



# Proficiency Workflow

## Getting Started Guide



**Proprietary Notice**

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

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 General Electric Company. Information contained herein is subject to change without notice.

© 2023, General Electric Company. All rights reserved.

**Trademark Notices**

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

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

All other trademarks are the property of their respective owners.

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

[doc@ge.com](mailto:doc@ge.com)

<b>Chapter 1. Get Started Guide.....</b>	<b>6</b>
Installation Requirements.....	6
Key Concepts.....	6
System Health and Program Use.....	6
Regional Settings.....	8
Daylight Saving Time.....	9
Special Keyboard Buttons.....	9
Log Files.....	9
Compatibility and Upgrading with GE Products.....	9
Pre-Installation Consideration.....	10
Architecture Considerations.....	10
Prerequisites for Windows 2012 R2 Installations.....	11
Configure Windows Authentication for Workflow.....	12
Windows Services for Workflow.....	13
Security Certificates.....	14
Firewall Ports.....	21
Database Backup and Restore.....	22
Multiple Servers.....	22
Server Clustering and Failover.....	24
Enable Connection between Workflow and SQL Server.....	25
License Management.....	26
Performance Counters.....	26
Installation Procedures.....	30
Install a single application server and client.....	30
Install a remote client.....	35
Configure multiple servers on a single machine.....	37
Revert multiple servers on a single machine back to a single server.....	39
Multiple Server Installation.....	40
One-click Deployment.....	44
Command-line (Silent) Installation.....	48
Uninstall Workflow.....	50
Server Clustering Implementation.....	50

Supported and Validated Cluster Configurations.....	50
Microsoft Failover Cluster Manager for Windows Servers.....	54
Install Microsoft Failover Cluster Manager.....	54
Configure the Microsoft Failover Cluster Manager.....	55
Configure quorum options for a cluster.....	57
Configure the primary cluster server.....	57
Configure the failover cluster server.....	58
Configure a local client for a cluster node (32-bit).....	59
Configure a local client for a cluster node (64-bit).....	60
Server Clustering and One-Click Deployment.....	60
Clustering Tips.....	60
Deploy the Web Task List.....	62
Web Task List Deployment.....	62
Configure security certificates for a reverse proxy.....	62
Configure an IIS reverse proxy for the Web Task List.....	63
Configure an Apache reverse proxy for the Web Task List.....	65
Inbound and Outbound Rules for Apache.....	66
Connect to the Web Task List.....	67
Log On Overview.....	70
Log On Overview.....	70
Log on to Workflow client.....	70
Automatically log into Workflow.....	71
GE Single Sign On (SSO).....	72
Authentication.....	73
Post-Installation Configuration.....	75
Post-installation Configuration.....	75
Running with a Standard Windows User Account.....	75
Configure web proxy settings for Local System account.....	76
Modify security certificates.....	76
Modify site configuration.....	77
Monitor system configuration and status.....	79
Modify the server configuration for a remote client.....	80

Modify the Microsoft Active Directory Services.....	80
Modify your application server database.....	81
Configure a server instance.....	83
Configure product options.....	84
Change architecture mode.....	85
Add or remove performance counters.....	86
Display the host server name in the Workflow client.....	86
Client and Server Configurations.....	87
Server Limit Overrides.....	90
Upgrade Workflow.....	95
Upgrading Workflow.....	95
Install a Reporting Database.....	98
Reporting Database.....	98
Install the reporting database.....	99
Configure Component Services.....	101
Uninstall the reporting database.....	102
Upgrade a replicated database.....	103
Terminal Server.....	106
Remote Desktop Session Host.....	106
Remote Desktop Services (Terminal Services).....	106
Getting Started with Remote Desktop Session Host.....	107
Workflow with Windows Remote Desktop Session Host Installation and Configuration.....	111
Troubleshoot Your Workflow Remote Desktop Session Host Environment.....	114
Frequently-Asked Questions About Using Workflow with Remote Desktop Session Host.....	115
ActiveX Task Controls.....	116
Task Controls in GE HMIs.....	116
Task List Configuration.....	116
Install the ActiveX Task List.....	117
Modify the ActiveX Task List installation configurations.....	118
Workflow Task Client.....	119
Overview.....	119

Install the Task Client.....	119
Configure the Task Client.....	126
Import Equipment Model.....	128
Create an User Account in Operations Hub.....	129
Access the Task Client.....	130
Uninstall the Task Client.....	133
Troubleshooting Task Client Issues.....	133
Installation Security.....	136
Installation Security.....	136
Defense in Depth.....	137
Anti-Virus Software.....	137
Data Execution Prevention.....	137
Software Patching.....	137
Platform Configuration and Hardening.....	138
Contact Information.....	138
<b>Chapter 2. Index.....</b>	<b>a</b>

# Chapter 1. Get Started Guide

## *Installation Requirements*

### *Key Concepts*

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 Workflow 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

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 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 servers 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 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 \(page 79\)](#) display to monitor server configuration and status. In these states of site health, you can also [move product options between servers \(page 77\)](#) to accommodate changing conditions, as necessary.



## Related concepts


[Multiple Servers \(page 22\)](#)

## Related tasks

[Configure product options \(page 84\)](#)

## *Regional Settings*


The following regional settings are supported.

 **Note:** Open Enterprise supports the same regional settings as Workflow.

## Workflow 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 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 Workflow is running.

## Setting the System Default Locale

The selected locale must be set as the system default.

## Workflow Web-based Application Settings

In order to capture the date and time settings accurately in Google Chrome and Mozilla<sup>®</sup> FireFox<sup>®</sup>, 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.

## *Daylight Saving Time*

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

### **Related reference**

Time Events ([page](#) )

## *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*

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 GE Products*

Please refer to the WorkflowIPI PDF for information on upgrading Workflow, compatibility with earlier versions and other GE Products. You can find the WorkflowIPI.pdf in the Documentation folder of the Workflow installation media or in the Proficy Workflow\Help folder after installation. By default this is C:\Program Files (x86)\Proficy\Proficy Workflow\Help.


## *Pre-Installation Consideration*

### *Architecture Considerations*

If you are installing an 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**.

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 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 Workflow 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 Workflow application server or Workflow 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 Workflow application server, the Workflow 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 Workflow client (for example, configuration screens and displays) must target either *Any CPU* or *x86*, because Workflow 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 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.

### Related tasks

[Change architecture mode \(page 85\)](#)

## *Prerequisites for Windows 2012 R2 Installations*

To install the Application Server, Reporting, Extension servers, or ActiveX Task List on Windows<sup>®</sup> Server 2012 R2, the April 2014 update rollup for Windows<sup>®</sup> Server 2012 R2 (KB2919355) must already be applied.

 **CAUTION:** If this update is missing, the Visual C++ 2015 Redistributable packages installed by the Workflow installer will fail. These packages must be manually uninstalled, and then the necessary Windows updates must be applied before you attempt the Workflow installation again. If you do not uninstall the Visual C++ 2015 Redistributable packages before retrying the Workflow installation, the installation will appear to be successful but the WorkflowServer service will fail to start.

 **Important:** These recovery steps also apply if you attempt to install Workflow 2.5 SP2 on Windows<sup>®</sup> 7 Professional without SP1 or Windows<sup>®</sup> Server 2008 R2 without SP1.

## *Configure Windows Authentication for Workflow*

You can configure Workflow to use Windows authentication to connect to a remote SQL Server instance.

To configure Workflow to use Windows authentication, you must use the Windows **Credential Manager** to create a credential specifying the Windows username and password that the Workflow server should use to connect to the database.

The credential on the Workflow server machine must identify the remote SQL Server by IP or fully-qualified domain name (FQDN) and may need to explicitly specify the port depending on the SQL Server configuration.

During the installation of the Workflow server, you will have the opportunity to specify the **hostname** and **port** exactly as it was specified in the credential. Use a comma to separate the hostname and port number per the SQL Server connection string syntax.

1. Click **Start > Control Panel > All Control Panel Items > Credential Manager**.
2. Select **Windows Credentials**, and then click **Add a Windows credential**.  
The **Credentials** dialog box appears.
3. Enter values into the fields, as follows:
  - Enter the hostname in the **Internet or network address** field. (e.g., `sql2016server:49785`)
  - Enter the username that Workflow should use to connect to the database into the **User Name** field.
  - Enter the password associated with the username you entered into the **Password** field.

- Click **OK**.

4. In the **Database Configuration** section during the installation of the Workflow server, do the following:

- Enter the hostname and port number in the **Server** field, just as you did for the credential. (e.g., `sql2016server,49785`)
- Enter the database name in the **Database** field.
- Select **Windows Authentication** from the **Authentication** drop-down list.
- Click **Save**.


Workflow is now configured to use Windows authentication to connect to a SQL Server.

## *Windows Services for Workflow*

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

### **Standard Server Installation Services**

These services are installed as part of 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.

#### **Workflow 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.

#### **Workflow 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 Workflow application server is installed on.

#### **SOAAdam**

This service is available if you are using a Microsoft ADAM/LDS instance.

## *Security Certificates*

### Security Certificates

Security certificates must be installed on all Workflow 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 Workflow 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 Workflow 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 Workflow 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**.

**Related tasks**[Modify security certificates \(page 76\)](#)**Related reference**[Security Certificate Options \(page 15\)](#)**Security Certificate Options**

Server security certificate options differ 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 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	<p>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.</p> <p>After selecting this option, in the <b>Certificate File</b> field, click <b>Browse</b> to locate and select the zip file containing the security certificates that you exported.</p>



Option	Description
Use the certificates already installed on this server	<p>Post-installation configuration only: this option is available when you use the <b>Configure Certificates</b> tool. It allows you to use existing certificates that were installed with a previous version of this application.</p> <p>To import certificates, select the <b>Enable certificate import for advanced configuration</b> check box, and then click <code>Import</code>. Click <b>View</b> to view each certificate after it has been imported.</p>

## 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	<p>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.</p> <p>After selecting this option, in the <b>Certificate File</b> field, click <b>Browse</b> to locate and select the zip file containing the security certificates that you exported.</p>

## 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.

**Related concepts**[Security Certificates \(page 14\)](#)**Related tasks**[Modify security certificates \(page 76\)](#)**Install Certificates on older Operating Systems**

You can create certificates on a Windows 10 or Windows Server 2016 machine and transfer them to a machine with an older operating system.

If you would like to use valid, self-signed certificates for a Workflow installation on an operating system other than Windows 10 or Windows Server 2016, you can do the following:

1. Manually generate the certificates using **Powershell New-SelfSignedCertificate** on a Windows 10 or Windows Server machine.
2. Export the certificates using **MMC**.
3. Import the certificates to the selected Workflow server machine using Workflow **ConfigureCertificates**.
4. Import the SSL certificate using Workflow **ConfigureCertificates**.

1. Manually generate the certificates on a Windows 10 or Windows Server 2016 machine.

- a. Use the following **New-SelfsignedCertificate** parameters to generate the certificates:

Certificate Name	New-SelfSignedCertificate command parameters
ProficySelfSignedCA	<pre>New-SelfSignedCertificate -CertStoreLocation "cert:LocalMachine\My" -DnsName "ProficySelfSignedCA" -FriendlyName "ProficySelfSignedCA" -HashAlgorithm SHA256 -KeyExportPolicy Exportable -KeyLength 2048 -KeySpec KeyExchange -KeyUsage CertSign, CRLSign, DigitalSignature -KeyUsageProperty All -NotAfter \$([datetime]::now.AddYears(3)) -Subject "CN=ProficySelfSignedCA"</pre>
ProficySTS	<pre>\$proficyCACert = Get-ChildItem -Path cert:\LocalMachine\My   ?{\$_.Subject -eq "CN=ProficySelfSignedCA"}  New-SelfSignedCertificate -CertStoreLocation "cert:LocalMachine\My" -DnsName "ProficySTS" -FriendlyName "ProficySTS" -HashAlgorithm SHA256 -KeyExportPolicy Exportable - KeyLength 2048 -KeySpec KeyExchange - NotAfter \$([datetime]::now.AddYears(3)) -Signer \$proficyCACert -Subject "ProficySTS"</pre>

Certificate Name	New-SelfSignedCertificate command parameters
ProficyPlatform	<pre>\$proficyCACert = Get-ChildItem -Path cert:\LocalMachine\My   ?{\$_.Subject -eq "CN=ProficySelfSignedCA"}  New-SelfSignedCertificate -CertStoreLocation "cert:\LocalMachine\My" -DnsName "ProficyPlatform" -FriendlyName "ProficyPlatform" -HashAlgorithm SHA256 -KeyExportPolicy Exportable - KeyLength 2048 -KeySpec KeyExchange - NotAfter \$([datetime]::now.AddYears(3)) -Signer \$proficyCACert -Subject "ProficyPlatform"</pre>
SSL certificate	<pre>\$proficyCACert = Get-ChildItem -Path cert:\LocalMachine\My   ?{\$_.Subject -eq "CN=ProficySelfSignedCA"}  New-SelfSignedCertificate -CertStoreLocation "cert:\LocalMachine\My" -DnsName "localhost", "&lt;ipAddress&gt;" -FriendlyName "localhost" -HashAlgorithm SHA256 - KeyExportPolicy Exportable -KeyLength 2048 -KeySpec KeyExchange -NotAfter \$([datetime]::now.AddYears(3)) -Signer \$proficyCACert -Subject "&lt;hostname&gt;"  Where &lt;ipAddress&gt; and &lt;hostname&gt; are the IP Address and the Hostname of the Workflow application server machine.</pre>

b. Run **Powershell** as an administrator to create the certificates.

2. Export the certificates from the **Local Computer > Personal** store, using the Microsoft Management Console (MMC) certificate snap-in.
  - a. For each certificate, select **export the private key**.
  - b. On the **Export File Format** dialog, select **Personal Information Exchange - PKCS #12 (.PFX)** format.
  - c. Uncheck the **Include all certificates in the certification path if possible** check box.
  - d. Check the **Export all extended properties** check box.
  - e. Export all of the certificates to the same directory, naming each **.pfx** file with the certificate name (Issued To) of the certificate it contains. Use the same password for each certificate.
  - f. Combine the certificates into a **.zip** file and copy the **.zip** file to the Workflow server machine.
  - g. Unzip the file for use.

 **Note:**


- If you leave the **Include all certificates in the certification path if possible** check box selected, the **ProficySelfSignedCA** cert is re-imported into the **Local Machine > Personal** store when you import the **SSL** certificate in a later step. You will then have to remove it.

- Exporting using the same password and naming each file with the **Issued To** name is mandatory for importing on the Workflow application server using **ConfigureCertificates**.

### 3. Import the certificates using Workflow **ConfigureCertificates**.

- a. On the selected Workflow server, run:  
`C:\Program Files (x86)\Proficy\Proficy Workflow\Program  
\ConfigureCertificates.exe`
- b. Select the **Import Certificates** option.
- c. Select the **.zip** file you copied for importing (not the individual .pfx files).  
The three Proficy certificates are imported from the .zip files into the correct locations.
- d. Click **Save**.  
Once saved, an SSL certificate is generated and bound to the Workflow ports. This SSL certificate must be removed before proceeding to the next step.
- e. Using MMC, remove the **SSL** certificate from the **LocalMachine > Personal** store. You will replace this certificate in the next step.

### 4. Import the **SSL** certificate using Workflow **ConfigureCertificates**.

- a. On the selected Workflow server, run:  
`C:\Program Files (x86)\Proficy\Proficy Workflow\Program  
\ConfigureCertificates.exe`
  - b. Select **Use the certificates already installed on this server** option.
  - c. Select the **Enable certificate import for advanced configuration** check box.
  - d. Click the ellipses (...) in the **Import** column for the **SSL/TLS Server Certificate**, and browse to the folder containing the exported certificates.
  - e. Select the **SSL** certificate. This is the certificate with the **Issued To** equal to the Workflow application server hostname.
-  **Note:** You may need to change the file browser selection from **.cer** to **All Files** to see **.pfx** file.
- f. Follow the prompts to import the **SSL/TLS Server Certificate**.
  - g. Click **Save** to bind the Workflow ports to this certificate.

## Related concepts

[Security Certificates \(page 14\)](#)

## Related tasks

[Use self-signed certificates for the web server \(page 20\)](#)

[Modify security certificates \(page 76\)](#)

## Related reference


[Security Certificate Options \(page 15\)](#)

## Use 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.

### Related reference


[Security Certificate Options \(page 15\)](#)

## 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 remote clients.

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

- 8447
- 8012
- 8111
- 8112
- 8020
- 8201
- 8202
- 8203
- 8204

 **Important:** As of Workflow version 2.6, the default port for REST services hosted by Workflow is changed from 8444 to 8447. The REST service port is NOT changed during upgrade of existing installations and remains 8444.

GE Web HMI and GE Workflow do not work together if installed on the same machine as both applications require the use of port 8444. You must change the port number in your Workflow server information in Web HMI. If no port information is provided, the default is used. For information

about resolution of port conflicts, see [Resolve Port conflicts between prior Workflow installations and Web HMI \(page \)](#). For existing Workflow installations prior to 2.6, Workflow and Web HMI ports are both set to 8444, making applications installed on the same machine incompatible.

## *Database Backup and Restore*

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 the Microsoft web site for additional information on backing up, restoring, and maintaining your SQL Server database.

## *Multiple Servers*

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 Workflow 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 SOA Server 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 SOA Server 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 SOA Server, 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 SOA Server 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 SOA Server 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 **Configure Site** tool to move product options and related services among server instances.

 **Note:** The Core product option and services must reside on the SOA Server instance.

Beginning with 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 Workflow program. For more information, see **System Health and Program Use**.

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



## Related concepts

[Architecture Considerations \(page 10\)](#)

[Multiple Server Installation on Multiple Machines \(page 40\)](#)

[Server Clustering and Failover \(page 24\)](#)

[System Health and Program Use \(page 6\)](#)

## Related tasks

[Configure multiple servers on a single machine \(page 37\)](#)

[Modify site configuration \(page 77\)](#)

## Server Clustering and Failover

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

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.

Workflow works with the Microsoft Failover Cluster Manager to ensure high availability of the Workflow application server. If the primary server node in the cluster experiences difficulties, 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 Workflow in a clustered environment.

1. Overviews of the **Supported and Validated Cluster Configurations**.
2. Instructions for using the **Microsoft Failover Cluster Manager for Windows Servers** 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 Cluster Server**.
6. Instructions for **Export Server Security Certificates for an Extension Server** from the primary cluster server in preparation for installing them on the failover server.
7. Instructions for configuring the **Failover Cluster 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 also supports clustering. For complete information about installing, configuring, and maintaining SQL Server *failover* clustering, see the following topics on the Microsoft Development Network web site: SQL Server Failover Cluster Installation; 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.

### Related concepts

[Microsoft Failover Cluster Manager for Windows Servers \(page 54\)](#)  
[Supported and Validated Cluster Configurations \(page 50\)](#)

### Related tasks

[Install a single application server and client \(page 30\)](#)  
[Configure a server instance \(page 83\)](#)  
[Install Microsoft Failover Cluster Manager \(page 54\)](#)  
[Configure the Microsoft Failover Cluster Manager \(page 55\)](#)  
[Configure the primary cluster server \(page 57\)](#)  
[Export server security certificates for an extension server \(page 41\)](#)  
[Configure the failover cluster server \(page 58\)](#)

### Related reference

[Server Clustering and Failover Software Requirements \(page \)](#)  
[Server Clustering and Failover Hardware Requirements \(page \)](#)

## *Enable Connection between Workflow and SQL Server*

In order for Workflow to connect to any edition of Microsoft<sup>®</sup> SQL Server 2012 or later, you must configure SQL Server to enable the *db\_owner* role on the SOADB database for the applicable login account.

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

For increased security when using Windows authentication, you can modify the properties for the Workflow Server service after installing Workflow, to define a custom login name and credentials. (For more information, see Microsoft<sup>®</sup> Windows help.) Another alternative is to select SQL Server

authentication when installing Workflow. In either of these scenarios, you must add the user-specified login account to SQL Server, and then enable the *db\_owner* role for that account.

For information on adding a login account to SQL Server, mapping a login to a database, and setting database roles, see the Microsoft® SQL Server help.

## *License Management*

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

To access the online help for the GE License Client, perform the following step.

From the desktop Start Menu, select **General Electric > License Help**.

The License Client online help opens.

 **Note:** For more information regarding licensing, see <http://support.ge-ip.com/licensing>

## *Performance Counters*

### 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 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.

Counter Name	Description
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 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 Workflow.

Counter Name	Description
Events Queued Messages to Subscribers	<p>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 <math>N</math> subscribers to a given event, there will be <math>N</math> Events Queued Messages to Subscribers for each event generated.</p>
Events DTL Subscriptions	<p>Records the number of DTL points being subscribed to.</p> <p>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 WorkflowClients subscribing to the WorkflowTaskInstanceEvent, there should be one Events DTL Subscription and three Events Remote Subscriptions.</p>
Events Remote Subscriptions	<p>Records the number of subscribers to events on another server (such as those requiring DTL subscription).</p> <p>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 WorkflowClients subscribing to the WorkflowTaskInstanceEvent, there should be one Events DTL Subscription and three Events Remote Subscriptions.</p>
Events DTL Change Rate	<p>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).</p>


Counter Name	Description
Events Messages to Subscribers Rate	Reports the number of events per second being sent to subscribers. In a stable system, if there are <i>N</i> subscribers to a given event, the Events Messages to Subscribers Rate will be <i>N</i> times the Events DTL Change Rate (assuming only that event is being generated). If the Events Messages to Subscribers Rate is less than <i>N</i> times the Events DTL Change Rate, 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...**

**Add counters**

**Enter...**

```
<installfolder>ProficyServer[exe] /
installperformancounters
```

To...	Enter...
<b>Remove counters</b>	<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.

### Related tasks

[View performance counters \(page 30\)](#)

### 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.

### Related tasks

[Add or remove performance counters \(page 29\)](#)

### Related reference


[DTL Counters \(page 26\)](#)

[Events Counters \(page 27\)](#)


## *Installation Procedures*

### *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 Client and Application Server**.

 **Note:** If the splash screen does not appear, run `InstallFrontEnd.exe` on the root directory of the installation folder.

The setup wizard appears.

2. Click **Application Server**.

The **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	<ol style="list-style-type: none"> <li>a. Accept the default destination folder or browse for a new location, and then click <b>Next</b>.</li> </ol> <p>The <b>AD LDS Integration</b> page appears.</p>
64-bit	<ol style="list-style-type: none"> <li>a. Accept the default <b>Destination Folder (32-bit)</b>, or browse for a new location.           <p> <b>Important:</b> 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.</p> </li> <li>b. Accept the default <b>Destination Folder (64-bit)</b>, or browse for a new location.</li> <li>c. Select either 32-bit or 64-bit depending on the architecture in which you want the server to operate.           <p> <b>Tip:</b> The default is 64-bit, but you may also select 32-bit. If your environment changes after installation, you can use the <b>Configure Server</b> tool to change the architecture.</p> </li> <li>d. Click <b>Next</b>.</li> </ol> <p>The <b>AD LDS Integration</b> page appears.</p>

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




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


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 a 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. Click **Next**.  
The **Database Configuration** page appears.

9. 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 your existing database**.

---

To configure SQL Server settings...	Then...
<b>Automatically</b>	a. Select the <b>Use a local database with Windows Authentication</b> check box.
	 <b>Note:</b> To use this option, the following SQL Server conditions apply: <ul style="list-style-type: none"> <li>• Installed locally, AND</li> <li>• Designated as default Local Host, AND</li> <li>• Uses Windows Authentication</li> </ul>
	b. Proceed to step 10.
<b>Manually</b>	a. Clear the <b>Use a local database with Windows Authentication</b> check box.
	b. Proceed to step 9.

---

10. 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 with a default instance you may 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.
  - If you select **SQL Server Authentication**, proceed to step d.
- d. Enter the **User Name** and **Change Password** that are configured for SQL Server authentication, and then proceed to step 10.

Authentication:


- Password character restrictions: <, >, &, '.
- The account used for SQL Authentication must have access to create new databases.
- To install the application server and related SIMs, the SQL Server Management Studio server role, *db\_owner*, is required.
- For regular database use during run time, the SQL server login account requires *db\_owner* and *dbcreator* privileges. After adding these roles in SQL Server Management Studio, run the Configure Database tool to update log on credentials. For more information, see the **Modify your Workflow application server database** section in the Workflow help.

11. Click **Next**.

The **Security** page appears.

12. 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.

13. **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:

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


 **Note:** Selecting this check box displays the SSO Authentication option when a user logs on,

- ii. Select an identify provider option that complies with the level of restrictions and security required for your application.

 **Note:** The **Production Identity Provider** option provides greater security for your application.

- b. Select the **Allow Password Change** 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 **Enforce User Lockout** check box, and then set the lockout threshold, duration, and timeframe values. This check box is selected by default.

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

- d. Select the **Enforce Password Complex 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.

- e. Select Web HMI Access and enter the Web HMI Host name if you wish to access the **Workflow Task List** from your Web HMI installation.

14. Click **Next**.


The **Security Certificates** page appears.

15. Select the appropriate certificate option. For full descriptions of the certificate options, see **Security Certificate Options**.


16. Click **Next**.

If the computer you are installing on has an enabled firewall, the **Firewall Settings** page appears.

17. If required, make note of the port numbers to open in the firewall, and then click **Next**.


 **Important:** If your system uses a firewall, you must follow the instructions on the **Firewall Setting** page and open ports 8447, 8012, 8111, 8112, 8020, 8201, 8202, 8203, and 8204 to incoming TCP traffic. For information on opening a port in your firewall, see 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.

18. 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.

19. When the installation is complete, click **Exit**.

 **Note:** If the installation fails, or you want to change a configuration setting after the installation completes, you can open the appropriate standalone component to configure the required information. For more information, see **Post Installation Configuration**.

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

#### **Related concepts**

[Post-installation Configuration \(page 75\)](#)

#### **Related tasks**

[Connect to the Web Task List \(page 67\)](#)


#### **Related reference**

[Security Certificate Options \(page 15\)](#)

## *Install a remote client*

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


Install a single application server and client.

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

#### **Prerequisites**

[Install a single application server and client \(page 30\)](#)

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

 **Note:** If the splash screen does not appear, run `InstallFrontEnd.exe` on the root directory of the installation folder.

The setup wizard appears.

2. Click **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 **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 hostname of the computer on which the Workflow server is installed.
- 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 Workflow server to which you are connecting.


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 Workflow client.  
A message appears stating: Updates are available. Click OK to start Workflow Update.
11. Click **OK**, and then, on the **Workflow Update** page, click **Install Updates**.
12. When the updates have finished installing, click **Restart Client**.

## *Configure multiple servers on a single machine*

After installing 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.

### **Install a single application server and client.**

#### **Important:**


- You must exit all instances of 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 2b) and port number (see step 2f).

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: Proficity Server, Proficity STS, Proficity Publisher Service.
2. Create a new server instance using the **Configure Server** tool.


- a. On the server machine, On the server machine, click **Start > All Programs > General Electric > 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 the port number for the server instance. This value must be unique if multiple server instances are run on the same machine.

 **Note:** For the **IP Address** field: Peer servers will contact this server instance at the specified IP address. If the specified address is `255.255.255.255`, then the address will be determined at server start as the first IPv4 address found in the DNS records for the hosting machine's host name. If the address is incorrect, then an appropriate address should be specified here.

- g. Click **Save**.  
The following service has now been created: Proficiency 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 **Port** field, enter the port number for the server instance. This value must be unique if multiple server instances are run on the same machine.
- 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 computer, click **Start > All Programs > General Electric > 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 the Workflow client using either the **Start** menu or desktop icon.

### Related tasks

[Install a single application server and client \(page 30\)](#)

## *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 Workflow that are located on the server that you are working on.

1. On the server computer, click **Start > All Programs > General Electric > 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.

### **Related concepts**

[Multiple Servers \(page 22\)](#)

[Multiple Server Installation on Multiple Machines \(page 40\)](#)

### **Related tasks**

[Install a single application server and client \(page 30\)](#)

[Modify site configuration \(page 77\)](#)

[Install Multiple Servers \(page 41\)](#)

[Configure a server instance \(page 83\)](#)

[Configure multiple servers on a single machine \(page 37\)](#)

## *Multiple Server Installation*

### Multiple Server Installation on Multiple Machines

After installing the 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 product options that you may license and/or custom service providers that you develop.

Installing Workflow on extension servers involves two main steps:

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

### **Related concepts**

[Multiple Servers \(page 22\)](#)

### **Related tasks**

[Export server security certificates for an extension server \(page 41\)](#)

[Install a single application server and client \(page 30\)](#)

[Modify site configuration \(page 77\)](#)

[Install Multiple Servers \(page 41\)](#)


[Configure a server instance \(page 83\)](#)

[Revert multiple servers on a single machine back to a single server \(page 39\)](#)

[Configure multiple servers on a single machine \(page 37\)](#)

### Prerequisites for Windows 2012 R2 Installations

To install the Application Server, Reporting, Extension servers, or ActiveX Task List on Windows<sup>®</sup> Server 2012 R2, the April 2014 update rollup for Windows<sup>®</sup> Server 2012 R2 (KB2919355) must already be applied.

 **CAUTION:** If this update is missing, the Visual C++ 2015 Redistributable packages installed by the Workflow installer will fail. These packages must be manually uninstalled, and then the necessary Windows updates must be applied before you attempt the Workflow installation again. If you do not uninstall the Visual C++ 2015 Redistributable packages before retrying the Workflow installation, the installation will appear to be successful but the WorkflowServer service will fail to start.

 **Important:** These recovery steps also apply if you attempt to install Workflow 2.5 SP2 on Windows<sup>®</sup> 7 Professional without SP1 or Windows<sup>®</sup> Server 2008 R2 without SP1.

### 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 > General Electric > Workflow > Configuration > Export Certificates**.  
The **Export Workflow Application Server Certificates** page appears.
2. In the **Export Folder** field, enter the folder path or browse to the location where the certificates are to be exported.
3. In the **Password** field, enter a password to secure the exported certificates, which will be used when importing the certificates to the extension servers.
4. Click **Save**.  
A file with the extension .zip is created, which contains the certificates required on the extension servers.
5. Click **Exit**.

### Install Multiple Servers

This application provides multiple server capability, allowing you to install the 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 product options that you may license and/or custom service providers that you develop.

Before you can install multiple servers, you must install a single application server and client and export server security certificates for an extension server.

 **Important:**


- If you are installing or upgrading an extension server (Workflow or User), you must have already installed or upgraded an 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 Workflow or install it again, all sample resource files are overwritten.

**Prerequisites**

[Install a single application server and client \(page 30\)](#)

[Export server security certificates for an extension server \(page 41\)](#)

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

 **Note:** If the splash screen does not appear, run `InstallFrontEnd.exe` on the root directory of the installation folder.

The setup wizard appears.

2. Click **Application Server**.

The **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	<b>Workflow Server</b>
server to host custom service provider	<b>User Server</b>

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...
<b>32-bit</b>	<ol style="list-style-type: none"> <li>a. Accept the default destination folder or browse for a new location, and then click <b>Next</b>.</li> </ol> <p>The <b>Database Configuration</b> page appears.</p>


---

**If the architecture is...****64-bit****Then do this...**

- a. Accept the default **Destination Folder (32-bit)**, or browse for a new location.

 **Note:** This is the installation location for 32-bit components. Do not install 32-bit components to the 64-bit installation directory. If you do, the installation will fail.

- b. Accept the default **Destination Folder (64-bit)**, or browse for a new location.
- c. 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.

- d. 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 to which you want to connect.
- 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.
  - If you select **SQL Server Authentication**, proceed to step 6d.
- d. Enter the **User Name** and **Password** that are configured for SQL Server authentication, and then proceed to step 7.


7. Click **Next**.

The **Security Certificates** page appears.


## 8. Import the security certificates:

 **Important:** If you have not already exported the security certificates from the main server, you must do so now before proceeding. For more information, see **Export server security certificates for an extension server**.


- 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 installation computer has an enabled firewall, the **Firewall** page appears.
11. If required, make note of the port numbers to open in 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 8447, 8012, 8111, 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 the installation completes, you can open the appropriate standalone component to configure the required information. For more information, see **Post-Installation Configuration**.

## Related concepts

[Post-installation Configuration \(page 75\)](#)

## *One-click Deployment*

One-click deployment allows you to deploy 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 Workflow will be discontinued in a future release of the software. The client installation should be used when one-click installation is discontinued.

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/ms228998(VS.85).aspx)
  - <http://msdn.microsoft.com/en-us/library/ms752346.aspx>

When an administrator installs 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 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.

### Related concepts

[Server Clustering and One-Click Deployment \(page 60\)](#)


[Security Certificates \(page 14\)](#)

### Related tasks

[Configure security certificates for a click-once client \(page 46\)](#)

## 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 Workflow server installation.

 **Note:** Support for one-click installation of Workflow will be discontinued in a future release of the software. The client installation should be used when one-click installation is discontinued.

1. In the 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. In Available Snap-ins, double-click **Certificates**.
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`.

### Related concepts

[Security Certificates \(page 14\)](#)

### Related tasks

[Modify security certificates \(page 76\)](#)

[Install a single application server and client \(page 30\)](#)

[Configure security certificates for a reverse proxy \(page 62\)](#)

### Related reference

[SSL Security Configuration \(page \)](#)


[Security Certificate Options \(page 15\)](#)

Display the host server name in the Proficy client for a one-click client

By default, the server name is displayed in the client, next to the server state icon. However, if you want to display a more meaningful name for your server, you can configure an alias so that the alias is displayed in the client rather than the actual server name.

You must install Workflow 2.5 SIM3 (or greater) before performing this task.

1. On the click-once Workflow client computer, navigate to the click-once installation folder; for example, `C:\Users\\AppData\Local\Apps\2.0\ZJZ3X90C.HGM\9A05RKG3.TKC\prof..tion_15359f3836613cd4_0002.0005_14ea60ef7e3d4b0f\Data`.

 **Note:** The installation folder can be found in the updater log.

2. Open the `UserStartup.xml` file in a text editor.

The following code shows samples of multiple server names and aliases. You can copy this code into the `UserStartup.xml` file, before the closing `</ServerConnectionInfo>` element, and then change the `Name` and `Alias` elements to reflect your server information.

```
<ServerAliases>
  <ServerAlias>
    <Name>localhost</Name>
```



```

<Alias>QA Server</Alias>
</ServerAlias>
<ServerAlias>
  <Name>Product-WIN81</Name>
  <Alias>Development Server</Alias>
</ServerAlias>
<ServerAlias>
  <Name>devwin7ex64dev</Name>
  <Alias>Product Server</Alias>
</ServerAlias>
</ServerAliases>

```

When you launch the Workflow client, the alias that you configured for the server is displayed next to the state



icon.


## 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 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
<b>/s</b>	<p>Runs the installation setup (SetupApplicationServer.exe or SetupWebServer.exe) in silent mode; that is, the installation occurs without displaying the user interface.</p> <p><b>Note:</b> The installation fails if the Proficy services are running. See <b>/fs</b>.</p> <p>You must use the <b>/c</b> parameter in conjunction with the <b>/s</b> parameter and provide a valid configuration file name.</p>
<b>/fs</b>	<p>Same as the <b>/s</b> parameter, but stops and restarts running services when performing an upgrade installation.</p>
<b>/t filepath</b> (where <code>filepath</code> is the user-defined file name)	<p>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.</p> <p><b>Note:</b> For security reasons, passwords are not included in the configuration data.</p>

Command Line Parameter	Description
<p>PropertyName=value (where <b>PropertyName</b> is a configuration file property)</p>	<p>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:</p> <ul style="list-style-type: none"> <li>• parameter name matching is not case sensitive</li> <li>• double quotes around values are required to preserve white space (for example, PropertyA="a value with spaces")</li> <li>• command-line parameter values supersede property values supplied in a configuration file</li> <li>• double quotes in values are permitted, but must be doubled (for example, PropertyB="""quoted"" value")</li> </ul> <p><b>Examples: Setting Password Properties</b></p> <p>Include one or more of the following on the command line to set the respective passwords to the value, <b>secret</b>.</p> <ul style="list-style-type: none"> <li>• AdministratorPassword=secret</li> <li>• KspUserPassword=secret</li> <li>• CertificatePassword=secret</li> <li>• CertificateServicePassword=secret</li> </ul>
<p><b>/c</b> filepath (where <code>filepath</code> is the user-defined file name)</p>	<p>Runs the installation setup (<code>SetupApplicationServer.exe</code> or <code>SetupWebServer.exe</code>) and uses the configuration data found in the configuration file. When used with the <b>/s</b> parameter, the installation runs in silent mode.</p> <p> <b>Note:</b> You can use the configuration file that was created using the <b>/t</b> command line parameter or you can use the sample configuration file provided in the install directory.</p> <p>If you use the configuration file created by using the <b>/t</b> parameter, you must add the passwords before using that file with the <b>/c</b> parameter.</p>
<p><b>/l</b> filepath (where <code>filepath</code> is the logging directory)</p>	<p>Overrides the default location for the installation log file.</p>

Command Line Parameter	Description
<p><b>/p</b> installation type option (where <code>installation type option</code> values are specific to the product being installed)</p>	<p>Runs <code>SetupApplicationServer.exe</code>, 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:</p> <p><b>SetupApplicationServer.exe</b></p> <ul style="list-style-type: none"> <li>• <b>Server</b>: Installs a application server in Single Server mode.</li> <li>• <b>WorkflowServer</b>: Installs a application server in Workflow Extension Server mode.</li> <li>• <b>UserServer</b>: Installs a application server in User Extension Server mode.</li> <li>• <b>Client</b>: Installs a Workflow client.</li> </ul> <p> <b>Note:</b></p> <ul style="list-style-type: none"> <li>• These values are case-sensitive.</li> <li>• The <b>/p</b> parameter cannot be used in conjunction with silent mode (that is, the <b>/s</b> parameter) and/or a configuration file (that is, the <b>/c</b> parameter).</li> </ul>

## Uninstall Workflow

The following topic guides you through the process of removing 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 application 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 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 Workflow, it is important to determine your architecture 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.

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

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

### **Related concepts**

[One Cluster, Two Nodes \(page 51\)](#)

[Two Clusters, Two Nodes Each \(page 52\)](#)

[Three Clusters, Two Nodes Each \(page 53\)](#)

### **Related reference**

[Server Clustering and Failover Hardware Requirements \(page \)](#)

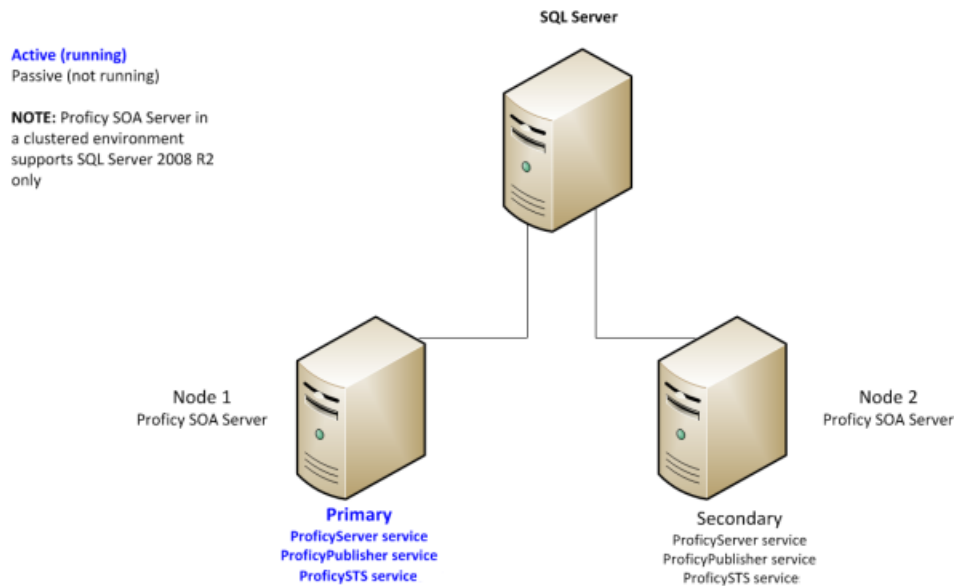
[Server Clustering and Failover Software Requirements \(page \)](#)

### 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 application servers in one cluster. Each application server must run the Proficy Server, Proficy Publisher Service, and Proficy STS services.

Figure: Two Application servers in a single cluster

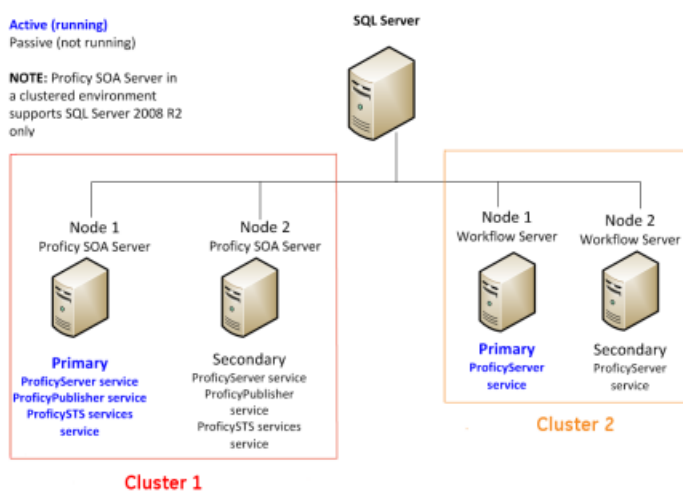


### Two Clusters, Two Nodes Each

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

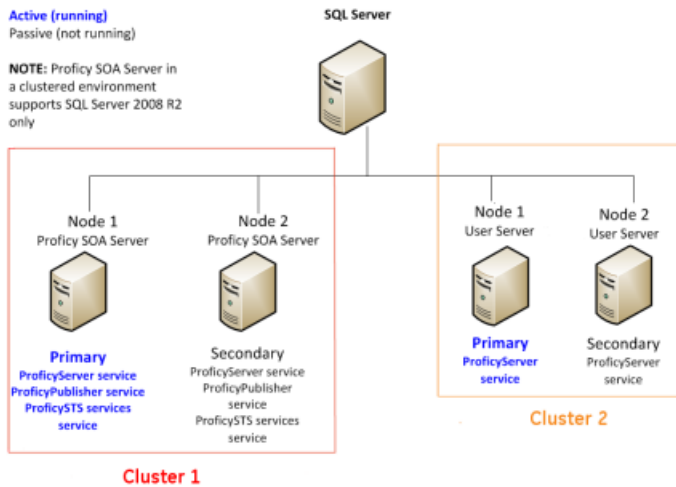
The following figures show examples of two application servers with two Workflow engines, in separate clusters, and two application servers with two User servers, in separate clusters, respectively.

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



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

*Figure: Two Application servers and two User servers, in separate clusters*



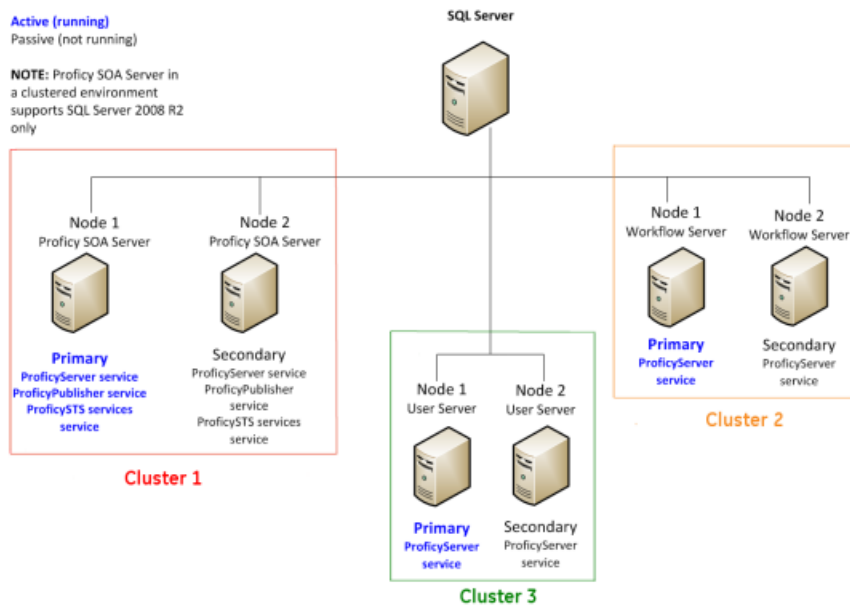
Each application server must run the Proficy Server, Proficy Publisher Service, and Proficy STS services. Each User server must run the Proficy Server service.

### 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 application servers, two Workflow engines, and two User servers, each in its own cluster. Each 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: Two Application 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 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.

### Related tasks

[Configure the primary cluster server \(page 57\)](#)

[Configure the Microsoft Failover Cluster Manager \(page 55\)](#)

[Install Microsoft Failover Cluster Manager \(page 54\)](#)


## *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 application server on both cluster nodes, pointing to the same database, before performing the following procedure.

### **Prerequisites**

[Install Microsoft Failover Cluster Manager \(page 54\)](#)

[Install a single application server and client \(page 30\)](#)


This procedure is based on a Windows<sup>®</sup> Server 2012 R2 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 service.

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 GE software 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 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 b-d.  
The **Status** indicates that the roles are *Partially Running*.
  - f. For Proficy Certificate, repeat steps b-d.
  - g. In the **Roles** window, select the name you entered in step 3g.
  - 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.

### Related concepts

[Post-installation Configuration \(page 75\)](#)


### Related tasks

[Configure a server instance \(page 83\)](#)

## *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 application server on your primary server machine, you must configure the machine as the primary cluster server to begin the clustering process.

### Prerequisites

[Install a single application server and client \(page 30\)](#)

1. On the primary server machine, On the primary server machine, click **Start > All Programs > General Electric > Workflow > Configuration > Configure Server**.  
The **Configure Server** tool appears.
2. Select the **Create an 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 role (not the name of the cluster itself) 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 Proficiency 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 extension servers.
2. Configure the Failover Cluster Server.

### **Related tasks**

[Modify security certificates \(page 76\)](#)

[Export server security certificates for an extension server \(page 41\)](#)

[Configure the failover cluster server \(page 58\)](#)

## *Configure the failover cluster server*

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

### **Prerequisites**

[Install a single application server and client \(page 30\)](#)

[Configure the primary cluster server \(page 57\)](#)

[Export server security certificates for an extension server \(page 41\)](#)

1. On the backup server machine, click **Start > All Programs > General Electric > 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 > General Electric > 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.


**i Tip:** If your Workflow 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.

#### **Prerequisites**

[Install a single application server and client \(page 30\)](#)

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, `ProficiencyClient.exe.config`, make these changes. To find this file, go to `<install location>\Program Files (x86)\Proficy\Proficy Workflow\Program\ProficiencyClient.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.

#### **Prerequisites**

[Install a single application server and client \(page 30\)](#)

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.

#### **Related concepts**

[One-click Deployment \(page 44\)](#)

## 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 Server Cluster**, **Configure the Failover Cluster Server**, and **Modify Security Certificates**.

### 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)** and **Configure a local client for a cluster node (64-bit)**.

### Running a Clustered Multi-server Environment

When running with both a clustered 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.

#### Related tasks

[Configure a local client for a cluster node \(32-bit\) \(page 59\)](#)

[Configure a local client for a cluster node \(64-bit\) \(page 60\)](#)

[Configure the primary cluster server \(page 57\)](#)

[Configure the failover cluster server \(page 58\)](#)

[Modify security certificates \(page 76\)](#)

## *Deploy the Web Task List*

### *Web Task List Deployment*

The Web Task List is automatically installed with the application server installation of 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 application server installation.

1. In the 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`.

- From **Certificates (Local Computer)**, expand `Personal\Certificates`, and then add `ProficySTSPublicKey.cer`.

### Related concepts

[Security Certificates \(page 14\)](#)

### Related tasks

[Modify security certificates \(page 76\)](#)

[Install a single application server and client \(page 30\)](#)

### Related reference

[SSL Security Configuration \(page \)](#)

[Security Certificate Options \(page 15\)](#)

## 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.

**i 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.

**📄 Note:** Before you make any changes to Internet Information Services (IIS), you may want to export your existing configuration to review it. For more information on an existing Microsoft utility, refer to <https://www.iis.net/learn/get-started/getting-started-with-iis/getting-started-with-appcmdexe>


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

- HTTP Logging
- Tracing


**i 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.
- Install the IIS ARR 2.5 (or later) module from <http://www.iis.net/download/ApplicationRequestRouting>.
  - In the **Install** window, click **Options**.
  - In the **Change Options** window, when asked which web server you want to use, click the **IIS** check box.
  - Click **OK**, and then click **Install**.



 **Note:** The URL Rewrite 2.0 module installs automatically.

6. Start the Internet Information Service (IIS) Manager application.
7. From the **Start** menu, click **Administrative Tools > Internet Information Services (IIS) Manager**.
8. Enable the server to act as a proxy.

 **Note:** This is a server-wide setting.

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

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.

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 that you want to configure.
2. From the **Actions** panel, click **Explore** to open Windows Explorer to the physical directory on disk for your web site.
  - The default location for **Default Web Site** is `C:\inetpub\wwwroot`.
  - In this location, you see a file named `web.config`.
3. Open another Windows Explorer window and navigate to your 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`.
4. In the Workflow installation directory, go to the folder **Reverse Proxy Config (IIS)** for the reverse proxy configuration files.
  - a. From the **Reverse Proxy Config (IIS)** directory, copy the following files to your web site's directory:
    - `rewriteMaps.config`
    - `rules.config`
    - `outboundRules.config`
  - b. 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:

5. Update the `rewrite.Maps.config` file with the actual server names, as follows:
  - 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 whose `rewriteMaps.config` file you want to update.
  - b. Double-click the **URL Rewrite** icon.
  - c. From the **Actions** panel, click **View Rewrite Maps**. **URL Rewrite Maps** opens in the central panel.
  - d. Double-click **ComputerNames**. **Edit Rewrite Map** opens in the central panel.
  - e. 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.
  - f. 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.
  - g. Repeat steps 5e and 5f for each server listed in the **Edit Rewrite Map** panel.

#### Related concepts

[Security Certificates \(page 14\)](#)

#### Related tasks

[Install a single application server and client \(page 30\)](#)

[Configure security certificates for a reverse proxy \(page 62\)](#)

[Configure an Apache reverse proxy for the Web Task List \(page 65\)](#)

#### Related reference

[SSL Security Configuration \(page \)](#)

[Security Certificate Options \(page 15\)](#)

## *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 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`.

### Related reference

[Inbound and Outbound Rules for Apache \(page 66\)](#)

## *Inbound and Outbound Rules for Apache*

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

### Inbound Rules

<b>SSLProxyEngine On:</b>		
ProxyPass	/Proficy/	http:// YourSOAWorkflow.company.com:8020/ Proficy/
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/SOAPProject/	https:// YourSOAWorkflow.company.com:8203/ SOAServer/SOAPProject/
ProxyPassReverse	/SOAServer/SOAPProject/	https:// YourSOAWorkflow.company.com:8203/ SOAServer/SOAPProject/

<b>SSLProxyEngine On:</b>		
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

<b>AddOutputFilterByType</b> <b>SUBSTITUTE text/xml</b>	
SUBSTITUTE	"s <SOAServerName>.*</SOAServerName>  <SOAServerName> <b>YourApacheServer.company.com</b> </ SOAServerName> i"
SUBSTITUTE	"s <StsServiceName>.*</StsServiceName>  <StsServiceName> <b>YourApacheServer.company.com</b> </ StsServiceName> i"
SUBSTITUTE	"s <StsSecurePort>.*</StsSecurePort>  <StsSecurePort>443</StsSecurePort> i"
SUBSTITUTE	"s <HttpsSamlPort>.*</HttpsSamlPort>  <HttpsSamlPort>443</HttpsSamlPort> i"
SUBSTITUTE	"s <WorkflowServerName>.*</WorkflowServerName>  <WorkflowServerName> <b>YourApacheServer.company.com</b> </ 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:// <b>YourApacheServer.company.com</b> :443/ \$2</a:anyURI>\$3 i"

## Related tasks

[Configure an Apache reverse proxy for the Web Task List \(page 65\)](#)

## 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.

**i Tip:** To improve performance, ensure that caching is enabled in Internet Explorer.

### Prerequisites

[Install a single application server and client \(page 30\)](#)

[Configure an IIS reverse proxy for the Web Task List \(page 63\)](#)

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	<p><a href="https://myiisserver.example.com/Proficy/Workflow/WebTaskList.html">https://myiisserver.example.com/Proficy/Workflow/WebTaskList.html</a></p> <p><b>Note:</b> Assumes reverse proxy IIS web server is externally accessible via host name <code>myiisserver.example.com</code> with an SSL certificate specifying that host name listening on standard port 443 (default).</p>
Apache Reverse Proxy	<p><a href="https://myapacheserver.example.com/Proficy/Workflow/WebTaskList.html">https://myapacheserver.example.com/Proficy/Workflow/WebTaskList.html</a></p> <p><b>Note:</b> Assumes reverse proxy Apache web server is externally accessible via host name <code>myapacheserver.example.com</code> with an SSL certificate specifying that host name listening on standard port 443 (default).</p>

---


## Web Server

## URL

### 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.

Assumes 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 Workflow server of the Proficy STS security certificate.

### Related concepts

[Security Certificates \(page 14\)](#)

### Related tasks

[Configure security certificates for a reverse proxy \(page 62\)](#)

[Configure an Apache reverse proxy for the Web Task List \(page 65\)](#)

### Related reference

[SSL Security Configuration \(page \)](#)

[Security Certificate Options \(page 15\)](#)

# Log On Overview

## Log On Overview

After installing Workflow, the primary administrator user configured during installation can manually log into 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 Workflow users, Windows users, and SSO (GE Single Sign on).

### Related concepts

[Security Concepts \(page \)](#)

[Login and Logout Capabilities \(page \)](#)

[Manual Login and Logout \(page \)](#)

[Automatic Login and Logout \(page \)](#)

[Windows Domain-Based Security \(page \)](#)

[Multiple Sessions of Workflow \(page \)](#)

## Log on to Workflow client


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

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

### Prerequisites

[Windows Domain-Based Security \(page \)](#)



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

If...	Then do the following...
<p><b>An instance of Workflow is <u>not</u> running on the workstation.</b></p>	<ol style="list-style-type: none"> <li>a. Launch the Workflow client using either the <b>Start</b> menu or desktop icon.</li> <li>b. On the main Workflow screen, click <b>Log in to Workflow</b>.</li> </ol> <p> <b>Note:</b> You can also use this path if an instance of Workflow is already running on the workstation.</p>

If...	Then do the following...
An instance of <b>Workflow</b> is running on the workstation,	a. On the Workflow toolbar, click <b>New Session</b> .

The **Workflow Login** dialog box appears.

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


Select...	If...
<b>Workflow Authentication</b>	Your user profile is part of the Workflow application.
<b>Windows Authentication</b>	Your user profile is part of the Windows domain.   <b>Important:</b> To log in using Windows Authentication, your server and client(s) must be on a domain. The domain field is populated using the domain that the computer joins. If the user logging in is from a different domain, this field is populated using the domain that this user belongs to.
<b>SSO Authentication</b>	Your user profile is part of SSO security.   <b>Note:</b> SSO Authentication is not available if it has not been enabled.

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

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

- In the **Password** field, enter your password.

- If applicable, in the **Domain** field, enter the domain name.

 **Note:** To log in using Windows Authentication, your server and client(s) must be on a domain. The domain field is populated using the domain that the computer joins. If the user logging in is from a different domain, this field is populated using the domain that this user belongs to.

- Click **OK**.

#### Related concepts

[Login and Logout Capabilities \(page 5\)](#)

[Multiple Sessions of Workflow \(page 5\)](#)

[System Health and Program Use \(page 6\)](#)



## *Automatically log into Workflow*

The default method of logging in to 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.

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

### **Prerequisites**

[Configure automatic login \(page 6\)](#)

1. Launch the Workflow client using either the **Start** menu or desktop icon.  
If automatic login is enabled and configured, the user credentials are authenticated and the Workflow client appears.
2. If applicable, launch additional sessions of 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.

### **Related concepts**


[Automatic Login Authentication \(page 6\)](#)

[Windows Domain-Based Security \(page 6\)](#)


[System Health and Program Use \(page 6\)](#)

## *GE Single Sign On (SSO)*

You can configure Workflow to use GE Single Sign On (SSO) authentication when your users log on to the Workflow 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 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:** To log in to Workflow, the system must be in a state of either *Complete* or *Partial* health. For more information, see **System Health and Program Use**.

## **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 select either the **Production Identity Provider** or **Non-Production Identity Provider** option. During a new installation or an upgrade, when you select the **Use SSO** (Single Sign On) check box, the **Production Identity Provider** option is selected by default.

The Production Identity Provider option provides greater security for your application. The Non-Production Identity Provider can be used for non-production environments, such as test environments.

## 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 Workflow user account. That is, if a user with a valid SSO ID but no Workflow user account tries to log in to Workflow, the SSO Authentication Failed event is triggered and causes the Workflow 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.

### Related concepts

[Workflow User Password Security \(page 6\)](#)  
[System Health and Program Use \(page 6\)](#)

### Related tasks

[Install a single application server and client \(page 30\)](#)  
[Configure GE Single Sign on \(SSO\) \(page 6\)](#)

## Authentication



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

### Authentication Types

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




The computer you use to log in, stores the authentication type in the `proficyclient.exe.config` file. When you start a new client on that computer, the authentication type that you had selected during your previous login session is automatically selected. However, if another user had successfully logged in to that computer with a different authentication type between now and the previous time you had logged in, then 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
Workflow Authentication	System-defined	Your user profile is part of the Workflow application.
Windows Authentication	System-defined	<p>Your user profile is part of the Windows domain.</p> <p> <b>Important:</b> To log in using Windows Authentication, your server and client(s) must be on a domain. The domain field is populated using the domain that the computer joins. If the user logging in is from a different domain, this field is populated using the domain that this user belongs to.</p> <p>You must have added your user accounts to one or more active directory universal or global groups that are mapped to Workflow groups.</p> <p>The computer stores the domain name you enter in the <code>proficyclient.exe.config</code> file. When you start a new client, that domain name appears in the <b>Domain</b> field. However, if another user successfully logged in under a different domain since your last log on, that domain name will be displayed.</p> <p>If you attempt to log in under a different domain but the authentication fails, the domain name is not updated in the <code>proficyclient.exe.config</code> file.</p>
SSO Authentication	System-defined	<p>Your user profile is part of SSO security.</p> <p> <b>Note:</b> SSO Authentication is not available if it has not been enabled.</p>

## Login Properties

Property	Value	Description
User Name	User-defined	Specifies your unique user name


Property	Value	Description
Password	User-defined	Specifies your unique password.   <b>Note:</b> 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 when the <b>Windows Authentication</b> option is selected.
Change Password	N/A	Click this link to open the <b>Proficy Workflow Change Password</b> dialog box where you can create a new password.   <b>Note:</b> This link is available only if this feature is enabled.
Auto Login	System-defined	Click this button to automatically log in the Workflow.   <b>Note:</b> This button is available only when the Windows Authentication option is selected <u>and</u> automatic login is configured.

## *Post-Installation Configuration*

### *Post-installation Configuration*

This 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 for assistance.

### *Running with a Standard Windows User Account*

Users who are not 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 Workfkow. 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...
<p><b>accounts to use a static proxy server with exclusions</b></p>	<p>a. Execute: <code>bitsadmin /util /setieproxy localsystem MANUAL_PROXY proxysrv:8080 ";*. contoso.com"</code></p> <p>b. Replace <code>proxysrv</code>, <code>8080</code>, and <code>contoso.com</code> with your organization's proxy server addresses address, port, and exclusions.</p>
<p><b>account to use proxy.pac file</b></p>	<p>a. Execute: <code>bitsadmin /util /setieproxy localsystem AUTOSCRIP http:// contoso.com/proxy.pac</code></p> <p>b. Replace <code>proxysrv</code> with your organization's pac file addresses.</p>

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

### Related concepts

[Web Services Service Provider \(WSSP\) \(page \)](#)

### Related tasks

[Add a web services definition \(page \)](#)

[Install a single application server and client \(page 30\)](#)

## *Modify security certificates*

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

Before you modify security certificates:

- Copy security certificates and transfer the copies to your extension servers.
- Update the security certificates to match the server.

### **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 servers. The SSL/TLS Server Certificate must be unique to each server.
- If you change the certificate option on your servers, 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**

Beginning with Workflow 2.5, legacy certificates are no longer supported.

1. On the server machine, On the server machine, click **Start > All Programs > General Electric > 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**.
3. Click **Save**, and then click **Exit**.

### **Related concepts**

[Post-installation Configuration \(page 75\)](#)

[Security Certificates \(page 14\)](#)

### **Related tasks**

[Install a single application server and client \(page 30\)](#)

[Modify the server configuration for a remote client \(page 80\)](#)

[Use self-signed certificates for the web server \(page 20\)](#)

### **Related reference**

[Security Certificate Options \(page 15\)](#)

## 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 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 computer, click **Start > All Programs > General Electric > Workflow > Configuration > Configure Site**.  
The **Configure Site** tool appears.
2. Modify the server configuration, as required.

### If you want to...


**Designate a server or a product option as essential**

**Designate a server or a product option as nonessential**


**Move a product option between servers**

### Then do this:

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.

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.

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.

---

**If you want to...****Disable a product option****Then do this:**

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 Workflow program. For more information, see **System Health and Program Use**.

**Related concepts**

[System Health and Program Use \(page 6\)](#)

**Related tasks**

[Configure a server instance \(page 83\)](#)


*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 site 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.

### Related concepts

[System Health and Program Use \(page 6\)](#)

[Multiple Servers \(page 22\)](#)

### Related tasks

[Modify site configuration \(page 77\)](#)

## *Modify the server configuration for a remote client*

Use the **Server Configuration** tool to synchronize any changes you may have made to the 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 > General Electric > 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 > General Electric > 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.

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

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 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 before you install Workflow. For more information, see **Software Requirements** in the Workflow IPI documentation.


In order for Workflow to connect to Microsoft® SQL Server at runtime, you must configure SQL Server to enable the *db\_owner* role for the applicable login account. For more information, see **Enable Connection between Workflow and SQL Server**.

The Workflow installation automatically selects the default SQL Server instance. For example, 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** and **3** of this procedure.

1. Click Start > All Programs > General Electric > 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...
<b>Automatically</b>	<ol style="list-style-type: none"> <li>a. Select the Use a local database with Windows Authentication check box.</li> </ol> <p> <b>Note:</b> To use this option, the following SQL Server conditions apply:</p> <ul style="list-style-type: none"> <li>• Installed locally, AND</li> <li>• Designated as default Local Host, AND</li> <li>• Uses Windows Authentication</li> </ul>
<b>Manually</b>	<ol style="list-style-type: none"> <li>b. Proceed to step <b>4</b>.</li> </ol> <ol style="list-style-type: none"> <li>a. Clear the Use a local database with Windows Authentication check box.</li> <li>b. Proceed to step <b>3</b>.</li> </ol>

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 with a default instance, you may 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**.
  - If you select SQL Server Authentication, proceed to step **3.d**.


- d. Enter the `User Name` and `Password` that are configured for SQL Server authentication, and then proceed to step 4.

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


## *Configure a server instance*

The **Configure Server** tool is used to create an 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 > General Electric > Workflow > Configuration > Configure Server**.
2. Select the Create an 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 **P2P Configuration** section:
  - a. In the **IP Address** field, enter the IP address of the server instance.

 **Note:** Peer servers will contact this server instance at the specified IP address. If the specified address is 255.255.255.255, then the address will be determined at server start as the first IPv4 address found in the DNS records for the hosting machine's host name. If the address is incorrect, then an appropriate address should be specified here.

- b. In the **Port** field, enter the port number for the server instance. This value must be unique if multiple server instances are run on the same machine.
10. Click **Save**, and then click **Exit**.

## Related concepts

[Server Clustering and Failover \(page 24\)](#)

## Related reference


[Windows Services for Workflow \(page 13\)](#)


## Configure product options

Using the **Configure Product Options** tool, you can install and configure 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** 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:

### Prerequisites

[Install a single application server and client \(page 30\)](#)

[Install Multiple Servers \(page 41\)](#)

1. On the server machine, click **Start > All Programs > 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...**

**Installing a product option.**

#### **Then do this...**

- a. Click **Install**.

Your directory opens at the `ProductOptions` folder within the `Workflow` installation directory.

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

---


**If you are...****Uninstalling a product option.**

 **Note:** You cannot uninstall the default product options that are included in the server installation.

**Then do this...**

- a. Select the product option you want to uninstall.
  - b. Click **Uninstall**.
  - c. Click **Save**, then click **Exit**.
- 

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**.

**Related concepts**

[Architecture Considerations \(page 10\)](#)

## *Change architecture mode*

When initially installing an 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.

**Prerequisites**

[Architecture Considerations \(page 10\)](#)

1. On the machine that the server is installed on, click **Start > All Programs > General Electric > Workflow > Configuration > Configure Server**.  
The **Configure Server** tool appears.
2. Select the Create an 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 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...
<b>Add counters</b>	<installfolder>ProficyServer[exe] / installperformancounters
<b>Remove counters</b>	<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.

### **Related tasks**

[View performance counters \(page 30\)](#)

## *Display the host server name in the Workflow client*

By default, the server name is displayed in the client, next to the server state icon. However, if you want to display a more meaningful name for your server, you can configure an alias so that the alias is displayed in the client rather than the actual server name.

You must install Workflow 2.5 SIM3 (or greater) before performing this task.

1. On the Workflow client computer, navigate to the C:\Program Files (x86)\Proficy\Proficy Workflow\Program\Data folder.
2. Open the UserStartup.xml file in a text editor.


The following code shows samples of multiple server names and aliases. You can copy this code into the `UserStartup.xml` file, before the closing `</ServerConnectionInfo>` element, and then change the `Name` and `Alias` elements to reflect your server information.

```
<ServerAliases>
  <ServerAlias>
    <Name>localhost</Name>
    <Alias>QA Server</Alias>
  </ServerAlias>
  <ServerAlias>
    <Name>Product-WIN81</Name>
    <Alias>Development Server</Alias>
  </ServerAlias>
  <ServerAlias>
    <Name>devwin7ex64dev</Name>
    <Alias>Product Server</Alias>
  </ServerAlias>
</ServerAliases>
```

When you launch the Workflow client, the alias that you configured for the server is displayed next to the state icon.


## *Client and Server Configurations*

Workflow supports adding server and client configurations that are not included in the respective configuration files.

 **CAUTION:** Performance can be affected if values are adjusted in the configuration files.

The following steps apply to both client and server configuration files.

1. Determine which configuration(s) and value(s) you want to add to the applicable file.
2. Use the following XML element example to configure the file.

 **Note:** All new configurations must be added to the `<appSettings>` element.

```
<appSettings>
  <add key="ServerStatePingInterval" value="10" />
</appSettings>
```



 **Note:**

- If the configuration is for a client, then start a new client for the new configuration to take effect.
- If the configuration is for the SOA or STS service, then restart that service for the new configuration to take effect.






## Client Configuration

All client configurations are added to the `ProficyClient.exe.config` file.

Configuration	Description
<code>ServerStatePingInterval</code>	Specifies the server state refresh interval. Sites with a large number of clients may need to increase this interval to prevent high load from the continuous pings. The default value is 30 seconds.
<code>NavigatorSearchMaximumDisplayResults</code>	Specifies the maximum number of objects that can be displayed in the navigator's search results area. The default value is 500.
<code>ChannelPoolMaxIdleAgeHours</code>	<p>Specifies the maximum amount of time (in hours) that a channel is held idle in the pool before being destroyed due to inactivity. The default value is 24 hours; the minimum value is 1 hour. If a valid value is not found or the value is less than the minimum, then the default value is used.</p> <p> <b>Note:</b> GE recommends a value no greater than 168 hours (one week) for practicality and to avoid possible overflow when converting to milliseconds. It is significant because channel creation is expensive when the server is busy. Thus we want to reuse channels where possible, especially where sites have an expensive event or operation occurring at a regular frequency. Setting this value to a period longer than the site event frequency allows channels to be maintained from the last occurrence so that few, if any, channels need to be created to satisfy the operation.</p>
<code>OperationTimeoutSeconds</code>	Specifies the WCF operation timeout. The default value is 600 seconds.
<code>ReceiveTimeoutMinutes</code>	<p>Specifies the WCF receive timeout. The default value is 48 hours. If this value is configured as 0, the <code>TimeSpan</code> maximum value is used.</p> <p> <b>Note:</b> The time span value must be at least double the <code>ChannelPoolMaxIdleAgeHours</code> value.</p>
<code>UseDefaultWebProxy</code>	Indicates whether the auto-configured HTTP proxy of the system should be used, if available. The default value is <code>True</code> .
<code>UserPermissionsRefreshMinutes</code>	Specifies the length of time it takes for a permission change to take effect. The default value is 1 minute.

## Server Configuration: SOA Service

The following configurations are added to the `ProficyServer.exe.config` file.

Configuration	Description
WorkflowDomainServiceStartupPollingFrequencyInSeconds	Specifies the Workflow domain service start up polling frequency (in seconds). This configuration is used to check the essential services status. Waits for all essential service providers to start before starting the Workflow domain service. The default value is 10 seconds. If the configured value is less than 1 second, then the default value is used.
CacheBasePath	Specifies the root directory for all client caches. The default value is C:\Users\ <myusername>\AppData\Local.</myusername>
LicensePollPeriodMinutes	Specifies the read and update license interval. The default value is 10 minutes. The maximum value is 24*60 minutes and the minimum value is 1 minute.
sqlCommandTimeout	Specifies the SQL command timeout (in seconds), from the configure file. A value of 0 indicates no limit (an attempt to execute a command will wait indefinitely). The default value is 30 seconds.
ChannelPoolMaxIdleAgeHours	<p>Specifies the maximum amount of time (in hours) that a channel is held idle in the pool before being destroyed due to inactivity. The default value is 24 hours; the minimum value is 1 hour. If a valid value is not found or the value is less than the minimum, then the default value is used.</p> <p> <b>Note:</b> GE recommends a value no greater than 168 hours (one week) for practicality and to avoid possible overflow when converting to milliseconds. It is significant because channel creation is expensive when the server is busy. Thus we want to reuse channels where possible, especially where sites have an expensive event or operation occurring at a regular frequency. Setting this value to a period longer than the site event frequency allows channels to be maintained from the last occurrence so that few, if any, channels need to be created to satisfy the operation.</p>
logStatistics	<p>Indicates whether to log client dispatch details. The default value is <code>False</code>.</p> <p> <b>Note:</b> This configuration must enable tracing in the configuration file:</p> <pre data-bbox="834 1486 1419 1583">&lt;logger name="ProxyClientDispatcher"   threshold="DEBUG"&gt; &lt;file value=%TraceDir%\ProxyClientDispatcher.log"/&gt; &lt;/logger&gt;</pre>
ReceiveTimeoutMinutes	<p>Specifies the WCF receive timeout. The default value is 48 hours. If this value is configured as 0, the <code>TimeSpan</code> maximum value is used.</p> <p> <b>Note:</b> The time span value must be at least double the <code>ChannelPoolMaxIdleAgeHours</code> value.</p>
OperationTimeoutSeconds	Specifies the WCF operation timeout. The default value is 600 seconds.

Configuration	Description
UseEquipmentClassStoredProcedures	Indicates whether to use stored procedures to update equipment class properties to improve performance. The default value is <code>False</code> .
HistorianDeleteTimeout	Specifies the Historian deletion timeout. The default value is <code>300</code> seconds.
HistorianManualSyncOnly	Indicates whether Historian synchronization will only be triggered manually rather than automatically on startup. The default value is <code>False</code> .
HistorianCustomCollectorNames	Specifies the Historian collector names to synchronize that are not registered collectors in your Historian server. Use a comma (,) as a separator.
EquipmentProvisioningTimeout	<p>This timeout configuration is for the equipment provisioning tool to process provisioning commands. By default, the equipment provisioning process times out if the processing time exceeds 10 minutes. For very large amounts of commands (for example, tens of thousands), 10 minutes may be insufficient preventing the provisioning from completing. If required, the timeouts can be adjusted.</p> <p>The following appSetting can be added. The value is the timeout in seconds.</p> <pre>&lt;add key="EquipmentProvisioningTimeout" value="1200" /&gt;</pre> <p>If a value greater than 10 minutes is used, the WCF timeout must also be adjusted higher than the default of 10 minutes.</p> <pre>&lt;add key="OperationTimeoutSeconds" value="1200" /&gt;</pre>
DisplayCacheFolder	<p>Specifies a custom folder path to store user display projects and assemblies on client machines. The path must be absolute; however, environment variables can be used as part of the path. For example:</p> <pre>"%ProgramData%\Workflow Displays"</pre> <p>The default path is the <code>Proficy Workflow</code> folder in your <code>My Documents</code> folder.</p>

## Server Configuration: SOASecurity Token Service

The following configurations are added to the `ProficySTS.exe.config` file.

Configuration	Description
MaximumClockSkew	Specifies the maximum allowable time difference between the system clocks of the two parties that are communicating. The default value is <code>5</code> minutes. Use a maximum value of <code>10</code> minutes.

## Server Limit Overrides

There are many limits in the Proficity SOA server that can be changed without recompiling any source. These limits are changed by adding a named file with the new limits to the Program folder.

The following steps apply to all server limits that you want to override.

1. Determine which server limit(s) and limit group(s) you want to override.
2. In the Program folder, (that is, <install\_dir>\Proficity\Proficity Workflow \Program, create a file called <LimitGroup>.lim. For example, to change a limit in the SystemLimits group, name the file SystemLimits.lim.
3. Add the XML content to the file, as shown in the following example. Add a <limit> element for each limit you want to override.

```
<?xml version="1.0" encoding="utf-8" ?>
<limitOverrides>
  <limit name="QueryResultLimit" warningThreshold="5000"
  errorThreshold="5000" />
</limitOverrides>
```

## DmsLimits

Limit	Description
ConstraintLimit	Specifies the maximum number of references between the same parent and child. The default warningThreshold is 4 and the default errorThreshold is 4.
PrimaryKeyLimit	Specifies the maximum number of components (properties and references) that can make up a primary key. The default warningThreshold is 6 and the default errorThreshold is 6.
AttributeLimit	Specifies the maximum number of attributes that can be defined in a Model Object Type. The default warningThreshold is 100 and the default errorThreshold is 100.
ReferenceLimit	Specifies the maximum number of references that can be defined on a Model Object Type. The default warningThreshold is 20 and the default errorThreshold is 20.
SessionObjectLimit	Specifies the maximum number of objects that a session can contain. The default warningThreshold is 20000 and the default errorThreshold is 20000.
ClassesPerInstanceLimit	Specifies the maximum number of Classes that can be added to an instance. The default warningThreshold is 50 and the default errorThreshold is 50.

<b>Limit</b>	<b>Description</b>
ClassPropertyLimit	Specifies the maximum number of properties that can be added to a class. The default warningThreshold is 1000 and the default errorThreshold is 1000.
TotalPropertyLimit	Specifies the maximum number of properties (that is, the associated class properties and instance properties combined) that can be on an instance. The default warningThreshold is 5000 and the default errorThreshold is 5000.

## ProductionLimits

<b>Limit</b>	<b>Description</b>
S95IdLength	Specifies the maximum length of the S95 ID attribute for S95 resources. The default warningThreshold is 50 and the default errorThreshold is 50.
DescriptionLength	Specifies the maximum length of the Description attribute for S95 resources. The default warningThreshold is 255 and the default errorThreshold is 255.
UnitOfMeasureLength	Specifies the maximum length of the unit of measure fields for S95 resources. The default warningThreshold is 50 and the default errorThreshold is 50.

## ProductionModelLimits

<b>Limit</b>	<b>Description</b>
SegmentHierarchyDepth	Specifies the maximum number of levels that can be in the process or product segment hierarchy. The default warningThreshold is 4 and the default errorThreshold is 4.
Number OfProcessSegments	Specifies the maximum number of process segments that can be in a project. The default warningThreshold is 5000 and the default errorThreshold is 5000.
NumberOfAssociatedProcessSegments	Specifies the maximum number of process segments that can be associated with a product segment. The default warningThreshold is 1 and the default errorThreshold is 1.
NumberOfResourceSpecificationsPerSegment	Specifies the maximum number of a particular type of resource specification (material/equipment/personnel) that can be created for one segment. The default warningThreshold is 500 and the default errorThreshold is 500.
NumberofResourceSpecificationsPerSegmentRequirement	Specifies the maximum number of a particular type of resource specification (material/equipment/personnel) that can be associated with one segment requirement. The default warningThreshold is 1000 and the default errorThreshold is 1000.

<b>Limit</b>	<b>Description</b>
NumberOfResourceSpecificationsForMasterSegment	Specifies the maximum number of a particular type of resource specification (material/equipment/personnel) that can be created for a Master Segment. The default warningThreshold is 1200 and the default errorThreshold is 1200.
NmberOfSegmentsPerWorkDefinition	Specifies the maximum number of segments in a work definition. The default warningThreshold is 50 and the default errorThreshold is 50.
NumberOfOverallSegmentsPerWorkDefinition	Specifies the maximum number of segments, under all hierarchy levels, in a work definition. The default warningThreshold is 200 and the default errorThreshold is 200.
NumberOfParametersPerSegmentRequirement	Specifies the maximum number of parameters that can be associated with a segment requirement. This value is twice the maximum number of parameters per process/product segment. The default warningThreshold is 200 and the default errorThreshold is 200.
NumberOfWorkRequestsPerArchive	Specifies the maximum number of work requests that can be archived at once. The default warningThreshold is 500 and the default errorThreshold is 500.

## SystemLimits

<b>Limit</b>	<b>Description</b>
ExampleLimit	Specifies an example of a Server Core Limit. The default warningThreshold is 123 and the default errorThreshold is 124.
NameLength	Specifies the default system limit for the maximum length of object names. The default warningThreshold is 50 and the default errorThreshold is 50.
PropertyNameLength	Specifies the default system limit for the maximum length of object property names. The default warningThreshold is 200 and the default errorThreshold is 200.
DescriptionLength	Specifies the default system limit for the maximum length of object descriptions. The default warningThreshold is 255 and the default errorThreshold is 255.
QueryResultLimit	Specifies the maximum number of results to return in a WCF query. The default warningThreshold is 5000 and the default errorThreshold is 5000.

## WorkflowLimits

<b>Limit</b>	<b>Description</b>
CategoryDefinitionsLimit	Specifies the maximum number of category definitions. The default warningThreshold is 1000 and the default errorThreshold is 1000.

<b>Limit</b>	<b>Description</b>
CompletionCodeDefinitionsLimit	Specifies the maximum number of completion code definitions. The default warningThreshold is 1000 and the default errorThreshold is 1000.
ConcurrentDebugSessionsLimit	Specifies the maximum number of concurrent debug sessions. The default warningThreshold is 10 and the default errorThreshold is 10.
ConcurrentWorkflowInstancesLimit	Specifies the maximum number of concurrent workflow instances. The default warningThreshold is 1000 and the default errorThreshold is 1000.
EventScopeEventHandlerLimit	Specifies the maximum number of events allowed to be queued for an event scope activity at runtime. The default warningThreshold is 10 and the default errorThreshold is 10.
FaultDefinitionLimit	Specifies the maximum number of fault definitions. The default warningThreshold is 1000 and the default errorThreshold is 1000.
ResourceUserVersionLimit	Specifies the maximum number of resource user versions. The default warningThreshold is 1000 and the default errorThreshold is 1000.
SubprocessDefinitionLimit	Specifies the maximum number of subprocess definitions. The default warningThreshold is 1000 and the default errorThreshold is 1000.
TaskClientTaskHistoryResultsLimit	Specifies the maximum number of task client and history results. The default warningThreshold is 1000 and the default errorThreshold is 1000.
WorkflowDefinitionsLimit	Specifies the maximum number of workflow definitions. The default warningThreshold is 1000 and the default errorThreshold is 1000.
WorkflowScheduleLimit	Specifies the maximum number of workflow schedules. The default warningThreshold is 3000 and the default errorThreshold is 3000.
UserActivityLimit	Specifies the maximum number of user activities. The default warningThreshold is 500 and the default errorThreshold is 500.
DataItemLimit	Specifies the maximum number of data items. The default warningThreshold is 100 and the default errorThreshold is 100.
UserActivityNestingLimit	Specifies the maximum number of user activity nesting levels. The default warningThreshold is 5 and the default errorThreshold is 5.

## FormLimits

Limit	Description
EventDefinitionsLimit	Specifies the number of event definitions allowed to be defined on a form. The default warningThreshold is 15 and the default errorThreshold is 15.
DataItemDefinitionsLimit	Specifies the number of data item definitions allowed to be defined on a form. The default warningThreshold is 20 and the default errorThreshold is 20.
InputParameterDefinitionsLimit	Specifies the number of input parameter definitions allowed to be defined on a form. The default warningThreshold is 100 and the default errorThreshold is 100.
OutputParameterDefinitiosLimit	Specifies the number of output parameter definitions allowed to be defined on a form. The default warningThreshold is 100 and the default errorThreshold is 100.
ServiceProviderDefinitionsLimit	Specifies the number of Service Provider method definitions allowed to be defined on a form. The default warningThreshold is 20 and the default errorThreshold is 20.

## ResourceLimits - For Database Provider

Limit	Description
MaximumDatabaseConnectionLimit	Specifies the maximum number of connections that can be held. The default warningThreshold is 100 and the default errorThreshold is 100.
MaximumDatabaseStatementsLimit	Specifies the maximum number of statements that can be held. The default warningThreshold is 500 and the default errorThreshold is 500.

## ResourceLimits - For Web Service Provider


Limit	Description
MaximumWebServicesLimit	Specifies the maximum number of web services that can be held. The default warningThreshold is 100 and the default errorThreshold is 100.

## *Upgrade Workflow*



## Upgrading Workflow


Please refer to the WorkflowIPI PDF for information on upgrading Workflow, compatibility with earlier versions and other GE Products. Read this topic for general information about upgrading your applications.

 **Important:** When you upgrade the application server, you must also upgrade all of the remote clients that connect to that server to use the same version of Workflow.

## Upgrade Paths

You can upgrade Workflow without having to uninstall the program.

- From Workflow 2.5 SP4 to Workflow 2.6
- From Workflow 2.5 SP3 to Workflow 2.5 SP4
- From Workflow 2.2 SP2 to Workflow 2.5 SP4
- From Workflow 2.5 SP1 to Workflow 2.5 SP4
- From Workflow 2.5 to Workflow 2.5 SP4
- From Workflow 2.5 SP2 to Workflow 2.5 SP3
- From Workflow 2.5 SP1 to Workflow 2.5 SP3
- From Workflow 2.5 to Workflow 2.5 SP3
- From Workflow 2.2 SP1 to Workflow 2.5 SP3
- From Workflow 2.5 SP1 to Workflow 2.5 SP2
- From Workflow 2.5 to Workflow 2.5 SP2
- From Workflow 2.5 to Workflow 2.5 SP1
- From Workflow 2.1 to Workflow 2.5
- From Workflow 2.2 service pack 1 (SP1) to Workflow 2.5
- From Vision 6.2 to Vision 6.3

 **Note:** All versions of Vision prior to version 6.3 must be uninstalled before being upgraded to Workflow 2.5 SP1.

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

 **Note:** You must first upgrade Workflow 1.5 SP4 to Workflow 2.0.

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

## GE Historian

If you use GE Historian as a data source, then when you upgrade Workflow to v2.5 SP2 the existing GE Historian server address is automatically displayed in the **Server Name** field in the **Data Source**

**Editor.** You cannot change the server's alias (that is the name displayed in the **Historian Servers** list in the navigator). To change the alias, you must delete the connection, and then add a new one. For more information, see **Change the Historian Server** and **Add an Historian Server**.


## Legacy Certificates

Starting with 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 an 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 Workflow 2.2 SP1, you must bind them again inside the Form activity (see **Configure a 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 Workflow 2.2 SP1.

## Upgrading a Clustered Environment

After upgrading Workflow on the primary server machine, you must reconfigure that machine as the primary server (see **Configure the Primary Cluster Server**) in the cluster, as well as reconfigure the failover server (see **Configure the Failover Cluster 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**.

## 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


Workflow 2.0 supports Windows domain names with personnel names and login names. If you choose to use the new functionality included with Workflow 2.0 (that is, active directory universal or global groups mapped to Workflow 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*.

 **CAUTION:** If you were using Windows user accounts in a prior version of 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 backslash 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 Workflow.

## *Install a Reporting Database*

### *Reporting Database*

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.

 **Note:** The user account used for reporting synchronization (this can be a different user than the SOA database user), must have the following SQL server roles:

- *SQLAgentOperatorRole* for the msdb database, in order to initiate the SQL Agent job
- *Db\_owner* on the reporting database

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


### Related concepts

[Reporting \(page \)](#)


## *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.

You must have installed a supported SQL Server version before you install the reporting database (see **Software Requirements**). 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** for more information. However, if the application server computer meets the requirements for both databases, they can be installed on the same computer.

If more than one version of SQL Server is installed, the integration services used for the reporting database will be the most recent version.


 **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 Server Replication](#).

1. From the application splash screen, click **Install 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**.

a. In the **SQL** field, enter the name of the SQL Server where the SQL database is located.

b. In the **Database** field, enter the name of the production (SQL) database that you will connect to for synchronization.

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.

6. In the **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 Windows administrator user name and password.
- The **Advanced user authentication settings (Use SSO, Allow Password Change, Enforce User Lockout, and Enforce Password Complex Rules)** do not apply when installing the reporting database.

8. Click **Install**.

9. When the installation is complete, click **Exit**.

### Related concepts

[Reporting Database \(page 98\)](#)

### Related tasks


[Manually synchronize databases \(page \)](#)


[Upgrade a replicated database \(page 103\)](#)

[Configure Component Services \(page 101\)](#)

## Configure Component Services

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

 **Important:** You can perform these steps either before or after installing the 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, stating that "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 2-6.

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.

## *Uninstall the reporting database*


When you uninstall reporting, the database remains intact; however, you lose the ability to synchronize the data from your production database. Uninstalling reporting does not affect the production database or the data contained in it; you can still run reports on the data stored in the database.

1. From the **Control Panel**, click **Programs and Features**.  
The **Uninstall or change a program** dialog box appears, displaying all of the programs installed on the computer.
2. Select **Reporting**, and then click **Uninstall**.
3. In the confirmation message box, click **Yes**.  
The **Uninstall Reporting** message box appears stating, "Uninstalling the Proficy Reporting application will not remove the Reporting database or the SQL Agent job from SQL Server. For a complete uninstall of this application, these should be removed manually following the uninstall."
4. Click **OK**.

## *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 Reporting Database.
2. Open the **Services** window to stop all services: click **Start > 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 Microsoft 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, and then run ProficyInstaller to upgrade the ProficyServer programs and database.
  7. Edit the *Create Replication* script.
    - a. In Microsoft SQL Server Management Studio, from the **File** menu, click **File > Open File**.
    - b. Navigate to the folder where you saved the scripts generated in step 3.
    - 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 passwords 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 Workflow client.

### Related concepts

[Reporting Database \(page 98\)](#)

### Related tasks

[Install the reporting database \(page 99\)](#)

[Manually synchronize databases \(page \)](#)

## *Terminal Server*

### *Remote Desktop Session Host*

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

#### **Security**

Encryption and other security measures protect the data exchanges between the Workflow Remote Desktop Session Host and the clients.

**Lightweight client machines**

The 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 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 (Workflow). Workflow automatically starts at log in, and the users do not have access to the Windows desktop. When they exit Workflow, they log out of the Remote Desktop Session Host account.

**Handheld environments**

Remote Desktop Services enables wireless handheld devices to display 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.

## Workflow Remote Desktop Session Host Environment

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

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


A separate session of 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 Workflow. The users' experience is nearly identical to running Workflow on their local machines. If you have clients and servers in your Workflow Remote Desktop Session Host environment, you can access and manage any of the servers from a thin client.

## *Getting Started with Remote Desktop Session Host*

Before installing Workflow on a Windows<sup>®</sup> 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<sup>®</sup> Server 2008 R2, visit the Microsoft<sup>®</sup> web site at:

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

 **Important:** Before installing the 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.

## Workflow Remote Desktop Session Host Limitations

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

- Location-based functionality in 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<sup>®</sup> Server 2008 R2 or Windows<sup>®</sup> Server 2012 installed.
- Workflow does not support running a Remote Desktop Session Host on Windows<sup>®</sup> Vista.
- Although Windows supports machine names of up to 15 characters, 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 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<sup>®</sup> Performance Monitor can help you to determine the optimal number of Remote Desktop Session Host sessions your server can handle.

## Hardware Requirements for Remote Desktop Session Host

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 for Remote Desktop Session Host

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

 **Note:** Ge Digital highly recommends that you install the latest Service Pack and Windows Updates.

## Licensing Requirements

GE Digital 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<sup>®</sup> Server 2008 R2, visit Microsoft<sup>®</sup>'s web site:


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

### *Workflow Remote Desktop Session Host Clients for Windows<sup>®</sup> Server 2008 r2*

When a Windows<sup>®</sup> 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<sup>®</sup> Server 2008 R2 client computer, you need to purchase Windows Remote Desktop Services Client Access Licenses (RDSCALs) from Microsoft<sup>®</sup>. When you first set up the 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.

 **Important:** 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<sup>®</sup> to obtain a replacement license.

### *Workflow Licensing*


All hardware and software keys distributed to run 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 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<sup>®</sup> Server 2008 R2 Remote Desktop Services

Remote Desktop Services must be enabled on the Windows<sup>®</sup> Server 2008 R2 computer that will be used as the Remote Desktop Session Host.

 **Important:** These steps must be performed before you install Workflow.

For more information about Remote Desktop Session Host, refer to the Remote Desktop Services section of the Windows<sup>®</sup> Server 2008 R2 Help or visit Microsoft's web site at: [http://technet.microsoft.com/en-us/library/dd647502\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd647502(WS.10).aspx).

1. On the Windows<sup>®</sup> 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 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 into a Remote Desktop Session Host from Windows<sup>®</sup> 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**.

#### **Related tasks**

[Configure a Remote Desktop to Connect to a Remote Desktop Session Host \(page 113\)](#)

## *Workflow with Windows Remote Desktop Session Host Installation and Configuration*

After enabling Installing Remote Desktop Services and its licensing, you can install and configure Workflow on a Remote Desktop Session Host.



## Prerequisites for 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 Workflow on a Remote Desktop Session Host, GE Digital strongly recommends that you complete the following Windows administrative tasks on the 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 Workflow on a Remote Desktop Session Host

Follow the installation steps, as outlined in the Workflow Getting Started Guide, to install 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 Efficiency Analyzer security to define the rights each user has in Efficiency Analyzer after logging in. For example, you can add further restrictions in Efficiency Analyzer 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 Workflow client program.  
  
For example, if you installed 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 Efficiency Analyzer product.  
  
For example, if you installed 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.

### Related concepts

Key Sets ([page](#) )

### Configure a Remote Desktop to Connect to a Remote Desktop Session Host

Windows<sup>®</sup> Server 2008 R2, Windows<sup>®</sup> 7, and Windows<sup>®</sup> 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 digital 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 Workflow Remote Desktop Session Host Environment*

To successfully troubleshoot your 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.

<b>For this problem area...</b>	<b>Verify...</b>
Performance	<p>Should you run fewer clients?</p> <p>Server performance increases with the following:</p> <ul style="list-style-type: none"> <li>• Faster processors</li> <li>• More processors (dual, quad)</li> <li>• More memory</li> <li>• Reduced graphic refresh rate on clients</li> </ul>
Connection	<ul style="list-style-type: none"> <li>• Is your connection problem for all connections or user specific?</li> <li>• Can the Administrator start a session locally and remotely?</li> </ul>

For this problem area...	Verify...
Environment	<ul style="list-style-type: none"> <li>• Can you create a session on the server?</li> <li>• Is the problem the same for all users including Admin?</li> <li>• Can you create a new client session?</li> <li>• Can you create a client that opens Notepad?</li> </ul>

For more information, suggestions, and tips for troubleshooting your Workflow Remote Desktop Session Host environment, refer to the Windows<sup>®</sup> Server 2008 R2 Help and the Microsoft<sup>®</sup> 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.	<p>You have started multiple sessions at the same time or multiple users have logged on using the same account.</p> <p>Multiple users cannot log on using the same account. Start one session at a time.</p> <p>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 Internet Information Services (IIS) Manager Configuration Console.</p>
The text insertion cursor in a 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 Workflow with Remote Desktop Session Host*

The following list outlines some of the frequently-asked questions about using Workflow with Remote Desktop Services.

How can I determine the number of Remote Desktop Session Host connections that my Workflow license supports?

If you have an M4 key, run the Proficy License Viewer (Proficy.ManagementConsole.exe). Select the Workflow product icon to display Workflow information.

## *ActiveX Task Controls*

### *Task Controls in GE HMIs*

The Workflow Task List can be integrated into other GE HMI applications.

Workflow task controls can be integrated into existing HMI applications, such as HMI/SCADA CIMPLICITY and 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.

#### **Related concepts**

[Tasks \(page \)](#)

[The Task List \(page \)](#)

#### **Related reference**

[Task Management for Administrators \(page \)](#)

### *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 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.
- Workflow task controls and GE HMIs are related, but work independently from each other. Therefore, user names and logins are separate.
- Like the 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**. If you install the ActiveX Task List on a different machine than the application server, you must access the Configure Client tool from the following location: `../Program Files/Proficy/Proficy Task List/Program`.


**Related concepts**


[Task Controls in GE HMIs \(page 116\)](#)

**Related tasks**


[Modify the server configuration for a remote client \(page 80\)](#)

*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.

 **Note:** 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**.


### Related concepts

[Prerequisites for Windows 2012 R2 Installations \(page 11\)](#)

### Related tasks

[Modify the ActiveX Task List installation configurations \(page 118\)](#)

## *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**. If you install the ActiveX Task List on a different machine than the 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...
<b>Manual Login</b>	prompt the user to enter a user name and password at each login.
<b>Control Property</b>	allow the user to view the user name and password in the host's object properties.
<b>Password Encryption</b>	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 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**.

### Related tasks

[Modify the server configuration for a remote client \(page 80\)](#)

## Workflow Task Client

### Overview

This topic provides an overview on how to install and start working with the workflow task client in the Operations Hub application.

- [Install the workflow task client \(page 119\)](#) from the ISO file.
- [Configure the task client \(page 126\)](#) widget in Operations Hub.
- [Access the task client \(page 130\)](#) features in Operations Hub.

### Related tasks

[Install the Task Client \(page 119\)](#)

[Uninstall the Task Client \(page 133\)](#)

[Generate an Equipment Model for Web HMI \(page \)](#)

[Import Equipment Model \(page 128\)](#)

[Create an User Account in Operations Hub \(page 129\)](#)

[Add Users and Personnel Classes \(page \)](#)

### Related reference

[Troubleshooting Task Client Issues \(page 133\)](#)

### Install the Task Client

This information guides you through the process of installing the task client on the Operations Hub server.

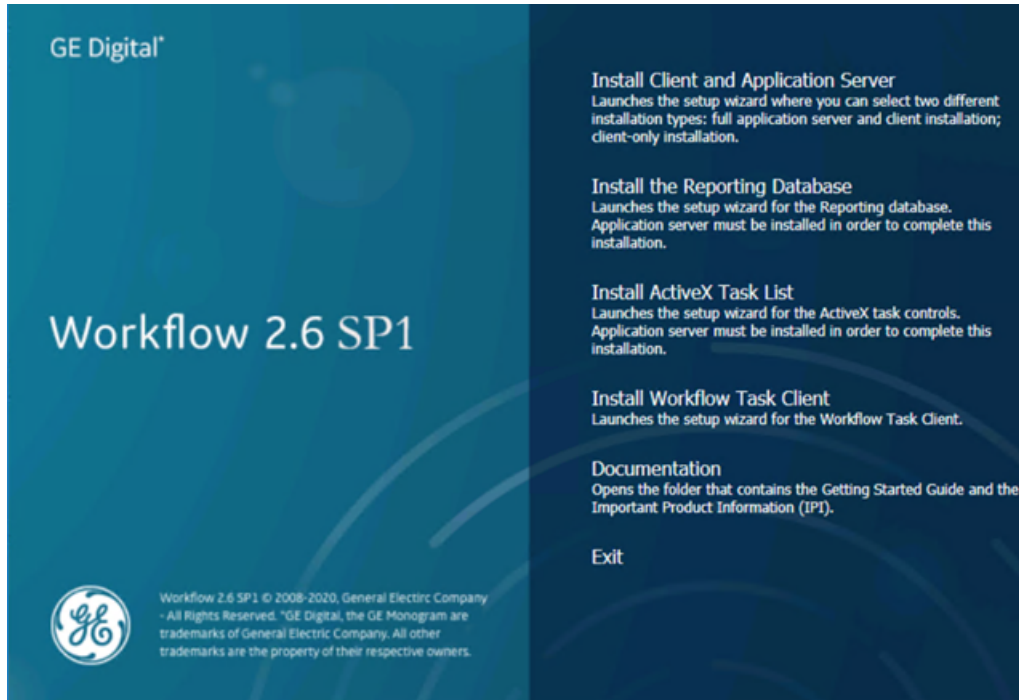
Install Operations Hub 1.7 on the machine you want to run the task client installer.


 **Note:** For instructions, refer to the Operations Hub UAA Installation Guide provided along with the Operations Hub installation package.

The task client installer is shipped as a part of the Workflow 2.6 SP1 installation package.



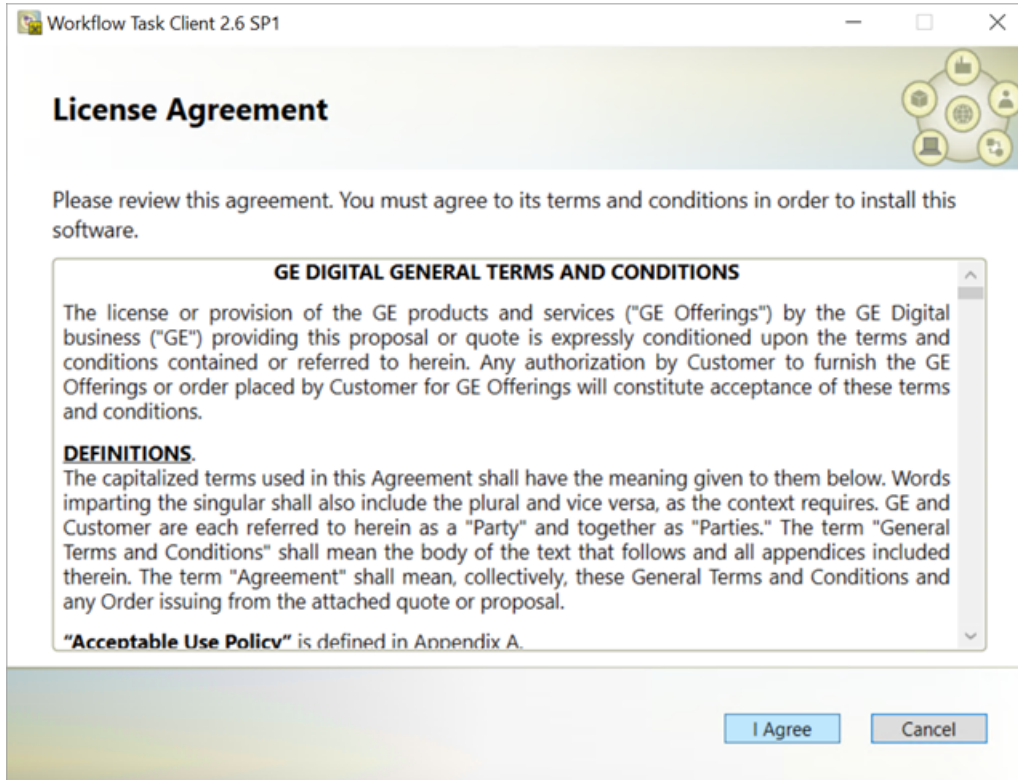
1. Copy the Workflow 2.6 SP1 ISO file to the machine where you want to install the task client, and run the file.
2. From the application splash screen, click **Install Workflow Task Client**.



 **Note:** If the splash screen does not appear, run `InstallFrontEnd.exe` on the root directory of the installation folder.

The **License Agreement** page appears.

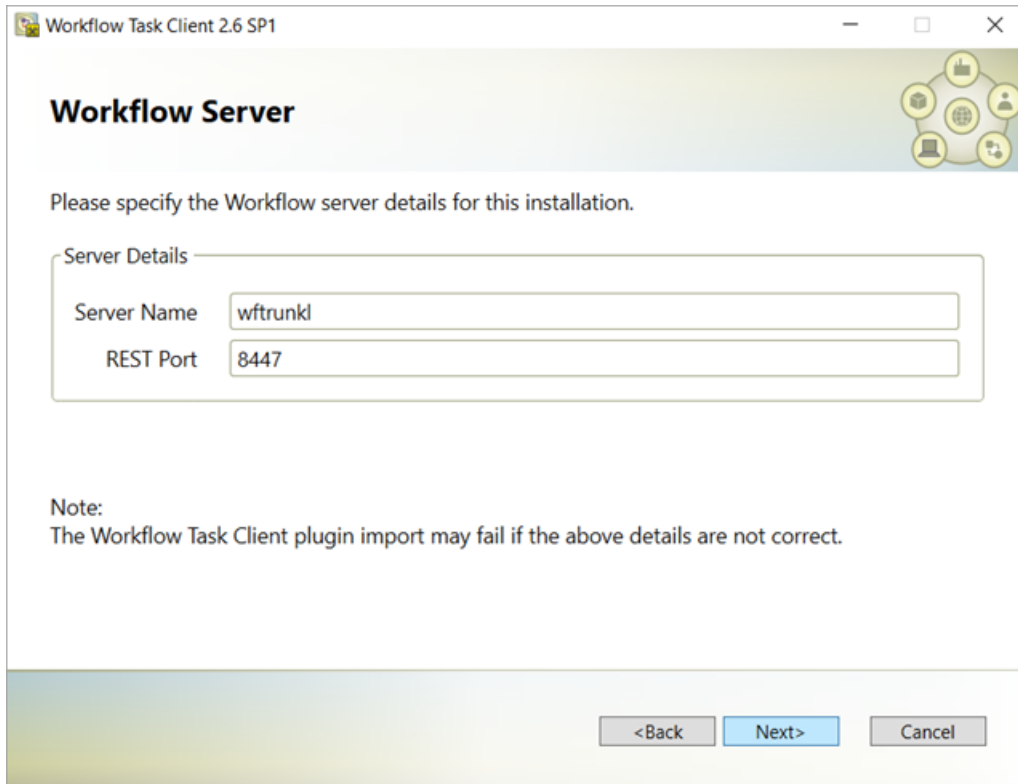
3. Review the license agreement, and then click **I Agree**.



The **Workflow Server** page appears.

4. Enter the details as specified in the following table:



Field	Description
Server Name	Enter the host name or IP address of the Workflow server.
REST Port	Enter the Workflow port number that allows the REST API calls. The task client widget in Operations Hub uses this port to request data from the Workflow application. 8447 is the default Workflow port number.



5. Click **Next**.

The **Operations Hub Server** page appears.

6. Enter the details as specified in the following table:

Field	Description
OpsHub Server Name	Enter the Operations Hub server name (FQDN or host name) as per the configuration of UAA server.  <b>Note:</b> Ensure that the auto populated OpsHub server name is correct.
Port No.	Enter the Operations Hub UAA server port number. 443 is the default UAA port number.
Tenant Username	Enter the username of the administrator who has read-write permissions to access the Operations Hub database. <code>OphubAdmin</code> is the default tenant username.  <b>Note:</b> The tenant username is case-sensitive.
Tenant Password	Enter the password for the administrative user you entered in the <b>Tenant Username</b> box.

Workflow Task Client 2.6 SP1

## Operations Hub Server

Please specify the Operations Hub server details for this installation.

Server Details

OpsHub Server Name: windows2016-01

Port No.: 443

Tenant Username: OphubAdmin

Tenant Password: \*\*\*\*\*



Note:  
Tenant Username is case sensitive. The Workflow Task Client plugin import may fail if the above details are not correct.

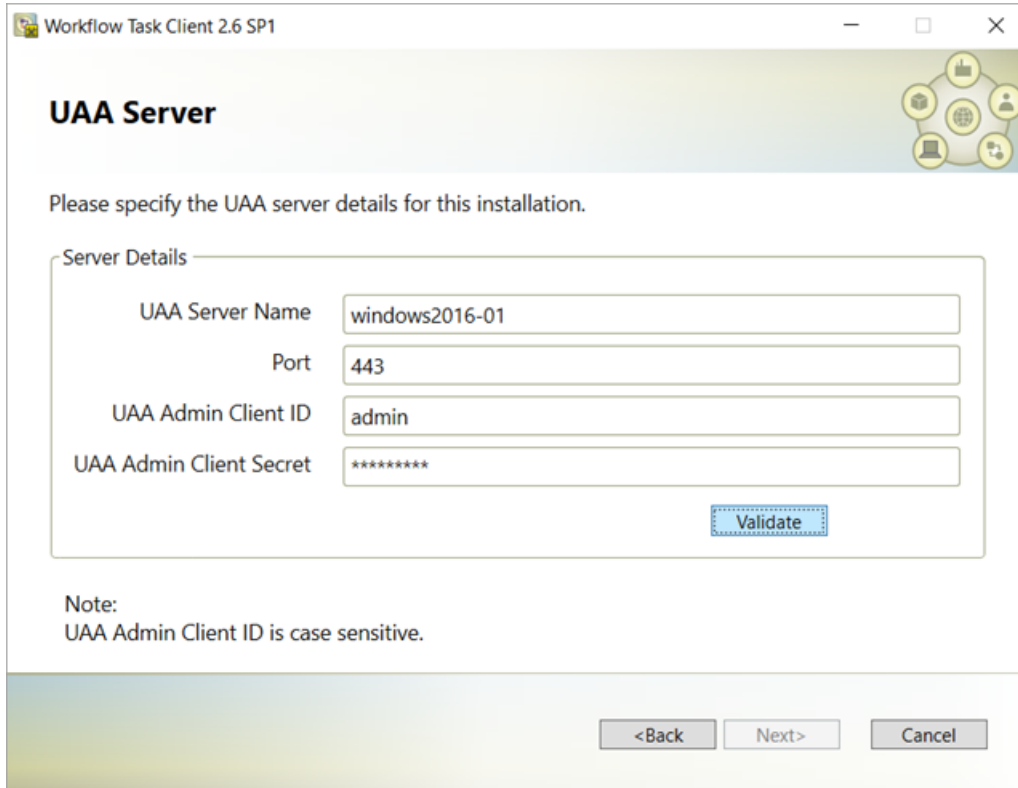
<Back Next> Cancel

7. Click **Next**.

The **UAA Server** page appears.

8. Enter the UAA Server details for authenticating the users to access the Workflow task client as specified in the following table.

Field	Description
UAA Server Name	Enter the Operations Hub UAA server name (FQDN or host name) as per the configuration of UAA server.   <b>Note:</b> Ensure that the auto populated UAA server name is correct.
Port	Enter the Operations Hub UAA server port number.
UAA Admin Client ID	Enter the client ID of the Operations Hub UAA administrator.   <b>Note:</b> The UAA admin client ID is case-sensitive.
UAA Admin Client Secret	Enter the client secret of the Operations Hub UAA administrator.




The screenshot shows a window titled "Workflow Task Client 2.6 SP1" with a sub-header "UAA Server". Below the header, there is a navigation icon set. The main content area contains the instruction "Please specify the UAA server details for this installation." followed by a "Server Details" section. This section has four input fields: "UAA Server Name" with the value "windows2016-01", "Port" with "443", "UAA Admin Client ID" with "admin", and "UAA Admin Client Secret" with "\*\*\*\*\*". A "Validate" button is positioned below the secret field. A "Note:" section states "UAA Admin Client ID is case sensitive." At the bottom of the window, there are three buttons: "<Back", "Next>", and "Cancel".

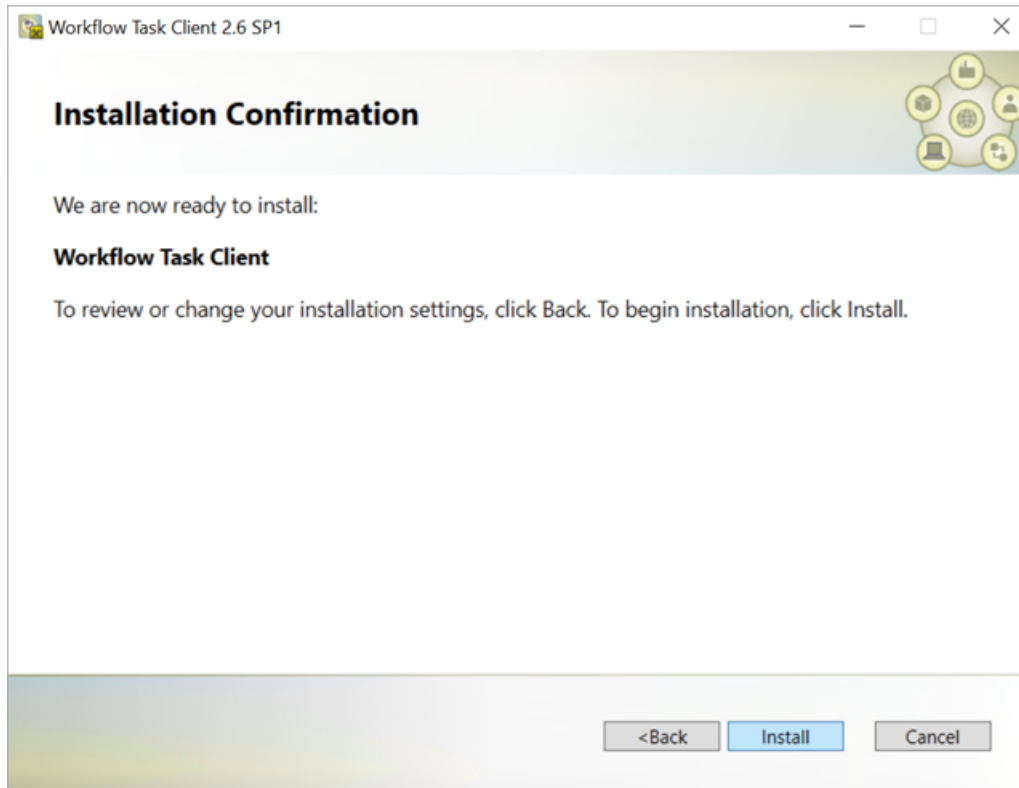
9. Click **Validate** to verify the UAA server credentials.

A message appears to inform whether the user account authentication is successful. If **PASS**, then you can proceed to install workflow task client. If **FAIL**, then you must enter the correct credentials.

10. Click **Next**.

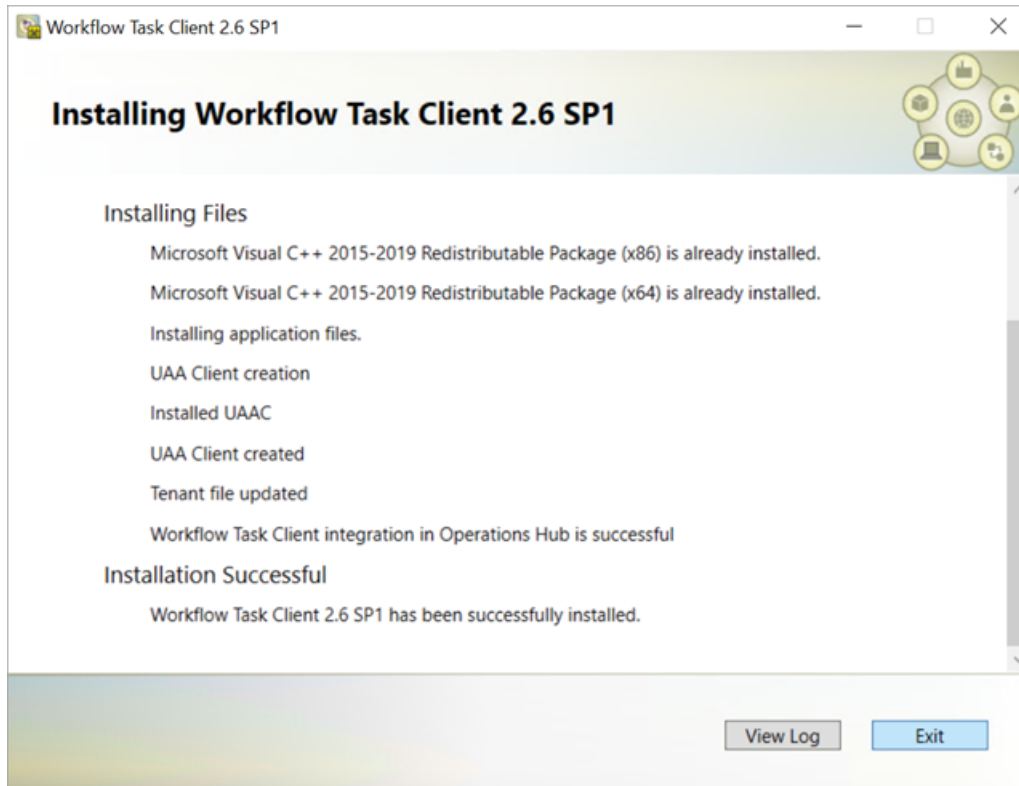
The **Installation Confirmation** page appears.

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



11. Click **Install**.

The Installing Workflow Task Client 2.6 SP1 page appears, updating the status of the installation.



12. When the installation is complete, click **Exit**.  
The task client is added to the Operations Hub application.

The task client is added with the following information in Operations Hub:

- The Workflow Tasklist application is available under **APPS**.
- The entity `WF_User_Credentials` is created under **ENTITIES** to save user logins.
- The queries `DeleteWorkflowUser`, `getWorkflowUser`, and `InsertWorkflowUser` are created under **QUERIES**.
- `TASK LIST` and `TASK COUNT` are added as system widgets in Operations Hub.

[Configure the task client \(page 126\)](#) widget in Operations Hub.

#### Related tasks

[Uninstall the Task Client \(page 133\)](#)

#### Related reference

[Troubleshooting Task Client Issues \(page 133\)](#)

## *Configure the Task Client*

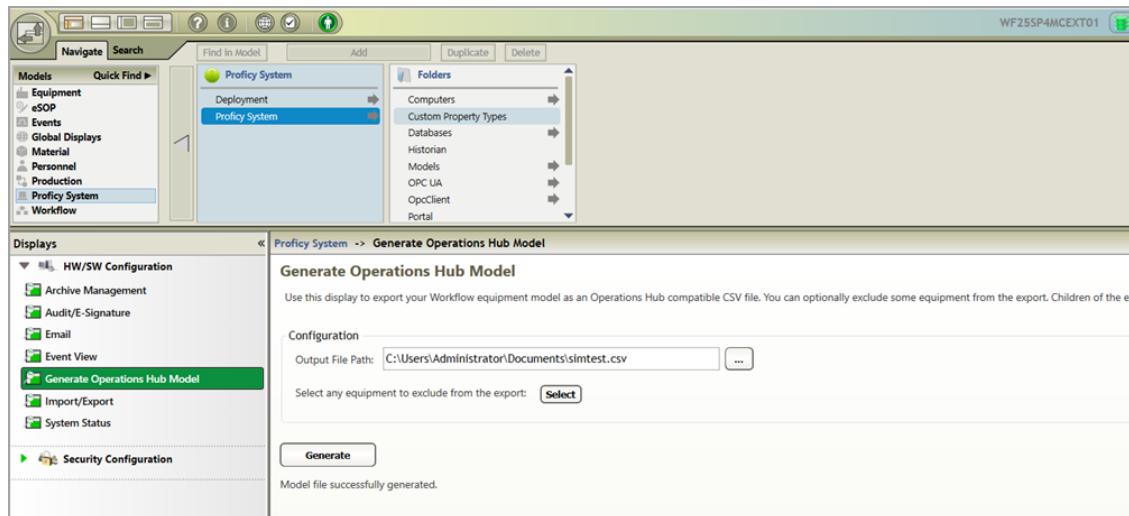
This topic describes how to enable the task client widget to operate in the Operations Hub web server environment.

Install the Workflow and the Operations Hub applications on different servers.

To configure the task client widget, equipment models from the Workflow application are exported to a .csv file, and imported into the Operations Hub application.

1. In the Workflow server, do the following:


- a. Select an equipment model you want to export, and then select **Generate Operations Hub Model**.
- b. Provide a location to save the exported file, and select **Generate**.



The equipment model data is exported to a .csv file format, and saved in the specified location.

2. In the Operations Hub server, do the following:

- a. [Import the .csv file created in step 1 \(page 128\)](#) to Operations Hub.
- b. In the main navigation menu, select **APPS**, and then select Workflow Tasklist application. The Pages workspace appears.
- c. Select **Tasklist View**.  
The pages associated to the task list appear in a container. **TASK LIST**, and **TASK COUNT** are system widgets that cannot be deleted.
- d. Select the **Task List** page in the container.  
The **GETASKLIST PROPERTIES** tab settings appears on the right pane.
- e. Provide **DATA** settings as specified in the table below:

 **Note:** Scroll down in the settings section to find the data settings after the general and display settings.



Parameter	Selection	Description
WorkflowServer	Manual	Enter the URL address of the Workflow server to connect.
RefreshRate	Manual	Enter the time in seconds at which rate the task client will refresh to get the latest data from the Workflow server (for example, 5).
Height	Manual	Enter the preferred height of the task client widget (for example, 600).

f. Select **Save App**.

The application settings are saved.

- Create identical user accounts in Workflow and Operations Hub.
- [Log in to the Operations Hub web client \(page 130\)](#) to connect and work with the task client widget.

### Related tasks

[Generate an Equipment Model for Web HMI \(page \)](#)

[Import Equipment Model \(page 128\)](#)

[Create an User Account in Operations Hub \(page 129\)](#)

[Add Users and Personnel Classes \(page \)](#)



## *Import Equipment Model*

By importing the Workflow equipment models, you can manage the tasks assigned to you from within the Operations Hub application.

Ensure that the Workflow equipment models are exported to a Web HMI model .csv file.

An equipment model is configured in the Workflow application. For more information, refer to the Equipment Model topic in the *Resource Information and Configuration* section of the complete Workflow user guide.

1. Access Operations Hub.
2. In the main navigation menu, select **ADMIN**.
3. In the Admin workspace, select **Import/Export**.  
The **Model Import/Export** page appears.

 **Tip:** Select  to hide the navigation pane that overlaps the page.

4. To import, browse and select the exported .csv file from Workflow, and select **Import**.

The imported information is visible under Objects and Object Types in the Admin workspace.

### Related tasks

[Generate an Equipment Model for Web HMI \(page \)](#)

## Create an User Account in Operations Hub

This topic describes how to create an user account in Operations Hub.

Only a tenant administrator can create and manage developers.

1. In the main navigation menu, select **MANAGE**, and then select **Developers** or **App Users**.
2. Select **Add new user**.  
The **New Account** window appears.
3. Enter values in the available fields as described in the following table.

Field	Description
<b>Username</b>	Enter the user name that the user will use to log in to Operations Hub. The value must be unique.
<b>E-mail</b>	Enter the email ID of the user. The value must be unique.
<b>First Name</b>	Enter the first name of the user.
<b>Last Name</b>	Enter the last name of the user.
<b>Password</b>	Enter a password that the user will use to log in to Operations Hub. The password must meet the following criteria: <ul style="list-style-type: none"> <li>• Must contain between 8 and 15 characters</li> <li>• Must include at least one number</li> <li>• Must include at least one uppercase or lowercase letter</li> </ul>
<b>Repeat Password</b>	Enter the password that you have entered in the Password field.

Field	Description
<b>Only GE Groups</b>	Select this check box if you only want to view groups associated with GE products in the Groups list box.
<b>Groups</b>	Select <code>iqp.user</code> group to assign to this user.
<b>Apps</b>	Select <code>Workflow Tasklist</code> to allow the user to access this application.

4. Select **Create**.

The user is created. If you have created a developer, an application user is also created.

### Access the Task Client

Use the Task Client widget to display task lists from the Workflow application in Operations Hub.

Create identical user accounts for the Operations Hub web server and the Workflow server. You must be able to log in to both the servers using the same username and password combination.

The Workflow Task List is integrated with Operations Hub. You do not have to log in to the Workflow application to manage your tasks. You can log in to the Operations Hub application, and connect to Workflow with the help of the task client widget to manage tasks.

1. Log in to the Operations Hub web client.

The login page to connect to the Workflow server appears.




The image shows a login form with three input fields and a button. The first field is labeled 'Username:' and contains the text 'admin'. The second field is labeled 'Password:' and contains a series of dots. The third field is labeled 'Server Address:' and contains the URL 'https://wftrunkl:8447/'. Below the fields is a blue button labeled 'Log On' with a mouse cursor pointing to it.

2. Enter the details as specified in the following table:


Field	Description
Username	The account username that has permission to access the Workflow application.
Password	The password for the username you entered in the <b>Username</b> box.
Server Address	The URL address to connect to the Workflow server. This URL is populated based on the properties provided for the Task Client widget in Operations Hub.

3. Select **Log On**.

The task count icon indicates the status of your workflow connection.



Status	Description
	<p>Indicates that the Workflow server is disconnected due to either of these reasons:</p> <ul style="list-style-type: none"> <li>• You are not logged in to the server.</li> <li>• Internet connection is lost.</li> <li>• Workflow server is down.</li> </ul> <p> <b>Note:</b> All tasks in Operations Hub remain disabled until a connection is established.</p>
	<p>Indicates that the Workflow server is connected.</p> <p>Once connected, the task count shows the number of workflow tasks. If the count is 0, it means there are no workflows.</p>


The user login credentials are encrypted and stored under **ENTITIES** in Operations Hub. You will not be prompted for login details again for the saved user accounts.


 **Note:** Whenever the Workflow server is down, or if there is no internet, the lost connection status is indicated in red. All tasks in Operations Hub remain disabled until a connection is established.

4. Select  to show the workflow equipment context navigation.


For more information, refer to the Equipment Context topic in the *Operator Task List in the Workflow Client* section of the complete Workflow user guide.









5. Select  or  to navigate and select any of these equipment contexts: Big Enterprise, Big Unit, or Big Area.

The equipment context set up shown in Operations Hub is created in the Workflow application. The list of tasks for the selected equipment context appears. Based on the list of tasks, the task count number  also gets updated.

 **Note:** Logged in users in Operations Hub can view only the tasks that are assigned to them in the Workflow application.

6. Use these options to work with the tasks:

Icon	Description
	<p>Select to filter tasks or task steps by task name, priority, personnel assignment, step state, and expiry values. For more information, refer to the Task List Filtering topic in the <i>Operator Task List in the Workflow Client</i> section of the complete Workflow user guide.</p>

Icon	Description
	Select the <b>Tasks for Equipment</b> toggle to show or hide the tasks associated to the equipment location only.
	Select to start and run scheduled tasks. For more information, refer to the Start Task topic in the <i>Operator Task List in the Workflow Client</i> section of the complete Workflow user guide.
	Select to manually start a specific task step.
	Select to view and save a copy of the linked documents. For more information, refer to the Document(s) topic in the <i>Operator Task List in the Proficiency Client</i> section of the complete Workflow user guide.
	Select to view the instructions to complete a task or task step. This option is available only when there are work instructions defined for the task or task steps.
	<p>Select to access the following menus, and perform task related actions:</p> <ul style="list-style-type: none"> <li>• <b>Set Priority:</b> You can set a priority number for the task to run.</li> <li>• <b>Jump to Task Step:</b> You can skip some steps and jump to a specific task step in a scheduled flow.</li> <li>• <b>Enter Expiry Comment:</b> You can enter a reason for the task delay. The option to add a comment is available only after the task or task step has expired.</li> <li>• <b>Cancel Task:</b> You can cancel running a specific task or task step.</li> <li>• <b>Reassign Personnel:</b> You can reassign specific task steps to a different person or equipment location.</li> <li>• <b>Acquire:</b> You can acquire a specific task step if it is available.</li> <li>• <b>Release:</b> You can only release those steps that you have acquired. When you release a task step, it is available for other operators to acquire.</li> </ul> <p>For more information, refer to the complete Workflow user guide.</p>
	Select to access the forms attached to a task step, and update them. For more information, refer to the <i>Forms and User Displays Authoring Guide</i> section of the complete Workflow user guide.
	<p><b>Note:</b> You can load only HTML forms in the Operations Hub Task Client. Windows presentation framework (WPF), Silverlight, and .NET rich client forms are not supported.</p>

**Note:** For added security, electronic signatures are configured in Workflow for specific tasks, task steps, or forms. In such cases, a dialog box appears requesting you to sign in for verification before accomplishing any task related action.

### Related tasks

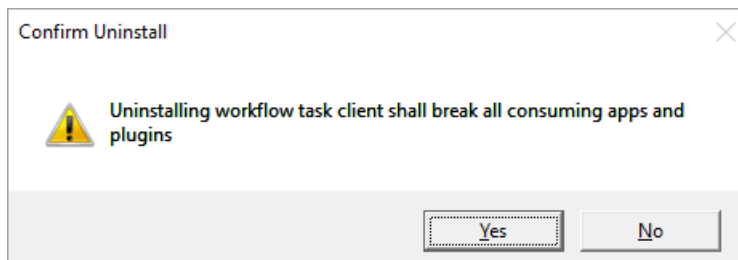
[Create an User Account in Operations Hub \(page 129\)](#)

[Add Users and Personnel Classes \(page \)](#)

## Uninstall the Task Client

This topic describes the steps to uninstall the task client plugin.

1. From the **Control Panel**, go to **Programs and Features**.  
The **Uninstall or change a program** dialog box appears, displaying all the programs installed on the computer.
2. Select **Workflow Task Client**, and then **Uninstall**.
3. In the confirmation message box, click **Yes**.  
The uninstallation process verifies once again to confirm the task client removal as it may lead to breaking any applications associated to it.
4. Click **Yes** to proceed with uninstallation.



A message appears when the uninstallation is complete.

5. Click **OK** to close the message dialog box.  
Uninstalling the task client removes the plugin information from Operations Hub **APPS**, **ENTITIES**, and **QUERIES**.

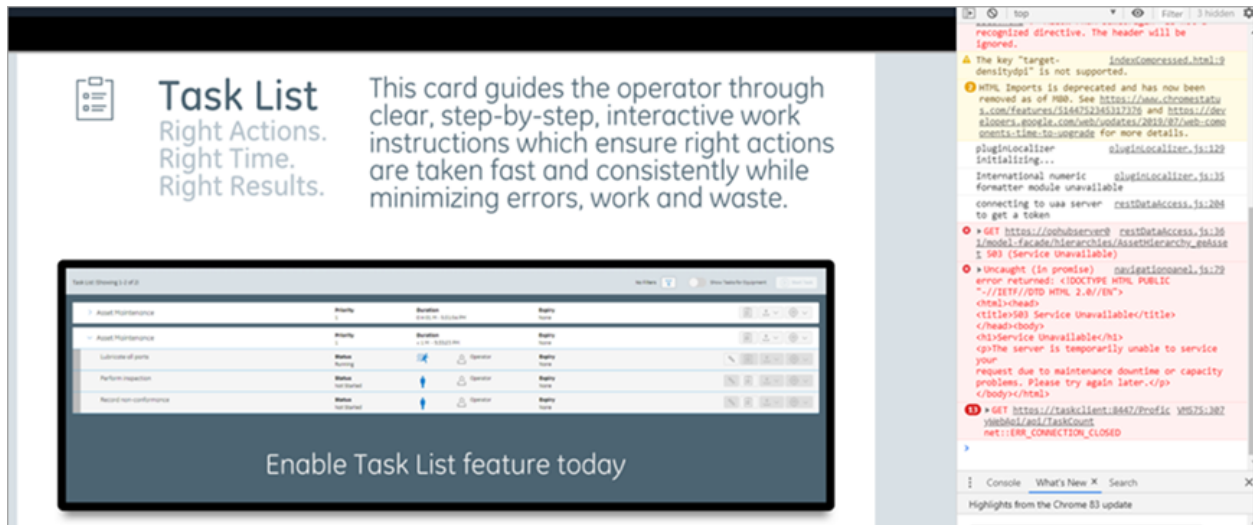
Task Client is uninstalled.

## Troubleshooting Task Client Issues

This topic describes how to troubleshoot issues that you encounter when working with task client in Operations Hub.

## Connection Errors

If this screen appears, either the internet connection is lost, or the Workflow server cannot be reached. On inspection, the `ERR_CONNECTION_CLOSED` implies that the connection to the Workflow is not established.



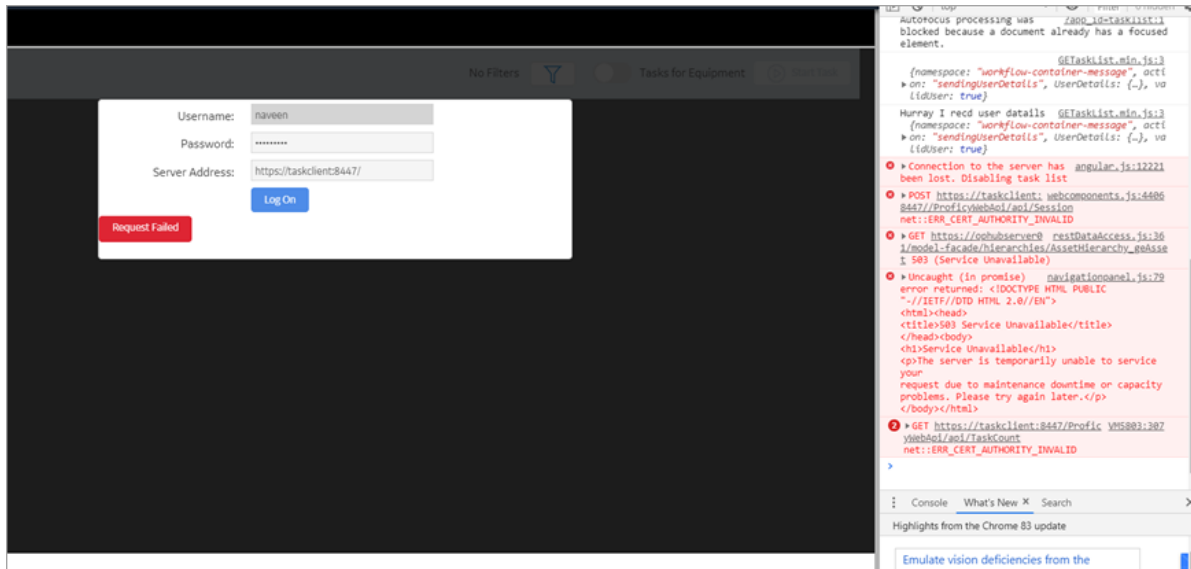
To troubleshoot the Workflow server connection errors, check for the following:

- Add the IP address of the Workflow server to your Windows hosts file: `c:\Windows\System32\Drivers\etc\hosts`.
- Ensure the Workflow server URL entered under **GETASKLIST PROPERTIES** in the Operations Hub administrative environment includes a trailing forward slash. For example, `https://taskclient:8447/`
- Verify the Workflow server URL saved for user login credentials under **ENTITIES** in Operations Hub also includes the trailing forward slash.

## Security Certificate Errors

If using certificates that are signed by a Trusted Certificate Authority, you may not encounter this error. If this screen appears, it is possible that you have a self-signed SSL Certificate. To troubleshoot the certificate issue, perform the following steps:

- In the browser inspect element, right-click the `ERR_CERT_AUTHORITY_INVALID` error link, and then click **Open in new tab**.



- In the new tab, click **Advanced**.
- Click the **Proceed to task client (unsafe)** link.
- Return to the task client application tab, and refresh the browser.

## References to WebHMI

If using an older version of Workflow, you may come across these WebHMI references when you access the task client plugin properties. The references appear only when you add new instances of the task client plugin to application pages in Operations Hub.

- WebHMIUrl
- WebHMIUsername
- WebHMIPassword

To resolve the WebHMI references issue, upgrade to the Workflow 2.6 SP1 SIM 4 version.

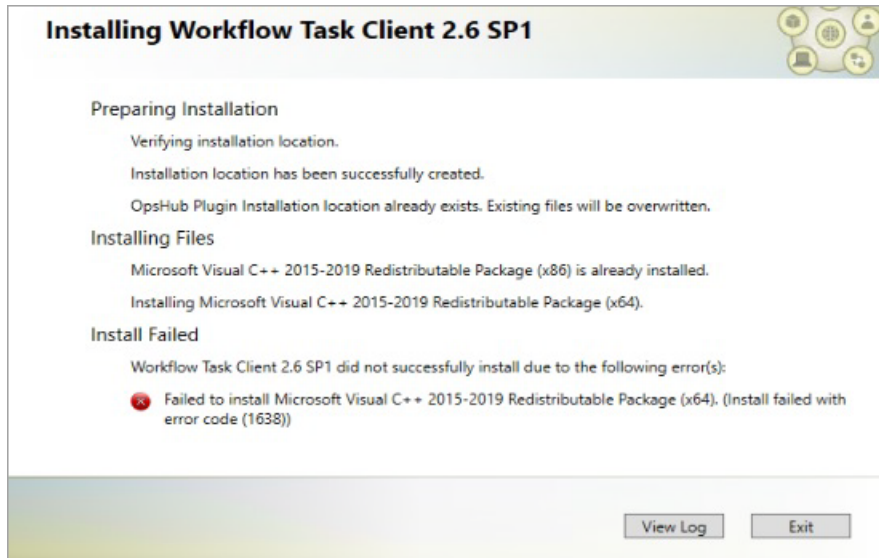
## Server Communication Error

If you are on Operations Hub 1.7 and directly apply task client 2.6 SP1 SIM 2 version, it leads to an error in communicating with the server. Operations Hub 1.7 communicates using `app_id`, whereas the task client looks for `app_name` to communicate with the server. This issue does not occur if you are on Operations Hub 2.0, which also communicates via `app_name` in its URLs.

To resolve the communication issue with Operations Hub 1.7, upgrade to the Workflow 2.6 SP1 SIM 4 version.

## Operations Hub Interoperability





As a workaround to address VC++ (x64) failure, follow these steps to install Task Client on Operations Hub 2.1.

1. Uninstall the VC++ 2015-2019 Redistributable (x64) version installed with Operations Hub 2.1.
2. Open the Workflow install media, navigate to the `\\Installers\Resources\Microsoft\2015_2019` folder, and run the `vc_redist.x64.exe`.
3. Open the Services console dialog and restart these services:
  - GE Operations IQP PostgreSQL Database
  - GE Operations UAA PostgreSQL Database
4. [Install the Task Client \(page 119\)](#).
5. Install the VC++ 2015-2019 Redistributable (x64) version that got installed with Operations Hub 2.1.

## *Installation Security*

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

More information on security, including GE security advisories and security patch notifications, can be found online.

Please visit our website at [https://digitalsupport.ge.com/en\\_US/Alert/GE-Security-Advisories](https://digitalsupport.ge.com/en_US/Alert/GE-Security-Advisories).

## *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 encourages customers to use third-party anti-virus (AV) software of their choice and to keep it current with the latest updates.

While GE 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 Workflow product defect discovered while running any AV software, GE 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 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 Workflow product defect discovered while running DEP, GE will make all reasonable efforts to provide a solution.

## *Software Patching*

Installing software patches is an integral part of security.

## Patching GE Software

GE recommends that customers keep their software up-to-date by applying the latest Software Improvement Module (SIM) to their deployed GE products. SIMs add new functionality, fix bugs, and address security vulnerabilities. Security advisories and security-related SIMs can be found on the GE website at [https://digitalsupport.ge.com/en\\_US/Alert/GE-Security-Advisories](https://digitalsupport.ge.com/en_US/Alert/GE-Security-Advisories). Customers can also sign up for notification of new SIMs and security advisories on the website.

## Patching Third-Party Software

GE also recommends that customers keep operating systems, databases, and other third-party software in their environment up-to-date with the latest security patches from the software vendor. GE regularly validates the compatibility of selected GE products with third-party operating system security patches. More information on this process can be found on the GE Support website at [https://digitalsupport.ge.com/en\\_US/Alert/GE-Security-Advisories](https://digitalsupport.ge.com/en_US/Alert/GE-Security-Advisories).

## *Platform Configuration and Hardening*

GE 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.org>.
- *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:	<a href="https://digitalsupport.ge.com">https://digitalsupport.ge.com</a>
Comments about our manuals and online Help:	<a href="mailto:doc@ge.com">doc@ge.com</a>
Additional information:	<a href="https://www.ge.com/digital/products">https://www.ge.com/digital/products</a>

## 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 <https://digitalsupport.ge.com>.

### Americas

Online Technical Support:	<a href="https://digitalsupport.ge.com">https://digitalsupport.ge.com</a>
Telephone:	1-800-433-2682 1-617-725-2696 (if toll free 800 option is unavailable)
Technical Support e-mail:	<a href="mailto:digitalsupport@ge.com">digitalsupport@ge.com</a>
Order Services (formerly Customer Care) e-mail:	<a href="mailto:GEDClientServices@ge.com">GEDClientServices@ge.com</a>
Sales Support (formerly Inside Sales) e-mail:	<a href="mailto:GEDigitalSalesSupport@ge.com">GEDigitalSalesSupport@ge.com</a>
Primary language of support:	English

### Europe, Middle East, and Africa

Online Technical Support:	<a href="https://digitalsupport.ge.com">https://digitalsupport.ge.com</a>
Telephone:	+800 1-433-2682 +420-296-183-331 (if toll free 800 option is unavailable or dialing from a mobile telephone)
Technical Support e-mail:	<a href="mailto:digitalsupport.emea@ge.com">digitalsupport.emea@ge.com</a>
Order Services (formerly Customer Care) e-mail:	<a href="mailto:GEDClientServices@ge.com">GEDClientServices@ge.com</a>
Sales Support (formerly Inside Sales) e-mail:	<a href="mailto:GEDigitalSalesSupport@ge.com">GEDigitalSalesSupport@ge.com</a>
Primary language(s) of support:	English, French, German, Italian, Czech, Spanish

### Asia Pacific

Online Technical Support & GlobalCare:	<a href="https://digitalsupport.ge.com">https://digitalsupport.ge.com</a>
Telephone:	+86-400-842-4213 +65-3157-4914 (India, Indonesia and Pakistan)
Technical Support e-mail:	<a href="mailto:digitalsupport.apac@ge.com">digitalsupport.apac@ge.com</a>
Order Services (formerly Customer Care) e-mail:	<a href="mailto:GEDClientServices@ge.com">GEDClientServices@ge.com</a>
Sales Support (formerly Inside Sales) e-mail:	<a href="mailto:GEDigitalSalesSupport@ge.com">GEDigitalSalesSupport@ge.com</a>
Primary language(s) of support:	Chinese, English

# Index

## A

- About
  - task controls in Proficy HMIs
    - 116
- Active Directory Lightweight Directory Service
  - modify
    - 80
- Active Directory, see ADAM
  - post-installation changes
    - 80
- ActiveX Task List
  - install
    - 117
  - task list
    - 118
- AD LDS
  - configure
    - 80
- Add
  - counters, performance
    - 29,86
  - performance counters
    - 29,86
- Apache
  - configure
    - 65
  - rules
    - 66
- Application server
  - configure security certificates
    - 76
- Architecture mode
  - change
    - 85
  - options
    - 10
- Authentication, see Login
  - 70,70
- Automatic login
  - 71

## B

- Backup SQL Server
  - 22

## C

- Certificates
  - configure click once
    - 46
  - configure reverse proxy
    - 62
  - export
    - 41
  - options
    - 15
  - reverse proxy
    - 67
  - security
    - 14
  - self-signed, web server
    - 20
  - Web Task List
    - 67
- Change
  - architecture mode
    - 85
- Client
  - configuration
    - 87
  - install
    - 35
  - server configuration
    - 80
- Cluster configuration
  - 80
- Clustering
  - 24
    - configure
      - failover manager
        - 55
      - local client with cluster node, 32-bit server
        - 59

- local client with cluster node, 64-bit server
    - 60
    - quorum options
      - 57
  - failover manager
    - 54
  - install
    - failover manager
      - 54
  - one cluster, two nodes
    - 51
  - one-click deployment configuration
    - 60
  - supported and validated configurations
    - 50
  - three clusters, two nodes
    - 53
  - tips
    - 60
  - two clusters, two nodes
    - 52
- Compatibility
  - upgrading
    - 9
  - Workflow products
    - 9
- Configuration
  - ActiveX task list
    - 118
  - client
    - 87
  - component services
    - reporting database
      - 101
  - date and time
    - 8
  - Failover Cluster Manager
    - 55
      - configure quorum options
        - 57
  - local client with cluster node, 32-bit server
    - 59
  - local client with cluster node, 64-bit server
    - 60
  - regional language
    - 8
- regional settings
  - 8
- Remote Desktop Session Host
  - remote desktop connection
    - 113
  - Windows Server 2008 R2
    - 111
- server
  - 87
- server limit overrides
  - 90
- supported failover clustering
  - 50
- Terminal Server
  - remote desktop connection
    - 113
  - Windows Server 2008 R2
    - 111
- validated failover clustering
  - 50
- Configuration tool
  - 116
- Configure
  - failover cluster
    - 80
  - server for remote client
    - 80
  - server instance
    - 83
  - SQL Server 2012
    - 25
  - SQL server for application server
    - 81
- Contacts
  - regional
    - 138
  - technical support
    - 138
- Counters
  - DTL
    - 26
  - events
    - 27
- Counters, performance
  - 26

- add
    - 29,86
  - delete
    - 29,86
  - log
    - 29
  - view
    - 30
- D**
- Database
    - modify
      - 81
  - Daylight saving time
    - 9
  - Delete
    - counters, performance
      - 29,86
    - performance counters
      - 29,86
  - Deploy
    - one-click
      - 44
  - Disk witness
    - configure
      - 57
  - Display
    - host server name
      - Proficy client
        - 86
      - host server name in Proficy client
        - one-click client
          - 47
  - DTL
    - counters
      - 26
- E**
- Enable
    - Remote Desktop Services
      - Windows Server 2008 R2
        - 110
    - Terminal Services
      - Windows Server 2008 R2
        - 110
  - Events
    - counters
      - 27
- Export**
- security certificates
    - 41
- F**
- Failover Cluster Manager
    - 54
  - Failover clustering
    - 24
      - configure
        - 55
          - quorum options
            - 57
      - install
        - 54
      - manager
        - 54
      - one cluster, two nodes
        - 51
      - one-click deployment configuration
        - 60
      - supported and validated configurations
        - 50
      - three clusters, two nodes
        - 53
      - tips
        - 60
      - two clusters, two nodes
        - 52
  - Failover server
    - clustering
      - 58
  - File share witness
    - configure
      - 57
  - Firewall settings
    - 21
  - Frequently Asked Questions
    - Remote Desktop Session Host
      - 115
    - Terminal Server
      - 115
- G**
- GE Single Sign On (SSO)
    - 72
  - Getting started
    - Remote Desktop Session Host

107  
Terminal Server  
107

## H

Hardware  
requirements  
Remote Desktop Session Host  
108  
Terminal Server  
108  
HMI, see Task controls  
116  
Host server name  
display in Proficy client  
86  
one-click client  
47

## I

IIS reverse proxy  
web task list  
63  
Inbound rules  
apache  
66  
Installation  
ActiveX task controls  
117  
architecture considerations  
10  
client only  
35  
counters, performance  
26  
Failover Cluster Manager  
54  
multiple servers  
41  
one-click deployment  
44  
performance counters  
26  
Remote Desktop Session Host  
Windows Server 2008 R2  
111  
reporting database  
99

server  
command line  
48  
silent  
48  
server and client  
30  
Terminal Server  
Windows Server 2008 R2  
111  
Windows 2012 R2  
prerequisites  
11,40  
Workflow  
Remote Desktop Session Host  
112  
Terminal Server  
112

## K

Key concepts  
Workflow  
6  
Keyboard buttons  
special  
9

## L

License Management  
26  
Licenses  
External Connector  
Remote Desktop Session Host  
109  
Terminal Server  
109  
hardware key  
Remote Desktop Session Host  
109  
Terminal Server  
109  
requirements  
Remote Desktop Session Host  
109  
Terminal Server  
109  
Limit  
overrides



- server
  - 90
- Limitations
  - Remote Desktop Session Host
    - 108
  - Terminal Server
    - 108
- Log
  - counters, performance
    - 29
  - performance counters
    - 29
- Log files
  - 9
- Login
  - 70, 70,73
    - automatically
      - 71
- M**
  - Microsoft SQL Server
    - backup and restore
      - 22
    - maintenance plan
      - 22
  - Modify
    - Active Directory Lightweight Directory Service
      - 80
    - ActiveX task list
      - 118
    - AD LDS
      - 80
    - database, application server
      - 81
    - security certificates
      - 76
  - Multiple servers
    - configure after installation
      - 37
    - deploy product options
      - 22
    - install
      - 41
    - revert to single servers
      - 39
- N**
- Nodes
  - configure local client, 32-bit server
    - 59
  - configure local client, 64-bit server
    - 60
- O**
  - One-click
    - certificates
      - 46
  - One-click client
    - display host server name
      - 47
  - One-click deployment
    - 44
      - server cluster environment
        - 60
  - Open Enterprise
    - regional settings
      - 8
  - Outbound rules
    - apache
      - 66
  - Override
    - server limits
      - 90
- P**
  - Performance counters
    - 26
      - add
        - 29,86
      - delete
        - 29,86
      - log
        - 29
      - view
        - 30
  - Permissions
    - folder
      - 75
  - Ports
    - 21
  - Post-installation
    - 75
      - Active Directory services
        - 80
      - configure SQL Server 2012

- 25
- modify SQL server configuration
  - 81
- monitor system configuration and status
  - 79
- multiple servers on single machine
  - 37
- multiple servers to single servers
  - 39
- product options
  - 84
- security certificate configuration
  - 76
- server configuration
  - 77
    - remote client
      - 80
  - server instance configuration
    - 83
  - system health determinants
    - 6

- Post-installation configuration
- ActiveX Task List
  - 116
- Primary server
- clustering
  - 57
- Product options
- install
  - 84
- moving between servers
  - 77
- uninstall
  - 84
- Proficy Authentication, see Login
- 70,70
- Proficy client
- display host server name
  - 86
    - one-click client
      - 47
- Proficy Workflow
- uninstall
  - 50
- Proxy
- local system

- 76
- Q**
  - Quorum options
    - configure
      - 57
- R**
  - Regional settings
    - web applications
      - 8
  - Workflow client
    - 8
  - Remote Desktop Services
    - enable on Windows Server 2008 R2
      - 110
    - environment
      - 107
    - features
      - 106
  - Remote Desktop Session Host
    - 106
      - configuration
        - 111
      - configure remote desktop connection
        - 113
      - External Connector licensing
        - 109
      - frequently asked questions
        - 115
      - getting started
        - 107
      - hardware requirements
        - 108
      - install Workflow
        - 112
      - installation
        - 111
      - licensing requirements
        - 109
      - limitations
        - 108
      - log on from Windows 7
        - 111
      - prerequisites
        - 111
      - software requirements
        - 108

- specify starting program at login
  - 112
- troubleshoot
  - 114
    - known problems
      - 115
    - specific problems
      - 114
- Replicated database
  - reporting
    - 103
- Reporting
  - upgrade replicated database
    - 103
- Reporting database
  - configure component services
    - 101
  - install
    - 99
  - uninstall
    - 102
- Requirements
  - hardware
    - Remote Desktop Session Host
      - 108
    - Terminal Server
      - 108
  - hardware key licensing
    - Remote Desktop Session Host
      - 109
    - Terminal Server
      - 109
  - licensing
    - Remote Desktop Session Host
      - 109
    - Terminal Server
      - 109
  - software
    - Remote Desktop Session Host
      - 108
    - Terminal Server
      - 108
- Restore SQL Server
  - 22
- Reverse proxy
  - certificates

- 62,67
- IIS
  - 63
- URLs
  - 67
- Run
  - Proficy client
    - standard Windows user account
      - 75

## S

- Security
  - certificate options
    - 15
  - certificates
    - 14
  - click-once certificates
    - 46
  - configure server certificates
    - 76
  - reverse proxy certificates
    - 62
- Server
  - configuration
    - 87
  - extension
    - 41
  - install
    - 30
  - multiple
    - 41
  - installation
    - command line
      - 48
    - silent
      - 48
- Server cluster configuration
  - 80
- Server clustering
  - 24
    - failover server
      - 58
    - one cluster, two nodes
      - 51
    - one-click deployment configuration
      - 60
    - primary server

- 57
- supported and validated configurations
  - 50
  - three clusters, two nodes
    - 53
  - tips
    - 60
  - two clusters, two nodes
    - 52
- Server configuration
  - assign product options
    - 77
- Server instance
  - affects of configuration on program use
    - 6
  - configure
    - 83
  - monitor configuration and status
    - 79
- Server status
  - changing
    - 77
- Service providers
  - install
    - 84
  - uninstall
    - 84
- Services
  - 13
- Single Sign On (SSO)
  - GE
    - 72
- Software
  - requirements
    - Remote Desktop Session Host
      - 108
    - Terminal Server
      - 108
- SQL Server
  - configure 2012
    - 25
  - modify
    - 81
- SQL Server, see Microsoft SQL Server
  - 22
- SSO

- GE
  - 72
- SSO Authentication, see Login
  - 70,70
- Startup program
  - configure
    - Remote Desktop Session Host
      - 112
    - Terminal Server
      - 112
- Support, technical
  - 138
- System
  - monitor configuration and status
    - 79
- System health
  - affects on program use
    - 6
  - determinants of
    - 6

**T**

- task client
  - troubleshoot
    - 133
- Task controls
  - 116
    - install
      - 117
    - modify
      - 118
    - post-install configuration
      - 116
- Technical support
  - 138
- Terminal Server
  - 106
    - configuration
      - 111
    - configure remote desktop connection
      - 113
    - External Connector licensing
      - 109
    - frequently asked questions
      - 115
    - getting started
      - 107

- hardware requirements
  - 108
- install Workflow
  - 112
- installation
  - 111
- licensing requirements
  - 109
- limitations
  - 108
- log on from Windows 7
  - 111
- prerequisites
  - 111
- software requirements
  - 108
- specify starting program at login
  - 112
- troubleshoot
  - 114
    - known problems
      - 115
    - specific problems
      - 114
- Terminal Services
  - enable on Windows Server 2008 R2
    - 110
  - environment
    - 107
  - features
    - 106
- Time zones
  - daylight saving time
    - 9
  - UTC
    - 9
- Troubleshoot
  - task client
    - 133
- Troubleshooting
  - Remote Desktop Session Host
    - 114
      - known problems
        - 115
      - specific problems
        - 114
  - Terminal Server
    - 114
      - known problems
        - 115
      - specific problems
        - 114
  - U**
    - Uninstall
      - Proficiency Workflow
        - 50
      - reporting database
        - 102
    - Upgrade
      - compatibility with Workflow products
        - 9
      - replicated database, reporting
        - 103
    - Upgrade paths
      - 95
    - User account
      - standard Windows
        - 75
    - UTC
      - 9
  - V**
    - View
      - counters, performance
        - 30
      - performance counters
        - 30
  - W**
    - Web server
      - certificates, self-signed
        - 20
    - Web Task List
      - certificates
        - 67
      - connect
        - 67
      - IIS reverse proxy
        - 63
      - URLs
        - 67
    - Windows
      - 2012 R2

- prerequisites for installation
  - 11,40
- 7
  - log on to Remote Desktop Session Host
    - 111
  - log on to Terminal Server
    - 111
- authentication, see Login
  - 70,70
- standard user accounts
  - 75
- Windows services
  - 13
- Workflow
  - install
    - Remote Desktop Session Host
      - 112
    - Terminal Server
      - 112
  - key concepts
    - 6
  - regional settings
    - 8
  - upgrade paths
    - 95