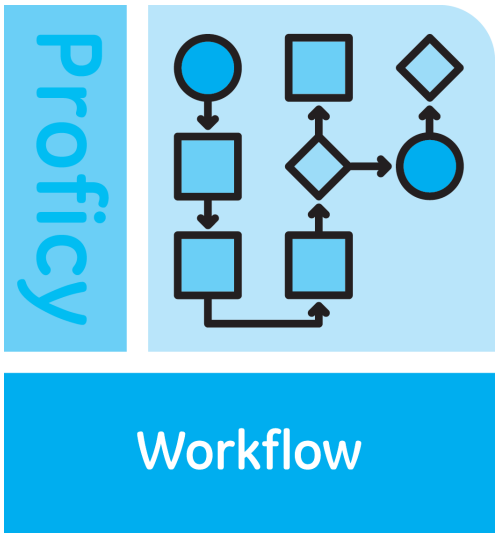
GE
Intelligent Platforms



Proficy* Workflow 2.5

GETTING STARTED GUIDE

Proficy* Workflow

GETTING STARTED

Version 2.5
March 2015

Disclaimer of Warranties and Liability

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

Trademark Notices

© 2015, General Electric Company. All rights reserved.

Proficy is a trademark of GE Intelligent Platforms, Inc., a wholly-owned subsidiary of General Electric Company.

* Indicates a trademark of General Electric Company and/or its subsidiaries.

All other trademarks are the property of their respective owners.

All other product names and marks identified throughout this book are trademarks or registered trademarks of their respective companies. They are used throughout this book in editorial fashion only. No such use, or the use of any trade name, is intended to convey endorsement or affiliation.

No part of this publication may be reproduced in any form, or stored in a database or retrieval system, or transmitted or distributed in any form by any means, electronic, mechanical photocopying, recording or otherwise, without the prior written permission of GE Intelligent Platforms. Information contained herein is subject to change without notice.

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

Contents

Getting Started Guide..... 4
Key Concepts..... 4
System Health and Program Use..... 4
Regional Settings..... 5
Daylight Saving Time..... 6
Special Keyboard Buttons..... 6
Log Files..... 6
Compatibility and Upgrading with Proficy Products..... 6
System Requirements..... 8
Hardware Recommendations..... 9
Hardware Requirements..... 11
Software Requirements..... 12
Pre-installation Considerations..... 20
Architecture..... 20
Services..... 21
Active Directory for the Web Server..... 22
Security Certificates..... 23
Firewall Ports..... 26
Database Backup and Restore..... 26
Multiple Servers..... 27
Server Clustering and Failover..... 28
Reverse Proxy Configuration for a Web Server..... 29
Configure SQL Server 2012..... 30
License Management..... 30
Performance Counters..... 31
Installation Procedures..... 34
Install a single application server and client..... 34
Install the web server..... 37
Install a remote client..... 38
Configure multiple servers on a single machine..... 39
Revert multiple servers to a single server..... 40
Multiple Server Installation on Multiple Machines..... 40
One-Click Deployment..... 43
Command Line (Silent) Installation..... 44
Uninstall Proficy Workflow..... 46
Server Clustering Implementation..... 47
Supported and Validated Cluster Configurations..... 47
Failover Cluster Manager for Windows..... 49
Install Failover Cluster Manager..... 49
Configure the Failover Cluster Manager..... 50
Configure quorum options for a cluster..... 50
Configure the primary cluster server..... 51
Configure the failover cluster server..... 51
Configure a local client for a cluster node (32-bit)..... 52
Configure a local client for a cluster node (64-bit)..... 52
Server Clustering and One-Click Deployment..... 52
Clustering Tips..... 52
Web Task List Deployment..... 53
Configure security certificates for a reverse proxy..... 53
Configure an IIS reverse proxy..... 54
Configure an Apache reverse proxy..... 55

Connect to the Web Task List....57
Log On Overview....58
Log in to the client....58
Automatically Log On....60
GE Single Sign On (SSO)....60
Authentication....61
Post-installation Configuration....63
Running with a Standard Windows User Account....63
Configure web proxy settings for Local System account....63
Modify security certificates....64
Modify site configuration....64
Monitor system configuration and status....66
Modify the server configuration for a remote client....66
Modify AD LDS....66
Modify your application server database....67
Modify your web server database....68
Modify your web server password....68
Configure a server instance....68
Configure product options....69
Change architecture mode....70
Add or remove performance counters....70
Upgrading....70
Upgrade to a newer version....72
Notes on Upgrading Proficy Vision....73
Upgrade custom forms....74
Database Migration....75
Move a database....75
Reporting Database....76
Install the reporting database....76
Configure Component Services....77
Uninstall the reporting database....78
Upgrade a replicated database....78
Remote Desktop Session Host....80
Remote Desktop Services (Terminal Services)....80
Getting Started....81
Proficy Workflow with Windows Remote Desktop Session Host Installation and Configuration....83
Troubleshoot Your Proficy Workflow Remote Desktop Session Host Environment....85
Frequently Asked Questions....86
ActiveX Task Controls....86
Task List Configuration....86
Install the ActiveX Task List....87
Modify the installation configurations....87
Security....88
Defense in Depth....88
Anti-virus software....88
Data Execution Prevention....89
Software Patching....89
Platform Configuration and Hardening....89
Contact Information....89

Getting Started Guide

Welcome to Proficy* Workflow!

Before you begin installing this product, please take some time to review this guide.

IMPORTANT: Please read the Important Product Information (IPI) provided to you for the latest information about this application, including new features, system requirements, and release notes.

Key Concepts

Proficy Workflow is a unifying architecture for our software products, and a framework to leverage existing applications and functionality. The role of this product is to provide the components and services which, when adopted by a product line, drives common operational behavior and support.

This product gives you a flexible foundation for building applications and interfacing with other software. It contains the tools you need to create applications that can be used to facilitate the management and analysis of activities in your enterprise.

You can customize your environment to:

- host editors for building Proficy applications
- display HMI screens for monitoring plant activities
- display workflow tasks to operators on the plant floor
- accept input into forms that can be created and routed to clients throughout the enterprise

Proficy Workflow also provides a configurable event engine that can trigger workflows and other code based on different types of internal and external triggers.

System Health and Program Use

As part of configuring a Proficy Workflow system, you indicate which servers should host which product options, and designate servers and product options as either essential or nonessential. These designations in combination with server status determine site health and affect the ability to log in and use this software.

If you designate a server as essential when configuring the system, all associated product options are automatically designated as essential. If you designate any product option as essential, the server that is hosting that option is automatically designated as essential, but the essential status of other product options hosted by the server remains unchanged.

NOTE: The server(s) hosting the Core and Workflow product options are designated as essential by default, and this designation cannot be changed.

The designation of servers as either essential or nonessential and the state and accessibility of servers has implications for the health of the system and, therefore, the ability to log in and use the Proficy Workflow program, as follows:

- When all servers, both essential and nonessential, are running and reachable, system health is considered *Complete*. In this scenario, the site health indicator in the toolbar is green, users can log in to the program, and all program and product option functionality is available.
- When one or more nonessential servers are not running or are unreachable, system health is considered *Partial*. In this scenario, the site health indicator in the toolbar is yellow, active users remain logged in to the program, and inactive users can log in, but program functionality tied to product options hosted on compromised servers is unavailable.

  NOTE: Specifically, related displays become inaccessible, binding to related external data faults, and related events stop firing. In addition, workflows that consume related data or monitor related events fail (making it

a recommended practice to wrap such operations in fault handlers). Upon restoration of server availability, display inaccessibility and data-binding, event-firing, and workflow failure are automatically reversed. However, any work that was being performed using a display when a related server became unavailable may be lost.

- When one or more essential servers that do not host the Core product option are not running or are unreachable, system health is considered *Waiting*. In this scenario, the site health indicator in the toolbar is yellow, active users are logged out of the program, and inactive users cannot log in.

  NOTE: In this case, upon restoration of the essential server(s), users active at the time of interruption are automatically logged back in to the program, and functionality is restored to the level in accordance with the current health of the site.
- When the server that hosts the Core product option (typically, SOAServer) is not running or is unreachable, system health is considered *Unavailable*. In this scenario, the site health indicator in the toolbar is gray, active users are logged out of the program, and inactive users cannot log in.

  NOTE: In this case, upon restoration of the server that hosts the Core product option, users active at the time of interruption are automatically logged back in to the program, and functionality is restored to the level in accordance with the current health of the site.

When system health is either *Complete* or *Partial*, you can use the **System Status** display to monitor server configuration and status. In these states of site health, you can also move product options between servers to accommodate changing conditions, as necessary.

Regional Settings

The following regional settings are supported.

NOTE: Proficy Open Enterprise supports the same regional settings as Proficy Workflow.

- Proficy Client-based Regional Settings on page 5
- Proficy Web-based Application Settings on page 6

Proficy Client-based Regional Settings

Supported Settings

- Decimal symbol - one character
- Digit grouping symbol
- List separator - one character
- Time style
- Time separator
- Short date style
- Date separator

NOTE: The decimal symbol and the digit grouping symbol cannot be the same character. Also, the time separator and the date separator cannot be the same character.

Formatting the Time and Date

Avoid changing the time style or short date style in regional settings to values that are outside of the standard styles provided. Changing these values to non-standard styles may result in improperly formatted times and dates in some parts of Proficy Workflow.

This software supports the following short date formats, some of which may not be available in certain language versions of Windows:

- dd/mm/yy or dd/mm/yyyy
- dd/yy/mm or dd/yyyy/mm
- mm/dd/yy or mm/dd/yyyy

- mm/yy/dd or mm/yyyy/dd
- yy/dd/mm or yyyy/dd/mm
- yy/mm/dd or yyyy/mm/dd

Formatting the Regional Language Setting

Avoid changing the language setting when Proficy Workflow is running.

Setting the System Default Locale

The selected locale must be set as the system default.

Proficy Web-based Application Settings

In order to capture the date and time settings accurately in Google Chrome and Mozilla® Firefox®, you must change the language settings in these browsers. Changing these settings reflects the date and time that is pertinent to the selected language. For Internet Explorer, your current language settings are automatically applied. For more information on supported browsers, see Browser Requirements on page 16

Daylight Saving Time

In Proficy Workflow, all dates and times are stored independent of time zones, in UTC format.

Special Keyboard Buttons

Some computer keyboards have special buttons for e-mail launch, Internet launch, search, and other functions. These keyboard buttons may disable certain key macros or allow users to circumvent security measures.

We recommend that you reprogram or disable the software that operates such special buttons. Refer to your computer's documentation for instructions on disabling these buttons.

Log Files

Proficy Workflow provides a number of log files that you can use to assist you in troubleshooting various aspects of your system.

On all supported operating systems, the log files are located in: <installdir>\ProgramData\Proficy\Logs.

TIP: To access the ProgramData folder, you must show the hidden folders on your system.

The log files for all installations are also accessible from the program group; that is, **Start** > **All Programs** > **Proficy** > **Proficy Workflow** > **Logs**.

Compatibility and Upgrading with Proficy Products

If you plan to use one or more other Proficy products with Proficy Workflow, it is important to first determine whether the version of each such product is compatible with the latest version of this application.

Compatible Proficy Products

Proficy Workflow may be used with a number of other Proficy products. Depending on the product or product version, you may need to run Proficy Workflow in a particular architecture mode or take additional measures during set up to ensure compatibility between the products. If so, the notes in the following table provide the necessary details.

NOTE: Changes to the OnDemandProvider Class. A new abstract method called GetChecksum was added to the OnDemandProvider class. Classes derived from the OnDemandProvider class must implement this new

method. This change was required so that the client (via IBrowse.QueryChecksum) can determine when the navigator content must be updated from the server.

Proficy Workflow	Proficy CIMPLICITY	Proficy Historian	Proficy iFIX	Proficy Open Enterprise	Proficy Plant Applications	Proficy Plant Applications Service Provider (PASP)	Proficy Portal	Proficy for Manufacturing Discrete
2.5	8.1 8.2 9.0 9.0 R2	4.5 5.0 5.5 6.0	5.0 5.1 5.5 5.8	2.2	Not Supported	Not Supported	Not Supported	Not Supported
2.2 SP1	8.1 8.2	4.5 5.0 5.5	5.0 5.1 5.5 5.8	2.2	6.2	2.2	3.5	6.3 SP1 6.3 SP2 6.4
2.2	8.1 8.2	4.5 5.0 5.5	5.0 5.1 5.5 5.8	2.2	6.2	2.2	3.5	6.3
2.1	8.1 8.2	4.5 5.0 5.5	5.0 5.1 5.5	1.6	5.0 6.0 6.1	1.5	3.5	6.2

NOTE:

The following notes apply to product versions compatible with Proficy Workflow 2.5:

- Proficy CIMPLICITY 9.0: End points names must not exceed 32 characters.

The following notes apply to product versions compatible with Proficy Workflow 2.2, 2.2 SP1, 2.5:

- Proficy CIMPLICITY 8.1 and 8.2: OPC is recommended for exchanging data between Workflow and CIMPLICITY.
- Proficy Historian 5.0: Data types added to Proficy Historian 5.0 (ihUInt64, ihUInt32, ihUInt16, ihByte, ihBool) are not supported for binding to parameters or local variables in Proficy Workflow.

The following notes apply to product versions compatible with Proficy Workflow 2.1:

- Proficy Historian 5.0: Data types added to Proficy Historian 5.0 (ihUInt64, ihUInt32, ihUInt16, ihByte, ihBool) are not supported for binding to parameters or local variables in Proficy Workflow 2.1.
- Proficy Open Enterprise 1.6: This version can run only with the 32-bit version of Proficy Workflow; however, the 32-bit version can be installed on a 64-bit machine. For more information, see Architecture Considerations on page 20.
- Proficy Plant Applications 6.1: This version cannot be installed directly on top of Proficy Workflow 2.1. You must first install Proficy Workflow 2.0, then install Proficy Plant Applications 6.1, and then upgrade Proficy Workflow to version 2.1.
- Proficy Plant Applications 6.2: A number of Plant Applications displays can be viewed in Proficy Workflow. Plant Applications licensing is required. Displays that can be viewed include Non-Production Time, Downtime

+, Waste+, Alarms, Schedule, Genealogy, and a number of related Autolog displays. For more information, see **Using Plant Applications Displays in the Proficy Client** in the Plant Applications Help for instructions to set up the displays.

- Proficy Plant Applications Service Provider 1.5
  - Installing the PASP with a new installation of a Proficy Workflow 2.1 legacy server is not supported. However, you can upgrade a legacy server to a previous version of Proficy Workflow that is running the PASP.
  - Version 1.5 must be run on a 32-bit User Server installation of Proficy Workflow to be compatible with Proficy Workflow 2.1. It cannot be run on a 64-bit User Server installation of Proficy Workflow. However, the 32-bit User Server can be installed on a 64-bit machine. For more information, see Architecture Considerations on page 20.

Compatible Upgrade Paths

The information in this section indicates the current product compatibility when upgrading from Proficy Workflow 2.2 to Proficy Workflow 2.5.

Task List

Proficy Workflow with:	Proficy client Task List	Supported
	ActiveX Task List	Supported
Proficy Vision 6.1 with:	Web Task List	Not Supported
	Proficy Mobile Task List	Not Supported
Proficy Vision 6.2 with:	Proficy Mobile Task List	Not Supported
Independent Host with:	Web Task List	Supported

Service Providers

Proficy Historian 4.0, 5.0, 5.5, 6.0	Supported
Plant Applications Service Provider (PASP)	Not Supported
Plant Applications (direct connection)	Not Supported
Custom Service Provider **NOTE:** Service providers that target versions of the .NET framework before version 4.5 must be recompiled targeting .NET 4.5.	Not Supported

System Requirements

The hardware and software requirements you require to install Proficy Workflow.

Before you begin installing your this application, we highly recommend that you start by reviewing the **Important Product Information**, where you can read the latest release notes and the most current information about Proficy Workflow.

Hardware Recommendations

This section describes the recommended hardware specifications which are needed for Proficy Workflow to perform well.

Since Proficy Workflow is a very flexible product with very broad capabilities, there are a variety of ways that this product is used. The table below provides some general guidelines for hardware recommendations based on some sizing specifications.

Project Specification	Small System	Medium System*	Large System*
Equipment Model Objects	0 – 500	500 – 2,500	2,500 +
Equipment Model Properties	0 – 5,000	5,000 – 500,000	500,000 +
Material Definitions	0 – 1,000	1,000 – 10,000	10,000 +
Material Lots	0 – 1,000	1,000 – 5,000	5,000 +
Production Model Objects	0 – 500	500 – 1,000	1,000 +
Production Variables	0 – 5,000	5,000 – 10,000	10,000 +
Number of Workflows	0 – 100	100 – 1,000	1,000 +
Running Workflows	0 – 50	50 – 500	500 +
Concurrently Executing Workflows**	0 – 5	5 – 25	25 +
Configured Events	0 – 50	50 – 500	500 +
Events Triggering per Hour	0 – 15	15 – 100	100 +
Work Requests in System	0 – 100	100 – 1,000	1,000 +
Active Work Requests	0 – 25	25 – 500	500 +
Active Clients	1 – 25	25 – 100	100 +
Recommended Server RAM	8 GB	16 GB	32 GB
Recommended Server CPUs	2 CPUs @ 3GHz	4 CPUs @ 3GHz	8 CPUs @ 3GHz

*Many systems do not use all of the capabilities of Proficy Workflow, so some projects may match some specifications in the small system column with other specifications in the medium or large system column. Choose the column that more closely matches the targeted system.

**Any running workflow that is waiting for user input in a task form can be considered *paused* and is considered to be a running workflow but not an executing workflow.

Additional Factors for Hardware Recommendations

Special Application Factors

Server recommendations may need to be increased when the application uses intensive processing or significant disk access. Examples of these scenarios include reading and parsing data files from disk, custom logging or writing to output data files, advanced mathematics in code activities, custom service providers, communicating with third party products, and so on.

SQL Server on the Proficy Workflow Server

The hardware recommendations above are for servers where the SQL Server is not on the Proficy Workflow server system. If you choose to run SQL Server on the Proficy Workflow server, then you must add RAM and CPUs to the recommended amounts.

Running on a Virtualized Machine

The hardware recommendations above are for a server that is not running in a virtualized environment. For servers that are running in a virtualized environment such as a VMWare or Hyper-V image, the recommended amounts must be exclusively allocated to the server image and have as much available physical resources on the virtualization server. For example, if a server needs 8GB of RAM, then that much RAM must be allocated to the image, and the virtualization server must have 8GB of physical RAM available for that image. If the image runs out of physical RAM on the virtualization server, performance degrades significantly.

Running Other Applications

All the hardware recommendations are assuming that the machine is dedicated to running the Proficy Workflow server. If you are planning to run other applications on the machine, you will need to increase the CPU and RAM requirements appropriately to handle running these applications. This includes other GE Intelligent Platforms applications, such as Proficy Historian, Proficy CIMPLICITY, or Proficy iFIX.

Using Windows® Server 2008 R2 or Windows® Server 2012 as the Operating System

Newer Microsoft operating systems have greater hardware requirements than older ones. Windows® Server 2008 R2 and newer use significantly more memory and more CPU. For equivalent performance, add an additional 2 GB of memory and an additional processor.

Additional Recommendations for the SQL Server Machine

For optimum performance, the databases, transaction logs, tempdb, non-clustered indexes, and back-ups should be installed on separate hard drives where possible. The following RAID specifications are also recommended:

- SQL database: RAID 0+1, RAID 1 or RAID 5
- SQL transaction logs: RAID 0+1 or RAID 1, and should be a separate physical device
- SQL tempdb: RAID 0+1 or RAID 1
- SQL indexes: RAID 0+1 or RAID 1
- Back-ups: RAID 0 (no fault tolerance, but faster writes) or RAID 5

Additionally, the following SQL Server configuration is recommended:

- SQL Server machine: 4 GB RAM (*required minimum*)
- Use Mixed Mode security
- Exclude the database files from anti-virus scanning
- Use multiple processors for every installation
- Enable the default backup job or create a maintenance plan
- For tempdb, the number of files configured should be based on the number of processors that the server has (for more information, see Optimizing tempdb Performance)

Other Performance Considerations

The guidelines described here are not the only aspects of a system to be considered to ensure optimum performance. Each individual system should be evaluated for other potential sources of performance issues. Examples of other sources of problems may include, but are not limited to, the following:

- Networking throughput between Proficy Workflow server and client
- Networking throughput between Proficy Workflow server and SQL Server
- Data throughput between the Proficy Workflow server and data sources such OPC servers, Proficy Historian, Proficy iFIX, and Proficy CIMPLICITY.
- The number of client instances active on a single client machine

Hardware Requirements

This section describes the minimum hardware required to run Proficy Workflow and all products that work with it.

Hardware Requirements for an Application Server

This section describes the hardware required for your product installation.

- 4-socket 8 Core 32 GB RAM
- Windows Server x64 OS
- 200 GB free hard disk space
- Network interface software for network communications, and TCP/IP network protocol
- SVGA or better color graphics monitor and a 100% IBM-compatible 24-bit graphics card capable of 1024x768 resolution and at least 65535 colors
- XGA or better color graphics monitor and a 100% IBM-compatible 24-bit graphics card capable of 1024x768 resolution and at least 65535 colors
- Two-button mouse with scroll wheel or compatible pointing device (*such as a touch screen*)

Hardware Requirements for Single Servers

This section describes the hardware required for your product installation.

Server Deployment

NOTE: These requirements apply whether you are installing a multiple server configuration (that is, a core server and a Workflow server), or a failover cluster.

- 3 GHz Core™ 2 Duo processor with 8 GB RAM (*minimum*)
- 50 GB free hard disk space (*minimum*)
- DVD-ROM drive
- Network interface software for network communications, and TCP/IP network protocol
- One parallel port or free direct-connect USB port
- XGA or better color graphics monitor and a 100% IBM-compatible 24-bit graphics card capable of 1024x768 resolution and at least 65535 colors
- Minimum monitor support
- Two-button mouse with scroll wheel or compatible pointing device (*such as a touch screen*)

Hardware Requirements for Extension Servers

This section describes the hardware required for your product installation.

- 3 GHz Core™ 2 Duo processor with 8 GB RAM (*minimum*)
- 50 GB free hard disk space (*minimum*)
- Network interface software for network communications, and TCP/IP network protocol
- One parallel port or free direct-connect USB port
- XGA or better color graphics monitor and a 100% IBM-compatible 24-bit graphics card capable of 1024x768 resolution and at least 65535 colors
- Minimum monitor support
- Two-button mouse with scroll wheel or compatible pointing device (*such as a touch screen*)

Hardware Requirements for User Servers

This section describes the hardware required for your product installation.

- 3 GHz Core™ 2 Duo processor with 4 to 8 GB RAM (*dependent on how much activity the server is expected to manage*)
- 50 GB free hard disk space (*minimum*)
- DVD-ROM drive
- Network interface software for network communications, and TCP/IP network protocol
- One parallel port or free direct-connect USB port

- XGA or better color graphics monitor and a 100% IBM-compatible 24-bit graphics card capable of 1024x768 resolution and at least 65535 colors
- Minimum monitor support
- Two-button mouse with scroll wheel or compatible pointing device (*such as a touch screen*)

Hardware Requirements for Clients
This section describes the hardware required for your product installation.

- 3 GHz Core™ 2 Duo processor with 2 GB RAM (*minimum*)
- 20 GB free hard disk space (*minimum*)
- DVD-ROM drive
- Network interface software for network communications, and TCP/IP network protocol
- SVGA or better color graphics monitor and a 100% IBM-compatible 24-bit graphics card capable of 1024x768 resolution and at least 65535 colors
- Two-button mouse with scroll wheel or compatible pointing device (*such as a touch screen*)

Hardware Requirements for a Reporting Database
This section describes the hardware required for your product installation.

- 3 GHz Core™ 2 Duo Processor with 3 GB RAM (*minimum*)
- 50 GB free hard disk space (*minimum*)
- DVD-ROM drive
- Network interface software for network communications, and TCP/IP network protocol
- One free direct-connect USB port
- XGA or better color graphics monitor and a 100% IBM-compatible 24-bit graphics card capable of 1024x768 resolution and at least 65535 colors
- Two-button mouse with scroll wheel or compatible pointing device (*such as a touch screen*)

Server Clustering and Failover Hardware Requirements
This section describes the hardware required for your product installation.

The hardware requirements set by Microsoft for clustered server configurations must be met for systems deploying Proficy Workflow with cluster support.

- *Failover* clustering is supported on Proficy Workflow 1.5 SP4 and greater.
- SQL Server must be installed in a central location on the domain.

IMPORTANT:

- All computers in a *failover* cluster must be on a domain.
- *Failover* clustering is not supported on Proficy legacy servers.
- Proficy Workflow server clustering provides support against hardware failures only.

Custom services managed by clustering must maintain their state in shared persistent memory (typically a database), and the state must always be in a consistent state because failover can occur at any time.

Software Requirements

This section describes the minimum software requirements for your installation, including the recommended operating system and database.

The clocks on all Proficy Workflow servers and clients must be synchronized. This protects against certain kinds of threats and provides accurate logging and timestamps.

NOTE: In order to communicate with remote clients, the Proficy application server must be installed on a domain. If you install the it off the domain, it can only be used for development purposes, not for production purposes.

Application Server Software Requirements

This section describes the software requirements for your installation.

Installation

When using a client in remote desktop session, the selected object in the navigator is now updating with the current display and you can change the available displays list.

The following list describes the software required to install and use Proficy Workflow and the application server.

NOTE: In addition to the following material, see Architecture Considerations on page 20 for information on options related to operation mode when installing on a 64-bit computer.

Operating System Options

The following operating systems are supported:

- Microsoft® Windows® 7 Professional (32- or 64-bit)
- Microsoft® Windows® 8 (64-bit)
- Microsoft® Windows® Server 2008 SP2 (32-bit only)
- Microsoft® Windows® Server 2008 R2 (64-bit)

  NOTE: Terminal server environments are supported only on Windows Server 2008 R2 (64-bit).
- Microsoft® Windows® Server 2012 Standard (64-bit)
- Microsoft® Windows® Server 2012 R2 (64-bit)

SQL Server Options

The Proficy Workflow installation automatically selects the default SQL Server instance. If SQL Server 2012 and SQL Server 2008 are both installed, SQL Server 2008 may be the default instance. In this scenario, if you want to use SQL Server 2012 instead, you must select this instance as the default as part of manually configuring your SQL Server settings. For more information, see the topic corresponding to the type of installation you will be performing.

The Proficy project is installed into this SQL Server database. SQL Server can be installed on a different computer that is also on the domain or workgroup; however, you must ensure that network configurations allow appropriate machine communication.

SQL Server must be configured with both Windows and SQL Server authentication.

The following SQL Server systems are supported:

- Microsoft® SQL Server 2008 Standard or Enterprise Edition (32- or 64-bit)
- Microsoft® SQL Server 2008 R2

  NOTE: Changes to the SQL Server database recovery model have occurred. For more information, please visit the GE Intelligent Platforms Knowledge Base website at http://support.ge-ip.com/support/index?page=kbchannel, and then search for the related article, KB16204.
- Microsoft® SQL Server 2008 Express

  NOTE: If you are using SQL Server Express with the Proficy application server, you cannot use the Proficy Reporting Database.
- If you are using SQL Server Express with the Proficy application server, you cannot use the Proficy Reporting Database.
- Microsoft® SQL Server 2012 Enterprise (32- or 64-bit)
- Microsoft® SQL Server 2012 Business Intelligence (32- or 64-bit)
- Microsoft® SQL Server 2012 Standard (32- or 64-bit)
- Microsoft® SQL Server 2012 Express (32- or 64-bit)

NOTE: In order for Proficy Workflow to connect to any edition of Microsoft® SQL Server 2012, you must configure SQL Server to enable the *sysadmin* role for the applicable login account. For more information, see Enable Connection between Proficy Workflow and SQL Server 2012 on page 30.

Other Requirements

- Microsoft® .NET Framework 4.5 (Full Framework)

  NOTE: Custom display or form assemblies that target earlier versions of .NET will continue to function as before. However, saving changes made to such custom assemblies requires that they be upgraded, which is accomplished in different ways, based on the version of .NET:

  - For an assembly that pre-dates .NET 4.0, you must upgrade the assembly when you open it. Failure to do so results in an error and the inability to save the edited assembly.
  - For an assembly that targets .NET 4.0, the assembly is upgraded automatically when opened, and changes to such assemblies can be saved as before.

  Service providers that target versions of the .NET framework before version 4.5 must be recompiled targeting .NET 4.5.
- Microsoft® AD LDS (Active Directory Lightweight Directory Service) or ADAM (Active Directory Application Mode) with SP1 (available from http://www.microsoft.com/downloads/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en)

  NOTE:

  - If you are using Microsoft Windows 7, Windows Server 2008, or Windows Server 2012, using AD LDS is recommended, which can be added as Windows components/features in the **Programs** applet of the **Control Panel**.
  - For demonstration, evaluation, or pilot systems, you can use Simulated Directory mode rather than using ADAM or AD LDS. In this mode, the system functions the same way. However, you must use ADAM or AD LDS to run large systems that have hundreds of clients connecting simultaneously.
- Microsoft® Excel 2007 or 2010. To use Excel 2007, you must manually install the Primary Interop Assemblies (for Import/Export operations). These assemblies are included in the Excel 2010 installation.

  - http://msdn.microsoft.com/en-us/library/kh3965hw.aspx
  - http://www.microsoft.com/downloads/details.aspx?familyid=59DAEBAA-BED4-4282-A28C-B864D8BFA513&displaylang=en
  - http://technet.microsoft.com/en-us/library/cc179091.aspx
- Microsoft® Internet Explorer 7 or greater
- For web-based forms, Microsoft® Internet Explorer 10 or greater is required

  NOTE: Internet Explorer 10 is only supported on the following operating systems:

  - Windows® 7 SP1
  - Windows® 8
  - Windows® Server 2008 R2 with SP1
  - Windows® Server 2012
- Microsoft® Internet Information Services (IIS) 7.0 or greater

  The following services, with one exception, must be enabled:

  - Common HTTP Features: Static Content; Default Document; HTTP Errors; HTTP Redirection

    NOTE: For security purposes, consider disabling Directory Browsing.
  - Application Development: ASP. NET; .NET Extensibility; ASP; ISAPI Extensions; ISAPI Filters
  - Security: Basic Authentication; Windows Authentication; URL Authorization; Request Filtering
  - Management Tools: IIS Management Console
- Windows Communication Foundation HTTP Activation

NOTE: This component must be turned on to complete the installation process. However, due to the sequence that this component is enabled related to IIS components, HTTP Activation may not work correctly. This situation occurs because the web server has not correctly connected to the application server. We recommend that you run the following command before installing the application server.

1. In administrator mode, open a **Command Prompt** window.
2. Navigate to C:\Windows\Microsoft.Net\Framework\v4.0.30319>.
3. At the command prompt, type aspnet_regiis.exe –iru.

   For example: C:\Windows\Microsoft.Net\Framework{64}\v4.0.30319>aspnet_regiis.exe –iru

Other Supported Software

NOTE: Proficy Portal and all features associated with this product are no longer supported with Proficy Workflow.

- VMWare Server or VMWare ESX Server

  NOTE: VMWare servers are supported to use any of the supported operating systems.

  IMPORTANT: Advanced features of ESX Server (that is, VMotion, VMWare VMFS, and Clustering support) are not supported.
- Hyper-V virtualization system for x86-64 systems
- Remote Desktop Session Host (Terminal Services)
- Proficy Historian 3.5 or greater

Optional Requirements

- Microsoft® Silverlight™ Runtime 5.0 and the Silverlight SDK 5.0

  NOTE: Silverlight is required to access and develop forms and displays in the Silverlight Designer, and to view Silverlight forms and displays in the Global Viewer.

  IMPORTANT: Support for Silverlight and Silverlight forms will be discontinued with the next major release of the software.

Web Server Software Requirements

This section describes the software requirements for your installation.

NOTE:

- You must install the Proficy application server before installing the web server.
- Connecting the web server to the Proficy application server in a failover cluster environment is not currently supported.

Operating System Options

The following operating systems are supported:

- Microsoft® Windows® Server 2008 (64-bit only)
- Microsoft® Windows® Server 2008 R2
- Microsoft® Windows® Server 2012 Standard (64-bit)
- Microsoft® Windows® Server 2012 R2 (64-bit)

Other Requirements

If the following products are not installed on your system, they will be automatically installed. If you are using a version of these products that is not supported, the installation process will stop. You must uninstall the incorrect version, and then start the installation process again.

- Java™ SE Development Kit 7, version JDK 1.7, upgrade 71

- Node.js® version 0.10.33-0.10.36 (64-bit)

  NOTE: Previous installations of this product may have left undesired information in the PATH environment variables and may not have removed all installed files. This information must be removed before installing the web server.

Browser Requirements

- Microsoft® Internet Explorer 11 or greater
- Mozilla® Firefox® 28 or greater

  NOTE: In order to avoid certificate errors when using this browser, we recommend that you purchase your own certificates or follow the browser's instructions on trusting certificates.
- Google Chrome 29 or greater

Extension (Workflow and User) Servers Software Requirements
This section describes the software requirements for your installation.

Workflow and user extension servers have the same software requirements as the main application server installation.

Operating System Options
The following operating systems are supported:

- Microsoft® Windows® 7 Professional (32- or 64-bit)
- Microsoft® Windows® 8 (64-bit)
- Microsoft® Windows® Server 2008 SP2 (32-bit only)
- Microsoft® Windows® Server 2008 R2 (64-bit)

  NOTE: Terminal server environments are supported only on Windows Server 2008 R2 (64-bit).
- Microsoft® Windows® Server 2012 Standard (64-bit)
- Microsoft® Windows® Server 2012 R2 (64-bit)

SQL Server Options

The Proficy Workflow installation automatically selects the default SQL Server instance. If SQL Server 2012 and SQL Server 2008 are both installed, SQL Server 2008 may be the default instance. In this scenario, if you want to use SQL Server 2012 instead, you must select this instance as the default as part of manually configuring your SQL Server settings. For more information, see the topic corresponding to the type of installation you will be performing.

The Proficy project is installed into this SQL Server database. SQL Server can be installed on a different computer that is also on the domain or workgroup; however, you must ensure that network configurations allow appropriate machine communication.

SQL Server must be configured with both Windows and SQL Server authentication.

The following SQL Server systems are supported:

NOTE: The Proficy project is installed into this SQL Server database. SQL Server can be installed on a different computer that is also on the domain or workgroup; however, you must ensure that network configurations allow appropriate machine communication.

- Microsoft® SQL Server 2008 Standard or Enterprise Edition (32- or 64-bit)
- Microsoft® SQL Server 2008 R2

  NOTE: Changes to the SQL Server database recovery model have occurred. For more information, please visit the GE Intelligent Platforms Knowledge Base website at http://support.ge-ip.com/support/index?page=kbchannel, and then search for the related article, KB16204.
- Microsoft® SQL Server 2008 Express

NOTE: If you are using SQL Server Express with the Proficy application server, you cannot use the Proficy Reporting Database.

- Microsoft® SQL Server 2012 Enterprise (32- or 64-bit)
- Microsoft® SQL Server 2012 Business Intelligence (32- or 64-bit)
- Microsoft® SQL Server 2012 Standard (32- or 64-bit)
- Microsoft® SQL Server 2012 Express (32- or 64-bit)

NOTE: In order for Proficy Workflow to connect to any edition of Microsoft® SQL Server 2012, you must configure SQL Server to enable the *sysadmin* role for the applicable login account. For more information, see Enable Connection between Proficy Workflow and SQL Server 2012 on page 30.

Other Requirements

- Microsoft® .NET Framework 4.5 (Full Framework)

  NOTE: Custom display or form assemblies that target earlier versions of .NET will continue to function as before. However, saving changes made to such custom assemblies requires that they be upgraded, which is accomplished in different ways, based on the version of .NET:

  - For an assembly that pre-dates .NET 4.0, you must upgrade the assembly when you open it. Failure to do so results in an error and the inability to save the edited assembly.
  - For an assembly that targets .NET 4.0, the assembly is upgraded automatically when opened, and changes to such assemblies can be saved as before.

  Service providers that target versions of the .NET framework before version 4.5 must be recompiled targeting .NET 4.5.
- Microsoft® AD LDS (Active Directory Lightweight Directory Service) or ADAM (Active Directory Application Mode) with SP1 (available from http://www.microsoft.com/downloads/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en)

  NOTE:

  - If you are using Microsoft Windows 7, Windows Server 2008, or Windows Server 2012, using AD LDS is recommended, which can be added as Windows components/features in the **Programs** applet of the **Control Panel**.
  - For demonstration, evaluation, or pilot systems, you can use Simulated Directory mode rather than using ADAM or AD LDS. In this mode, the system functions the same way. However, you must use ADAM or AD LDS to run large systems that have hundreds of clients connecting simultaneously.
- Microsoft® Excel 2007 or 2010. To use Excel 2007, you must manually install the Primary Interop Assemblies (for Import/Export operations). These assemblies are included in the Excel 2010 installation.

  - http://msdn.microsoft.com/en-us/library/kh3965hw.aspx
  - http://www.microsoft.com/downloads/details.aspx?familyid=59DAEBAA-BED4-4282-A28C-B864D8BFA513&displaylang=en
  - http://technet.microsoft.com/en-us/library/cc179091.aspx
- Microsoft® Internet Explorer 7 or greater

Optional Requirements

- Microsoft® Silverlight™ Runtime 5.0 and the Silverlight SDK 5.0

  NOTE: Silverlight is required to access and develop forms and displays in the Silverlight Designer, and to view Silverlight forms and displays in the Global Viewer.

  IMPORTANT: Support for Silverlight and Silverlight forms will be discontinued with the next major release of the software.

Client-only Software Requirements

This section describes the software requirements for your installation.

Requirements

A client-only machine contains only the Proficy Workflow client application and must connect to another machine that has the Proficy application server installed.

NOTE: If you have a client-only installation, it must be the same version as the server it is connected to.

- The following operating systems are supported:
  - Microsoft® Windows® 7 Professional (32- or 64-bit)
  - Microsoft® Windows® 8 (64-bit)
  - Microsoft® Windows® Server 2008 R2 (64-bit)
  - Microsoft® Windows® Server 2008 SP2 (32-bit only)
  - Microsoft® Windows® Server 2012 Standard (64-bit)
  - Microsoft® Windows® Server 2012 R2 (64-bit)
- Microsoft® .NET Framework 4.5 (Full Framework)

  NOTE: Custom display or form assemblies that target earlier versions of .NET will continue to function as before. However, saving changes made to such custom assemblies requires that they be upgraded, which is accomplished in different ways, based on the version of .NET:

  - For an assembly that pre-dates .NET 4.0, you must upgrade the assembly when you open it. Failure to do so results in an error and the inability to save the edited assembly.
  - For an assembly that targets .NET 4.0, the assembly is upgraded automatically when opened, and changes to such assemblies can be saved as before.

  Service providers that target versions of the .NET framework before version 4.5 must be recompiled targeting .NET 4.5.
- Microsoft® Excel 2007 or 2010. To use Excel 2007, you must manually install the Primary Interop Assemblies (for Import/Export operations). These assemblies are included in the Excel 2010 installation.
  - http://msdn.microsoft.com/en-us/library/kh3965hw.aspx
  - http://www.microsoft.com/downloads/details.aspx?familyid=59DAEBAA-BED4-4282-A28C-B864D8BFA513&displaylang=en
  - http://technet.microsoft.com/en-us/library/cc179091.aspx
- Microsoft® Internet Explorer 7 or greater
- For web-based forms, Microsoft® Internet Explorer 10 or greater is required

  NOTE: Internet Explorer 10 is only supported on the following operating systems:

  - Windows® 7 SP1
  - Windows® 8
  - Windows® Server 2008 R2 with SP1
  - Windows® Server 2012

Optional Requirements

- Microsoft® Silverlight™ Runtime 5.0 and the Silverlight SDK 5.0

  NOTE: Silverlight is required to access and develop forms and displays in the Silverlight Designer, and to view Silverlight forms and displays in the Global Viewer.

  IMPORTANT: Support for Silverlight and Silverlight forms will be discontinued with the next major release of the software.

Reporting Database Software Requirements
This section describes the software requirements for your installation.

- The following operating systems are supported:
  - Microsoft® Windows® 7 Professional (32- or 64-bit)
  - Microsoft® Windows® 8 (64-bit)
  - Microsoft® Windows® Server 2008 R2 (64-bit)
  - Microsoft® Windows® Server 2008 SP2 (32-bit only)
  - Microsoft® Windows® Server 2012 Standard (64-bit)
  - Microsoft® Windows® Server 2012 R2 (64-bit)
- The following SQL Server systems are supported:
  - Microsoft® SQL Server 2012 Enterprise, Business Intelligence, or Standard (32- or 64-bit)
  - Microsoft® SQL Server 2008 Standard or Enterprise Edition (32- or 64-bit)

    NOTE:

    - SQL Server Integration Services must be installed with SQL Server.
    - If you are using SQL Server Express with the Proficy application server, you cannot use the Proficy Reporting Database.
- Microsoft® Internet Explorer 7 or greater

Web Task List Software Requirements
This section describes the software requirements for your installation.

The following list describes the software required to install the Web Task List.

- The following operating systems are supported:
  - Microsoft® Windows® 7 Professional (32- or 64-bit)
  - Microsoft® Windows® 8 (64-bit)
  - Microsoft® Windows® Server 2008 SP2 (32-bit only)
  - Microsoft® Windows® Server 2008 R2 (64-bit)
  - Microsoft® Windows® Server 2012 Standard (64-bit)
  - Microsoft® Windows® Server 2012 R2 (64-bit)
- Microsoft® .NET Framework 4.5 (Full Framework)

  NOTE: Custom display or form assemblies that target earlier versions of .NET will continue to function as before. However, saving changes made to such custom assemblies requires that they be upgraded, which is accomplished in different ways, based on the version of .NET:

  - For an assembly that pre-dates .NET 4.0, you must upgrade the assembly when you open it. Failure to do so results in an error and the inability to save the edited assembly.
  - For an assembly that targets .NET 4.0, the assembly is upgraded automatically when opened, and changes to such assemblies can be saved as before.

  Service providers that target versions of the .NET framework before version 4.5 must be recompiled targeting .NET 4.5.
- Microsoft® Internet Explorer 7 or greater
- Microsoft® Silverlight Runtime 5.0

Server Clustering and Failover Software Requirements
This section describes the software requirements for your installation.

Operating System Options

The following operating systems are supported:

- Microsoft® Windows® Server 2008 R2 (64-bit)

- Microsoft® Windows® Server 2012 Standard (64-bit)
- Microsoft® Windows® Server 2012 R2 (64-bit)

Virtual Machine Support
As part of our development testing and qualification, we make extensive use of VMWare workstations, VMWare ESX servers, and Microsoft HyperV.

The software is qualified on a variety of operating systems:

- Windows 7
- Windows Server 2008 SP2
- Windows® Server 2008 R2
- Windows® Server 2012

Our most current VM testing is based on VMWare Workstation 6.0; VMWare ESX server 3.5, 4.0, 4.1; and Microsoft HyperV on Windows 2008 R2 and Windows 2012. VMWare ESX and Microsoft HyperV are currently very reliable virtualization platforms. Proficy Workflow does not target any specific hardware or virtualization platform.

GE Intelligent Platforms supports the functional operation of the product if it is run on a supported operating system in VMWare ESX or Microsoft HyperV, and will address any functional issues related to the software in those environments.

GE Intelligent Platforms cannot guarantee performance of the software in a virtualized environment due to the wide range of parameters associated with the hardware, configuration, memory settings, third-party software, and number of virtual machines running, all of which can affect performance. GE Intelligent Platforms does not assist with the proper configuration of virtualization software. It is up to the customer to ensure that the performance of the image has been optimized with the correct settings and configuration before we can provide support on performance related issues.

It is your responsibility to ensure that the performance of the Proficy Workflow software and application are adequate to meet the needs of your run-time environment. GE Intelligent Platforms does not support issues related to functionality that is not available as a result of running in a virtual machine. GE Intelligent Platforms cannot guarantee the functionality or performance of third-party products used with the application. You must check with the vendor of those applications for their ability to run in a virtualized environment.

Each virtual machine instance that is using our software is required to have a valid license. Any customer using virtualization needs to use a software key.

Pre-installation Considerations

In addition to system requirements, you should be aware of several other areas of consideration before installing Proficy Workflow.

Architecture Considerations

If you are installing a Proficy application server or extension server (that is, Workflow or User) on a 64-bit computer, you can configure the server for either 32-bit or 64-bit operation.

When installing for the first time, you indicate your preference at installation time, whereas when upgrading, the installation maintains the existing configuration by default. In both cases, however, components that enable either 32- or 64-bit server operation are installed to your system, and you can subsequently use the **Configure Server** tool to change between 32- and 64-bit mode, as outlined under Change architecture mode on page 70.

If you are using a 64-bit operating system and are installing to the default installation location, do not remove (x86) from the default installation directory path. Windows detects that Proficy Workflow is a 32-bit process, and defaults to C:\Program Files (x86)\Proficy.... If you remove (x86) from the default installation location on a 64-bit operating system, your installation will fail.

NOTE: Client-only installations are restricted to 32-bit operation, regardless of installation location.

Default Installation Locations by Architecture Type

By default, program installation locations by architecture type are as follows:

- 64-bit: C:\Program Files\Proficy\Proficy Workflow\Program
- 32-bit: C:\Program Files (x86)\Proficy\Proficy Workflow\Program

Determining Current Architecture Mode

Any time after installation, you can consult the **Processes** tab of **Windows Task Manager** to ascertain the architecture mode that the Proficy Server service is currently running under. If operating in 32-bit mode, the ProficyServer.exe listing is appended with **32*.

Implications for Product Options and Service Providers

The **ProficyPackager** and **ProficyInstaller** tools are available in both the 32-bit and 64-bit installation locations, and you can package and install product options from either folder. When you run Proficy application server or Proficy client, the need to update product options is automatically determined depending on where you installed the product options from. For example, if you package and install a product option from the 64-bit folder, and run the 64-bit Proficy application server, the Proficy client (which runs only in 32-bit mode) will automatically invoke the **ProficyUpdater** tool to update the product option in the 32-bit folder.

Product option assemblies that are loaded by the Proficy client (for example, configuration screens and displays) must target either *Any CPU* or *x86*, because Proficy client runs only in 32-bit mode.

Implications for running service providers are as follows:

- Service providers that were built using a target architecture of *Any CPU*, can be run in either 32- or 64-bit mode.
- Service providers that were built to target x86 (32-bit) architecture can be run only in 32-bit mode.

  NOTE: This is typically the case when the service provider references a C++/CLI library with 32-bit dependencies.
- Service providers that were built to target x64 (64-bit) architecture can be run only in 64-bit mode.

  NOTE: This is typically the case when the service provider references a C++/CLI library with 64-bit dependencies.

Maintenance of Configuration Settings

After an upgrade installation on a 64-bit computer that was previously running the 32-bit version of Proficy Workflow, the server configuration file in the 32-bit location (C:\Program Files (x86)\Proficy\ProficyWorkflow \Program\ProficyServer.exe.config) retains all pre-existing system settings, whereas the configuration file in the 64-bit location (C:\Program Files\Proficy\ProficyWorkflow\Program\ProficyServer.exe.config) contains new default settings. If you want to switch from 32-bit to 64-bit operation but continue using your previously implemented configuration settings, you should migrate the settings in the 32-bit version of the configuration file to the 64-bit version.

Windows Services for Proficy Workflow

There are several Windows services that must be running in order for Proficy Workflow to function properly.

Standard Server Installation Services

These services are installed as part of Proficy Workflow. They are configured to start automatically on system startup.

NOTE: If these services do not start up automatically, you can manually start them, in any order, from the Control Panel's Administrative Tools.

Proficy Server	Supports most of this product's functionality. It must be running at all times.
Proficy STS	Authenticates application users. It must be running at all times.
Proficy Publisher Service	Publishes data to the active directory (Microsoft ADAM/LDS). It must be running if you are using ADAM/LDS.
Proficy Certificate	Generates security certificates.

Support Server Installation Services

The following services are available from other applications:

SQL Server	This service runs on whichever machine the SQL Server is installed on, including the machine the Proficy application server is installed on.
SOAAdam	This service is available if you are using a Microsoft ADAM/LDS instance.

Configure Predix to use Active Directory for the web server

To connect your web server, you must complete configuration settings for your active directory.

Configuration Files

NOTE: A system administrator must modify the properties within the authentication provider's configuration files to ensure Predix can work with the web server's active directory.

You can find the related configuration files in the following directory: <installdir>\Program Files\Proficy\Proficy Vision\Predix\kernel\dsp\conf.

File: dsp.authentication.ldap.conf

JAAS-based LDAP: Configuration Required

You can modify this file to ensure the appropriate parameters are configured for your environment.

dsp.authentication.ldap.jaas.realm=ldap

Specify the authentication realm assigned to the provider, which should be set to the full name of the active directory domain, such as, edmdev.ge.com.

dsp.authentication.ldap.jaas.rank=1

Specify rank used to break ties if modules with the same realm exist in the container.

dsp.authentication.ldap.connection.url=ldap://3.26.202.11:389

Specify the URL used to connect to the LDAP server. It supports both the "ldap://" and "ldaps://" scheme.

dsp.authentication.ldap.connection.username=CN=geftest,OU=Special,OU=Edmonton,DC=edmdev,DC=ge,DC=com

Specify the user name required to authenticate the initial LDAP bind. If no user name is specified, the connection is anonymous. For active directory, a user name is required.

dsp.authentication.ldap.connection.password=******

Specify the domain password used to authenticate the initial LDAP bind.

dsp.authentication.ldap.user.base.dn=OU=Special,OU=Edmonton,DC=edmdev,DC=ge,DC=com

Specify the distinguished name used to find the base directory where users are located.

dsp.authentication.ldap.user.filter=(sAMAccountName=%u)

Specify the filter used to find users in the LDAP directory.

dsp.authentication.ldap.user.search.subtree=true

Set to true if the user search should descend into sub trees recursively.

dsp.authentication.ldap.role.base.dn=OU=Special,OU=Edmonton,DC=edmdev,DC=ge,DC=com

Specify the based X500 distinguished name used to look for roles.

dsp.authentication.ldap.role.filter=(uniqueMember=CN=%u)

Filter used to look for roles.

dsp.authentication.ldap.role.name.attribute=cn

Specify the role attribute that contains the string used to identify the role.

dsp.authentication.ldap.role.search.subtree=true

Set to true if the role search should descend into sub trees recursively.

dsp.authentication.ldap.authentication=simple

Specify the authentication method to use with the LDAP server, which is either "none" or "simple". The default is "simple".

File: dsp.authentication.core.conf

This file requires that only one parameter be modified for your environment.

dsp.authn.manager.realm.isRealmFirst=true

Modification required for active directory support.

dsp.pluggableauthentication.implName=com.ge.dsp.proficy.pluggableid.PAM

Specifies the plug-in to use for the Pluggable Authentication Service. Do not modify.

dsp.authn.manager.realm.separator=@

Character that is used to separate the realm from the user name. Do not modify.

Security Certificates

Security certificates must be installed on all Proficy application server and client machines in your system.

Security certificates are used to protect your identifiable information and to protect your computers from unsafe software. A certificate is a statement verifying the identity of a person or the security of a website.

During the application installation process, certificates are automatically generated using the Proficy Certificate service. Alternatively, you can select a security certificate for the ProficyPlatform, Proficy STS, and SSL/TLS server services.

You can configure the following types of certificates:

- Self-signed certificates generated during the installation process.
- Existing certificates that you installed and configured for a previous version of the application.

The Proficy client computer must verify and trust the identity of the server before it can securely send a user's login and password credentials and complete the authentication process. To establish this trust, the client must trust the root of the server's certificate. That is, the client must have the certificate of the Certificate Authority (CA) that issued the server certificate in their Trusted Root Certificate Authorities store.

When you generate new certificates or use existing certificates, the following steps will occur.

- Install a trusted root certificate.
- Install a certificate to a Certificate Store (by default, the Personal Certificate Store).
- Install generated self-signed certificates to the proper Certificate Store(s).
- Register the SSL certificates to IP ports assigned to the Proficy application server.
- Provide the option to use existing certificates configured for a previous version of the application.

IMPORTANT: The SSL/TLS Server Certificate must be unique to each server.

For information on changing or updating security certificates post-installation, see Modify security certificates on page 64.

Security Certificate Options

There are several server security certificate options for you to choose from. These options differ slightly depending on the type of server you are configuring.

Full Server Certificate Options

The following table describes the type of security certificates available for use on a single full server.

NOTE: Starting with Proficy Workflow 2.5, legacy certificates are no longer supported.

Option	Description
Generate new and unique certificates	This option allows you to automatically generate new self-signed certificates. If you are installing in a multiple server or server failover cluster environment, more configuration is required on those servers.
Import certificates	This option allows you to import certificates that were generated on and exported from a main server. This option is used when installing extension servers in a multiple server or server failover cluster environment and can also be used to install the same certificates on multiple single servers. After selecting this option, in the **Certificate File** field, click **Browse** to locate and select the zip file containing the security certificates that you exported.
Use the certificates already installed on this server	Post-installation configuration only: this option is available when you use the **Configure Certificates** tool. It allows you to use existing certificates that were installed with a previous version of this application. To import certificates, select the **Enable certificate import for advanced configuration** check box, and then click **Import**. Click **View** to view each certificate after it has been imported.

Extension Server Certificate Options

The following table describes the type of security certificates available for use on an extension server; that is, in a multiple server or server failover cluster environment.

Option	Description
Import certificates	This option allows you to import the certificates that are installed on the main server. You must manually export the certificates from the main server to a defined location, and then import the certificates to the extension server. This option will generate an SSL certificate if the main server is using certificates generated by the installation.

Option	Description
	After selecting this option, in the **Certificate File** field, click **Browse** to locate and select the zip file containing the security certificates that you exported.

Client Certificate Options

When you install a remote client, the certificates that you installed on the server (that is, the single server or the main server in a multiple server or server cluster environment) are automatically downloaded and installed on the client.

If the certificates on the server are modified in any way, each client connected to the server will also have to be updated so that the certificates match those on the server.

Mozilla® Firefox® Browser Support

You may receive errors when using Proficy Vision in Firefox. In order to avoid certificate errors when using this browser, we recommend that you purchase your own certificates or follow the browser's instructions on trusting certificates.

Proficy Vision Certificate Support

Proficy Vision installs the web server with a self-signed certificate. We recommend that you use a SSL certificate from a Certificate Authority.

If you are using self-signed certificates, you must install them on client machines in order to access the web server. Download the certificate to your client machine by accessing http://yourservername:8008/Certs/Help For more information, see Using self-signed certificates for the web server on page 25.

Using SSL certificates purchased from a Certificate Authority (CA)

This procedure demonstrates how to use a SSL certificate from a real certificate authority to use with Proficy Vision.

1. Obtain the SSL certificate and certificate key.
2. Copy the key and certificate files to the following directory: <installpath>\WebServer\ssl
3. From the configuration file, <installpath>\WebServer\serverConfig.json, add the file names to:
   a) sslKeyFile: "./ssl/key file name"
   b) sslCertFile: "./ssl/certificate file name"
   c) If the SSL key is encrypted, update sslPassphrase with the key password. If the SSL key is not encrypted, ignore this setting.

Using self-signed certificates for the web server

If you are using self-signed certificates, you must install them on client machines in order to access the web server. Download the certificate to your client machine by accessing http://yourservername:8008/Certs/Help

1. From the root certificate link, save the certificate file as Root.cer.
2. Open a command prompt window.
3. At the command prompt, enter **mmc**.
4. From the **File** menu, click **Add/Remove Snap-in**.
5. Select **Certificates**, and then click **Add**.
   The **Certificates snap-in** dialog box appears.
6. Select **My user account**, click **Finish**, and then click **OK**.
7. Expand **Certificates - Current User** > **Trusted Root Certificate Authorities** > **Certificates**.
8. Right-click **Certificates**, select **All Tasks**, and then click **Import**.
   The **Certificate Import Wizard** appears.

9. To start, click **Next**, and then in the **File Name** field, enter Root.cer.
10. Click **Next**.
11. Select Place all certificates in the following store.
12. Click **Browse**.
13. Select **Trusted Root Certificate Authorities**.
14. Click **Next**, and then click **Finish**.
15. Close all open windows.
16. Restart your browser, and then connect to the server.

NOTE: For Firefox users, perform the following steps:

- Navigate to your web server; for example, https://yourservername.

  The **This Connection is Untrusted** page appears.
- Expand the section, **I Understand the Risks**.
- Click **Add Exception**.
- Click **Confirm Security Exception**.

  NOTE: If this page does not refresh, clear the check box **Permanently store this exception**, and then try again.
- You can now access the server from this browser.

Firewall Ports

During server installations, the installation setup detects whether there is a firewall on the computer. You must either disable the firewall or configure it to allow communication with the server.

The following is a list of the inbound TCP ports you can open on the server computer to allow communication:

- 8444
- 8443
- 8012
- 8112
- 8020
- 8201
- 8202
- 8203
- 8204

The Proficy Vision web server uses the following TCP ports to allow communication:

- 443 (default; can be configured): used for secure access to the web server
- 8008: used to retrieve self-signed security certificates

IMPORTANT: For information related to upgrading and ports, see Ports and IIS on page 73.

Database Backup and Restore

Proficy Workflow utilizes SQL Server to store information. In order to ensure that the integrity of the information is maintained, it is important to back up your database on a regular basis.

In addition to backing up and restoring your SQL Server database, maintenance plans can assist in keeping your systems up and running. Refer to your SQL Server manual or Microsoft's web site for additional information on backing up, restoring, and maintaining your SQL Server database.

Multiple Servers

Proficy Workflow provides the ability to install across multiple servers, each of which hosts a set of services. A multi-server environment is transparent and appears to be a single server to remote clients.

Operational Overview

In a multi-server Proficy site, each installed product option may be hosted by a different server, and each server must be able to determine where each product option resides. To accomplish this, the servers refer to a shared configuration data model. Client programs, such as forms or custom clients, can connect to any server and be redirected to the server that is hosting the service(s) required for the product option in question. Because client programs communicate with product options using service methods and events, neither the user nor the client program is aware of which server is hosting the product option.

Multi-server Considerations

Configuring your system with multiple servers, whether on a single machine or on multiple machines, provides various benefits.

- If you want to run a 32-bit service provider but your system is configured as 64-bit, you can configure a user server to host the 32-bit service provider.
- If you want to run a non-essential service provider but doing so may cause your system to crash, you can configure a user server to host the service provider, thus isolating it from the SOAServer and preventing a system failure.
- If you want to conduct performance monitoring, you can configure a user server and divide the service providers into groups to determine which service provider(s) is causing memory leaks.
- A user server that hosts custom service providers can be restarted more quickly than a single SOAServer that hosts all of your service providers and product options. When new service providers are added to the user server, only the user server needs to be restarted, reducing down time.
- 32-bit machines allow only 3 GB of memory per process. Running multiple servers provides a workaround to this memory constraint.

Configuring your multi-server system on a single machine provides various benefits over configuring a multi-machine system.

- Configuring multiple servers on a single machine is faster and easier, especially in terms of security certificates. After the security certificates have been configured for the main SOAServer, those certificates apply to all servers on that machine. If you configure servers on multiple machines, you must configure security certificate on each machine.
- Communication times between servers and clients is faster on a single machine setup.
- Configuring multi-server failover clustering is faster and easier.

Configuration Overview

In addition to the primary SOAServer instance, which by default hosts both the Core and Workflow product options, you can configure extension servers. All of these servers can be configured on either separate machines or on a single machine. These servers can take the form of a Workflow server, to host the Workflow product option, and/or one or more User servers, to host product options other than the Core and Workflow options. Upon installing a Workflow server, the Workflow product option and related services automatically move from the SOAServer instance to the Workflow server instance. Likewise, upon installing a User server, product options other than the Core and Workflow options automatically move to the User server instance.

NOTE: Workflow and User servers should not be installed at multiple sites across a WAN.

After installing extension servers, you can use the **Configure Site** tool to move product options and related services among server instances.

NOTE: The Core product option and services must reside on the SOAServer instance.

Beginning with Proficy Workflow 2.1, you can also designate whether servers and/or product options are essential to your use of the program, as well as disable any product options designated as nonessential.

NOTE: The Core and Workflow product options and services and the servers that host them cannot be designated as nonessential.

The designation of servers and production options as either essential or nonessential and the state and accessibility of servers has implications for the health of the site and, therefore, the ability to log in and use the Proficy Workflow program. For more information, see System Health and Program Use on page 4.

For more information about implementing a multiple-server installation of Proficy Workflow, see Architecture Considerations on page 20, Multiple Server Installation on Multiple Machines on page 40, and Server Clustering and Failover on page 28.

Server Clustering and Failover

Proficy Workflow provides the ability to implement Microsoft® Windows Clustering, which allows you to configure your server environment to be fault tolerant.

Proficy Workflow allows you to configure a *failover* cluster to maintain a consistent image of the cluster on all nodes. It also allows nodes to transfer resource ownership on demand.

A cluster is a group of independent computer systems working together as a unified computer resource. A cluster provides a single name for clients to use, a single administrative interface, and guarantees that data is consistent across nodes.

Proficy Workflow works with the Microsoft Failover Cluster Manager to ensure high availability of the Proficy application server. If the primary server node in the cluster experiences difficulties, Proficy Workflow is automatically started on another node to take over (a process known as failover). Server high availability is managed through the Microsoft Cluster Manager.

The following information will guide you through the deployment of Proficy Workflow in a clustered environment.

1. Overviews of the validated and supported cluster configurations.
2. Instructions for using the Microsoft Failover Cluster Manager to create a cluster.
3. Instructions for installing the Microsoft Failover Cluster Manager.
4. Instructions for configuring the Microsoft Failover Cluster Manager.
5. Instructions for configuring the primary server.
6. Instructions for exporting security certificates from the primary cluster server in preparation for installing them on the failover server.
7. Instructions for configuring the failover server.

Assumptions

It is assumed that the reader has a thorough knowledge of the following information:

- Microsoft® Failover Clustering
- Microsoft Windows server environments

Additionally, it is assumed that the instructions and guidelines provided by Microsoft for deploying server clusters using Microsoft Windows servers has been followed. For information about server clusters, visit the Microsoft TechNet web site.

SQL Server Clustering

Microsoft SQL Server also supports clustering. For complete information about installing, configuring, and maintaining SQL Server *failover* clustering, see the following topics on the on the Microsoft Development Network web site: SQL Server Failover Cluster Installation (for SQL Server 2012); or, Getting Started with SQL Server 2008 R2 Failover Clustering.

You can also visit the Microsoft Development Network web site to access information about the high availability features supported by the various editions of SQL Server.

Reverse Proxy Configuration for a Web Server

A reverse proxy is a dedicated Internet-facing web server that accepts incoming requests and proxies them to one or more internal servers. This topology is highly recommended when deploying the Web Task List over the Internet, as it provides increased security by limiting and controlling the exposure of internal servers and services.

Certificate Requirements

The following certificates need to be trusted on the web server.

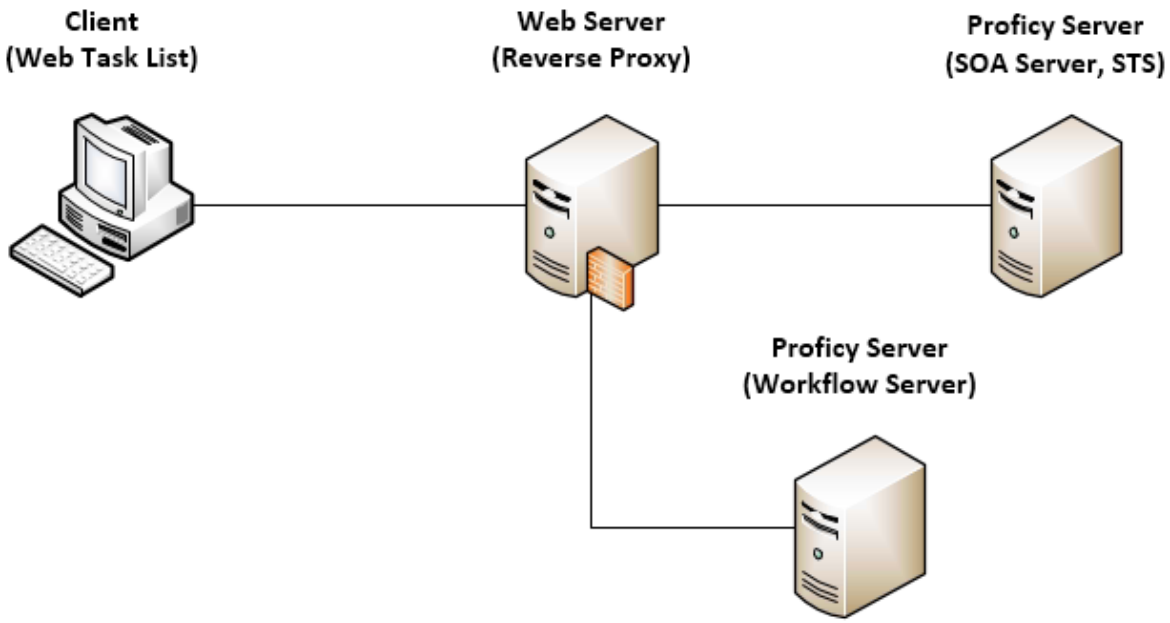
- signing certificate authority
- Proficy STS

Prerequisites

In order to configure a web server as a reverse proxy for the Web Task List, you must ensure that several prerequisites are met. These prerequisites are common for both IIS and Apache reverse proxy setups.

- A web server running either:
  - Microsoft IIS v7.0 or v7.5
  - Apache 2.2.20
- Web server is correctly configured with a web site that servers connect to via HTTPS:
  - Web server is accessible via the host name (for example, mywebserver.example.com)
  - Binding for the HTTPS scheme on port 443 is secured using an SSL certificate
  - SSL certificate is signed by a Trusted Root Certification Authority issued in the name of the web server (for example, CN=mywebserver.example.com)

    NOTE: Certificates signed by a self-issued Trusted Root CA will be trusted by clients only if they are also configured to trust the self-issued Trusted Root CA itself.
  - Firewall allows incoming TCP traffic for port 443
- A single server or multi-server installation of Proficy Workflow.
  - Proficy servers are able to serve traffic on all configured ports to external hosts, including any firewalls.
- Web server has been configured to trust the SSL certificates used by the Proficy servers.
  - Certificates may be generated during the Proficy Workflow server installation and can be exported using the Export Certificates tool.
- Web Task List is configured and tested on the intranet.



For more information on configuring a reverse proxy for use with the Web Task List, see Web Task List Deployment on page 53.

Enable Connection between Proficy Workflow and SQL Server 2012

In order for Proficy Workflow to connect to any edition of Microsoft® SQL Server 2012, you must configure SQL Server to enable the *sysadmin* role for the applicable login account.

If you are using Windows authentication for Proficy Workflow, this account is by default *NT AUTHORITY\SYSTEM*, which is predefined in SQL Server.

For increased security when using Windows authentication, you can modify the properties for the Proficy Server service after installing Proficy Workflow, to define a custom login name and credentials. (For more information, see Microsoft® Windows help.) Another alternative is to select SQL Server authentication when installing Proficy Workflow. In either of these scenarios, you must add the user-specified login account to SQL Server, and then enable the *sysadmin* role for that account.

For information on adding a login account to SQL Server, see the Microsoft® SQL Server help. The following procedure outlines the steps for enabling the *sysadmin* role for a login account in SQL Server. Both of these processes can be done either before or after installing Proficy Workflow.

1. On the machine that SQL Server 2012 is installed to, open SQL Server Management Studio.
2. In the navigation tree, expand the **Security** branch, and then the **Login** branch.
3. Under the **Login** branch, right-click the applicable entry, and then select **Properties**.
   The **Login Properties** dialog box appears.
4. In the **Select a page** pane, click **Server Roles**.
5. In the **Server roles** pane, select the **sysadmin** check box, and then click **OK**.

License Management

The Proficy License Manager provides a single, easy-to-use tool to both view and manage online software licensing.

To access the online help for the Proficy License Manager, perform the following steps.

NOTE: For more information regarding licensing, see http://support.ge-ip.com/licensing.

From the desktop, select **Start** > **Programs** > **Proficy Common** > **License Documentation**.

The Proficy License Manager online help opens.

Performance Counters

Windows performance counters are exposed as objects with counters. The counters are grouped into two categories: DTL and Events.

Installation

When the application server is installed, the performance counters are installed automatically and uninstalled when the server is uninstalled.

DTL Counters

You can use DTL counters in Proficy Workflow.

Counter Name	Description
DTL Pending Packets Acknowledged	Shows how many non-specific packet acknowledgements are in the queue. If this number starts increasing, it indicates that DTL is having difficulties processing.
DTL Received Packets Queued	Monitors the queue from the RxThread to PacketProcessThread. If you are generating many events with multiple clients, this counter should increment.
DTL Received Packets Dropped	DTL limits the size of the queue from the RxThread to the PacketProcessThread to a maximum of 1,000 (ReceiveQueueLimit) packets. If the RxThread gets a packet when the queue is full, the packet is dropped, and this counter increments.
DTL Send Packets Queued	Monitors the queue of packets to be sent, which is added to by the BuildPacketThread and emptied by the TxThread. Normally, this queue is not busy. It indicates that something is generating packets faster than they are being transmitted. If your network connection is slow, or is very busy and generating a high volume of events, this counter may increase.
DTL Record Rate Changed	Reports the number of change records per second coming into the DTL subsystem (typically from an event subsystem), which is the event producer side of the multi-server system. When events are generated, this rate counter moves.
DTL Change Records Queued	Monitors the queue of change records coming from the Events subsystem (and possibly others) that are emptied by the BuildPacketThread. Because the BuildPacketThread pauses to try to get multiple changes per packet, this counter should change when there are a high volume of events.
DTL Change Records Dropped	The queue of change records is limited to 1,000. If more change events come in than can fit in the queue, DTL starts dropping change records, and this counter

Counter Name	Description
	increases. Typically, this counter does not move, but if the events are generated fast enough, it may move.

Events Counters
You can use events counters in Proficy Workflow.

Counter Name	Description
Events Queued Messages to Subscribers	Monitors the queue in the events subsystem for the subscribers. Typically, a high volume of events cause this rate counter to increment. If there are *N* subscribers to a given event, there will be *N* Events Queued Messages to Subscribers for each event generated.
Events DTL Subscriptions	Records the number of DTL points being subscribed to. The event subsystem re-uses DTL subscriptions so that multiple event clients requesting the same DTL point create only one subscription. Thus, if there are three ProficyClients subscribing to the WorkflowTaskInstanceEvent, there should be one Events DTL Subscription and three Events Remote Subscriptions.
Events Remote Subscriptions	Records the number of subscribers to events on another server (such as those requiring DTL subscription). The event subsystem re-uses DTL subscriptions so that multiple event clients requesting the same DTL point create only one subscription. Thus, if there are three ProficyClients subscribing to the WorkflowTaskInstanceEvent, there should be one Events DTL Subscription and three Events Remote Subscriptions.
Events DTL Change Rate	Reports the number of events per second being fed to the event subsystem from DTL, which is the subscriber side of the multi-server system. When events are generated, this rate counter changes. The DTL Change Record Rate and the Events DTL Change Rate represent the input side and output side, respectively, of the DTL link for events and, in a stable system, should be the same value (with some room for movement).
Events Messages to Subscribers Rate	Reports the number of events per second being sent to subscribers. In a stable system, if there are *N* subscribers to a given event, the Events Messages to Subscribers Rate will be *N* times the Events DTL Change Rate (assuming only that event is being generated). If the Events Messages to Subscribers Rate is less then *N* times the Events DTL Change Rate,

Counter Name	Description
	the Events Queued Messages to Subscribers should increase.

Log performance counters
Using this procedure, you can write (increment/decrement) to the performance counter.

1. To add performance counting to your system, select the ProficyServer.exe.config file from the following folder: <installdir>\Proficy\Proficy Workflow\Program.
2. By default, the performance counter key is false. To start logging performance, set it to true in the following code.

```
<appSettings>
   <add key="EnablePerformanceCounters" value="false"/>
</appSettings>
```

NOTE: When EnablePerformanceCounters is false, then the logging counters do not increment or decrement. If the value of the key is changed (from either true to false or false to true) after the server is started, the server must be re-started for this change to take effect.

Add or remove performance counters
Using this procedure, you can manually add performance counters to your system, or remove them. You must have administrative privileges in order to perform this action.

1. From the following location, you can add or remove performance counters: <installfolder>/ProficyServer.exe.
2. In ProficyServer.exe, enter the applicable command line.

To...	Enter...
Add counters	<installfolder>ProficyServer[exe] / installperformancounters
Remove counters	<installfolder>ProficyServer[exe] / uninstallperformancounters

IMPORTANT: If the counters are added/deleted (installed/uninstalled) after the server is started, then the server and the performance monitoring tool (perfmon) must be re-started for this change to take effect.

View performance counters
You can view performance counters using the Microsoft Windows **Reliability and Performance Monitor** application.

1. Click **Start** > **Run**.
2. In the **Open** field, enter perfmon, and then click **OK**.
3. From **Monitoring Tools**, select **Performance Monitor**.
   A graph region appears.
4. Right click the graph region, and from the menu, select **Add Counters**.
   The following categories appear: DTL and Events.
5. Expand these categories to view more information.

Installation Procedures

There are various installation options for this software.

Install a single application server and client

The following information guides you through the full installation process of the application server and client.

NOTE: During this installation process, you are required to create an Administrator user. This user is automatically assigned all permissions, which will allow you to create and define your user and security permissions.

1. From the application splash screen, click **Install Proficy Client and Application Server**.

   NOTE: If this splash screen does not appear, run InstallFrontEnd.exe on the root directory of the installation folders.

   The setup wizard appears.
2. Click **Proficy Application Server**.
   The **Proficy Application Server Type** page appears.
3. Select **Core server**, and then click **Next**.
   The **License Agreement** page appears.
4. Review the license agreement, and then click **I Agree**.
   The **Installation Folders and Architecture** page appears.
5. Proceed as applicable based on the architecture of your computer.

If the architecture is...	Then do this...
32-bit	1. Accept the default destination folder or browse for a new location, and then click **Next**. The **AD LDS Integration** page appears.
64-bit	1. Accept the default **Destination Folder (32-bit)**, or browse for a new location. **IMPORTANT:** This is the installation location for 32-bit components. Do not install 32-bit components to the 64-bit installation directory; otherwise, the installation will fail. 2. Accept the default **Destination Folder (64-bit)**, or browse for a new location. 3. Select either 32-bit or 64-bit depending on the architecture in which you want the server to operate. **TIP:** The default is 64-bit, but you may also select 32-bit. If your environment changes after installation, you can use the **Configure Server** tool to change the architecture. 4. Click **Next**. The **AD LDS Integration** page appears.

6. To integrate Active Directory Lightweight Directory Services (AD LDS), do one of the following.

If AD LDS is...	Then...
NOT installed	You are given information regarding its use. If it is not required, then click **Next**.

If AD LDS is...	Then...
Installed in a test and/or development environment	Select the **Do not use Microsoft Directory Services** check box, and then click **Next**.
Installed in a production environment	Click **Next**.

7. If you are using AD LDS, perform the following procedure.
   a) Clear the **Do not use AD LDS** check box.
   b) In the **Directory Instance** section, in the **Name** field, enter an instance name for the ADAM directory.
   c) In the **Port (LDAP)** and **Port (SSL)** fields, enter valid port numbers.
   d) In the **User Credentials** section, in the **Name** field, enter the name of a user that is a member of the local computer's Administrators Group.
   e) In the **Domain** field, enter the name of your company's domain.
   f) In the **Password** field, enter the password for the user you entered in the **Name** field.
8. Specify the SQL Server database settings for this application based on the configuration of your environment.

   NOTE: To create a backup copy of the database that you choose, select **Back up existing databases**. Selecting this option backs up the following databases: SOADB, KSP, and KSPWork.

To configure SQL Server settings...	Then...
Automatically	1. Select the **Use a local database with Windows Authentication** check box. **NOTE:** To use this option, the following SQL Server conditions apply: • Installed locally, AND • Designated as default Local Host, AND • Uses **Windows Authentication** 2. Proceed to step 10 on page 36.
Manually	1. Clear the **Use a local database with Windows Authentication** check box. **NOTE:** To use this option, the following SQL Server conditions must NOT apply: • Installed locally, OR • Designated as default Local Host, OR • Uses **SQL Server Authentication** 2. Proceed to step 9 on page 35. **NOTE:** You can have only one KSP database on a SQL Server.

9. Specify your SQL Server settings, as follows:

   IMPORTANT: Changes to the SQL Server database recovery model have occurred. For more information, please visit the GE Intelligent Platforms Knowledge Base website at http://support.ge-ip.com/support/index?page=kbchannel, and then search for the related article, KB16204.

   a) In the **Server** field, enter or select the name of the SQL Server that you want to connect to.

      NOTE: If the SQL Server is installed locally, enter localhost.
   b) In the **Database** field, enter the name of your SQL Server database, or click the drop-down arrow to search for all databases located on the specified server.

      NOTE: If the specified database does not exist, it will be created for you.

c) From the **Authentication** list, select the type of authentication that you want to use, and then proceed based on your selection.

- If you select **Windows Authentication**, proceed to step 10 on page 36.
- If you select **SQL Server Authentication**, proceed to step 9.d on page 36.

d) Enter the **User Name** and **Password** that are configured for SQL Server authentication, and then proceed to step 10 on page 36

NOTE: Authentication:

- Password character restrictions: <, >, &, '
- The person whose user name is used for SQL authentication must have authority to create new databases.
- For regular database use during run time, a user requires only *db_owner* privileges, not administrative privileges.
- SQL Server must be configured with both Windows and SQL Server authentication.

10. Click **Next**.
The **Security** page appears.
11. Specify the administrator's authentication credentials.
a) In the **Name** field, accept the default name or enter a new name.
b) In the **Password** field, enter a password.

NOTE: If password complexity is enabled and configured, the Administrator password must follow the same rules as defined for user passwords.

c) In the **Confirm Password** field, enter the password again.
12. Optional: You can specify one or more advanced authentication settings. If you do not want to use this feature, clear all check boxes, and then click **Next**.
a) To use GE SSO authentication:

NOTE: For important information on setting up and enabling SSO in your facility and for your users, see GE Single Sign On (SSO) on page 60.

1. Select the **Use SSO (Single Sign On)** check box.

TIP: Selecting this check box displays the SSO Authentication option when a user logs on.

2. In the **SSO Server URL** field, enter the address for your SSO server that you obtained from the **GE SSO Security** group.
3. In the **SiteMinder Agent Server URL** field, enter the address of the web server where SiteMinder is installed.

b) Select the **Change user password** check box if you want to allow users to change their login password at any time.

Selecting this check box displays the Change Password option when a user logs on.

c) Select the **Lock user account** check box, and then set the lockout threshold, duration, and timeframe values. This check box is selected by default.

NOTE: The Administrator account is also restricted by the lockout settings.

d) Select the **Enforce user password complexity rules** check box, then select Simple, Normal, or Advanced to determine the level of complexity for your passwords.

On new installations, this check box is selected by default. When upgrading versions, this check box is cleared by default.

13. Click **Next**.
The **Security Certificates** page appears.
14. Select the appropriate certificate option. For full descriptions of the certificate options, see Security Certificate Options on page 24.
15. Click **Next**.
The **Web Service** page appears.

16. Specify the Internet Information Services (IIS) domain and website where the application server web service is hosted.
    a) In the **Host Name** field, enter your IIS server domain name that you have previously created.
    b) In the **Website** field, select your HTTPS-configured website.
17. Specify the password for the SQL Server user account, KSPUser, that will be created for the web service.

    NOTE: This password must comply with your SQL Server password complexity rules. If you are installing the Proficy Vision web server, you must retain this password to use during that installation process.

    a) In the **Password** field, enter your user account password.
    b) In the **Confirm Password** field, enter your password again.

    If the computer you are installing on has an enabled firewall, the **Firewall** page appears.
18. If required, make note of the port number to open on the firewall, and then click **Next**.

    IMPORTANT: If your system uses a firewall, you must follow the instructions on the **Firewall** page and open ports 8444, 8443, 8012, 8112, 8020, 8201, 8202, 8203, and 8204 to incoming TCP traffic. For information on opening a port in your firewall, see the online help for your Windows operating system.

    The **Installation Confirmation** page appears.

    TIP: At any time during the configuration process, you can click **Back** to return to a previous page to change your settings.
19. Click **Install**.
    The **Installation** page appears, displaying the status of each installation step.

    NOTE: In certain situations, a system restart is required after installation. If this is the case, a corresponding message is displayed among the listed status messages.
20. When the installation is complete, click **Exit**.

    NOTE: If the installation fails, or you want to change a configuration setting after installation completes, you can open the appropriate standalone component to configure the required information. For more information, see this section: Post-installation Configuration on page 63.

The Web Task List is automatically installed with the Proficy application server installation of Proficy Workflow. Users can access the Web Task List using a web browser. For more information, see Connect to the Web Task List on page 57.

Install the Proficy Vision web server

The following information guides you through the installation process of the web server.

IMPORTANT: You must install the Proficy application server before installing the web server. After installing Proficy Vision, an administrative user must log on to the application in the browser before any domain users log on.

1. From the application splash screen, click **Proficy Vision Web Server**.

   NOTE: If this splash screen does not appear, run SetupWebServer.exe on the root directory of the installation folders.

   The **License Agreement** page appears.
2. Review the license agreement, and then click **I Agree**.
   The **Installation Folder** page appears.
3. Accept the default destination folder or browse for a new location, and then click **Next**.
   The **Proficy Application Server** page appears.
4. Configure the details of your Proficy application server, which were previously configured during this server's installation.
   a) In the **Host Name** field, enter the host name of your server.
   b) In the **Server** field, enter or select the name of the SQL Server that you want to connect to.

c) In the **Password** field, enter your KSPUser account password that was set during the installation of the application server.

NOTE: You must use the password that you used during the installation of the Proficy application server.

5. Click **Next**.
The **Digital Certificates** page appears.
6. To access the Proficy Certificate service, in the **Certificate Service** section, enter the credentials of a Windows administrator account on the application server system.

NOTE: The **URL** and **User Name** fields are automatically populated with your system information and Administrator user name. You can choose to modify these fields.

7. Click **Next**.
The **Web Server Details** page appears.
8. Configure the details for your web server.
a) In the **Host Name** field, enter the host name of your server.
b) In the **Port** field, enter an unused port number on which to run the web services.
9. Click **Next**.
The **Installation Confirmation** page appears.

TIP: At any time during the configuration process, you can click **Back** to return to a previous page to change your settings.

10. Click **Install**.
11. When the installation is complete, click **Exit**.

Install a remote client

This information guides you through the process of installing a remote client on a different machine than the Proficy application server.

NOTE: You must install the Proficy application server before you install a client because you require an available server to connect to.

1. From the application splash screen, click **Install Proficy Client and Application Server**.

NOTE: If this splash screen does not appear, run InstallFrontEnd.exe on the root directory of the installation folders.

The setup wizard appears.

2. Click **Proficy Client Only**.
The **License Agreement** page appears.
3. Review the license agreement, and then click **I Agree**.
The **Installation Folder** page appears.
4. Accept the default destination folder or browse for a new location, and then click **Next**.
The **Proficy Application Server** page appears.
5. Specify the name of the application server that this client will connect to.
a) In the **Computer Name** field, enter the name of the computer where the server you want to connect to is installed.

- If you are configuring a full server or in a multiple server environment, enter the name of the computer that the server you want to connect to is installed on.
- If you are configuring a server cluster environment, enter the cluster name used when you set up your cluster.

NOTE: You can also use the IP address for the server if the server uses a static IP address.

b) In the **Instance Name** field, enter the name of the server instance you want to connect to.
c) In the **HTTP Port** field, enter the port number required to allow communication with the server.
d) Click **Next**.

The **Security Certificates** page appears.

6. The security certificates are automatically downloaded from the server that you are connecting to.
7. Click **Next**.
   The **Installation Confirmation** page appears.

   TIP: At any time during the configuration process, you can click **Back** to return to a previous page to change your settings.
8. Click **Install**.
   The **Installation** page appears, displaying the status of each installation step.

   NOTE: In certain situations, a system restart is required after installation. If this is the case, a corresponding message is displayed among the listed status messages.
9. When the installation is complete, click **Exit**.
10. Launch the Proficy client.
    A message appears stating: Proficy updates are available. Click OK to start Proficy Update.
11. Click **OK**, and then, on the **Proficy Update** page, click **Install Updates**.
12. When the updates have finished installing, click **Restart Client**.

Configure multiple servers on a single machine

After installing Proficy application server, you can configure a multiple server environment onto a single machine. This procedure demonstrates how to create two additional server instances; however, you can create as many instances as you require.

IMPORTANT:

- You must exit all instances of Proficy Workflow that are located on the server that you are working on.
- You must stop all running workflows on your system before creating a new server instance and corresponding services.
- For each server instance, use a unique server name (see step 2.b on page 39) and port number (see step 2.f on page 39).

You can configure multiple servers on a single machine for two main reasons.

- If your SOAServer must run on a 32-bit system and is approaching 3 GB of memory usage, then you can move workflows or service providers to a separate server instance to reduce memory usage on the SOAServer.
- If custom service providers are unstable and you must restart SOAServer frequently, you can move customer service providers to separate server instances.

1. Open the **Services** window to stop all services.
   a) From the **Start** menu, go to **Control Panel** > **Administrative Tools** > **Services**.
   b) In the **Name** column, click **Stop the service** for each of the following services: Proficy Server, Proficy STS, Proficy Publisher Service.
2. Create a new server instance using the **Configure Server** tool.
   a) On the server machine, click **Start** > **All Programs** > **Proficy** > **Proficy Workflow** > **Configuration** > **Configure Server**.
   b) In the **Name** field, enter a name for the new server instance, such as WorkflowServer.
   c) In the **Description** field, enter a description for the server instance.
   d) Click the **Advanced Configuration** arrow.
   e) Select **64 bit** to run the server using that architecture.

      NOTE: We recommend that you use a 64-bit system unless your service provider requires 32-bit.
   f) In the **P2P Configuration** section, in the **Port** field, enter a new port number that is not being used for any other server.
   g) Click **Save**.
      The following service has now been created: Proficy Server - Workflow Server.

h) Click **Back**.
i) In the **Name** field, enter a new name for SOAServer, such as UserServer32.
j) In the **Description** field, enter a description for the server instance.
k) Click the **Advanced Configuration** arrow.
l) Select **32 bit** to run the server using that architecture.
m) In the **P2P Configuration** section, in the **Port** field, enter a new port number that is not being used for any other server.
n) Click **Save**.

IMPORTANT: After saving the entered data, port numbers are validated to ensure that the same one is not used more than once. To find a new port number, enter a number that is close to the existing one. If a port is already in use, an error will occur. You are then required to return to the entry fields and enter all data again.

The following service has now been created: Proficy Server - UserServer32.

3. Move service providers to the new server instances using the **Configure Site** tool.
   a) On the server machine, click **Start** > **All Programs** > **Proficy** > **Proficy Workflow** > **Configuration** > **Configure Site**.
   The **Configure Site** tool appears.
   b) In the **Application Server Instances and Enabled Product Options** pane, select the service provider from SOAServer that you want to transfer to the new instances, and then drag and drop it below the new host servers, WorkflowServer and UserServer32. Repeat this process until all service providers have been moved.
   c) Click **Save**.
4. Open the **Services** window to start each service again.
   a) In the **Name** column, click **Start the service** to start each of the following services again: Proficy Server, Proficy STS, Proficy Publisher Service, Proficy Server - UserServer32, Proficy Server - WorkflowServer.
5. Launch Proficy client using either the **Start** menu or desktop icon.

Revert multiple servers on a single machine back to a single server

After configuring multiple servers on a single machine, you can return to your original single server environment.

IMPORTANT: You must exit all instances of Proficy Workflow that are located on the server that you are working on.

1. On the server machine, click **Start** > **All Programs** > **Proficy** > **Proficy Workflow** > **Configuration** > **Configure Site**.
2. In the **Application Server Instances and Enabled Product Options** pane, select the service providers (for example, WorkflowServer and UserServer32) that you want to transfer back to SOAServer, and then drag and drop them. Repeat this process until all service providers have been moved.
3. For each instance, select the **Delete on save** check box.
4. Click **Save**.
   All services will stop running, the service providers will be reconfigured, and the unused server instances and their services will be removed. The remaining services will then start again.

Multiple Server Installation on Multiple Machines

After installing the Proficy application server to host the Core services on one machine, you can set up additional machines to host extension servers in the form of a Workflow server, for the Workflow services, and one or more User servers, for Proficy product options that you may license and/or custom service providers that you develop.

Installing Proficy Workflow on extension servers involves two main steps:

1. Export security certificates
2. Install the extension server(s)

Export server security certificates for an extension server

After installing the main application server in a multiple server environment, you must export the server security certificates and install them on your extension servers. During the extension server installation process, you must import these security certificates.

1. On the main server computer, click **Start** > **All Programs** > **Proficy** > **Proficy Workflow** > **Configuration** > **Export Certificates**.
   The **Export Proficy Server Certificates** page appears.
2. In the **Export Folder** field, enter the path or browse to the location where you want to export the certificates to.
3. In the **Password** field, enter a password to secure the exported certificates, and to use when importing the certificates to the extension server(s).
4. Click **Save**.
   A file with the extension .zip is created, which contains the certificates required on the extension server(s).
5. Click **Exit**.

Install multiple servers

This application provides multiple server capability, allowing you to install the Proficy application server to host the core services on one machine and a Workflow server to host the Workflow services on another machine. You can also choose to install one or more User servers to host other Proficy product options that you may license and/or custom service providers that you develop.

IMPORTANT:

- If you are installing or upgrading an extension server (Workflow or User), you must have already installed or upgraded a Proficy application server of the same version to host the Core services on a separate machine.
- In a multiple server environment, eSOP is automatically installed on the Workflow server.When you upgrade Proficy Workflow or install it again, all sample resource files are overwritten.

1. From the application splash screen, click **Install Proficy Client and Application Server**.

   NOTE: If this splash screen does not appear, run InstallFrontEnd.exe on the root directory of the installation folders.

   The setup wizard appears.
2. Click **Proficy Application Server**.
   The **Proficy Application Server Type** page appears.
3. Click **Extension server**, select one of the following options, and then click **Next**.

To install a...	Click...
dedicated workflow server	Workflow Server
server to host custom service provider	User Server

   The **License Agreement** page appears.
4. Review the license agreement, and then click **I Agree**.
   The **Installation Folders and Architecture** page appears.
5. Proceed as applicable based on the architecture of the computer you are installing to:

If the architecture is...	Then do this...
32-bit	1. Accept the default destination folder or browse for a new location, and then click **Next**. The **Database Configuration** page appears.
64-bit	1. Accept the default **Destination Folder (32-bit)**, or browse for a new location.

If the architecture is...	Then do this...
	NOTE: This is the installation location for 32-bit components. Do not install 32-bit components to the 64-bit installation directory; otherwise, the installation will fail. 2. Accept the default **Destination Folder (64-bit)**, or browse for a new location. 3. Select either 32-bit or 64-bit depending on the architecture in which you want the server to operate. **TIP:** The default is 64-bit, but you may also select 32-bit. If your environment changes after installation, you can use the **Configure Server** tool to change the architecture. 4. Click **Next**. The **Database Configuration** page appears.

6. Specify your SQL Server settings, as follows:

   NOTE: These settings must be the same as for the core server.

   a) In the **Server** field, enter or select the name of the SQL Server that you want to connect to.
   b) In the **Database** field, enter the name of your SQL Server database, or click the drop-down arrow to search for all databases located on the specified server.
   c) From the **Authentication** list, select the type of authentication that you want to use, and then proceed based on your selection.
      - If you select **Windows Authentication**, proceed to step 7 on page 42.
      - If you select **SQL Server Authentication**, proceed to step 6.d on page 42.
   d) Enter the **User Name** and **Password** that are configured for SQL Server authentication, and then proceed to step 7 on page 42.

7. Click **Next**.
   The **Security Certificates** page appears.
8. Import the security certificates as follows:

   IMPORTANT: If you have not already exported the security certificates from the main server, you must do so now before proceeding.

   a) In the **Certificate File** field, enter the path or browse to the location where you exported the security certificates from the main server.
   b) Select the .zip file that you created on the main server, and then click **OK**.
   c) In the **Password** field, enter the password that was set when you exported the security certificates.
9. Click **Next**.
   The imported certificates are listed.
10. Click **Next**.
    If the computer you are installing on has an enabled firewall, the **Firewall** page appears.
11. If required, make note of the port number to open on the firewall, and then click **Next**.

    IMPORTANT: If your system uses a firewall, you must follow the instructions on the **Firewall** page and open ports 8444, 8443, 8012, 8112, 8020, 8201, 8202, 8203, and 8204 to incoming TCP traffic. For information on opening a port in your firewall, see the online help for your Windows operating system.

    The **Installation Confirmation** page appears.

    TIP: At any time during the configuration process, you can click **Back** to return to a previous page to change your settings.

12. Click **Install**.
    The **Installation** page appears, displaying the status of each installation step.

    NOTE: In certain situations, a system restart is required after installation. If this is the case, a corresponding message is displayed among the listed status messages.
13. When the installation is complete, click **Exit**.

    NOTE: If the installation fails, or you want to change a configuration setting after installation completes, you can open the appropriate standalone component to configure the required information. For more information, see this section: Post-installation Configuration on page 63.

One-Click Deployment

One-click deployment allows you to deploy Proficy Workflow to users without running a client installation on their computers. It also provides the ability for a client to update itself when the server is upgraded.

IMPORTANT: Support for one-click installation of Proficy Workflow will be discontinued in a future release of the software. The client installation should be used in place of one-click installation upon discontinuation of the latter.

Before you can use one-click deployment, you must complete the following prerequisites:

- Microsoft® .NET Framework 4.5 (Full Framework)

  NOTE: Custom display or form assemblies that target earlier versions of .NET will continue to function as before. However, saving changes made to such custom assemblies requires that they be upgraded, which is accomplished in different ways, based on the version of .NET:

  - For an assembly that pre-dates .NET 4.0, you must upgrade the assembly when you open it. Failure to do so results in an error and the inability to save the edited assembly.
  - For an assembly that targets .NET 4.0, the assembly is upgraded automatically when opened, and changes to such assemblies can be saved as before.

  Service providers that target versions of the .NET framework before version 4.5 must be recompiled targeting .NET 4.5.
- The NetTCPPortSharing service must be enabled and started.
- Security certificates cannot be deployed remotely. Install your certificates by manually installing a copy of the certificates from the server. Certificates can be copied from the server to a disk or other portable device, and then installed, or by using your IT department's method of delivering and installing files.
- MIME types must be added to each computer in order for the .manifest and .deploy files to work correctly. For more information, see the following:

  - http://msdn.microsoft.com/en-us/library/ms228998(VS.85).aspx
  - http://msdn.microsoft.com/en-us/library/ms752346.aspx
  - http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/cd72c0dc-c5b8-42e4-96c2-b3c656f99ead.mspx?mfr=true

When an administrator installs Proficy Workflow on a server computer, the files required for the one-click deployment are installed when you perform a server installation.

On 32-bit computers, these files are located in a folder called Deployment in the following location:

<install dir>\Program Files\Proficy\Proficy Workflow\Program\Deployment

On 64-bit computers, these files are located in a folder called Deployment in the following location:

<install dir>\Program Files (x86)\Proficy\Proficy Workflow\Program\Deployment

An Administrator user must share this folder on the server computer, and then users can access it through a web page. The file used for one-click deployment is:

ProficyClient.application

You can create a web page, a button, or any means of access you want to use to make one-click deployment available to your users.

Each time a user invokes one-click deployment, it checks for any code updates, such as patches and service packs, that have been applied to the server (and subsequently to the one-click deployment files) and applies those changes to the one-click client. This allows your users to always be working with the same version of code as the server.

After installing Proficy Workflow on the server computer, you can copy the Deployment folder to another location for users to access. If you copy the folder to another location, you must re-copy the folder whenever code updates are applied in order for users to get the updates.

IMPORTANT: Do not move the Deployment folder from its install location. If this folder is moved, code updates cannot be applied to it.

Configure security certificates for a click-once client

For a click-once client, use this procedure to install certificates using the certificate authority generated by the Proficy Workflow server installation.

NOTE: Support for one-click installation of Proficy Workflow will be discontinued in a future release of the software. The client installation should be used in place of one-click installation upon discontinuation of the latter.

1. In the Proficy Workflow installation directory, go to the following folder to find the required certificate files: <installdir>\Program Files\Proficy\Proficy Workflow\Certificates\Export.
2. Copy the following certificate files to your click-once computer:
   - ProficySelfSignedCA.pfx
   - ProficySTS.pfx
3. For a click-once client running on Windows, run mmc.exe.
4. From the **Console** window, go to the **File** menu, and then select **Add/Remove Snap-in**.
   The **Add or Remove Snap-ins** dialog box appears.
5. In **Available Snap-ins**, double-click **Certificates**.
   The **Certificates snap-in** dialog box appears.
6. Select **Computer account**, click **Next**, select **Local computer**, and then click **Finish**.
7. Click **OK**.
8. From **Certificates (Local Computer)**, expand Trusted Root Certification Authorities\Certificates, and then add ProficySelfSignedCA.pfx.
9. From **Certificates (Local Computer)**, expand Personal\Certificates, and then add ProficySTS.pfx.

Command Line (Silent) Installation

You can install the server, client, or hosts using command line parameters. You can also use this method to install multiple servers, ensuring that the same configuration data is used in all instances.

Command Line Parameters

NOTE: Starting with Proficy Workflow 2.5, legacy certificates are no longer supported. For new server certificates, select the Generate new and unique certificates option.

Command Line Parameter	Description
/s	Runs the installation setup (SetupApplicationServer.exe or SetupWebServer.exe) in silent mode; that is, the installation occurs without displaying the user interface.

Command Line Parameter	Description
	NOTE: The installation fails if the Proficy services are running. See /fs. You must use the /c parameter in conjunction with the /s parameter and provide a valid configuration file name.
/fs	Same as the /s parameter, but stops and restarts running services when performing an upgrade installation.
/t filepath (where filepath is the user-defined file name)	Runs the installation setup (SetupApplicationServer.exe or SetupWebServer.exe), including the user interface, and creates a configuration file that contains all of the installation configuration data. **NOTE:** For security reasons, passwords are not included in the configuration data.
PropertyName=value (where PropertyName is a configuration file property)	Individual configuration file properties, such as passwords, can be set using a command line by providing the property name and value separated by an equals sign (=). The property name cannot have spaces and values with spaces must be enclosed in double quotes. The following rules apply: • parameter name matching is not case sensitive • double quotes around values are required to preserve white space (for example, PropertyA="a value with spaces") • command-line parameter values supersede property values supplied in a configuration file • double quotes in values are permitted, but must be doubled (for example, PropertyB="a ""quoted"" value") **Examples: Setting Password Properties** Include one or more of the following on the command line to set the respective passwords to the value, secret. • AdministratorPassword=secret • KspUserPassword=secret • CertificatePassword=secret • CertificateServicePassword=secret
/c filepath (where filepath is the user-defined file name)	Runs the installation setup (SetupApplicationServer.exe or SetupWebServer.exe) and uses the configuration data found in the configuration file. When used with the /s parameter, the installation runs in silent mode. **NOTE:** You can use the configuration file that was created using the /t command line parameter or you can use the sample configuration file provided in the install directory.

Command Line Parameter	Description
	If you use the configuration file created by using the /t parameter, you must add the passwords before using that file with the /c parameter.
/l filepath (where filepath is the logging directory)	Overrides the default location for the installation log file.
/p installation type option (where installation type option values are specific to the product being installed)	Runs SetupApplicationServer.exe or SetupWebServer.exe, including the user interface, without displaying the installation type selection screen, instead automatically selecting the installation type based on the value specified for the command line parameter. Valid parameter values based on product type are as follows: **SetupApplicationServer.exe** • Server: Installs a Proficy application server in Single Server mode. • WorkflowServer: Installs a Proficy application server in Workflow Extension Server mode. • UserServer: Installs a Proficy application server in User Extension Server mode. • Client: Installs a Proficy client. **SetupWebServer.exe** • Application: Installs the Proficy application server. • Web: Installs the Proficy Vision Web Server. **NOTE:** • These values are case sensitive. • The /p parameter cannot be used in conjunction with silent mode (that is, the /s parameter) and/or a configuration file (that is, the /c parameter).

Uninstall the application

The following topic guides you though the process of removing Proficy Workflow software from your system.

NOTE: If you generated security certificates or used pre-existing certificates from a previous version of this application, those certificates are not removed when you uninstall your Proficy application server server or remote client.

1. From **Control Panel**, go to your programs listing.

2. If applicable, select **ADAM Instance SOAAdam**, and then click **Uninstall** (depending on your operating system).
3. In the confirmation message box, click **Yes**.
4. Select Proficy Workflow (*<installation type>*), and then click **Uninstall** (depending on your operating system).
5. In the confirmation message box, click **Yes**.

Server Clustering Implementation

Supported and Validated Cluster Configurations

Before you begin installing Proficy Workflow, it is important to determine what your architecture is so you can know where to install your servers.

There are three environments that have been validated and are supported.

- One cluster, two nodes
- Two clusters, two nodes each
- Three clusters, two nodes each

The only supported configuration of cluster groups is as follows.

- Proficy application server (single server) cluster group
- Proficy application server, Workflow Engine (multi-server) cluster group
- Proficy application server, User Server (multi-server) cluster group
- Proficy application server, Workflow Engine, and User Server (multi-server) clustered groups

Connecting the web server to the Proficy application server in a failover cluster environment is not currently supported.

One Cluster, Two Nodes

One of the environments supported and validated for server clustering is a single cluster with two nodes.

The following figure shows an example of two Proficy servers in one cluster. Each Proficy application server must run the Proficy Server, Proficy Publisher Service, and Proficy STS services.

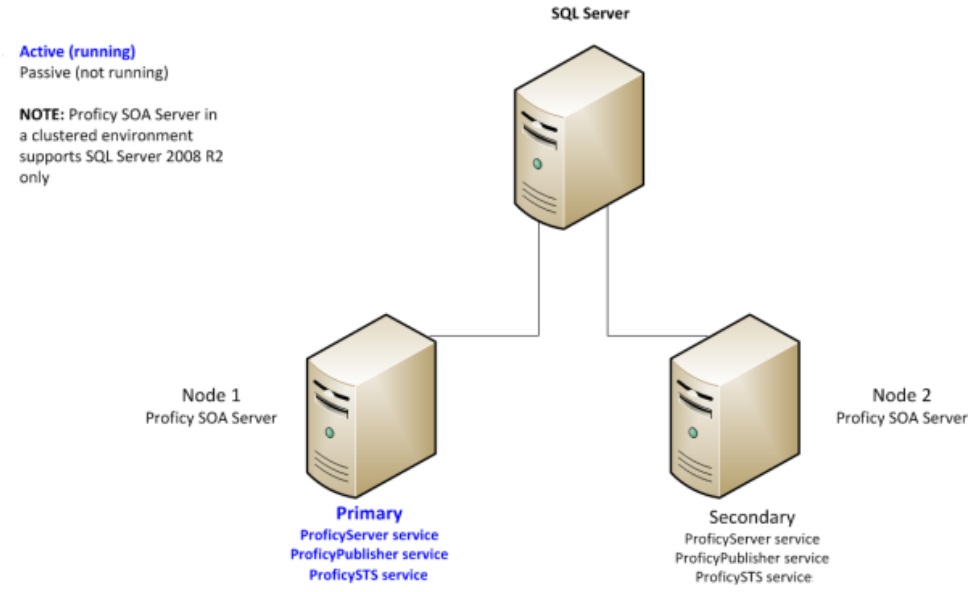


Figure 1: Two Proficy servers in a single cluster

Two Clusters, Two Nodes Each

One of the environments supported and validated for server clustering is two clusters with two nodes each.

The following figures show examples of two Proficy application server servers with two Workflow engines, in separate clusters, and two Proficy application server servers with two User servers, in separate clusters, respectively.

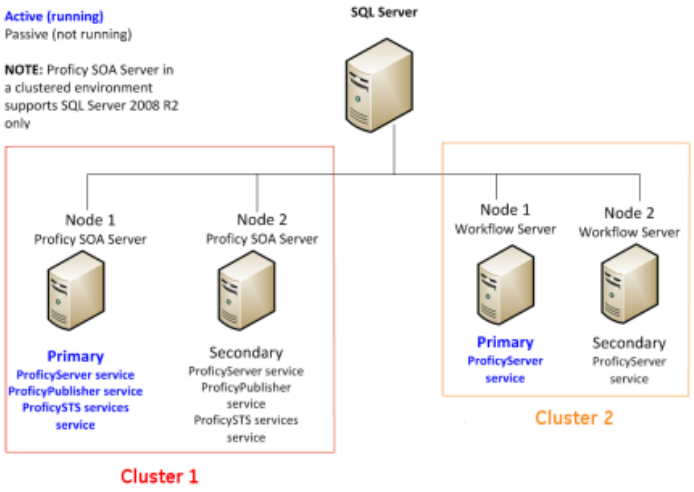


Figure 2: Two Proficy servers and two Workflow engines, in separate clusters

Each Proficy application server server must run the Proficy Server, Proficy Publisher Service, and Proficy STS services. Each Workflow engine must run the Proficy Server service.

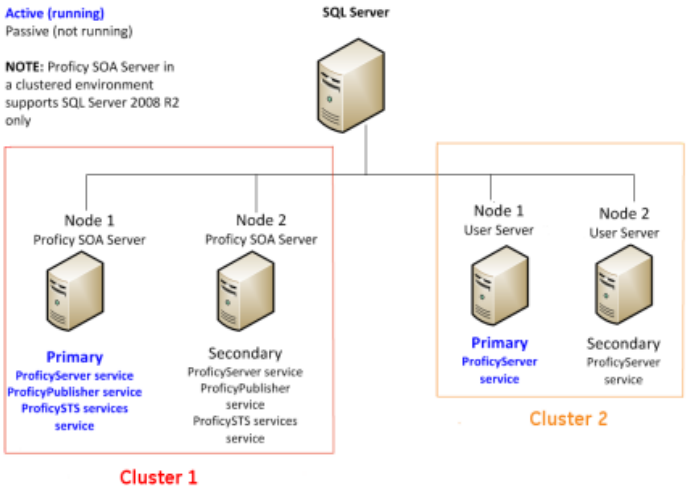


Figure 3: Two Proficy servers and two User servers, in separate clusters

Each Proficy application server server must run the Proficy Server, Proficy Publisher Service, and Proficy STS services. Each User server must run the Proficy Server service.

Three Clusters, Two Nodes Each

One of the environments supported and validated for server clustering is three clusters with two nodes each.

The following figure shows an example of two Proficy servers, two Workflow engines, and two User servers, each in its own cluster. Each Proficy application server must run the Proficy Server, Proficy Publisher Service, and Proficy STS services. Each Workflow engine and each User server must run the Proficy Server service.

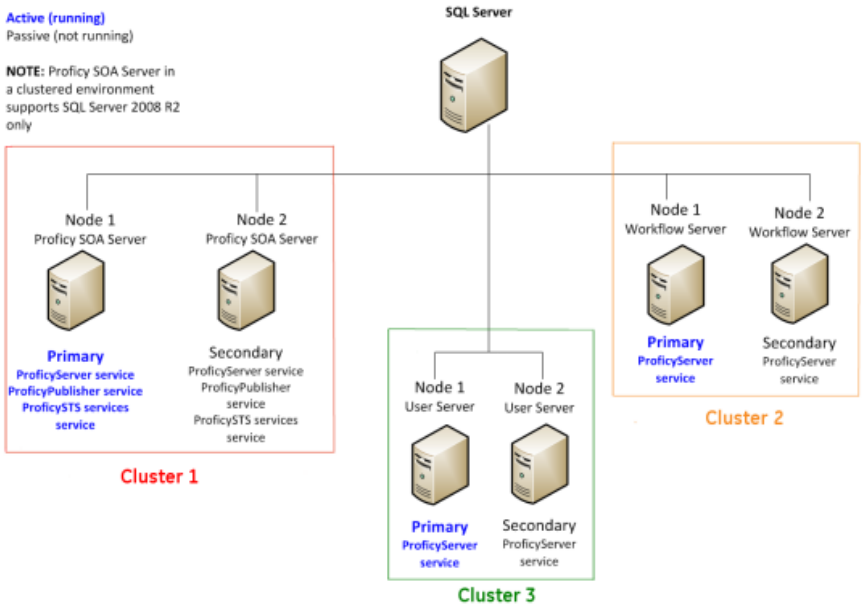


Figure 4: Two Proficy servers, two Workflow engines, and two User servers, in separate clusters

Microsoft Failover Cluster Manager for Windows Servers

The Microsoft Failover Cluster Manager is used to create the cluster and to add nodes to the cluster.

If failover clustering is not installed, use the **Server Manager** to install it.

NOTE: Depending on your server requirements, visit the related Microsoft TechNet web sites for more information.

The Microsoft Failover Cluster Manager is used to create two new DNS entries: one to manage your server cluster, and one for the services you intend to cluster. For a Proficy application server cluster (even in a multi-server environment), you must add the Proficy Server, Proficy Publisher Service, Proficy STS, and Proficy Certificate services for clean installations, as well as upgrades.

If you are using clusters in a multi-server environment and clustering Workflow and/or User servers, only the Proficy Server service needs to be added for those servers.

Install Microsoft Failover Cluster Manager

The Microsoft Failover Cluster Manager must be installed in order to configure your failover cluster.

1. On the server computer, click **Start** > **Administrative Tools** > **Server Manager**.
   The **Server Manager** dialog box appears.
2. To configure the related server, select **Add roles and features**.
   The **Add Roles and Features Wizard** appears.
3. Select **Features** > **Failover Clustering** > **Next**.
4. Click **Install**.
5. When the installation completes, click **Close**.

Configure the Microsoft Failover Cluster Manager

The Microsoft Failover Cluster Manager is used to create a new DNS entry to manage your server cluster.

IMPORTANT: You must have installed Proficy application server on both cluster nodes, pointing to the same database, before performing the following procedure.

This procedure is based on a Windows® Server 2012 environment. If you are using Windows 2008 R2, ensure that you add the Proficy Publisher Service and Proficy STS services as children of Proficy Server.

1. On the server computer, click **Start** > **Administrative Tools** > **Failover Cluster Manager**.
   The **Failover Cluster Manager** dialog box appears.
2. From the **Actions** menu, select **Create Cluster**.
   The **Create Cluster Wizard** appears.
3. Follow the wizard prompts to create your cluster, as follows:
   a) Enter a management name for the cluster.
   b) Add the nodes that will be part of the cluster; that is, the primary and failover servers.
   c) In the **Failover Cluster Manager**, expand the cluster from the left hand side, and then click **Roles**.
   d) Click **Configure Role**.
      The **High Availability Wizard** appears.
   e) Click **Generic Service**, and then click **Next**.
   f) Click Proficy Server, and then click **Next**.
   g) Enter a name for the server. This name is required when running various Proficy tools.
   h) Click **Next**, and then **Next** again to bypass the storage and registry settings.
   i) Review the confirmation, click **Next**, and then click **Finish**.
4. To add Proficy support services, perform the following procedure.
   a) In the **Roles** window, in the **Status** column, wait until the status changes to *Running*.
   b) Right-click the role that you created, click **Add Resource**, and then select **Generic Service**.
   c) Click Proficy STS, and then click **Next**.
   d) Review the confirmation, click **Next**, and then click **Finish**.
   e) For Proficy Publisher Service, repeat steps 4.b on page 50 to 4.d on page 50.
      The **Status** indicates that the roles are *Partially Running*.
   f) For Proficy Certificate, repeat steps 4.b on page 50 to 4.d on page 50.
   g) In the **Roles** window, select the name you entered in 3.g on page 50.
   h) Click **Start Role**.
      The **Status** indicates that the roles are *Running and Online*.
   i) Click **Stop Role**.

After setting up the failover cluster, the services will be running on both servers. You must either manually stop the services on the failover server, or move the service to the primary server. This enables the services on only the primary server.

NOTE: To run any post-installation configuration tools, you must turn off the cluster to avoid a failover. For all tools, except Configure Server, you are required to run the tools on one node only of the cluster. For configuring the server, you must run the tool on all nodes.

Configure quorum options for a cluster

Although this application does not require a disk for clustering, it is recommended that you configure either a file share witness or a disk witness.

1. On the server computer, click **Start** > **Administrative Tools** > **Failover Cluster Manager**.
   The **Failover Cluster Manager** dialog box appears.
2. Select the cluster you want to configure.

   TIP: If the cluster you want to configure is not displayed, then in the console tree, right-click **Failover Cluster Manager**, click **Manage a Cluster**, and then select or specify the cluster you want to configure.

3. From the **Actions** menu, click **More Actions**, and then click **Configure Cluster Quorum Settings**.
4. Follow the instructions in the wizard to select the quorum configuration for your cluster.

   If you choose a configuration that includes a disk witness or file share witness, follow the instructions for specifying the witness.
5. Optional: After the wizard completes and the **Summary** page appears, click **View Report** to view a report of the tasks that the wizard performed.

Configure the primary cluster server

After installing the Proficy application server on your primary server machine, you must configure the machine as the primary cluster server to begin the clustering process.

1. On the primary server machine, click **Start** > **All Programs** > **Proficy** > **Proficy Workflow** > **Configuration** > **Configure Server**.
   The **Configure Server** tool appears.
2. Select the **Create a Proficy Application Server Instance** option.
3. Select the **Make this machine a primary for a new failover cluster** check box.
4. In the **Cluster Name** field, enter the name of the cluster you created in the Microsoft Failover Cluster Manager.
5. Click **Save**, and then click **Exit**.
6. Regenerate the security certificates for the cluster by running the Configure Proficy Service Certificates tool, and choose the **Generate new certificates unique to this installation** option.

IMPORTANT: After configuring the primary cluster server, you must complete the following procedures to finish the clustering process.

1. Export the server security certificates in preparation for installing them on your failover and/or extension server(s).
2. Configure the failover cluster server on page 51.

Configure the failover cluster server

After configuring the primary Proficy application server cluster server and exporting the server security certificates, you can configure the failover cluster server.

1. On the backup server machine, click **Start** > **All Programs** > **Proficy** > **Proficy Workflow** > **Configuration** > **Configure Server**.
   The **Configure Server** tool appears.
2. Select the **Make this machine a failover backup of an existing Server Instance** option.
3. From the **Choose existing cluster** drop-down list, select the cluster that you want this machine to be the failover backup for.
4. Click **Save**, and then click **Exit**.
5. On the backup server machine, click **Start** > **All Programs** > **Proficy** > **Proficy Workflow** > **Configuration** > **Configure Certificates**.
   The **Security Certificates** page appears.
6. Select the **Import certificates** option, and then import the certificates, as follows:
   a) In the **Certificate File** field, click **Browse**, and then locate and select the .zip file containing the security certificates that you exported when you configured the primary server in the cluster.
   b) In the **Password** field, enter the password that you set when you exported the security certificates from the primary server.
   c) Click **Next**.
   The page changes to indicate that the files contained in the exported certificate file have been loaded.
   d) Click **Save**.

Configure a local client for a cluster node (32-bit)

If you want to run a cluster node on a 32-bit system, follow this procedure.

TIP: If your Proficy client starts but tries to update its product options and fails, then you must restart the Proficy Server service. Restarting this service ensures that the client product options are upgraded.

1. To set up a local client, perform the following procedure.
   a) Create a copy of the file, UserStartup.xml. To find this file, go to <install location>\Program Files (x86)\Proficy\Proficy Workflow\Program\Data\UserStartup.xml.
   b) Name the new copy UserStartupClient.xml.
   c) In the new file, change ServerDNSName to the name of the new cluster. For example, if it is called soaCluster2012: <ServerDNSName>soaCluster2012</ServerDNSName>.
2. In the file, ProficyClient.exe.config, make these changes. To find this file, go to <install location>\Program Files (x86)\Proficy\Proficy Workflow\Program\ProficyClient.exe.config.

   NOTE: It is recommended that you make a backup copy of this file before proceeding.

   a) From the line <add key="stsUrl" value="http://<computer node name>:8112/ProficySTS">, change <computer node name> to the name of the cluster, such as soaCluster2012.
   b) In the following two lines, change the old file name (UserStartup.xml) to the new file name (UserStartupClient.xml).
      - <add key="url" value="./Data/UserStartupClient.xml">
      - <add key="UserStartupUrl" value="./Data/UserStartupClient.xml">

Configure a local client for a cluster node (64-bit)

If you want to run a cluster node on a 64-bit system, follow this procedure.

- Point the file, UserStartup.xml, to the cluster instead of the node.

  To find this file, go to <install location>\Program Files (x86)\Proficy\Proficy Workflow\Program\Data \UserStartup.xml.

Server Clustering and One-Click Deployment

If you have implemented a server cluster environment and you want to use one-click deployment in that environment, additional configuration is required to set up the one-click deployment.

There are two methods to choose from to configure one-click deployment in a server cluster environment.

- Modify the userstartup.xml file on each client to use the cluster address.
- Update the userstartup.xml.deploy file on the server, in the Proficy Workflow\Program\Deployment \1_5_0_0\Program\Data directory, and then regenerate the one-click deployment install.

Clustering Tips

Use the clustering tips to ensure your failover cluster runs smoothly.

Security Certificates

When setting up a clustered environment, you must regenerate and export Proficy security certificates as part of configuring the primary cluster server, and then import the certificates when configuring the failover cluster server. Symptoms of incorrect security certificate configuration include the inability to create or display Silverlight forms and the Web Task List. For more information on setting up security certificates for a clustered environment, see Configure the primary cluster server on page 51, Configure the failover cluster server on page 51, and Modify security certificates on page 64.

Proficy Server Service is Marked for Deletion

Occasionally, after a server configuration, the Proficy Server service is marked for deletion. You can restore the service by running the **Configure Server** tool again.

Clients on Clustered Proficy Servers

Clients that are installed with clustered Proficy servers will work only if the server is the primary server.

NOTE: If you have a cluster with multiple nodes, the cluster must be pointing to the client name, and the server that each node is running on must state the role name for the cluster. For more information, see Configure a local client for a cluster node (32-bit) on page 52 and Configure a local client for a cluster node (64-bit) on page 52.

Running a Clustered Multi-server Environment

When running with both a clustered Proficy application server and clustered Workflow/User servers, you must restart the primary server and then, after a few minutes, restart the primary Workflow/User server. This can be performed using the Microsoft Failover Cluster Manager by taking the servers offline, and then putting them back online.

Web Task List Deployment

The Web Task List is automatically installed with the Proficy application server installation of Proficy Workflow. Users can access the Web Task List using a web browser.

A reverse proxy is highly recommended when deploying the Web Task List, as it provides increased security by limiting and controlling the exposure of internal servers and services. You can configure either an Internet Information Services (IIS) reverse proxy or an Apache reverse proxy for use with the Web Task List. In either case, you must also configure the necessary certificates before connecting to the Web Task List.

Configure security certificates for a reverse proxy

For a secure reverse proxy, use this procedure to install certificates to your web server using the certificate authority generated by the Proficy application server installation.

1. In the Proficy Workflow installation directory, go to the following folder to find the required certificate files: <installdir>\Program Files\Proficy\Proficy Workflow\Certificates\Export.
2. Copy the following certificate files to your web server:
   - ProficySelfSignedCAPublicKey.cer
   - ProficySTSPublicKey.cer
3. For a web server running on Windows, run mmc.exe.
4. From the **Console** window, go to the **File** menu, and then select **Add/Remove Snap-in**.
   The **Add or Remove Snap-ins** dialog box appears.
5. In **Available Snap-ins**, double-click **Certificates**.
   The **Certificates snap-in** dialog box appears.
6. Select **Computer account**, click **Next**, select **Local computer**, and then click **Finish**.
7. Click **OK**.
8. From **Certificates (Local Computer)**, expand Trusted Root Certification Authorities\Certificates, and then add ProficySelfSignedCAPublicKey.cer.
9. From **Certificates (Local Computer)**, expand Personal\Certificates, and then add ProficySTSPublicKey.cer.

Configure an IIS reverse proxy for the Web Task List

The information provided in this section is specific to configuring Internet Information Services (IIS) to act as a reverse proxy using the Application Request Routing (ARR) and URL Rewrite modules.

1. **Prerequisites**

   TIP: Before installing IIS Application Request Routing (ARR), it is recommended that you enable HTTP Logging and Tracing features for IIS first. Tracing makes it possible to diagnose problems with reverse proxy rewrite rules.

   a) From the **Control Panel**, go to **Windows Features** to enable the following IIS settings:

   - HTTP Logging
   - Tracing

     TIP: To make it easier to diagnose problems, tracing must be enabled before installing ARR.

   - The ARR and URL Rewrite modules only install their trace providers if those IIS features are already enabled. You can install them later by enabling the IIS HTTP Logging and Tracing features and reinstalling or repairing ARR.
   - Tracing is disabled by default.

   b) Install the IIS ARR 2.5 (or later) module from http://www.iis.net/download/ApplicationRequestRouting.

   c) In the **Install** window, click **Options**.

   d) In the **Change Options** window, when asked which web server you want to use, click the **IIS** check box.

   e) Click **OK**, and then click **Install**.

   NOTE: The URL Rewrite 2.0 module installs automatically.

   f) Start the Internet Information Services (IIS) Manager application.

   1. From the **Start** menu, click **Administrative Tools** > **Internet Information Services (IIS) Manager**.

   g) Enable the server to act as a proxy.

   NOTE: This is a server-wide setting.

   1. From the **Connections** panel, select the server you want to configure.
   2. From the **IIS** section in the central panel, double-click **Application Request Routing Cache**.
   3. From the **Actions** panel, in the **Proxy** section, click **Server Proxy Settings**. **Application Request Routing** opens in the central panel.
   4. Select the **Enable proxy** check box, and then in the **Actions** panel, click **Apply**.

2. **Configuration**

   The URL Rewrite rules apply to a single web site. These instructions and rules assume that your server already is configured with a web site, such as Default Web Site, with an HTTPS binding on port 443 that uses a certificate that is trusted by the client machines.

   a) In the Internet Information Services (IIS) Manager, in the **Connections** panel, under the server you are currently configuring, expand the **Sites** node, and then select the web site that you want to configure.

   b) From the **Actions** panel, click **Explore** to open Windows Explorer to the physical directory on disk for your web site.

   1. The default location for **Default Web Site** is C:\inetpub\wwwroot.
   2. In this location, you see a file named web.config.

   c) Open another Windows Explorer window and navigate to your Proficy Workflow installation directory.

   - On 32-bit systems, the default location is C:\Program Files\Proficy\Proficy Workflow.
   - On 64-bit systems, the default location is C:\Program Files (x86)\Proficy\Proficy Workflow.

   d) In the Proficy Workflow installation directory, go to the folder **Reverse Proxy Config (IIS)** for the reverse proxy configuration files.

   1. From the **Reverse Proxy Config (IIS)** directory, copy the following files to your web site's directory:

- rewriteMaps.config
- rules.config
- outboundRules.config

2. For a sample of the web.config showing how to configure the <rewrite> element under <system.webServer>, go to the **Reverse Proxy Config (IIS)** directory. If your web site's web.config has:
   - no customization, you can overwrite the file with the sample
   - some customization but no rewrite rules, you can copy the <rewrite> element from the sample and add it as a child of the <system.webServer> element in your web site's web.config
   - rewrite rules already configured, you must merge the existing rules and the rules provided for the reverse proxy manually

e) Update the rewrite.Maps.config file with the actual server names, as follows:

1. In the Internet Information Services (IIS) Manager, in the **Connections** panel, under the server you are currently configuring, expand the **Sites** node, and then select the web site whose rewriteMaps.config file you want to update.
2. Double-click the **URL Rewrite** icon.
3. From the **Actions** panel, click **View Rewrite Maps**. **URL Rewrite Maps** opens in the central panel.
4. Double-click **ComputerNames**. **Edit Rewrite Map** opens in the central panel.
5. From the **Original Value** column, select a server, and then from the **Actions** panel, click **Edit Mapping Entry**. The **Edit Mapping Entry** dialog box appears.
6. In the **New Value** field, enter the actual server name, as follows:
   - For the WebServerHostName, enter the fully qualified name of the computer where your Web Task List is installed.
   - For all other server values, enter the fully qualified name of the computer where your servers are installed.
7. Repeat steps 2.e.v on page 55 and 2.e.vi on page 55 for each server listed in the **Edit Rewrite Map** panel.

Configure an Apache reverse proxy for the Web Task List

The information provided in this section is specific to configuring Apache to act as a reverse proxy.

To perform this configuration, you must already be familiar with Apache.

NOTE: This procedure assumes that the Proficy application server and Workflow are co-resident on the same host.

1. Enable these modules in httpd.conf:
   - mod_proxy
   - mod_proxy_http
   - mod_substitute
2. Add the rules from the **Inbound Rules** section to httpd.conf.
3. Add the rules from the **Outbound Rules** section to httpd.conf.

Inbound and Outbound Rules for Apache

Follow these rules when configuring an Apache reverse proxy for the Web Task List.

Inbound Rules

SSLProxyEngine On:		
ProxyPass	/Proficy/	http://YourSOAWorkflow.company.com:8020/Proficy/

SSLProxyEngine On:		
ProxyPassReverse	/Proficy/	http://YourSOAWorkflow.company.com:8020/Proficy/
ProxyPass	/proficy/	http://YourSOAWorkflow.company.com:8020/Proficy/
ProxyPassReverse	/proficy/	http://YourSOAWorkflow.company.com:8020/Proficy/
ProxyPass	/ProficySTS/	https://YourSOAWorkflow.company.com:8012/ProficySTS/
ProxyPassReverse	/ProficySTS/	https://YourSOAWorkflow.company.com:8012/ProficySTS/
ProxyPass	/SOAServer/SOAProject/	https://YourSOAWorkflow.company.com:8203/SOAServer/SOAProject/
ProxyPassReverse	/SOAServer/SOAProject/	https://YourSOAWorkflow.company.com:8203/SOAServer/SOAProject/
ProxyPass	/SOAServer/System/	http://YourSOAWorkflow.company.com:8020/SOAServer/system/
ProxyPassReverse	/SOAServer/System/	http://YourSOAWorkflow.company.com:8020/SOAServer/system/
ProxyPass	/WorkflowServer/	https://YourSOAWorkflow.company.com:8203/WorkflowServer/
ProxyPass	/WorkflowServer/	https://YourSOAWorkflow.company.com:8203/WorkflowServer/

Outbound Rules

AddOutputFilterByType SUBSTITUTE text/xml	
SUBSTITUTE	"s|<SOAServerName>.*</SOAServerName>|<SOAServerName>**YourApacheServer.company.com**</SOAServerName>|i"
SUBSTITUTE	"s|<StsServiceName>.*</StsServiceName>|<StsServiceName>**YourApacheServer.company.com**</StsServiceName>|i"
SUBSTITUTE	"s|<StsSecurePort>.*</StsSecurePort>|<StsSecurePort>443</StsSecurePort>|i"

AddOutputFilterByType SUBSTITUTE text/xml	
SUBSTITUTE	"s|<HttpsSamlPort>.*</HttpsSamlPort>|<HttpsSamlPort>443</HttpsSamlPort>|i"
SUBSTITUTE	"s|<WorkflowServerName>.*</WorkflowServerName>|<WorkflowServerName>**YourApacheServer.company.com**</WorkflowServerName>|i"
SUBSTITUTE	"s|<WorkflowSamlPort>.*</WorkflowSamlPort>|<WorkflowSamlPort>443</WorkflowSamlPort>|i"
SUBSTITUTE	"s|<HttpPort>.*</HttpPort>|<HttpPort>443</HttpPort>|i"
SUBSTITUTE	"s|(.*)<a:anyURI>.*:.*?/(.*)</a:anyURI>(.*)|$1<a:anyURI>https://**YourApacheServer.company.com**:443/$2</a:anyURI>$3|i"

Connect to the Web Task List

The information in this section guides you through the process of connecting to the Web Task List.

You can configure and use a dedicated reverse proxy for increased security when using the Web Task List over the Internet.

TIP: To improve performance, ensure that caching is enabled in Internet Explorer.

When the Full Server installation and reverse proxy configuration have been completed, the Web Task List can be accessed using the following URLs.

Web Server	URL
IIS Reverse Proxy	https://myiisserver.example.com/Proficy/Workflow/WebTaskList.html **NOTE:** Assumes reverse proxy IIS web server is externally accessible via host name myiisserver.example.com with an SSL certificate specifying that host name listening on standard port 443 (default).
Apache Reverse Proxy	https://myapacheserver.example.com/Proficy/Workflow/WebTaskList.html **NOTE:** Assumes reverse proxy Apache web server is externally accessible via host name myapacheserver.example.com with an SSL certificate specifying that host name listening on standard port 443 (default).
Direct	http://mysoaserver:8020/Proficy/Workflow/WebTaskList.html On the Full Server machine, a link to this URL is available from: **Start menu** > **Proficy** > **Proficy Workflow** > **Task Lists** > **Web Task List**. **NOTE:** The direct link is for intranet and testing only. We recommend using reverse proxy to use the Web Task List over the Internet to limit exposure to internal machines and services as part of a secure architecture.

Web Server	URL
	Assumes Proficy Workflow server is internally accessible via host name mysoaserver with an SSL certificate specifying that host name listening on standard port 8203 (default). A certificate is configured like this by default during a standard Full Server installation. The machine must also install the Proficy STS security certificate.

Certificates

The machine running the Web Task List must trust the SSL certificates used by the server. If the SSL certificate is signed by a trusted root certificate authority (CA), then the client (that is, the Web Task List) machine must trust the signing CA by adding it to the Trusted Root Certificate Authority certificate store for the machine.

NOTE: SSL certificates purchased from a reputable certificate authority will already be trusted.

For a direct connection, the Web Task List machine must also install the Proficy STS security certificate into the Personal certificate store for the machine.

For a reverse proxy configuration, the web server must trust the signing CA by adding it to the Trusted Root Certificate Authority certificate store for the machine. The Web Task List machine only needs to trust the SSL certificate for the web server and does not need to trust the SSL certificate used by the Proficy Workflow server of the Proficy STS security certificate.

Log On Overview

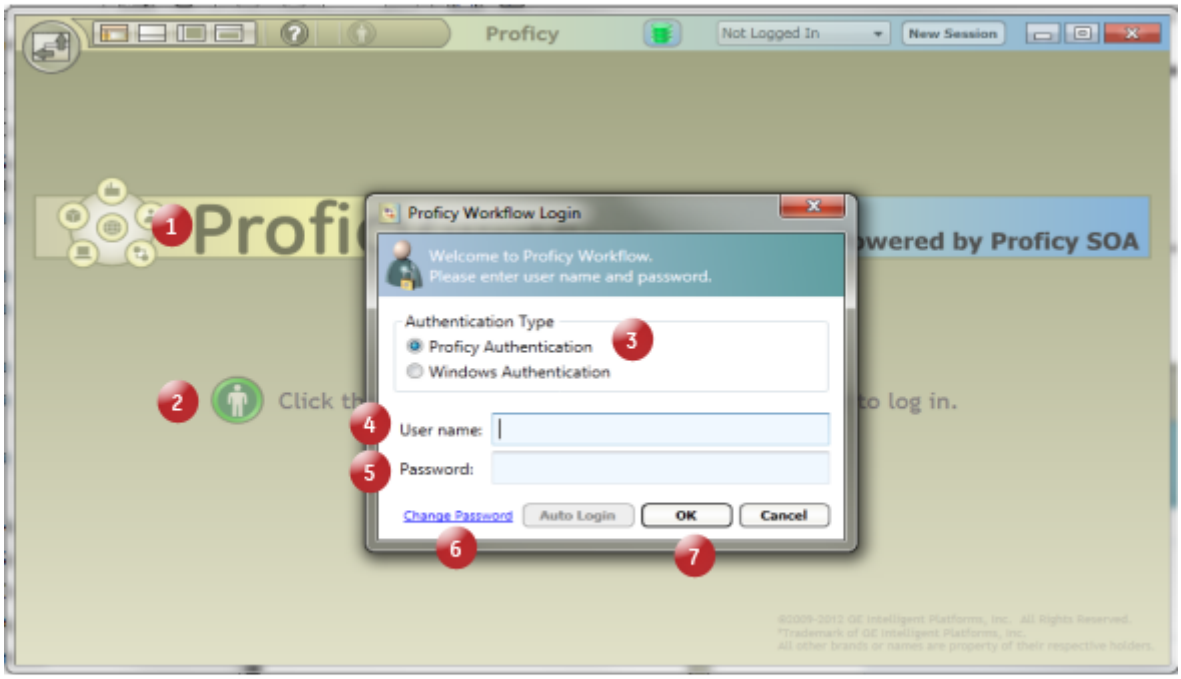
After installing Proficy Workflow, the primary administrator user configured during installation can manually log in to the program and configure system security. As part of this process, additional users are specified and log in mode and authentication method are established.

Available log-in modes are manual and automatic; available authentication methods are Proficy, Windows, and SSO (GE Single Sign on).

Log on to Proficy client

You can log on to the Proficy client in one of two ways: automatic and manual. This procedure outlines the steps to manually log in to the system.

In order to log in to Proficy Workflow, the system must be in a state of either *Complete* or *Partial* health. For more information, see System Health and Program Use on page 4.



1. Use one of the following methods to log on..

If...	Then do the following...
An instance of Proficy Workflow is not running on the workstation.	1. Launch Proficy client using either the **Start** menu or desktop icon. 2. On the main Proficy Workflow screen, click **Log in to Proficy**. **NOTE:** You can also use this path if an instance of Proficy Workflow is already running on the workstation.
An instance of Proficy Workflow is running on the workstation.	1. On the Proficy Workflow toolbar, click **New Session**.

The **Proficy Workflow Login** dialog box appears.

2. In the **Authentication Type** section, select the type appropriate to your user profile.

Select...	If...
Proficy Authentication	Your user profile is part of the Proficy Workflow application.
Windows Authentication	Your user profile is part of the Windows domain. **IMPORTANT:** To log in using Windows Authentication, your server and client(s) must be on a domain.
SSO Authentication	Your user profile is part of *SSO* security. **NOTE: SSO Authentication** is not available if it has not been enabled.

3. In the **User Name** field, enter your user name.

NOTE: If you are logging in using **SSO Authentication**, this field is labelled **User ID**.

4. In the **Password** field, enter your password.
5. If applicable, in the **Domain** field, enter the domain name.
6. Click **OK**.

Automatically log in to Proficy Workflow

The default method of logging in to Proficy Workflow, and the only method available immediately after a new installation, is manually. However, the system can be configured to allow automatic login, in which case the steps for logging in are those outlined in this procedure.

In order to log in to Proficy Workflow, the system must be in a state of either *Complete* or *Partial* health. For more information, see System Health and Program Use on page 4.

1. Launch Proficy client using either the **Start** menu or desktop icon.
   If automatic login is enabled and configured, the user credentials are authenticated and the Proficy Workflow client appears.
2. If applicable, launch additional sessions of Proficy Workflow.
3. If you log out of any session for any reason, the **Login** dialog box appears. Click **Auto Login** to log in again with the appropriate credentials.

GE Single Sign On (SSO)

You can configure Proficy Workflow to use GE Single Sign On (SSO) authentication when your users log on to the Proficy client.

NOTE: GE Single Sign On applies only to GE businesses.

Within GE, all employees are assigned an SSO ID that grants them access to internal GE web pages and resources. When Proficy Workflow is installed within a GE business, you have the option to enable SSO authentication, so that users enter their SSO ID and password to access the system.

NOTE: In order to log in to Proficy Workflow, the system must be in a state of either *Complete* or *Partial* health. For more information, see System Health and Program Use on page 4.

Configuration Settings

GE SSO authentication can be configured during the installation process, or at any time after installation using the **Configure Security** tool.

When setting up SSO authentication, you must configure the SSO server and SiteMinder Agent URLs. Each GE business has SiteMinder installed to protect resources on its own web server. SiteMinder Agent provides authentication for all web-based applications. The Proficy application server must be able to access this web server in order to authenticate SSO credentials. User information is retrieved from the SSO Server.

A file named Headers.asp is included with the Proficy Workflow installation. Its location is: C:\Program Files \Proficy\Proficy Workflow\Programs. This file must be hosted on the SiteMinder Agent web server, and then the SSO security group must protect the file under SiteMinder.

The Proficy application server makes a request to Headers.asp to get information about the SSO user who is trying to log in. The following table lists and describes the returned header information.

Header	Description
HTTP_SM_USER	The SSO ID of the user
HTTP_GIVENNAME	First name of the SSO User
HTTP_SN	Last name of the SSO User
HTTP_GESSOSTATUS	Status of the SSO account

Header	Description
HTTP_MAIL	E-mail address of the SSO User

When the GE SSO security group sets up Headers.asp, they must make sure that these headers are included in the response.

User Account Setup

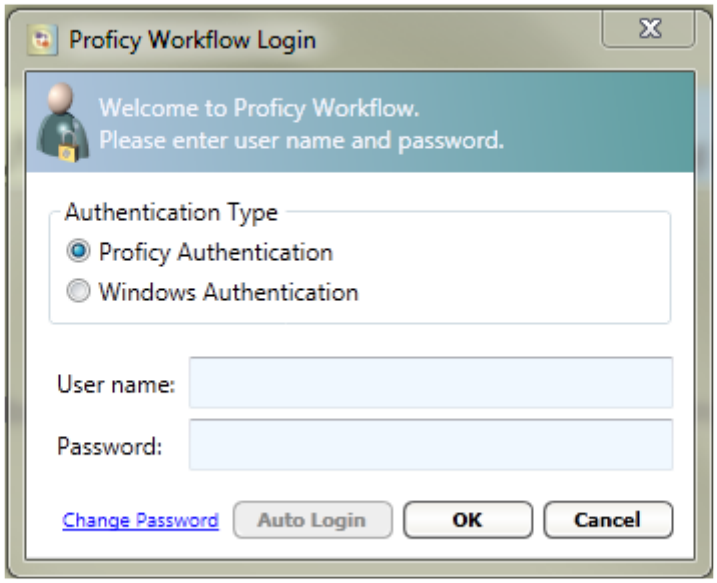
After you configure your system for SSO authentication, you can manually set up each user's account to link to their SSO account. The account login name must be the user's SSO ID.

You can also use the SSO Authentication Failed event to schedule a workflow that will create a Proficy user account. That is, if a user with a valid SSO ID but no Proficy user account tries to log in to Proficy Workflow, the SSO Authentication Failed event is triggered and causes the Proficy user account to be created. The SSO Authentication Failed event contains the user's SSO ID, full name, and e-mail address.

IMPORTANT: Make sure that each user belongs to the SSO Users group before creating their SSO user account. The SSO Users group is a default security group located within the Personnel model.

Authentication

The **Proficy Workflow Login** dialog box is used to log in to Proficy Workflow.



Authentication Types

The following information applies to all regular logins except the Mobile-sized Task List:

The computer you log on to stores the authentication type in the proficyclient.exe.config file. When you start a new client on that computer, the authentication type you selected during your previous logon is automatically selected. However, if another user successfully logged in on that computer since your last logon using a different authentication type, that authentication type will be selected.

If you attempt to log in using a different authentication type but the authentication fails, the authentication type is not updated in the proficyclient.exe.config file.

Property	Value	Description
Proficy Authentication	System-defined	Your user profile is part of the Proficy Workflow application.
Windows Authentication	System-defined	Your user profile is part of the Windows domain. **IMPORTANT:** To log in using Windows Authentication, your server and client(s) must be on a domain. You must have added your user accounts to one or more Active Directory Universal Groups that are mapped to Proficy groups. The computer stores the domain name you enter in the proficyclient.exe.config file. When you start a new client, that domain name appears in the **Domain** field. However, if another user successfully logged in under a different domain since your last logon, that domain name will be displayed. If you attempt to log in under a different domain but the authentication fails, the domain name is not updated in the proficyclient.exe.config file.
SSO Authentication	System-defined	Your user profile is part of *SSO* security. **NOTE: SSO Authentication** is not available if it has not been enabled.

Login Properties

Property	Value	Description
User Name	User-defined	Specifies your unique user name
Password	User-defined	Specifies your unique password. **NOTE:** Your password must conform to the defined password complexity rules.
Domain	User-defined	Specifies the Windows domain that your user profile is part of. This field is available on when the **Windows Authentication** option is selected.
Change Password	N/A	Click this link to open the **Proficy Workflow Change Password** dialog

Property	Value	Description
		box where you can create a new password. **NOTE:** This link is available only if this feature is enabled.
Auto Login	System-defined	Click this button to automatically log in the Proficy Workflow. **NOTE:** This button is available only when the **Windows Authentication** option is selected and automatic login is configured.

Post-installation Configuration

The section provides information about configuring your system after installing the application.

If the installation fails, or you want to change a configuration setting after installation completes, you can open each of the installation wizard configuration pages as a standalone tool and make the required changes.

CAUTION: Changes to your installation configuration should be performed only by advanced users. If you make changes on your own, unpredictable results and behavior may occur. Contact GE Intelligent Platforms for assistance.

Running with a Standard Windows User Account

Users who are not Proficy Workflow administrators must be given permission to access certain folders in order to view log files and to be able to load forms.

- To provide the ability to load forms, ensure your users have permission to access C:\Program Data\Proficy \Logs.
- To provide access to log files, ensure your users have permission to access C:\Users\<User>\My Documents \Proficy Workflow.

  When a form is opened, it is retrieved from the database and copied to the client computer to be loaded into Proficy Workflow. If the **My Documents** folder is in a network storage location, that location is locked by user permissions, preventing the form from being created.

Configure web proxy settings for Local System account

Before defining a web service, you must configure web proxy settings for your Local System account based on your network requirements.

You may not need to change your network settings.

1. Configure Internet web proxy setting using BITSAdmin in one of the following ways.

   NOTE: For more information on BITSAdmin Tool, go to: http://msdn.microsoft.com/en-us/library/aa362813%28VS.85%29.aspx

To set...	Then do this...
accounts to use a static proxy server with exclusions	1. Execute: bitsadmin /util /setieproxy localsystem MANUAL_PROXY proxysrv:8080 ";*. contoso.com" 2. Replace proxysrv, 8080, and contoso.com with your organization's proxy server addresses address, port, and exclusions.

To set…	Then do this…
account to use proxy.pac file	1. Execute: bitsadmin /util /setieproxy localsystem AUTOSCRIPT http://contoso.com/proxy.pac 2. Replace proxysrv with your organization's pac file addresses.

2. From an administrative command line window, run the commands for the account that you want to change.

Modify security certificates

The **Configure Certificates** tool is used to change or update the security certificates you configured during the server installation.

Related Server Notes

- For an extension server installation (that is, a multiple server or server failover cluster), you must copy the ProficyPlatform and Proficy STS security certificates from the main server onto a disk or other portable device, and then transfer those certificate copies to your extension server(s). The SSL/TLS Server Certificate must be unique to each server.
- If you change the certificate option on your server(s), all remote clients connected to those servers must have their security certificates updated to match the server. Use the **Configure Client** tool to download the new versions of the certificates.

Upgrading

Starting with Proficy Workflow 2.5, legacy certificates are no longer supported.

1. On the server machine, click **Start** > **All Programs** > **Proficy** > **Proficy Workflow** > **Configuration** > **Configure Certificates**.
   The **Security Certificates** page appears.
2. Select the appropriate certificate option. For full descriptions of the certificate options, see Security Certificate Options on page 24.
3. Click **Save**, and then click **Exit**.

Modify site configuration

Using the **Configure Site** tool, you can modify site configuration by moving product options between servers, deleting servers that are not hosting product options, and, beginning with Proficy Workflow 2.1, designating whether servers or the product options that run on them are essential and/or disabling product options.

1. On the server machine, click **Start** > **All Programs** > **Proficy** > **Proficy Workflow** > **Configuration** > **Configure Site**.
   The **Configure Site** tool appears.
2. Modify the server configuration, as required.

If you want to…	Then do this:
Designate a server or a product option as essential	Select the **Essential** check box beside the server or product option listing. **NOTE:** Essential servers must remain running in order for users to access the program. If you designate a server as essential, all associated product options are automatically designated as essential. If you designate any product option as essential, the server that is hosting that option is automatically designated as essential, as indicated by the color filling in the **Essential** check box, but the essential status of other product options hosted by the server remains unchanged.

If you want to...	Then do this:
Designate a server or a product option as nonessential	Clear the **Essential** check box beside the server or product option listing. **NOTE:** If one or more product options assigned to a server is designated as essential, you cannot designate the server as nonessential. Nonessential servers must remain running in order for the program to be fully operational; however, if a nonessential server stops running, users can still access the program.
Move a product option between servers	In the **Application Server Instances and Enabled Product Options** pane, click the product option listing, and then do one of the following: • Click the **Move Up** or **Move Down** button until the listing is located below the server that you want to host the option. • Drag and drop it below the server that you want to host the option.
Disable a product option	In the **Application Server Instances and Enabled Product Options** pane, click the product option listing, and then do one of the following: • Click **Disable**. • Drag and drop the listing to the **Disabled Product Options** pane. **NOTE:** Disabled product options remain installed but are deactivated. Essential product options cannot be disabled.
Enable a disabled product option	In the **Application Server Instances and Enabled Product Options** pane, select the server that you want to host the product option, and then in the **Disabled Product Options** pane, click the listing for the product option and do one of the following: • Click **Enable**. • Drag and drop the listing to the **Application Server Instances and Enabled Product Options** pane.
Remove a server	Select **Delete on save** beside the server listing. **NOTE:** Only servers that are not hosting product options can be removed. To subsequently add a server, use the Configure Server tool.

3. Click **Save**, and then click **Exit**.

The designation of servers and production options as either essential or nonessential and the state and accessibility of servers has implications for the health of the site and, therefore, the ability to log in and use the Proficy Workflow program. For more information, see System Health and Program Use on page 4.

Monitor system configuration and status

After installing this application, you can monitor the configuration of the system, including which servers and product options are installed and whether those components are designated as essential. In addition, you can ascertain the operational status of the configured servers.

1. In the navigator, click **Proficy System** > **Proficy System**.
2. In the **Displays** panel, click **System Status**.
   The **System Status** display appears in the workspace, listing the servers configured for the site. For each server, the display reflects whether the server is designated as essential; the essential and nonessential product options (or services) hosted on the server, if applicable; and whether the server is *Stable* or *Unreachable*.

   NOTE: The **System Status** display is read-only. However, you can use the **Configure Site** tool to modify system configuration, including designating whether servers or the product options that run on them are essential, moving product options between servers, disabling product options, and/or deleting servers that are not hosting product options.

Modify the server configuration for a remote client

Use the **Server Configuration** tool to synchronize any changes you may have made to the Proficy application server with remote clients.

IMPORTANT: The **Server Configuration** tool is available only for client-only installations.

1. On the client computer, click **Start** > **All Programs** > **Proficy** > **Proficy Workflow** > **Configuration** > **Configure Client**.
   The **Server Configuration** tool appears.
2. Optional: In the **Computer Name** field, enter the name of the computer where the server you want to connect to is installed.
   - If you are configuring a full server or in a multiple server environment, enter the name of the computer that the server you want to connect to is installed on.
   - If you are configuring a server cluster environment, enter the cluster name used when you set up your cluster.
3. Optional: In the **Instance Name** field, enter the name of the server instance you want to connect to.
4. Optional: In the **HTTP Port** field, enter the port number required to allow communication with the server.
5. Click **Save**, and then click **Exit**.

Modify the Microsoft Active Directory Services

The **Configure AD LDS Integration** tool provides the ability to configure Active Directory Lightweight Directory Service for your production environment.

1. On the server machine, click **Start** > **All Programs** > **Proficy** > **Proficy Workflow** > **Configuration** > **Configure Directory Services**.
   The **AD LDS Integration** page appears.
2. To integrate Active Directory Lightweight Directory Services (AD LDS), do one of the following.

If AD LDS is...	Then...
NOT installed	You are given information regarding its use. If it is not required, then click **Next**.
Installed in a test and/or development environment	Select the **Do not use Microsoft Directory Services** check box, and then click **Next**.
Installed in a production environment	Click **Next**.

3. If you are using AD LDS, perform the following procedure.

a) Clear the **Do not use AD LDS** check box.
b) In the **Directory Instance** section, in the **Name** field, enter an instance name for the ADAM directory.
c) In the **Port (LDAP)** and **Port (SSL)** fields, enter valid port numbers.
d) In the **User Credentials** section, in the **Name** field, enter the name of a user that is a member of the local computer's Administrators Group.
e) In the **Domain** field, enter the name of your company's domain.
f) In the **Password** field, enter the password for the user you entered in the **Name** field.

4. Click **Save**, and then click **Exit**.

Modify your Proficy application server database

The **Configure Database** tool provides the ability to make changes to your SQL Server database, as well as change the database you want to connect to.

You must install SQL Server 2012 or SQL Server 2008 before you install Proficy Workflow. For more information, see Software Requirements on page 12.

IMPORTANT: Changes to the SQL Server database recovery model have occurred. For more information, please visit the GE Intelligent Platforms Knowledge Base website at http://support.ge-ip.com/support/index?page=kbchannel, and then search for the related article, KB16204.

In order for Proficy Workflow to connect to any edition of Microsoft® SQL Server 2012, you must configure SQL Server to enable the *sysadmin* role for the applicable login account. For more information, see Enable Connection between Proficy Workflow and SQL Server 2012 on page 30.

The Proficy Workflow installation automatically selects the default SQL Server instance. If SQL Server 2012 and SQL Server 2008 are both installed, SQL Server 2008 may be the default instance. In this scenario, if you want to use SQL Server 2012 instead, you must select this instance as the default as part of manually configuring your SQL Server settings. For instructions, see steps 2 on page 67 and 3 on page 67 of this procedure.

1. Click **Start** > **All Programs** > **Proficy** > **Proficy Workflow** > **Configuration** > **Configure Database**.
   The **Database Configuration** page appears.
2. Specify the SQL Server database settings for this application based on the configuration of your environment.

To configure SQL Server settings...	Then...
Automatically	1. Select the **Use a local database with Windows Authentication** check box. **NOTE:** To use this option, the following SQL Server conditions apply: • Installed locally, AND • Designated as default Local Host, AND • Uses **Windows Authentication** 2. Proceed to step 4 on page 68.
Manually	1. Clear the **Use a local database with Windows Authentication** check box. **NOTE:** To use this option, the following SQL Server conditions must NOT apply: • Installed locally, OR • Designated as default Local Host, OR • Uses **SQL Server Authentication** 2. Proceed to step 3 on page 67.

3. Specify your SQL Server settings, as follows:
   a) In the **Server** field, enter or select the name of the SQL Server that you want to connect to.

NOTE: If the SQL Server is installed locally, enter localhost.

b) In the **Database** field, enter the name of your SQL Server database, or click the drop-down arrow to search for all databases located on the specified server.

NOTE: If the specified database does not exist, it will be created for you.

c) From the **Authentication** list, select the type of authentication that you want to use, and then proceed based on your selection.

- If you select **Windows Authentication**, proceed to step 4 on page 68.
- If you select **SQL Server Authentication**, proceed to step 3.d on page 68.

d) Enter the **User Name** and **Password** that are configured for SQL Server authentication, and then proceed to step 4 on page 68.

4. Click **Save**, and then click **Exit**.

Modify your Proficy Vision web server database

The **Database Connect Utility** enables you to change your SQL Server configuration information for the web server. As a result, you do not have to install the web server again in order to make changes. After using this tool, parameters are stored in encrypted configuration files.

1. To start this tool, do one of the following:
   - In the directory, <installdir>/Program Files/Proficy/ProficyVision/ServerTools, double-click UpdateDatabaseConfiguration.cmd.
   - In a command prompt window, start the tool.
2. When prompted, confirm that you want to update the database connection information.
3. At the command prompt, enter the SQL Server machine name, database name, user name, and password. The Predix service is restarted, which takes several minutes.
4. Start or refresh your web server's browser to see the updates.

Modify your Proficy Vision web server password

Access to the web server by an administrator is protected by a Secure Shell (SSH) protocol. The SSH password is generated randomly during installation. Follow this procedure to change the SSH password.

1. Download the Jasypt Java library from http://www.jasypt.org/.
2. At a command prompt, enter the following command to generate an encrypted SSH password, and then replace NewPassword with a password of your choice: <jasypt installation>/bin/digest.sh algorithm="SHA-512" stringOutputType=base64 input=NewPassword prefix="{CRYPT}" suffix="{CRYPT},admin"
3. After the encrypted password string is generated, stop the Predix kernel.
4. In /kernel/etc/user.properties/kernel/etc/, open users.properties.
5. Set admin= to the generated password string by copying and pasting it into the file.
6. Restart the Predix kernel.

Configure a server instance

The **Configure Server** tool is used to create a Proficy application server instance, as well as to configure server clustering.

IMPORTANT: The default user setting for this service is Local System Account. When upgrading your application, the user setting will return to the default setting.

NOTE: If you are configuring servers for clustering, you must ensure that you run this tool on all nodes of the cluster.

1. On the server machine, click **Start** > **All Programs** > **Proficy** > **Proficy Workflow** > **Configuration** > **Configure Server**.
2. Select the **Create a Proficy Application Server Instance** option.

3. In the **Name** field, enter a name for the server instance.
4. Optional: In the **Description** field, enter a description for the server instance.
5. Click the **Advanced Configuration** arrow.
6. Select or clear the **Do not create Windows Service for this Server Instance** check box, depending on whether you want this server instance to run as a Windows service.
7. If you are configuring the server instance to run as a Windows service, and the architecture of the computer you are configuring the instance on is 64-bit, configure the **Run service under the following architecture** setting to indicate your preference for operational mode as either 32-bit or 64-bit.
8. In the **Service Ports** fields, enter the port numbers for each of the service port types.
9. In the **IP Address** field, enter the IP address of the server instance.
10. In the **Port** field, enter the port number for the server instance.
11. Click **Save**, and then click **Exit**.

Configure product options

Using the **Configure Product Options** tool, you can install and configure Proficy product options that you license and/or service providers that you have created .

Proficy services must be stopped on the server prior to configuring product options.

If you have created and packaged your service provider, you must copy it to an accessible location.

NOTE: Refer to Architecture Considerations on page 20 for guidelines on deploying service providers based on architecture mode.

IMPORTANT: Product Options Installation Information. When using the ActiveX Task List, product option updates made on the server are not automatically deployed to applications using the Task List. The ProficyUpdater.exe application must be run manually, with administrative privileges, in order to deploy production option updates on each client machine using ActiveX Task List.

Install one of the following server types:

1. On the server machine, click **Start** > **All Programs** > **Proficy** > **Proficy Workflow** > **Configuration** > **Configure Product Options**.
   The **Configure Product Options** tool appears, displaying the product options currently configured on the server, including those included by default as part of the server installation.
2. Proceed as applicable based on whether you are installing or uninstalling a product option:

If you are...	Then do this...
Installing a product option.	1. Click **Install**. Your directory opens at the ProductOptions folder within the Proficy Workflow installation directory. 2. Proceed to step 3 on page 69.
Uninstalling a product option. **NOTE: You cannot uninstall the default product options that are included in the server installation.**	1. Select the product option you want to uninstall. 2. Click **Uninstall**. 3. Proceed to step 7 on page 70.

3. Select the product option file you want to install, and then click **Open**.

   NOTE: You can select only one product option at a time to install.

   The product option is installed, and then the **Configure Site** dialog box appears.
4. In the **Application Server Instances and Enabled Product Options** pane, select the server that you want to host the product option.
5. In the **Disabled Product Options** pane, click the listing for the product option, and then do one of the following:

- Click **Enable**.
- Drag and drop the listing to the **Application Server Instances and Enabled Product Options** pane.

6. Indicate whether the product option is essential by selecting or clearing the **Essential** check box.
7. Click **Save**, and then click **Exit**.

Change architecture mode

When initially installing a Proficy application server or extension server (that is, Workflow or User) on a 64-bit computer, you can elect to run the server in either 32-bit or 64-bit mode. If your environment changes subsequent to installation, you can use the **Configure Server** tool to change the architecture mode accordingly.

1. On the machine that the server is installed on, click **Start** > **All Programs** > **Proficy** > **Proficy Workflow** > **Configuration** > **Configure Server**.
   The **Configure Server** tool appears.
2. Select the **Create a Proficy Application Server Instance** option.
3. Click the **Advanced Configuration** arrow.
4. In the **Run service under the following architecture** section, select 32-bit or 64-bit to indicate the operational mode you want to switch to.
5. Click **Save**, and then click **Exit**.

Add or remove performance counters

Using this procedure, you can manually add performance counters to your system, or remove them. You must have administrative privileges in order to perform this action.

1. From the following location, you can add or remove performance counters: <installfolder>/ProficyServer.exe.
2. In ProficyServer.exe, enter the applicable command line.

To...	Enter...
Add counters	<installfolder>ProficyServer[exe] / installperformancounters
Remove counters	<installfolder>ProficyServer[exe] / uninstallperformancounters

IMPORTANT: If the counters are added/deleted (installed/uninstalled) after the server is started, then the server and the performance monitoring tool (perfmon) must be re-started for this change to take effect.

Upgrading Proficy Workflow and Proficy Vision

Read this topic for general information about upgrading your applications.

IMPORTANT: When you upgrade Proficy application server, you must also upgrade all of the remote clients that connect to that server to use the same version of Proficy Workflow. You can upgrade Proficy Workflow without having to uninstall the program.

Upgrade Paths

The following upgrade paths are supported:

- From Proficy Workflow 2.1 to Proficy Workflow 2.5
- From Proficy Workflow 2.2 service pack 1 (SP1) to Proficy Workflow 2.5
- From Proficy Vision 6.2 to Proficy Vision 6.3

NOTE: You must first upgrade or uninstall any versions prior to Proficy Vision 6.2 before upgrading to Proficy Workflow 2.5.

- From Proficy Workflow 2.1 to Proficy Workflow 2.2 service pack 1 (SP1)
- From Proficy Workflow 2.0 to Proficy Workflow 2.2 service pack 1 (SP1)
- From Proficy Workflow 1.5 service pack 4 (SP4) to Proficy Workflow 2.2 SP1

NOTE: You must first upgrade Proficy Workflow 1.5 SP4 to Proficy Workflow 2.0.

If you are upgrading from an earlier version of Proficy Workflow, contact Technical Support.

- Legacy Certificates on page 71
- Upgrading Extension Servers on page 71
- Upgrading Microsoft® .NET Framework 4.5 (Full Framework) on page 71
- Upgrading Web-based Forms for the Task List on page 71
- Upgrading a Clustered Environment on page 71
- SQL Server Database Replication on page 72
- Password Security on page 72
- Windows Users on page 72

Legacy Certificates

Starting with Proficy Workflow 2.5, legacy certificates are no longer supported.

Upgrading Extension Servers

If you are installing or upgrading an extension server (Workflow or User), you must have already installed or upgraded a Proficy application server of the same version to host the Core services on a separate machine.

Upgrading Microsoft® .NET Framework 4.5 (Full Framework)

NOTE: Custom display or form assemblies that target earlier versions of .NET will continue to function as before. However, saving changes made to such custom assemblies requires that they be upgraded, which is accomplished in different ways, based on the version of .NET:

- For an assembly that pre-dates .NET 4.0, you must upgrade the assembly when you open it. Failure to do so results in an error and the inability to save the edited assembly.
- For an assembly that targets .NET 4.0, the assembly is upgraded automatically when opened, and changes to such assemblies can be saved as before.

Service providers that target versions of the .NET framework before version 4.5 must be recompiled targeting .NET 4.5.

Upgrading Web-based Forms for the Task List

If you have web-based forms as part of an existing workflow that you have created prior to the release of Proficy Workflow 2.2 SP1, you must bind them again inside the Form activity in order for them to function in the Task List.

NOTE: This upgrading issue affects existing web-based forms only, and not HTML5 web forms that are created in Proficy Workflow 2.2 SP1.

Upgrading a Clustered Environment

After upgrading Proficy Workflow on the primary server machine, you must reconfigure that machine as the primary server in the cluster, as well as reconfigure the failover server in the cluster.

SQL Server Database Replication

When upgrading the application, if you are using a replicated database and have replication turned on, you must turn it off, upgrade, and then turn it on again. You must also upgrade the replicated database. For more information, see Upgrade a replicated database on page 78.

Password Security

During an upgrade installation, the account lockout capability is automatically enabled; all other password security features are disabled, by default. To enable any of the other password security features, you must use the **Configure Security** tool after the upgrade installation has successfully completed.

Windows Users

Proficy Workflow 2.0 supports Windows domain names with personnel names and login names. If you choose to use the new functionality included with Proficy Workflow 2.0 (that is, Active Directory Universal Groups mapped to Proficy groups), then when your Windows users log in, their personnel name and login name will both be updated to include the domain name, and the personnel name will change to match the login name. For example, the personnel name *John Smith* and login name *johnsmith* will both change to *<domain name>\johnsmith*.

WARNING: If you were using Windows user accounts in a prior version of Proficy Workflow, any workflows that reference individual users will no longer work! These personnel names will NOT be updated when the Windows users log in. You must manually change these names to include the domain name with a back slash character between the domain name and personnel name. However, if you reference personnel classes in your workflows, no change is required; the workflows will work as they did in the previous version of Proficy Workflow.

Upgrade to a newer version of Proficy Workflow

This procedure describes how to upgrade your version without uninstalling the previous version.

NOTE:

- Administrative user names and passwords used during your initial installation are not retained during upgrading process. You can set these credentials again during this process.
- Starting with Proficy Workflow 2.5, legacy certificates are no longer supported.

1. Execute the installation software. If this splash screen does not appear, run InstallFrontEnd.exe on the root directory of the installation folders.

   NOTE: If you have legacy certificates installed, follow this procedure:

   - Open the Configure Certificates tool, and then click **Save**.
   - At the **Security Certificates** page, select the Generate new and unique certificates option.
   - After the certificate configuration process finishes successfully, start the installation process again.
2. Review the license agreement, and then click **I Agree**.
   The **Web Service** page appears.
3. Specify the Internet Information Services (IIS) domain and website where the application server web service is hosted.
   a) In the **Host Name** field, enter your IIS server domain name that you have previously created.
   b) In the **Website** field, select your HTTPS-configured website.
4. Specify the password for the SQL Server user account, KSPUser, that will be created for the web service.

   NOTE: This password must comply with your SQL Server password complexity rules. You may enter an existing password, or create a new one.

   a) In the **Password** field, enter your user account password.
   b) In the **Confirm Password** field, enter your password again.

   The **Application Upgrade** page appears.

5. Optional: If you want a backup of your SQL Server database and have not performed your own backup, select the Do not back up the database automatically option.

   TIP: At any time during the configuration process, you can click **Back** to return to a previous page to change your settings.

   IMPORTANT: Changes to the SQL Server database recovery model have occurred. For more information, please visit the GE Intelligent Platforms Knowledge Base website at http://support.ge-ip.com/support/index?page=kbchannel, and then search for the related article, KB16204.
6. Click **Install**.
   The **Installation** page appears, displaying the status of each installation step.
7. When the installation is complete, click **Exit**.

NOTE: If the installation fails, or you want to change a configuration setting after installation completes, you can open the appropriate standalone component to configure the required information. For more information, see this section: Post-installation Configuration on page 63.

Notes on Upgrading Proficy Vision

This topic provides information related to upgrading for this release.

Product Changes

GE Intelligent Platforms is undergoing a web technology transformation. To stay current with the latest web and mobile technologies, we have introduced a new HTML5-based Proficy Vision container, as well as Proficy Historian-based web content, in this version.

As a result of these changes, content previously released for Proficy Vision 6.2 and earlier versions is not compatible with this HTML5 release, including web content previously with:

- Proficy Plant Applications 6.2
- Proficy Real-Time Operational Intelligence (RtOI)
- Equipment Insight

Web content for all Proficy products and solutions will be continuously upgraded and improved. If you are using content from one of these products, contact Technical Support for more information about upgrading.

Upgrade Path

You must first upgrade or uninstall any versions prior to Proficy Vision 6.2 before upgrading to Proficy Workflow 2.5.

Plug-ins

Any plug-ins that you have installed that are related to Proficy Vision 6.2 or earlier are not supported in the upgraded version.

Ports and IIS

Proficy Vision 6.3 now utilizes a new web server and no longer requires Internet Information Services (IIS). When upgrading, you must be aware of the ports that you want to use for your web server.

Using IIS with Proficy Vision 6.2

If you have been using IIS in a previous version of Proficy Vision, but it is not required for other web sites in your organization, then do the following:

- Go into IIS and delete the bindings for HTTPS.

  TIP: For instructions, read the Microsoft Windows® Server Internet Information Services (IIS) Manager article, Add or Edit Site Binding Dialog Box).

Using IIS with Proficy Vision 6.3

If you are upgrading to Proficy Vision 6.3 and IIS is still required for other applications in your enterprise, you must install Proficy Vision on a new port (default: 443):

- During installation, at the **Web Server Details** page, enter a new port (for example, myvisionservername:444).

  TIP: You must remove the old port and add the new port. Restarting the Internet Information Services (IIS) service alone will not unbind the ports.

Upgrade custom forms

Before upgrading and starting the Proficy Workflow 1.2 or 1.5 server, ensure that all of your custom form DLLs are located in the following directory: ..\Data\AllUsers\Displays.

If you added forms or user displays using Proficy Workflow 1.0 or 1.01, and those forms had dependencies on any Proficy assemblies, there are additional steps for upgrading.

For each form or user display in the system, do the following:

1. Check for errors.
   - In the navigator, select the form or user display, and then click Global Viewer. If additional upgrade steps are required, an error displays in the Feedback Zone, indicating that the existing item could not be loaded.

     NOTE: If you are using GEFanuc.Platform.FormsLibrary.dll, skip to step 3 and use the new file, Proficy.Platform.FormsLibrary.dll, found in the **Program** folder in the install directory.
2. Update the project.
   a) In Visual Studio, open the source code project you originally used to build the custom form.

      NOTE: This source code should be found somewhere on your system; it is not persisted in the Proficy Workflow database.
   b) Update references to GEFanuc assemblies.

      View the project's references to see the list of assemblies it is dependent upon.

      NOTE: Since Proficy Workflow version 1.01, the Proficy assemblies have been renamed from *GEFanuc.*.dll* to *Proficy.*.dll*; therefore, any references to assemblies named *GEFanuc.** must be removed and re-added to point to the renamed assembly. For example, if the project previously referenced *GEFanuc.Platform.Core.DisplayFramework.dll*, then the project must be updated to reference *Proficy.Platform.Core.DisplayFramework.dll*.
   c) Update references to *GEFanuc* namespaces.
      - The namespaces have also been changed from *GEFanuc.** to *Proficy.**. Therefore, any other references to *GEFanuc* in your project must also be changed to Proficy.
3. Build the project.
   - Build your project and continue fixing errors until you have a successful build.
4. Save your changes.

   In the Proficy client, select the form or user display in the navigator and open it in the **Display Editor**. An error may display indicating that the assembly or class is invalid. If the error displays, do the following:
   a) In the **.NET Assembly** field, browse to the updated version of the assembly you want to use for the form.
   b) In the **Class Name** field, select the appropriate class name to use.
   c) Click **Save** to save your changes to the server and make the form available to other clients.
5. Validate the form.
   - Open the form in the Global Viewer or run it in a workflow to ensure the form works as expected.

Database Migration

If you have created your Proficy Workflow database in a development or test environment, you can migrate your database to another environment without having to import or recreate all of the data.

This information is intended for advanced users only. If you are unsure of the steps to proceed, contact Technical Support.

IMPORTANT: Changes to the SQL Server database recovery model have occurred. For more information, please visit the GE Intelligent Platforms Knowledge Base website at http://support.ge-ip.com/support/index?page=kbchannel, and then search for the related article, KB16204.

You must be familiar with backing up and restoring databases in order to successfully migrate your Proficy Workflow database from one SQL Server environment to another.

Custom Workflow Activities and Service Provider Dependencies

If you have custom workflow activities or dependencies for custom service providers that are not packaged with the service provider, you must copy and move those files manually from the source Proficy application server machine to the destination Proficy application server machine.

Single Server and Multi-server Environments

If you are moving from a multi-server environment to a single server environment, you can remove the extra sites when you run the **Configure Site** tool. If you are moving from a single server environment to a multi-server environment, there are extra steps to configure the sites. For more information, see Configure Site.

Move a database

You can move a SQL Server database from one machine to another to allow you to use the same data in another environment, such as moving from a development environment to a test environment.

IMPORTANT: Changes to the SQL Server database recovery model have occurred. For more information, please visit the GE Intelligent Platforms Knowledge Base website at http://support.ge-ip.com/support/index?page=kbchannel, and then search for the related article, KB16204.

- The version of Proficy Workflow must be the same on both the source machine and the destination machine.
- All of the associated software that is installed on the source machine must also be installed on the destination machine (for example, Proficy Historian, and so on).
- You must be familiar with backing up and restoring databases in order to successfully migrate your Proficy Workflow database from one SQL Server environment to another.

1. On the source SQL Server machine, make a backup copy of the database to either a network drive or a portable device, such as a CD.
2. On the destination SQL Server machine, restore the database in SQL Server.

NOTE: The remaining steps are performed on the destination server machine; that is, the machine that hosts the SOAServer that will point to and use the database on the destination SQL Server machine.

3. On the server machine, run the Configure Database tool, and then click **Save**.
4. On the server machine, run the Configure Server tool, and then click **Save**.
5. On the server machine, run the Configure Site tool to ensure that all of your extension servers and product options are configured correctly, and then click **Save**.
6. On the server machine, run the Configure Directory Services tool, and then click **Save**.
7. Start the Proficy services.

Proficy Reporting Database

Proficy Workflow includes an option to install a reporting database. This database can be used with any valid reporting tool, and allows you to build reports on up-to-date data that you synchronize from your production database.

For more information on the Proficy Reporting Database, see Reporting.

Install the reporting database

The reporting database allows you to use the data synchronized from your production database to build reports for your facility. You can use any reporting tool to extract the information from the reporting database and create your reports.

NOTE: If you plan on frequent synchronization for reporting purposes, we recommend that you replicate your database and run reporting against the replicated database. This measure reduces the risk of system timeout or shutdown due to locking of tables in the production database. If upon trying to save data after replication, you receive an error similar to "System.Data.SqlClient.SqlException (0x80131904): Length of LOB data (88064) to be replicated exceeds configured maximum 65536," use SQL statements to increase the volume of data to replicate.

Example:

```
sp_configure 'max text repl size', 2147483647
GO
RECONFIGURE
GO
```

For information on setting up database replication, visit the Microsoft Developer Network website and review the article, SQL ServerReplication.

You must have installed a supported SQL Server version before you install the reporting database (see Software Requirements on page 12). In addition, you must select the SQL Server Integration Service (SSIS) component when you install SQL Server. Select the SQL Reporting Services component, as well, if you want to use SQL as your reporting tool.

NOTE: We recommend that you install the reporting database on a separate computer from the production database to prevent performance issues on the production database. In this scenario, additional configuration changes are required. Refer to Configure Component Services on page 77 for more information. However, if the Proficy application server computer meets the requirements for both databases, they can be installed on the same computer.

If both SQL Server 2008 and SQL Server 2012 are installed, the integration services used for the reporting database are those for SQL Server 2012.

1. From the application splash screen, click **Install Proficy Reporting Database**.

   NOTE: If this splash screen does not appear, run SetupReporting.exe on the root directory of the installation folders.

   The **License Agreement** page appears.
2. Review the license agreement, and then click **I Agree**.
   The **Installation Folder** page appears.
3. Accept the default destination folder or browse for a new location, and then click **Next**.
4. In the **Configure Reporting SQL Server** area, enter the following information, and then click **Next**.
   a) In the **Server** field, accept the default value if the reporting database is on the local machine with the default instance. If the SQL Server named instance is used, enter the SQL Server name and instance name; for example, <*servername*>\<*instance name*>.

      NOTE: The Reporting SQL Server must be local.
   b) In the **Database** field, enter the name of the reporting database. This creates a new database; however, if a database of the same name already exists, this database will append to the existing one.

c) From the **Authentication** list, select the type of authentication you want to use. If you choose to use integrated security, select **Windows Authentication**; otherwise, select **SQL Server Authentication**, and then enter the user name and password for the SQL Server.

5. In the **Configure SQL Server** area, perform one of the following actions:
   - Leave the **Use a local SQL database with Windows Authentication** check box selected, and then click **Next**.
   - Clear the **Use a local SQL database with Windows Authentication** check box, enter the following information, and then click **Next**.
     1. In the **SQL** field, enter the name of the SQL Server where the SQL database is located.
     2. In the **Database** field, enter the name of the production (SQL) database that you will connect to for synchronization.
     3. From the **Authentication** list, select the type of authentication you want to use. If you choose to use integrated security, select **Windows Authentication**; otherwise, select **SQL Server Authentication**, and then enter the user name and password for the SQL Server.
6. In the **Proficy Workflow Server Configuration** area, enter the following information, and then click **Next**.
   - In the **Server computer name** field, enter the fully qualified name of the server computer.
7. In the **Configure Security** area, enter an Administrator user name and password.

   IMPORTANT:
   - You cannot use a Windows user name and password to configure security for the reporting database; it MUST be a valid Proficy Workflow Administrator user name and password.
   - The **Advanced user authentication settings** (that is; Enable SSO, Enable user password change at login, Enable user account lockout, and enable user password complexity rules) do not apply when installing the reporting database.
8. Click **Install**.
9. When the installation is complete, click **Exit**.

Configure Component Services

If your production database is on a different computer than the Proficy Reporting Database, the following configuration changes are required.

IMPORTANT: You can perform these steps either before or after installing the Proficy Reporting Database; however, you must complete these configuration changes before you run your reporting data synchronization.

NOTE: For this procedure, your production database server is the "server," while the reporting database server is the "client."

1. Verify that the Distributed Transaction Coordinator service is running on both the server and client computers.
   a) From the **Start** menu, point to **Administrative Tools**, and then click **Services**.
   b) If the Distributed Transaction Coordinator service is not running, right-click it, and then click **Start**.
2. On the server computer, from the **Start** menu, point to **Administrative Tools**, and then click **Component Services**.
3. In the left navigation tree, click **Component Services**, and then expand **Computers**.
4. Right-click **My Computer** and select **Properties**.
   The **My Computer Properties** dialog box appears.
5. Click the **MS DTC** tab.

   IMPORTANT: If you are using Windows 7, Windows Server 2008, or Windows Server 2012, you must use the following path to retrieve these computer properties: Component Services> Computers>My Computer>Distributed Transaction Coordinator>Local DTC
6. Click **Security Configuration**.
   The **Security** page appears.

7. Select the following check boxes:
   - **Network DTC Access**
   - **Allow Remote Clients**
   - **Allow Inbound/Outbound Administration**
   - **Enable Transaction Internet Protocol (TIP) Transactions**
8. Click **OK**.
   A message appears telling you "MS DTC Service will be stopped and restarted. All dependent services will be stopped. Please press Yes to proceed." Click **Yes**.
9. In the **My Computer Properties** dialog box, click **OK**.
10. If required, reboot your production database server.

    NOTE: We recommend that you reboot your production database server.
11. On the client computer, repeat steps 2 on page 77 through 6 on page 77.
12. Select the **Network DTC Access** and **Allow Inbound/Outbound Administration** check boxes.
    The DTC Service is stopped and restarted.
13. Restart the client computer.
14. Verify that the Distributed Transaction Coordinator service is running on both the server and client computers, and, if required, repeat step 1 on page 77.

Uninstall the reporting database

When you uninstall the reporting database, you can choose to remove it completely from the computer or maintain the database but lose the ability to synchronize the data from your production database. Uninstalling the reporting database does not affect the production database or the data contained in it.

1. From **Control Panel**, double-click **Add or Remove Programs**.
   The **Add or Remove Programs** dialog box appears, displaying all of the programs installed on the computer.
2. Select **Proficy Reporting**, and then click **Remove**.
3. In the confirmation message box, click **Yes**.
4. In the **Uninstall Reporting** message box, click **Yes** if you want to completely remove the reporting database from the computer. If you select **No**, the reporting database remains on the computer, but the ability to synchronize with the production database is lost; however, you can still run reports on the data stored in the database.

Upgrade a replicated database

When upgrading the application, if you are using a replicated database and have replication turned on, you must turn it off, upgrade, and then turn it on again. You must also upgrade the replicated database.

1. Disable any scheduled synchronization jobs for the Proficy Reporting Database.
2. Open the **Services** window to stop all services: from the **Start** menu, go to **Control Panel** > **Administrative Tools** > **Services**.
3. In Microsoft SQL Server Management Studio, generate the create and drop scripts:

   NOTE: For use later in this procedure, you must note the location of where you saved the scripts.

   a) In the Subscriber/Distributor instance, right-click the **Replication** folder, and then click **Generate Scripts**.
   The **Generate SQL Script** dialog box appears.
   b) To generate the **Create** script, in the **Script the commands** section, select To create or enable the components, and then click **Generate Script**.
   c) To generate the **Drop** script, in the **Script the commands** section, select To drop or disable the components, and then click **Generate Script**.
4. To disable replication, execute the **Drop** script.
5. Verify that all objects beneath the SQL Server Management Studio **Replication** folder have been deleted.

6. From the installation directory where your SQL Server is hosted, go to Program Files\Proficy\Proficy Workflow \Program, run ProficyInstaller to upgrade the ProficyServer programs and database.
7. Edit the **Create Replication** script.
   a) In SQL Server Management Studio, from the File menu, go to **Open** > **File**.
   b) Navigate to the file where you saved the scripts generated in step 3 on page 78.
   c) Select the **Create SQL** script.
   d) Locate the section denoted by this comment, /****** End: Script to be run at Publisher ******/, and then add the following lines after it.

      NOTE: You must change the name of the Distribution database and the user names to match your system.

```
-- Create users in the Distribution database
USE [DistributionDB];
GO
CREATE USER [QASYSTESTSQLSRV\SqlDistAgent]
  FOR LOGIN [QASYSTESTSQLSRV\SqlDistAgent]
EXEC sp_addrolemember N'db_owner',
  N'QASYSTESTSQLSRV\SqlDistAgent';
CREATE USER [QASYSTESTSQLSRV\SqlLogReaderAgent]
  FOR LOGIN [QASYSTESTSQLSRV\SqlLogReaderAgent];
EXEC sp_addrolemember N'db_owner',
  N'QASYSTESTSQLSRV\SqlLogReaderAgent';
  CREATE USER [QASYSTESTSQLSRV\SqlSnapshotAgent]
  FOR LOGIN [QASYSTESTSQLSRV\SqlSnapshotAgent];
EXEC sp_addrolemember N'db_owner',
  N'QASYSTESTSQLSRV\SqlSnapshotAgent';
```

8. Add all of the passwords back into the file. The Create Generation process does not write the user account passwords to the file.
   a) Find all occurrences of @job_password = null.
   b) Replace null with the log on password that precedes it. If the preceding @job_login is also null, do not edit the password so that it remains set to null.

```
-- Before:
exec [SystemTest2v2].sys.sp_addlogreader_agent @job_login = N'QASYSTESTSQLSRV
\SqlLogReaderAgent', @job_password = null
-- After:
exec [SystemTest2v2].sys.sp_addlogreader_agent @job_login = N'QASYSTESTSQLSRV
\SqlLogReaderAgent', @job_password = 'proficy'

-- Do not change passwwords for null job_logins
exec [SystemTest2v2].sys.sp_addqreader_agent @job_login = null, @job_password = null
```

9. Execute the **Create Replication** script.

   NOTE: This script will have some errors because it will try to publish database objects that were removed from the database as part of the upgrade.
10. Re-enable the replication, and then add the new database tables and objects to the publication in order to push them to the replicated database:
    a) Expand your database directory and the **Replication** folder, right-click **Local Publications**, and then select **Properties**.
    b) Select **Articles**, and then select all unchecked items to include them in the publication.

       NOTE: The subscription must be re-initialized to include the new articles. We recommend re-initializing all articles in the subscription using a full snapshot. For instructions, read the Microsoft Developer Network article, Reinitializing a Subscription
11. After replication is working against the upgraded database, install the Reporting upgrade, and point it to the replicated database.

12. Test reporting synchronization by running a manual Sync from the Proficy client.

Remote Desktop Session Host

This information is intended for system integrators, IT administrators, and engineers responsible for setting up and optimizing a Proficy Workflow Remote Desktop Session Host environment.

This information assumes familiarity with your network environment, as well as:

- Microsoft® Windows® Server 2008 R2
- Microsoft® Windows® Server 2012
- Microsoft® Windows Licensing
- Microsoft® Windows Remote Desktop Services
- Citrix® technologies including licensing

Remote Desktop Services (Terminal Services)

With Remote Desktop Services for Microsoft® Windows® Server 2008 R2 and Windows® Server 2012, you can centrally manage and execute Proficy Workflow.

The Remote Desktop Session Host environment is a thin-client architecture where all application processing occurs centrally on the server. By installing a small piece of thin-client software from Microsoft® or connecting through an Internet Explorer 7 (or higher) browser, thin clients can initiate and run individual instances of Proficy Workflow on the server. Only graphic, keyboard, and mouse instructions are sent back and forth between the client and the server, which minimizes network traffic.

Using Remote Desktop Services provides:

Ease of maintenance	You install only one copy of Proficy Workflow on a server, from which multiple users can run clients. Upgrades and SIMs need to be installed only on the server.
Remote access with built-in technology	With Remote Desktop Communication (RDC) and Internet Explorer 7 or higher, clients from Windows 7 can connect to the Proficy Workflow Remote Desktop Session Host to access Proficy Workflow.
Security	Encryption and other security measures protect the data exchanges between the Proficy Workflow Remote Desktop Session Host and the clients.
Lightweight client machines	The Proficy Workflow Remote Desktop Session Host locally processes the software that the clients execute. Clients connecting to the server through a remote desktop session do not need the processing power usually required to run Proficy Workflow.
Specialized environments	Remote Desktop Services allows you to tightly control user accounts. For example, you can configure user accounts to start and execute a single program (Proficy Workflow). Proficy Workflow automatically starts at log in, and the users do not have access to the Windows desktop. When they exit Proficy Workflow, they log out of the Remote Desktop Session Host account.
Handheld environments	Remote Desktop Services enables wireless handheld devices to display Proficy Workflow.

Controlled access to files	With Windows file protection, you can limit the directories users are allowed to access and modify, such as for forms, displays, and import/export files.

Proficy Workflow Remote Desktop Session Host Environment
Proficy Workflow Remote Desktop Session Host allows multiple clients to run individual instances of Proficy Workflow from one server.

Thin clients access the Remote Desktop Session Host through Microsoft® Remote Desktop Protocol (RDP) or Citrix® Independent Computing Architecture (ICA) protocol. No Proficy Workflow software is installed or runs on the thin-client machine.

A separate session of Proficy Workflow runs on the Remote Desktop Session Host for each thin client. This allows very thin clients with minimal client-side resources to execute an individual instance of Proficy Workflow. The users' experience is nearly identical to running Proficy Workflow on their local machines. If you have clients and servers in your Proficy Workflow Remote Desktop Session Host environment, you can access and manage any of the servers from a thin client.

Getting Started

Before installing Proficy Workflow on a Windows® Server 2008 R2 or computer, you must enable and set up the Windows Remote Desktop Session Host.

For the most up-to-date Remote Desktop Session Host information for Windows® Server 2008 R2, visit the Microsoft® web site at:

http://technet.microsoft.com/en-us/library/dd647502(WS.10).aspx

IMPORTANT: Before installing the Proficy Workflow Remote Desktop Session Host, be aware of its limitations and software and licensing requirements. You should also spend some time planning a sound network and security strategy, and user and machine naming conventions.

Proficy Workflow Remote Desktop Session Host Limitations
The Proficy Workflow Remote Desktop Session Host has a number of limitations and assumptions.

- Location-based functionality in Proficy Workflow does not work with Remote Desktop Services. That is, workflow tasks that are assigned to a location, key set permissions assigned to a specific computer, and any computer configurations, including layout and auto login/logout, will not work on a Remote Desktop Session Host.
- The Remote Desktop Session Host computer must have Windows® Server 2008 R2 or Windows® Server 2012 installed.
- Proficy Workflow does not support running a Remote Desktop Session Host on Windows® Vista.
- Although Windows supports machine names of up to 15 characters, Proficy Workflow node names are limited to eight characters.
- Depending on your settings, some keyboard shortcuts (such as Ctrl+Alt+Delete) may be disabled or remapped.
- User accounts must be created with logins after installing Proficy Workflow.

Scalability

The number of clients supported by a server varies according to the server's processing power and memory. If you use good optimization techniques, you should be able to run more clients with better performance per server.

The Microsoft® Performance Monitor can help you to determine the optimal number of Remote Desktop Session Host sessions your server can handle.

Hardware Requirements

The following information describes the recommended hardware requirements for a Remote Desktop Session Host environment.

- One 3Ghz CPU for every three clients connected to the Remote Desktop Session Host (*minimum*)

  NOTE: If the clients are expected to manage high levels of activity, decrease the number of clients per CPU to two.
- 500MB RAM per client (*minimum*)

Software Requirements

Proficy Workflow Remote Desktop Session Host requires Proficy Workflow and the Windows® Server 2008 R2 Standard or Enterprise Edition or the Windows® Server 2012 operating system.

NOTE: GE Intelligent Platforms highly recommends that you install the latest Service Pack and Windows Updates.

Licensing Requirements

GE Intelligent Platforms recommends that you install your Remote Desktop Session Host on a computer that is not a domain controller. Ensure that you back up the Remote Desktop Session Host licenses regularly to prevent data loss.

For the most up-to-date Remote Desktop Session Host license information on Windows® Server 2008 R2, visit Microsoft®'s web site:

http://technet.microsoft.com/en-us/library/dd647502(WS.10).aspx

Proficy Workflow Remote Desktop Session Host Clients for Windows® Server 2008 R2

When a Windows® Server 2008 R2 client connects to the Remote Desktop Session Host with External Connector Licensing disabled, the license from the client is used. The first time that you connect to the server, that license is activated.

If you are running a non-Windows® Server 2008 R2 client computer, you need to purchase Windows Remote Desktop Services Client Access Licenses (RDSCALs) from Microsoft®. When you first set up the Proficy Workflow Remote Desktop Session Host, you have a 120-day temporary license to run a maximum of 10 client machines from the server. The first 10 Windows client machines that connect to the server will reserve the licenses.

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

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

Proficy Licensing

All hardware and software keys distributed to run Proficy Workflow contain software to enable licensing for Remote Desktop Session Host client computers.

For example, if you purchase a ten-client license, software embedded in the key allows ten concurrent client users and prevents an eleventh client access to Proficy Workflow. When a client disconnects from Remote Desktop Session Host, another client can then access it.

NOTE: You still need enough RDSCALs to license all the devices that will connect to the server. Be aware that even if you have the appropriate number of Remote Desktop Session Host licenses enabled, performance issues may prevent you from connecting.

Enable Windows® Server 2008 R2 Remote Desktop Services

Remote Desktop Services must be enabled on the Windows® Server 2008 R2 computer that will be used as the Remote Desktop Session Host.

IMPORTANT: These steps must be performed before you install Proficy Workflow.

For more information about Remote Desktop Session Host, refer to the Remote Desktop Services section of the Windows® Server 2008 R2 Help or visit Microsoft's web site at: http://technet.microsoft.com/en-us/library/dd647502(WS.10).aspx.

1. On the Windows® Server 2008 R2 computer, click **Start** > **Administrative Tools** > **Server Manager**.
   The Server Manager dialog box appears.
2. Click **Roles**, and then click **Add Roles**.
   The **Select Server Roles** page of the **Add Roles Wizard** appears.
3. Select **Remote Desktop Services**, and then click **Next**.
   The **Select Role Services** page appears.
4. Select the **Remote Desktop Session Host** and **Remote Desktop Licensing** check boxes.

   You can select additional role services, but no other services are required.

   IMPORTANT: If your Proficy application server is configured to use AD LDS (Active Directory Lightweight Directory Services), a warning message appears. Click **Install Remote Desktop Session Host anyway (not recommended)**.
5. Click **Next**.
   The **Specify Authentication Method for Remote Desktop Session Host** page appears.
6. Select an option to indicate whether network level authentication is required, and then click **Next**.
   The **Specify Licensing Mode** page appears.
7. Select an option to specify the Remote Desktop licensing mode that you want this Remote Desktop Session Host server to use, and then click **Next**.
   The **Select User Groups Allowed Access to this RD Session Host Server** page appears.
8. Click **Add** to add the required users or user groups that can connect to this Remote Desktop Session Host server, and then click **Next**.
   The **Configure Client Experience** page appears.
9. Select the functionality you want to provide to the users connecting to a remote desktop session, and then click **Next**.
   The **Configure Discovery Scope for RD Licensing** page appears.
10. Optional: Select the **Configure a discovery scope for this license server** check box, and then configure it as follows:
    a) Select the appropriate option for the discovery scope.
    b) Click **Browse** to select the location for the RD Licensing database.
11. Click **Next**.
    The **Confirm Installation Selections** page appears.

    NOTE: At any time during the configuration process, you can click **Previous** to go to a previous page to change your settings.
12. Click **Install**.

    If instructed to do so, restart the computer for the changes to take effect.

Log on to a Remote Desktop Session Host from Windows® 7

1. Click **Start** > **All Programs** > **Accessories** > **Remote Desktop Connection.**
   The **Remote Desktop Connection** dialog box appears.
2. Enter or select a computer name, and then click **Connect**.
   The Log On to Windows dialog box appears.
3. Enter a user name and password, and then click **OK**.

Proficy Workflow with Windows Remote Desktop Session Host Installation and Configuration

After enabling Installing Remote Desktop Services and its licensing, you can install and configure Proficy Workflow on a Remote Desktop Session Host.

Prerequisites for Proficy Workflow on a Remote Desktop Session Host
Prior to installing any applications for use with Remote Desktop Session Host clients, refer to the Microsoft® Remote Desktop Session Host documentation regarding concept, configuration, and use of ROOTDRIVE.

Before you begin installing and configuring Proficy Workflow on a Remote Desktop Session Host, GE Intelligent Platforms strongly recommends that you complete the following Windows administrative tasks on the Proficy Workflow server machine.

IMPORTANT: If you do not follow the recommended steps for the correct Windows Remote Desktop Session Host Configuration, your applications may not function correctly.

1. From the C:\Windows\Application Compatibility Script folder, run **chkroot.cmd**.
   The RootDrv2.cmd file is created.
2. In a text editor, open the RootDrv2.cmd file from the C:\Windows\Application Compatibility Script folder.
3. At the end of the file, on the Set RootDrive= line, add a drive letter.
   For example: Set RootDrive=W:
4. Save the RootDrv2.cmd file.
5. Run the RootDrv2.cmd file.
6. Verify that your Remote Desktop Session Host is set up and functioning.

Install Proficy Workflow on a Remote Desktop Session Host
Follow the installation steps, as outlined in the Proficy Workflow Getting Started Guide, to install Proficy Workflow on a Remote Desktop Session Host.

Specify the program that starts when the user logs on to the Remote Desktop Session Host
You can create a secure environment that prevents operators from performing unauthorized actions, such as using the Ctrl+Alt+Delete key combination to shut down the Remote Desktop Session Host. You can configure this in Windows, with user properties and group policies.

Be aware that you can use Proficy Workflow security to define the rights each user has in Proficy Workflow after logging in. For example, you can add further restrictions in Proficy Workflow by setting permissions for the group the user is a member of.

1. On the Remote Desktop Session Host machine, log in to Windows as an administrator.
2. Click **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Computer Management.**
   The Computer Management dialog box appears.
3. In the System Tools folder, double-click **Local Users and Groups**.
4. Select the **Users** folder.
5. Right-click the user you want to configure, and then select **Properties**.
   The Properties dialog box appears.
6. Click the **Environment** tab.
7. In the Starting Program area, select the **Start the following program at logon** check box.
8. In the **Program File Name** field, enter the path to the Proficy client program.

   For example, if you installed Proficy Workflow to the default location, enter:

   C:\Program Files\Proficy\Proficy Workflow\Proficy Client.exe
9. In the **Start in** field, enter the path of the Proficy Workflow product.

   For example, if you installed Proficy Workflow to the default location, enter:

   C:\Program Files\Proficy\Proficy Workflow
10. Click **OK**.
11. Repeat steps 5 through 10 for each user you want to configure.
12. Click **OK** to close the Computer Management dialog box.

Configure a Remote Desktop Connection to Connect to a Remote Desktop Session Host
Windows® Server 2008 R2, Windows® 7, and Windows® Server 2012 provides the Remote Desktop Connection to configure and connect to a remote Remote Desktop Session Host.

1. Click **Start** > **All Programs** > **Accessories** > **Remote Desktop Connection.**
   The **Remote Desktop Connection** dialog box appears.
2. Click **Options**.
3. On the **General** tab, in the **Computer** field, enter or select a name from the drop-down list.
4. In the **User name** field, enter a user name and, if applicable, preface it with your domain name followed by a backslash.
5. Click the **Display** tab.
6. Leave the default remote desktop size but, if required, change the color setting.
7. Click the **Experience** tab.
8. Select the performance options that your client requires. GE Intelligent Platforms recommends that you clear all check boxes except **Persistent bitmap caching**.
9. Select the **Reconnect if connection is dropped** check box.
10. Click **Connect** to connect to the Remote Desktop Session Host.

Troubleshoot Your Proficy Workflow Remote Desktop Session Host Environment

To successfully troubleshoot your Proficy Workflow Remote Desktop Session Host environment, you first need to isolate the source of your problem.

Troubleshoot Specific Remote Desktop Session Host Problems
After isolating your problem area, use the information in the following table to begin troubleshooting.

For this problem area...	Verify...
Performance	Should you run fewer clients? Server performance increases with the following: • Faster processors • More processors (dual, quad) • More memory • Reduced graphic refresh rate on clients
Connection	• Is your connection problem for all connections or user specific? • Can the Administrator start a session locally and remotely?
Environment	• Can you create a session on the server? • Is the problem the same for all users including Admin? • Can you create a new client session? • Can you create a client that opens NotePad?

For more information, suggestions, and tips for troubleshooting your Proficy Workflow Remote Desktop Session Host environment, refer to the Windows® Server 2008 R2 Help and the Microsoft® Remote Desktop Session Host online documentation.

Troubleshoot Known Remote Desktop Session Host Problems
The following table lists some specific troubleshooting information for known Remote Desktop Session Host problems.

Problem	Solution
Registry locks, behaves like "Duplicate Node Names" on the network.	You have started multiple sessions at the same time or multiple users have logged on using the same account. Multiple users cannot log on using the same account. Start one session at a time. If the same user is logged on multiple times, consider using the End Session setting. The End Session setting logs off the user upon disconnect. To use this setting, select the End Session check box located under Override User Settings in the RDP Properties of the Remote Desktop Services Configuration Console.
The text insertion cursor in a Proficy Workflow Text object does not appear.	The cursor blink rate in the control panel is set to the lowest setting for Remote Desktop Session Host. Set the blink rate to 1 above the slowest setting.

Frequently-Asked Questions About Using Proficy Workflow with Remote Desktop Session Host

The following list outlines some of the frequently-asked questions about using Proficy Workflow with Remote Desktop Services.

How can I determine the number of Remote Desktop Session Host connections that my Proficy Workflow license supports?
If you have an M4 key, run the Proficy License Viewer (Proficy.ManagementConsole.exe). Select the Proficy Workflow product icon to display Proficy Workflow information.

Task Controls in Proficy HMIs

The Proficy Workflow Task List can be integrated into other Proficy HMI applications.

Workflow task controls can be integrated into existing HMI applications, such as Proficy HMI/SCADA CIMPLICITY and Proficy HMI/SCADA iFIX. Workflow tasks are displayed in your application so you can operate them from within these applications. You use the ActiveX Task List and Task Indicator controls to interact with and view workflow tasks.The ActiveX Task List provides users with a list of tasks for a workflow. The Task Indicator provides a user with relevant information regarding the status of the ActiveX Task List.

Proficy Task List Configuration

The configuration tool allows you to modify server information and its authentication credentials.

Before configuring the ActiveX Task List, note the following information:

- Each installation of the ActiveX Task List can connect to only one Proficy Workflow server at a time.
- At a single workstation, only one Task Indicator object and one ActiveX Task List object can be connected at a time per HMI application instance.
- Proficy task controls and Proficy HMIs are related, but work independently from each other. Therefore, user names and logins are separate.
- Like the Proficy Workflow client, the NET. TCP Port Sharing service must be enabled to use the Task List in a host application.

- To change the server name, use the **Configure Client** tool. For more information, see Modify the server configuration for a remote client on page 66. If you install the ActiveX Task List on a different machine than the Proficy application server, you must access the **Configure Client** tool from the following location: ../Program Files/Proficy/Proficy Task List/Program.

Install the ActiveX Task List

IMPORTANT: Product Options Installation Information. When using the ActiveX Task List, product option updates made on the server are not automatically deployed to applications using the Task List. The ProficyUpdater.exe application must be run manually, with administrative privileges, in order to deploy production option updates on each client machine using ActiveX Task List.

NOTE: At a single workstation, only one Task Indicator object and one ActiveX Task List object can be connected at a time per HMI application instance.

1. From the application splash screen, click **Install ActiveX Task List**.

   NOTE: If the splash screen does not appear, double-click SetupTaskList.exe from the root directory of the installation folders.

   The **License Agreement** page appears.
2. Review the license agreement, and then click **I Agree**.
   The **Installation Folder** page appears.
3. Accept the default destination folder or browse for a new location, and then click **Next**.
   The **Proficy Workflow Server Configuration** page appears.
4. In the **Server Name** field, enter the name of the server that you want to install the ActiveX Task List on.
   The **Security Certificates** page appears.
5. The security certificates are automatically downloaded from the server you are connecting to.
6. Click **Next**.
   The **Configure Task List Authentication** page appears.
7. From the **Authentication Type** drop-down menu, select one of three login options, and then click **Next**.

   If you want the user name and password:

   - entered manually, select **Manual Authentication**, or
   - exposed in plain text, select **Control Property Authentication**, or
   - saved automatically after initial setup, select **Password Encryption Authentication**.

     NOTE: You must first configure users using the **Configure Client** tool.

   The **Installation Confirmation** page appears.

   TIP: At any time during the configuration process, you can click **Back** to return to a previous page to change your settings.
8. Click **Install**.
   The **Installation** page appears, displaying the status of each installation step.
9. When the installation is complete, click **Exit**.

Modify the ActiveX Task List installation configurations

NOTE: To change the server name, use the **Configure Client** tool. For more information, see Modify the server configuration for a remote client on page 66. If you install the ActiveX Task List on a different machine than the Proficy application server, you must access the **Configure Client** tool from the following location: ../Program Files/Proficy/Proficy Task List/Program.

1. From the **Start** menu, select the **Task List Configuration**.
   The **Proficy Task List Configuration** page appears.
2. To add or modify a server, in the **Server Name** section, enter the fully qualified name of a server.
3. To modify the login authentication, in the **Server Authentication** section:

Select...	To...
Manual Login	prompt the user to enter a user name and password at each login.
Control Property	allow the user to view the user name and password in the host's object properties.
Password Encryption	log the user in automatically.

4. If you selected **Password Encryption** in the **Server Authentication** section, add user credentials in the **User Configuration** section:
   a) In the **Users** panel, click **Add**.
   b) In the **Details** panel, in the **User Name** field, enter an existing Proficy Workflow user name.
   c) In the **Password** field, enter your user account password.
   d) In the **Confirm Password** field, enter your password again.
5. Click **Save**.

Security

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

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

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

More information on security, including GE Intelligent Platforms security advisories and security patch notifications, can be found online.

Please visit our website at http://www.ge-ip.com/security.

Defense in Depth

Defense in depth is the concept of using multiple layers of security to raise the cost and complexity of a successful attack.

To carry out a successful attack on a system, an attacker would need to find not just a single exploitable vulnerability, but would need to exploit vulnerabilities in each layer of defense that protects an asset.

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

Anti-virus software

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

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

Data Execution Prevention

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

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

Software Patching

Installing software patches is in integral part of security.

Patching GE Intelligent Platforms Proficy Software

GE Intelligent Platforms recommends that customers keep Proficy software up-to-date by applying the latest Software Improvement Module (SIM) to their deployed Proficy products. SIMs add new functionality, fix bugs, and address security vulnerabilities. Security advisories and security-related SIMs can be found on the GE Intelligent Platforms website at http://www.ge-ip.com/security. Customers can also sign up for notification of new SIMs and security advisories on the website.

Patching Third-Party Software

GE Intelligent Platforms also recommends that customers keep operating systems, databases, and other third-party software in their environment up-to-date with the latest security patches from the software vendor. GE Intelligent Platforms regularly validates the compatibility of selected GE Intelligent Platforms products with third-party operating system security patches. More information on this process can be found on the GE Intelligent Platforms Support website at http://www.ge-ip.com/security.

Platform Configuration and Hardening

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

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

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

Contact Information

If you purchased this product through an Authorized Channel Partner, please contact the seller directly.

General Contact Information

Online technical support & GlobalCare:	www.ge-ip.com/support
Comments about our manuals and online Help:	doc@ge.com
Additional information:	www.ge-ip.com
Solution Provider:	solutionprovider.ip@ge.com
Authorization:	authorization.ip@ge.com

Technical Support

If you have technical problems that cannot be resolved with the information in this guide, please contact us by telephone or e-mail, or on the web at www.ge-ip.com/support.

Americas

Online technical support:	www.ge-ip.com/support
Telephone:	1-800-433-2682
International Americas direct dial:	1-434-978-5100
Technical support e-mail:	support.ip@ge.com
Customer care e-mail:	customercare.ip@ge.com
Inside Sales:	insidesales.ip@ge.com
Primary language of support:	English

Europe, Middle East, and Africa

Online technical support:	www.ge-ip.com/support
Telephone:	+800 1-433-2682 +1 780-401-7717 if the 800 option is not available in your country, or if dialing from a mobile telephone
Technical support e-mail:	support.emea.ip@ge.com
Customer care e-mail:	customercare.emea.ip@ge.com
Inside Sales:	insidesales.emea.ip@ge.com
Primary language(s) of support:	English, French, German, Italian, Czech, Spanish

Asia Pacific

Online technical support & GlobalCare:	www.ge-ip.com/support
Telephone:	+86-400-820-8208
	+86-21-3217-4826 (India, Indonesia, and Pakistan)
Technical support e-mail:	support.cn.ip@ge.com (China)
	support.jp.ip@ge.com (Japan)
	support.in.ip@ge.com (other Asian locales)
Customer care e-mail:	customercare.apo.ip@ge.com
	customercare.cn.ip@ge.com (China)