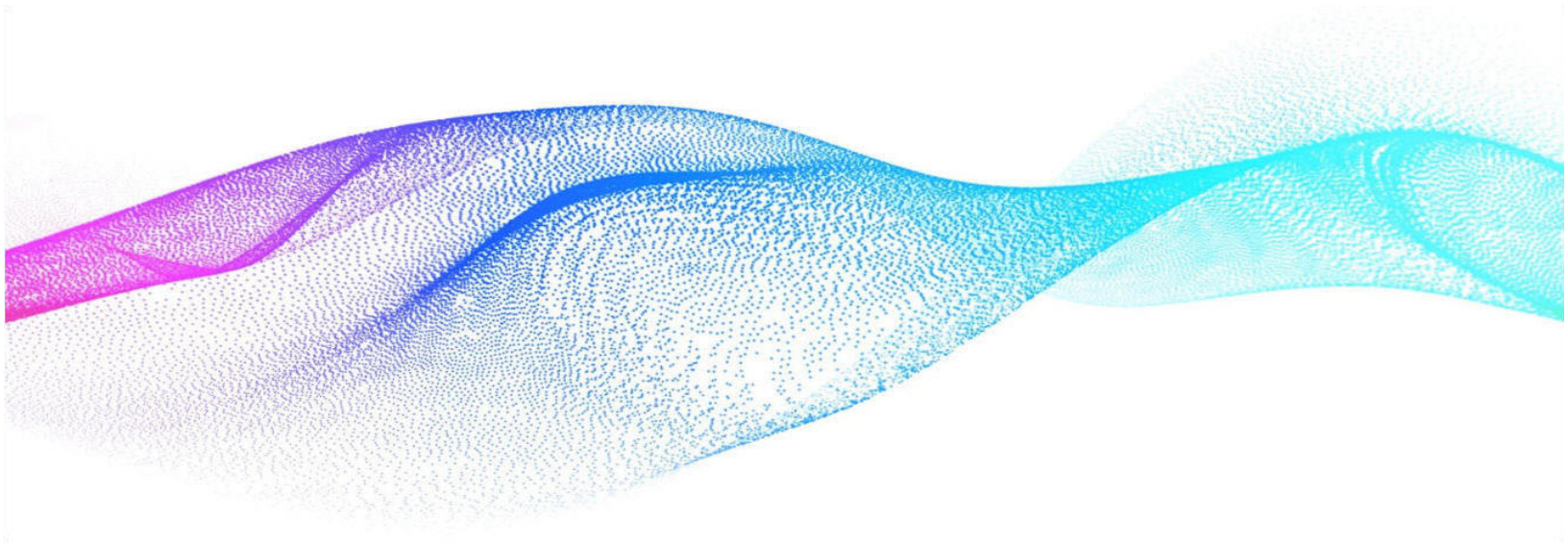
WORKSOFT®
Trust in Automation



Worksoft Certify Installation Guide

Worksoft Certify Installation Guide

Version 14.1

© Copyright 2025 by Worksoft, Inc. All rights reserved.

Worksoft is a business name of Worksoft, Inc. Information in this document is subject to change and revision without notice. The software described herein may only be used and copied as outlined in the Software License Agreement. No part of this manual may be reproduced by any means, electronic or mechanical, for any purpose other than the purchaser's personal use, without prior written permission from Worksoft.

Worksoft provides this documentation "as is" without warranty of any kind, either express or implied. Worksoft may revise information in this document without notice and does not represent a commitment on the part of Worksoft, Inc.

Worksoft, Inc. may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents except as expressly provided in any written license agreement from Worksoft, Inc.

Patent

Worksoft Certify®

U.S. Patent No. 7,600,220

Trademarks

Worksoft Certify® is a registered trademark of Worksoft, Inc.

All other trademarks and trade names mentioned in this guide are the property of their respective owners.

Third-Party Copyrights

This product includes software developed and copyrighted by the following persons or companies:

Data Dynamics, Ltd., ActiveReports

Microsoft® Enterprise Library

Infragistics® NetAdvantage®

Apache Logging Services log4net

Antlr ANTLR

The above copyright holders disclaim all responsibility or liability with respect to its usage or its effect upon hardware or computer systems.

PN WCIG 141 01152025

Table of Contents

Chapter 1 Before You Install Worksoft Certify

In This Chapter

Overview

Before installing and configuring Worksoft Certify, complete the following tasks:

- Verify that your application server has the needed system requirements installed. For more information, see the Worksoft Help Portal.
- Set up a database server and create a Certify database. For more information, see"Creating a Certify Database" on page 8.
- Configure your application server. For more information, see Chapter 2, "Preparing Your Application Server," on page 12.
- Install and configure Worksoft Portal and all infrastructure services on the application server. For more information, see the Worksoft Help Portal.

Worksoft Certify Enterprise Package

The Worksoft Certify Enterprise package consists of the following components:

Component	Description
Worksoft Certify Site Prep.zip	This zip file contains the following items: • CertifyConfigTool folder - Contains the Certify configuration tool. • Database Scripts folder- Contains the utility and scripts that you will use to create and update your Certify database. • *Certify Enterprise Installation Guide* link
CertifySetup.exe	Worksoft Certify client installer allows you to select which interfaces to install.
Certify Services directory	Contains the **CertifyServices.exe** executable that installs the following services on your application server: • AutoUpdates - Installs the Worksoft Certify Auto Update tool. Administrators can upgrade all Certify clients with this tool. • Certify Web API - Works on a service layer that accelerates processes for remote users. • Certify Results API - Worksoft Certify Results API allows you to view Certify results and generate reports without having Worksoft Certify installed.
Documents	Contains the *Worksoft Certify Installation Guide* link.

Preparing the Database

When configuring your database server, you must estimate how large your databases will become by figuring out usage. To help you determine your hardware requirements, Worksoft has provided the three following types of usage models:

Usage Model	Number of Users	Usage
Light	Up to 10 users	Generate a small number of processes with a low volume of test results weekly.
Medium	10 to 20 users	Generate a higher number of processes with a moderate and increasing volume of test results daily.
High	10 to 20 users (or more)	Generate a very high number of processes with a high and increasing volume of test results daily.

Light Usage Model

This usage model is the typical starting point for most Worksoft customers. If you are starting with more than 10 users, your usage may quickly outgrow the Light Usage model. In that case, follow the Medium Usage model recommendations.

The requirements for the Light Usage model are based on the following assumptions:

- Nightly execution has not been established yet because the test automation is still being built.
- Results maintenance is implemented with Certify SQL maintenance jobs once regular process execution has begun.
- Screenshots are only taken on a failed process step or a specific step.

Medium Usage Model

The primary reason for choosing this model is the number of processes and executions you expect to be running on a daily basis.

The requirements for the Medium Usage model are based on the following assumptions:

- Certify process execution is done daily across 50 virtual machines, and 700 transactional Certify processes are executed continuously for 8 hours.
- Results maintenance is implemented with a Certify SQL maintenance job to archive and delete results.
- Screenshots are only taken on a failed process step or a specific step.

High Usage Model

You should implement the High Usage model if you have 10 or more concurrent users creating test processes with Certify and executing a large number of processes nightly to account for future growth.

The requirements for the High Usage model are based on the following assumptions:

- Certify process execution is done daily across 120+ virtual machines, and 1,500 top-level Certify processes are executed continuously for 8 hours.
- Results maintenance is implemented with a Certify SQL maintenance job to archive and delete results.
- Screenshots are only taken on a failed process step or a specific step.

Creating a Certify Database

Before creating the Certify database, Microsoft SQL Server should be installed on the database server. Read the system requirements in the Worksoft Help Portal to verify that you have a supported version of SQL Server. Download the software from Microsoft's website.

Use the Certify Configuration tool to specify the type of database you are using with Certify and how to connect to that database. The Configuration tool requests the following database information:

- Location of the database server
- Name of the database
- User ID for accessing the database server
- Password for accessing the database server

A configuration file containing the specifics of the database connection is created. You will need to share this file for distribution with each Certify client.

If you did not purchase the SAP MasterContent database, you will use the Apply.exe utility to install the database scripts in the Database Scripts directory in the Worksoft Certify Site Prep.zip file. Your database administrator may want to review each script before populating the database.

▶ *To create a Certify database with the Apply.exe tool:*

1 Locate the Apply.exe utility within your Certify Enterprise distribution folder:

```
...\Worksoft Certify Site Prep\Site Prep\Database Scripts\CertifyDatabase
```

2 Double-click **Apply.exe**.

The Apply tool opens.

3 In the text fields, enter the following database connection information:

- Database server name
- Database name

4 If using the Windows authentication security option, select the option. Go to Step 6.

5 If you selected SQL database authentication, enter the database user name and password in the text fields.

6 Click **Start**.

The Apply utility begins to create the new database.

If patches need to be applied, refer to the Readme file included with the patch to upgrade your database.

Populating Your Certify Database

After creating your database, you will populate your Certify database. If you purchased Worksoft's SAP MasterContent database, then you will populate your database through the SQL Server Management tool.

▶ *To create a Certify database from the SAP MasterContent database:*

1. Launch SQL Server Management Studio from **Start > All Programs > Microsoft SQL Server**.

   The SQL Server Login dialog opens.
2. Connect to the server where the database you are creating for Certify will reside.
3. Right-click **Databases** and select **Restore Database**.

   The Restore Database dialog opens.
4. In the Destination for Restore section of the General page, enter the new database name.
5. In the Source for Restore section, select **MasterContent.bak**.

   Depending on the software version, the exact file name will vary. You may need to use the **Browse** button to select your database.
6. Click **OK**.

   The database is created.

   If patches need to be applied, refer to the Readme file included with the patch to upgrade your database.

Upgrading Your Database

When you upgrade the Worksoft Certify application, Worksoft recommends upgrading all of your Certify databases, including the Certify results archival folder, to the same version.

Before you install the Certify upgrade on your production server, you need to test and verify the upgrade release by doing the following tasks:

- Before you install Certify, execute your critical Certify processes using this test database to verify that the test machine is set up correctly. Take note of the test results prior to the upgrade.
- Create a full backup of your production Certify database.
- In a test environment, upgrade your Certify database and verify that it contains all your data, including variables, recordsets, layouts, processes, requirements, etc.
- Execute your critical Certify processes again to see if the results are still the same as before the upgrade. If you have a number of discrepancies, do not proceed with the upgrade and notify Worksoft Support.
- Once the tests are complete and you have verified the upgrade works, you are ready to upgrade your production server. Before upgrading your production machine, all users must be signed out of the Certify production database.

▶ To upgrade your Certify database:

1 Locate the Apply.exe utility within your Certify distribution:

```
...\Worksoft Certify Site Prep\Site Prep\Database Scripts\UpdateDatabase
```

2 Double-click **Apply.exe**.

The Apply utility opens.

3 In the text fields, enter the following database connection information:

- Database server name
- Database name

4 If you will use the Windows authentication security option, select the option. Go to Step 6.

5 If you selected SQL database authentication, enter the user name and password in the text fields to access the database server.

6 Click **Start** to begin updating your database.

Maintaining Your Database

Worksoft provides database maintenance scripts to help improve Certify performance. These scripts allow you to:

- Archive results to a separate database
- Delete results

These database scripts are found in the following directory:

`SitePrep\Database Scripts\Results Maintenance`

Based on how Certify is being used, your database administrator determines whether to delete your results or archive them on a separate database. Database maintenance should be performed by the database administrator. For information on using these database maintenance scripts, see Worksoft Customer Support.

Compressing Images in Your Database

Certify compresses images without affecting the readability of the image content. Duplicate images are only saved once in the database. By storing only one copy of an image, lower storage space is used, and performance degradation is prevented.

New tables are created to store images, and they are mapped to the test step results. The existing LogImageData rows are changed to LogFileStream rows after you have upgraded your database.

Upgrading Your Database with over 500K LogImageData Rows

If you have over 500,000 LogImageData rows in your database, you need to use the upgrade and migration executables in the **UpdateDatabase - Post Upgrade Migration** directory.

▶ *To upgrade your large database:*

1. Locate the Apply.exe utilities within your Certify distribution package:

   ```
   ...\Worksoft Certify Site Prep\Site Prep\Database Scripts\UpdateDatabase - Post Upgrade Migration
   ```

2. Before you install the Certify upgrade on your production server, you need to test and verify the upgrade release.

3. Use the Apply.exe tool in the **1. Upgrade** directory to upgrade your database:

   ```
   ...\Worksoft Certify Site Prep\Site Prep\Database Scripts\UpdateDatabase - Post Upgrade Migration\1.Upgrade
   ```

4. After you have upgraded your database, use the Apply.exe tool in the **2. Migration** directory:

   ```
   ...\Worksoft Certify Site Prep\Site Prep\Database Scripts\UpdateDatabase - Post Upgrade Migration\2. Migration.
   ```

   After running the Post-Upgrade Migration scripts, screenshots can be viewed.

Transaction Log Settings

To ensure the transaction logs for the Certify database do not grow out of control and cause you to experience performance issues, perform the following:

- Set your maintenance plans to back up the transaction logs periodically.
- Optionally, change the recovery model of the Certify database to **Simple Recovery mode** so that you are able to maintain your transaction log growth and have less maintenance. Databases that have a Full Recovery mode will have substantially larger transaction logs.

  If your company's IT policy does not allow the database to run in Simple Recovery Mode, then use the Full Recovery mode. Verify that you have enough disk space for the log files on your database server.

Chapter 2 Preparing Your Application Server

In This Chapter

Configuring Your Application Server

In order to transform your application server into a web server to host Worksoft Certify, Microsoft® Internet Information Services (IIS) must be installed and the Server Manager must be configured.

These procedures assume that you have not already configured your IIS. If you have already set up the Roles and Features, verify that the following Role Services have been selected.

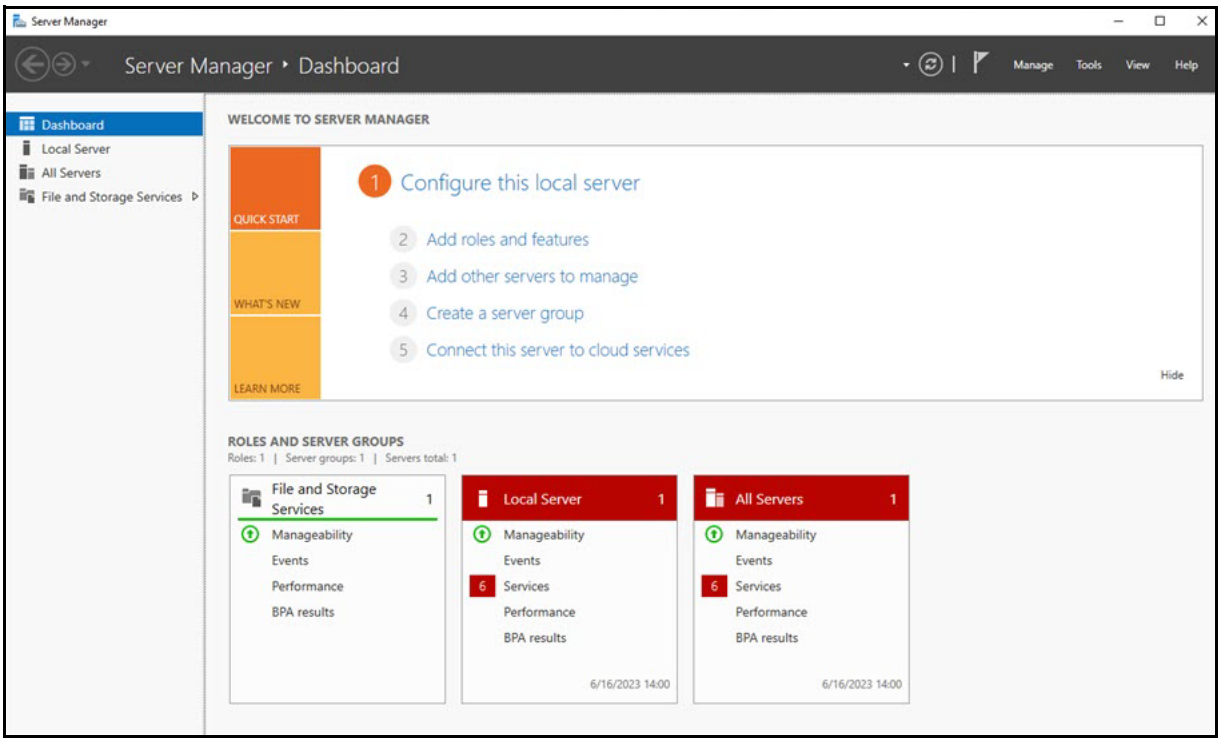
Adding Roles and Features

The Server Manager allows you to add specific roles and features to your web server that are required for Worksoft products.

▶ *To add roles and features to your web server:*

1 From the Start menu, select **Server Manager**.

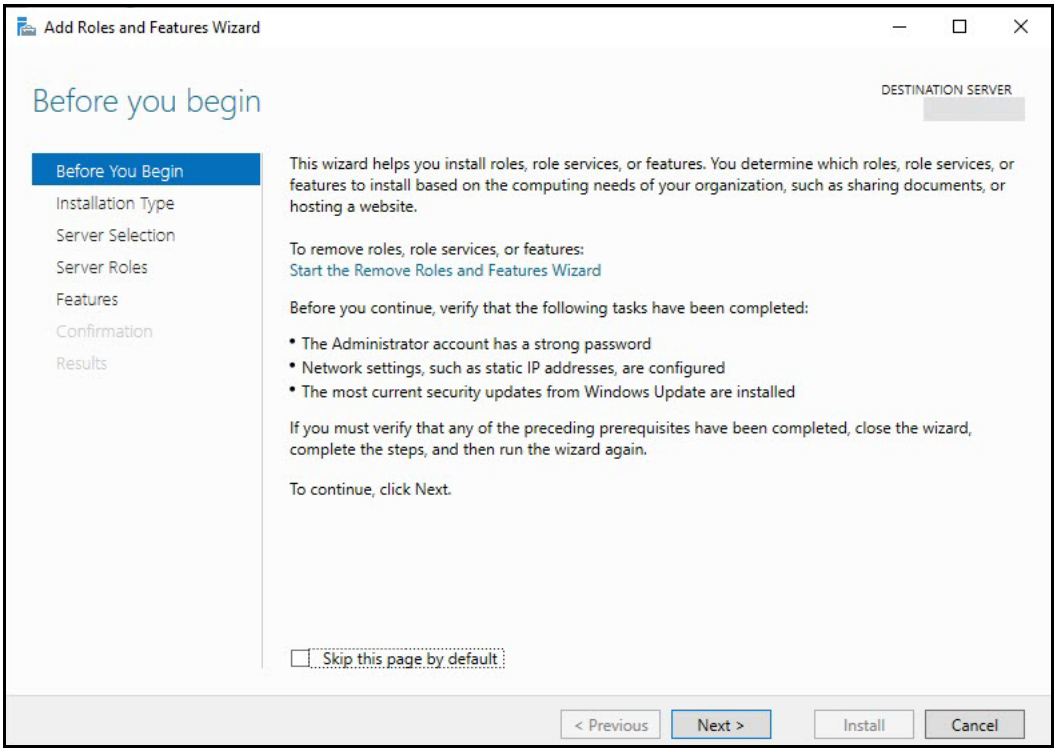
The Server Manager opens.



2 In the Navigation pane, select **Dashboard**.

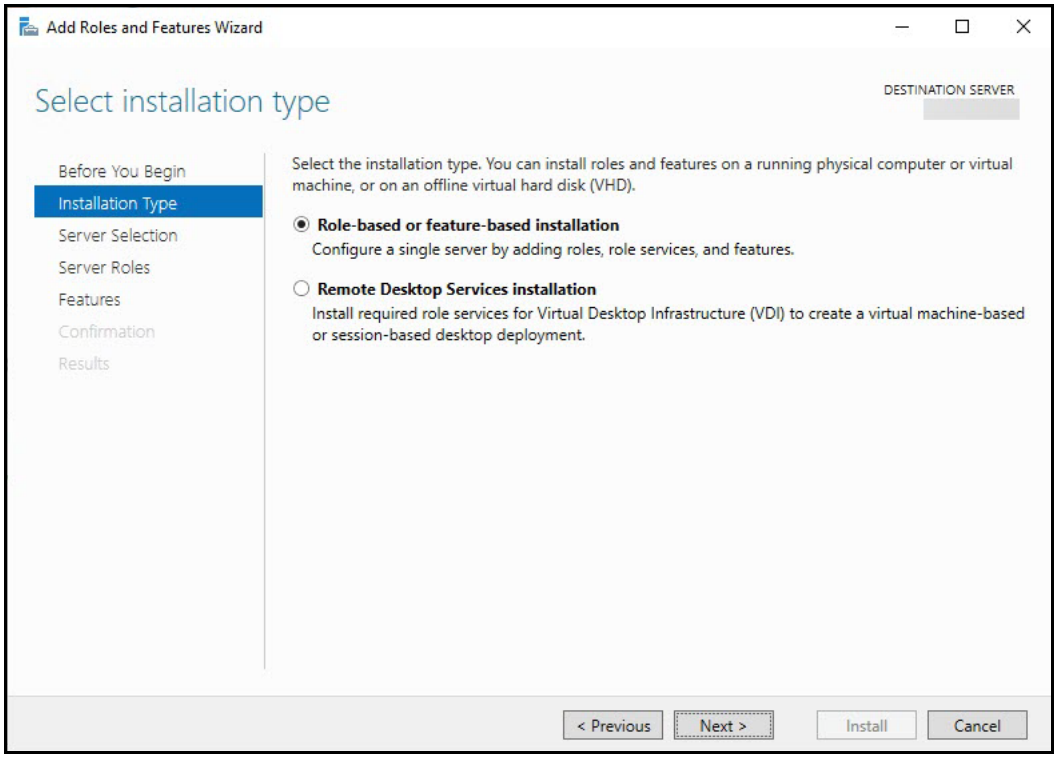
3 In the Summary Tasks pane, select **Add Roles and Features**.

The Add Roles and Features Wizard opens.



4 Click **Next**.

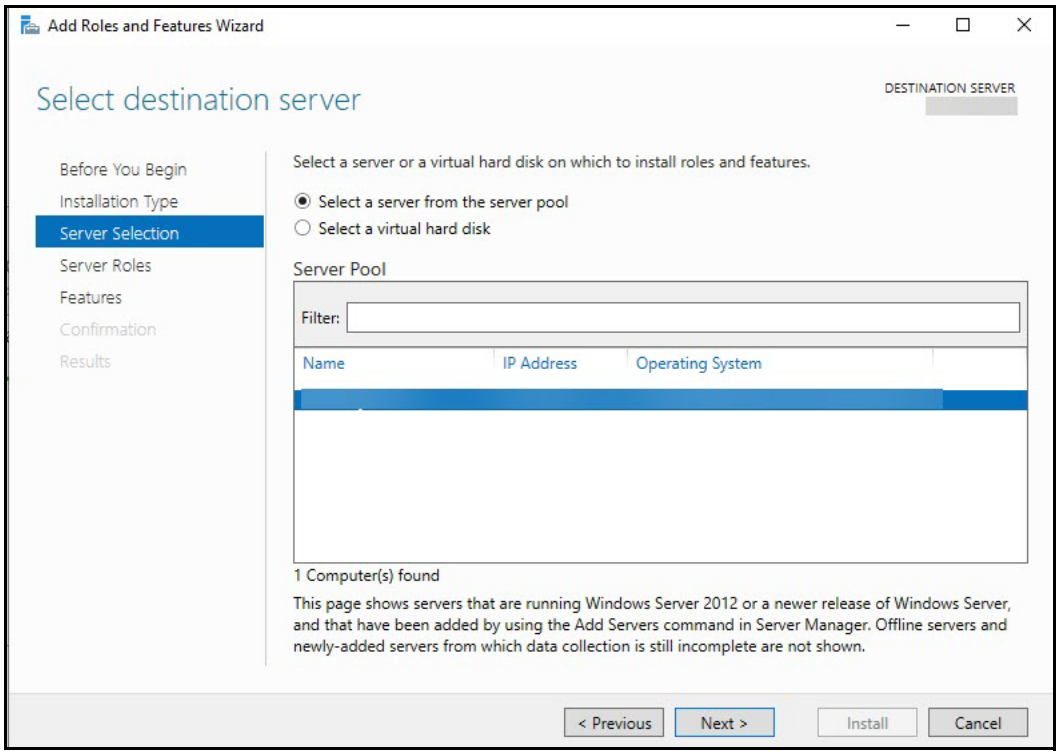
The Select Installation Type page opens.



5 Select the **Role-based or feature-based Installation** option.

6 Click **Next**.

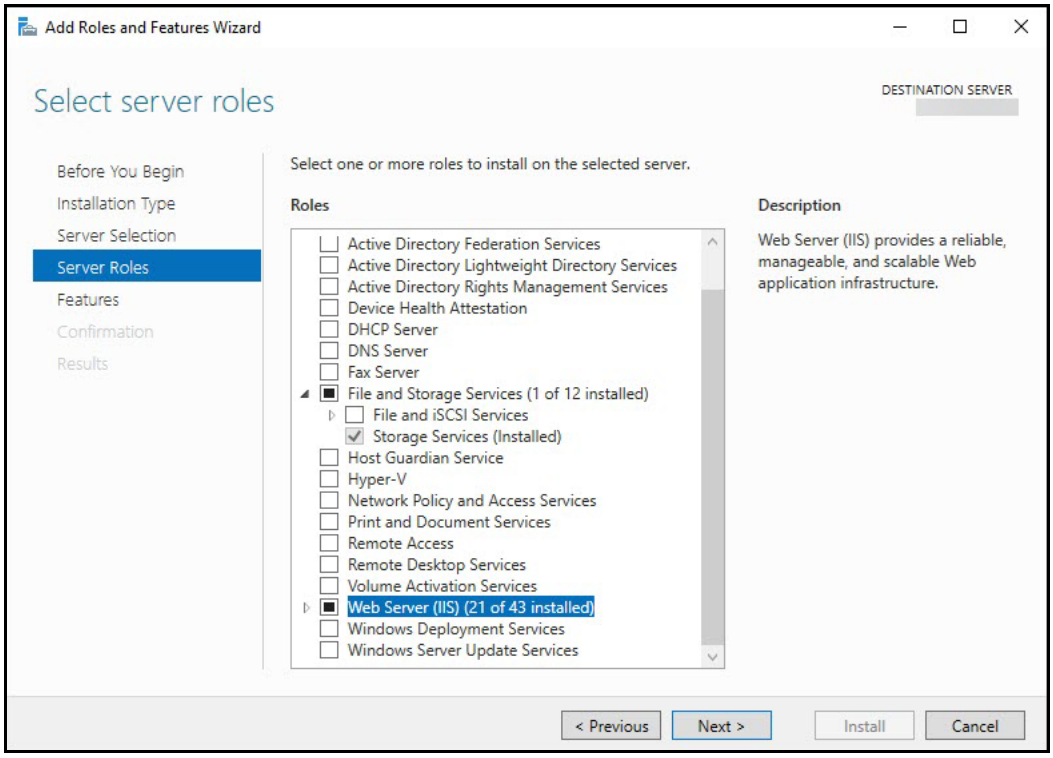
The Select Destination Server page opens.



7 Select a server.

8 Click **Next**.

The Select Server Roles page opens.

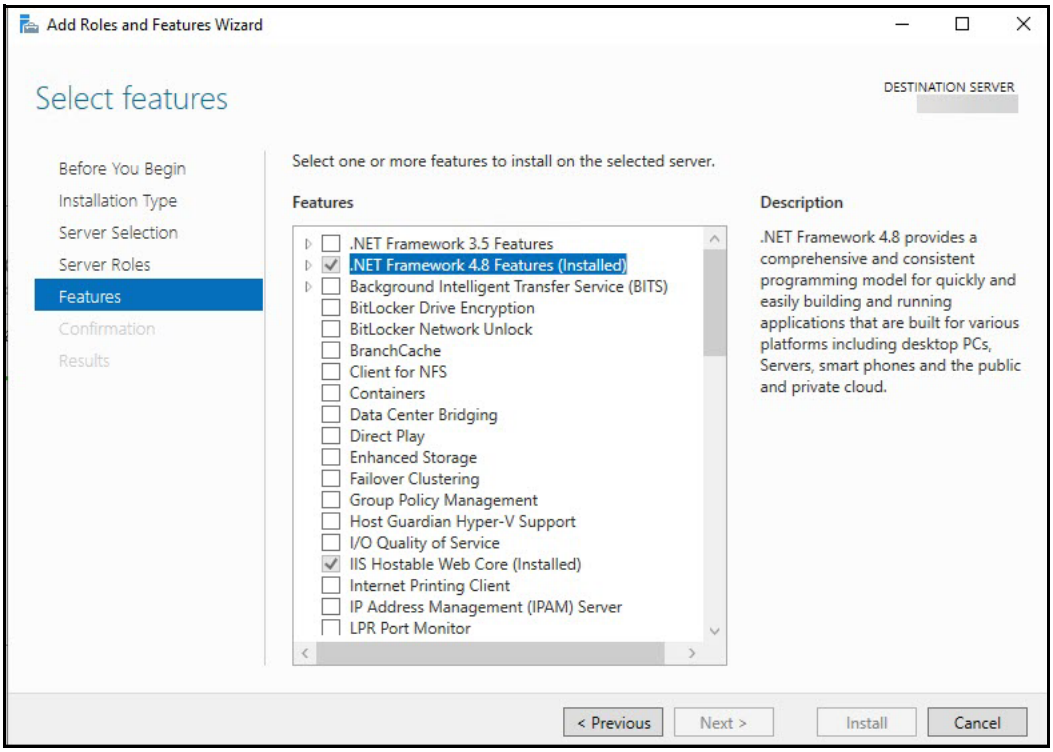


9 From the Server Roles list, select the following roles:

- **File Services**
- **Web Server (IIS)**

10 Click **Next**.

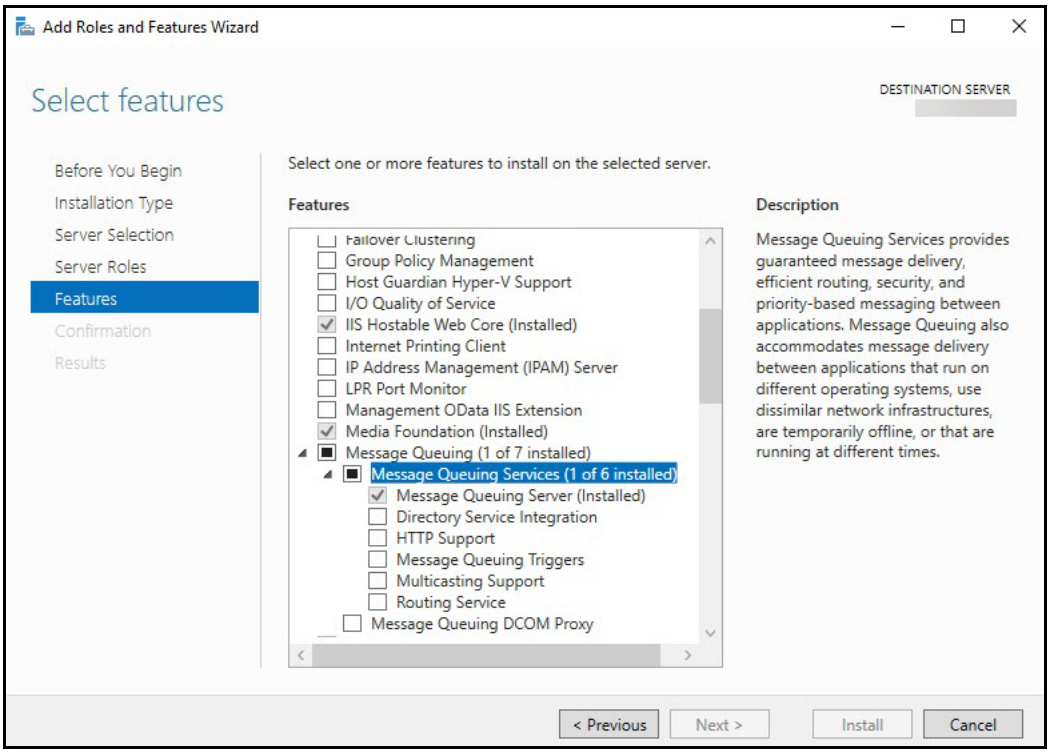
The Select Features page opens.



11 Select the following features:

- **.NET Framework 4.8 Features** and all of its child nodes
- **WCF Services** and all of its child nodes
- **IIS Hostable Web Core** and **Media Foundation**

12 Verify that **Message Queuing Services** and **Message Queuing Server** are enabled.



13 Use the scroll bar to verify the **Windows Process Activation Service** is enabled with the following child nodes:

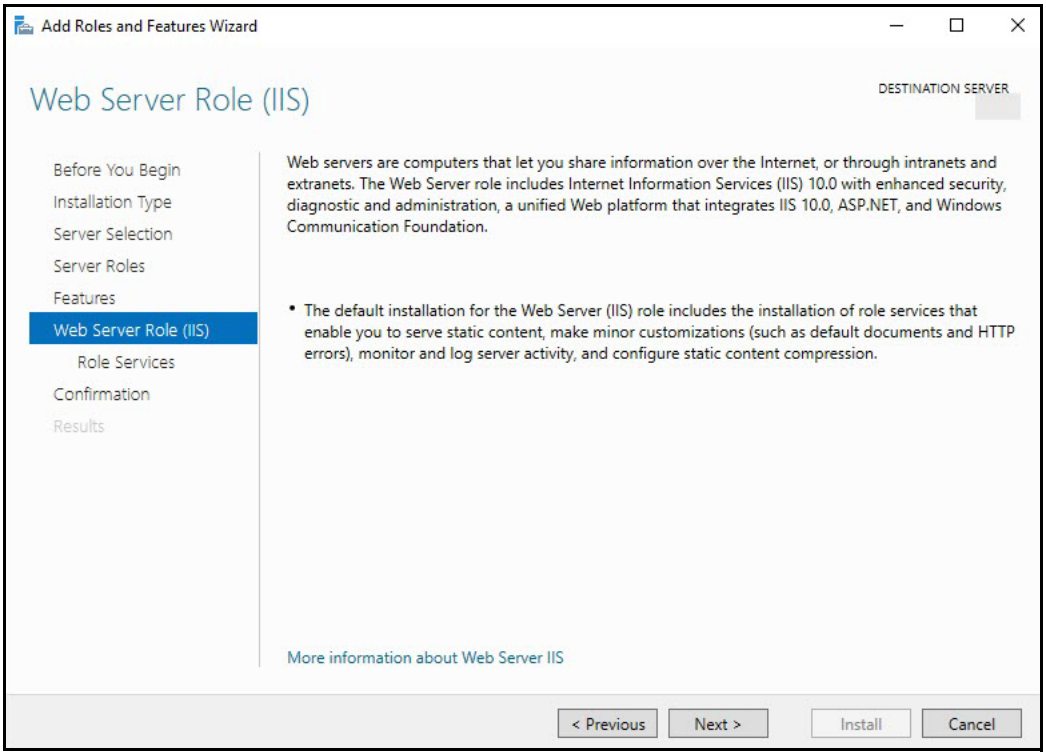
- **Process Model**
- **Configuration APIs**

14 Click **Next**.

Configuring the Web Server Role (IIS)

The Web Server Role (IIS) page opens if you have not already installed the web server.

1 In the Navigation pane, click **Role Services** under Web Server Role (IIS).



The Select Role Services page opens.

2 In the Role Services list, use the scroll bar to select the following services.

If you have already set up the Roles and Features, verify that the following services have been selected.

Node	Child Nodes
Common HTTP Features	Default Document Directory Browsing HTTP Errors Static Content WebDAV - Verify that this option is disabled. Worksoft's RESTful Services will not work correctly if enabled.
Health and Diagnostics	HTTP Logging Request Monitor
Performance	Static Content Compression Dynamic Content Compression
Security	Request Filtering Basic Authentication
Application Development	.NET Extensibility 4.8 Application Initialization ASP ASP.NET 4.8 CGI ISAPI Extensions ISAPI Filters WebSocket Protocol
Management Tools	IIS Management Console IIS Management Scripts and Tools Management Service

3 Click **Next**.

The Confirm Installation Selections page appears.

4 Click **Install** to install the role services.

Configuring Application/Json MIME Type Compression

After you have enabled Dynamic Content Compression within IIS, you need to verify HTTP Compression for the application/json MIME type. Certify Automator's mode uses Dynamic Content Compression to improve performance, and HTTP compression must be enabled for the application/json MIME type.

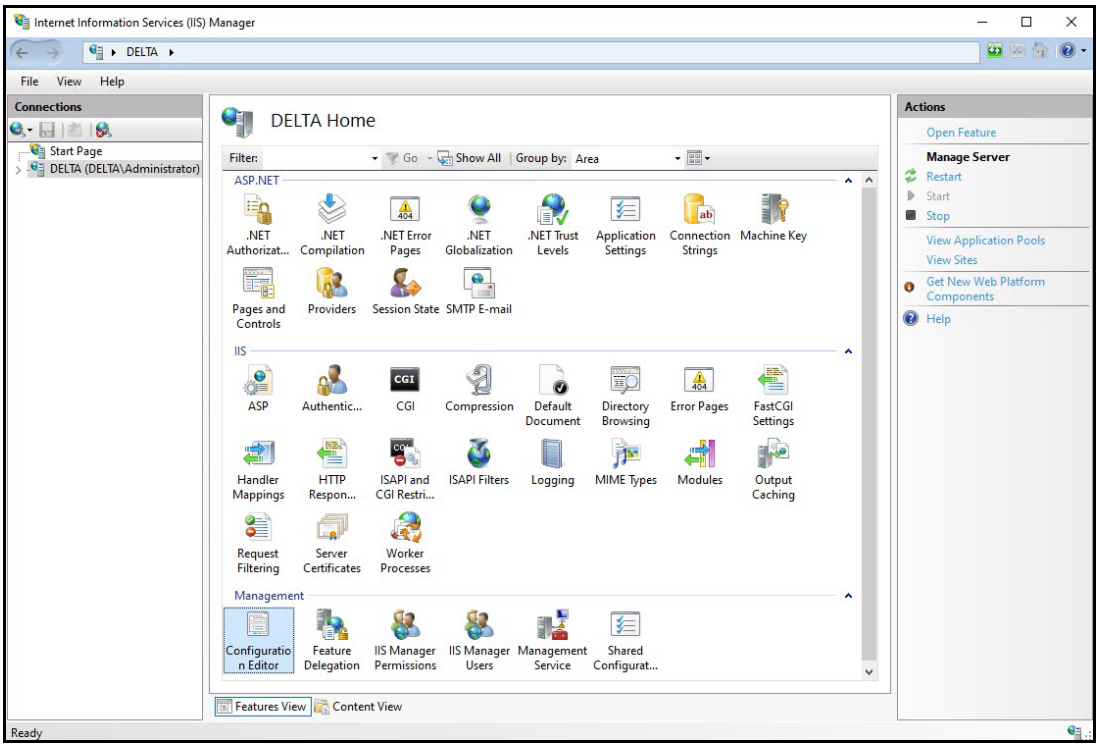
When the Dynamic Content Compression feature is enabled, it will overwrite any previous HTTP compression settings.

▶ *To verify application/json MIME type compression:*

1 Open **IIS Manager**.

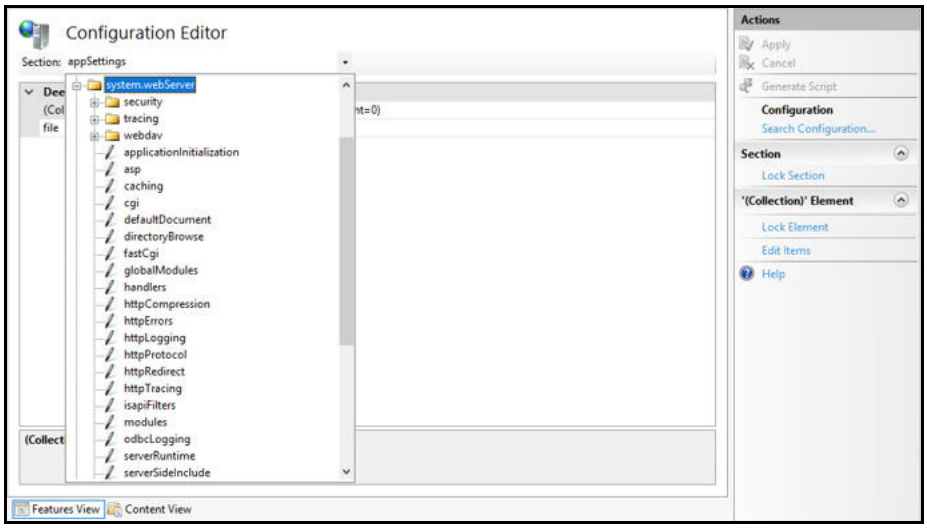
2 In the left Navigation pane, click on your server.

3 In the Management section, double-click the **Configuration Editor**.

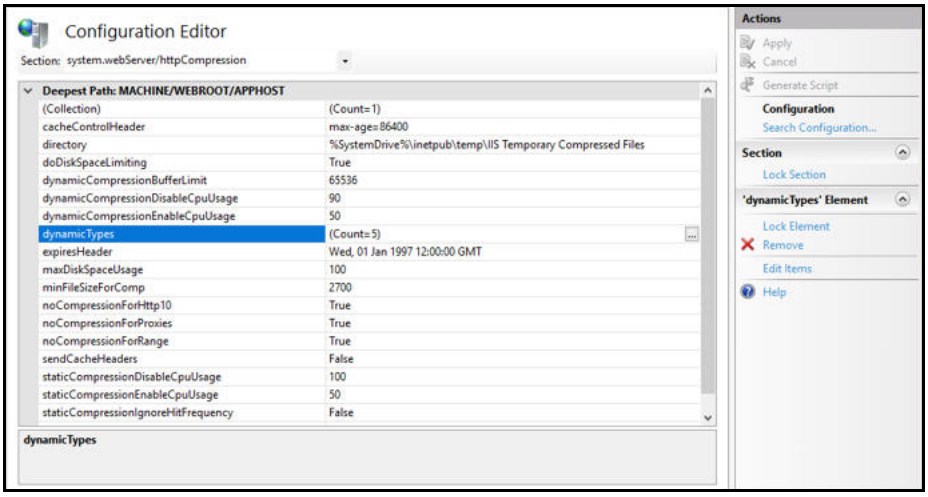


The Configuration Editor opens.

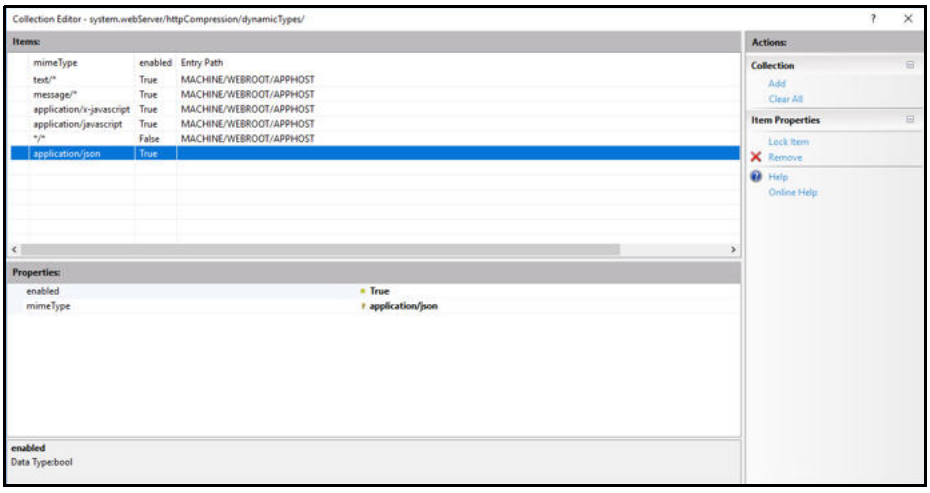
4 From the Section drop-down list, select **system.webServer > httpCompression**.



5 In the httpCompression section, click **dynamicTypes**.

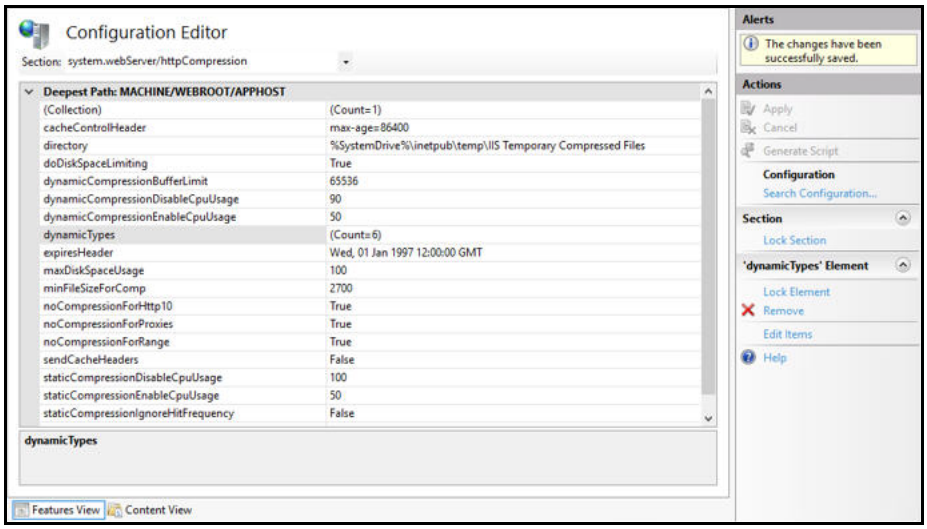


6 Verify that **application/json** is listed in the dynamic compression mime types. If it is not listed, click the **Add** button in the Collection section to add it.



7 After you completed your verification or addition, click the **Close** button

The Configuration Editor opens.



8 Click **Apply** to apply your changes.

9 Verify that dynamicTypes lists a count of six.

10 Close the editor.

Enabling IIS Services

You will now need to verify that several IIS services are enabled.

▶ *To verify IIS services are enabled:*

1 If the Server Manager is not open, select **Administrative Tools > Server Manager** from the Start menu.

The Server Manager opens.

2 In the Navigation pane, select **IIS**.

3 Scroll down to the Services section.

4 In the Services pane, verify that the following services are enabled and running:

- **World Wide Web Publishing Service**
- **Web Management Service**
- **Application Host Helper Service**
- **Windows Process Activation Service**

5 If any of these window services are not running, start the services.

To start a service, select the service from the list and click **Start** in the right menu. You can also start services by going to **Administrative Tools > Services** on your machine.

Chapter 3 Installing Worksoft Certify Services

In This Chapter

Overview

This chapter contains information on how to install and configure Worksoft Certify Services, which consists of the following services:

- **AutoUpdates**

  Administrators can upgrade all Certify clients by using Worksoft Certify Auto Update. For more information, see the Worksoft Help Portal.

- **Certify Web API**

  Certify automates functional testing across all enterprise applications and interfaces, and it validates critical business processes to ensure that they work.

- **Certify Results API**

  Certify Results API allows you to view Certify results and generate reports without having Certify installed. Users can query a Certify database using RESTful API calls, and view result attributes, processes, and process attributes. Data is returned in JSON format for third-party reporting tools to display and provide calculations.

Installing Worksoft Certify Services

Before you install Worksoft Certify, you must install **Worksoft Portal**. The Worksoft Portal is an administration tool that registers the following information for Worksoft products:

- Database settings
- Licenses
- Users
- Groups
- Email SMTP settings
- Tenants
- Integrations

Certify leverages this information from Worksoft Portal. Go to the Worksoft Customer Portal to download Worksoft Portal.

For system requirements and installation guides, go to the Worksoft Help Portal.

▶ *To install Worksoft Certify Services:*

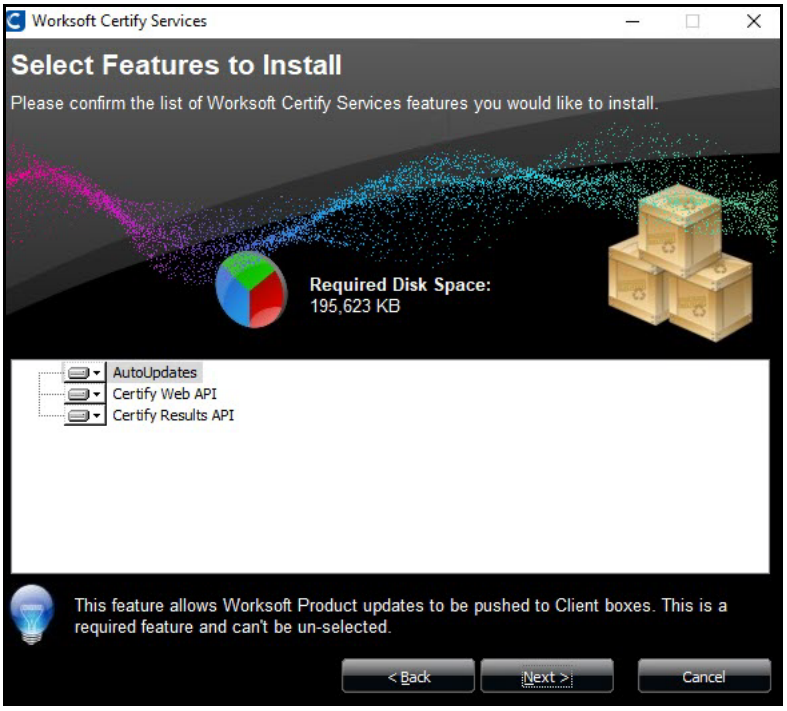
1 In your software distribution directory, open the **Certify Services** directory.

2 Right-click the **CertifyServices.exe** file and select **Run as administrator**.

The Worksoft Certify Services Install Wizard opens.

3 Click **Next** to begin the installation process.

The Select Features to Install page opens.



4 Select the Certify Services features that you want to install.

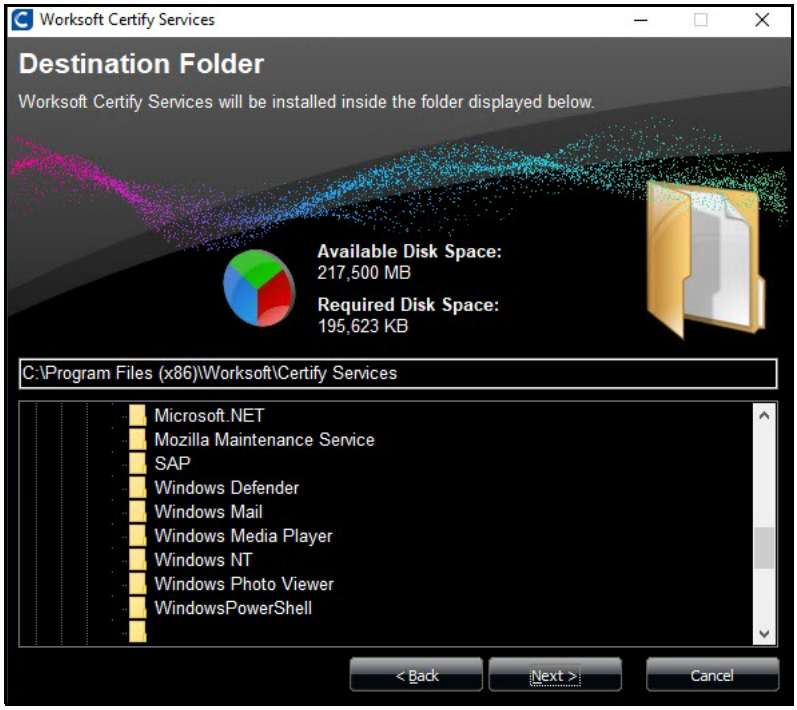
By default, all three services are installed.

If you do not want one of the services installed, click the arrow next to that feature and select **Entire feature will be unavailable**.

AutoUpdates can not be removed. The AutoUpdates is disabled unless you enable it. For more information, see the Worksoft Help Portal.

5 Click **Next**.

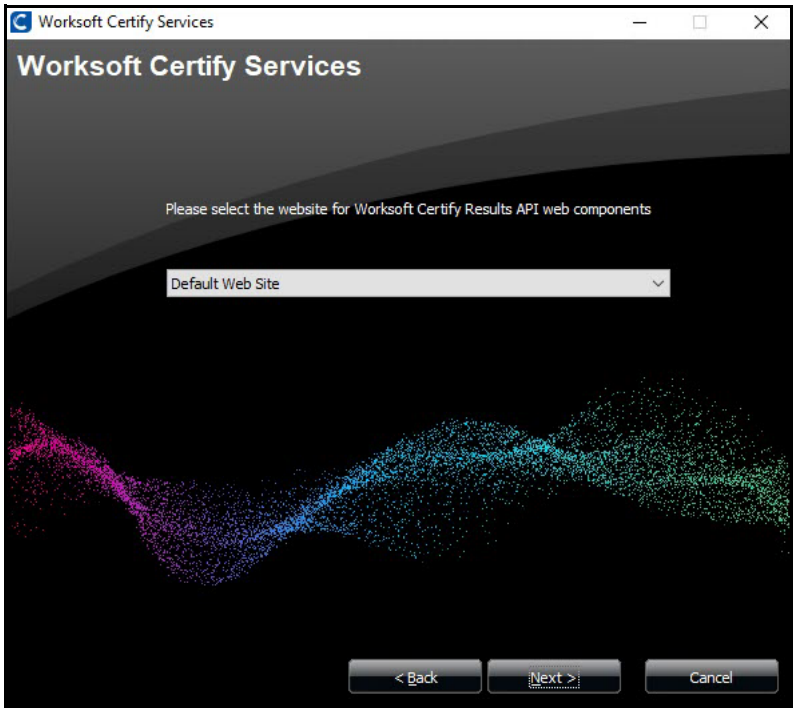
The Destination Folder page opens.



6 If you want to accept the default directory for your installation files, click **Next**.

If you do not want to accept the default directory for the installation files, select a different installation directory and click **Next**.

The Worksoft Certify Results API Web Site Components page opens.



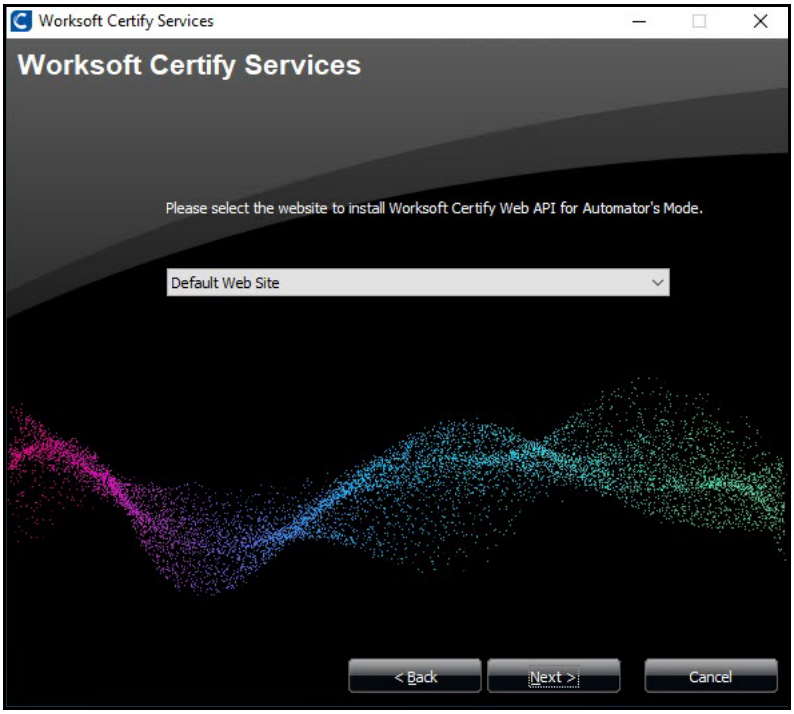
7 If you want to use the virtual default application that the installer creates, keep the value **Default Web Site**.

If you created a custom web site, then select your site from the drop-down list.

Worksoft recommends that you manually create your web site through IIS so that port numbers are handled properly. If you choose to create a web site from this page by entering a new name, the default port 80 is assigned to this web site.

8 Click **Next**.

The Worksoft Certify Web API for Automators Web Site page opens.



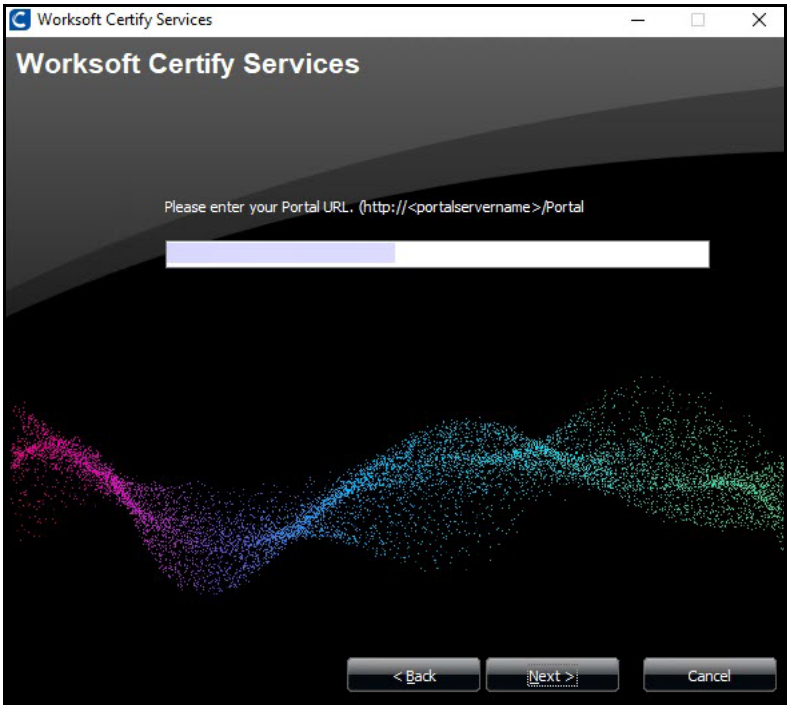
9 If you want to use the virtual default application that the installer creates, keep the value **Default Web Site**.

If you created a custom web site, then select your site from the drop-down list.

Worksoft recommends that you manually create your web site through IIS so that port numbers are handled properly. If you choose to create a web site from this page by entering a new name, the default port 80 is assigned to this web site.

10 Click **Next**.

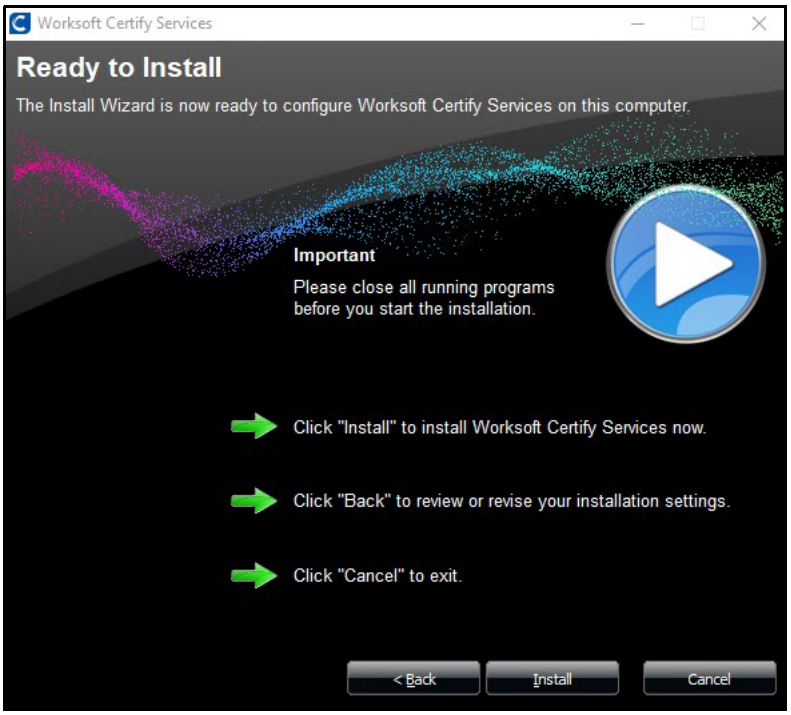
The Worksoft Portal URL page opens.



11 If you do not have Worksoft Portal installed, click **Next**.

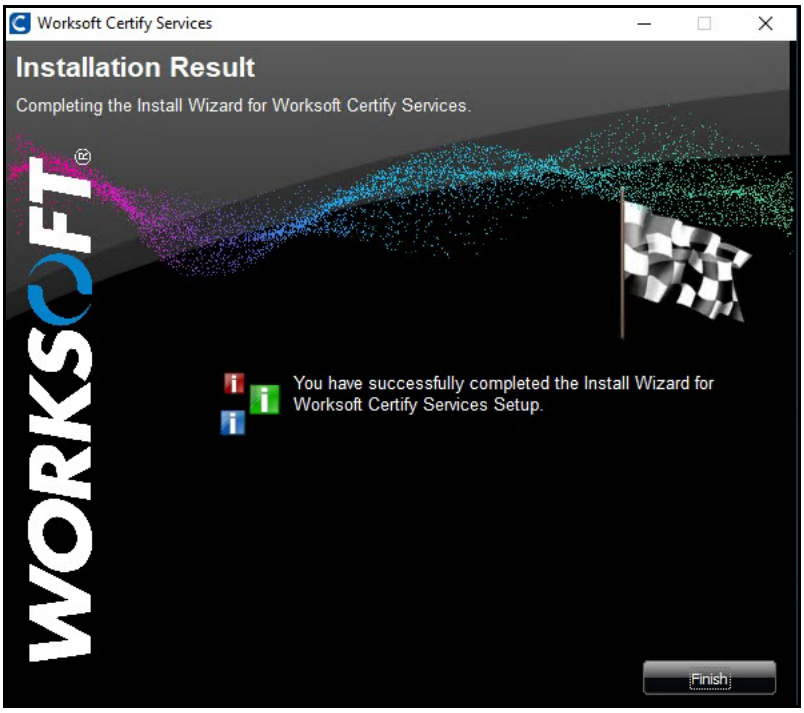
If you do have Worksoft Portal installed, enter the URL address and click **Next**.

The Ready to Install page opens.



12 Click **Install** to begin the installation.

After the installation completes, the Installation Result page opens.



13 Click **Finish**.

Verifying IIS Settings

You need to verify the following IIS settings:

- UploadReadAheadSize setting
- Preload Enabled setting is set to true.

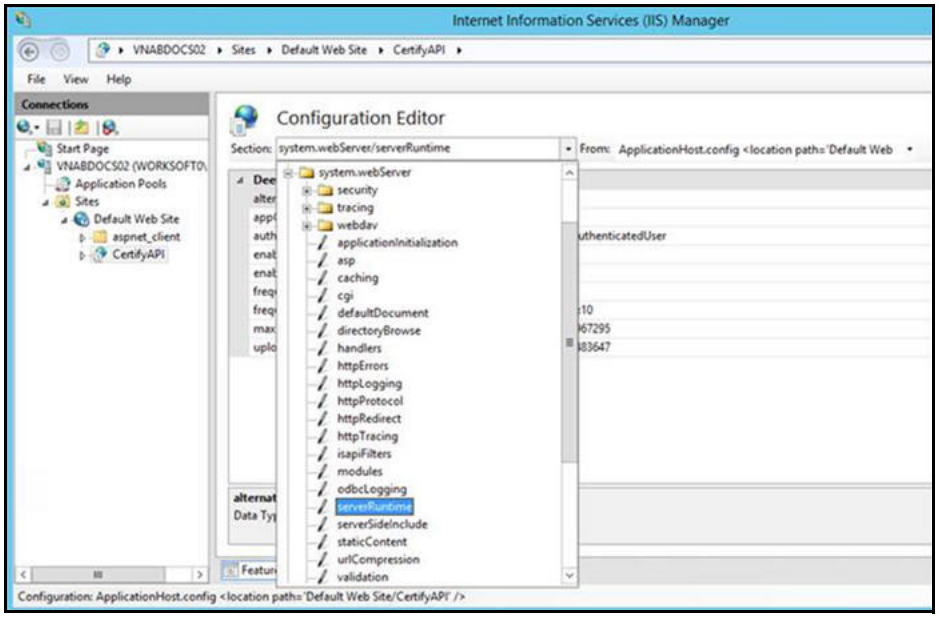
▶ *To verify your UploadReadAheadSize setting:*

1 Open IIS Manager.

2 In the Connections pane, select **Sites > Default Web Site > CertifyAPI**.

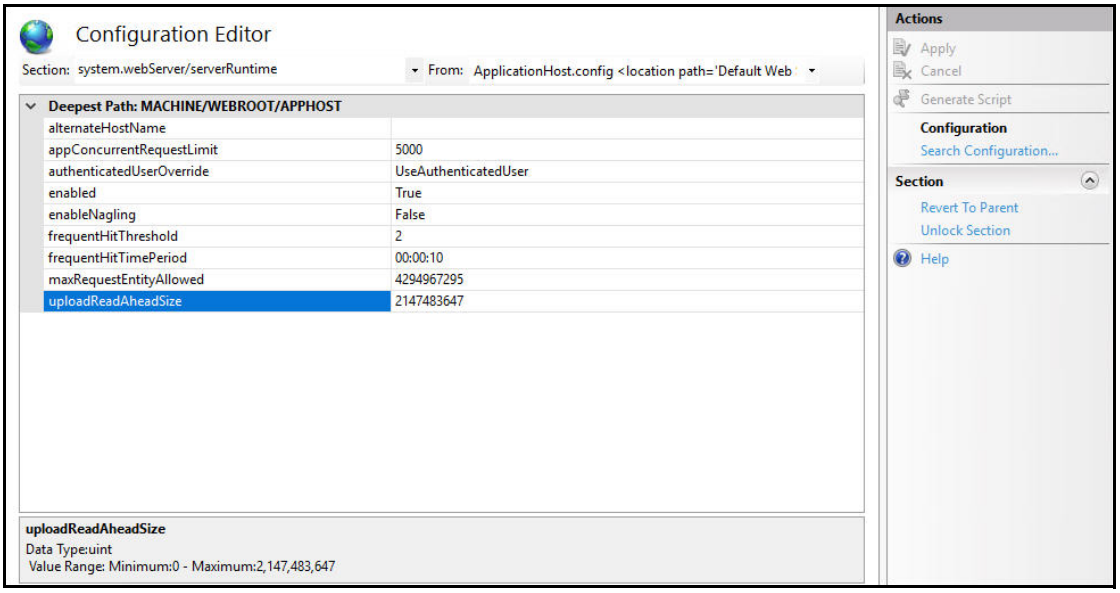
3 In the Management section, double-click **Configuration Editor**.

The Configuration Editor opens.



4 From the Section drop-down list, select **serverRuntime**.

5 Verify that the uploadReadAheadSize value is set to **2147483647**.



6 Close the Configuration Editor after you have verified the value.

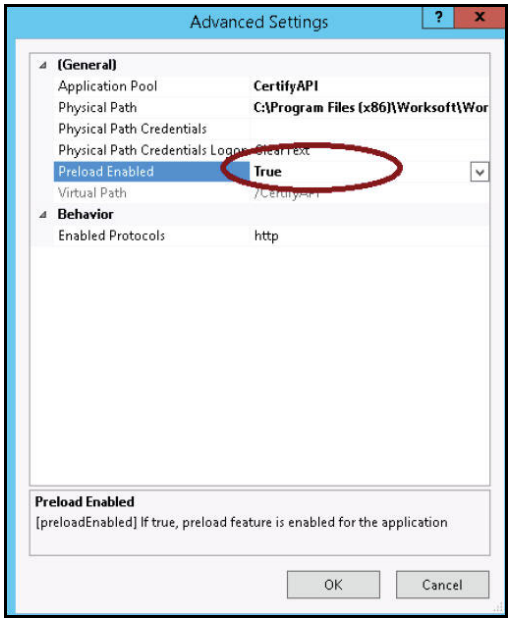
▶ *To verify the Preload Enabled setting:*

1 Open IIS Manager.

2 In the Connections pane, select **Sites > Default Web Site > CertifyAPI**.

3 In the Actions pane, select **Advanced Settings**.

The Advanced Settings dialog opens.



4 Verify that the Preload Enabled setting is set to **True**.

5 Click **OK**.

Using Windows Authorization

If you want to use Windows authorization for your SQL server, you need to complete the following:

- Update the Web.config file
- Set up a service account
- Enable Windows Authentication in IIS
- Configure application pool setting
- Configure SQL Server access

▶ *To update the Web.config file:*

1 Open the following directory:

```
C:\Program Files(x86)\Worksoft\Certify Services\Certify Web API
```

2 Open the **Web.config** file in a text editor.

3 In the update system.web section, you need to set the following:

- authentication mode = Windows
- identify impersonate = false

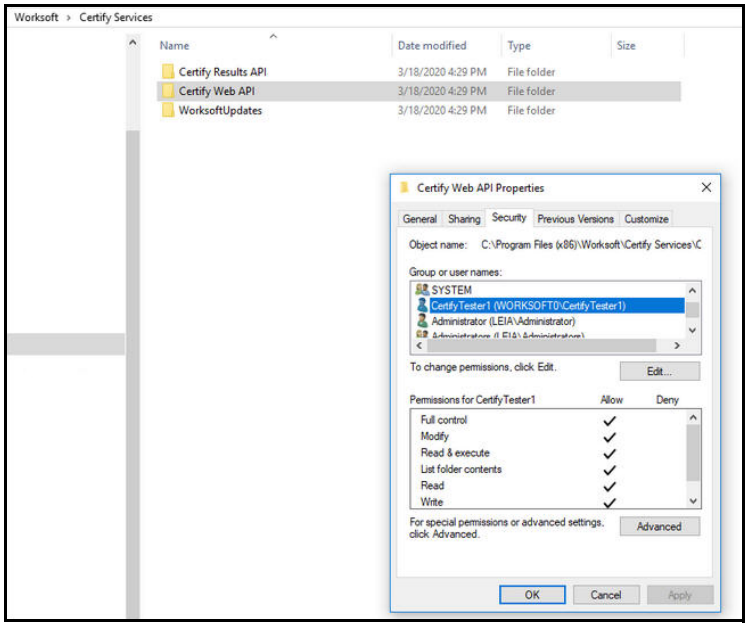
See example below:

```
<system.web>
…….
<authentication mode="Windows"/>
<identity impersonate="false"/>
</system.web>
```

▶ *To set up a Service account for Certify Services:*

You must create a Service account to execute API requests. Example: **`CertifyTester1\worksoft0`**

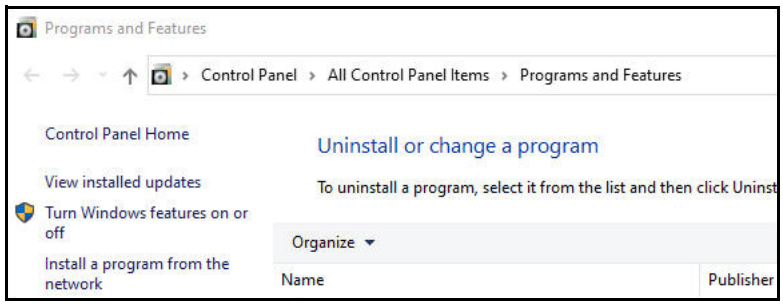
After installing Certify Services, sign in to the Certify API Server and provide **Full** control to the Certify Web API directory above the Service account as shown below.



▶ *To enable Windows Authentication in IIS*

1 From the Start menu, select **Control Panel > Programs and Features**.

The Programs and Features window opens.



2 Click **Turn Windows features on or off**.

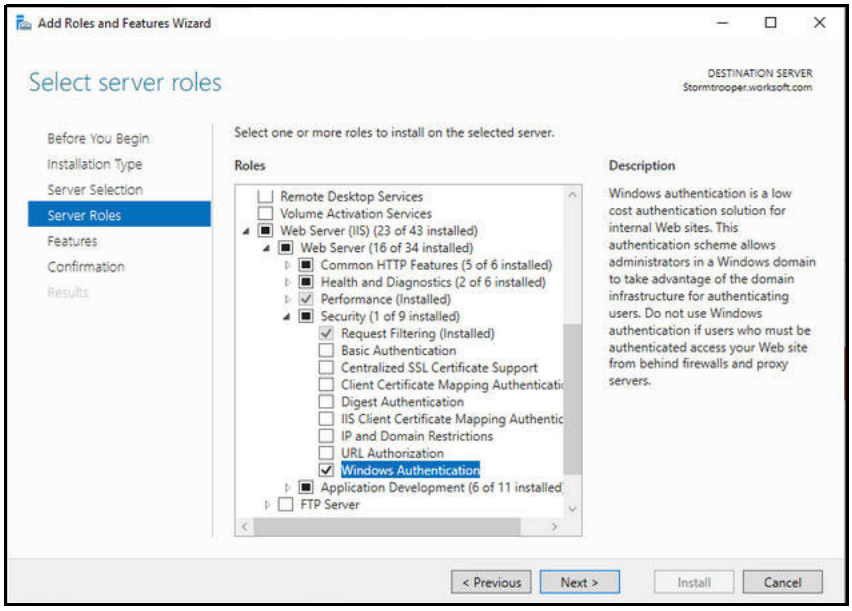
The Windows Features dialog opens.

3 In the Features list, expand **Internet Information Services > World Wide Web Services**.

4 Select **Add Roles and Features**.

The Add Roles and Features Wizard opens.

5 Click **Next** until come to the **Server Roles** page.



6 Expand the **Web Server IIS** role.

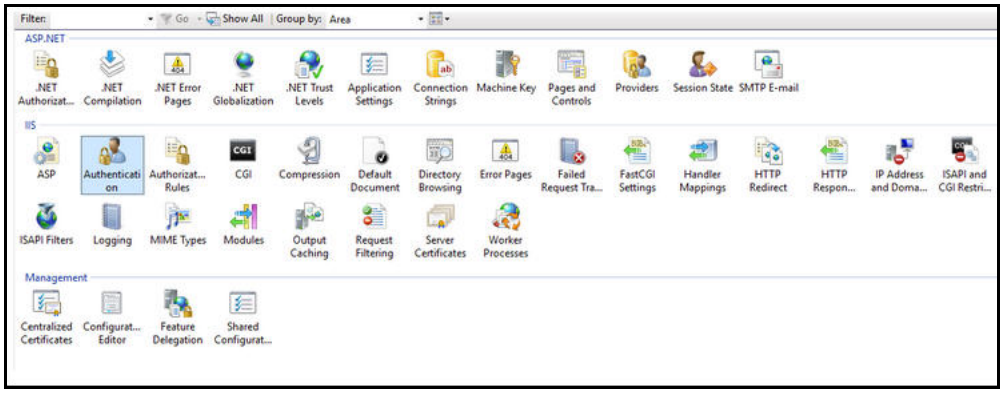
7 Under Security, select the **Windows Authentication** option.

8 Click **Next** until the Install option is enabled.

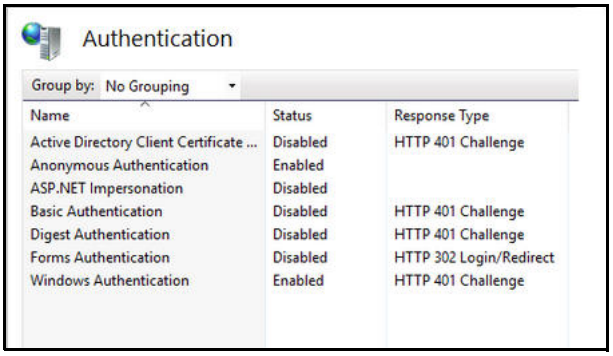
9 Click **Install** to complete the configuration.

10 Open the **IIS Manager**.

11 Click **Authentication**.

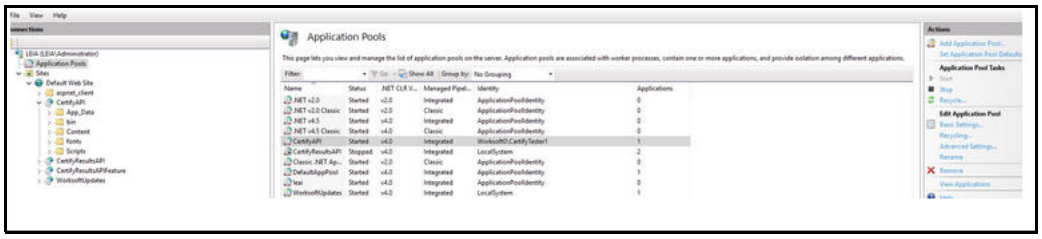


12 Enable **Windows Authentication** and disable all other Authentications.

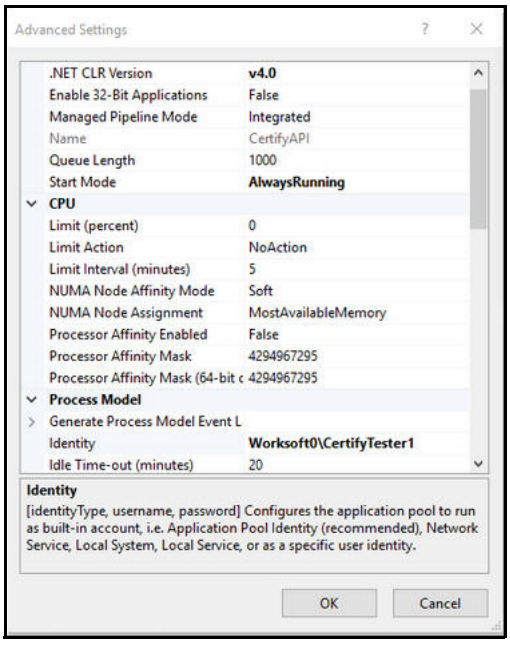


▶ *To create a custom account application pool setting:*

1 Select **Application Pools > CertifyAPI**.

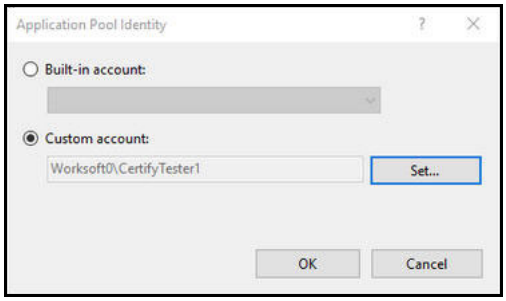


2 In the Edit Application Pool section, select **Advanced Settings**.



3 Select **Identity** from the list.

The Application Pool Identity dialog opens.



4 Select **Custom account**.

5 Click **Set**.

The Set Credentials dialog opens.

6 Enter the Service account user name and password.

7 Click **OK**.

8 In the Set Credentials dialog, click **OK**.

9 In the Advanced Settings dialog, click **OK**.

▶ *To configure SQL Server access:*

Your database administrator needs to add the Service account to Logins under Security in order to provide access to the Certify database.

Troubleshooting

If you are having trouble with Worksoft Certify Services, open your Worksoft Certify API URL in a browser to verify that your meta data appears:

```
https://<servername>/CertifyAPI/odata/$metadata
```

Chapter 4 Installing and Configuring the Worksoft Certify Client

In This Chapter

Installing Worksoft Certify Client

Verify that the recommended system requirements are met on each computer where the Certify client will run. Go to the Worksoft Help Portal to view the system requirements.

You must have full administrator rights on the computer in which you plan to install Certify.

▶ *To install the Worksoft Certify client:*

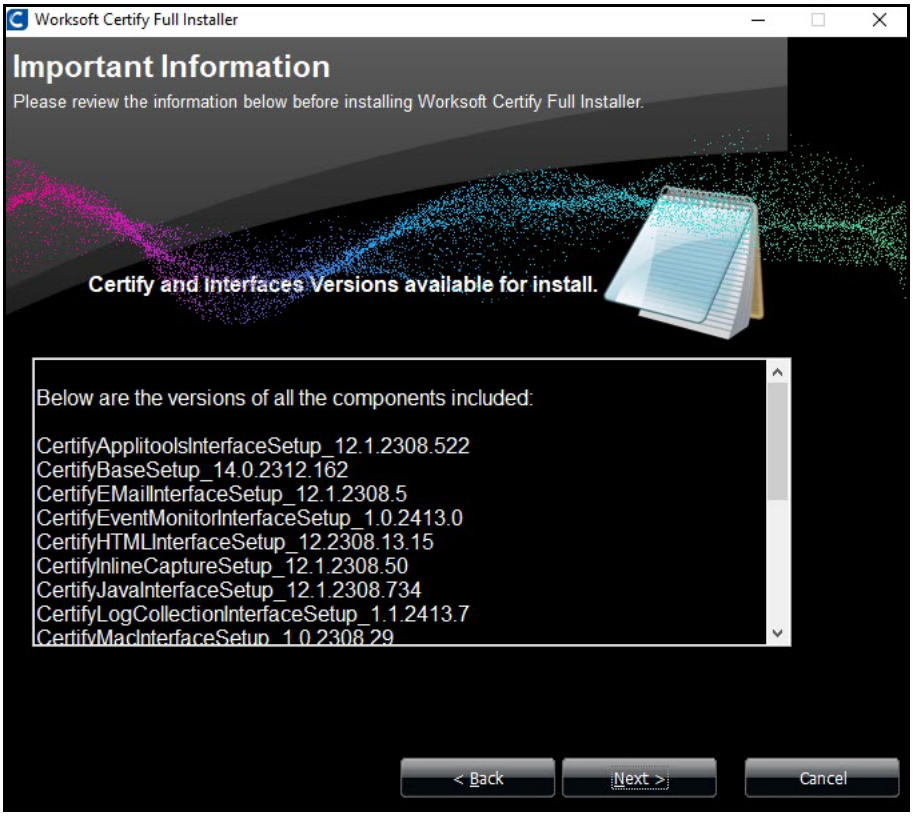
1 If needed, temporarily disable anti-virus software and close all open applications on your computer.

2 Right-click the **CertifySetup.exe** file and select **Run as Administrator**.

The Worksoft Certify Install Wizard opens.

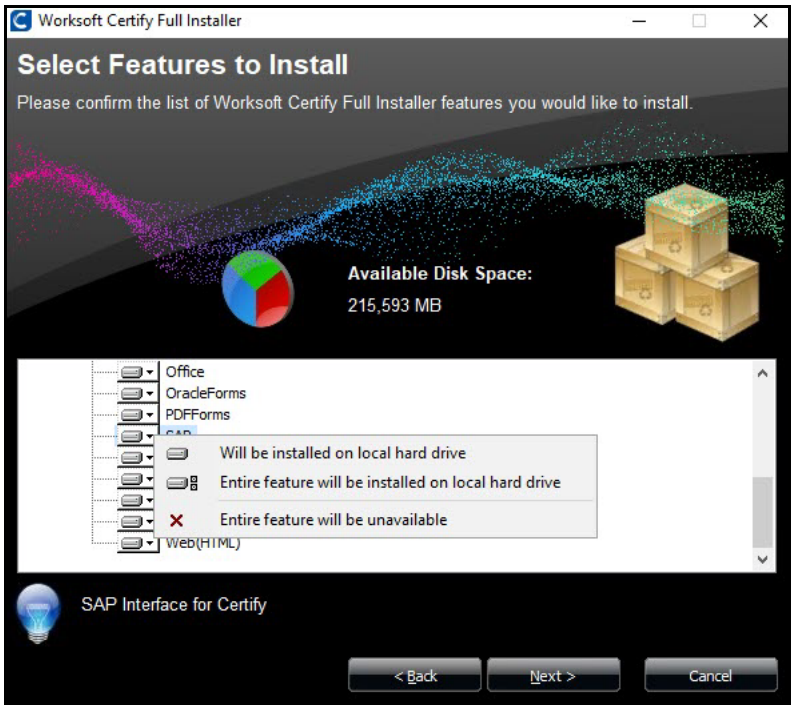
3 Click **Next**.

4 The Important Information page opens.



5 Review the information and click **Next**.

The Select Features to Install page opens.



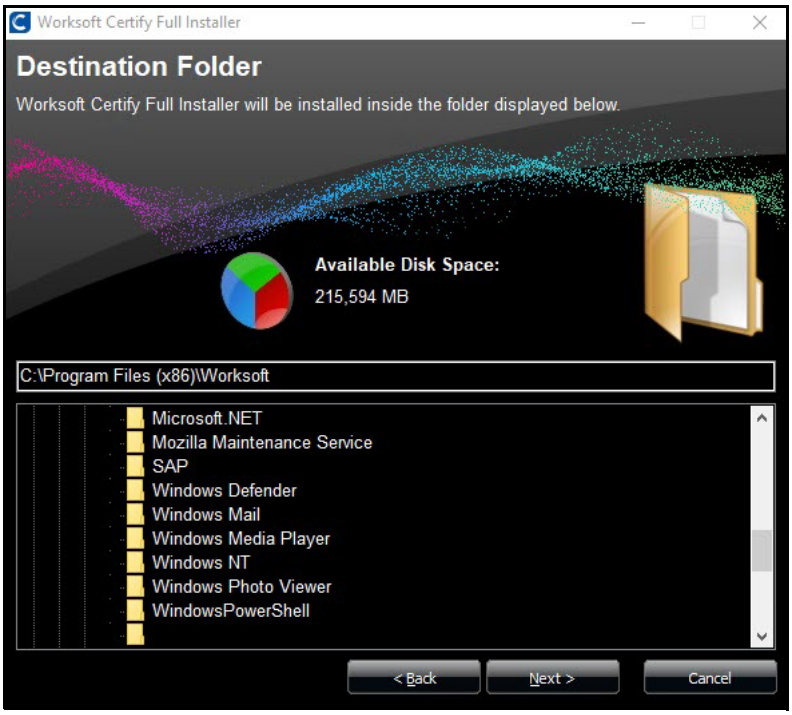
6 Select the features and interfaces you want to install. By default, all interfaces are selected for installation.

7 If you do not want to install one of the features or interfaces, click the drop-down arrow next to it and select **Entire feature will be unavailable**.

When you select a product or service, a description appears under the list.

8 Click **Next**.

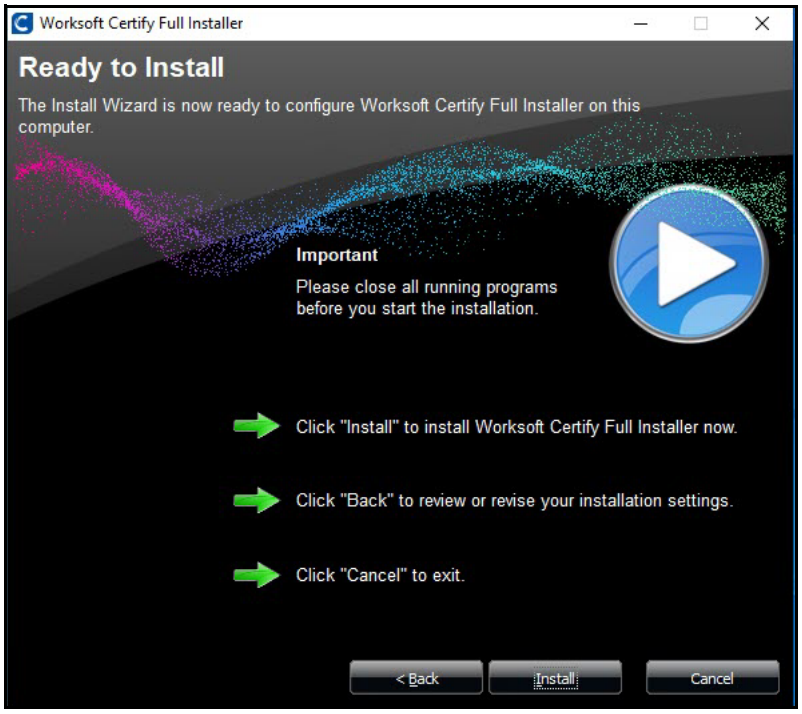
The Destination Folder page opens.



9 If you want to accept the default directory for your installation files, click **Next**.

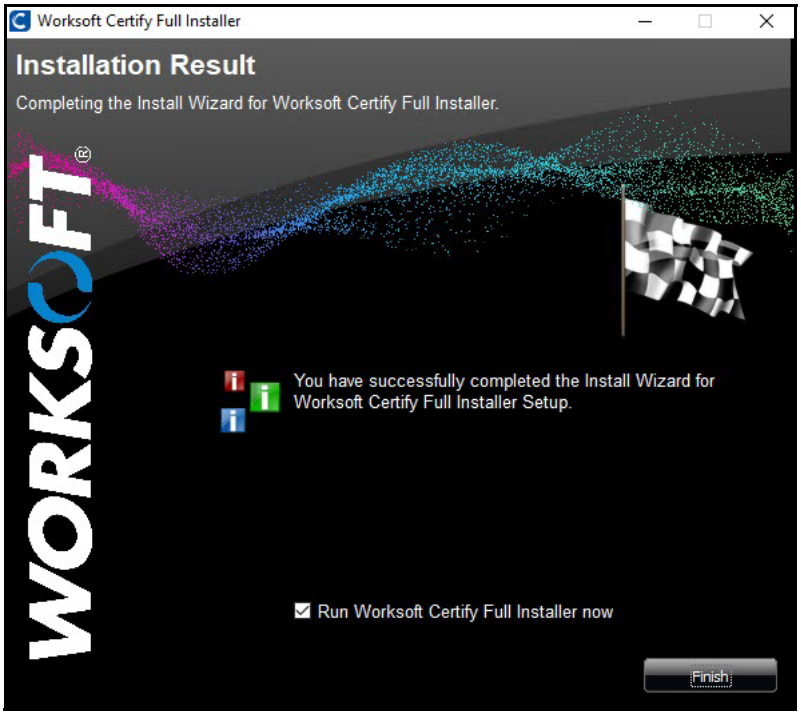
If you do not want to accept the default directory for the installation files, select a different installation directory and click **Next**.

The Ready to Install page opens.



10 Click **Next** to begin the installation.

The installation completes, and the Setup Complete page opens.



11 If you do not want to open Certify, cancel the **Run Worksoft Certify Now** option.

12 Click **Finish**.

You are now ready to configure your Certify test environment.

Configuring the Worksoft Certify Client

After you have installed Worksoft Certify, you must configure the following settings with the Certify Configuration tool:

- Database
- Licensing
- Auto Update

The Certify Configuration tool creates a file named **Worksoft.Certify.exe.config**. You can find this file in your `C:\Program Files (x86)\Worksoft\Certify\Client` folder.

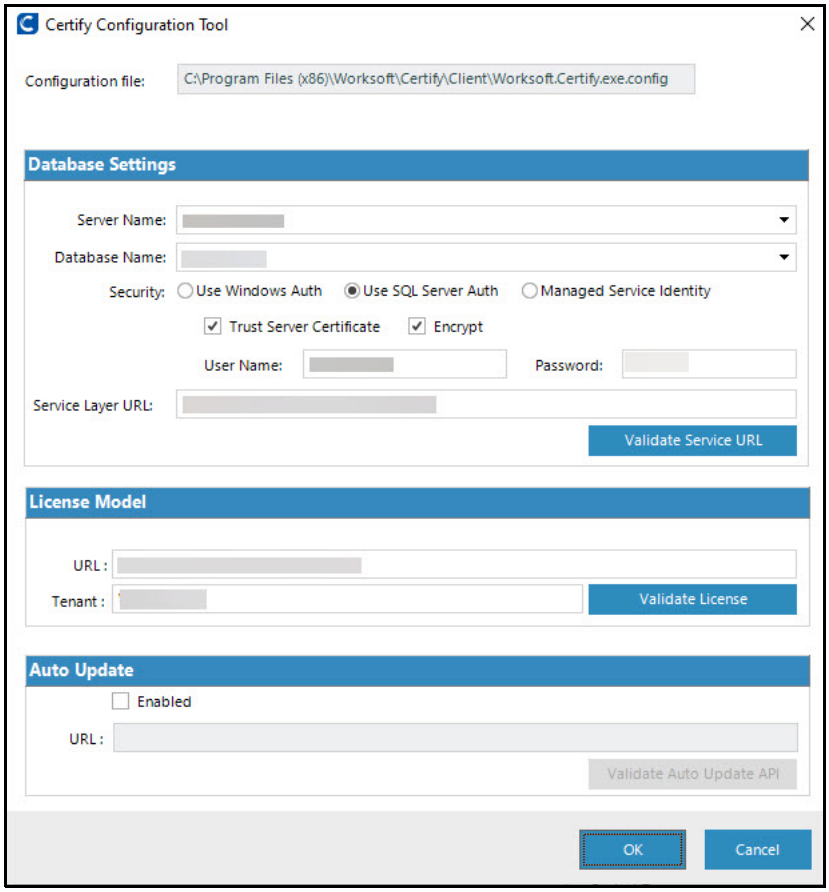
The configuration settings control access to the Certify system, database, the license server, and web server. Current settings are created at the time of installation.

▶ *To configure the Worksoft Certify client:*

1 Open Worksoft Certify by double-clicking on the **Certify** desktop icon.

2 From the Certify menu, select **Configure > Certify > Database and Licensing**.

The Certify Configuration tool opens.



3 In the Server Name field, select a database server from the drop-down list or enter a server name.

4 In the Database Name field, enter a database name or select a database from the drop-down list.

Before you can select a database from the drop-down list, you must set up your security authentication. Go to **Step 5**.

5 In the Security section, select one of the following security authorizations and enter the needed information:

Security Option	Description
Use Windows Auth	Use Windows authentication.
Use SQL Server Auth	Use SQL Server authentication. Enter the SQL Server user name and password in the respective fields.
Managed Service Identity	Use Managed Service Identity authentication. In the User ID field, enter the ID.

6 If you selected to use Windows authorization or SQL Server authorization, you must select the **Trust Server Certificate** option

By choosing this option, the client trusts the certificate the server provides. While this option allows encrypted connections to the database server, it bypasses security between the client and server.

By default, SQL Server automatically installs a self-signed certificate that can be used by default. However, some organizations may want to install a custom certificate.

7 If you selected to use Windows authorization or SQL Server authorization, you must select the **Encrypt** option.

A certificate must be installed on the SQL Server to encrypt the communication channel from the Certify API to the SQL Server database.

8 In the Service Layer URL field, enter the URL address for the web server that is hosting Worksoft Certify Services.

Example: `https://servername/certifyapi`

9 Click **Validate Service URL** to test your connection.

10 In the License Model section, enter the Worksoft Portal URL and tenant information.

Use **Default** as your tenant name unless you already have tenants created.

Example: `https://servername/Portal`

11 Click **Validate License** to test the connection.

If for some reason the test fails, troubleshoot the license server connection.

12 If you want to enable the Worksoft Certify Auto Update service, select the **Enabled** option in the Auto Update section.

Enter the URL address for the web server that is hosting Worksoft Certify Services with **/worksoftupdates** in the address.

Example: `https://servername/worksoftupdates`

13 Click **Validate Auto Update API** to test the connection.

For information on how to configure Worksoft Certify Auto Update, see Enabling Worksoft Certify Auto Update.

14 Click **OK**.

A message opens stating that you need to restart Certify to save your configuration.

15 Click **Yes** to close Certify.

16 Open Certify and sign in again.

Configuring Interfaces

Before you begin using Certify, you need to verify that your machine has the system requirements installed and configured for the interfaces you plan to use. To view interface system requirements, see the Worksoft Help Portal.

For information on how to configure interfaces, see the Worksoft Certify Interfaces section in the Worksoft Help Portal.

Distributing Worksoft Certify Installation Files

If you are installing Worksoft Certify on multiple workstations, create a directory on a shared drive to distribute the following files:

- Worksoft Certify installer - **CertifySetup.exe**
- Worksoft Certify configuration file - **Worksoft.Certify.exe.config**

These files must be located in the same folder in order for Certify to install correctly.

▶ *To distribute the Certify client installation files to users:*

1 Create a **CertifyInstall** directory on a shared drive and provide access to all Certify users.

2 From the Worksoft Certify package, copy **CertifySetup.exe** and paste it into the **CertifyInstall** folder.

3 Copy the **Worksoft.Certify.exe.config** file from the single workstation where you installed Certify and paste into the CertifyInstall folder.

This file is located in the following folder:

```
C:\Program Files (x86)\Worksoft\Certify\Client
```

4 Notify the Certify users of the following:

- Name and location of the CertifyInstall directory
- Instructions for installing Certify

Deploying Worksoft Certify Client Updates

You can deploy Worksoft Certify updates by creating a master desktop image.

Some IT organizations create a master desktop image of a user's machine with a Worksoft Certify client installed. This image should be considered a single client machine.

To deploy the new patch package, you must start the Certify client at least once. If you do not start the Certify client, the files will not be placed in the correct directories, and any DLL files will not be registered.

Chapter 5 Using a Citrix Server Environment

In This Chapter

Overview

This chapter provides you with the following information needed if you are using Worksoft Certify client with Citrix XenApp®:

- Configuring your Citrix server
- Accessing Worksoft Certify client through the Citrix client
- Troubleshooting

Verify that the recommended system requirements are met on each computer where the Certify client will run. Go to the Worksoft Help Portal to view the system requirements.

Configuring Your Citrix Server

When using Worksoft Certify in a Citrix XenApp environment, all applications that Certify needs to access must be shared in the same Citrix session ID with Certify. Worksoft recommends using Citrix in the Published Desktop mode with Certify so that no additional configuration will be needed.

You will need to install the following applications on the same Citrix server:

- Worksoft Certify client
- Any application under test, such as an SAP GUI application
- Any third-party tool, such as SmartBear® Software TestExecute™ or Microfocus Application Lifecycle Management®

If you cannot run Citrix in Published Desktop mode, enable sharing in the Citrix session. Install Certify and all required applications on the same Citrix server to ensure applications are shared on the same Citrix session ID.

Setting Your Citrix Server to Install Mode

Before you install Worksoft Certify client to a Citrix machine, the machine must be in the **Install** mode.

▶ *To set your Citrix server to Install mode:*

1. Sign in to the Citrix server as a local administrator.
2. Open a **Command Prompt** window as an Administrator.
3. To put your Citrix server to Install mode, enter `change user /install` in the Command Prompt window.
4. Press **<Enter>**.

   Your server is now in the Install mode, and you are ready to install Certify. For more information, see Chapter 4, "Installing and Configuring the Worksoft Certify Client," on page 39.

Setting Your Citrix Server to Execute Mode

After installing Certify, you need to set your Citrix Server to **Execute** mode.

▶ *To set your Citrix server to Execute mode:*

1. Restore the **Command Prompt** window.
2. To put your Citrix server to Execute mode, enter **`change user /execute`** in the Command Prompt window.
3. Press **<Enter>**.

   Your server is now in the Execute mode.
4. Close the Command Prompt window.

Accessing Worksoft Certify Through the Citrix Client

Worksoft Certify client, the application under test, and any third-party applications must be published on the Citrix server as an application. You do not need to publish Certify Learn utilities because they can be launched from the Certify menu. To access the Certify command line functionality in Citrix, export the batch file and then publish the batch file as a Citrix-published application.

Each application that you publish must use an explicit user. Worksoft does not recommend using an anonymous user because customizations and user preferences will be lost after the user logs out.

Depending on Citrix configuration, Certify can be accessed through the Citrix client two ways:

- Signing in to a published desktop
- Using Certify as a published application

Signing in to a Published Desktop

No additional configuration is needed if you select to access Certify by logging on to a published desktop. During a remote desktop session, Certify will interact with any other applications are running in the same unique session.Using Certify as a Published Application

As a published application, Certify can not be accessed through a remote desktop session, and it will only interact with other published applications launched in the same client's unique session. Certify will be unable to interact with any local application running on the client machine.

Like most Windows applications, the Certify client needs write access to the Application data directory for the user. Under recommended settings from Citrix, the Application data directory should be writable and maintained across the Citrix farm for each Citrix user using the Roaming profile. For more information on the best practices for setting up profile types, see http://support.citrix.com/article/CTX110351.

Troubleshooting

This section provides solutions to issues that you may encounter when using Citrix XenApp with Certify.

Issue: After installing the Certify client, Certify will not start and reports Unhandled Exception errors when trying to connect to the database server.

Cause: Your Citrix server may not be able to reach the Domain Name Server (DNS) for your system to resolve server names into IP addresses.

Solution: Verify that the Citrix server can access your DNS to resolve server names. If you can not access your DNS, then change the names of the license server and the database server in the Worksoft.Certify.exe.config file to the actual IP addresses. After you have made these changes, you will need to restart Certify.

Issue: Screen captures in Certify reports display as "black boxes" with screen fields and other objects displayed as white outlines on the screen.

Cause: The Citrix server's desktop display color depth is less than 16-bit.

Solution: The minimum supported resolution for Certify screen captures in Citrix is 16-bit.

Issue: Running the SAP interface and receive the following error, "wsTest.Main: wsSAP.dll cannot be loaded".

Cause: Worksoft Certify was installed by a user without the required administrator permission, or Worksoft Certify was not installed through the Windows Control panel.

Solution: Sign in as the server administrator and reinstall Certify using the Windows Control panel.

Issue: Certify SAP and HTML Learn utilities are not working, and an error message opens.

Cause: You do not have permissions to open the utilities on the Citrix machine.

Solution: Open permissions on your Citrix machine for the following directory:
`C:\Program Files\Worksoft`.

Chapter 6 Using a Windows Terminal Server Environment

In This Chapter

Configuring Your Terminal Server

This chapter provides information on configuring your Terminal Server to work with the Worksoft Certify client.

Before you begin using your Terminal Server with Certify, the following applications must be installed on the same server:

- Worksoft Certify client
- Any application under test, such as an SAP GUI application
- Any third-party tool, such as SmartBear® Software TestExecute™

Verify that the recommended system requirements are met on each computer where the Certify client will run. Go to the Worksoft Help Portal to view the system requirements.

Setting Your Terminal Server to Install Mode

When you install Worksoft Certify client to a Terminal Server, the machine must be in the **Install** mode.

▶ *To set your terminal server to Install mode:*

1. Sign in to the Terminal Server as a local administrator
2. Open a **Command Prompt** window as an Administrator.
3. To put your Terminal Server to Install mode, enter `change user /install` in the Command Prompt window.
4. Press **<Enter>**.

   Your server is now in the Install mode.

   Your server is now in the Install mode, and you are ready to install Certify. For more information, see Chapter Chapter 4, "Installing and Configuring the Worksoft Certify Client," on page 39.

Setting Your Citrix Server to Execute Mode

After installing Certify, you need to set your Terminal Server to **Execute** mode.

▶ *To set your terminal server to Execute mode:*

1. Restore the **Command Prompt** window.
2. To put your Terminal Server to Execute mode, enter `change user /execute` in the Command Prompt window.
3. Press **<Enter>**.

   Your server is now in the Execute mode.
4. Close the Command Prompt window.

Appendix A Worksoft Certify Firewall Port Settings

For Microsoft SQL Server, Certify uses the default port and protocol specified by the manufacturer. To permit Certify to work through a firewall, you must open the default TCP/IP port 1433. For more information, go to the following web site: http://support.microsoft.com/kb/287932

Specifying a SQL Server Port Number for Your Database

Microsoft provides a way to change this port number if TCP/IP port 1433 is already being used by another application in your network or if it is restricted in your network environment due to security constraints. For information on changing the default SQL Server port on the server itself, go to the following web site: http://support.microsoft.com/kb/823938.

After you change your port number, you need to modify your **Worksoft.Certify.exe.config** file with this new port number setting.

▶ *To modify the Worksoft.Certify.exe.config file to specify a different database server port number:*

1. In the `C:\Program Files\Worksoft\Certify\Client` folder, open the **Worksoft.Certify.exe.config** file in a text editor, such as Notepad.
2. Scroll down to the `<appSettings>` section and locate the line containing:
   `<add key = "DATABASESERVER", value = "{server name}" />`
3. Modify the value to specify the new port number by including a comma and the port number after the server name:

   ```
   <add key="DATABASESERVER" value="{server name},{port number}" />
   ```

   EXAMPLE:

   To specify that Certify connects to the SQL Server via port 1434, you would use:

   ```
   <add key="DATABASESERVER" value="localhost,1434" />
   ```

Appendix B Worksoft Certify Silent Installation

Certify Services

Silent Install

To run Certify Services installation silently, run the installer from the command line and add **/s** option to the executable:

```
CertifyServices.exe /s
```

To install specific component:

For Certify Web API:

```
CertifyServices.exe /s certifyapi=true
```

For Certify Results API:

```
CertifyServices.exe /s resultsapi=true
```

For Certify Results API with Worksoft Portal:

```
CertifyServices.exe /s Portal_URL=http://servername/portalsuite
```

Installation Log File

The default installation log is located at **%userprofile%** of the user who installed Certify Services. If you want to override the install log file location, enter the following string to provide an override for install log file location:

```
CertifyServices.exe /s /l=C:\temp\CertifyServicesInstalllog.txt
```

Silent Uninstall

To uninstall Certify Services silently, run the installer from the command line and enter the following string:

```
CertifyServices.exe /s MODIFY=FALSE REMOVE=TRUE
```

Both components are removed.

Certify Client

Silent Install

To run the Certify client installation silently, run the installer from the command line and add **/s** option to the executable.

Install all features (default) on default path (C:\Program Files (x86)\Worksoft):

```
<installerPath>\CertifySetup.exe /s
```

Install in non-default path:

```
<installerPath>\Install all features (default) on default path (C:\Program Files (x86)\Worksoft):
```

```
<installerPath>\CertifySetup.exe /s targetdir="C:\temp\Worksoft" (will install all the interfaces in their individual folders under C:\temp\worksoft
```

Interface selection during silent install:

When installing Certify using the installation wizard, all components are selected for installation unless the parameter value is set to "false."

Example:

```
<installerPath>\CertifySetup.exe /s AppliTools=false Email=false UIA=false Web=false
```

This example installs all interfaces except AppliTools, Email, UIA, and Web (HTML) interfaces.

Listed below are the interface parameters:

- AppliTools
- EventMonitor
- Java
- Mac
- Mobile
- Office
- PDFForms
- Silverlight
- UIA
- Web
- Email
- InlineCapture
- LogCollection
- Mainframe-LT
- NetUI
- OracleForms
- SAP
- SOAPUI
- Utilities

Installation Log File

The default installation log is located at **%userprofile%** of the user who installed Certify.

```
<installerPath>\CertifySetup.exe /s /l=C:\temp\myInstalllog.txt
```

Silent Uninstall

To uninstall the Certify client silently, run the installer from the command line and enter the following string:

```
CertifySetup.exe /s MODIFY=FALSE REMOVE=TRUE UNINSTALL=YES
```