Profile Manager, and others) will not open in the Webspace session.

- **Dell Wyse T50 Thin Client**: This client is not supported or tested on the current version of Webspace.
- **Enhanced Failover:** iFIX Enhanced Failover is not supported if the Webspace Server is running on either of the SCADA machines configured in a redundant pair. Enhanced Failover is supported, however, if the Webspace Server machine is separate to the SCADA pair.
- **Environment Protection:** iFIX WorkSpace environment protection settings from the web session are not supported.
- **FIX32 Nodes:** Be aware that connections to FIX32 nodes are not supported by Webspace. For instance, in this case, you should not have animations or datalinks that point to FIX32 SCADA nodes in your web session pictures. This includes WorkSpace .GRF and View .ODF picture files.
- **iFIX Alarm ODBC:** Alarm ODBC in the Webspace client is not supported.
- **Integrated Windows Authentication**: Only available to users who sign-in from Windows computers that are members of the same domain as the Webspace Server.
- **Modem Connections:** Connecting a client to the Webspace Server using a modem is not supported.
- **Network Folder for Logs:** Webspace Server logs stored directly in a network folder are not supported.
- **Older Operating Systems.** For example, the following operating systems are NOT supported with the Webspace Server: Microsoft Windows XP, Microsoft Windows Server 2003, the 32-bit versions of Microsoft Windows 7 and Microsoft Windows 8.x (32-bit only). The following operating systems are not supported for clients: Microsoft Windows Pocket PC and Windows CE.
- **Operations Hub:** You cannot install Operations Hub by GE Digital on the same computer as the Webspace Server.
- **Operations Hub Webspace Widget:** This widget does not support configuring relay server-based dependent hosts.
- **Plant Applications:** Plant Applications is not supported in this version of Webspace. Customers requiring either a 32-bit application or Plant Applications support should not upgrade Webspace to version 5.0 or greater.
- **Power Users:** Logging into Webspace Server as a Power User is not supported. To open a session to the server, log in as a member of the standard Users group.
- **Remote Desktop:** The Microsoft Remote Desktop Client is not supported in Webspace sessions.
- **Right-to-left Languages:** Right-to-left languages are not supported.
- **Running iFIX as a Service on the Webspace Server machine**: You cannot run iFIX as a service on the Webspace Server.

- **Running the Webspace Client and Server on the Same Computer:** Running Webspace sessions (browser or desktop client) on the same machine where the Webspace Server is installed is not supported.
- **Running the SCADA Server on the Same Machine as your Webspace Server:** It is strongly NOT recommended to run the Webspace Server on the same computer as your SCADA Server. The SCADA Server should reside on a different machine than the Webspace Server. An exception to this guideline would be a small system (with less than 5 Webspace clients) that does not used advanced iFIX capabilities such as Enhanced Failover.
- **Terminal Server:** A Terminal Server running on the same machine as the Webspace Server is not supported.
- **THISNODE feature:** THISNODE, which applies to the View nodes communicating with a remote SCADA, is not supported from the web session.
- **UNC Paths and Install:** Installing the product from UNC paths is not supported or recommended.
- **Undocumented Command Line Options:** The following startup parameters are not currently supported from a browser shortcut: bInBrowser, compression, printerconfig, clientframe, multimonitor, width, height, embed, noscale, clientscale, and ClientDPIScalingEnabled.
- **Undocumented Functionality:** Some items mentioned in the previous user help, such as the logon.html, the support request wizard, licensing servers, smart card authentication, and the AllClients.html are not supported in the current Webspace product. If it is not documented, it is not supported.
- **VMWare Advanced features:** Advanced features of ESXi Server, such as VMotion and Clustering support, have not been tested with Webspace. VMware WorkStation and Player are not supported. USB to serial communications is not supported. Power meter functions and options, and suspending images to conserve power are not supported. Setting up additional device connections to the virtual machine through a HOST is not supported.
- **Web HMI:** You cannot install Web HMI by GE Digital on the same computer as the Webspace Server.

# Software Requirements

### Server Operating Systems

**Important:**
Since operating systems have continuous updates, be sure to run the Windows update feature to get the latest software.

- Microsoft® Windows® Server 2022
- Microsoft® Windows® Server 2019
- Microsoft® Windows® 11
- Microsoft® Windows® 10 (Build 21H2 or higher).

Be aware that:

- Microsoft Windows 11 Build 22H2 is currently not supported.
- Windows Server operating systems are recommended for multi-user environments.
- The Webspace Server is not supported on 32-bit operating systems.
- Make sure you have the latest Windows updates and certificates installed (and that your certificate paths are correct). Webspace has been validated using the latest updates as of January 2023.

### Browsers

- Mozilla® Firefox®
- Apple® Safari 12 or later on Mac OS X
- Google® Chrome
- Microsoft® Edge

### Client Operating Systems

- Microsoft® Windows® 11 Pro and Enterprise (64-bit)
- Microsoft® Windows® 10 Pro and Enterprise (32-bit/64-bit)
- Microsoft® Windows® 7 with Service Pack 1 (32-bit/64-bit)
- Mac OS X 10.13 and later
- Red Hat Enterprise Linux and 7 and 8 (64-bit)
- CentOS 7 and 8 (64-bit)
- SUSE Linux Enterprise Desktop 12 and 15 (64-bit)
- Ubuntu 19 and 20 (64-bit)
- iOS 12.0 and later
- Android 9.0 or later on ARM processors, including Chromebooks manufactured in or after 2019

**Note:**
The following operating systems are not supported for Webspace client sessions: Windows Pocket PC and Windows CE.

### Web Server Software

- Microsoft® .NET Framework 4.5 installed on your Web Server.
- Microsoft Internet Information Server (IIS) 7.x, or 8.x.
- Apache HTTP Server 2.x.

**Important:**
Apache and IIS Web servers and their sub-components (such as, OpenSSL) must be maintained and patched as per the latest security guidelines provided by their respective software vendors. The security of Webspace sessions depends on the security that the web servers provide.

### Mobile Operating Systems

- Apple iOS 12 or later, including the iPad, iPhone, and iPod Touch.
- Android version 9.xx or later, and 4GB of memory or greater. (Webspace Android Client only supports ARM processors.)

For iPad tablets, you must install the CA certificates on the iPad clients to establish a trusted connection and to receive live data.

### Support for Applications Using DirectX

Applications that use DirectX, such as Microsoft Office 2013 or Office 2016, will not run in Webspace sessions on Windows Server 2008 R2 or Windows 7 when Windows Update KB 2670838 is installed. To work around this issue, uninstall KB 2670838.

Background: Windows Update KB 2670838 replaces the user-mode DirectX runtime with a version that requires display drivers to support DirectX. The Webspace display driver does not support DirectX in versions 4.71 and earlier. Beginning in version 4.8, the Webspace display driver supports DirectX, but only on Windows 8, Windows 8.1, Windows Server 2012 and Windows Server 2012 R2. The Webspace driver only supports DirectX on these versions of Windows because it relies on a Windows component that is not available in earlier versions of Windows.

### Other GE Software Requirements

- Network interface software for network communication and certain I/O drivers for your GE applications. TCP/IP must be enabled as a network protocol on your computers in your setup. Configure any external firewall and any software firewall on the server to allow TCP port 491. (By default, Webspace listens on registered port 491 for TCP packets.)

- Administrators must have administrative rights on the server to perform the installation.
- The ASP .NET feature must be enabled on your Web Server.
- Proper GE licensing software must exist on all computers in your setup.
- If you are using third-party software along with Webspace, make sure that the third-party software is also supported for the operating system you are running Webspace on.
- An I/O driver for SCADA servers. GE supplies I/O drivers for many programmable controllers, or you may purchase a driver separately.

### Compatibility with Other GE Products

| GE Digital Product | Required Version |
|---|---|
| CIMPLICITY | 10.0 or greater. |
| iFIX | 6.1 or greater. |

## Hardware Requirements

**Important:**
While running the Webspace Server and the SCADA Server on the same machine is supported, it is strongly recommended that production SCADA Server reside on a different machine than the Webspace Server. Also, SpeedStep® technology is not supported and must not be enabled on either server.

### Webspace Server - Fewer than 5 Clients

The following minimum hardware recommendations apply when using the Webspace Server on a low-end machine supporting fewer than five Webspace sessions, and Webspace projects with pictures that have a small number of animation, shapes, and graphics:

- For iFIX: A 3.0 GHz Intel® Core™ i5 Processor or equivalent.  For better performance, please consider using higher.
- For CIMPLICITY: In general, a Webspace Server with CIMPLICITY can support a 500 MHz CPU.
- Webspace supports a maximum round-trip latency of 500 milliseconds.
- 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.

> **Note:**
> With VMware ESXi Server, the host and guest operating system need to synchronize against an external physical Network Time Protocol (NTP) 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 8 GB RAM. For better performance, please consider using more.
- A minimum of 10 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 SCADA alarm and historical data files can 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 GE products, such as CIMPLICITY and iFIX, impose additional requirements. Refer to the Important Product Information (IPI) topic in the product's electronic books for specific system requirements.
- A DVD drive.
- 100 MBit or faster Full Duplex TCP/IP-compatible network interface adapter for 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:**
> Webspace does not support IPv6. If you disable IPv6 to use Webspace, 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 with 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.

### Webspace Server - Up to 60 Clients

The following minimum hardware recommendations apply when using the Webspace Server on a high-end machine that can support up to 60 clients:

- For iFIX: 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).
- For CIMPLICITY: In general, a Webspace Server with CIMPLICITY can support a 500 MHz CPU.
- Webspace supports a maximum round-trip latency of 500 milliseconds.
- 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.

> **Note:**
> With VMware ESXi Server, the host and guest operating system need to synchronize against an external physical Network Time Protocol (NTP) 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 32 GB RAM. For better performance, please consider using more.
- A minimum of 10 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 SCADA alarm and historical data files can 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 GE products, such as CIMPLICITY or iFIX, impose additional requirements. Refer to the Software Requirements and Hardware Requirements sections for specific system requirements.
- A DVD drive.
- 100 MBit or faster Full Duplex TCP/IP-compatible network interface adapter for 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:**
> Webspace does not support IPv6. If you disable IPv6 to use Webspace, 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 with 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.

> **Note:**
> For better performance, considering using an external graphics card with a PCI-E interface adapter with 512MB RAM or better.

- Two-button mouse or compatible pointing device (such as a touch screen) that is capable of opening a context menu.

### Webspace Clients

The speed of the client computer viewing the Webspace client session through a browser can also impact performance. Faster client machines typically load Webspace pictures much quicker, and have improved performance while those pictures are open. For instance, in testing, a slow client with 512 MB RAM and 1.5 GHz processor had picture load times approximately 1.5 times longer than a faster client with 1 GB RAM and 3.0 GHz processor.

Network speeds and connection types also impact performance for a Webspace session. A 100 MBit or faster network adapter, which is recommended, allows the Webspace session to utilize optimum speed for its performance. Companies using VPN connections for Webspace sessions may experience a decrease in performance.

> **Important:**
> Running Webspace client sessions (browser or desktop client) on the same computer as a Webspace Server is not supported. Webspace does not support running the Webspace client sessions on a 64-bit Internet Explorer browser; only 32-bit Internet Explorer browsers are supported.

## Known Issues

The following table lists the known issues in Proficy Webspace.

| Defect Number | Area | Description |
|---|---|---|
| N/A | Sound | Sound Does Not Work in Webspace Sessions |

| Defect Number | Area | Description |
|---|---|---|
| | | To play sounds in Webspace sessions, re-install proficy-host.windows_x64.exe on your web server. You can find this executable on the install media in the WebServer folder. If Webspace is installed in a virtual environment, make sure the Audio card is connected to the host and that it is available to the virtual machine when powered on. |
| DE5356 | Uninstall | Uninstall keeps Display Driver.<br><br>After a Webspace uninstall, all Webspace components should be removed. However, after a reboot, the iFIX Webspace Display Driver is still in the Device Manager.<br><br>When upgrading Webspace, you may be prompted to uninstall iFIX Webspace. After the uninstall and a system reboot, the iFIX Webspace Display Driver may still be in the Device Manager. You must manually remove the iFIX Webspace Device Driver. |
| US12012 | Sound | When you turn on the Sound Option for the first time in an iFIX Webspace session, the client session may fail.<br><br>After attempting to turn on the Sound Option, stop and then start your Proficy Webspace Application Publishing Service found in Control Pane->System and Security->Administrative Tools->Services. Otherwise, reboot. Then, this allows you to toggle this option on and off. |
| DE8244 | The /p option with iFIX 5.5 and higher versions | The /p command line option does not work in iFIX 5.5 and higher versions.<br><br>The /p command line option is not supported in iFIX 5.5 and higher versions, and will not work. For example, the following command line results in an error:<br><br>"C:\Program Files (x86)\Proficy\Proficy Webspace\Client \Proficy.exe" -h MyServer -c -a iFIX -r IFIX /puserscreen.grf. |

| Defect Number | Area | Description |
|---|---|---|
| DE8323 | Long File Names on Disk Volume | Webspace displays the error " Can Not Start SCADA on Browser session" when iFIX 5.8 and Webspace 5.0 are installed on a disk volume that has 8dot3name disabled.<br><br>When using Webspace with iFIX 5.8 on a disk volume with only long file name support (8dot3name disabled), then iFIX SIM iFIX58_SCU_001 is required to start a Webspace session. This issue does not exist with iFIX 5.9 or greater. |
| DE10226 | iFIX .NET Component | "Failed to create component" error appears when re-opening an iFIX picture that contains a .NET Component.<br><br>This error will not be encountered if the CacheEnable property in your iFIX picture is set to False. |
| US12012 | Client | Sound Not Working Properly on Webspace Client.<br><br>When an Administrator enables the Sound option on the Client Access tab of the Host Options dialog box in the Webspace Admin Console, the Windows Audio Service may fail to start. If this happens, sounds will not play on Webspace clients. |
| N/A | Windows 10 Hosts | 32-bit Version of Internet Explorer Fails to Start.<br><br>The 32-bit version of Internet Explorer fails to start in Webspace sessions on Windows 10 hosts. Use Microsoft Edge instead. |
| N/A | Windows 10 and Windows Server 2016 hosts | Password Expiration Message Box Clipped.<br><br>On Windows 10 and Windows Server 2016 hosts, the message that notifies a user that his or her password is about to expire is clipped. |
| N/A | Windows 8.1 and Windows 10 Clients | Cannot Add a Client Printer.<br><br>Cannot add a client printer from Windows 8.1 and Windows 10 clients when the Universal Printer Driver and Windows Printers Drivers are both enabled in the Webspace Admin Console. |

| Defect Number | Area | Description |
|---|---|---|
| N/A | Windows 7 | Office 2013 and Other Applications Using DirectX Do Not Run in Webspace Sessions.<br><br>Applications such as Office 2013 that use DirectX will not run in Webspace sessions on Windows Server 2008 R2 or Windows 7 when Windows Update KB 2670838 is installed. To work around this issue, uninstall KB 2670838.<br><br>Background: Windows Update KB 2670838 replaces the user-mode DirectX runtime with a version that requires display drivers to support DirectX. The Webspace display driver does not support DirectX in versions 4.8.1 and earlier. Beginning in version 4.8.2, the Webspace display driver supports DirectX, but only on Windows 8, Windows 8.1, Windows Server 2012, and Windows Server 2012 R2. The Webspace driver only supports DirectX on these versions of Windows because it relies on a Windows component that is not available in earlier versions of Windows. |
| N/A | IIS | MIME Types for Needed Extensions Do Not Exist.<br><br>When the web server on the host is IIS, and IIS is configured to only serve documents with file extensions that are registered MIME types, files with the following extensions may not download: .deb, .crx, .dmg, .xpi. For example, Firefox may display the following error message when a user attempts to install the plug-in: “Not a valid install package.” To resolve this issue, define a MIME type for the needed extensions as described in Microsoft Knowledge Base article 326965 (http://support.microsoft-.com/kb/326965). For the Chrome Extension, specify the MIME type as application/gg-chrome. |
| N/A | Total Defense Anti-Virus | Sessions Fail to Start on Webspace Hosts after an Upgrade of the Operating System.<br><br>Sessions fail to start on Webspace hosts after the operating system is upgraded. To work around this issue, uninstall and reinstall the Webspace Display Driver: Users |

| Defect Number | Area | Description |
|---|---|---|
| | | must disable the firewall from Total Defense Anti-Virus before a client is able to connect to a Webspace host. |
| DE106751 | iFIX Autologin | iFIX Windows Autologin user does not work with the Webspace Client.<br><br>For Webspace auto login to work, be sure to enable the Integrated Windows Authentication option in the Host Options dialog box > Authentication tab, and add the SHOWIFIXLOGIN=0 line in the Fixuserpreferences.ini file in the iFIX Local folder under the WebspacePreferences section. |
| N/A | Firefox | Encrypted browser session does not open in Firefox.<br><br>Firefox does not, by default, recognize certificates in the Windows certificate store. Use an enterprise policy to add CA certificates and set the *ImportEnterpriseRoots* key to True. In Firefox, type about:config to access the configuration. Configure the security.enterprise_roots.enabled setting to true. For more information, see: https://support.mozilla.org/en-US/kb/setting-certificate-authorities-firefox |
| N/A | Zero Install App | When you run the Webspace App and the Webspace App is either not installed or not enabled (for example, the useApp URL parameter is set to false), only text can be cut, copied, or pasted between local and remote applications.<br><br>In addition, users must type CTRL+X, CTRL+C, and CTRL +V to cut, copy, and paste text between local and remote applications. In this configuration, the Cut, Copy, and Paste menu options of applications running in a Webspace session cannot be used to transfer data between local and remote applications; they can only be used to transfer data between applications that are running within the Webspace session. |
| N/A | Internet Explorer | When a user runs the Webspace App in Internet Explorer and the Webspace App is either not installed or not en- |

| Defect Number | Area | Description |
|---|---|---|
| | | abled, the first time the user types CTRL+X, CTRL+C, or CTRL+V, Internet Explorer may display the following message:<br><br>“Do you want to allow this webpage to access your Clipboard?<br><br>After the user dismisses this message by clicking either Allow access or Don’t allow, double characters may be displayed every time the user presses a key. To work around this issue, press and release the CTRL key.<br><br>In addition, in the case where the user types CTRL+C, the selected text may be replaced by a “c”. To work around this issue, use the application’s Undo function (e.g., type CTRL+Z) to restore the deleted text.<br><br>The above message is only displayed once per session. These issues do not occur when the user subsequently presses CTRL+X, CTRL+C, or CTRL+V to cut, copy, or paste text within an instance of the Webspace Web App. |
| N/A | All browsers | When you run the Webspace App in Google Chrome or Mozilla Firefox and types CTRL+N or CTRL+T, the browser opens a new window or a new tab, respectively. Similarly, when a user runs the Webspace Web App in Internet Explorer and types CTRL+O or CTRL+P, Internet Explorer opens its File Open or Print dialog, respectively. In these, and other cases, browsers do not allow the Webspace App to suppress their default behavior. |
| N/A | Safari | When the Webspace App is moved to a background tab on Safari on Mac OS X, the client is disconnected from the session. |
| N/A | Internet Explorer 11 | When users browse to Webspace Hosts from Internet Explorer 11 on Windows 7, they are prompted to install the Webspace App even if the app has been installed. |
| N/A | Scaling | DPI Scaling may not work in the Webspace App. |

| Defect Number | Area | Description |
|---|---|---|
| N/A | All browsers | The Webspace App may not start automatically after it is installed. If this happens, click the reload link. |
| N/A | Windows Server 2019 | When the Webspace Host installer is run on Windows Server 2019, the computer may not restart when the installer's Restart button is clicked. If this occurs, simply restart the computer from the Start menu. |
| N/A | 64-bit Chrome and Firefox | No content is displayed in the browser when 64-bit Chrome or 64-bit Firefox is run in a Webspace session. To work around this issue in Firefox, set browser.tabs.remote.autostart.2.false in about:config. There is no known workaround for this issue in Chrome |
| N/A | Microsoft Word | Files cannot be saved on the local computer from Microsoft Word running in a Webspace session on a Windows 10 host. |
| N/A | Webspace Admin Console | The context-sensitive help does not display or displays the wrong content. The workaround is to use the help from the Help menu from within the application. |
| N/A | Session Startup | Sometimes the time needed to start the first WebSpace client session appears long. This applies to the first session only. |
| DE116666 | Session Startup | When using the certificate installed with Webspace and strong encryption, you cannot start a Webspace session with the IP address of the WebSpace server. The IP address cannot be used for the host name. Use the Full Computer Name in the URL instead. |
| N/A | Session Startup | The WebSpace session cannot be established and an HTTP Error 500.19 Internal Server Error appears. If this occurs, delete the Web.config file in C:\Program Files\Proficy\ ProficyWebspace\Web folder, and then try to establish a connection again. |
| N/A | Relay Server | When using the Failover Relay Server with Strong Encryption, the clients are not able to connect to a secondary Webspace Server. |

| Defect Number | Area | Description |
|---|---|---|
| | | In this instance, Webspace client sessions can connect to the primary Webspace server. But, when the primary server becomes unavailable, clients are unable to connect. |
| DE190281 | Startup | When using the Webspace widget on an Operations Hub page and the iFIX Access Control is disabled, the Windows built-in Administrator user account or a Standard user account (a user who only belongs to the USERS group) can launch the iFIX Workspace from a Webspace session without the UAC (consent.exe) appearing. However, any user who belongs to the Administrators group will see the the UAC prompt. If iFIX Access Control is enabled, no UAC promopts appear. |
| N/A | Loose Mode | When running WebSpace Sessions in “Loose Mode” (using command-line options useApp=true&embed=false) or using the Desktop Client (Proficy WebSpace - AllUsers App), the iFIX Screen Saver experiences blank screen issues. This is a known limitation and there is currently no workaround. |

# Fixed Defects

The following table lists the defects fixed in Webspace 6.2.

| Case Number | Area | Description |
|---|---|---|
| N/A | N/A | There are currently no defects to report here. |

# Chapter 2. Introduction

## Introduction to Webspace from GE Digital

The Webspace product from GE Digital is an add-on option for the iFIX and CIMPLICITY products. The Webspace product allows you to open pictures in run mode from a web session. The Webspace product is a server-based, thin-client solution that eliminates the need for Citrix MetaFrame or Windows Terminal Services.

The following sections provide general information on the Webspace product, and how to configure, administer, and use it with either iFIX or CIMPLICITY:



**Important:**
Plant Applications is not supported in Webspace 6.2. Customers requiring Plant Applications support should not upgrade Webspace.

## Language Support

The English language Webspace product can run on any supported regional operating system. For example, for iFIX these are English, Chinese, Japanese, Polish, Russian, French, or German, but we recommend using English regional settings. The language of the installed Webspace product does not need to match the language of the iFIX or CIMPLICITY software that you are running.

For more information on the available product version for each language, contact your regional Sales Representative. For a detailed list of the supported Windows Operating Systems (OS) for Webspace, refer to the System Requirements tab in the IPI.

### Unsupported Items

SCADA client/server configurations with different OS languages are not supported. For instance, connecting an English SCADA Server (on an English OS) with a German View node or iClient (on a German OS) is not supported. However, Webspace sessions can log in from operating systems in other languages if the input language is added to the Webspace Server, and keyboard layout for the client is set in that locale. For more information, refer to the Configuring Multiple Input Locales *(on page 69)* section.

## Webspace Features

The Webspace product provides the following features:

- **Client Access:** Provides transparent access to client-side resources like printers, files, sounds, and so on. It also provides seamless integration of client drives, and client machines' serial and parallel ports.
- **Client-Side Password Caching:** With this feature, the user's name and password are taken from the Webspace Server Logon dialog box after the first manual authentication and used automatically when the user accesses the web client again from that machine.
- **Dependent Servers:** A Webspace Server that is connected to a Relay Server. Multiple Dependent Servers are used for load balancing, as the Relay Server choses the one with the lowest number of running sessions.
- **Display Capability:** The Webspace session displays all graphics developed using the Workspace as is, and without conversion.
- **Encryption:** Provides support for a computer networking protocol that manages server authentication, client authentication, and encrypted communication between servers and clients.
- **Enhanced Failover:** The Webspace Server supports the iFIX Enhanced Failover configuration only when the Webspace Server machine is separate to the SCADA pair. The Webspace Server does not support Enhanced Failover while running on either of the SCADA machines configured in a redundant pair. The Webspace session will successfully switch over to the secondary SCADA in a failover scenario.
- **Exporting Data:** The Webspace sessions support exporting of data from Trend Charts and Historian to a local drive.
- **Inactivity Time-out:** Through the Webspace Admin Console, administrators can specify time limits for the number of minutes of client inactivity.

- **Independent Server:** A Single Webspace Server running with a client application, such as iFIX or CIMPLICITY.
- **Licensing:** The Webspace Server manages a server-based license for Webspace sessions and iFIX or CIMPLICITY functionality.
- **Multiple Sessions:** Webspace supports running multiple sessions on the same computer; however, each session will consume a license. Each open browser window (even if logged on under the same user name) consumes a license.
- **Network Access:** The Webspace Server communicates through a standard TCP/IP port, across a firewall. The Webspace sessions can also communicate with the Webspace Server through a single port across the firewall.
- **ODBC Connections:** The Webspace sessions support ODBC connections as supported by the Webspace Server to connect to relational database tables.
- **Other Applications:** The Webspace session supports running other applications. For instance, in the iFIX WorkSpace shell, you can run other applications such as Excel, Crystal Reports, and SQL Stored procedures. This is similar to the functionality on an iClient machine.
- **Other Products:** The Webspace sessions support displaying client controls from other products.
- **Relay Server Configuration:** Webspace Servers can be configured as Relay Servers to support Load Balancing (one Relay Server and two Dependent Servers) and High Availability (two Relay Servers and two Dependent Servers). In a High Availability scenario, one of the Relay Servers is designated as a the Failover Relay Server with a Backup license.
- **Reporting:** The Webspace Server supports reporting of client activities, such as connections, disconnections, logins, and logouts, to the Event Log.
- **SCADA Identity Protection:** When the SCADA and Webspace Server are used together on separate machines, the Webspace Server will not expose the details of the SCADA Server such as the IP address.
- **Security:** Webspace is secured with both product security and Windows security.
- **Session Shadowing:** This feature allows an administrator and a session owner to view and control a single session. Only administrators can connect to running Webspace sessions, but only with permission from the session's user.
- **Session Time-out:** Through the Webspace Admin Console, administrators can specify time limits for the number of minutes that sessions are allowed to run on a Webspace Server.
- **Standard Security:** The Webspace Server follows standard Windows security synchronized with the GE product.
- **Time Zone Redirection:** This option allows web sessions to run in the time zone of the client computer, regardless of the time zone that is selected on the Webspace Server.

- **Webspace Admin Console Dashboard:** Allows the system administrator to manage the Webspace Server application.
- **VPN Support:** The web session supports connecting to the Webspace Server through VPN connections.

# Webspace Components

## Webspace Server

The following components are installed as part of the Webspace Server:

| Component | Description |
|---|---|
| Proficy Webspace Application Publishing Service | The Proficy Webspace Application Publishing Service receives client connection requests, authenticates users on the Webspace Server, and launches Webspace sessions. |
| Webspace Relay Client Manager Service | The Webspace Relay Client Manager Service manages the web sessions on the dependent application servers in a Relay Server configuration. |
| Webspace Server License Manager Service | The Webspace Server License Manager Service manages a server-based license for Webspace Clients and product functionality. Each Webspace session consumes a license. Each open browser window (even if logged on under the same user name) consumes a license. |
| Webspace Admin Console | The Webspace Admin Console is a Windows application that is installed on the Webspace Server. Administrators use this tool to manage Webspace Server settings. |
| GE Software | iFIX or CIMPLICITY software. It is recommended that you install and run your SCADA Server on another, separate computer. |

## Webspace session

The following clients can be used for Webspace sessions (on the client computer):

- Microsoft® Windows® Internet Explorer 11 (32-bit)
- Mozilla® Firefox® 52 and later (standard and ESR, 32-bit and 64-bit)
- Apple Safari 9 or later on Mac OS X
- Google Chrome with Windows 7, Windows 8.1, Windows 10, and Chromebook

- Microsoft Edge
- Windows Desktop Client

# Unsupported Features for Webspace

**Important:**
It is strongly NOT recommended to run the Webspace Server on the same computer as your SCADA Server. The SCADA Server should reside on a different machine than the Webspace Server.

The Webspace product does not support use with:

- **Not Listed Browsers:** Other browsers such as Netscape and Opera.
- **Microsoft Internet Explorer (64-bit) Browser:** WebSpace does not support running the WebSpace client sessions on a 64-bit Internet Explorer browser; only 32-bit Internet Explorer browsers are supported.
- **Change Management:** Change Management from GE Digital is not supported. For iFIX, be sure that the Logon on WorkSpace Startup option is cleared on the Change Management tab in the User Preferences dialog box in the WorkSpace.
- **Configure Mode for the iFIX WorkSpace:** Webspace sessions in configure mode are not supported. Only the WorkSpace run mode is supported. By default, when you log on to a Webspace session from a supported browser, you automatically enter run mode. Several configuration tools (such as Key Macro Editor, Visual Basic Editor, Startup Profile Manager, and others) will not open in the Webspace session.
- **Dell Wyse T50 Thin Client**: This client is not supported or tested on the current version of Webspace.
- **Enhanced Failover:** iFIX Enhanced Failover is not supported if the Webspace Server is running on either of the SCADA machines configured in a redundant pair. Enhanced Failover is supported, however, if the Webspace Server machine is separate to the SCADA pair.
- **Environment Protection:** iFIX WorkSpace environment protection settings from the web session are not supported.
- **FIX32 Nodes:** Be aware that connections to FIX32 nodes are not supported by Webspace. For instance, in this case, you should not have animations or datalinks that point to FIX32 SCADA nodes in your web session pictures. This includes WorkSpace .GRF and View .ODF picture files.
- **iFIX Alarm ODBC:** Alarm ODBC in the Webspace client is not supported.

- **iFIX Screen Saver:** The iFIX Screen Saver is not supported in Webspace sessions. The iFIX Screen Saver settings only apply to the iFIX applications running on the Webspace Server itself, and not to web sessions.
- **Modem Connections:** Connecting a client to the Webspace Server using a modem is not supported.
- **Network Folder for Logs:** Webspace Server logs stored directly in a network folder are not supported.
- **Older Operating Systems.** For example, the following operating systems are NOT supported with the Webspace Server: Microsoft Windows XP, Microsoft Windows Server 2003, the 32-bit versions of Microsoft Windows 7 and Microsoft Windows 8.x (32-bit only). The following operating systems are not supported for clients: Microsoft Windows Pocket PC and Windows CE.
- **Operations Hub:** You cannot install Operations Hub by GE Digital on the same computer as the Webspace Server.
- **Plant Applications:** Plant Applications is not supported in this version of Webspace. Customers requiring either a 32-bit application or Plant Applications support should not upgrade Webspace to version 5.0 or greater.
- **Power Users:** Logging into Webspace Server as a Power User is not supported. To open a session to the server, log in as a member of the standard Users group.
- **Remote Desktop:** The Microsoft Remote Desktop Client is not supported in Webspace sessions.
- **Right-to-left Languages:** Right-to-left languages are not supported.
- **Running iFIX as a Service on the Webspace Server machine**: You cannot run iFIX as a service on the Webspace Server.
- **Running the Webspace Client and Server on the Same Computer:** Running Webspace sessions (browser or desktop client) on the same machine where the Webspace Server is installed is not supported.
- **Running the SCADA Server on the Same Machine as your Webspace Server:** It is strongly NOT recommended to run the Webspace Server on the same computer as your SCADA Server. The SCADA Server should reside on a different machine than the Webspace Server. An exception to this guideline would be a small system (with less than 5 Webspace clients) that does not used advanced iFIX capabilities such as Enhanced Failover.
- **Terminal Server:** A Terminal Server running on the same machine as the Webspace Server is not supported.
- **THISNODE feature:** THISNODE, which applies to the View nodes communicating with a remote SCADA, is not supported from the web session.
- **UNC Paths and Install:** Installing the product from UNC paths is not supported or recommended.

- **Undocumented Command Line Options:** The following startup parameters are not currently supported from a browser shortcut: bInBrowser, compression, printerconfig, clientframe, multimonitor, width, height, embed, noscale, clientscale, and ClientDPIScalingEnabled.
- **Undocumented Functionality:** Some items mentioned in the previous user help, such as the logon.html, the support request wizard, licensing servers, smart card authentication, and the AllClients.html are not supported in the current Webspace product. If it is not documented, it is not supported.
- **VMWare Advanced features:** Advanced features of ESXi Server, such as VMotion and Clustering support, have not been tested with Webspace. VMware WorkStation and Player are not supported. USB to serial communications is not supported. Power meter functions and options, and suspending images to conserve power are not supported. Setting up additional device connections to the virtual machine through a HOST is not supported.
- **Web HMI:** You cannot install Web HMI by GE Digital on the same computer as the Webspace Server.

# Chapter 3. Configuration

## Configuration Overview - Webspace

The Webspace Server allows you to log on and run iFIX or CIMPLICITY from a web session. However, in order to do so, you must first configure your Webspace Server through the Webspace Admin Console.

You may deploy three different types of Webspace Servers:

- Independent Server
- Dependent Server (for Load Balancing)
- Relay Server (for Load Balancing) and Failover Relay Server (for High Availability)

See "Advanced Topics" section for information on configuring Load Balancing and High Availability.

The following sections provide information on how to access, use, and configure Webspace and its options through the Webspace Admin Console:



## Installing Webspace

This topic describes how to install Proficy Webspace.

1. On the SCADA Server computer (recommended), install iFIX Server or CIMPLICITY Server.
2. On your Web Server, uninstall any previous builds of Webspace.
3. On your Web Server, if it is not already installed, install the iFIX View node or CIMPLICITY Viewer/ Server software (for supported versions see the System Requirements tab, "Compatibility with Other GE Products" section).

> **Tip:**
> For CIMPLICITY, while the Viewer is supported, it is recommended that you use a CIMPLICITY HMI Server 75 I/O Development & Runtime System. This Server is the lowest CIMPLICITY Server I/O count that you can have that allows for network access. It also provides the best flexibility for any centralized client node.

4. Shut down any GE applications or services that run on startup. For instance, if you have GE Digital's Historian for SCADA Collectors configured to start when you start Windows, use the Services window to shut them down.
5. Confirm that a supported version of Microsoft Internet Information Server (IIS) or Apache HTTP Server was installed beforehand. If it is not, install it now, as the Webspace install requires it.
6. If installing on Microsoft Windows 8.x 64-bit, Microsoft Windows 2008 R2, or Microsoft Windows Server 2012 64-bit, ensure that the ASP.NET feature is enabled:
    - In Microsoft Windows 8.x, from the Control Panel > Programs and Features, click, "Turn Windows Features on or off." In the Windows Features list, enable the following option: Internet Information Services > World Wide Web Services > Application Development Features > ASP .NET 4.5 or ASP .NET. Click OK to install.
    - In Microsoft Windows Server 2008, open the Server Manager, and from the tree view, click Roles and then click Add Roles link on the Roles page. From the Add Roles Wizard, click Next to get to the Server Roles page. Enable the following role:  Web Server (IIS). Next, from the Role Services page, select the following feature: Web Server > Application Development > ASP .NET. Click Next and then click Install.
    - In Microsoft Windows Server 2012, open the Server Manager, and click Add Roles and Features. From the Add Roles and Features Wizard, click the Server Roles link (or click through the wizard until you get to this page). Enable the following role: Web Server (IIS) > Web Server  > Application Development > ASP .NET 4.5. Click Next until you get to the Confirmation page, and then click Install.

**NOTE:** Microsoft Windows 8.x and Windows Server 2012 come with ASP .NET pre-installed and registered. Be sure to install the latest Windows updates. If ASP.NET 4.5 has not been registered on the Web server, you need to manually configure your Web server for ASP.NET 4.5 in order for your site to run correctly.  For example, to register ASP .NET for IIS on Windows 7 use the command line: %SYSTEMROOT%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -i. For more information on installing using the command line refer to the Microsoft MSDN web site: http://msdn.microsoft.com/en-us/library/ms229858(v=vs.100).aspx. For more information on installing other ways, refer to MSDN:http://msdn.microsoft.com/en-us/library/5a4x27ek(v=vs.110).aspx. Also be sure to install the latest Windows updates.

> **Important:**
> On Microsoft Windows 7, DO NOT enable the Microsoft .NET 3.5.1 > Windows Communication Foundation HTTP Activation feature.

7. Ensure that TCP/IP is enabled prior to installation. Configure any external firewall and any software firewall on the server to allow TCP port 491.
8. Log in as a user with Administrator rights and start the Webspace installation.
9. From the Welcome screen, click Next.
10. On the License Agreement screen, to continue the installation, accept the terms of the license agreement, and click Next.
11. On the Choose Destination Location screen, leave the defaults and click Next.
12. On the Logon credentials screen, enter the User Name and Password for the user you plan to use as the administrator for this Webspace installation (for the IIS Webspace application pool), and click Next.
13. On the Ready to Install the Program screen, click Install to begin the installation.
14. When the installation is completed, click Finish and then restart the computer.
15. Continue with configuration steps for your iFIX or CIMPLICITY.

# Configuration Guidelines

### iFIX Configuration

Be aware of the following:

- It is recommended that if security is enabled, that the iFIX SCADA Server and the Webspace Server reside on the same network. These same user account names will later need to be added to the Webspace Server.
- When adding users through the Security Configuration application in iFIX, be sure to select the Windows Security option for the user.
- When assigning security privileges in iFIX, use care when allowing application features that could allow write access, such as the "Database Save/Reload" and "Runtime Visual Basic Editor" features, as well as creating pictures with Datalinks, or any other means to write values into tags. Use Security Areas and Security Groups to further restrict access. Also, use care when creating and sharing schedules in iFIX, so that unintended VBA code is not activated inadvertently by web sessions. For more information on iFIX Security, refer to the Configuring Security Features e-book in the iFIX online help.

**Important:**
In an Enhanced Failover setup, make sure that the primary and secondary servers are separate from the Webspace Server.

**Important:**
If iFIX is installed after Webspace, manually create and configure a WEB.SCU file if iFIX is to be used with Webspace on the SCADA Server computer.

**Note:**
Be aware that the Webspace Server uses the same WEB.SCU for all Webspace clients, similar to how a Terminal Server uses the same SCU for all iFIX thin client users. For this reason, the global security paths (Use These Paths for All Startup Profiles) option in the Edit > Configuration dialog box of the iFIX Security Configuration application on the Webspace Server is unavailable for editing and appears greyed out. This is intentional so that all iFIX user sessions share the same security configuration. You cannot change this setting.

1. Update the HOSTS file with the name of the SCADA Server, to ensure the highest reliability for connectivity. If the SCADA Server node name is different from the computer name that it was installed on, you also need to add this name to the HOSTS file. The HOSTS file on the Webspace Server should be identical to the one on the SCADA Server.
2. In Windows (Workgroup or Domain, preferably Domain), add the user accounts that you want to use with the Webspace Server. You must have the privileges to do so.
3. If you want to enable security on the iFIX SCADA node (most likely), add these same users to the iFIX SCADA through the Security Configuration application (Edit > User Accounts). iFIX must be running to access this tool and enable security (Edit > Configuration).
4. In the iFIX System Configuration (SCU) tool, ensure that the Network Configuration is set to TCP/IP (Configure > Network), and that SCADA is enabled (Configure > SCADA).
5. Create your pictures.

On the Web Server computer:

1. Update the HOSTS file with the name of the SCADA Server, to ensure the highest reliability for connectivity. If the SCADA Server node name is different from the computer name that it was installed on, you also need to add this name to the HOSTS file. The HOSTS file on the Webspace Server should be identical to the one on the SCADA Server.

2. In Windows (Workgroup or Domain, preferably Domain), add the user accounts that you want to use with the Webspace Server. If you are on a domain, you may have already done this. You must have the privileges to do so.
3. In the iFIX Security Configuration program, add these same users accounts (Edit > User Accounts), and enable security (Edit > Configuration). iFIX must be running to access this tool and enable security. Unlike the SCADA Server, this step is not optional on the iFIX Webspace Server.
4. If an iFIX View node is not installed before you install Webspace, you will need to manually create the WEB.SCU file; the WEB.SCU will not automatically be created if you install Webspace before iFIX View node. When configured for Webspace, none of the iFIX SCU's on Webspace Server should be configured to start iFIX as service, as this is an unsupported configuration.
5. In the iFIX System Configuration (SCU) tool, open the WEB.SCU file.
6. Verify that Network Configuration is set to TCP/IP (Configure > Network), that SCADA is disabled (Configure > SCADA), and that Workspace.exe appears in your tasks list (Configure > Tasks). By default, these settings are automatically configured during install. If these settings are not correct, update them now.
7. Specify the name of your iFIX SCADA Server in the Remote Nodes list (Configure > Network).
8. Either copy your pictures from the SCADA Server to the PIC folder on the iFIX Webspace Server (recommended for optimum performance), or map a drive to your PIC folder on your SCADA Server.
9. If you map a drive for pictures, and you are using shared drives with Local Windows users (not on the Domain), make sure that the user is present on both the Webspace Server machine, and the machine which contains the shared folder. In the SCU on the Webspace Server, open WEB.SCU and point the picture folder to that mapped drive letter (Configure > Paths).
10. If you map a drive for pictures, update the LoginScript.bat file provided in the C:\Program Files \Proficy\iFIX Webspace Server\Programs folder with the mapped drive information, and then add the script name to the Session Startup options in the Webspace Admin Console. For more information, refer to the online help for the Webspace Admin Console.
11. Optionally, in the Webspace Admin Console, configure printer options and other session properties. For more information, refer to the online help for the Webspace Admin Console.
12. If you want to configure multiple input locales for your web sessions, add the input language and keyboard layout for that locale to the Regional Settings on the Webspace Server. For more information, refer to the online help for the Webspace Admin Console.

TIPS:

- You can find the HOSTS file in the C:\WINDOWS\system32\drivers\etc folder.
- Use a text editor such as Notepad to edit the HOSTS file, and do not add a file extension to the file.
- An example entry in the HOSTS file is as follows: 198.212.170.4 SCADA01. If SCADA1 was the iFIX SCADA Server node name, but the computer name where the iFIX SCADA Server

was installed was AREA1, you would need to add a second line to the HOSTS file for AREA1:
198.212.170.4 AREA1.

- If you do not know the TCP/IP address of the SCADA computer, run the IPCONFIG command on the SCADA Server.
- The same, identical entries should appear in the HOSTS file for the SCADA Server and the Webspace Server.

- Be aware that the last SCU file saved in the System Configuration tool is the one that runs when iFIX starts. This is important to remember if you have the iFIX SCADA and the iFIX Webspace on the same machine. Although this configuration is not recommended, you may find this implementation on small systems (with less than 5 Webspace clients) that do not used advanced iFIX capabilities like Enhanced Failover.

## CIMPLICITY Configuration

- On the Web Server computer, configure Windows-based security or Standard CIMPLICITY security for CIMPLICITY.
- Make sure the same security is configured for both the CIMPLICITY Server and Webspace Servers.

- Make all of the paths (with their folders) that will be shared for the Web Clients read-only. This will avoid running into the Microsoft's limitation for sharing files.
- On the CIMPLICITY Server, to publish a web page for a CIMPLICITY CimView screen, right-click the CIMPLICITY Options application and run as Administrator. On the Proficy Webspace tab, click the "Create a Web Page" button. The next dialog box allows you to select the screen that you want and creates a web page for it; if it does not pick up the default Webspace directory to place the html file in, you will need to enter it. If it's an Apache server, you will need to browse to the location of the Apache Server; by default, the Apache Server location is: "C:\Program Files (x86)\Apache Software Foundation\Apache2.2\htdocs\ProficyWebspace."
- Run the CimView screen(s) natively in Cimview.exe on the Webspace Server to ensure proper Viewer-to-Server communications are established. Since your CIMPLICITY project server(s) are most likely remote to the Webspace Server, it is highly recommended that CIMPLICITY Deployment is configured to synchronize files with the Webspace Server (and keep them up-to-date).
- Do not use shared CimView screens. If you do, every client that connects will need to create their own share, which could run the server out of resources. This could increase the time it takes a user to log in, and could make the server fail.
- A separate CimView.exe and CimLayout.exe session runs for each Webspace session with CIMPLICITY.

- For the CIMPLICITY Windows Desktop Client, be sure that the command line parameter "-r" specifies the command line parameters for CIMVIEW. For example, -r CIMVIEW "C:\MyProject \screens\MyScreen.cim" will open the correct screen, as long as -r comes after the -a parameter, and all the other parameters are correct. For example: "C:\Program Files (x86)\Proficy\Proficy Webspace Client\Client\Proficy.exe" -h MyServer -c -a CimView -r CIMVIEW "c:\screens \userscreen.cim"
- Do not configure the Webspace machine for Power Save or Lock; either feature can block Web Clients from connecting or cause them to lose an active connection.
- If the session has been configured to Zoom to Best fit, the CimView screen will fit into the ActiveX container. The ActiveX container will conform to the Internet Explorer size when the URL is accessed.
- The ActiveX Control or plug-in fits into the size of the browser when the URL is accessed; the size does not change when you resize the browser. Therefore, make sure the browser is the size you want before you go to the URL that will start the Webspace session.
- Make sure in a redundant SCADA server setup, that the primary and secondary servers are separate from the Webspace server.
- Optionally, in the Webspace Admin Console, configure printer options and other session properties. For more information, refer to the online help for the Webspace Admin Console.
- If you want to configure multiple input locales for your web sessions, add the input language and keyboard layout for that locale to the Regional Settings on the Webspace Server. For more information, refer to the online help for the Webspace Admin Console.

- On the Web Server computer, configure Windows-based security or Standard CIMPLICITY security for CIMPLICITY.

### Terminal Services Configuration

Do not install Webspace on a CIMPLICITY or iFIX Server that has already been configured as a Terminal Server. This type of installation is not supported.

# Apache Configuration Still Supported in Webspace Upgrades

This topic describes how to configure SSL when the Apache HTTP Server 2.4 (httpd-2.4.29-Win64-VC15) web service is installed on the Webspace Server, which was a configuration supported in earlier versions of Proficy Webspace. You can continue to use this older configuration or upgrade to the new one; Webspace now has its own web server. The newer version of Webspace (version 6.2 and greater) does not require the use of either Apache or IIS.

**Note:**
If IIS is installed, the World Wide Web Publishing service must be stopped and disabled before downloading and installing Apache. After you install Apache, you want to verify that you can connect without encryption. Then, you can enable HTTPS and update your certificate.

### Stop the WWW Publishing Service

To stop the service:

1. From Services, right-click World Wide Web Publishing service and select Properties.
2. From the Properties dialog box, select Disabled and from the Startup type drop-down menu and click the Stop button.
3. Click OK to continue.

After the service is stopped, you can now install the Apache HTTP Server.

### Install the Apache

1. Go to http://www.apachelounge.com/download/ and download the latest version. The version tested with Webspace was httpd-2.4.29-Win64-VC15.zip.
2. Download and install C++ Redistributable Visual Studio 2017. The version tested with Webspace can be downloaded from the following link: https://aka.ms/vs/15/release/VC_redist.x64.exe
3. Extract httpd-2.4.29-Win64-VC15.zip onto the Webspace Server machine into the C:\Apache24 directory.
4. On the Start menu, point to All Programs, Accessories, and then Command Prompt. Right-click Command Prompt and Run as administrator.
5. In the Command Prompt window, type the following:

```
cd C:\Apache24\bin

httpd -k install

httpd -k start
```

### Verify that Ports are Open and Connection Can Be Made

After you install the server, you may need to open port 80 in the firewall if it is not already open. If SSL is running, verify that port 443 is open using the following steps:

1. Open c:\Apache24\bin and run ApacheMonitor.exe. From the system tray, open the Apache Monitor and verify that the service has started.
2. Open c:\Apache24\htdocs and create a directory called proficywebspace.
3. Copy the contents of c:\Program files\Proficy\Proficy Webspace\Web into c:\Apache24\htdocs \proficywebspace directory.
4. Open a browser on the Webspace Server and go to try to login to start a session.

### Enable the HTTPS Connection for Strong Encryption

To enable HTTPS connection:

1. Load the ssl module for Apache by uncommenting the line "Module ssl_module modules/ mod_ssl.so" in the C:\Apache24\conf\httpd.conf file.
2. Include the httpd-ssl.conf file by uncommenting the line "Include conf/extra/httpd-ssl.conf" in the C:\Apache24\conf\httpd.conf file.
3. Update the server certificate, server key, and the folder path for root certificate in the C: \Apache24\conf\extra\httpd-ssl.conf file by either giving a relative path if the certificates are in Apache24 folder, or an absolute path, and uncomment the following lines:

```
SSLCertificateFile "C:/Program Files/Proficy/Proficy Webspace/Programs/ProficyWSCerts/pki/Proficy_WSServer.crt"

SSLCertificateKeyFile "C:/Program Files/Proficy/Proficy

 Webspace/Programs/ProficyWSCerts/pki/Proficy_WSServer.key"

SSLCACertificatePath "C:/Program Files/Proficy/Proficy Webspace/Programs/ProficyWSCerts/pki/"
```

   If you get an error related to shmcb session cache, comment out the line referring to the session cache by putting a # sign at he beginning of the line, like this:

```
#SSLSessionCache "shmcb:${SRVROOT}/logs/ssl_scache(512000)"
```

### Update the Certificates

To complete the chain of trust, import the root certificate on the client node from where you are going to launch the browser to connect to Webspace.

# Certificates

## Certificate Overview

For strong security, you can use a server certificate that you purchase from a Certificate Authority (CA) that is trusted by the client operating system. The CA will require a Certificate Signing Request (CSR).

When you install Webspace, there is also an option on the install menu to Install Certificates which allows you to create a certificate.

> **Important:**
> When using the certificate installed with Webspace and Strong Encryption, you cannot start a Webspace session with the IP address of the WebSpace server. The IP address cannot be used for the host name. Use the Full Computer Name in the URL instead.

Optionally, you can create your own certificate authority as well. There are many third-party applications and systems to assist in the creation and maintenance of a certificate authority that interoperate with the OpenSSL toolkit. These tools should be able to generate signed server certificates for use with Webspace without modification.

### How to Install a Self-Signed Certificate from the Webspace Install Menu

1. To view the installer menu, open the Installfrontend.exe on the install media.
2. Click the Install Certificates option. The Webspace Certificate Configuration Tool appears.
3. Leave the defaults, or make changes as necessary to the folder and file names, and so on. After doing any changes in configuration, click Update Configuration.
4. To generate the self-signed certificates and other steps required for certificate binding, click Create and Bind.
5. Review the status in the Create Certificates, Import Certificates, and IIS Site Binding sections.
6. If these sections do not appear to update after the action completes, click the Restart IIS Site option. Sometimes you need to restart IIS to see that the binding that was created.
7. Close the Webspace Certificate Configuration Tool.

### Important Information When Working with a Relay Server

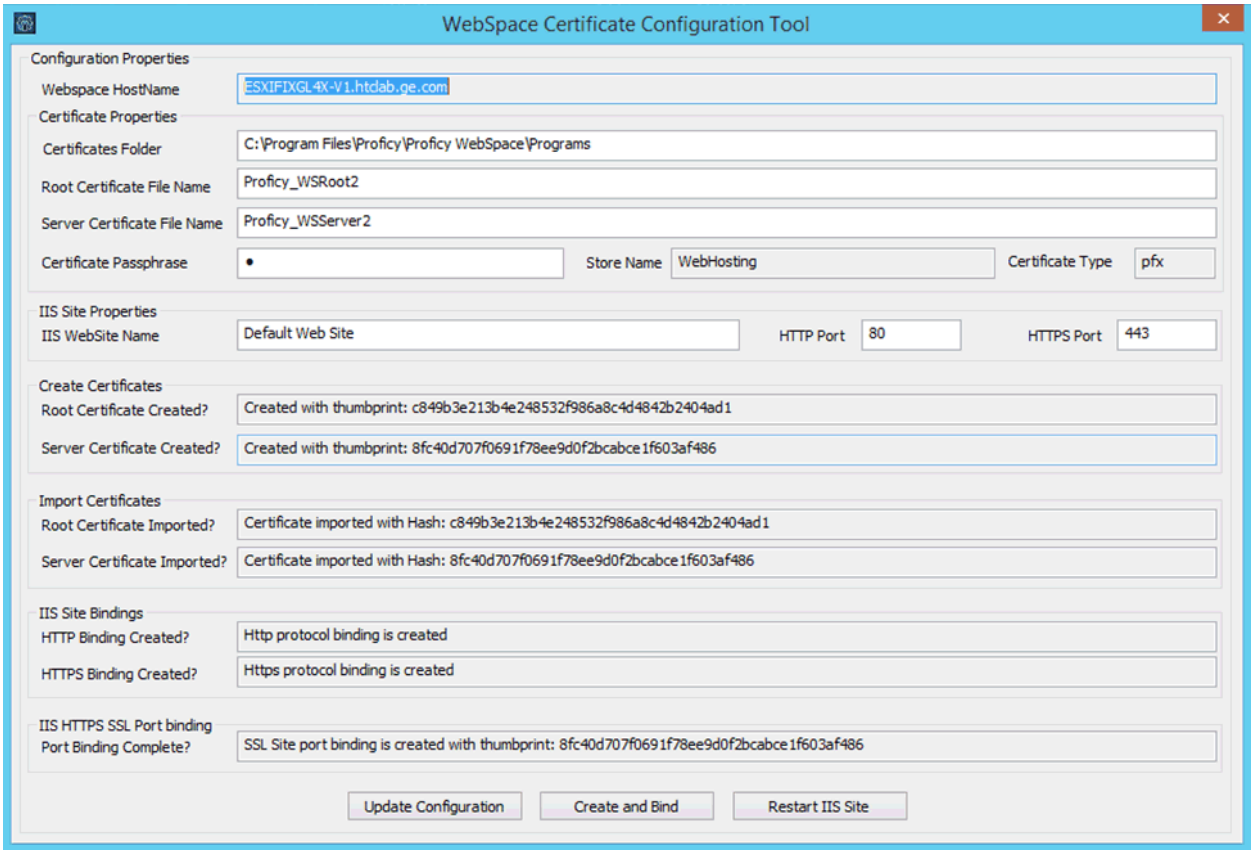
For a Relay Server to work with Strong Encryption, install the Relay Server Root certificate on Webspace Dependent Server and all clients. The Failover Relay Server with Strong Encryption is not supported.

### How to Troubleshoot or Repair a Lost/Corrupted Certificate Created from the Webspace Install

1. From the Webspace install menu, click the Install Certificates option. The Webspace Certificate Configuration Tool appears.
2. Click Create and Bind. This action regenerates the self-signed certificates.
3. Review the status in the Create Certificates, Import Certificates, and IIS Site Binding sections.

4. If these sections do not appear to update after the action completes, click the Restart IIS Site option. Sometimes you need to restart IIS to see that the binding that was created.
5. Restart the Webspace Certificate Configuration Tool by clicking the Install Certificates option from the installer menu again, and review the status in those sections again.

## Example of a Successful Certificate Installation




## How to Select the Server Certificate in the Webspace Admin Console

1. Launch the Webspace Admin Console, and select Tools and then Host Options.
2. Select the Security tab.
3. Change the Transport to Encrypted and increase the Encryption to 256-bit AES, if you have a high-encryption license. If not, leave it at 56-bit. The option to increase is only available if your license includes the Strong Encryption option.
4. In the Certificate field, browse to the Proficy_WSServer.crt created in default certificate folder: C:\Program Files\Proficy\Proficy WebSpace\Programs\ProficyWSCerts\pki (or from whatever the folder it was created) and click OK.
5. Enable the Notify users when connections are secure for testing purposes.

6. Click OK.
7. If you want to start a Webspace session from a different computer, the Proficy_WSRoot.crt certificate file will need to be installed on that system. Copy the Proficy_WSRoot.crt file from the Webspace server folder on local system (by default it is C:\Program Files\Proficy\Proficy WebSpace\Programs\ProficyWSCerts\pki, or whatever folder you chose to create it in), to the destination computer. Double-click the certificate and choose the option to Install Certificate. Install it in the certificate store, Trusted Root Certification Authorities.
8. Use the Webspace HostName to browse the Webspace session. For encrypted sessions, IP addresses are not supported using the Proficy_WSServer.crt.

## Obtaining a Trusted Server Certificate

To obtain a server certificate from a CA that is trusted by the client operating system, consult the documentation from the CA of your choice using the following information as a guide. The CA will require a Certificate Signing Request (CSR).

### To generate a CSR

1. Download the latest version of OpenSSL fromhttps://www.openssl.org/source/.
2. Install OpenSSL on the Webspace Server.
3. Click Start, and then Run.
4. Type cmd, and press Enter.
5. Type the following command to generate a private key for the server: `[OPENSSL_DIR]\bin\openssl genrsa –out server.key 2048` where OPENSSL_DIR is the path to the directory in which OpenSSL is installed (e.g., C:\OpenSSL).
6. Type the following command:

```
[OPENSSL_DIR]\bin\openssl req –sha256 –new –key server.key –out server.csr
```

Running this command will prompt you for the attributes to be included in your certificate, as follows:

**Country Name:** US **State:** your state **Locality**: your city

**Organization:** your company name **Organizational Unit**: your department **Common Name:** your server's name

**E-mail Address:** your e-mail address

Unless you are using a wildcard SSL Certificate, the Common Name *must* match the host name of the Webspace host (the name that users will specify when connecting to the host). Any variation in the name

will cause the client to issue a warning when connecting. The output of the above command will be a file named **server.csr**, which can be sent to your CA. Since Webspace's SSL implementation is based on the OpenSSL toolkit, the tools used are the same as those used in other OpenSSL-based products, such as the Apache mod_ssl package. Follow instructions provided by your CA for the mod_ssl package to obtain a certificate for your server.

When your CA sends you the signed server certificate file, save it as server.crt. Copy this file and the server.key file (generated in step 5 above) to a directory on the Webspace host that can be accessed from the System account and accounts that belongs to the Administrator group but that cannot be accessed from normal user accounts. Finally, select the signed certificate file in the Webspace Admin Console, as described below.

### To select the server certificate

1. From the Webspace Admin Console, click Tools and then Host Options.
2. Click the Security tab.
3. In the Transport list, select SSL.
4. Type or browse to the path to the server's certificate (e.g., server.crt) file in the SSL Certificate box.
5. Click OK.

Webspace requires that the certificate and its key be in PEM format. When requesting a certificate from a third-party CA, GE recommends requesting it in PEM format. If this is not possible and the certificate can only be delivered in DER format, it can be converted to PEM format using the following command:

```
openssl x509 -inform der -in MYCERT>cer -out MYCERT.pem
```

The resulting MYCERT.pem file can then be renamed to MYCERT.crt for use in Webspace.

## Using an Intermediary SSL Certificate with Webspace

When using an intermediary SSL certificate with Webspace, you must concatenate your existing certificate with the intermediary certificate. The following example uses the Go Daddy intermediary certificate.

1. Take the .crt and .key files that are being used on the Webspace host.
2. Download the Go Daddy intermediary certificate (for example: GODaddyCA.crt). This should have come with the original certificate purchase but can also be located at the following Go Daddy site: https://certs.godaddy.com/Repository.go
3. Concatenate your .crt and the intermediary .crt file. (Combine them into a third file as follows: copy test_server.crt+GODaddyCA.crt server.crt.)

4. Rename the key file from step 1 to server.key so that it matches the newly created server.crt file.
5. Copy these two files onto the Webspace host (for example: c:\Data).
6. Launch the Webspace Admin Console, and select Tools and then Host Options, and click the Security tab.
7. Change the transport to SSL and increase the encryption level to 256-bit AES, if you have a high-encryption license. If not, leave it at 56-bit. The option to increase is only available if your license includes the Strong Encryption option.
8. Browse to the SSL certificate server.crt in c:\data and click OK. You should not see an error message at this point if you have .crt and .key files with the same prefix.
9. Enable Notify users when connections are secure for testing purposes.
10. Click OK.
11. Start a Webspace session from a different system.

## Using an Intermediary SSL Certificate on iOS and Android

In order for the Webspace app on iOS or Android to trust a server certificate, it must be able to trust the entire SSL certificate chain, including any intermediate certificates and all root certificates. Use these steps to make a server certificate that will provide the entire SSL certificate chain.

1. Obtain all .crt files included in your certificates chain, and .key files being used on the Webspace Host.
2. Concatenate your .crt and all intermediate and root .crt files. (Combine them into a final file as follows: copy test_server.crt+intermediate.crt+root1.crt+root2.crt server.crt)

   **Note:**
   There may be 0 or more intermediate files and 1 or more root files. If your .crt file is self-signed, you will just need to rename your .crt file to server.crt.

3. Rename the key file from step 1 to server.key so that it matches the newly created server.crt file.
4. Copy these two files onto the Webspace Host (for instance: c:\Data).
5. Launch the Admin Console.
6. On the Tools menu, click Host Options.
7. Click the Security tab.
8. Change the transport to SSL and increase the encryption level to 256-bit AES, if you have a high-encryption license. If not, leave it at 56-bit.
9. Browse to the SSL certificate server.crt in c:\data and click OK. You should not see an error message at this point if you have .crt and .key files with the same prefix.
10. Enable Notify users when connections are secure for testing purposes.

11. Click OK.
12. Start a Webspace session from an iOS or Android device.

### Firefox and Certificates

Firefox does not, by default, recognize certificates in the Windows certificate store. Use an enterprise policy to add CA certificates and set the ImportEnterpriseRoots key to True. In Firefox, type about:config to access the configuration. Configure the security.enterprise_roots.enabled setting to true. For more information, see: https://support.mozilla.org/en-US/kb/setting-certificate-authorities-firefox.

## Self-Signed Certificates

### Creating Your Own Certificate Authority

Sites with many Webspace hosts can create their own certificate authority, then sign each server's certificate from this authority and install the certificate authority certificates onto each client. This will prevent any warnings about untrusted authorities, without requiring the site to obtain a third-party certificate for each server.

There are many third-party applications and systems to assist in the creation and maintenance of a certificate authority that interoperate with the OpenSSL toolkit. These tools should be able to generate signed server certificates for use with Webspace without modification.

A certificate authority is a virtual organization that will sign each of your server keys, allowing the client to assert that the server keys are authentic and have not been tampered with.

To establish the certificate authority, a CA key and self-signed certificate must be created. After the CA certificate and key are created, import the CA certificate on the client device via the Internet Options dialog. Finally, the server keys are signed using the CA certificate, which will allow the client machines to recognize the authenticity of the signatures and allow connections to the server without warning the user about the trustworthiness of the CA.

**Note:**
Nine files are created during this process: ca.key, ca.csr, ca.crt, ca.cfg, ca.serial, server.cfg, server.key, server.crt, and server.csr.

### Using SSL Transport in Webspace

When using self-signed certificates with Webspace, these steps outline the setup for running in Webspace over HTTPS.

1. Create your certificate authority and generate the SSL certificate. The commands needed to create CA key and certificate are:

```
openssl genrsa -out ca.key 2048

openssl req -sha256 –new –key ca.key -out ca.csr
```

2. Create the ca.cfg file with the following content:

```
extensions = x509v3

[ x509v3 ]

subjectAltName = email:copy

basicConstraints = CA:true,pathlen:0

nsComment = "GE Digital CA"

nsCertType = sslCA
```

3. Create the CA certificate using command:

```
 openssl x509 –req -sha256 –extfile ca.cfg –days 1825 –signkey ca.key –in ca.csr -out ca.crt
```

4. Rename ca.cfg to server.cfg.
5. Remove the basicConstraints line.
6. Modify nscomment to reflect your Company Name.
7. Change nsCertType to 'server'.
8. Create a file to hold certificate serial numbers by running the command:

```
echo 01 > ca.serial
```

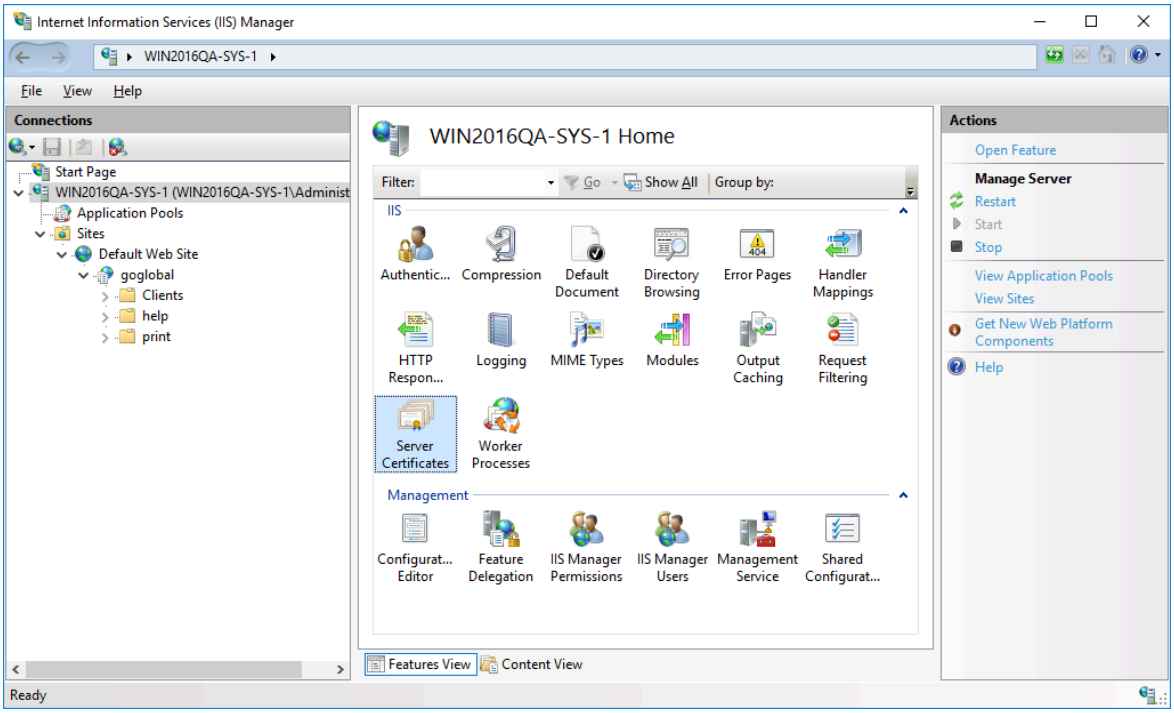
9. Create the server key and certificate signed by the CA using below commands:

```
openssl genrsa –out server.key 2048

openssl req -sha256 –new –key server.key –out server.csr

openssl x509 –req -sha256 –extfile server.cfg –days 1825 –CA ca.crt –CAkey ca.key –CAserial ca.ser

ial –in server.csr –out server.crt
```

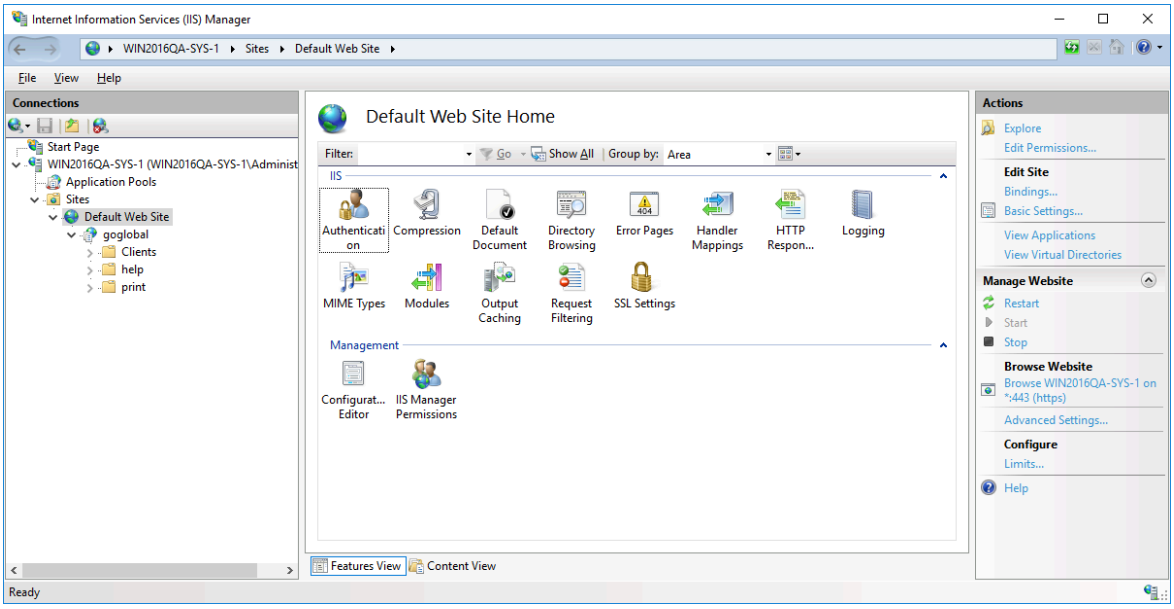
**Note:**
In options common name part is the host name of the server.

10. Assign the generated server certificate in step Webspace Admin Console on the Options > Security tab.
11. Restart the Proficy Webspace Application publishing service.

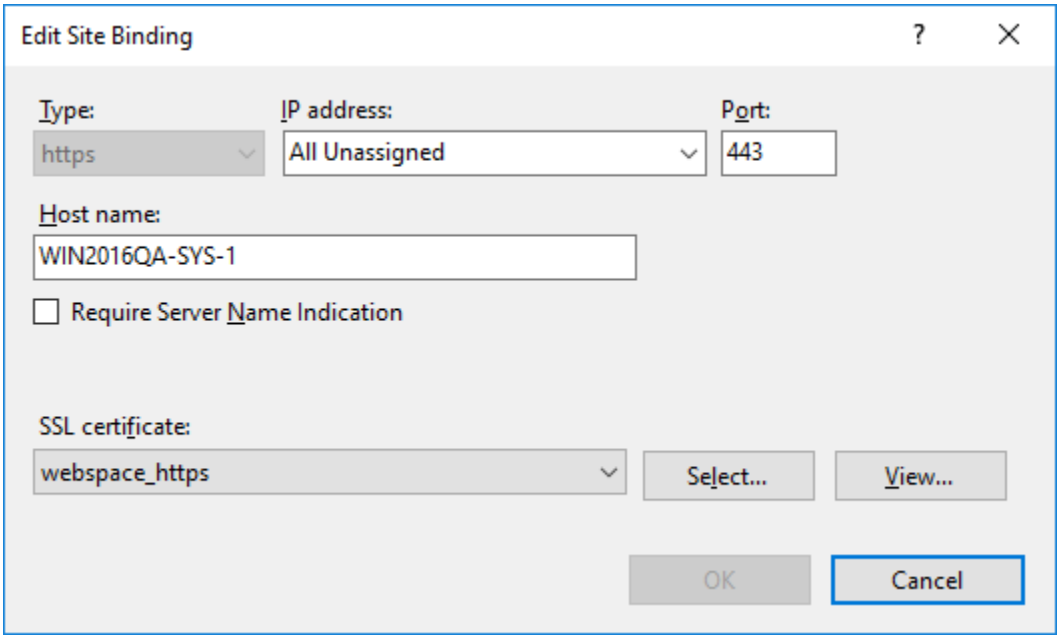
12. In the IIS manager window, select the host name and then Server Certificates.




13. In the Server certificates window, click Create Self Signed Certificate.
14. Select the Default website and Bindings option.




15. Add a HTTPS binding with the certificate created in the previous step.




16. Restart the Default website in IIS manager
17. Confirm that IIS is setup correctly by opening a browser and enter the https://hostname. It should open the IIS default page. This indicates that the https settings in IIS are configured correctly.
18. Try to connect to an application in the Webspace client. This should start the iFIX or CIMPLICITY application in the Webspace browser window.

## Creating Mapped Drives on the Webspace Server

If you want mapped drives to be available for web users, you can use a batch file on the Webspace Server to log on to share these drives, rather than directly mapping them through Windows Explorer.

For iFIX, an example of a batch file, LoginScript.bat, is provided in the C:\Program Files\Proficy\Proficy iFIX\Programs folder. A batch file, such as this example, can run on a global-basis when any user logs on, or on a user-specific basis. For steps on how to add a batch file script to the logon process, either global or user-specific, refer to the Logon Scripts *(on page 102)* section. If the Administrator wants to change the location of the batch file, be aware that the new location must be accessible to all the web users.

**Note:**
User-specific project paths for Webspace sessions are not supported. For example, you cannot use different directory paths for iFIX files, such as pictures, across multiple users. If you need to support this, it is suggested that you use iFIX with Terminal Server, instead of Webspace.

If all users require access to the same network share through a drive mapping, the drive mapping will generally need to be defined in a logon script, such as defined in the LoginScript.bat example.

If you are using shared folders with Local Windows users (not on the Domain), make sure that the user is present on both the Webspace Server machine, and the machine which contains the shared folder.

Be aware that the Webspace Server cannot back up logs to a network folder. For example, if you type a UNC path or a mapped network drive in the folder edit box, the following message is displayed: "Please specify a usable Windows folder where log files may be written."

Be aware of the Microsoft limitation on shared directories. Please see article KB5062 on the GE Knowledgebase: http://www.ge-ip.com/support.

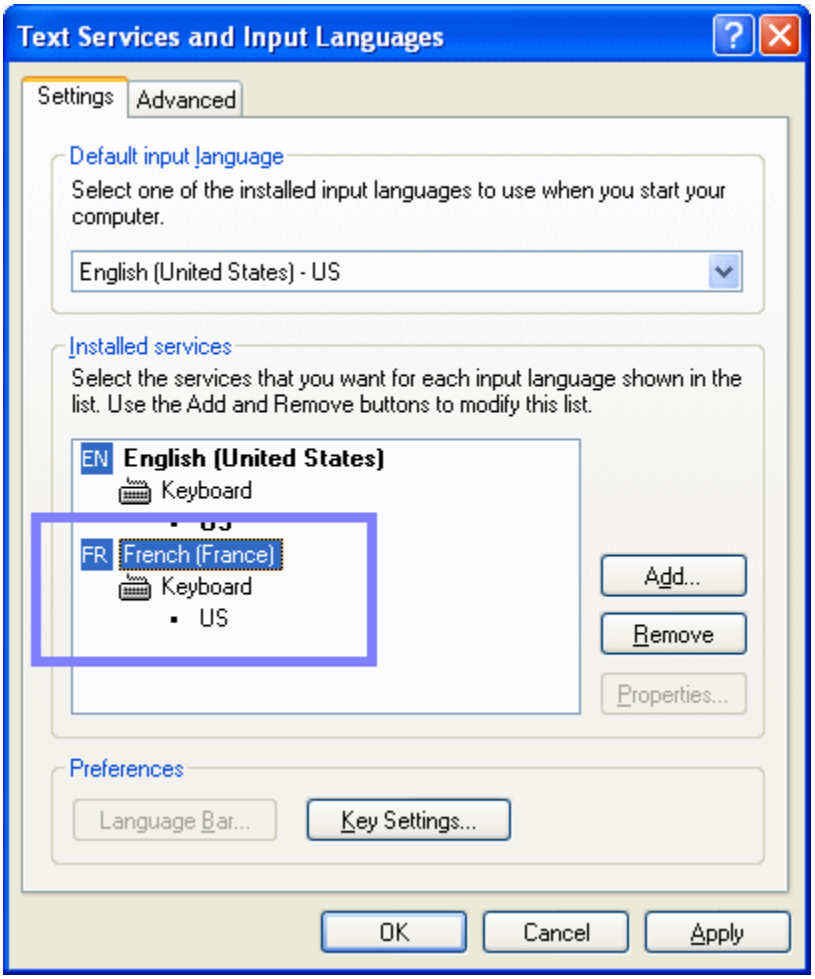
Mark all of the paths (with their folders) that will be shared for the Web Clients as read-only. This will avoid running into the Microsoft's limitation for sharing files.

## Configuring Multiple Input Locales

The Webspace session can be configured to allow users with different input locales to log into the Webspace Server. Although the Webspace Server supports only the same operating system language as the iFIX or CIMPLICITY computer, Webspace sessions can log in from operating systems in other languages. However, for this to work, the input language must be added to the Webspace Server, and keyboard layout for that locale must be set.

**Note:**
Users will not be able to switch input locales when the Webspace Sign In dialog box is displayed. The input locale for the default language of the Webspace Server will be used instead. On Windows clients, the selected input locale of server-based applications is not displayed in the system tray of the client computer.

For example, say your English Webspace Server is on an English Windows computer. Your Webspace session is a browser running on a French Windows machine. For this scenario to work, you must add the French input language to the Regional and Language Options on the Webspace Server. The French input language must be set to an English keyboard, however. The following figure shows an example:




## Allowing Clients on Non-English Operating Systems to Connect to the Webspace Server

1. Log on interactively to the Webspace Server computer that you want to add the Input Locale with an administrator account.
2. On the Start menu, point to Settings, Control Panel, and then click Regional and Language Options. The Regional and Language Options dialog box appears.
3. Click the Languages tab.
4. In the Text services and input locales area, click Details. The Text Services and Input Languages dialog box appears.
5. In the Installed Services area, click Add. The Add Input Language dialog box appears.
6. In the Input Language field, select the language you want to allow. For example, in the above graphic, you would select French.

7. In the Keyboard Layout/IME field, select US. This indicates that the physical keyboard should be set to a U.S. English keyboard layout. If the physical keyboard is not US, select the appropriate keyboard layout.
8. Click OK.
9. On the Text Services and Input Languages dialog, click OK. You are returned to the Regional and Language Options dialog box.
10. Click the Advanced tab.
11. Select the "Apply all settings to the current user account and to the default user profile" check box. A message box appears.

> **Important:**
> Users will not be able to switch input locales when the Logon dialog is displayed. The input locale for the default language of the Webspace Server will be used. For web sessions, the selected input locale of the Webspace Server is not displayed in the system tray of the client computer.

12. Click OK to continue.
13. Click OK to close the Regional and Language Options dialog.

## Installing Additional Keyboard Layouts and IMEs

Before clients can use keyboards and/or IMEs that are different from the server's, the files used to support them must be installed on the Webspace Server. In most cases the layouts are copied during the installation of the operating system, but East Asian and right-to-left input languages are not. For example, the following steps guide you on how to install these keyboard layouts.

1. Open the Server's Control Panel on the Server that clients will log into.
2. Double-click the Regional and Languages Options icon. A Regional and Language Options dialog box opens.
3. Select the Languages tab.
4. Click either or both of the check boxes in the Supplemental language support box. A message may open reporting the amount of disk space that will be required for the checked option.

> **Note:**
> You may need to provide the Windows Server DVD or the network share name to complete the file installation.

5. Click OK. Files for the checked languages will be installed.

6. Restart your computer.
   As a result of these steps, additional files will be copied to your machine. Support for the new languages will become available after the computer is rebooted.

### Understanding Keyboard Layouts Behind the Scenes

Be aware of the following when working with keyboard layouts:

- If the standard mechanisms are unable to provide the session with a keyboard layout, the Webspace Server will attempt to load a keyboard layout that matches the client's keyboard.
- The Windows Client will send the default keyboard layout (but not an IME) of the operating system, which will be used by the server to attempt to load the keyboard layout that best matches the client. This means that in most installations that do not utilize IMEs, the administrator is not required to perform any special configurations.
- Standard language keyboards have Windows keyboard layouts that are identical to the language's locale ID. For example, the French locale ID is 040C and the standard French keyboard layout is 0000040C.
- If the keyboard is not standard there might be mismatches. The keyboard layouts of non-standard keyboards are not unique across all Windows platforms. If all clients within an installation of Webspace use the same non-standard keyboard, the fallback layout text registry key can be used to specify it for all sessions. This will ensure that all clients will get the proper keyboard for each session.
- Client computers have different non-standard keyboards the best way to communicate this to the server is to specify the keyboard layout in the command line option or plug-in/applet tag parameter. For information on command line options, refer associated client to the section.

**Note:**
When connecting to a Chinese Webspace Server, the Sign In dialog appears from the shortcut along with the IME bar specifying Chinese as the default language. Clicking CTRL + Space bar does not toggle the languages. Users must manually click the IME bar with the mouse pointer to select English. Without manually clicking the IME bar, users will be unable to type a user name and password to log in.

## Running the Webspace Admin Console

The left panel of the Webspace Admin Console lists all Webspace Servers running the Proficy Webspace Application Publishing Service *(on page 184)*. By default, the Webspace Admin Console displays

information for the server running on your machine. To connect to other servers and view information about them, click the server name from the list of Webspace Servers.

If a server's icon displays a red X, the administrator does not have administrative rights on the server. If a server's icon displays a red x and is grayed out, the server is no longer running the Proficy Webspace Application Publishing Service or it has been turned off. In either case, the administrator is unable to access that server from the Webspace Admin Console application.

Click the All Servers icon in the left panel of the Webspace Admin Console to view a list of all active sessions on the network. This allows you to view active sessions without connecting to individual servers. This is also helpful for locating a particular session's server.

The Status Bar is displayed at the bottom of the Webspace Admin Console window. The Status Bar provides brief descriptions of menu commands when the mouse pointer is placed over that item in the menu. The Status Bar indicates the name of the Webspace Server currently being accessed, as well as the CPU utilization and memory usage for that server, as calculated by the Windows Task Manager. The last two items on the Status Bar, Sessions and Processes, indicate the number of sessions and the number of processes running on the active Webspace Server.

If All Servers is selected, the Sessions number will reflect all the sessions running on the network, and the Processes number will reflect all the processes on the network.

1. From the Webspace Admin Console, on the View menu, click Options. The Options dialog box appears.
2. Select the Status Bar check box, or click View and then Status Bar.

> **Note:**
> For a list of Webspace Admin Console shortcuts, see Keyboard Shortcuts for the Webspace Admin Console *(on page 175)*. In the Webspace Admin Console's dialog boxes, you can easily get Help by right-clicking an item, and then clicking What's This? A pop-up window will appear, displaying a brief explanation of the item. You can also get Help by clicking ? on the title bar of a dialog box and then selecting an item.

# Adding Applications to the Webspace Admin Console

For clients to run an application through Webspace, the application must be added to the Webspace Admin Console. Clients are then able to connect to the Webspace Server and to access the application. When adding applications to the Webspace Admin Console, you can specify startup parameters that control how the application opens and what processes are initiated when the application is started.

1. In the tree, from the list of All Hosts, select the server name that you want to add the application.
2. Click the Applications tab.
3. Click the Add button. The Add Application dialog box appears.
4. Enter the Executable Path. For example: C:\Program Files\Proficy\Proficy Webspace\Programs \ProficyWeb.exe.

   If you browsed for the application's .exe file in the preceding step, the file name will automatically be entered in the Display Name box. This name is displayed to users in the Program Window. You can keep the default display name, or you can type a new one. The application's Display Name cannot consist entirely of spaces and it cannot contain a backslash (\). This field cannot be left blank.

   If you browsed for the application's executable file, the path name of the directory will automatically be displayed in the Start Directory box. Otherwise, you will need to type the full path name of the directory in which you want the application to start.
5. In the Start Directory box, type the full path name of the directory in which you want the application to start. For example: C:\Program Files\Proficy\Proficy Webspace\Programs.
6. In the Startup State section, select whether the application starts maximized, minimized, or in normal mode.
7. In the Command-Line Options box, you can pass on launch parameters for the application. For example:

| **Application** | **Examples of Command-Line Options** |
|---|---|
| iFIX | IFIX /s"C:\Program Files (x86)\Proficy\Proficy iFIX\LOCAL\WEB.SCU" |
| CIMPLICITY | CIMVIEW or CIMLAYOUT (depends on the CIMPLICITY application you want to configure) For example: CIMVIEW /keypad "C:\Program Files (x86)\Proficy\Proficy CIMPLICITY\projects\CIMPDEMO\screens\1airhouse.cim" where: /keypad is an optional command line argument for cimview.exe. |

8. Click the Change Icon button if you would like to replace the application's default icon. Select a new icon from the Change Icon dialog box.
9. Click OK when you are finished.
10. Restart the Proficy Webspace Application Publishing Service. For steps, refer to the Restarting the Proficy Webspace Application Publishing Service *(on page 120)* section.

# Secure Deployment and Whitelisting

We strongly advise you to follow recommended practices with respect to network cybersecurity. For example, our products should be placed within a protected electronic security boundary, such as behind a properly configured firewall, and monitored by a properly tuned Intrusion Detection System (IDS) or an Intrusion Prevention System (IPS). Industrial Control System products should NOT be connected to the business network or directly to the Internet. (VPN is an example of a countermeasure that can be deployed.)

## Manually Configure a SandBox with Whitelist Entries for Files and Programs

The SandBox feature allows administrators to restrict user access to files and programs on a Webspace host (server) based on whitelist entries. These restrictions apply to users only, not to administrators or members of the Administrators Group. As a security practice, GE recommends assigning least-privileged user accounts for Webspace access. This is a security configuration hardening feature, which allows only the executables required for iFIX or CIMPLICITY to be launched through the Webspace interface. It helps mitigate security risks associated with unintended usage of Webspace.

## Whitelisting Overview

The Webspace server installation does not include a user interface for configuring SandBox white list entries. You can, however, manually edit the WorkspacePropertyDefinitions.xml file (typically in the C:\ProgramData\Proficy\WorkspacePropertyDefinitions.xml folder) to add files and programs to the white list for a Webspace server installation. The SandBox feature for files and/or programs must be enabled before specifying white list entries.

**Important:**
To enable whitelisting functionality, whitelisting must be enabled on ALL servers, including Relay Servers.

## How the Whitelist Works

Whitelisted files are specified by a fully qualified directory path. The SandBox will allow access to all files within a directory that is listed in the whitelist for files, including subdirectories. The WorkSpace profile directory, %USERPROFILE%, including all subdirectories, is automatically added to the files whitelist when a session starts.

Programs can be added to these desktops in four ways:

- Place the actual program executable module in a desktop folder. (for example, C:\Users\Public \Desktop\ExampleApp.exe)
- Place a shortcut to the program executable module in a desktop folder (for example, C:\Users \ExampleUser\Desktop\ExampleApp.lnk)
- Place a document that has an associated program in a desktop folder (for example, C:\Users \Public\Desktop\ExampleDoc.doc)
- Place a shortcut to a document that has an associated program in a desktop folder (for example, C:\Users\ExampleUser\Desktop\ExampleDoc.lnk).

**Note:**
The associated program of a whitelisted file, which is not in a desktop folder, is not automatically added to the programs whitelist.

Once the WorkspacePropertyDefinitions.xml file has been edited, the changes must be propagated to the DefaultWorkspaceProperties.xml file as shown in the next section.

### Configuration

The Webspace product will deploy a WorkspacePropertyDefinitions.xml file that will include all paths and programs needed by iFIX and CIMPLICITY, but with the default set to disable SandBox. After installation, the Application Publishing Service generates a DefaultWorkspaceProperties.xml file from the values in the WorkspacePropertyDefinitions.xml file. The Application Publishing Service derives its settings from the DefaultWorkspaceProperties.xml file.

System administrators can make additional changes by editing DefaultWorkspaceProperties.xml.

### Enabling the SandBox Feature

For files:

1. Stop the Application Publishing Service.
2. In a text editor, such as Notepad, open WorkspacePropertyDefinitions.xml.
3. Locate the filesSandboxEnabled property id, set the value to true, save the file, and restart the Application Publishing Service.

```
<propertygroup id="UserSandbox">

<property id="filesSandboxEnabled">

<label>User sandbox</label>

<description>Enables the user sandbox feature.</description>

<type>BOOL</type>
```

```
<defaultvalue>true</defaultvalue>

<constraints/>
```

For programs:

1. Stop the Application Publishing Service.
2. In a text editor, such as Notepad, open WorkspacePropertyDefinitions.xml.
3. Locate the programsSandboxEnabled property id, set the value to true, save the file, and restart the Application Publishing Service.

```
<property id="programsSandboxEnabled">

<label>Programs</label>

<description>Users may only run programs specified in the Programs white list.</description>

<type>BOOL</type>

<defaultvalue>true</defaultvalue>

<constraints/>
```

## Important Information

Be aware of the following:

- The value for filesSandboxEnabled in the WorkspacePropertyDefinitions.xml is case-sensitive and must be all in lowercase ("true" or "false").
- When using filesSandBoxEnabled=true, and iFIX is not installed to the default install folder, the root drive of the iFIX installation needs to be allowed read access. For example, add the line "E:\", ACCESS_READ | ACCESS_ALLOW_VISIBLE_CHILDREN; to the filesRequiredWhiteList section. Also, if the documentation is not installed to the default install folder, make sure that the ProficyDoc folder is denied access by listing it in the WorkspacePropertyDefinitions.xml. For example, change "%ProgramFiles(x86)%\Proficy\ProficyDoc",ACCESS_DENIED; to "E:\Program Files (x86)\Proficy \ProficyDoc",ACCESS_DENIED;

## Adding Folders to the Whitelist

In the C:\ProgramData\Proficy\WorkspacePropertyDefinitions.xml file, locate the "filesWhiteList" property:

```
<property id = "filesWhiteList">

<label>Files</label>

<description>Files and directories that users are allowed to access from the session.</description>

<type>STRING</type>

<defaultvalue>
```

```
</defaultvalue>
<constraints></constraints>
</property>
```

You can add multiple directory paths between the <defaultvalue> tags using one path per line, enclosed in double quotes, no leading white space, and ending with a comma and a semicolon, („;). Expandable environment variables can be included. For example:

```
<property id = "filesWhiteList">
<label>Files</label>
<description>Files and directories that users are allowed to access from the session.</description>
<type>STRING</type>
<defaultvalue> "C:\Departments\Accounting\Templates",; "%ALLUSERSPROFILE%\ExampleApp",;
</defaultvalue>
<constraints></constraints>
</property>
```

### Adding Program Files to the Whitelist

In the C:\ProgramData\Proficy\WorkspacePropertyDefinitions.xml file, locate the "programsWhiteList" property:

```
<property id = "programsWhiteList">
<label>Programs</label>
<description>Programs that users are allowed to run from the session.</description>
<type>STRING</type>
<defaultvalue>
</defaultvalue>
<constraints></constraints>
</property>
```

You can add multiple program file paths between the <defaultvalue> tags, using one path per line, enclosed in double quotes, no leading white space, ending with a semicolon (;). Expandable environment variables can be included.

For example, here is how you would add two executables:

```
<property id = "programsWhiteList">
<label>Programs</label>
<description>Programs that users are allowed to run from the session.</description>
<type>STRING</type>
```

```
<defaultvalue> "C:\ExampleApp\bin\ExampleApp.exe"; "%SystemRoot%\regedit.exe";
</defaultvalue>
<constraints></constraints>
</property>
```

### Applying Whitelisting Dynamically

The most efficient way to apply any whitelisting changes is as follows:

1. Stop the Application Publishing Service.
2. Delete the DefaultWorkspaceProperties.xml file.
3. Edit the WorkspacePropertyDefinitions.xml file.
4. Re-start the Application Publishing Service.

A new DefaultWorkspaceProperties.xml will now be generated.

An easier way to make changes is to simply modify the DefaultworkspaceProperties.xml file itself. This doesn't require an APS restart. But be aware that if this modified file ever gets deleted, the edited settings will be lost since an APS restart will generate the file from WorkspacePropertyDefinitions.xml. As a best practice, you should keep a backup of a working XML.

### Custom Applications

For custom applications, you will need to add the path and the programs to the corresponding lists (property id="filesWhiteList" and property id="programsWhitelist") with the right permissions to the path (ACCESS_READ | ACCESS_WRITE, ACCESS_ALLOW_ALL_CHILDREN, ACCESS_ALLOW_DESCENDANTS, or ACCESS_DENIED).

### CIMPLICITY Project Paths

You will need to add all project paths to "filesWhitelist" with ACCESS_READ, ACCESS_WRITE, ACCESS_ALLOW_ALL_CHILDREN, and ACCESS_ALLOW_DESCENDANTS permissions.

## Optimizing Webspace Server Performance

To optimize the performance of the Webspace Server, use the following tips:

## Setup Recommendations

- Restrict usage of mapped drives on the Webspace Server. The more mapped drives available, the longer it takes to log on to the Webspace Server.
- Try to limit the number of user and global logon scripts that you configure to run on the Webspace Server.
- If the SCADA Server and the Webspace Server are on different computers, avoid running iFIX on the Webspace Server machine.
- If the SCADA Server and the Webspace Server are on different computers, copy the needed shared files from the SCADA Server onto the Webspace Server machine. Use local copies of pictures on the Webspace Server machine.

- For printer driver options, only select the minimum set you need (such as the Universal driver).

- If you want to view pictures with historical information, make sure that you install Historian from GE Digital or the Historian Client Tools on the Webspace Server.

- Always start the browser session in full screen so that the WorkSpace uses more of the browser client area. Be aware that in browser sessions in full screen mode (your iFIX User Preferences are set to open pictures in full screen mode), you cannot Alt+Tab to other open applications such as Word or Excel that appear behind the Webspace application.

## Picture Recommendations

- Restrict the usage of high color graphics, such as bitmaps, as they take longer to load and tax system resources depending on the size and resolution. Try to use smaller sized files and at a lower resolution. Combine multiple bitmaps into a single image.
- For iFIX, disable auto-scaling on the Webspace Server (User Preferences > Picture Preferences) if you do not want the resolution of graphics and text in your pictures to change (and be auto-sized) when you open a picture from a web session. By default, auto scaling is enabled. You may want to disable this feature if text or images appear slightly distorted from the original picture when viewed via the web session.
- For iFIX, disable picture caching on the Webspace Server (User Preferences > Picture Preferences). By default, picture caching is enabled. Although it speeds up the picture performance, it will slow down the processing on the Webspace Server. If any memory needs to be freed up on the server, it is a good idea to disable picture caching.
- If you use Enhanced Charts in iFIX, use Bitmap/Gradient Styles sparingly.

- Minimize the number of pictures that are open at the same time in your Webspace client. In iFIX, try to avoid using the OpenPic command in pictures. We have found in testing that the OpenPic command results in slower performance. The ReplacePic command is preferred.
- If using Portal controls in your pictures, and you experience display issues in the Webspace sessions try some of these suggestions:
    - If Internet Explorer does not display these Portal controls, clear any proxy server settings. (On the Tools menu, click Internet Options. In the Internet Options dialog box, click the Connections tab and then the LAN Settings button to access proxy settings.) Next, clear the User JRE version for applet option in the Advanced Settings. (On the Tools menu, click Internet Options. In the Internet Options dialog box, click the Advanced tab and then scroll to the Java (Sun) category and locate the User JRE version for applet option.)
    - If the web browser's security levels are set to allow only trusted sites, make sure you add the Portal Server to the list of trusted sites.

- Refresh rates on pictures can also impact browser performance. In Webspace, by default, datalinks, animations, and charts (Enhanced and Standard) in pictures will refresh at a rate no faster than once per second. 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, Webspace will refresh the data no faster than every 5 seconds. For instance, even if you set the refresh rates in the Alarm Summary object to be faster, Webspace will not allow a rate faster than every 5 seconds.

You can adjust these default settings without opening any pictures. Open the FixUserPreferences.ini file on the iFIX Webspace Server. (By default, for iFIX, this file is located in the C:\Program Files\Proficy \Proficy iFIX\LOCAL folder. Scroll to the following section and enter larger numbers:

```
[WebspacePreferences]

DataRefreshThrottleInSecs=1

AlarmSummaryThrottleInSecs=5
```

A larger number for either of these settings (a slower refresh rate) is intended to improve the Webspace performance when opening pictures and may also improve mouse click response time.

**Note:**
If you have slower refresh rates entered in the objects in your pictures, Webspace will not reset the refresh rate settings to the lower default values of 1 and 5 when you open a picture.

The acceptable values for the DataRefreshThrottleInSecs are: 1, 2, 5, 10, 15, 30, and 60. Any other number will be reset to the lowest value it is closest to. For example, a 3 will become a 2, a 4 will become a 2, a 13 will become a 10, a 35 will become a 30, a 59 will become a 30, and a 65 will become a 60.

An acceptable value for AlarmSummaryThrottleInSecs is any whole number less than or equal to 300. If you enter a number greater than 300, it will be set to 300.

**Important:**
Use caution when changing these .ini settings, since user data displayed in Webspace is refreshed at these rates.

### Improving Picture Open Time

- If you do experience performance issues (for instance, a picture takes a long time to open, or the CPU on the Webspace Server or Client starts to spike), try opening the picture on a client (View node). If you notice similar performance issues on the client, consider modifying your pictures. For instance, you may want to set the picture refresh rates to a slower rate than the default. On a high-end server, the login time for the Webspace session is approximately 1.5 times that of a Windows View Node. For example, if your Windows View Node takes 30 seconds to start iFIX and open the picture, then the web browser will take approximately 45 seconds.
- If you experience high CPU usage on the Webspace Server, and you are using Alarm Summary objects in your pictures, try to reduce the number of rows displayed in the Alarm Summary object. Also, when viewing pictures from the web sessions, try closing any unnecessary pictures that display Alarm Summary objects. When multiple web sessions display pictures with Alarm Summary objects that include multiple rows, the CPU usage on the Webspace Server may rise. In this scenario, if you reduce the number of rows and open pictures, the CPU usage on the Webspace Server should improve.
- If login time (the time from when you enter the Webspace URL to the display of the login dialog box) increases with each successive client browser connection, this may indicate that the CPU usage on the server may be too high and there may be a hardware limitation on the web server. Consider using a higher-end server.

### Network Considerations

- The speed of the computer running the Webspace session from a browser can impact performance. Faster client machines typically load iFIX pictures much quicker, and have improved performance while those pictures are open. For instance, in testing, a slow client with 512 MB RAM

and 1.5 GHz processor had picture load times approximately 1.5 times longer than a faster client with 1 GB RAM and 3.0 GHz processor.

- Network speeds and connection types also impact performance for a Webspace session. A 100BaseT network adapter, which is recommended, allows the Webspace session to utilize optimum speed for its performance. Companies using VPN connections for Webspace sessions may experience a decrease in performance.
- Network bandwidth and traffic appears to have a significant impact on system performance. Higher traffic networks experience degraded load times and picture performance.
- Network capability in a Relay Server configuration is especially important, as it directly impacts system performance. A Relay Server will perform better on a network with greater speed and bandwidth.

# Chapter 4. Administration

## Administering the Webspace Server

The Webspace Admin Console allows you to administer, monitor, and control client access to the Webspace Server, and to add or remove Webspace sessions. It displays a list of the users logged on to a Webspace Server, along with the Webspace sessions the users are running, and the time the session was started. The Webspace Admin Console lets you terminate sessions and end processes taking place on the server.

Administrators use the Webspace Server to monitor processes, sessions, and server activity. The following sections provide information on functions the administrator may want to perform or know more about:



## Administration Window Overview

The Webspace Admin Console displays information about your Webspace Server. This information includes:

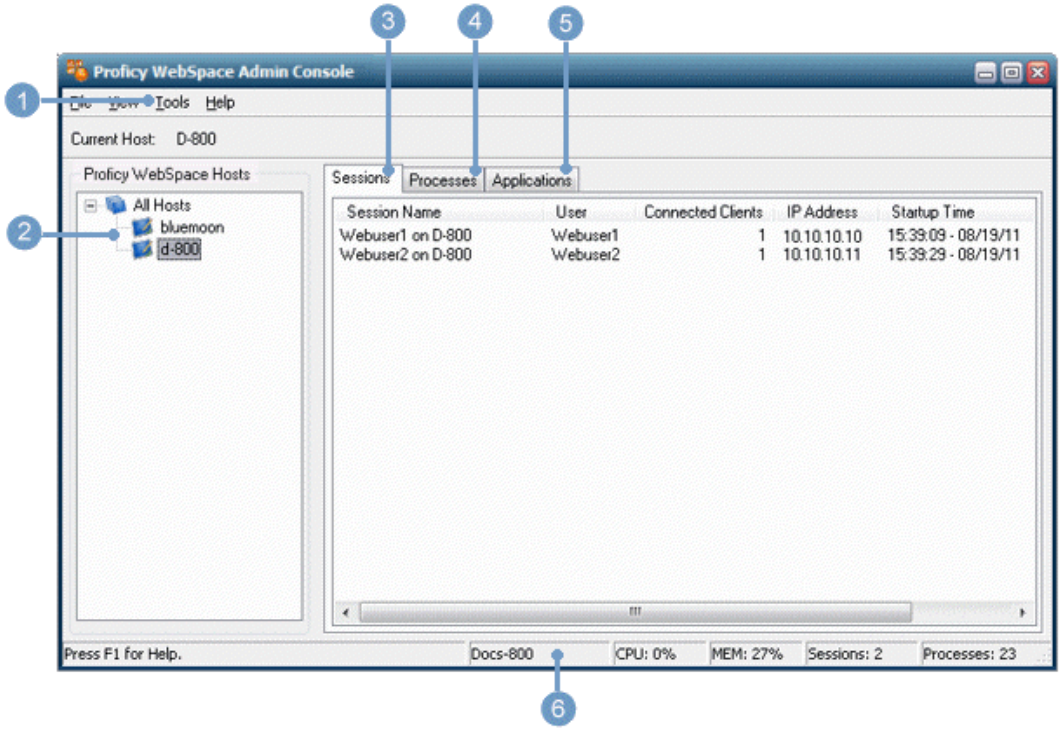
- Server activity and processes taking place on the server.
- A list of the users logged onto a selected Webspace Server.
- Applications users are running.
- Times that applications were started.

This information enables you to perform several administrative tasks, such as:

- Determine which applications are no longer being used and whether additional servers are required.
- Monitor clients.
- Administer sessions and processes including: Terminate user and End processes running on the server.
- Control client access to the Webspace Server.

### Window Overview

The following figure shows an example of the Webspace Admin Console.




The following table outlines each of the areas in the Webspace Admin Console.

| Screen Area | Description |
|---|---|
| | The Tools menu is where you access the Host Options dialog box *(on page 87)* to configure your Webspace Server. |
| | **The Tree View Pane**<br>The tree view portion of this window displays a list of Webspace Servers on the network and their status. For a list of icons and descriptions, refer to the Tree View Icons *(on page 84)* section in this topic. |

| Screen Area | Description |
|---|---|
| | **Important:**<br>You must belong to the Administrators group on each Webspace Server in order to access that server from the Webspace Admin Console. Without administrative rights on a server, you will be unable to add applications and terminate processes, and so on.<br><br>If a red X displays on the icon, the administrator does not have administrative rights on the server. If the server's icon has a red X and is grayed out, the server is no longer running the Application Publishing Service, or it has been turned off. A dependent server is orphaned when its relay server has gone down. |
| | **The Sessions Tab**<br><br>Sessions can be connected, terminated or refreshed through this tab on the Webspace Admin Console window. Information displayed about each session includes: a unique identifier for the session name, the network user name for that session, number of clients connected to a session (2 or higher indicates the session is being shadowed), the IP address of the client computer from which the user is accessing the server, the date and time the user started the application, and the number of applications the user is accessing. |
| | **The Processes Tab**<br><br>Process information can be viewed, refreshed, or terminated from this tab.<br><br>**Note:**<br>Ending a process without giving users a chance to close their application can result in the loss of data. |
| | **The Applications Tab**<br><br>You can assign command line parameters for the associated application, or change the icon that displays for the application from this tab. |
| | **The Status Bar** The status bar provides the following for a selected Webspace Server currently being accessed:<br><br>• Name.<br>• CPU utilization.<br>• Memory usage. |

| Screen Area | Description |
|---|---|
| | • Number of running sessions.<br>• Number of running processes.<br><br>**Note:**<br>If All Hosts is selected, the Sessions number will reflect all the sessions running on the network, and the processes number will reflect all the processes on the network. |

### Tree View Icons

The following table describes the icons that can appear in tree view area of the Webspace Admin Console.

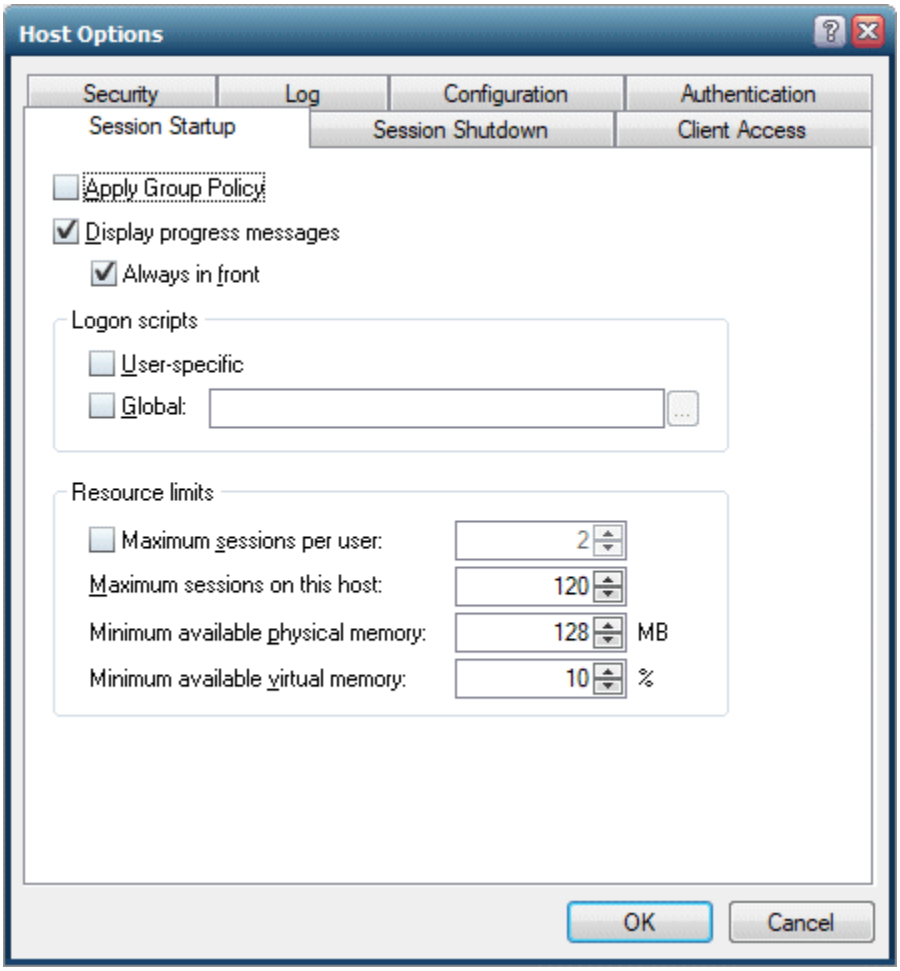
| Icon | Description | Status |
|---|---|---|
| | Webspace Server (Not part of a Relay Server Configuration) | Available |
| | Dependent Application Server (in a Relay Server Configuration) | Orphaned |
| | Relay Server | Unavailable |
| | Relay Server | Available |
| | Dependent Application Server (in a Relay Server Configuration) | Available |
| | Dependent Application Server (in a Relay Server Configuration) | Unavailable |

### Accessing the Webspace Admin Console

During the Webspace installation, a shortcut to the Webspace Admin Console is created by default. You can access the Webspace Admin Console from the desktop shortcut or from the Start menu. On the desktop, double-click the Webspace Admin Console icon, or on the Start menu, point to Programs, Proficy Webspace, and then click Admin Console.

## Host Options Dialog Box

The Host Options dialog box is accessed from the Tools menu, from the Options command. It contains information for configuring your Webspace Server. The Host Options dialog box with example settings is shown in the following figure.




The Host Options dialog box displays the following tabs:

## Session Startup

The Session Startup tab displays the following items:

| Item | Description |
|---|---|
| Apply Group Policy | Select to apply Group Policy to a user's session at startup. Using Group Policy and its extensions, administrators can:<br>• Manage registry-based policy.<br>• Assign scripts. |

| Item | Description |
|---|---|
| | • Redirect folders.<br>• Manage applications<br>• Specify security options. |
| Display Progress Mes-sages | Select to allow various progress messages to be shown to users during session startup, after a user is authenticated. Displayed messages include:<br>• A user's personal settings are being loaded.<br>• Group Policy is being applied.<br>• Network drives are being connected.<br>• Logon scripts are being run. |
| Always in Front | Select so that session startup progress messages will be displayed in front of all other windows. Clear to permit other windows to be placed in front of the progress messages. |
| Logon Scripts: User-specific | Enable to permit a user-specific executable file to be run during the individual logon process.<br>**Important:**<br>Authenticated users must have read and execute access to the logon script files. User-specific logon scripts are specified using the functionality provided by the operating system. |
| Logon Scripts: Global | Specifies the path of an executable file to be run for all users that log on to the server.<br>**Important:**<br>Authenticated users must have read and execute access to the logon script files. |
| Maxi-mum Ses-sions Per User | Allows you to specify the maximum number of sessions that a user may run concurrently. Clear the check box next to this field to allow each user to have an unlimited number of sessions. The default is to have an unlimited number of user sessions. |
| Maxi-mum Ses-sions on this Host | Specifies the maximum number of sessions allowed on this server. When the entered maximum sessions are reached on the Webspace Server, additional sessions are denied access. For example, if the maximum number of sessions is 25, the user who initiates the 26th session will be prevented from logging on. The default is 25 sessions per Webspace Server. |

| Item | Description |
|---|---|
| | **Important:**<br>In a relay server setting, Webspace checks the maximum sessions setting on the relay server AND its dependent application servers. The value entered for the Maximum sessions on the relay server is the maximum number of sessions that can be run concurrently on all dependent application servers assigned to that relay server. |
| Minimum Available Physical Memory | Specifies the minimum number of megabytes of physical memory that must be available for a session to start. When the available physical memory falls below the entered number (MB), additional users cannot log on. The default is 128 MB. |
| Minimum Available Virtual Memory | Specifies the minimum percentage of virtual memory that must be available for a session to start. When the available virtual memory falls below the entered percentage value, additional users cannot log on. The default is 10 percent (%). |

### Session Shutdown

The Session Shutdown tab displays the following items:

| Item | Description |
|---|---|
| Timeouts: Session | Lets you set a limit on how many minutes a session may run on a server. By default, this option is disabled. |
| Timeouts: Idle | Lets you specify a limit to the number of minutes of idle time allowed on a server, since the last mouse or keyboard input event was received in a session. By default, this option is disabled. |
| Idle Action | Select Disconnect to disconnect users when the idle limit has been reached, or select Log to log off users when the idle limit has been reached. |
| Warning Period | Lets you specify the number of minutes before a session or idle limit is reached when users are warned that they are about to be disconnected or logged off. This option may be select- |

| Item | Description |
|---|---|
| | ed if either Session or Idle is enabled. However, the Warning Period must be less than the session limit and idle limit settings. Values less than or equal to zero provide no warning period. |
| Grace Period | Lets you specify the number of minutes necessary to provide for a graceful shutdown of the application and all of its processes when a session is being closed. The Grace Period defaults to a value of 1 minute and should ONLY be changed at the instruction of GE Customer Support personnel. |
| Disconnected Sessions Terminate: Immediately | Select so that sessions will terminate as soon as their clients disconnect. |
| Disconnected Sessions Terminate: After | Lets you specify how many minutes sessions should remain running after their clients disconnect. For example, if the network connection is lost or if users unintentionally disconnect from Webspace, their session state is preserved for the length of time entered here. |
| Shared Account | Allows you to create an account that be shared by multiple users. If an administrator designates an existing user name as a shared account while that user is disconnected from his or her session, the session will remain running on the server until the termination limit has been reached. The session will then be terminated. Before specifying a shared account, verify in the Webspace Admin Console that there are no connected or disconnected sessions using that account.<br><br>**Note:**<br>Webspace does not support the use of domain names (for example, NORTH\johnq) for shared accounts. |

## Client Access

The Client Access tab displays the following items:

| Item | Description |
|---|---|
| Clipboard | Enables client clipboard support. Any clipboard data from the browser session is available only within the WorkSpace application. In order to copy the contents to other applications on the local disk of the client machine you must create a shell script within an object inside your WorkSpace picture that launches Notepad.exe, on the Webspace Server. After you do this, you can use this object to launch Notepad in run mode from the web session. Paste the contents into Notepad, and save this file to the local disk of web session computer. |
| Sound | Enables client sound support. Webspace supports sound capability for any application that uses PlaySound, sndPlaySound, or waveOut. It is not required that sound cards and/or speakers be installed on Webspace Servers. The client machine, however, does require a sound card and speakers. Audio support is disabled by default on the Webspace sessions.<br><br>**Important:**<br>Be aware that client sound capability requires the loading of Webspace libraries into session processes. This can affect the startup of a process, make some processes incompatible with Webspace, or have fatal consequences during suspend/resume operations. Use caution when enabling this setting. |
| Drives | Enables client file access. |
| Hide | Lets you specify the drives letter(s) of client drives you would like to hide. For example: A, B, G-J. Hidden drives are inaccessible to the user through the Webspace session. |
| Assign consecutive letters starting at... | Lets you remap client drives by listing client drives sequentially starting at a given drive letter. |

| Item | Description |
|---|---|
| Increment By... | Lets you remap client drives by incrementing client drive letters by a fixed value. |
| Universal Printer Driver | Enables the use of the Universal Printer Driver that can print to any client printer. When only the Universal Printer Driver is enabled, only the Universal Printer Driver will be used as a printer driver. No native drivers will be used. This is the default setting. The Universal Printer Driver uses a standard printing properties dialog box and may not offer some of the more advanced printing options other drivers do. The Universal Printer Driver can be used when the native driver is not available. When neither the Universal Printer Driver nor Windows Printer Drivers is enabled, no printers will be configured, and client printing is disabled.<br><br>**Note:**<br>A printer named Preview PDF is configured in each session when the Universal Printer Driver is enabled. Documents printed to this printer are automatically converted to a .pdf file and displayed on the client computer. Users can save, print, or email the document at their discretion. A PDF reader, such as Adobe Reader, is required on the client computer in order to use the Universal Printer Driver's PDF conversion feature. |
| Windows Printer Driver | Enables printers to be configured using already installed native drivers. When only the Windows Printer Drivers option is enabled, only native printer drivers that are installed on the Webspace Server will be used. If a printer's native driver is not installed, that printer will not be configured. To allow Webspace to automatically install native printer drivers that ship with Microsoft Windows click the Automatically install drivers. The Windows Printer Driver option is preferred when configuring proxy printers, if they are available and if settings allow them to be used. When both the Universal Printer Driver and the Windows Printer Drivers are enabled, and a printer's native driver is installed on the Webspace Server, the printer's native driver will be used to configure the printer. If it is not installed on the Webspace Server, the printer is configured to use the Universal Printer Driver. When Windows Printer Drivers and Automatically install drivers are enabled, only native printer drivers that are installed on the Webspace Server or those that are included with Windows will be used. If a printer's native driver is not installed and it is not included with Windows, that printer will not be configured. When neither the Windows Printer Drivers nor Universal Printer Driver is enabled, no printers will be configured, and client printing is disabled. |
| Automatically | Allows Webspace to automatically install native printer drivers that ship with Microsoft Windows. The Automatically Install Drivers option is only available when the Windows Printer Driver option is selected. |

| Item | Description |
|---|---|
| Install Drivers | |
| Automatically Update Clients | Lets you automatically update a Webspace Desktop Client when a user connects to a Webspace Server that is running a newer version.<br><br>**Note:**<br>The Automatically Update Clients option on the Client Access tab of the Webspace Admin Console is only available for the Windows Desktop Client. It does not apply to other clients such as Mozilla Firefox and Internet Explorer. |
| Serial and Parallel Ports | Allows applications running on the host to access client machines' serial and parallel ports. Serial and parallel ports are disabled by default. Be aware that Client Serial and Parallel Ports requires the loading of Webspace libraries into session processes. This can affect the startup of a process, make some processes incompatible with Webspace, or have fatal consequences during suspend/resume operations. As such, when Serial and Parallel Ports is enabled, a message box opens and asks for confirmation. |
| Video Replay | This feature is currently not supported for Webspace 6.2. |
| Open Files on Client | This feature is currently not supported for Webspace 6.2. |
| Use Client Time Zone | Select this option to run Webspace sessions in the time zone of the client computer. |

## Security

The Security tab displays the following items:

| Item | Description |
|---|---|
| Transport | Lets you select the protocol to use for communication between clients and Webspace Servers. When selecting the Encrypted transport, an Certificate file must be specified. |
| Port | Lets you change the port on which this Webspace Server is listening. |
| Encryption | Lets you specify the type of encryption of the data that is transmitted between the client and the server. Encryption includes:<br><br>• The client's user name and password, which are supplied during logon<br>• Any application data submitted by the client or returned by the server.<br><br>After you have selected an encryption type, all succeeding Webspace sessions will be encrypted. Sessions that are active when the feature is enabled will not be encrypted. A user must log off, then onto the Webspace Server for his or her session to be encrypted. |
| Certificate | Lets you specify the full path of the certificate that is required to use the Encrypted transport. You can obtain a certificate from a trusted Certificate Authority (CA) such as Verisign or Thawte, or you can create your own certificate authority and then sign your server certificates from this authority. When the Encrypted transport is selected, all connections to that Webspace Server use the Encrypted transport and the selected encryption algorithm, including connections from Webspace sessions. Consult the documentation from the CA of your choice using the following information as a guide to obtain a server certificate from a CA that is trusted by the client operating system. In order for a certificate to work in Webspace:<br><br>• A private key is required.<br>• The certificate must be in PEM format.<br><br>Consult Microsoft documentation for details. |
| Use Certificate for Web Connections to IIS (uncheck to re- | This feature is currently not supported for Webspace 6.2. |

| Item | Description |
|---|---|
| move instantly) | |
| Generate Certificate | This feature is currently not supported for Webspace 6.2. |
| Notify Users When Connections are Secure | Enable to notify users with a message when connections between client and server are secure. This option is only available when the Encrypted transport mode is selected. |

## Log

The Log tab displays the following items:

| Item | Description |
|---|---|
| Folder | Specifies a folder to which log files will be written and in which there are subfolders where backed up logs will be stored. The default location is: C:\Program Files\Proficy\Proficy Webspace\Log. Webspace Server does not support storing logs directly in a network folder. |
| Output Level | Specifies the level of information written to the log file, with numbers 1 to 6 capturing ever greater detail, and 0 capturing no output. The default level is 2. |
| Maintenance | Lets you select which action will be performed on log files that have reached the specified age or size. The action applies to the current log file as well as to those which are inactive. |
| Files More than ... days old | Specifies how many days old log files can become before being deleted or moved to the Backup subdirectory of the Log folder. The setting applies to the current log file as well as to those which are inactive. |
| or... MBs in size | Specifies at what size, in megabytes, log files are to be deleted or moved to the Backup subdirectory of the Log folder. The setting applies to the current log file as well as to those which are inactive. |

### Configuration tab

The Configuration tab displays the following items:

| Item | Description |
|---|---|
| Application Host | Click the **Dependent Host** option, and the specify the name or IP address of the Relay Server. The Relay Server manages the communication between Webspace Clients and a set of dependent application servers.<br><br>**Note:**<br>The **Independent Host** and **Farm Host** options are currently not supported. |
| Application Host Manager | Select the **Relay Load Balancer** option to enable the Webspace server to become a Relay Server for load balancing.<br><br>**Note:**<br>The **Farm Manager** option is currently not supported. |
| Backup License Manager | This feature is currently not supported for Webspace 6.2. |

### Authentication

The Authentication tab displays the following items:

| Item | Description |
|---|---|
| Standard Authentication | Allows users to log on with their user name and password every time they connect to the server. Users are added to the server's INTERACTIVE group and have the same access rights they would have if they logged on to the server at its console. This is the default setting.<br><br>**Note:**<br>To make the "Cache Passwords on the Client" option available for selection, you must have the Standard Authentication option selected. |
| Cache Passwords | Allows users to log on without having to enter their user name and password every time they connect to the server. Available only when Standard Authentication is enabled. With this option enabled, the Login dialog box will display a "Remember me on this Computer" check box. If a |

| Item | Description |
|---|---|
| on Client | user selects this check box on the first login from the client, the next time that user logs in from that same computer, the Logon dialog box will show the User Name and Password dialog box pre-populated with the previous login. All the user needs to do to continue is click Sign In. Passwords are encrypted on the server, transmitted over the network, and stored on client computers in user-private directories. Users are added to the server's INTERACTIVE group and have the same access rights they would have if they logged on to the server at its console. The cached password is saved in the following directory: C:\Documents and Settings\<user name> folder\Application Data\Proficy\Proficy Webspace\<server name>.dat |
| Integrated Windows Authentication | Allows users who sign in from Windows computers that are members of the same domain as the Webspace Server without having to re-enter their user name and password every time they connect to the server. When Integrated Windows Authentication is the only option enabled, users' passwords are never transmitted over the network. Users are added to the INTERACTIVE group, and passwords are cached on the server by default. If both Standard authentication and Integrated Windows authentication are enabled, the Webspace Server attempts to log in the user with Integrated Windows authentication first, and then Standard authentication, if Windows authentication fails.<br><br>**Tip:**<br>For Webspace auto login to work, be sure to enable the Integrated Windows Authentication option, and add the SHOWIFIXLOGIN=0 line in the Fixuserpreferences.ini file in the iFIX Local folder under the WebspacePreferences section. |
| Require two-factor Authentication | This feature is currently not supported for Webspace 6.2. |
| OpenID Connect authen- | This feature is currently not supported for Webspace 6.2. |

| Item | Description |
|---|---|
| tica-<br>tion | |

# User Account Settings

To access Webspace sessions on a Webspace Server, client users must log on to the server machine. When users start a Webspace session, they are prompted for their user name, password, and the name of the server they wish to access. This information is encrypted and passed to the Proficy Webspace Application Publishing Service *(on page 184)* running on the Webspace Server. The Proficy Webspace Application Publishing Service then performs the logon operation using standard multi-user features of Windows.

When a user logs on to a server and a domain is not specified, the Webspace Server first tries to authenticate the account on the local machine, then the machine's domain, and finally the trusted domains. Users can override this default behavior and specify a domain by typing the domain name followed by a backslash and their network user name in the user name field of the Logon dialog box. For example: NORTH\johng.

When a local user name on the Webspace Server is the same user name as a domain account, each with a different password, Webspace treats them as two separate accounts.

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

Users must be able to log on interactively (locally) on the Webspace Server. Assign local logon rights to users in Local Security Policy, Domain Security Policy, and Domain Controller Security Policy.

For more detailed information on administration of user accounts, please consult your Microsoft Windows Help.

## Setting File Permissions

As the system administrator, you may need to restrict user access to certain files and resources. Keep in mind that there are multiple users accessing the server.

Particularly in a Relay Server environment, it is recommended to write-protect your system and application folders so that users are unable to save files on a Webspace Server. Otherwise, the next time a user logs on to Webspace and is routed to a different server, the files and folders will be inaccessible.

You must use Windows Explorer to set the permissions for files on the server. By setting file permissions, you can restrict user access to applications, printers, and folders. Please note that file permissions can only be set on drives formatted with the Windows NT file system (NTFS). If you are using the FAT file system *(on page 182)*, you will be unable to set permissions for specific files or restrict access to applications.

Once an application's permissions have been set, you can assign specific parameters for the application with the Webspace Admin Console.

**Note:**
**:** While in Windows Explorer, open the Help for more information on setting file permissions.

## Setting up a Network Printer

If the printer on the Webspace Server is a network printer, and you want to allow printing on the web sessions to this printer, you must add the network printer to the Web Server. As the administrator, you can set up network printers for use by Webspace sessions. You must first create a port on the Webspace Server that connects directly to the server and then install the printer locally. This provides direct access to the printer.

Network printers are set up using the Windows Add Printer Wizard.

**Note:**
If a printer is physically connected to the Webspace Server, and you want to allow printing from the web sessions to this printer, no additional configuration changes need to be made on the Webspace Server or web session. If you want to allow printing in the web sessions from client printers, refer to the Client Printing *(on page 139)* section for information on how to configure.

1. On the Start menu, point to Settings, and then click Printers and Faxes.
2. Double-click the Add Printer icon.
3. Select local printer, then click Next.
4. Click Create a new port and select Local Port or Standard TCP/IP Port as the type. Click Next.
5. In the Port Name dialog, type the UNC path to the printer or the printer's IP address. For example: \ \PRINTSERVER\LASERPRINTER.

6. Select the printer manufacturer on the left and the printer model on the right or click Have Disk.
7. Follow the directions provided by the Add Printer Wizard to install the proper printer driver.

# Session Startup

For information on starting up Webspace sessions, refer to the following sections:



## Applying Group Policy

The Microsoft Group Policy is supported. Using Group Policy and its extensions, administrators can manage registry-based policy, assign scripts, redirect folders, and specify security options. For more information regarding this feature, go to: https://technet.microsoft.com/en-us/library/Hh147307(v=WS.10).aspx.

1. From the Webspace Admin Console, in the server tree, select the desired server from the list.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. On the Session Startup tab, select the Apply Group Policy check box.
4. Click OK.

**Note:**
It may take users longer to log on to the Webspace Server when the Group Policy is enabled.

## Displaying Progress Messages

After a user is authenticated, a message box that reports session startup progress can be displayed to users. When enabled, these messages inform users of the following:

- When their personal setting are being loaded.
- When Group Policy is being applied.
- When network drives are being connected.
- When logon scripts are being run.

1. From the Webspace Admin Console, in the server tree, select the desired server from the list.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Session Startup tab.
4. Select the Display progress messages check box.
5. To ensure that messages are displayed in front of all other windows, select Always in front check box.

   **Note:**
   If a logon script has the ability to display user interface to the user, the Always in front option should not be enabled. Otherwise, the logon script's user interface may be partially obscured by the progress message.

6. Click OK.

## Logon Scripts

Logon scripts allow administrators to configure the operating environment for Webspace users. Scripts may perform an arbitrary set of tasks such as defining user-specific environment variables and drive letter mappings.

Webspace supports two types of logon scripts: global scripts that execute for all users that log on to the server, and user-specific scripts that execute for individual users. Before loading the user's profile, Webspace checks to see if a script of either (or both) type has been specified. If so, Webspace runs the script(s) within the user's security context each time the user is authenticated.

**Note:**
User-specific project paths for Webspace sessions are not supported. For example, you cannot use different directory paths for iFIX files, such as pictures, across multiple users. If you need to support this, it is suggested that you use iFIX with Terminal Server, instead of Webspace.

User-specific logon scripts are specified using the functionality provided by the operating system. For example, the logon script for local users on a Windows 2000 server is specified as follows:

1. Right-click My Computer and click Manage.
2. Navigate to the \System Tools\Local Users and Groups\Users folder.
3. Select a user and click Properties.
4. Click Profiles.
5. In the Logon script box, type the file name of the user's logon script.

If the value entered in the Logon script box specifies a file name and extension only, Webspace searches for the file in the following directories, in the following order:

1. If the user's account is a domain account is the NETLOGON share of the primary domain controller (for example: \\pdcname\NETLOGON), or the domain subdirectory of the primary domain controller's SYSVOL share (for example: \\pdcname\SYSVOL\domainname).
2. If the user's account is a local account. For example: systemroot\System32\Repl\Import\Scripts or systemroot\sysvol\sysvol\domainname.

If the logon script is stored in a subdirectory of one of the above directories, precede the file name with the relative path of that subdirectory. For example: Admins\JohnG.bat.

Administrators specify global and user-specific logon scripts through the Webspace Admin Console's Session Startup dialog.

## Running User-specific Logon Scripts

1. From the Webspace Admin Console, in the server tree, select the desired server from the list.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Session Startup tab.
4. Select the User-specific check box.
5. Click OK.

## Running a Global Logon Script

1. From the Webspace Admin Console, in the server tree, select the desired server from the list.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Session Startup tab.
4. Select the Global check box.
5. In the field next to the check box, specify the path of the global script file.

   For example, you may want to add the LoginScript.bat, provided in the C:\Program Files\Proficy \Webspace Server\Programs folder as an example for configuring mapped drives, as a global script.
6. Click OK.

**Note:**
Authenticated users must have read and execute access to the logon script files. An example of a logon script is described in the Creating Mapped Drives on the Webspace Server *(on page 68)* section. The LoginScript.bat example described in this section can be applied on a global or user-specific basis.

## Setting Resource Limits

Webspace allows administrators to prevent users from starting new sessions when certain resource limits are exceeded on a Webspace Server. These limits help administrators prevent servers from becoming loaded to the point where users experience performance problems and random resource allocation failures. You can also limit the total number of session connections to the Webspace Server. And, you can prevent users from logging on when the available physical memory or virtual memory on a server falls below a given value.

These resource limits are especially important in a Relay Server configuration. For each dependent server in a Relay Server configuration, you must configure these limits.

## Limiting the Number of Sessions per User

1. From the Webspace Admin Console, in the server tree, select the desired server from the list.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Session Startup tab.
4. Select Maximum sessions per user check box.
5. In the field next to the check box, enter the maximum number of sessions allowed per user on this server.
6. Click OK.

## Limiting the Number of Sessions per Webspace Server

1. From the Webspace Admin Console, in the server tree, select the desired server from the list.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Session Startup tab.
4. In the Maximum sessions per host field, enter the total maximum number of sessions allowed for this server.
5. Click OK.

## Specifying the Minimum Available Physical Memory Necessary for this Server to Start a Session

1. From the Webspace Admin Console, in the server tree, select the desired server from the list.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Session Startup tab.
4. In the Minimum Available Physical Memory field, enter the minimum number of free megabytes (MBs) necessary for sessions to be allowed on this server.
5. Click OK.

## Specifying the Minimum Percentage of Virtual Memory Necessary for this Server to Start a Session

1. From the Webspace Admin Console, in the server tree, select the desired server from the list.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Session Startup tab.
4. In the Minimum Available Virtual Memory field, enter the minimum percentage number necessary for sessions to be allowed on this server.
5. Click OK.

## Logging in with One Login Dialog Box with iFIX

Webspace provides the ability to pass through the authenticated Windows user from the Webspace session without asking for re-authentication in iFIX.  To enable on the Webspace Server, select Tools > Options. From the Host Options dialog box, select the Authentication tab and then the Integrated Windows Authentication check box.

If enabled, no longer will you see the double logins: one for Webspace and one for the iFIX session. Logins are simplified to a single login with this feature enabled.

However, if you need to do writes within your picture from a Webspace session, the currently logged in user MUST be logged out and manually logged back in. In order to do this in iFIX, you need to have a login script in the picture to open the iFIX Login dialog box. For more information, refer to the LogIn Subroutine section of the iFIX Automation Reference. Otherwise, writes will not be allowed from the following:

- A Datalink
- An Alarm Acknowledgement (in the Alarm Summary or Command Expert)
- A Write Value change (Command Expert)

- A Ramp Value change (Command Expert)
- The Toggle Digital Value (Command Expert)
- The Toggle Scan (Command Expert)
- Within a DataEntry field (Slider Expert for example)
- Through EDA (using the EDAQUICK tool)

### How to Enable in iFIX

To enable this option in iFIX, edit the FixUserPreferences.ini in the iFIX Local folder. By default, this folder is: C:\Program Files\Proficy\Proficy iFIX\LOCAL. Add the SHOWIFIXLOGIN key and set its value to 0, as shown in the following snippet of code.

```
[WebspacePreferences]

DataRefreshThrottleInSecs=1

AlarmSummaryThrottleInSecs=5

SHOWIFIXLOGIN=0
```

By default, this feature is disabled for compatibility issues with previous versions.

**Note:**
For this option to work properly in a Relay Server setup, the SHOWIFIXLOGIN key update should exist in the FixUserPreferences.ini on all the dependent servers.

# Session Shutdown

For information on shutting down the Webspace session, refer to the following sections:



## Specifying the Session Limit

The session limit is the number of minutes that sessions are allowed to run on a Webspace Server.

1. From the Webspace Admin Console, in the server tree, select the desired server from the list.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Session Shutdown tab.

4. Select the Session check box.
5. In the field next to the check box, enter the number of minutes that a session is allowed to run on a server before its user is logged off.
6. Click OK.

   The minimum number of session time is 1 minute, and the maximum is 44640 minutes (31 days). This feature is disabled by default.

## Specifying the Idle Limit

Idle time refers to the number of minutes since the last mouse or keyboard input event was received in a session. The idle limit is the number of minutes of idle time that a Webspace Server allows.

1. From the Webspace Administration, in the server tree, select the desired server from the list.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Session Shutdown tab.
4. Select the Idle check box.
5. In the field next to the check box, enter the number of minutes of idle time allowed by the server.
6. From the Action drop-down list, select either Disconnect to disconnect users when the idle limit has been reached, or Log off to log users off when the idle limit has been reached.
7. Click OK.

   The minimum number of idle time is 1 minute, and the maximum is 44640 minutes (31 days). This feature is disabled by default.

## Specifying the Warning Period

The warning period represents the number of minutes before a session limit or idle limit is reached when users are warned they are about to be disconnected or logged off. For example, if the warning period is set to 2, users will be warned 2 minutes before the session limit or the idle limit is reached.

The warning period must be less than the session limit and idle limit settings. This feature is disabled by default.

1. From the Webspace Administration, in the server tree, select the desired server from the list.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Session Shutdown tab.
4. Select the Warning period check box.

> **Note:**
> Either a Session or Idle time-out must be configured for the Warning period check box to become available.

5. In the field next to the check box, enter the number of minutes before a session or idle limit is reached when users are warned that they are about to be disconnected or logged off.
6. Click OK.

### Specifying the Grace Period

The grace period allows you specify the number of minutes required to provide for a graceful shutdown of the application and all of its processes when a session is being closed. The Grace Period defaults to a value of 1 minute and should ONLY be changed at the instruction of GE Customer Support personnel.

1. From the Webspace Administration, in the server tree, select the desired server from the list.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Session Shutdown tab.
4. Select the Grace period check box.

> **Note:**
> Either a Session or Idle time-out must be configured for the Grace period check box to become available.

5. In the field next to the check box, enter the number of minutes after a logoff that users are able to save files and close applications, and so on.
6. Click OK.

   The minimum grace period value is 1 minute, and the maximum value is 15. By default, the grace period is 1 minute.

## Security Options

For information on Webspace security options, refer to the following sections:

- Authentication Overview *(on page 109)*
- Selecting the Transport Mode *(on page 111)*
- Encrypting Sessions *(on page 114)*

- Notifying Users of a Secure Connection *(on page 115)*
- Modifying the Server Ports *(on page 112)*
- Client-Side Password Caching *(on page 115)*
- Hiding Server Drives *(on page 116)*


## Authentication Overview

Webspace provides two methods of authentication:

- Standard Authentication (the default setting)
- Integrated Windows Authentication

Webspace requires that at least either Standard authentication or Integrated Windows authentication be enabled. If both Standard authentication and Integrated Windows authentication are enabled, the Webspace Server attempts to log the user on in the following order:

- Integrated Windows authentication.
- Standard authentication, if Windows authentication fails.

**Tip:**
For Webspace auto login to work, you must use the Integrated Windows Authentication option in the Host Options dialog box on Authentication tab. Additionally, in iFIX, you must add the SHOWIFIXLOGIN=0 line in the Fixuserpreferences.ini file in the iFIX Local folder under the WebspacePreferences section.

### Standard Authentication

Standard Windows authentication is the default method for authenticating users on a Webspace Server. Standard authentication allows users to sign in to a Webspace Server from the Logon dialog box by supplying their user name and password. Once authenticated, users are added to the server's INTERACTIVE group and given the same access rights as if they had signed in to the Webspace at its console.

Users logging onto a Webspace Server with standard authentication are:

- Added to the server's INTERACTIVE group.
- Granted the same access rights that they have when logging onto the server at its console.

**Important:**
In a Relay Server configuration, a user logs in to the Dependent Application Server, but the user credentials must also be authenticated at the Relay Server  to obtain a Webspace “license token."

Standard authentication includes logging on either with a user name and password supplied by any of the following:

- Logon dialog·box
- HTML parameters·
- Command-line arguments

Optionally, when Standard Authentication is enabled, you can also enable Client-Side Password Caching *(on page 115)* to allow the user name and password to be saved locally on the client, if the Remember Me on this Computer check box was selected in the Logon dialog box on the previous login. With the Remember Me on this Computer option enabled, the Logon dialog box appears with the user name and password pre-populated.

### Integrated Windows Authentication

Integrated Windows authentication allows users to connect to a Webspace Server and start a session without having to sign in to the server and re-enter their user name and password. When Integrated Windows authentication is the only option enabled, the user’s user name and password are never transmitted over the network. Instead, the Webspace simply runs the user’s session in the same security context as the Webspace Client. Users are added to the server's INTERACTIVE group, and passwords are cached on the server by default.

**Important:**
Integrated Windows authentication is only available to users who sign in from Windows computers that are members of the same domain as the Webspace Server.

**Note:**
When Integrated Windows authentication is the only option enabled, the user’s user name and password are never transmitted over the network. Instead, Webspace runs the user’s session in the same security context as the client.

To avoid these conditions, when Integrated Windows Authentication is enabled, Webspace automatically caches passwords on the server. Doing so allows users to sign in from Windows computers that are

members of the same domain as the Webspace Server without having to enter their user name and password every time they connect. Users are prompted for a password when first connecting to the server or following a password change. Passwords are stored within their respective profiles and can only be decrypted from within their respective security contexts. With subsequent connections to Webspace, users are automatically signed in and added to the host's INTERACTIVE group. They are granted the same access rights had they signed in to the host at its console.

Webspace caches passwords on the host using the industry standard encryption algorithms provided by Microsoft's Data Protection application programming interface (DPAPI). For more information about DPAPI search the MSDN Library (http://msdn.microsoft.com/library/default.asp) for "Windows Data Protection."

**Important:**
If User Account Control (UAC) is enabled on the Webspace Server, be aware that if you first log in to the Webspace Server console and then try to start a Webspace session on a remote client by logging in under the same user, you may experience issues with the application not being able to start on the Webspace Server. Log out of the Webspace Server console, and then log back in to the console to resolve this issue.

## Selecting the Transport Mode

Webspace supports transport protocols that provide communication between Windows and the Webspace Server. When selecting the Encrypted transport, an Certificate file must be specified. Certificates are required to secure communication between Webspace sessions and the Webspace Server. You can obtain a certificate from a trusted Certificate Authority (CA) such as Verisign or Thawte, or you can create your own certificate authority and then sign your server certificates from this authority.

**Important:**
The Apache and IIS web servers and their components (for example, OpenSSL) must be maintained and patched as per the latest security guidelines provided by their respective software vendors. The security of Webspace sessions depends on the security that the web servers provide.

1. From the Webspace Admin Console, in the server tree, select the desired server from the list.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Security tab.
4. In the Transport drop-down list, select TCP or Encrypted.

5. When selecting Encrypted transport, type or browse to the path of the server's certificate in the Certificate box.
6. Click OK.

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

## Modifying the Server Ports

When you install Webspace, and the firewall is enabled, the install automatically prompts you to add the Webspace to your exception list.  This allows users to access the Webspace Server through a firewall or router. Administrators can modify the Webspace Server port setting for the Proficy Webspace Application Publishing Service *(on page 184)*. The default port number for the Encrypted transport is 491.

In order for users to access Webspace through a firewall or router, administrators are able to modify the host port setting for the Application Publishing Service. The Application Publishing Service must be running on a dedicated port. Conflicts may arise if another service is running on the same port. The default port number for both TCP and SSL is 491.

Port 492 is the port used by the “Webspace Relay Client Manager Service" to centrally manage the Webspace user count in a Relay Server configuration. This port is not configurable through the Webspace Admin Console application.

1. In the Webspace Admin Console, in the Webspace Server tree, select the server.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Security tab.
4. In the Port edit box, enter a new port number.

   **Important:**
   The port can only be set to 443 if there is no web server on the computer configured to accept HTTPS connections. (Web servers accept HTTPS connections on port 443.) If the Application Publishing Service must accept connections on port 443 (to allow connections through proxy servers, for example), the web server must be run on a different computer.

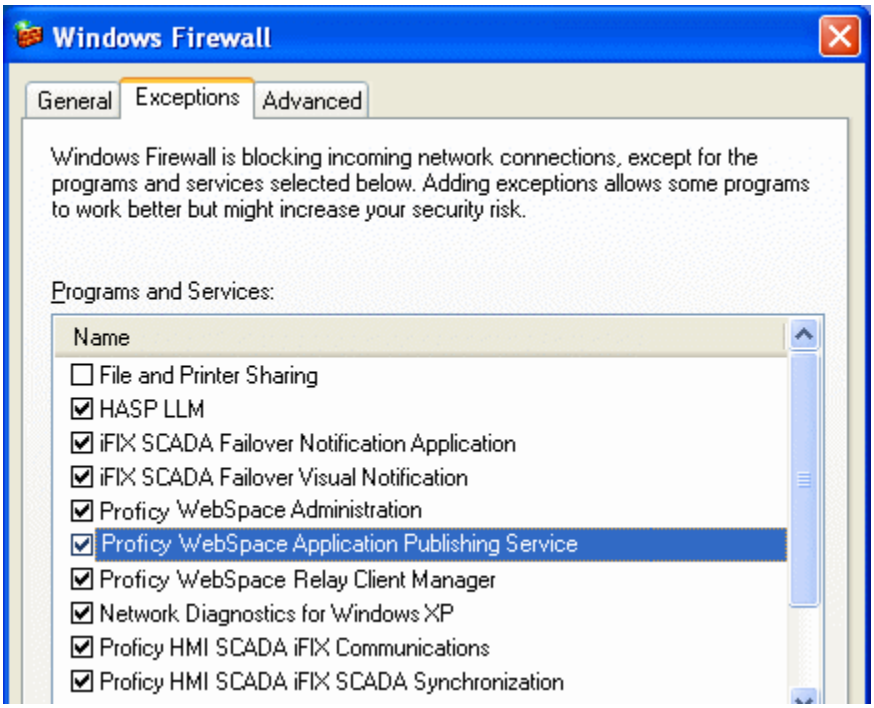
5. Click OK.

> **Note:**
> In a Relay Server Configuration, if you change the ports, make sure the port usage is the same on the Relay Server and each Dependent Application Server.

6. After changing the server port number, you must
    - Restart the service and any other services that depend on it. For example, if you change port 491 and you allow client printing, you must restart the "Proficy Webspace Application Publishing Service" and the Print Spooler Service in order for client printing to work on a port other than the default port 491.
    - Modify the port parameter from the Webspace hyperlink, if you are using a command line. Use the port parameter followed by the new port number. For example, for iFIX: http://WebspaceServerName/ProficyWebspace/iFIX.html?port=1667. For CIMPLICITY: "C:\Program Files (x86)\Proficy\Proficy Webspace\Client\Proficy.exe" -a CimView -h server1 -hp 1667.
    - Modify the port parameter argument, if using Webspace from a desktop shortcut or the Connection dialog box. Append the -hp argument (followed by the new port number) to the shortcut. For example, for iFIX: "C:\Program Files (x86)\Proficy\Proficy Webspace\Client\Proficy.exe" -a iFIX -h server1 -hp 1667. For CIMPLICITY: specify the host port in the .HTML file. For details, refer to the CIMPLICITY HTML File Overview *(on page 154)* (the table in the General Options section describes the hostport parameter).
    - If you specify the port number in the Connection dialog box when signing in to Webspace, in the Host Address box, type the host name or IP address, followed by a colon and the port

number (for example, server1:1667). If the new port number is not specified by either of these methods, users will be unable to sign in to Webspace.

- Enable the new port through your firewall software. For example, the following figure shows a list of Windows Firewall exceptions that includes the Webspace applications:




## Encrypting Sessions

For purposes of security, administrators can optionally encrypt all data transmitted between the client and the server. This includes the client's user name and password, which are supplied during logon, and any application data submitted by the client or returned by the server. Webspace supports the following encryption options:

- Encrypted, 56-bit DES (with certificate)
- Encrypted, 128-bit RC4 (with certificate)
- Encrypted, 168-bit 3DES (with certificate)
- Encrypted, 256-bit AES

1. From the Webspace Admin Console, in the Webspace Server tree, select the desired server from the list.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Security tab.
4. From the Encryption drop-down list, select an encryption level.

5. Click OK.

   After you have enabled encryption, all new Webspace sessions will be encrypted. Sessions that are active when the feature is enabled will remain unencrypted. The next time the user logs on to the Webspace Server, however, his or her session will be encrypted. The user must log off the Webspace Server, and log back on in order for his or her session to be encrypted.

## Notifying Users of a Secure Connection

When the Encrypted transport is selected as the transport mode, you can opt to notify users when connections are secure.

1. In the Webspace Admin Console, in the Webspace Server tree, select the server.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Security tab.
4. In the Transport list box, select Encrypted.
5. In the Certificate field, type or browse to the path of the server's certificate file.
6. Select the Notify users when connections are secure option.
7. Click OK.

## Client-Side Password Caching

**Note:**
To make the "Cache Passwords on the Client" option available for selection, you must have the Standard Authentication option selected on the Security tab in the Host Options dialog box.

Client-side password caching allows users who are not members of the Webspace Server's domain to log on without having to enter their user name and password every time they connect to the server.

With this option enabled, the Login dialog box will display a "Remember me on this Computer" check box. If a user selects this check box on the first login from the client, the next time that user logs in from that same computer, the Logon dialog box will show the User Name and Password dialog box pre-populated with the previous login. All the user needs to do to continue is click Sign In.

After the first manual authentication, the user logon credentials are encrypted on the server using the SYSTEM account context, transmitted over the network, and stored on client computers in user-private directories.

When the user makes subsequent connections to the server, the cached password is transmitted back to the server, where it is decrypted using the SYSTEM account context and then used to automatically log the user on to the Webspace Server. The user is added to the server's INTERACTIVE group and granted the same access rights had that user logged on to the server at its console. The Sign In dialog is displayed with the user name and password and with Remember me on this computer checked. If the user disables the Remember me on this computer option, the user's credentials will be deleted from the client computer.

Webspace caches passwords on the server using the industry standard encryption algorithms provided by Microsoft's Data Protection Application Programming Interface (DPAPI). For more information about DPAPI search the MSDN Library (http://msdn.microsoft.com/library/default.asp) for "Windows Data Protection."

1. From the Webspace Admin Console, on the server list, select the desired server.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Authentication tab.
4. Select the Cache Passwords on the Client check box.

   **Note:**
   This option is only available if the Standard Authentication option is also selected.

5. Click OK.

   On most platforms, the cached password is stored in the user's home directory in a .dat file named for the Webspace Server. For example, for the Webspace ActiveX Control, C:\Documents and Settings\user1\Application Data\Proficy\Webspace Server\server1.dat is an example location of the cached password. In this example, user1 is the user logged into the Webspace session, and server1 is the name of the Webspace Server.

   Client-side password caching is supported on Internet Explorer, Mozilla Firefox, and the Desktop Client.

   **Important:**
   If you are concerned about public computers retaining cached passwords, you should clear the Cache Passwords on the Client check box on the Webspace Server. By default, this option is cleared.

## Hiding Server Drives

Microsoft's Group Policy Objects lets you hide specific host drives. For instructions, see http://support.microsoft.com/kb/231289. To hide host drives, the Apply Group Policy option must be enabled in the Host Options dialog box in the Webspace Admin Console.

# Password Change

Password changes can be made through Windows security groups and accounts. Users can change passwords when:

- The administrator requires the user to change his or her password at the next logon. For more information, refer to the Changing Passwords at Next Logon *(on page 117)* section.
- The security policy is configured to prompt users to change passwords before expiration. For more information, refer to the Prompting Users to Change Passwords Before Expiration *(on page 118)* section.
- The user's password has expired. For more information, refer to the Prompting Users to Change Passwords After Expiration *(on page 118)* section.

## Changing Passwords at Next Logon

Administrators can require a user to change his or her password by checking the User must change password at next logon option in the Windows user configuration setup.

For Local accounts, you can access these properties by right-clicking My Computer and Selecting Manage. The Computer Management window appears. In the System Tools folder, there is a Local Users and Groups folder. Locate the user name in this folder, right-click it, select Properties, and then click the General tab.

1. From your web browser, access the Webspace default page (http://WebspaceServerName/ProficyWebspace) and select the appropriate Webspace session.
2. In the Logon dialog, type the user name and password. If the account does not exist in the domain in which the Webspace Server resides, include the domain name in the User name field as a prefix (for example: domain\username).
3. Click OK. The following message displays:

   ```
   You are required to change your password at first logon.
   ```

4. Click OK. The Change Password dialog box appears.
5. In the New Password and Confirm New Password fields, enter the new password.
6. Click OK.

## Prompting Users to Change Passwords Before Expiration

By default, users are prompted to change their passwords whenever they log on within 14 days of their password's scheduled date of expiration. Administrators can modify the change password "prompt" period by editing the Prompt user to change password security setting. For example, the Local security settings can be viewed and changed by clicking Start, and then pointing to Settings, Control Panel, Administrative Tools, and then Local Security Policy. The User Configuration folder contains the Security Settings.

**Note:**
Be aware that if you open a web session and the user name includes a password that is due to expire, the Password Expiration dialog box remains in the background and loses focus. As a workaround, move the Login dialog box to access the Password Expiration dialog box, and then click Yes and continue.

1. From your web browser, access the Webspace logon page (http://WebspaceServerName/ProficyWebspace) and select the appropriate Webspace session.
2. In the Logon dialog, type the user name and password. If the account does not exist in the domain in which the Webspace Server resides, include the domain name in the User name field as a prefix (for example: domain\username).
3. Click OK. The following message displays:

   ```
   "Your password will expire in x day(s). Do you want to change your password now? Yes/No"
   ```

   If you click No, the Webspace session starts. If you click Yes, the Change Password dialog appears.
4. If the Change Password dialog box appears, in the New Password and Confirm New Password fields, enter the new password and click OK.

## Prompting Users to Change Passwords After Expiration

This task explains how to log on after a password has expired.

1. From your web browser, access the Webspace default page (http://WebspaceServerName/ProficyWebspace) and select the appropriate Webspace session.
2. In the Logon dialog, type the user name and password. If the account does not exist in the domain in which the Webspace Server resides, include the domain name in the User name field as a prefix (for example: domain\username).

3. Click OK. The following message displays:

```
Your password has expired and must be changed.
```

4. Click OK. The Change Password dialog box appears.
5. In the New Password and Confirm New Password fields, enter the new password.
6. Click OK.

# Monitoring Server Activity

The Webspace Admin Console displays information about server activity and processes taking place on the Webspace Server. Administrators can use this information to determine whether additional servers are required, and which sessions are no longer being used.

The following sections provide more information on how to monitor and refresh server activity:



## Refreshing the Webspace Admin Console

You can update the information displayed in the Webspace Admin Console manually or you can set it to update automatically. If the Webspace Admin Console is set to update automatically, you can still update it manually at any time.

For information about setting the Webspace Admin Console to update automatically or manually, refer to the Setting the Refresh Rate in the Webspace Admin Console *(on page 119)* section.

1. From the Webspace Admin Console, on the server list, select the desired server.
2. On the View menu, click Refresh. The data should refresh in the window as you are viewing it.

## Setting the Refresh Rate in the Webspace Admin Console

You can set the Sessions, Processes, and Applications tabs in the main window of the Webspace Admin Console to manually refresh or to automatically refresh at a specified frequency.

## Setting the Refresh Rate to Allow Only Manual Refresh

1. From the Webspace Admin Console, on the server list, select the desired server.
2. On the View menu, click Options. The Options dialog box appears.
3. Select Manual.
4. Click OK.

## Setting the Refresh Rate to Refresh Automatically

1. From the Webspace Admin Console, on the server list, select the desired server.
2. On the View menu, click Options. The Options dialog box appears.
3. Select the Refresh every _ seconds option.
4. In the Seconds edit box, type a value.
5. Click OK.

## Restarting the Proficy Webspace Application Publishing Service

There may be times when you need to restart the Proficy Webspace Application Publishing Service. For example, if you change the SCU path on the Applications tab, after you already entered it for the first time, you will need to restart this service.

You can restart the service from the Webspace group on the Start menu, or from the Services window from the Windows Administrative tools.

1. On the Start menu, point to Programs, Proficy Webspace, and then click Stop Proficy Webspace Server.
2. Wait a few moments for the action to complete. A command window opens briefly and then closes.
3. On the Start menu, point to Programs, Proficy Webspace, and then click Start Proficy Webspace Server.
4. Wait a few moments for the action to complete. A command window opens briefly and then closes.

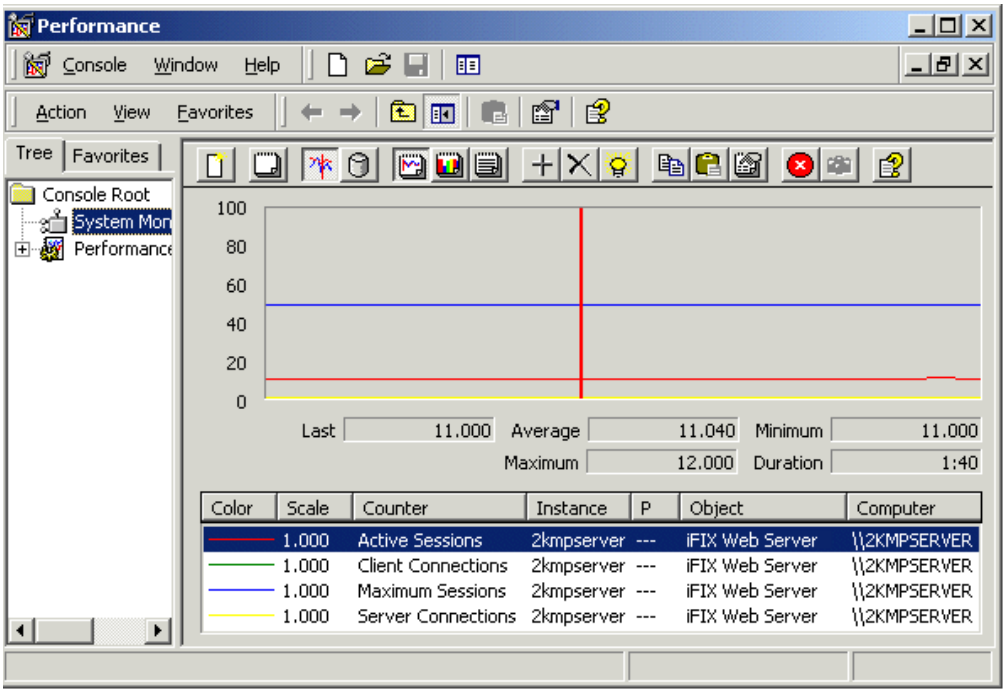
## Viewing Performance Counters

Webspace Server performance counters can be added to the Windows Performance Monitor to track the number of active sessions and the number of clients connected to a server. Webspace Server performance counters allow administrators to monitor server activity from any machine with network access to a Webspace Server. The Remote Registry Service (Regsvc.exe) must be enabled for remote performance monitoring to work.

1. On the Start menu, point to Programs, Settings, Control Panel, Administrative Tools, and then click Performance. The Performance window appears.
2. Click the + button to add counter(s). The Add Counters dialog box appears.
3. From the Performance Object drop-down list, locate and click Webspace Server.
4. From the Counter list, select the desired counters (Active Sessions, Client Connections, Maximum Sessions, Server Connections) and click Add.
5. Click Close.

Webspace Server performance counters include:

| Counter | Description |
|---|---|
| Client Connections | The total number of client connections on the Webspace Server. |
| Server Connections | Not applicable. |
| Active Sessions | For sessions host on that server, currently running on the computer. |
| Maximum Sessions | This displays the Maximum Sessions per user setting in the Host Options dialog, on the Session Startup tab. |



## Working with Sessions and Processes

The following sections describe how to view session and process information for the Webspace product:



## Viewing Session Information

The Webspace Admin Console displays the following session information: Session Name, User Name, Connected Clients, IP Address, Startup Time, and Applications. You can find this information on the Sessions tab.

1. To view session information, click the Sessions tab.
2. See the following table for a description of each field.

| Column | Description |
|---|---|
| Session Name | Unique identifier assigned to each session. |
| User | Network user name of the user accessing the server. |
| Connected Clients | The number of clients connected to a session. 0 indicates that no one is connected to the session (the client has disconnected). 1 indicates that the client is connected, and the session is active. 2 or higher indicates that the session is being shadowed. |
| IP Address | IP address of the client computer from which the user is accessing the server. (Each computer on a network has a unique IP address.) |
| Startup Time | Date and time the user started the application. |
| Applications | Number of processes the user is accessing. |

## Viewing Process Information

A process refers to the specific application that a client is running from the server. The Webspace Admin Console displays the following process information: Process Name, User Name, Startup Time, and Process ID.

1. To view process information, click the Processes tab.
2. See the following table for a description of each field.

| Column | Description |
|---|---|
| Name | Name of the application running on the server. |
| User | Network user name of the user accessing the application. |
| Startup Time | Date and time the user started the application. |
| Process ID | Process identification number assigned by the server's operating system. (The number for each running application matches the process identification number displayed in the Windows Task Manager.) |

## Ending Client Processes

Processes are any actions taking place on the Webspace Server that are initiated by a client. a Webspace session, for example, is a process. Each running Webspace session is assigned a unique name and process ID in the Windows Task Manager. These process names and IDs are duplicated in the Webspace Admin Console. Webspace Administrators can end any process from the Webspace Admin Console.

1. From the Webspace Admin Console application, in the main window, click the Processes tab.
2. Select the process or processes you want to end.
3. On the Tools menu, point to Processes, and then click Terminate.

## Reconnecting a Session

Session reconnect allows sessions to be maintained on a Webspace Server without a client connection. If the client's connection to the server is lost, intentionally or unintentionally, the user's session remains running on the Webspace Server for the length of the session time-out specified with the Webspace

Admin Console. Session reconnect allows users to return to their Webspace session in the exact state they left it.

If the network connection is lost or if users unintentionally disconnect from Webspace, their session state is preserved for the length of time specified in the Webspace Admin Console. After a user is authenticated through normal logon procedures, the Webspace Server determines if the user has an active session. If so, that session is resumed and appears exactly as it did prior to disconnection. If not, a new session is started. Users are also able to disconnect from one client and reconnect to the session from another client.

When attempting to reconnect to a disconnected session, users are required to specify their logon credentials.  After the server validates them, the server reconnects them to the disconnected session. If the session is hosted on a server that is part of a Relay Server configuration, the user is routed to his or her session without any indication that the session is on a Relay Server. If Integrated Windows authentication is available, users are automatically re-authenticated and re-connected to their session.

## Shadowing a Session

Session shadowing allows multiple users to view and control a single Webspace session. Only administrators can connect to running Webspace sessions, but only with permission from the session's user. A shadow session does not consume a license; however, each open browser window (even if logged on under the same user name) does consume a license.

1. From the Webspace Admin Console application, in the main window, click the Sessions tab.
2. From the Sessions Name column, select the session(s) you would like to shadow
3. On the Tools menu, point to Sessions, and then click ConnectFrom the Sessions Name column, select the session(s) you would like to shadow.

   -Or-

   From the Sessions Name column, right-click the session you would like to shadow, then click Connect.

   After the session is selected, a message is displayed to the session's user requesting permission to connect to the session. If the user clicks Yes, and allows access to his or her session, the connection is made immediately and the Webspace session opens in a new frame window.

   If the user clicks No and denies access, the following message is displayed on the server:

   ```
   The session's owner has denied access to the session.
   ```

Session shadowing will also be denied when the session is disconnected, when the session is in the process of shutting down, or when the user fails to respond within one minute. Connection is also denied in the event of a Webspace communication failure.

The Sessions tab in the main windows of the Webspace Admin Console displays the number of clients connected to a session. Two or more clients in the Connected Clients column indicates that the session is being shadowed. Disconnected sessions have 0 connected clients. To disconnect from a session and end session shadowing, simply close the frame window where the session is displayed.

**Note:**
When an Webspace session is being shadowed, the server's cursor remains on the client until that session is closed. It does not go away even when the session is no longer being shadowed.

## Terminating Sessions

When terminating a user's session, all Webspace sessions for that user stop, and the user is logged off the Webspace Server.

1. From the Webspace Administration application, in the main window, click the Sessions tab.
2. From the Session Name column, select the session(s) you want to terminate.
3. On the Tools menu, point to Sessions, and then click Terminate.

**Note:**
You can also right-click on the selected session(s) and click Terminate from the shortcut menu.

**Important:**
Terminating a session without giving users a chance to close their application can result in the loss of data.

## Setting the Session Termination Option

Administrators control how long Webspace sessions remain running on the Webspace Server through the Webspace Admin Console's Host Options dialog. Select the Immediately option if you want the Webspace

sessions and all running processes to be terminated as soon as the session disconnects. Select the After _ minutes option to specify the number of minutes that a session will remain running after a client has disconnected from the session. Figure the number of minutes (n) and enter (n+1) in the edit field that a session should remain running after the client disconnects. This extra minute allows the application to shut itself down gracefully instead of getting terminated immediately. The After 1-minute option is the default setting.

If you select the After 1-minute option, a shutdown message appears in the event log and the processes stop gracefully. With the Immediately option, running processes get terminated without notice, and stop immediately.

The Sessions tab in the main windows of the Webspace Admin Console displays the number of clients connected to a session. Disconnected sessions have 0 connected clients.

1. From the Webspace Admin Console, on the server list, select the desired server.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Session Shutdown tab.
4. In the Disconnected sessions terminate area, select one of the following disconnected session termination options:
    - Immediately
    - After _ minutes. In the edit box, type the number of minutes plus one that sessions should remain running after their clients disconnect. For example, if you want to leave it running 2 minutes, enter 3 minutes in this edit field.
5. Click OK.

# Log Files

The Webspace Server creates log files for certain Webspace processes. These files are stored in the log directory and are used to record program errors and events. With this information, Technical Support can diagnose and correct problems that may arise. This can be especially helpful for errors that are only reproducible on specific machines or with a specific application.

All log files, whether they pertain to the client or server machine, are located on the Webspace Server. By default, this path is: C:\Program Files\Proficy\Proficy Webspace\Log. In Log folder are three subfolders: Backup, Codes, and Templates. Be careful not to delete these folders. Webspace messages are recorded within log files prefixed with aps and followed by the date and time (to the nearest millisecond) the Webspace Application Publishing Service was started (for example: aps_2007-04-04_09-55-47-636.html). A new log file is created each time the Proficy Webspace Application Publishing Service is started. The

log file with the latest date and time stamp contains messages for the current or most recent instance of the Proficy Webspace Application Publishing Service.

Problems detected in the execution of Webspace are described by entries in the log file. Each entry is uniquely identified by an item number along with a date and time stamp, and a description of the event or program error. Technical Support uses this information to locate a problem's source and to determine its resolution.

Entries in the log file may also include prefixes for locating messages associated with an individual user's session. If the event occurred within the context of a given session, the name of the session will appear at the beginning of the message, for example, SuzyG on Server1. If the message prefix contains the connection name aps, the event occurred within the Proficy Webspace Application Publishing Service, but was not associated with a connection to another process.

For example, for "iexplore (1908) A client at IP address 3.26.60.91 disconnected from session Logon2 on Fxbifixoct", 1908 is the ID of the process in which the event took place, 3.26.60.91 is the IP address of the Webspace session, and Fxbifixoct is the name of the Webspace Server.

### Example Use of Log Files

Say for instance you cannot make a connection to the Webspace Server when you log on from a web session. It could be because you do not have enough physical or virtual memory available to make the connection. Set the output log level to 4 on the server, as described in the Setting the Output Level *(on page 128)* section, and try to log on again. If the issue was a memory issue, you would see a message similar to this in the log file:

"A session could not be created for user because only 62,935,040 bytes of physical memory were available. The minimum requirement is 134,217,728 bytes."

## Selecting a New Location for the Log Files

By default, log files are created and stored in the Log folder on the Webspace Server machine. By default, this folder is: C:\Program Files\Proficy\Proficy Webspace\Log. You can select a new location for the log files through the Webspace Admin Console's Host Options dialog.

Be aware that the Webspace Server cannot back up log files directly to a network folder. For example, if you type a UNC path or a mapped network drive in the folder edit box, the following message is displayed:

```
"Please specify a usable Windows folder where log files may be written."
```

1. From the Webspace Admin Console, on the server list, select the desired server.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Log tab.
4. In the Folder edit box, type the path to the new directory or browse to its location.

> **Note:**
> You should move the Backup folder and existing log files to the new location, along with the Templates and Codes subfolders.

## Setting the Output Level

Webspace offers the following log output levels:

| Level | Description |
|---|---|
| 0 | No output |
| 1 | Errors |
| 2 | Errors and Events (Default Setting) |
| 3 | Errors, Events and Warnings |
| 4 | Errors, Events, Warnings, and Diagnostic Messages |
| 5, 6 | Errors, Events, Warnings, Diagnostic Messages, and Trace Messages |

1. From the Webspace Admin Console, on the server list, select the desired server.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click Log tab.
4. In the Output level edit box, enter one of the above numeric values.

> **Important:**
> Setting the log output value to 5 or 6 may adversely affect Webspace performance. These output levels yield very large files, and should only be used in a controlled environment –

preferably when only one client is accessing the Webspace Server. The default value for the Output level is 2.

**Important:**
Changes to the Output Level are applied to Webspace sessions that are started after the change.

## Maintaining Log Files

Webspace creates a new log file every time the Proficy Webspace Application Publishing Service starts. Over time these files can accumulate and consume a significant amount of disk space. To help manage these files, Webspace lets you delete or backup log files and set file size or age limits. By default, the logs are stored in this folder on the Webspace Server: C:\Program Files\Proficy\Proficy Webspace\Log.

## Deleting Log Files

1. From the Webspace Admin Console, on the server list, select the desired server.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Log tab.
4. In the Maintenance area, from the drop-down list, select Delete.
5. In the Files more than _ days old field, specify how old (in days) log files can become before being deleted.
6. In the _ MBs in size field, specify at what size (in megabytes) log files are to be deleted.
7. Click OK.
8. Restart the Proficy Webspace Application Publishing Service.

## Backing Up Log Files

1. From the Webspace Admin Console, on the server list, select the desired server.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Log tab.
4. In the Maintenance area, from the drop-down list, select Back Up.
5. In the Files more than _ days old field, specify how old (in days) log files can become before being moved to the Backup subdirectory of the Log folder.
6. In the _ MBs in size field, specify at what size (in megabytes) log files are to be moved to the Backup subdirectory of the Log folder.
7. Click OK.

8. Restart the Proficy Webspace Application Publishing Service.

   Once every half hour, and each time it is started, the Proficy Webspace Application Publishing Service searches the Log folder for files that have not been modified for more than the specified number of days. It then either deletes the files or moves them to the Backup subdirectory of the Log folder. If while sweeping the log files, the Proficy Webspace Application Publishing Service finds that nothing that the age or size limit has been met in the current log file, it closes the file and installs a newly created file in its place.

   By default, inactive log files are backed up after 7 days or when the file size has reached 20 MB.

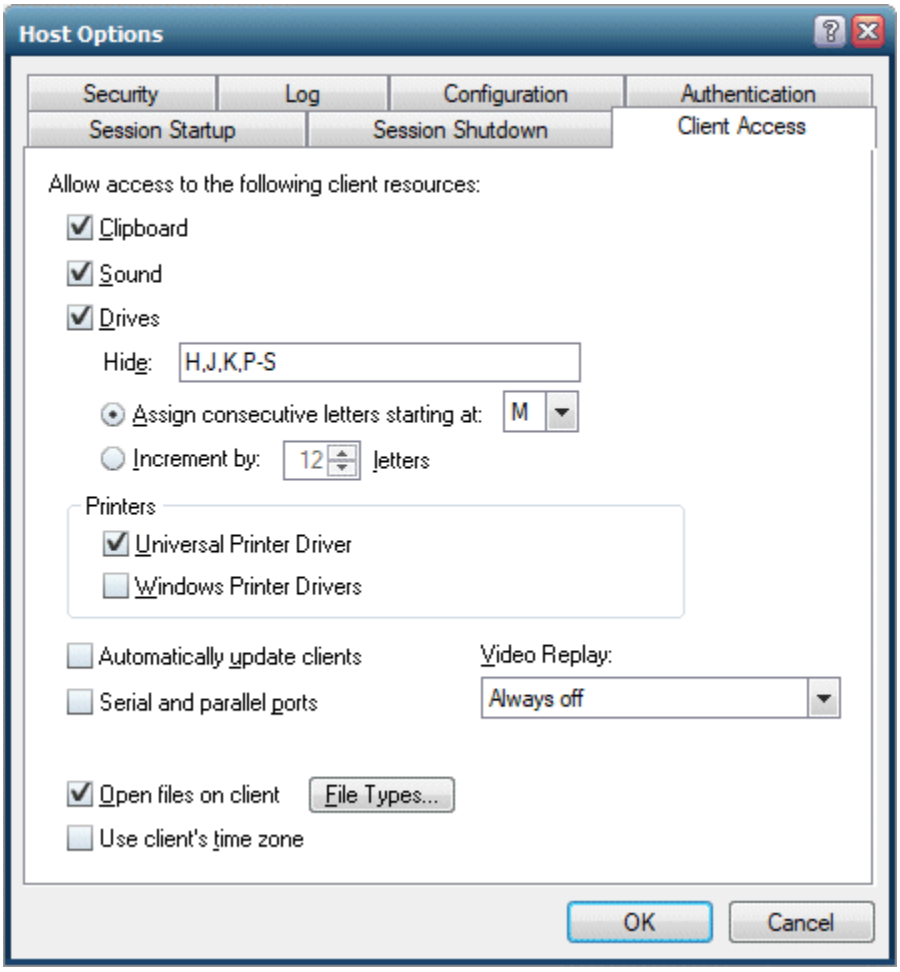
# Chapter 5. Optional Web Session Properties

## Configuring Optional Web Session Properties

There are other optional settings that you can configure for your Webspace session through the Webspace Admin Console. These include the following items:



Refer to each section for more information. All of these settings can be configured from the Client Access tab of the Host Options dialog box in the Webspace Admin Console, as shown in the following figures.




# Clipboard Access

You can cut and copy information from a Webspace session and paste it into applications running on a Webspace Server, and vice versa. Clipboard support is disabled by default.

1. In the Webspace Administration, select the desired server from the list of All Servers.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Client Access tab.
4. Click the Clipboard check box.
5. Click OK.

   Any clipboard data from the browser session is available only within the WorkSpace application. In order to copy the contents to other applications on the local disk of the client machine you must create a shell script within an object inside your WorkSpace picture that launches Notepad.exe,

on the Webspace Server. After you do this, you can use this object to launch Notepad in run mode from the web session. Paste the contents into Notepad, and save this file to the local disk of web session computer.

## Sounds

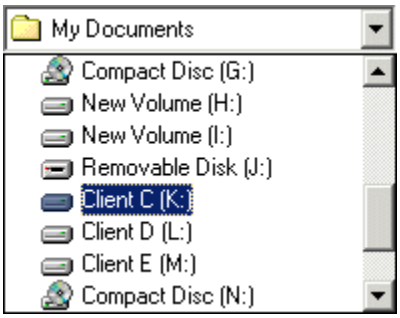
Webspace supports sound capability for any application that uses PlaySound, sndPlaySound, or waveOut. It is not required that sound cards and/or speakers be installed on Webspace Servers. The client machine, however, does require a sound card, speakers, and the Windows Media or Desktop Experience Feature to be enabled. Audio support is disabled by default on the Webspace sessions.

**Important:**
Be aware that client sound capability requires the loading of Webspace libraries into session processes. This can affect the startup of a process, make some processes incompatible with Webspace, or have fatal consequences during suspend/resume operations. Use caution when enabling this setting.

1. In the Webspace Administration, select the desired server from the list of All Servers.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Client Access tab.
4. Click the Sound check box.
5. Click OK.

## Drive Access

Webspace allows users to access files stored on the client computer, and to save files locally. Client drives will be listed in the application's Open and Save as dialog boxes, and are designated with a Client prefix. For example: Client C (K:), Client D (L:).



The dialog boxes list both client and server drives. In order for clients to open or save files locally, the client drives feature must be enabled on the Webspace Server. Support for client drives is disabled by default.

Webspace allows users to access USB drives. Removable drives such a floppy disks, CD ROMs, and DVD-ROMs are not supported as client drives.

1. In the Webspace Administration, select the desired server from the list of All Servers.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Client Access tab.
4. Select the Drives check box.
5. Click OK.

## Hidden Drives

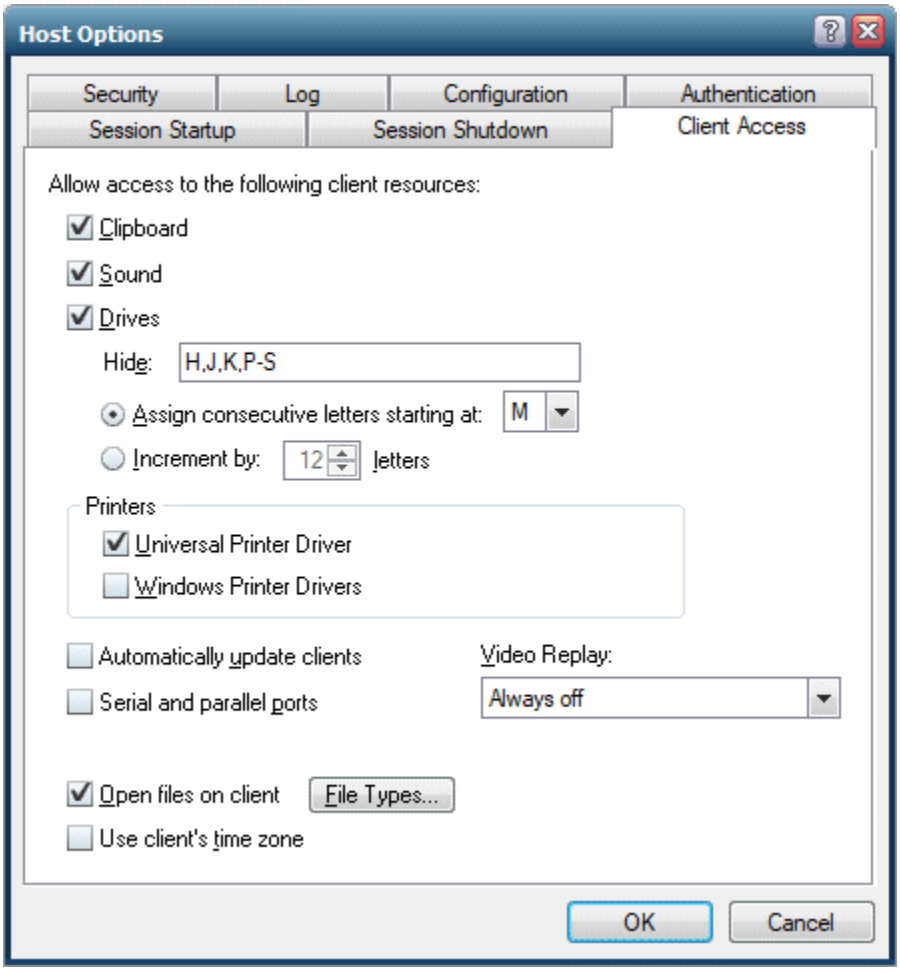
Through the Webspace Admin Console, administrators can hide drives on the client machine where the Webspace session runs, such as the operating system drive, floppy drive, and CD ROM drive. Hidden drives are inaccessible to the user through the Webspace session.

1. From the Webspace Admin Console, on the server list, select the desired server.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Client Access tab.
4. Select the Drives check box.
5. In the Hide field, enter the client drive letters you want to hide.

   **Note:**
   All client drives are mapped by default. Drives listed in the Hide box can be listed in any order. To hide server drives, see Hiding Server Drives *(on page 116)*.

6. Click OK.

   The following figure shows an example of hidden H, J, and K drives, along with drives P through S.




Microsoft's Group Policy Objects lets you hide specific host drives. For instructions, see http://support.microsoft.com/kb/231289. To hide host drives, the Apply Group Policy option must be enabled in the Host Options dialog box in the Webspace Admin Console application.

## File Usage Restrictions

As the system administrator, you may need to restrict user access to certain files and resources from the Webspace sessions. Keep in mind that there are multiple users accessing the server.

Particularly in a Relay Server environment, it is recommended to write-protect your system and application folders so that users are unable to save files on a Webspace Server. Otherwise, the next time a user logs on to Webspace and is routed to a different server, the files and folders will be inaccessible.

You must use Windows Explorer to set the permissions for files on the server, in an individual file-by-file or folder-by-folder basis. By setting file permissions, you can restrict user access to applications,

printers, and folders. File permissions can only be set on drives formatted with the Windows NT file system (NTFS). If you are using the FAT file system *(on page 182)*, you will be unable to set permissions for specific files or restrict access to applications.

Once an application's permissions have been set, you can assign specific parameters for the application with the Webspace Admin Console.

# Client Drive Remapping

With the Client Drives feature enabled, Webspace must ensure there is a one-to-one mapping between drive letters and the drives of the client and server computers. If a drive on the client and a drive on the server are assigned the same drive letter, Webspace must assign a new drive letter to one of the drives. Client drives can be remapped by either listing them sequentially starting at a given drive letter or incrementing their drive letters by a specified value.

## Listing Client Drives Sequentially Starting at a Given Drive Letter

1. From the Webspace Admin Console, on the server list, select the desired server.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Client Access tab.
4. Select the Drives check box.
5. Select the Assign consecutive letters starting at: _ option.
6. In the drop-down list next to the field, select the drive letter that should start the sequence.
7. Click OK.

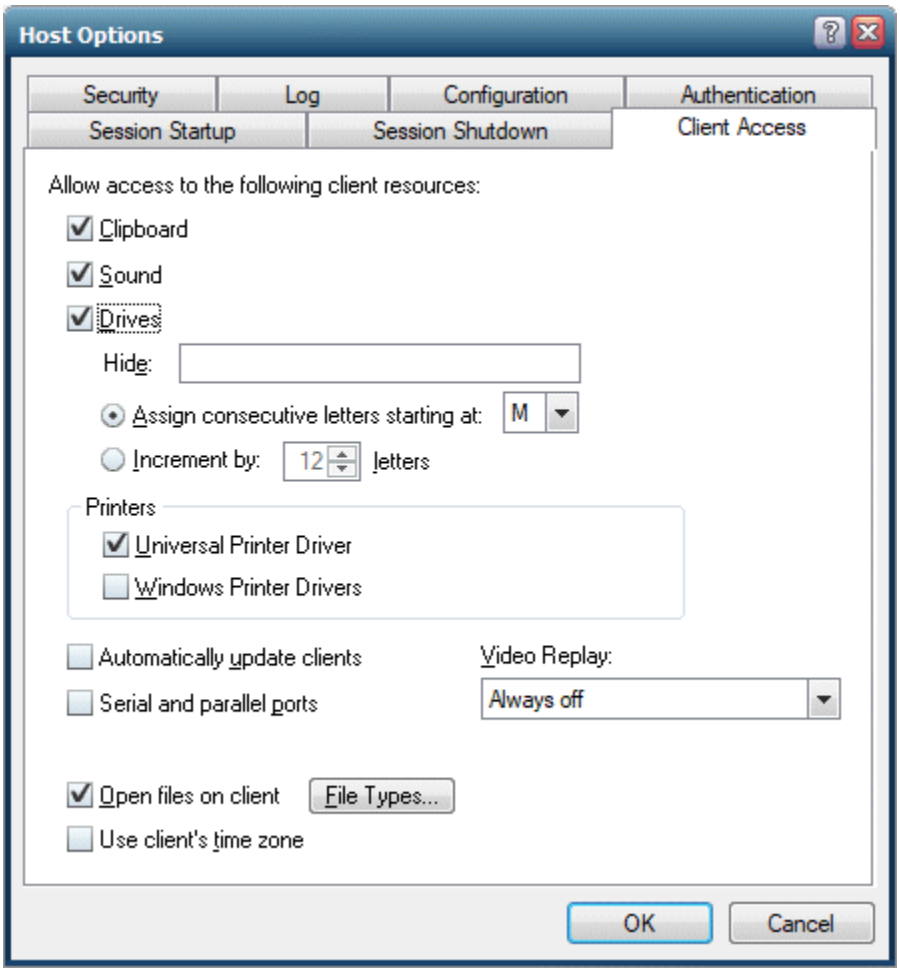
## Incrementing Client Drive Letters by a Fixed Value

1. From the Webspace Admin Console, on the server list, select the desired server.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Client Access tab.
4. Select the Drives check box.
5. Select the Increment by: _ option.
6. In the edit field, type a number greater than or equal to 1 that will yield the desired offset.
7. Click OK.

**Example 1**

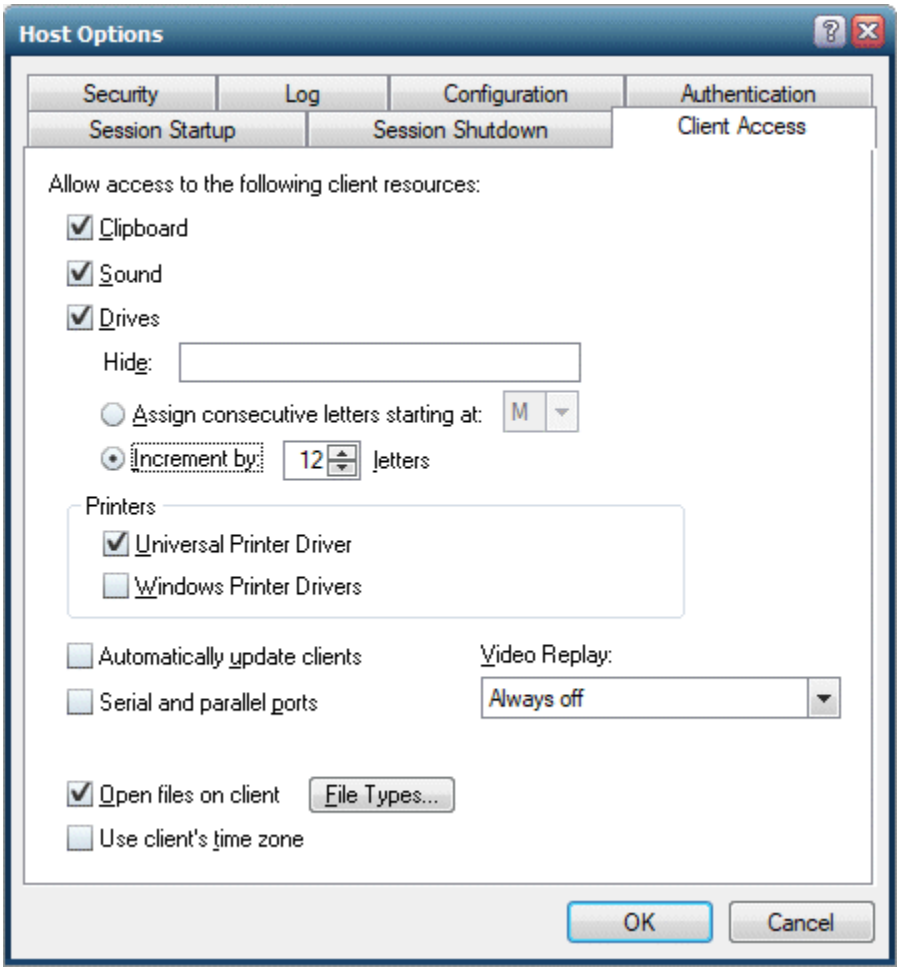
For example, if a client computer has A, C, D, and H drives, and the starting point is set to drive letter M, the client's drives will be remapped respectively to M, N, O, and P. If a drive letter is already

assigned to a drive, the next available letter is used. This feature is disabled by default. Once enabled, the default drive letter is M.




**Example 2**

For this example, if the client computer has the same drives as above (A, C, D, and H), and the offset is 12, each of the client's drives will be incremented by 12 letters. The drives will be remapped respectively to M, O, P, and T. The default value for this setting is 12.




# Port Access

Server-based applications can access modems, handhelds, and other devices that are connected to the serial and parallel ports of the client computer. This feature uses the client file protocol to transfer data between the client device and the Webspace Server. Client port access is enabled when the Serial and Parallel Ports option in the Host Options dialog is enabled. Serial and parallel port access is disabled by default.

**Note:**
Be aware that Client Serial and Parallel Ports requires the loading of Webspace libraries into session processes. This can affect the startup of a process, make some processes incompatible with Webspace, or have fatal consequences during suspend/resume operations. Use caution when enabling this setting.  A message box appears and asks for confirmation when Serial and Parallel Ports is checked.

1. In the Webspace Administration, select the desired server from the list of All Servers.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Client Access tab.
4. Select the Serial and Parallel Ports check box. A message box appears.
5. Click Yes to continue.
6. Click OK to save your settings and close the Host Options dialog box.

## Client Printing

Client printing is disabled by default. Administrators enable client-side printing through the Client Access tab on the Webspace Admin Console's Host Options dialog.

By default, Webspace automatically detects the client's default printer information after the user logs in the Webspace Server. This includes the default printer's port and printer driver. If the printer driver is not installed on the Webspace Server, Webspace will attempt to locate the driver and automatically install it.

Client printers are temporarily installed on the Webspace Server for the duration of the client's session. Printer drivers are installed permanently. Administrators can view the list of printers and drivers in the Printers folder on the Webspace Server.

**Important:**
The Print Spooler Service must be running on the Webspace Server in order to configure client printers.

**Note:**
If a printer is physically connected to the Webspace Server, and you want to allow printing from the web sessions to this printer, no additional configuration changes need to be made on the Webspace Server or Web Session.

**Important:**
If the printer on the Webspace Server is a network printer, and you want to allow printing on the web sessions to this printer, you must add the network printer to the GE Web Server. As the administrator, you can set up network printers for use by Webspace sessions. You must first create a port on the Webspace Server that connects directly to the server and then install the printer locally. This provides direct access to the printer. If you want to allow network printing from the Webspace Server within the web sessions, refer to the Network Printing *(on page 142)* and Setting up a Network Printer *(on page 100)* sections.

## Accessing Printer Drivers

Access a printer drivers using one the following sources:

| Source | Description |
|---|---|
| Universal Printer Driver | Enables the use of the Universal Printer Driver that can print to any client printer. When only the Universal Printer Driver is enabled, only the Universal Printer Driver will be used as a printer driver. No native drivers will be used. This is the default setting. The Universal Printer Driver uses a standard printing properties dialog box and may not offer some of the more advanced printing options other drivers do. The Universal Printer Driver can be used when the native driver is not available. When neither the Universal Printer Driver or Windows Printer Drivers is enabled, no printers will be configured, and client printing is disabled.<br><br>**Note:**<br>A printer named Preview PDF is configured in each session when the Universal Printer Driver is enabled. Documents printed to this printer are automatically converted to a .pdf file and displayed on the client computer. Users can save, print, or email the document at their discretion. A PDF reader, such as Adobe® Reader, is required on the client computer in order to use the Universal Printer Driver's PDF conversion feature. |
| Windows Printer Driver | Enables printers to be configured using already installed native drivers. When only the Windows Printer Drivers option is enabled, only native printer drivers that are installed on the Webspace Server will be used. If a printer's native driver is not installed, that printer will not be configured. To allow Webspace to automatically install native printer drivers that ship with Microsoft Windows click the Automatically install drivers. The Windows Printer Driver option is preferred when configuring proxy printers, if they are available and if settings allow them to be used. Native drivers are selected in the following order: |

| Source | Description |
|---|---|
| | a. **Printers Applet:** A user's manual selection of a printer driver in the Printers window takes precedence over all other driver selection methods. The Printers Applet is accessible via the Program Window which is the first window of the Windows Desktop Client.<br>b. **Mapped Printer Drivers:** MappedPrinterDrivers.xml contains a list of driver names that can be used for each driver. This file is generated by the Application Publishing Service, but can also be manually edited by administrators. For most Webspace deployments, administrators will not need to edit this file. It is used to specify which driver to use when a host's driver name does not identically match the client's, or when the administrator wants to override native drivers and force clients to use a different printer driver or the Universal Printer Driver. The MappedPrinterDrivers.xml file is usually found in the C:\ProgramData\Proficy or C:\Documents and Settings\All Users\Application Data\Proficy folder.<br>c. **Client driver name:** The driver with the exact name of the driver that is installed on the client is used to configure the proxy printer.<br><br>**Important:**<br>If the Windows Printer Drivers option is disabled in the Webspace Admin Console, this hierarchy is not applied.<br><br>When both the Universal Printer Driver and the Windows Printer Drivers are enabled, and a printer's native driver is installed on the Webspace Server, the printer's native driver will be used to configure the printer. If it is not installed on the Webspace Server, the printer is configured to use the Universal Printer Driver. When Windows Printer Drivers and Automatically install drivers are enabled, only native printer drivers that are installed on the Webspace Server or those that are included with Windows will be used. If a printer's native driver is not installed and it is not included with Windows, that printer will not be configured. When neither the Windows Printer Drivers or Universal Printer Driver is enabled, no printers will be configured, and client printing is disabled. |

## Designating Access to Printer Drivers

1. In the Webspace Admin Console, select the desired server from the list of All Servers.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Client Access tab.
4. Select the check box next to the desired printer source: Universal Printer Driver or Windows Printer Driver.

> **Note:**
> The Universal Printer Driver uses a standard printing properties dialog and may not offer some of the more advanced printing options other drivers do.

5. If you select the Windows Printer Driver and you want to allow for automatic installs of native drivers that ship with Windows, also select the Automatically Install Drivers check box.
6. Click OK.

### Disabling Client Printing

1. In the Webspace Admin Console, select the desired server from the list of All Servers.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Client Access tab.
4. Clear the check boxes next to both the Universal Printer Driver and Windows Printer Driver fields.
5. Click OK.

> **Note:**
> Client printers are temporarily installed on the Webspace Server for the duration of the client's session. Printer drivers are installed permanently. Administrators can view the list of printers and drivers in the Printers folder on the Webspace Server. If you start two or more web sessions, at the same time, with different user accounts from the same client system, client printers will only be available to the first session.

## Network Printing

If the printer on the Webspace Server is a network printer, and you want to allow printing from the web sessions to this printer, you must add the network printer to the Webspace Server. First create a port on the Webspace Server that connects directly to the server, and then install the printer locally. For steps, refer to the Setting up a Network Printer *(on page 100)* section.

If a printer is physically connected to the Webspace Server, and you want to allow printing from the web sessions to this printer, no additional configuration changes need to be made.

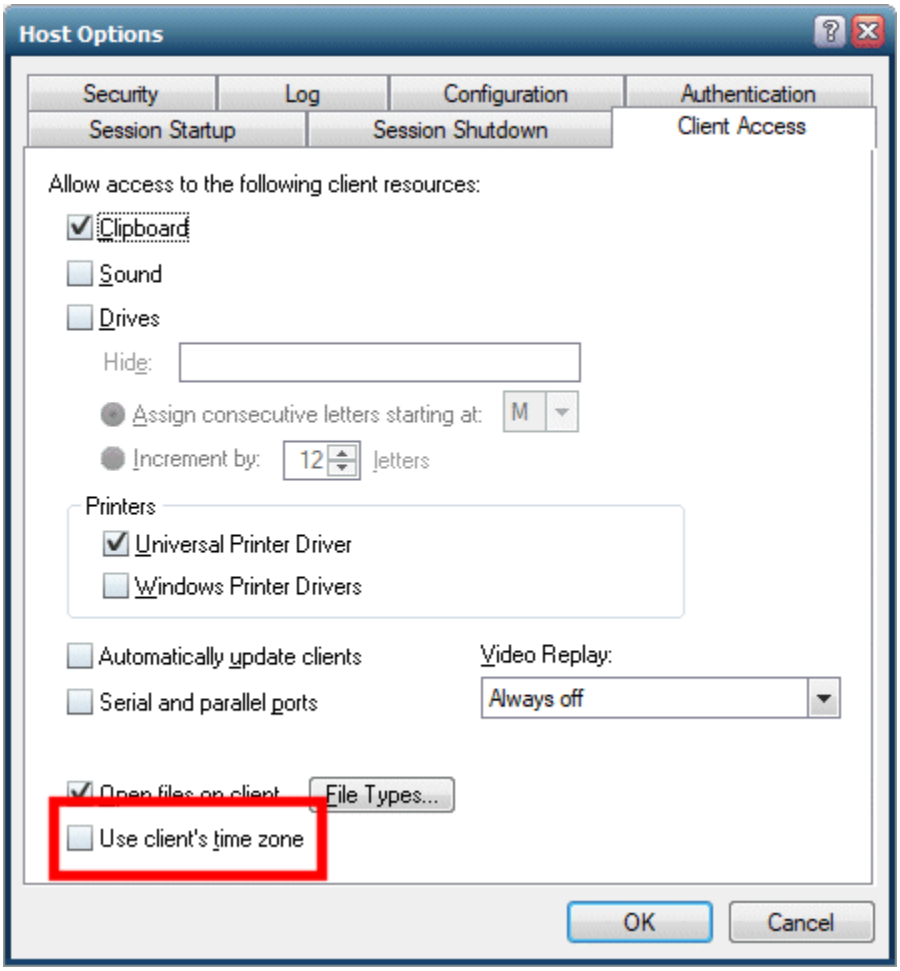
**Note:**
If you want to allow printing in web sessions from client printers, refer to the Client Printing *(on page 139)* section for information on how to configure.

# Client Time Zone Redirection

By default, all Webspace sessions are run in the time zone of the Webspace Server machine. Administrators can opt to run Webspace sessions in the time zone of the client computer by enabling the Use client's time zone option from the Webspace Admin Console. With the Use client's time zone option selected, timestamps and associated data viewed from Webspace sessions appear in the client's time zone instead of the Webspace Server's time zone.

For example, alarms, charts (Standard and Enhanced), Historical Trend Display, Current Date Stamp, Current Time Stamp, and the Historical Datalink will show time stamps and data based on the web client's time zone if the "Use client's time zone" is selected. Otherwise, the time zone of the Webspace Server is reflected in the time stamps and data being displayed.

The Client Time Zone feature is configured from the Webspace Admin Console's Host Options dialog, as shown in the following figure.




**Important:**
Be aware that when you select the Client Time Zone check box that these settings also affect data retrieved by any VisiconX queries in your pictures.

1. From the Webspace Admin Console, from the Server tree, select the server name you want to configure.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Client Access tab.
4. Select the "Use client's time zone" check box.
5. Click OK.

# Chapter 6. Deploying and Running Sessions

## Deploying and Running Webspace Sessions

Webspace allows you to open iFIX or CIMPLICITY pictures in run mode from a web session. Users can connect to a Webspace Server from any computer that supports a Webspace session. The following clients are currently supported:

- Microsoft® Windows® Internet Explorer 11 (32-bit)
- Mozilla® Firefox® 52 and later (standard and ESR, 32-bit and 64-bit)
- Apple Safari 9 or later on Mac OS X
- Google Chrome with Windows 7, Windows 8.1, Windows 10, and Chromebook
- Microsoft Edge
- Windows Desktop Client

### Running the Browser Client

Start your browser. In the URL box, type http:// followed by the Webspace Server computer name (or IP address) and then /ProficyWebspace. For example:

```
http://WebspaceServerName/ProficyWebspace
```

### Running the Browser Client in a Relay Server Configuration

To start the Webspace add-on in a high availability setup, use the following examples with the host and reconnect parameters. For iFIX:

```
http://RS_Server1/ProficyWebspace/iFIX.html?&host=RS_Server1;RS_Server2&autoreconnect=5
```

For CIMPLICITY:

```
http://RS_Server1/ProficyWebspace/CIMPLICITYScreenName.html?&host=RS_Server1;RS_Server2&autoreconnect=5
```

where RS_Server1 is the name of the primary Relay server, and RS_Server2 is the name of the backup Relay server. Select the appropriate product from the list. When the Logon dialog appears, type the following information: Your network user name in the User name field. Your network password in the Password field. Users are allowed three invalid logon attempts before the logon process shuts down.

### Tips for Specifying Relay Server Names

- Specify the addresses of the primary and failover relay servers using either their IP addresses (if SSL is not used) or their fully-qualified domain names (FQDNs). When using the IP addresses, if SSL is used, the common names of the SSL certificates on the primary and failover relay servers must match the fully-qualified domain names of the computers.
- When dependent hosts and/or client computers reside in a different domain (or domains) than the relay servers, it is generally advisable to reference the relay servers via their FQDNs. Otherwise, dependent hosts and client computers may be unable to resolve the addresses of the relay servers.

### Running the Windows Desktop Client

The Windows Desktop Client allows you to view WorkSpace pictures from a desktop application using web services. It does not require a web browser. Optionally, you can customize the command-line settings you use to open the Windows Desktop Client.

To run the Windows Desktop Client, you must have the full Webspace Client installed.

The Webspace Windows Desktop Client can be run by selecting the option on the Start menu, or by running a custom short-cut. When using the Webspace Windows Desktop Client, a custom short-cut configuration is required.

If launched without configuring the shortcut configured, you may encounter the following error: "Webspace failed to launch the Program window for your session. The problem is explained in your system administrator's log file."

1. On the Start menu, point to Programs > Webspace Client > Webspace Client, or double-click the shortcut you created on the desktop.  You may be required to enter the Host Address. The Desktop Client appears.
2. When the Logon dialog appears, type your network user name in the User name field, and your network password in the Password field. Users are allowed three invalid logon attempts before the logon process shuts down.

## Installing the Full Client

You can install the desktop client with the installer provided on the Webspace Server computer in the folder where you publish the Webspace files to be hosted by your IIS or Apache server, or from the Webspace install folder, which is the C:\Program Files\Proficy\Proficy Webspace\Web\Clients folder by default.

1. Obtain the client installer from the Webspace Server computer in the directory where you publish the Webspace files to be hosted by your IIS or Apache server, the DVD in the WebspaceServer subfolder, the Webspace install folder, which is by default the C:\Program Files\Proficy\Proficy Webspace\Web\Clients folder.
2. Copy this file to the client computer.
3. Double-click the .exe file to start the install. For non-administrators, double-click the proficy-client.exe file to install. For administrators, double-click the proficy-client.windows.exe file.
   The proficy-client.exe is installed under the user's User Profile and can only be run by the user who installed it. The proficy-client.windows.exe is installed under the Program Files (x86) directory and can be run by all users on the computer. Only the proficy-client.windows.exe install supports the automatic client update; this is because administrator rights are required to install the update service.
4. Click OK. The Welcome screen appears.
5. Click Next to continue. The License Agreement screen appears.
6. Select the "I accept the terms in the license agreement" and click Next to continue. The Destination Folder screen appears.
7. Leave the default and click Next to continue. The Setup Type screen appears.
8. Select Complete (which includes the Desktop Client, as well as the Internet Explorer, and Firefox plug-in), or Custom (to choose only the Desktop Client), and then click Next. The Ready to Install screen appears.
9. Click Install. After a few moments, the Completion screen appears.
10. Click Finish.
11. Confirm that the Desktop Client short-cut appears on the Start menu (on the Start menu, point to Programs > Webspace Client > Webspace Client).

# Creating Shortcuts

## Using a Custom Hyperlink Command to Open a Web Page

1. Open a web page in an editor.
2. Choose the editor's Insert Hyperlink option.
3. Enter the address of the host, followed by the desired hyperlink parameters. Refer to the Summary of Command-line Options *(on page 149)* for a full list of available options. For example, to pass user in command line, enter:

   ```
   http://WebspaceServerName/ProficyWebspace/iFIX.html?user=user_name
   ```

4. Save the page.

## Modifying the Default Settings on the Start Menu Option

These steps describe how to modify the default settings on the Start menu for the Windows Desktop Client. Be aware that the install path for Webspace changed in version 6.0. If you have any shortcuts configured, you will need to update them to use the correct path. For instance, the previous version of the Webspace Client installed to the C:\Program Files (x86)\Proficy\Proficy Webspace Client\Client\ folder. In Webspace 6.2, the path for the client is C:\Program Files (x86)\Proficy\Proficy Webspace\Client folder.

1. On the Start menu, point to Programs > Proficy Webspace > Proficy Webspace.
2. Right-click the Webspace Client and select Properties. The Webspace Client Properties dialog box appears.
3. On the Shortcut tab, in the Target field, add parameters you want to include after the path to Proficy.exe. Refer to the Summary of Command-line Options *(on page 149)* for a full list of available options. For example, this option will open the Windows Desktop Client with a server named MyServer, and includes command-line options for each program.
   For iFIX:

   ```
   "C:\Program Files (x86)\Proficy\Proficy Webspace\Client\Proficy.exe" -h MyServer -c -a iFIX -r
    IFIX /puserscreen.grf
   ```

   For a specific picture, specify -r IFIX /ppicname.grf. Be aware that iFIX 5.5 and higher versions do not support the **/p**picname.grf parameter in the command line.
   For CIMPLICITY:

   ```
   "C:\Program Files (x86)\Proficy\Proficy Webspace\Client\Proficy.exe" -h MyServer -c -a CimView -r CIMVIEW
    "c:\screens\userscreen.cim"
   ```

4. Click OK to save your changes.

## Creating a Desktop Shortcut for Windows Desktop Client

Be aware that the install path for Webspace changed in version 6.0. If you have any shortcuts configured, you will need to update them to use the correct path. For instance, the previous version of the Webspace Client installed to the C:\Program Files (x86)\Proficy\Proficy Webspace Client\Client\ folder. In Webspace 6.2, the path for the client is C:\Program Files (x86)\Proficy\Proficy Webspace\Client folder.

1. Right-click on the desktop, and select New and then Shortcut. The Create Shortcut dialog box appears.
2. In the Create Shortcut dialog box, browse to the Webspace executable file: "C:\Program Files (x86)\Proficy\Proficy Webspace\Client\Proficy.exe"
3. Add parameters after the path to Proficy.exe. Refer to the Summary of Command-line Options *(on page 151)* for a full list of available options. For example, this option will open the Windows

Desktop Client with a server named MyServer, and includes command-line options for each program.

For iFIX:

```
"C:\Program Files (x86)\Proficy\Proficy Webspace\Client\Proficy.exe" -h MyServer -c -a iFIX -r
 IFIX /puserscreen.grf
```

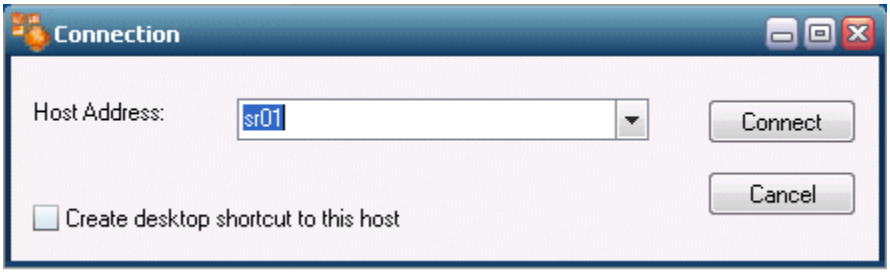
For a specific picture, specify -r IFIX /ppicname.grf. Be aware that iFIX 5.5 and higher versions do not support the **/p**picname.grf parameter in the command line.

For CIMPLICITY:

```
"C:\Program Files (x86)\Proficy\Proficy Webspace\Client\Proficy.exe" -h MyServer -c -a CimView -r CIMVIEW
 "c:\screens\userscreen.cim"
```

4. Type a name for the shortcut and click Finish.

> **Tip:**
> You can also create a Desktop shortcut automatically from the Connection dialog box. When you click on the Start menu, and point to Programs > Webspace Client > Webspace Client, a dialog box appears similar to the following figure. You can select the Create Desktop Shortcut to this Host option, as shown in the following dialog box.




## Command-line Options for Web Browser Clients

Optionally, you can use command-line settings to override the defaults of your Webspace session on open. Use command-line settings to override the defaults of your Webspace session on open. You can do this by either:

- Directly entering the commands following the web address when you type it into the browser, or from the hyperlink command you refer to on a custom web page. For example, the address plus command-options could read like this for iFIX: http://WebspaceServerName/ProficyWebspace/iFIX.html?user=user_name&password=actual_password. Or for CIMPLICITY, specify the command-line parameters in the .HTML file.  For details, refer to the CIMPLICITY HTML File Overview section.

- Changing the default settings for every user, by editing the Logon call in the index.html and index.htm files on the Webspace Server in the directory where you publish the Webspace files to be hosted by your IIS or Apache server. For example, you would modify the window.location.href = "iFIX.html?embed=true"; line in the index.html and index.htm files with the settings you want to change. For instance, you might want to change that line to allow for loose mode, instead of embedded mode: window.location.href = "iFIX.html?embed=false&useApp=true".

Be aware of the following when working with command-line options:

- Command-line passing of variables to CIMPLICITY is supported through the .HTML file. For details, refer to the CIMPLICITY HTML File Overview section.
- Parameters are optional and case-sensitive. They can be appended in any order.
- Command-line options that are also configurable in the Administration tool, override the default settings in the Webspace Admin Console.
- Before the first command-line option, and after the .html reference, add a ? symbol. For example: iFIX.html?user=user_name.
- After the first command, each additional command that you add should be appended with the & symbol before the additional command. For example: user=user_name&password=actual_password.
- Spaces within parameters must be replaced with the %20 symbol.

## Summary of Command-line Options for Web Browsers

Use the following table to review the available command-line options for Webspace startup in browsers.

| Option | Description |
|---|---|
| user=user_-name | The name of the user's account. |
| pass-word=ac-tual_pass-word | The user's password. |
| port=port_-number | The port on which the Webspace Server accepts connections. By default, this port number is 491. |
| auto-close=true\|false | Not supported in Webspace 6.2. |

| Option | Description |
|---|---|
| useApp=true\|false | By default, Webspace runs the zero-install client. You can change it so that Webspace automatically downloads (if it is not already installed) and runs the full app instead. Appending ?useApp=true to the logon URL will download the full Webspace app and run the full app. |
| installApp=true\|false | The installApp command works together with useApp.<br>When installApp=true, the user will be prompted to install the full Webspace app, if it is not already installed. If installApp=false, the user will not be prompted to install the full Webspace app and no link to install will be displayed.<br>Examples:<br>• When useApp=true&installApp=true the user will be prompted to install the single user app, and after installing, the session will open in the app (session will start in app but embedded in browser itself, as embed is true by default).<br>• When useApp=true&installApp=false the user will not be prompted to install app, but if app is already installed the session will start in the app.<br>• When useApp=true&embed=false the session opens in the app outside of browser. |
| embed=true\|false | This setting describes whether your web session runs in Loose mode or Embedded mode. When embed=true, Webspace sessions run within the browser window (in Embedded mode). When embed=false, applications run outside the browser window (in Loose mode). By default, embed=true.<br>**Note:**<br>With Webspace 6.2, embed=false (loose mode) works only when used with useApp=true. |
| bInBrowser=true\|false | Not supported in Webspace 6.2. |
| autoreconnect=i | Determines how many times the client will automatically attempt to reconnect after a broken connection. When autoreconnect=i in a URL, the client will automatically attempt to reconnect i number of times. 5 by default. |

## Command-line Options for the Windows Desktop Client

Use the following table to review the available command-line options for the Webspace startup in the Windows Desktop Client (Proficy.exe). Parameters are optional and case-sensitive. Parameters can be appended in any order with the exception of the -r option.  When the -r parameter is used, it must be the last parameter on the command-line, and it must be used with the -a parameter.

Optionally, you can use command-line settings to override the defaults of your Windows Desktop Client session on open. To add a command-line use, change the Properties on the shortcut you use on the Start menu to open the Windows Desktop Client, or create a new shortcut with the command-line options that you want to use.

Command-line options that are also configurable in the Administration tool, such as -hp and -ac, override the default settings in the Webspace Admin Console. Command-line options can only be appended to desktop shortcuts that call the "C:\Program Files\Proficy\Proficy Webspace\Client\Proficy.exe" file. In order to accommodate spaces in user names and passwords, quotation marks must be included when using command-line arguments.

### Summary of Command-line Options for the Windows Desktop Client

Use the following table to review the available command-line options for Webspace Desktop Client startup.

| Option | Description |
|---|---|
| -u user_-name | The name of the user's account. |
| -p actual_-password | The user's password. |
| -hp port_-number | The port on which the Webspace Server accepts connections. By default, this port number is 491. |
| -h host_-name | The name or IP address of your Webspace Server machine. |
| -c or -nc | -c enables compression. (Compression is enabled by default.)  -nc disables compression. |
| -f (0 \| 1) | This setting describes whether each session will be displayed in a bounding window. When you use -f followed by a 1, all applications running in the session will be displayed within a bounding window. When you follow the -f respectively with a 0, applications will be displayed within their own individual windows. |
| -geometry | The width and height of the client window. |

| Option | Description |
|---|---|
| | The command-line argument –geometry can be used to modify the size of the client window when the command-line argument –f is used. Without -geometry on the command-line, the client window will be maximized. When Webspace is run in loose window mode, -geometry has no effect. To resize the client window, append –geometry to the Webspace Client executable, followed by the desired width and height. For example, on Windows: “C:\Program Files\GraphOn\GO-Global\Client\gg-client.exe” -f –geometry=800x600 |
| -a app_-name | The application you want to open:<br>• iFIX<br>• CimView<br>• CimLayout<br>**Note:**<br>When using the -a option with CimView, the –r option must also be supplied. |
| - r app_-name parameters | The application you want to open, with the specified parameters. Examples with additional parameters include:<br>• iFIX /puserscreen.grf<br>• CimView "c:\screens\userscreen.cim"<br>• CimLayout “c:\CIMPLICITY_webfiles\layoutfile.cimlayout”<br>**Note:**<br>The -a option must be supplied before the -r option. The -r option does not replace the -a option. The -r option simply allows you to supply additional parameters for your application. |
| -autore-connect i | Determines how many times the client will automatically attempt to reconnect after a broken connection. When -autoreconnect is followed by i, the client will automatically attempt to reconnect i number of times. 5 by default. |
| -ac | Determines how printers are initialized at startup. When printerconfig ="all" or -ac is followed by all, all printers are automatically configured. When printerconfig = "none" or -ac is followed by none, printers are not automatically configured. When printerconfig = "default" or -ac is followed by default, the default printer is configured automatically. This is the default setting. |

| Option | Description |
|---|---|
| -clientscale | When followed by the percent scale factor, causes the Webspace app to scale the applications running in the session relative to applications running locally on the client computer. For example, adding -clientscale 200 to the command-line will cause applications running in the Webspace session to appear twice as large as applications running locally on the client computer. |
| -clientdpi | -clientdpi 1 enables the the Webspace app's DPI scaling feature. -clientdpi 0 disables the feature. When this option is specified, it overrides the value of the ClientDPIScalingEnabled property in the HostProperties.xml file on the host.<br><br>**Note:**<br>If you set this value to zero by entering -clientdpi 0, then the -clientscale command line will not be applicable. |

# Automatically Update the Desktop Client Version

Administrators can configure the Webspace Server to automatically update the Webspace Desktop Client when a user connects to a Webspace Server that is running a newer version. When enabled, when a user tries to connect and an upgrade is available, the following message appears:

"An update has been downloaded and will be available the next time you run Webspace."

**Note:**
The Automatically Update Clients option on the Client Access tab of the Webspace Admin Console is only available for the Windows Desktop Client. It does not apply to other clients such as Mozilla Firefox and Internet Explorer.

1. From the Webspace Administration, from the Server tree, select the server name you want to configure.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Client Access tab.
4. Select the "Automatically Update Clients" check box.
5. Click OK.

# CIMPLICITY HTML Files

CIMPLICITY .html files are created for Webspace based on entries that are made in the Create Web Page dialog box on the CIMPLICITY Server. You also can manually modify the values in created .html files. This section provides examples of these HTML files.

**Note:**
On the CIMPLICITY Server, to publish a web page for a CIMPLICITY CimView screen, right-click the CIMPLICITY Options and select Run as Administrator. On the Proficy Webspace tab, click the "Create a Web Page" button. The next dialog box allows you to select the screen that you want and creates a web page for it; if it does not detect the default Webspace directory to place the html file in, you will need to enter it. If it's an Apache server, you will need to browse to the location of the Apache Server; by default, the Apache Server location is: "C:\Program Files (x86)\Apache Software Foundation\Apache2.2\htdocs\ProficyWebspace."

**Important:**
The parameters listed in the HTML file are pulled from a DynamicGlobalViewApplication.js file. Do not edit the DynamicGlobalViewApplication.js file.

## Example HTML File for CimLayout

```
<!DOCTYPE HTML>

<html style="height:99%">

<head>


<TITLE>Proficy HMI/SCADA CIMPLICITY</TITLE>

<meta content="text/html;charset=utf-8" http-equiv="Content-Type"/>

<meta content="utf-8" http-equiv="encoding"/>

<meta http-equiv="X-UA-Compatible" content="IE=edge" />

<link rel=stylesheet type="text/css" href="style.css">

<SCRIPT LANGUAGE="JavaScript1.1" SRC="./version.js"></SCRIPT>

<SCRIPT LANGUAGE="JavaScript1.1" SRC="logon_PluginFunctions.js"></SCRIPT>

<SCRIPT LANGUAGE="JavaScript1.1" SRC="DynamicCIMPLICITYApplication.js"></SCRIPT>

<script src='./util.js'></script>

<script src='./handler.js'></script>


</head>

<body id="mainbody">

  <div id="mySidenav" class="sidenav" style="display:none">
```

```
   <div id="mySidenavContainer" class="sidenavcontainer">
    <div id="helpContainer" help-include-html="help/quickstart.html"></div>
   </div>
  </div>

  <div id="main">
   <div id="barFrame" style="display:none">
    <span id="notificationFrame"><a href="#" class="bright" id="getApp"></a></span>
    <div class="title"><img src="logo_white.png" height="25"></div>
   </div>
   <div id="msgFrame"></div>

   <div id="installApp" class="modal">
    <div class="modal-content">
     <div id="dialogFrame" class="dialog"></div>
    </div>
   </div>

   <div id="copyClipboardModal" class="copy-modal">
    <div class="copy-modal-content">
     <span class="close" onClick="closeCopyClipboardDialog()">&times;</span>
     <p>Click Copy to copy this link to the clipboard. You can then paste it into an email or instant message and share
 it with users.</p>
     <textarea id="copy_text" rows="2" style="width:90%" onClick="this.select();"></textarea><br/>
     <button id="copy" data-copytarget="#copy_text" onClick="copyToClipboard(this)">Copy</button>
    </div>
   </div>

   <iframe class="iframecontainer" id="iFrameLogon" width="800px" height="600px" border-style="hidden"></iframe>
  </div>
  <div id="params" name="$CIMVIEWFILEANDPARAMETERS" style="display:none"/>
</body>

<SCRIPT LANGUAGE=javascript >
 loadCIMPLICITYApplication('', '', '', 'Cimlayout', 'Cimlayout ' +
 document.getElementById('params').getAttribute('name'),
   'true', '$COMPRESSIONPARAM', '', '$AUTOCLOSEBROWSERPARAM', 'true', '$AUTOCONFIGPRINTERSPARAM');
```

```
</SCRIPT>


</html>
```

## Example HTML File for a CimView Screen

```
<!DOCTYPE HTML>
<html style="height:99%">
<head>


<TITLE>Proficy HMI/SCADA CIMPLICITY</TITLE>
<meta content="text/html;charset=utf-8" http-equiv="Content-Type"/>
<meta content="utf-8" http-equiv="encoding"/>
<meta http-equiv="X-UA-Compatible" content="IE=edge" />
<link rel=stylesheet type="text/css" href="style.css">
<SCRIPT LANGUAGE="JavaScript1.1" SRC="./version.js"></SCRIPT>
<SCRIPT LANGUAGE="JavaScript1.1" SRC="logon_PluginFunctions.js"></SCRIPT>
<SCRIPT LANGUAGE="JavaScript1.1" SRC="DynamicCIMPLICITYApplication.js"></SCRIPT>
<script src='./util.js'></script>
<script src='./handler.js'></script>


</head>
<body id="mainbody">
  <div id="mySidenav" class="sidenav" style="display:none">
   <div id="mySidenavContainer" class="sidenavcontainer">
    <div id="helpContainer" help-include-html="help/quickstart.html"></div>
   </div>
  </div>


  <div id="main">
   <div id="barFrame" style="display:none">
    <span id="notificationFrame"><a href="#" class="bright" id="getApp"></a></span>
    <div class="title"><img src="logo_white.png" height="25"></div>
   </div>
   <div id="msgFrame"></div>


   <div id="installApp" class="modal">
    <div class="modal-content">
```

```
     <div id="dialogFrame" class="dialog"></div>
    </div>
   </div>

   <div id="copyClipboardModal" class="copy-modal">
    <div class="copy-modal-content">
     <span class="close" onClick="closeCopyClipboardDialog()">&times;</span>
     <p>Click Copy to copy this link to the clipboard. You can then paste it into an email or instant message and share
 it with users.</p>
     <textarea id="copy_text" rows="2" style="width:90%" onClick="this.select();"></textarea><br/>
     <button id="copy" data-copytarget="#copy_text" onClick="copyToClipboard(this)">Copy</button>
    </div>
   </div>

   <iframe class="iframecontainer" id="iFrameLogon" width="800px" height="600px" border-style="hidden"></iframe>
  </div>
  <div id="params" name="$CIMVIEWFILEANDPARAMETERS" style="display:none"/>
</body>

<SCRIPT LANGUAGE=javascript >
 loadCIMPLICITYApplication('', '', '', 'CimView', 'CimView /noexit ' +
 document.getElementById('params').getAttribute('name'),
   'true', '$COMPRESSIONPARAM', '', '$AUTOCLOSEBROWSERPARAM', 'true', '$AUTOCONFIGPRINTERSPARAM');
</SCRIPT>

</html>
```

# Chapter 7. Advanced Topics

## Advanced Topics

The following sections provide information on advanced topics that may be not be referenced frequently:



## Load Balancing and High Availability

### Load Balancing

Load balancing is a technique used by the Relay Server to spread the work for the Webspace Server across two or more Dependent Servers. A Relay Server provides centralized control over one or more Dependent Servers. Relay Servers maintain client connections and distribute Webspace sessions across a set of load balanced Dependent Servers.

Load balancing:

- Allows Webspace sessions to be distributed across multiple dependent application servers.
- Is needed when the server resource requirements for a deployment exceed the capacity of a single server computer.
- Is done automatically and is transparent to the user.

The goals of load balancing include:

- Optimal resource utilization.
- Maximized throughput.
- Minimized response time.

## Supported Architectures

| Scenario | Webspace Server Type and Count | License Type and Count |
|---|---|---|
| 1 | Single Webspace Server | One (1) Single Webspace Server |
| 2 | Load Balanced Application. Requires two (2) Dependent Servers and one (1) Relay Server | • Two (2) Dependent Servers each with full Client Count<br>• One (1) Relay Server |
| 3 | Load Balanced + High Availability. Requires two (2) Dependent Servers and two (2) Relay Servers | • Two (2) Dependent Servers each with full Client Count<br>• Two (2) Relay Servers, one designated as Backup License |

## Load Balancing Requirements

- The Webspace Server must be installed on each of the servers in the configuration (on the Relay Server and each Dependent Server), along with IIS or Apache HTTP Server.
- Applications (iFIX or CIMPLICITY) are installed on Dependent Servers.
- Webspace Clients cannot connect directly to Dependent Servers – only Relay Servers.
- Each Dependent Server should be configured the same, with the same installed software, settings, and install locations. In other words, all software, pictures, and network access must be the same on each dependent application server in your configuration.

**Important:**
The command-line parameters on the Relay Server must always match the command-line parameters on the Dependent Servers. If using a stand-alone Webspace Relay Server (no iFIX or CIMPLICITY installed on the server), the command-line parameters need to be modified in the Webspace Admin Console tool to include the full path of the iFIX or CIMPLICITY product. For example, for iFIX, in the Webspace Admin Console, you would change the command-line from iFIX /s"WEB.SCU" to iFIX /s"C:\Programs Files (x86)\Proficy\Proficy iFIX\LOCAL \WEB.SCU" (where the path for the WEB.SCU points to where iFIX is installed on all dependent Webspace Servers - it should be the same location on all Dependent Servers).

- Dependent Servers do not need to be located on the same network as their associated Relay Server.
- When using a Relay Server, the Web Server must reside on the same network as the Relay Server.

- Users are authenticated on Dependent Servers.
- iFIX View nodes cannot connect directly to Dependent Servers.

### Server Selection

When a client connects to a Relay Server, the Relay Server attempts to start a session on the Dependent Server (host) that has the lowest number of running sessions as a percentage of the maximum number of sessions allowed for the server.

If the session fails to start on the selected server, the Relay Server successively attempts to start the session on other available servers until it finds one that can support the session.

If there are no available servers (for instance, if the number of running sessions on All Hosts equals the maximum number allowed), the following message is displayed to the user: You are already running as many sessions as you are allowed.

Otherwise, if the session cannot be started on any of the available dependent application servers, the following message is displayed to the user: Webspace failed to launch the Program Window for your session. The problem is explained in your System Administrator's log file.

In a Relay Server configuration, Webspace checks the maximum sessions settings on the Relay Server and its Dependent Servers. The maximum sessions value on the Relay Server is the maximum number of sessions that can be run concurrently on all Dependent Servers assigned to that Relay Server. To modify the Maximum sessions on this server setting, open the Webspace Administrator on the Dependent Application Server, and on the Host Options dialog box, select the Session Startup tab.

### Load Balancing and High Availability

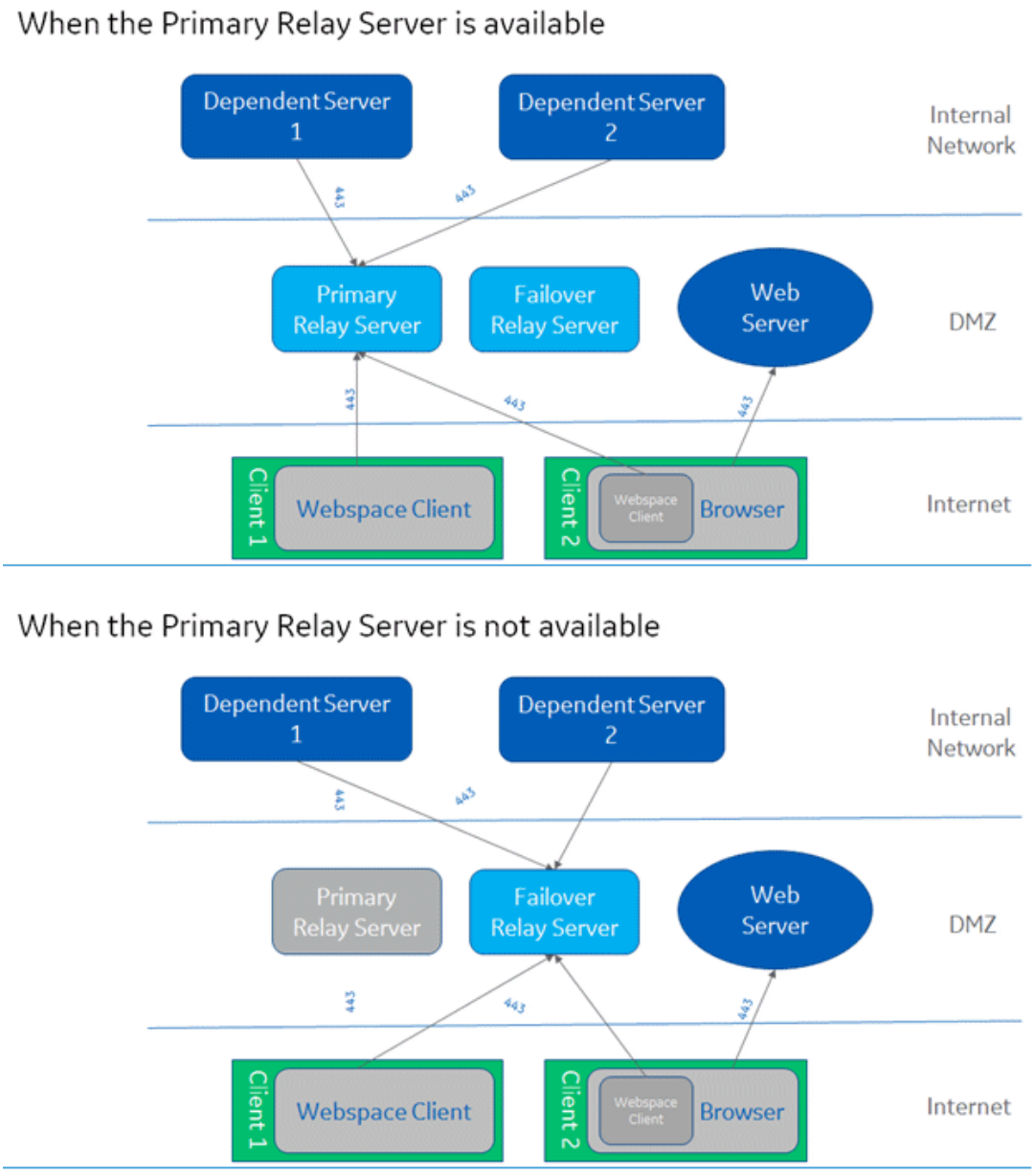
Adding High Availability to a Load Balanced solution means adding a second Relay Server designated as the Failover Relay Server. A Failover Relay Server can be configured using the Webspace Admin Console. Relay Servers know about each other, and all Clients and Dependent Servers know about each Relay Server. If a client fails to reach the Relay Server, it will attempt to reach the Failover Relay Server.

**Note:**
Connections from the Failover Relay Server will be slower than those from the Primary.

**Important:**
When the Primary system is completely shut down, a new client connection CANNOT be made.

Requirements:

- Two (2) Dependent Servers each with full Client Count.
- Two (2) Relay Servers, one designated as Backup License.
- The clients can't connect directly to the Dependent Servers, so Dependent Servers do not need a web server running on them.
- The Relay Server and the Failover Relay Server are configured to accept connections on port 443 because many corporate firewalls and proxy servers do not allow connections to Webspace's default port, 491. Webspace's clients support proxy tunneling, which allows them to tunnel Webspace's protocol over port 443.
- Since browsers also use port 443 to securely download the Webspace web pages over HTTPS, the web server must be on a different computer than the Relay Servers.




## Relay Server Configuration

A Relay Server is a Webspace server that provides centralized control over one or more Webspace servers. Relay Servers maintain client connections and distribute Webspace sessions across a set of load-balanced servers. Relay Servers appear in the Webspace Admin Console on the first level of the list of All Hosts as nodes with one or more Dependent Servers.

After configuring a server to run as a Relay Server with one or more Dependent Servers, Webspace load-balances client connections and ensures that sessions start successfully. If a session fails to start on the

selected server, the Relay Server selects another server and tries again until it finds one that can support the session.

When using a Webspace Relay Server in a standalone configuration (for Load Balancing Only), you must modify the command line (for iFIX) using the Webspace Admin Console. This modification is necessary because when the Relay Server is standalone, it cannot determine the default SCU path necessary to get the Webspace client to start correctly. You can also use the Relay Server in a high availability setup as well.

**Important:**
For the Relay Server to work with Strong Encryption, install the Relay Server Root certificate on Webspace Dependent Server and all clients. The Failover Relay Server with Strong Encryption is not supported.

### To configure a Webspace Server to operate as a Relay Server:

1. From the Webspace Admin Console, select the server from the list of All Hosts.
2. On the Tools menu, click Host Options.
3. Click the Configuration tab.
4. Select the Relay Load Balancer option.
5. Click OK. A message box appears indicating that the change will not take effect until the Proficy Webspace Application Publishing Service has been restarted.
6. Click OK.
7. From the Control Panel, stop and restart the Proficy Application Publishing Service from the Services option.

### To configure a Dependent Host:

1. From the Webspace Admin Console, select the server from the list of All Hosts.
2. On the Tools menu, click Host Options.
3. Click the Configuration tab.
4. Select the Application Host option.
5. Under Application Host, select the Dependent Host option.
6. In the Relay Load Balancer Address field, enter the name or IP address of the Relay Server. The fully qualified name or IP address of the Relay Servers must be provided on Dependent Server, otherwise an error dialog appears, and you will not be able to set the Relay Servers.
7. Click OK. A message box appears indicating that the change will not take effect until the Proficy Webspace Application Publishing Service has been restarted.

8. Click OK.
9. From the Control Panel, stop and restart the Proficy Application Publishing Service from the Services option. When the Proficy Application Publishing Service is restarted, the Dependent Server will appear beneath the Relay Server in the Webspace Admin Console's list of Proficy Webspace servers.

**Note:**
Before publishing an item on a mapped drive, verify that the drive is mapped to the same drive letter and location on the Dependent Servers as it is on the Relay Server. It is recommended that you install the same set of applications on each Dependent Server, using the same installation path.

### To start the Webspace client in a standalone configuration:

1. From the Webspace Admin Console main window, click the Applications tab.
2. From the list of applications that appear, select iFIX.
3. Click Properties. The Application Properties dialog box appears.
4. In the Command Line Options box, change the startup parameter.

**Note:**
This path should be the same path as the path that was configured on the Dependent Servers. For example, from iFIX, /s"C:\Program Files (x86)\Proficy\Proficy iFIX\LOCAL\WEB.SCU" shows the defaults that were chosen while installing a 64-bit operating system. Thus, when Dependent Servers are added, their Command Line Options change to iFIX /s"C:\Program Files (x86)\Proficy \Proficy iFIX\LOCAL\WEB.SCU" (passed from Relay Server).

**Note:**
If you do not change the Relay Server's Command Line Options from the default of iFIX /s"WEB.SCU", when Dependent Servers are added, their Command Line Options would change to iFIX /s"WEB.SCU" and the Webspace client will not start correctly.

**Important:**
In a standalone Relay Server configuration, the command line parameters for iFIX must always match the command line on the Dependent Servers for the Relay Server to use the correct SCU path.

### High Availability Configuration

Configuring high availability requires configuration on both the Relay Server and Dependent Server.

### To set up high availability on each Relay Server:

1. From the Webspace Admin Console, select the server from the list of All Hosts.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Session Shutdown tab.
4. In the Disconnected sessions terminate section, select the After option, and make sure the session shutdown has the disconnect set for longer than 10 minutes. This will allow sessions to connect back if there is a failover. An immediate disconnect will take away the session if a failover situation occurs.
5. Click the Configuration tab.
6. Select Application Host Manager.
7. Click Relay Load Balancer.
8. Click OK. A message box appears indicating that the change will not take effect until the Proficy Webspace Application Publishing Service has been restarted.
9. From the Control Panel, stop and restart the Proficy Application Publishing Service from the Services option. When the Proficy Application Publishing Service is restarted, the Dependent Server will appear beneath the Relay Server in the Webspace Admin Console's list of Proficy Webspace servers.

### To configure Dependent Hosts to support high availability Relay Servers:

1. From the Webspace Admin Console, select the server from the list of All Hosts.
2. On the Tools menu, click Host Options. The Host Options dialog box appears.
3. Click the Session Shutdown tab.
4. In the Disconnected sessions terminate section, select the After option, and make sure the session shutdown has the disconnect set for longer than 10 minutes. This will allow sessions to connect back if there is a failover. An immediate disconnect will take away the session if a failover situation occurs.
5. While still in the Host Options dialog box, click the Configuration tab.
6. In the Application Host area, under Dependent Host, in the Relay Load Balancer Address field, type the name or IP address of the primary and backup Relay Server you already configured in the edit field. The primary and backup Relay Server names or IP addresses must be separated by a semicolon. For example: RS_Server1;RS_Server2. The fully qualified name or IP address of the Relay Servers must be given on Dependent Server, otherwise an error dialog appears, and you will not be able to set the Relay Servers.

7. Click OK. A message box appears indicating that the change will not take effect until the Proficy Webspace Application Publishing Service has been restarted.
8. From the Control Panel, stop and restart the Proficy Application Publishing Service from the Services option. When the Proficy Application Publishing Service is restarted, the Dependent Server will appear beneath the Relay Server in the Webspace Admin Console's list of Proficy Webspace servers.

### To start a Webspace browser session in a high availability setup:

Use the following examples with the server and reconnect parameters.

For iFIX:

```
http://RS_Server1/ProficyWebspace/iFIX.html?&host=RS_Server1;RS_Server2&autoreconnect=5
```

where RS_Server1 is the name of the primary Relay Server, and RS_Server2 is the name of the backup Relay Server.

For CIMPLICITY:

```
http://RS_Server1/ProficyWebspace/CIMPLICITYScreenName.html?&host=RS_Server1;RS_Server2&autoreconnect=5
```

where RS_Server1 is the name of the primary Relay Server, and RS_Server2 is the name of the backup Relay Server.

**Note:**
When the Primary system is completely shut down, a new client connection CANNOT be made.

### To start a Windows Desktop Client in a High Availability Setup:

Use the –h command line argument with the address of the primary Relay Server, followed by a semi-colon, followed by the address of the failover Relay Server. Use the following examples with the host server and reconnect parameters.

For iFIX:

```
"C:\Program Files (x86)\Proficy\Proficy Webspace\Client\Proficy.exe" -h RS_Server1;RS_Server2 -autoreconnect=5 -c -a
 iFIX
```

where RS_Server1 is the name of the primary Relay Server, and RS_Server2 is the name of the backup Relay Server.

For CIMPLICITY:

```
"C:\Program Files (x86)\Proficy\Proficy Webspace\Client\Proficy.exe" -h RS_Server1;RS_Server2 -autoreconnect=5 -c -a
 CimView
```

where RS_Server1 is the name of the primary Relay Server, and RS_Server2 is the name of the backup Relay Server.

### Tips for Specifying Relay Server Names

- Specify the addresses of the primary and failover relay servers using either their IP addresses (if SSL is not used) or their fully-qualified domain names (FQDNs). When using the IP addresses, if SSL is used, the common names of the SSL certificates on the primary and failover relay servers must match the fully-qualified domain names of the computers.
- When dependent hosts and/or client computers reside in a different domain (or domains) than the relay servers, it is generally advisable to reference the relay servers via their FQDNs. Otherwise, dependent hosts and client computers may be unable to resolve the addresses of the relay servers.

### Relay Server Support

The following table outlines the Relay Server support.

| Mode | Relay Server | Relay Server and Dependent Server in Different Domains | Failover Relay Server | Failover Relay Server and Dependent Server in Different Domains |
|---|---|---|---|---|
| TCP (using IP Addresses or Host Names) | Supported | Supported | Supported | Supported |
| Encrypted (Host Names only with Strong Encryption) | Supported | Supported | Not Supported | Not Supported |

## Terminal Services and Webspace

When using Terminal Services and the Webspace Server:

- The Terminal Server cannot run on the same machine as the Webspace Server.
- The Terminal Services remote desktop is supported to remotely configure and administer a server.

- Terminal Services must run in administrative mode; do not use remote desktop for applications.
- On Microsoft Windows 2012, remote desktop provides you with two remote desktop connections as well as the console.

# Tips on Administrating User Accounts

### How Logins Work

To access applications on a Webspace Server, clients must sign in to the server machine. When a user starts a Webspace client, a prompt appears for a user name and password. This information is optionally encrypted (by default) and passed to the Webspace Application Publishing Service running on the Webspace Server. The Proficy Webspace Application Publishing Service then performs the logon operation on the Webspace Server using standard multi-user features of Windows. Next, the iFIX Security Login dialog box appears for the iFIX login. The user names and passwords should be the same for Windows and iFIX Security. (Optionally, you can configure password caching on the client for subsequent logins. For more information, refer to the Client-Side Password Caching *(on page 115)* section.)

When a user signs in to a Webspace Server and a domain is not specified, the Webspace Server first attempts to authenticate the account on the local machine, followed by the machine's domain, and lastly the trusted domains. Users can override this default behavior and specify a domain by typing the domain name followed by a backslash (\) and their network user name in the User name box of the Sign In dialog box (for example, NORTH\johng).

When a local user name on the Webspace Server is the same user name as a domain account, each with a different password, Webspace treats them as two separate accounts. Consider, for example, the following scenario:

- A local account on the Webspace Server, johng, with a password of local.
- A domain account, johng, with a password of domain.

When typing the user name johng with the password local in the Sign In dialog, the account will authenticate on the local Webspace Server. When typing johng with the password domain in the Sign In dialog, Webspace does not attempt to authenticate on the domain, but fails with an invalid user name or password. You must specify the domain name in the User name field in the Sign In dialog box (for example, NORTH\johng).

After a user is signed in, the Webspace relies on the server's operating system to provide the security necessary to run applications safely in a multi-user environment. Applications run in the security context

of the client user; this ensures private sessions. Access to all machines and network resources is governed by the operating system and the rights that have been granted to individual user's sessions.

Users must be able to log on interactively (locally) on the Webspace Server. Assign local logon rights to users in Local Security Policy, Domain Security Policy, and Domain Controller Security Policy.

### User Account Guidelines

- The same user name and password combination must be added to your user accounts in Windows and in iFIX to become a valid Webspace user.
- When adding user accounts in Windows, you can add them to the Workgroup or a Domain. However, it is preferable to use a Domain. Otherwise, you will need to map network drives, and use logon scripts *(on page 102)*.
- iFIX Windows Security must be enabled for each user you add on your Webspace Server in the iFIX Security Configuration program.
- When adding users through the Security Configuration application in iFIX, be sure to select the Windows Security option for the user.
- If you want to use Webspace with FIX Desktop, be aware that because iFIX security is enabled, logged in users must be authorized with the "FIX32 - Run a Task From View" rights in the iFIX Security Configuration application.
- When assigning security privileges in iFIX, use care when allowing application features that could allow write access, such as the "Database Save/Reload" and "Runtime Visual Basic Editor" features, as well as creating pictures with Datalinks, or any other means to write values into tags. Use Security Areas and Security Groups to further restrict access. Also, use care when creating and sharing schedules in iFIX, so that unintended VBA code is not activated inadvertently by web sessions. For more information on iFIX Security, refer to the Configuring Security Features e-book.
- The Webspace Server and the SCADA Server should reside on the same network.
- The Webspace Relay Server and dependent application servers with the Webspace installed, should all reside on the same network.

## Windows Configuration for Network and Client Printers

Your system may require the following Windows configuration to insure successful Webspace client printing: Custom names for client printers, Network printer setup, and Client printer setup in a multi-server environment.

## Customizing the Printer Name

Webspace installs a printer on the server for each printer that is configured on the client machine. These printers are called proxy printers and are the printers that are seen by users when printing via the Webspace session. By default, the name for the client's proxy printer installed on the Webspace Server is "*client_printer_name* (from *client_machine_name*)." So, for instance, if the client machine is named HRWorkstation and has a printer named "Xerox Phaser 6180MFP" attached to it, then the client's proxy printer on the Webspace Server will be named "Xerox Phaser 6180MFP (from HRWorkstation)." Since multiple users connect to a Webspace Server, these printers must be filtered so that users see only their own printers. This requires that each printer be assigned a unique identifier. A system administrator can specify the proxy printer format to ensure that each printer has a unique identifier. In addition, information can include the: User's name, Client computer's IP address, and the Client machine name.

1. Open the Windows Registry Editor.
2. Expand the HKEY_LOCAL_MACHINE key.
3. Locate the PrinterNameFormat key:

```
[SOFTWARE\Proficy\Proficy Webspace\AppServer\PrinterNameFormat]
```

4. Right-click PrinterNameFormat; select Modify on the Popup menu. (The default is "(from %C)".)
5. Enter one or more of the client printer customization tokens in the Value field. The available values are:

| Argu-ment | Description | Example |
|---|---|---|
| %U | User name | Wilson |
| %I | Client IP address | 192.168.100.14 |
| %M | Client MAC address | 001122334455 |
| %C | Client machine name | HRWorkstation |
| %S | Server machine name | Server1 |

6. Save and close the Registry Editor.
7. Restart the Webspace Server.

**Printer Name Format Guidelines**

- The following 2 characters are taken literally in the PrinterNameFormat string; they are not tokens: - @

- 12 characters that are not allowed are: ! , \ = / : * ? " < > |
- If any of the unallowed characters are used in the string, they are replaced with a hyphen

## Adding a Port to the Webspace Server

As the administrator, you can set up network printers for use by Webspace clients. You must first create a port on the Webspace Server that connects directly to the server and then install the printer locally. This provides direct access to the printer. Network printers are set up using the Windows Add Printer Wizard, and not the Client Printer Wizard, which is accessible through the Program Window.

1. On the Start menu, point to Settings and then click Printers. A new window opens.

> **Important:**
> Network printers are set up using the Windows Add Printer Wizard, and not the Client Printer Wizard, which is accessible through the Program Window.

2. Double-click the Add Printer icon.
3. Select local printer.
4. Click Next.
5. Click Create a new port; select Local Port as the type.
6. Click Next.
7. Type the UNC path to the printer in the Port Name dialog box. For example: you could enter \ \PRINTSERVER\LASERPRINTER or the printer's IP address.
8. Select the printer manufacturer on the left and the printer model on the right, or click Have Disk.
9. Follow the directions provided by the Add Printer Wizard to install the proper printer driver.

## Configuring Client Printers in a Multi-Server Environment

In a multi-server environment, a single Driver server can be a central location for printer drivers. The Driver server acts as a repository for all printer drivers that are available to Webspace clients. Printer drivers that are installed on the Driver server are replicated on each application server when a user requiring them logs onto the Webspace Server.

When a user configures a printer with a driver that is not already available on the Driver server, that driver is replicated on the Driver server and is available to all application servers with access to that Driver server.

If the Driver server and the Relay Server are:

- The same machine, no additional setup is required.
- Separate machines, the Driver server must:
    - Be accessible from the application servers.
    - Have a print$ share that points to the printer driver directory.

Users need:

- Read access to this share in order to install drivers from the Driver server.
- Write access to this share in order to install drivers to the Driver server.

If the Driver server and the Relay Server are on separate machines, provide the following:

- Read access to this share in order to install drivers from the Driver server.
- Write access to this share in order to install drivers to the Driver server.

# Working with the IIS Web Server

### IIS Installed Folder Location

If Webspace is installed on a computer with IIS, the installer will:

- Locate the root IIS Web directory that is identified in the Windows Registry.
- Install the client files (Webspace folder) under that directory.

### Webspace Server Installed Folder Location

The Webspace Server installs the client files in the Proficy Webspace\Web\Clients folder. The default location is:

C:\Program Files\Proficy\Proficy Webspace\Web\Clients

# Chapter 8. Reference

## Reference Information

For additional information on working with the Webspace product, refer to the following supplementary sections:



## How Do I...

Click any of the following links for step-by-step procedures:

- List client drives sequentially starting at a given drive letter *(on page 136)*
- Modify the server port setting *(on page 112)*
- Refresh the Webspace Admin Console *(on page 119)*
- Run a user-specific logon script *(on page 102)*
- Run a global logon script *(on page 102)*
- Run the Webspace Sessions *(on page 145)*
- Shadow a session *(on page 124)*
- Select a new location for the Log files *(on page 127)*
- Set output level for the logging *(on page 128)*
- Set permissions and restrictions for a file or an application *(on page 99)*
- Set the Refresh Rate on the Webspace Admin Console *(on page 119)*
- Set up a network printer *(on page 100)*
- Specify the minimum available physical memory necessary for this server to start a session *(on page 104)*
- Specify the minimum percentage of virtual memory necessary for this server to start a session *(on page 104)*
- Terminate a user's session *(on page 125)*
- View process information on the Webspace Admin Console *(on page 123)*
- View session information on the Webspace Admin Console *(on page 122)*

# Keyboard Shortcuts for the Webspace Admin Console

| Keyboard Combination | Action/Result |
|---|---|
| **Application Tab** | |
| Double-click application | Displays Application Properties dialog box |
| CTRL+A | Displays Application Properties dialog box. An installed application must be selected (on the Applications tab) in order for this keyboard shortcuts to work. |
| **Sessions Tab** | |
| DELETE | Terminates selected session |
| **Process Tab** | |

| Keyboard Combination | Action/Result |
|---|---|
| DELETE | Terminates selected process |
| **General** | |
| CTRL+TAB | Cycles through tabs |
| CTRL+SHIFT +TAB | Reverse cycles through tabs |
| CTRL+P | Displays Options dialog box |
| CTRL+B | Turns Status Bar on or off. |
| F1 | Displays Help for the Webspace Admin Console |
| F5 | Refreshes the Sessions, Processes, and Applications tabs |
| ALT+F4 | Exits the Webspace Admin Console |

# Editing Application Startup Properties

When you first configure the Webspace Server, you add the applications you want to run on the Applications tab. If you want to edit it later, you will need to restart the Proficy Webspace Application Publishing Service after you make the change.

1. From the Webspace Admin Console, in the main window, click the Applications tab.
2. From the list of applications, select an application from the list of applications.
3. Click Properties. The Application Properties dialog box appears.
4. Do any of the following:
    - In the Executable Path box, type a new path name. For example: C:\Program Files\Proficy \Proficy Webspace\Programs\ProficyWeb.exe.
    - In the Start Directory box, type the full path name of the directory in which you want the application to start. For example: C:\Program Files\Proficy\Proficy Webspace\Programs.
    - In the Command-Line Options box, type the startup parameters for the application. For example for iFIX: IFIX /s"C:\Program Files (x86)\Proficy\Proficy iFIX\LOCAL\WEB.SCU" and for CIMPLICITY: CIMLAYOUT or CIMVIEW (depends on the CIMPLICITY application you want to configure).
    - In the Display Name box, type a new display name for the application.

- In the Startup State section, select whether the application starts maximized, minimized, or in normal mode.
- Click the Change Icon button to browse for a new application icon.

5. Restart the Proficy Webspace Application Publishing Service. For steps, refer to the Restarting the Proficy Webspace Application Publishing Service *(on page 120)* section.

If you want to set up applications that use ODBC data sources, you must set up the ODBC drivers as system DSNs (data source names) for Webspace clients to be able to access the data sources. For more information about data sources, consult Microsoft's online help for the Windows ODBC Data Source Administrator.

Due to access restrictions, the Webspace Admin Console cannot verify the validity of paths specified in UNC format (for example: \\Machine Name\Folder Name\...) or that reside on a mapped network drive. If the Executable Path or Start Directory of a published application or item involves a mapped drive or is specified with a UNC path, the Webspace Admin Console will accept the specified path regardless of whether or not it is valid.

If the path is invalid, or if the client user does not have rights to access the specified executable file or folder, the published item will not appear in the Program Window. Select the item and click the Properties button. Try updating the item Executable Path or its Start Directory. If the item has been uninstalled or moved to a new location, it will not be displayed in the Webspace Admin Console once the Application Publishing Service has been restarted.

The Webspace Admin Console is unable to establish group and user settings for any item's path specified in UNC format or that resides on a mapped drive. The following message is displayed in the Webspace Admin Console's Application Users/Groups window for any application or file where this applies: "User/Group settings not available."

# Chapter 9. Glossary

## Glossary

### A

ActiveX *(on page 180)*

Proficy Webspace Application Publishing Service *(on page 184)*

### B

Bandwidth *(on page 180)*

Batch file *(on page 181)*

Binary file *(on page 181)*

Bridge *(on page 181)*

### C

Client/Server Mode *(on page 181)*

Webspace Admin Console *(on page 185)*

### D

Domain *(on page 182)*

### E

Ethernet *(on page 181)*

### F

FAT (file allocation table) *(on page 182)*

### G

Gateway *(on page 182)*

Group *(on page 182)*

**H**



**I**



**J**



**K**

**L**



**M**



**N**



**O**



**P**



**Q**

**R**

**S**



**T**



**U**



**V**

**W**



**X**

**Y**

**Z**

# A

## ActiveX

A set of technologies and tools developed by Microsoft® Corporation that enable software components to interact with one another in a networked environment, regardless of the language in which the components were created.

# B

## Bandwidth

A measure of the volume of information that can be transmitted over a communications link. Technically, bandwidth refers to the width of the frequency spectrum available on a certain technology.

### Batch file

An ASCII text file containing a sequence of operating-system commands, possibly including parameters and operators supported by the batch command language. When the user types a batch filename at the command prompt, the commands are processed sequentially. Also called batch program.

### Binary file

A file consisting of a sequence of 8-bit data or executable code, as distinguished from files consisting of human-readable ASCII text. Binary files are usually in a form readable only by a program, often compressed or structured in a way that is easy for a particular program to read.

### Bridge

A device that connects networks using the same communications protocols so that information can be passed from one to the other. A device that connects two local area networks, whether or not they use the same protocols

## C

### Client/Server Model

A model of computing whereby client applications running on desktops or personal computers access information on remote servers or host computers.

## D-E

### Dependent Application Server

A dependent application server is a Webspace Server that is connected to a Relay Server, and shares the Webspace sessions as directed by the Relay Server. A dependent application server also has the Webspace Server installed, along with IIS or Apache HTTP Server. However, unlike the Relay Server, only a few configuration items are entered in the Webspace Admin Console on each dependent application server. These items include the Relay Server name, the Maximum Number of Sessions setting, the

Minimum Available Physical Memory setting, the Minimum Available Virtual Memory setting, and the Client Access printer driver settings.

Each dependent application server (installed software and settings) should be a clone of the Relay Server. In other words, all software, pictures, and network access must be the same.

### Domain

A group of computers and devices on a network that are administered as a unit with common rules and procedures.

## F

### File Allocation Table

A list or table maintained to keep track of all the parts of a file so they can be linked together when the file is used again. Also referred to as the FAT file system.

## G

### Gateway

A computer that forwards and routes data between two or more networks of any size.

### Group

An account containing other accounts called members. The rights and permissions assigned to a group are also provided to its members.

## H-I

### Host

Any computer that provides services to remote users.

### HTTP

The communication protocol used to connect servers on the World Wide Web.

# J

## JavaScript

A scripting language developed by Netscape to help Web authors create and customize applications. Although JavaScript is commonly confused with Java, it was developed independently.

# L

## LAN

A group of computer systems in close proximity that can communicate with one another via some connecting hardware and software.

# M

## Menu Bar

The horizontal bar below the title bar that contains the names of all the application's menus.

# N

## Network

A communications system that links two or more computers.

## Network Computer

Computers or terminals with little or no memory or disk storage, network computers (NCs) are designed to connect to a network. NCs are more affordable than PCs and can be administered from a central network server.

## Network Drive

On a local area network, a disk drive whose disk is available to other computers on the network. Access to a network drive might not be allowed to all users of the network; many operating systems contain security provisions that enable a network administrator to grant or deny access to part or all of a network drive.

# O-P

## Port

A connection point on your computer where you can connect devices that pass data into and out of a computer, such as a printer.

## Proficy Webspace Application Publishing Service

A service that receives client connection requests, authenticates users on the Webspace Server, and launches the Webspace sessions.

# R

## Relay Server

The Relay Server is a Web server that provides centralized control over the Webspace Server, providing load balancing across a number of dependent application servers. The Relay Server maintains and distributes the client connections across each of the dependent application servers.

## Remote Access

The hookup of a remote computing device via communication lines such as phone lines or wide area networks to access network applications and information.

# S

## Server

Networked computer that provides resources or services to remote clients.

## SMTP

The Internet standard protocol for transferring electronic mail messages from one computer to another. SMTP specifies how two mail systems interface and the format of control messages they exchange to transfer mail.

## Status Bar

Usually located at the bottom of a window, the status bar provides information relating to the application.

# T

## TCP/IP

A combined set of protocols that performs the transfer of data between two computers. TCP monitors and ensures correct transfer of data. IP receives the data from TCP, breaks it up into packets, and ships it off to a network within the Internet.

## Title bar

The horizontal bar that contains the title of the window. The title bar is located at the top of the window.

# U

## URL

The name that uniquely identifies a page of a hypertext document accessible via the World Wide Web. For example: https://digitalsupport.ge.com.

## User Profile

A user profile includes all the per-user settings of the user's desktop environment, such as screen colors, screen savers, printer connections, window size and position, desktop arrangement, and so on.

# W

## WAN

A set of computers located in geographically diverse locations and connected for the purpose of sharing applications and data.

## Webspace Server

A computer that has the Webspace Server software installed on it.

## Webspace Admin Console

A 32-bit Windows application that is installed on a Webspace Server. The Webspace Admin Console is used by Webspace Administrators to manage Webspace user access.